

СПб ГУТ)))

всероссийская научно-методическая
конференция магистрантов и их руководителей

ПКМ

**ПОДГОТОВКА ПРОФЕССИОНАЛЬНЫХ КАДРОВ
В МАГИСТРАТУРЕ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ**

МАТЕРИАЛЫ КОНФЕРЕНЦИИ ПКМ-2022

СПб ГУТ)))

**ВСЕРОССИЙСКАЯ НАУЧНО-ТЕХНИЧЕСКАЯ И
НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ
МАГИСТРАНТОВ И ИХ РУКОВОДИТЕЛЕЙ**

**ПОДГОТОВКА ПРОФЕССИОНАЛЬНЫХ
КАДРОВ В МАГИСТРАТУРЕ
ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ
(ПКМ-2022)**



ПКМ

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

6 декабря – 8 декабря 2022 года

PKM.SUT.RU

**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ****ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-
БРУЕВИЧА»
(СПбГУТ)****Институт магистратуры**

УДК 621.39:004

ББК 32.74

Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2022). Всероссийская научно-техническая и научно-методическая конференция магистрантов и их руководителей; материалы конф. / Сост. Н.Н. Иванов. СПбГУТ. – СПб., 2023. – 1409 с.**ПРОГРАММНЫЙ КОМИТЕТ***Председатель***Машков Г.М.** – доктор технических наук, профессор, и.о. ректора СПбГУТ*Заместители председателя***Ивасишин С.И.** – кандидат технических наук, и.о. первого проректора – проректор по учебной работе СПбГУТ**Шестаков А.В.** – доктор технических наук, старший научный сотрудник, проректор по научной работе СПбГУТ*Ответственный секретарь***Бучатский А.Н.** – кандидат технических наук, доцент, директор института магистратуры СПбГУТ, заместитель председателя*Члены программного комитета***Владыко А.Г.** – кандидат технических наук, доцент, декан факультета фундаментальной подготовки СПбГУТ**Зикратов И.А.** – доктор технических наук, профессор, декан факультета информационных систем и технологий СПбГУТ**Иванов Н.Н.** – доктор технических наук, старший научный сотрудник, заместитель директора института магистратуры по научной работе СПбГУТ**Кирик Д.И.** – кандидат технических наук, доцент, декан факультета радиотехнологий связи СПбГУТ**Нестеров А.А.** – кандидат технических наук, доцент, начальник управления организации научной работы и подготовки научных кадров**Окунева Д.В.** – кандидат технических наук, доцент, декан факультета инфокоммуникационных сетей и систем СПбГУТ**Сотников А.Д.** – доктор технических наук, профессор, декан факультета цифровой экономики, управления и бизнес-информатики СПбГУТ**Шутман Д.В.** – кандидат политических наук, доцент, декан факультета социальных цифровых технологий СПбГУТ

Сборник подготовлен оргкомитетом конференции при поддержке сетевого издания «Информационные технологии и телекоммуникации», www.ijtt.ru

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ*Сопредседатели***Ивасишин С.И.** – кандидат технических наук, и.о. первого проректора – проректор по учебной работе СПбГУТ**Алексеев И.А.** – кандидат педагогических наук, проректор по воспитательной работе и связям с общественностью СПбГУТ*Ответственный секретарь***Степанов А.Б.** – кандидат технических наук, заместитель директора института магистратуры по учебной работе СПбГУТ*Члены организационного комитета***Гайдаш В.П.** – директор административно-хозяйственного департамента СПбГУТ**Григорян Г.Т.** – начальник управления маркетинга и рекламы СПбГУТ**Зыкова Н.В.** – начальник управления информационно-образовательных ресурсов СПбГУТ**Казаков Д.Б.** – начальник управления информатизации СПбГУТ**Чистова Н.А.** – и.о. проректора по развитию, директор финансово-правового департамента СПбГУТ

В материалах конференции размещены доклады, представленные на научно-методической конференции 2022 года, за исключением докладов, признанных лучшими по итогам работы секций научных направлений конференции и опубликованных в отдельном сборнике.

Предназначено для магистрантов, их руководителей, аспирантов, студентов старших курсов вузов Российской Федерации.

*Сайт конференции
pkm.sut.ru*

Научное издание

Вёрстка

Е. М. Еникеева, Д. А. Рожкова, А. Н. Данилова

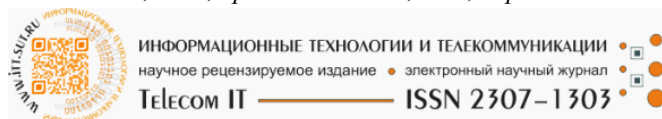
Дизайн логотипа Г. И. Юрьев

Подписано в печать 09.01.2023г.

91,88 уст.печ.л. Заказ 95-ИТТ-2023

Вышло в свет 31.01.2023г. Формат 60x90 1/8

Россия, СПб, пр. Большевиков, д.22, корп. 1



СОДЕРЖАНИЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАДИОЭЛЕКТРОНИКИ	20
1.1. Микроволновая техника: материалы, компоненты, устройства	20
Грохольский А.В. (СПбГУТ) Устройства частотной селекции в объемном интегральном исполнении	21
Жикин С.А., Седышев Э.Ю. (СПбГУТ) Диэлектрические резонаторы в интегральных схемах СВЧ	25
Книгиницкий Е.И (СПбГУТ) Генераторы СВЧ с задающими элементами в виде ОИС	29
Ларионова А.К., Седышев Э.Ю. (СПбГУТ) Генератор шума СВЧ на полупроводниковом диоде в интегральном исполнении	33
Леонтьев А.С., Седышев Э.Ю. (СПбГУТ) Устройства частотной селекции с возможностью перераспределения мощности на КЭР	38
Могилатов А.В., Седышев Э.Ю. (СПбГУТ) Пеленг СВЧ в объёмном интегральном исполнении	44
Пневский С.Б., Седышев Э.Ю. (СПбГУТ) Предпосылки создания кольцевой антенной решетки СВЧ диапазона с Дольф-Чебышевским распределением излучателей	48
Седышев Э.Ю., Шерстобитов А.А. (СПбГУТ) Спутниковый антенный модуль в объемном интегральном исполнении	53
1.2. Промышленная электроника	57
Богатырев К.Д. (СПбГУТ) Применение управляемого резонансного инвертора тока в длинноволновом радионавигационном передатчике	58
Воропаев П.В, Никитин Ю.А. (СПбГУТ) Варианты построения делителя с дробным коэффициентом деления	63
Гавриков И.И. (СПбГУТ) Исследование схемы источника питания для электронного оборудования	67
Гиниятуллин А.Э., Никитин Ю.А., Юрова В.А. (СПбГУТ) Вариант нониусного цифроаналогового преобразования	72
Гришин В.В., Колосько А.Г. (СПбГУТ) Масс-спектрометр и его использование при исследовании эффекта полевой эмиссии	76
Гуляев Р.С., Кузенов С.Р. (СПбГУТ) Производство водорода в мире: современное состояние и перспективы	80
Кучерявый А.И., Передистов Е.Ю. (СПбГУТ) Особенности заряда и разряда литиевых батарей. Недостатки пассивных и активных балансиров	85
Скороходов Н.Е. (СПбГУТ) Применение микроконтроллеров общего назначения в DC-DC преобразователях напряжения	90

РАДИОТЕХНОЛОГИИ СВЯЗИ	95
2.1. Медиа технологии и телерадиовещание	95
Антипин Б.М., Терновья А.К. (СПбГУТ) Оценка параметров излучений передатчиков радио вещательной службы средствами радиоконтроля	96
Вербицкий А.В., Швец М.А. (СПбГУТ) Исследование работы средств радиовещания на объекте РТПС в Н. П. Михайловка	101
Григорьев М.Н. (СПбГУТ) Исследование методов активного шумоподавления	106
Дудевич Д.Н. (СПбГУТ) Нормирование звуковых сигналов в телерадиовещании	110
Молчанов А.П. (СПбГУТ) Процесс работы современного телевидения: особенности развития систем гибридного вещания	115
Морозова Е.А. (СПбГУТ) Стабилизация видео	119
Сидоркина Д.С. (СПбГУТ) Технологии иммерсивной реальности	124
Сушко Я.Г., Федоров С.Л. (СПбГУТ) Развитие системы контроля и управления оборудованием телерадиопередающего центра	129
Татаренков Д.А., Горцуева А.С. (СПбГУТ) Применение искусственного интеллекта в графике	133
Татаренков Д.В., Чеботарева А.В. (СПбГУТ) Сравнение библиотек для управления адресными светодиодами	138
Тяжев Д.В. (СПбГУТ) Анализ существующих методов распознавания эмоций человеческого лица	141
Федоров С.Л., Волкова А.И. (СПбГУТ) Эволюция твердотельных телевизионных преобразователей свет-сигнал	146
Элежбиев А.Р. (СПбГУТ) Возможность импортозамещения оборудования цифрового эфирного телевизионного вещания стандарта DVB-T2 на примере вещания пакета РТПС-1	151
Юраков Д.М. (СПбГУТ) Возможности исследования беспроводных протоколов связи с помощью SDR на примере обратной разработки устройств, работающих в диапазоне LPD433	156
2.2. Подвижная связь и радиодоступ	160
Glazacheva O.V., Zaichenko A.A., Zheltova E.P. (SPbGUT) Prospects for the introduction of eSIM by mobile operators	161
Аскеров М.Т. (СПбГУТ) Анализ принципов работы функционала ANR в сетях LTE с поддержкой SON	165
Бабенко М.С. (СПбГУТ) Принцип построения системы связи для робототехнических комплексов, функционирующих в условиях интенсивных помех.	170
Бабурин Е.В. (СПбГУТ) Сравнительный анализ систем связи Ocusync и Lightbridge, применяемых в БПЛА компании DJI	175
Добрая О.П. (СПбГУТ) Оценка радиопокрытия сетей 5G с цифровыми моделями местности в среде Matlab	180
Зайченко А.А., Чичко Т.А. (СПбГУТ) Анализ проблемы обслуживания абонентов сетей мобильной связи в высокоскоростных поездах	185
Измесьева Е.А. (СПбГУТ) Особенности моделирования радиопередатчика сверхширокополосных сигналов на основе хаотических радиоимпульсов	190
Каранова Е.Е. (СПбГУТ) Анализ реализации протокола управления радиоресурсами RRC в имитационной модели сети LTE в симуляторе NS-3	194

Киселёв Т.В. (СПбГУТ) Способы связи с подводными объектами.....	199
Коротин В.Е., Вторых В.С. (СПбГУТ) Исследование эффективности рефарминга с точки зрения влияния на зоны покрытия сети	204
Косьянов М.Н., Воробьев О.В. (СПбГУТ) Виртуализация узлов ядра сети сотовой связи.....	208
Кузьмин А.А. (СПбГУТ) Исследование параметров радиоканала для передачи трафика в сетях стандарта New Radio	212
Ларионов А.Ю. (СПбГУТ) Динамическое управление частотно-орбитальным ресурсом низкоорбитальных спутниковых систем.....	217
Марковец В.А. (СПбГУТ) Разработка технологической сети для Россетей	221
Мартынова Е.А. (СПбГУТ) Анализ модели интерфейса X2 в симуляторе NS-3	226
Науменко В.Е. (СПбГУТ) Реализация высокоскоростного мобильного интернета вещей в сетях New Radio	230
Никитин И.А., Прилуцкая У.И. (СПбГУТ) Использование метода наименьших квадратов (LMS) в задачах цифрового диаграммообразования в сетях 5G	235
Рекель П.Ф. (СПбГУТ) Конфигурация и алгоритм работы наземных станций системы многопозиционного наблюдения	241
Родина К.А. (СПбГУТ) Выбор узла цифровой обработки при многоканальной передаче.....	246
Рошинский Р.С. (СПбГУТ) Обзор радиопараметров в сетях подвижной связи.....	249
Рютин К.Е., Фокин Г.А. (СПбГУТ) Использование SDR-технологии для задач сетевого позиционирования. Формирование информационного блока MIB.....	253
Скрылев С.А. (СПбГУТ) Моделирование радиопокрытия сетей радиодоступа с использованием трассировки лучей	259
Страшнов А.А. (СПбГУТ) Анализ особенностей реализации Massive MIMO для уменьшения помеховой обстановки.....	264
Тимофеев В.С. (СПбГУТ) Формирование требований к радиоканалу для связи с БПЛА на дальние расстояния	268
Ушакова В.А. (СПбГУТ) Анализ требований к интерфейсам транспортной сети в действующих и перспективных сетях мобильной связи.....	273
Ушкова И.Г., Фокин Г.А. (СПбГУТ) Прием метки ГНСС с помощью GPS/GLONASS-приемника	277
Шайхлеева Н.И. (СПбГУТ) Анализ сверхширокополосных импульсов	282
Шойтов И.А. (СПбГУТ) Разработка кроссплатформенного микроволнового IoT радара для indoor-позиционирования.....	286
2.3. Проектирование и технология радиоэлектронных средств	291
Дунаев Н.П. (СПбГУТ) Технологии металлизации напечатанных пластиковых деталей при быстром прототипировании устройств СВЧ диапазона	292
Есенбеков Р.М., Кирик Д.И. (СПбГУТ) Исследование методов конверсии изделий двойного назначения.....	297
Литвинов А.С. (СПбГУТ), Балабанов С.В. (ИХС РАН) Исследование зависимости прочностных характеристик изделия от параметров 3D-печати и используемого материала.....	301
Махалов Е.А. (СПбГУТ) Современное состояние функционирования и развития светодиодной техники, конструкторско-технологические проблемы повышения качества	306
Поленова Д.А., Мордовин В.Н. (СПбГУТ) Проектирование платы управления устройства климатического контроля с передачей данных	310

2.4. Радиотехнические системы и антенны	315
Афанасьев Н.А., Ликонцев А.Н. (СПбГУТ) Увеличение точности определения местоположения источника радиоизлучения путем использования известных источников сигнала.....	316
Глушанков Е.И., Кирсанов Д.М. (СПбГУТ) Адаптивная обработка сигналов с использование метода параллельной регуляризации RLS алгоритма	320
Глушанков Е.И., Мебония М.А. (СПбГУТ) Алгоритм декодирования блоковых кодов с использованием псевдообращения порождающей матрицы	325
Глушанков Е.И., Пуршель В.В. (СПбГУТ) Псевдослучайное включение антенн как метод повышения энергетической эффективности систем цифровой радиосвязи	328
Коровин К.О., Никитин М.А. (СПбГУТ) Создание приложение для расчета элементов согласования СВЧ-устройств	331
Лавров М.Н. (СПбГУТ) Алгоритм управления амплитудно-фазовым распределением тока в антенных элементах передающей фазированной антенной решетки	334
Ликонцев А.Н., Нев Д.А. (СПбГУТ) Оценка дальнейшего развития стандартов спутниковой передачи данных	337
Ликонцев А.Н., Осипова В.А. (СПбГУТ) Анализ технических решений, применяемых в сети спутниковой связи STARLINK.....	342
Червинко Е.И. (СПбГУТ) Исследование статистических характеристик оптического ToF-датчика расстояния VL53L0X.....	347
2.5. Цифровая обработка сигналов	352
Лебедев А.К., Чернов И.Н. (СПбГУТ) Разработка модуля приёма цифрового видеопотока на ПЛИС	353
Михаль Г.А., Муравьева И.В., Чернов И.Н. (СПбГУТ) Разработка системы удаленного управления стендовым оборудованием.....	357
2.6. Экология формирования информационного пространства	362
Белоцерковский М.В. (СПбГУТ) Природно-ресурсный потенциал Смоленской области и его интегральная оценка	363
Загребаяева Н.М. (СПбГУТ) Экологическая безопасность минераловатного производства.....	367
Карпекин А.А. (СПбГУТ) Блочная модульная водоочистная станция.....	372
Ковалева О.П. (СПбГЛТУ), Манвелова Н.Е., Огай А.И. (СПбГУТ) Экологические проблемы переработки макулатуры и пути их решения.....	376
Манвелова Н.Е., Чабаева Е.А. (СПбГУТ) Определение бензапирена в атмосферном воздухе методом высокоэффективной жидкостной хроматографии.....	381
Мороз Е.Е. (СПбГУТ) Динамика показателей качества воды в реке Самара и анализ влияющих на него антропогенных и техногенных факторов	386
Назаров И.В. (СПбГУТ) Природно-ресурсный потенциал Приморского Края и его интегральная оценка	391
Николаева О.А. (СПбГУТ) Социально-экологические проблемы объектов размещения отходов.....	395
Стурман В.И. (СПбГУТ) Приборное обеспечение и новые возможности исследования проблем электромагнитного загрязнения.....	401

Судьина Е.В. (СПбГУТ) Оценка влияния метеорологических параметров на концентрации загрязняющих веществ в атмосфере Кировского района Санкт-Петербурга.....	405
Сычёва Е.С. (СПбГУТ) Анализ шумового загрязнения территорий муниципальных округов №65 и №68 Приморского района г. Санкт-Петербурга (с применением ГИС-технологий).....	410

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ 414

3.1. Безопасность компьютерных систем и сетей связи 414

Абраменко Г.Т., Зрелова А.Л., Мельник М.В. (СПбГУТ) Разработка модели сигнатур атак обеспечивающих обнаружение атак и аномалий	415
Акопя Джон, Ушаков И.А. (СПбГУТ) Опрос по обнаружению сетевых аномалий на основе современных технологических тенденций	419
Александрова А.Г., Потомако Д.О. (СПбГУТ) Исследование системы защиты информации типового объекта КИИ на соответствие требованиям по защите информации	423
Александрова А.Г., Потомако Д.О. (СПбГУТ) Модель угроз для типового объекта КИИ, функционирующего в сфере атомной энергетики.....	428
Бабков И.Н., Федорова З.А. (СПбГУТ) Сравнение способов контроля состояния информационной безопасности на предприятии	433
Баракат Абдельрахман (СПбГУТ) Изучение защитных механизмов DNS-фарминга	438
Бирих Э.В., Волокушина К.П. (СПбГУТ) Разработка автоматизированного процесса по корреляции информации между таблицей базы данных PostgreSQL и Active Directory	443
Богомаз М.Э., Нечаев А.А. (СПбГУТ) Сравнительный анализ децентрализованной блокчейн платформы TON	448
Борисов В.И. (СПбГУТ) Исследование обновлённых принципов сбора цифровых уликов.....	453
Воронцов А.А., Шемякин С.Н. (СПбГУТ) Определение оптимальных булевых функций в классе малой размерности	458
Ворошнин Г.Е., Забзеев Е.А. (СПбГУТ) Архитектура устройства автоматизированного аудита безопасности сетей семейства IEEE 802.11.....	463
Данилова Ю.С., Штеренберг С.И. (СПбГУТ) Исследование возможностей SIEM MaxPatrol при выявлении инцидентов информационной безопасности	468
Дементьев Р.И., Держко Д.Я., Ушаков И.А. (СПбГУТ) Исследование механизмов построения DMVPN при переходе на отечественное оборудование.....	473
Демидов П.С., Ушаков И.А. (СПбГУТ) Исследование методов сетевой стеганографии StegTorrent и SkyDe.....	478
Дятченко А.А. (СПбГУТ) Сложности при проведении оценки соответствия системы защиты информации требованиям ГОСТ Р 57580.1-2017	483
Егорова А.Л. (СПбГУТ) Оценка рисков информационной безопасности в информационной инфраструктуре на базе облачного решения	488
Елизарова Л.Р., Израилов К.Е. (СПбГУТ) Классификация областей информационной безопасности с применением категориального деления	492
Емельяненко Г.Ю. (СПбГУТ) tПринцип организации защиты пользовательских терминалов от атаки типа MAC-SPOOFING	497
Иванилова Ю.А., Кравцова В.А., Ушаков И.А. (СПбГУТ) Исследование механизмов предотвращения DDoS-атак на маршрутизаторе Eltex ESR200.....	502

Кзаков Н.И., Петрова Т.В. (СПбГУТ) Разработка playbook Ansible для модуля обнаружения нелегитимных точек доступа семейства IEEE 802.11 в проводной корпоративной сети	507
Ковалев И.А., Фёдорова А.Э. (СПбГУТ) Исследование безопасного развёртывания веб-приложения в облачной инфраструктуре	511
Коломийцев Р.К. (СПбГУТ) Внутренние угрозы безопасности информации организации и методы противодействия	516
Крестьяшин Н.А., Пучков В.В. (СПбГУТ) Модель данных для защиты устройств умного дома от внешнего нарушителя.....	520
Кузьмина О.И., Дрепа В.Е. (СПбГУТ) Исследование систем определения местоположения клиентов беспроводных сетей семейства IEEE 802.11	525
Макарова А.К. (СПбГУТ) Подробный анализ классов уязвимостей в VoIP сетях	530
Макеев Н.А. (СПбГУТ) Анализ уязвимостей операционной системы Windows	534
Масютин М.Д., Салита А.С. (СПбГУТ) Стеганографические вложения в «STREAM CONTROL TRANSMISSION PROTOCOL»	539
Нагаева А.Д. (СПбГУТ) Уязвимости IoT-устройств под управлением ОС LINUX....	544
Нефедов В.В. (СПбГУТ) Методы внедрения самомодифицирующегося кода в исполняемые файлы ре-формата	549
Паршин Е.А. (СПбГУТ) Модели и алгоритмы оценки эффективности процессов DevSecOps	553
Паскидов Н.В. (СПбГУТ) Организация стеганографических каналов с использованием протокола HTTP.....	557
Петров П.Е. (СПбГУТ) Синтез метода выявления фишинговых сайтов для антифишинговой системы на основе машинного обучения.....	561
Попов А.А., Федорова О.В. (СПбГУТ) Сравнение скорости исполнения кода в нативной среде и среде WASM.....	566
Пучков В.В., Виткова Л.А (СПбГУТ, СПб ФИЦ РАН), Едемская Е.Д. (СПбГУТ) Принципы взаимодействия компонентов сети «Умный дом».....	570
Разумов Д.А., Шемякин С.Н. (СПбГУТ) Алгоритм Монтгомери умножения в поле Галуа	575
Салита А.С. (СПбГУТ) Стеганографические вложения в протокол «DOMAIN NAME SYSTEM»	580
Скорых М.А., Израилов К.Е. (СПбГУТ) Проблемные вопросы обнаружения ботнет-сетей на базе устройств интернета вещей.....	584
Таров Е.В., Шемякин С.Н. (СПбГУТ) Реализация модульных вычислений с большими числами на основе алгоритма Монтгомери	588
Ульянов Д.А., Гельфанд А.М. (СПбГУТ) SDN ЦОД на базе Cisco ACI	594
Филиппов А.А. (СПбГУТ) Методика анализа Max Patrol SIEM в организации	597
Джораев Х.А. (СПбГУТ) Безопасный обмен данными и схема доступа через блокчейн.....	602
Храмцов Д.О., Киструга А.Ю. (СПбГУТ) Исследование DoS атак на беспроводные сети на основе WPA-2 ENTERPRISE	607
Шабловский Я.К., Гельфанд А.М. (СПбГУТ) Изменение задержки в зависимости от количества узлов в кластере ONOS при включении/отключении коммутатора.....	612
Яссер М.В., Ковцур М.М. (СПбГУТ) Разработка комплекса лабораторных работ по функционированию WLAN контроллеров	615
3.2. Интернет вещей и гетерогенные сети	620
Абитов И.Д. (СПбГУТ) Анализ трафика облачного гейминга	621
Баталин Н.С., Лапцевич Г.П. (СПбГУТ) Альтернативные реализации $(p - 1) -$ метода Полларда.....	625

Выборнова А.И., Григорьев А.А., Толкачев А.С. (СПбГУТ) Перспективы развития квантовой криптографии в интернете вещей на примере метода квантовых блужданий.....	629
Герасимова Я.А. (СПбГУТ) Использование технологии OFDMA в WI-FI 6.....	634
Гераськин В.К. (СПбГУТ) Архитектура сети InfiniBand	638
Ермолаев Е.Е., Кукунин Д.С. (СПбГУТ) Big Data и туманные вычисления	643
Зенченко А.К. (СПбГУТ) Обеспечение информационной безопасности в программно-конфигурируемых сетях	648
Кукунин Д.С., Елисеева К.А. (СПбГУТ), Федотов И.О. (ООО «Естественный интеллект») Сравнительный анализ современных баз данных	654
Кукунин Д.С., Петушков И.О. (СПбГУТ) Исследование процесса расширения спектра сигнала в среде моделирования	661
Лохов Д.А., Парамонов А.И. (СПбГУТ) Анализ особенностей беспроводных сетей связи с высокой плотностью пользователей	665
Машошин Е.С. (СПбГУТ) Анализ и использование возможностей "Умного дома" для предоставления услуг с применением технологии туманных вычислений	670
Минеева В.Д. (СПбГУТ) Использование асимметричной системы шифрования для обеспечения безопасной передачи данных в сети WEB 3.0	675
Мутханна А.С.А., Леонова М.Д. (СПбГУТ) Архитектура предоставления системы услуг телеприсутствия и сферы применения тактильного интернета в роботизированных системах	679
Никитин Е.Д., Харламов М.А. (СПбГУТ) Определение и классификация наносетей. Молекулярные наносети и их применение. Электромагнитные наносети и их применение	684
Никонова Е.Ю. (СПбГУТ) Разработка методики субъективной оценки качества восприятия для дополненной реальности.....	691
Скоробогатова С.А. (СПбГУТ) Исследование эффективности технологии явного формирования луча в сетях Wi-Fi	696
Смирнова А.А. (СПбГУТ) Исследование эффективности применения кодирования LDPC в сетях Wi-Fi.....	701
Степанов А.М., Маколкина М.А. (СПбГУТ) Исследование взаимосвязи субъективных оценок QoE и параметра Хёрста для дополненной реальности	705
Тихонов А.М., Парамонов А.И. (СПбГУТ) Задачи исследования трафика и качества обслуживания в самоорганизующихся сетях с подвижными пользователями.....	710
Хасанова В.А. (СПбГУТ) Исследование параметров трафика устройств дополненной реальности в сетях связи.....	713
Шипицын Ю.С., Котов М.А., Мутханна А.С.А. (СПбГУТ) Обзор технологии ONAP для сетей будущего поколения	719
Щеглов С.А. (СПбГУТ) Исследование характеристик беспроводной локальной сети общежития СПбГУТ «Дальневосточное».....	724
3.3. Мультисервисные телекоммуникационные системы и технологии	728
Белозеров К.В, Кисляков С.В. (СПбГУТ) Анализ возможности применения аппарата теории игр для автоматизации процессов в инфокоммуникациях	729
Божедомов А.Ю., Гончаров Е.Е. (СПбГУТ) Анализ технологии NFV (виртуализация сетевых функций) для поставщиков телекоммуникационных услуг ...	732
Градовский М.В., Кисляков С.В. (СПбГУТ) Анализ современных инструментов DevOps.....	737
Елагин В.С., Тураев С.М. (СПбГУТ) Анализ мобильных сетей в двухрежимной программно-определяемой сетевой платформы SD-Core	741
Заяц М.П. (СПбГУТ) Искусственный интеллект в бизнес-процессах	745

Казаченко И.О., Просветов А.Ю. (СПбГУТ) Анализ технологий виртуализации для обеспечения слайсинга в сетях 5G	750
Кисляков С.В., Лочкарев Е.А., Сухомлинов Д.И. (СПбГУТ) Адаптация систем NRI и WFM к открытой цифровой архитектуре TM FORUM	755
Коничев Д.А., Ткачук А.В. (СПбГУТ) Разработка приложения с использованием микросервисной архитектуры для составления прогноза лавинной опасности и распространением его посредством телеграмм бота	760
Лихтциндер Б.Я., Садкова А.С. (ПГУТИ) Исследование трафика узла доступа с помощью системы АМС	765
Моисеева А.В. (СПбГУТ) Исследование микросервисной архитектуры для поддержки эксплуатационных процессов	769
Некрасов В.Н. (СПбГУТ) Анализ рынка и актуальность систем видеоконференцсвязи (ВКС).....	773
Якупов Д.О., Малахов С.В. (ПГУТИ) Применение имитационного моделирования в решении различного рода задач.....	777
3.4. Оптоэлектронные технологии (фотоника) в инфокоммуникациях	781
Агоштинью П.С., Какусилумезо С.Э. (СПбГУТ) Моделирование ВОСС с когерентным приемом и модуляцией DP-16-QAM	782
Андреева Е.И., Яковлев Н.В., Константинов Е.С. (СПбГУТ) Применение оптических солитонов для создания измерительных источников излучения.....	787
Андриевский Н.К., Былина М.С. (СПбГУТ) Многосердцевинное оптическое волокно с «траншеей» вокруг каждой сердцевины	791
Андрюнин А.И., Былина М.С. (СПбГУТ) Разработка виртуальной лабораторной работы по изучению интерферометра Маха-Цендера.....	797
Богданова Е.И., Головкина М.В. (ПГУТИ) Расчет параметров быстродействующего сверхпроводящего фильтра.....	802
Былина М.С., Бычков А.В., Гулятьева Л.А. (СПбГУТ) Многосердцевинное оптическое волокно с одномодовыми сердцевинами изолированными оболочками из воздушных капилляров.....	805
Былина М.С., Кажаяев М.В. (СПбГУТ) Терминальный четырехканальный мультиплексор для системы CWDM.....	811
Васильев Н.С., Клименко В.П. (СПбГУТ) Сравнительный анализ фотоприемных устройств для энергетического приема цифровых оптических сигналов	816
Гончаров Ф.М., Наседкин Б.А., Первушин Б.Е. (ИТМО) Увеличение соотношения сигнальных и опорных импульсов для фазовой компенсации в системах квантового распределения ключа на непрерывных переменных.....	821
Григоренко И.К. (СПбГУТ) Анализ методов несанкционированного воздействия в PON.....	826
Дмитриева Д.В., Цыганок А.Э. (СПбГУТ) Исследование спектральных характеристик оптического излучения источников и передающих оптических модулей	831
Дмитриева Д.С. (СПбГУТ) Разработка системы контроля радиоактивной обстановки на основе волоконно-оптических датчиков для водных бассейнов атомных электрических станций	836
Дюбов А.С., Калашникова Л.И. (СПбГУТ) Оптические поляризационно-независимые изоляторы для специальных применений	840
Дюбов А.С., Кузьмина В.Э. (СПбГУТ) Моделирование работы передатчика оптической системы связи.....	845
Дюбов А.С., Николаев Е.В. (СПбГУТ) Активные и пассивные компоненты перспективных волоконно-оптических сетей связи	850

Исупов А.И., Кравцова В.А., Орлов М.А., Сухомлинов Д.И. (СПбГУТ) Анализ областей применения CWDM и DWDM технологий	855
Карлин В.Э. (СибГУТИ) Волоконно-оптические датчики на принципе рассеяния Мандельштама-Бриллюэна	860
Лыков Г.Р. (СПбГУТ) Исследование процесса поддержания квазисолитонного режима распространения импульсов в одномодовом волокне с аномальной дисперсией	865
Матющенко М.С. (СПбГУТ) Исследование и моделирование волоконно-оптического датчика температуры и деформации на основе волоконных решеток Брэгга.....	870
Медведев И.Н. (СПбГУТ) Исследование различных стандартов оптических 100G трансиверов.....	876
Пилипова В.М., Давыдов В.В, Дмитриева Д.С., Пчелкин Г.А. (СПбГУТ) Разработка микроструктурированного оптического волокна с заданным модальным составом	880
Подопригора А.Н. (СПбГУТ) Применение киральных микроструктурированных оптических волокон в сенсорных приложениях	884
Поздняков А.А., Шоргин О.О., Свинтуховский П.В. (СПбГУТ) Проектирование, сборка, настройка и приемосдаточные испытания модели DWDM линии.....	888
Ступникова А.А. (СибГУТИ) Область применения датчиков на принципе рассеяния Мандельштама-Бриллюэна	893
Шайгараева Т.Н. (СибГУТИ) Практические приложения распределенных тензодатчиков	898
3.5. Программная инженерия	
Богомедова К.М., Израилов К.Е. (СПбГУТ) Сравнительный анализ языков Java и Kotlin с позиции написания безопасных программ	904
Ерохова Н.А., Пачин А.В. (СПбГУТ) Проблемы создания и эксплуатации умных зданий.....	909
Завацкая А.А. (СПбГУТ) Существующие проблемы в подходах к формированию систем идентификации пользователя на базе клавиатурного почерка.....	913
Искра И.И., Новиков С.С., Помогалова А.В. (СПбГУТ) Децентрализованный мессенджер на базе открытого протокола мгновенного обмена сообщениями с использованием технологий федеративной сети и мостов	918
Клабуков С.А., Федоров А.А. (СПбГУТ) Анализ проблематики эксплуатации систем обеспечения центров обработки данных.....	922
Кукушкин П.С., Кулигина Е.Э., Степаненков Г.В. (СПбГУТ) Система обмена сообщениями по шаблону проектирования «издатель – подписчик»	926
Мишаков В.А., Помогалова А.В. (СПбГУТ) DDNS как новый этап развития сервисов контроля и присвоения доменных имён	932
Мурашкин Н.А. (СПбГУТ) Анализ P2P-сетей на основе существующих решений ...	937
Николаева Л.А., Березкин А.А. (СПбГУТ) Базовый пайплайн идентификации лиц в системах транспортной безопасности	942
Самохина Н.Э. (СПбГУТ) Автоматизированные алгоритмы для оптимизации процесса контроля образовательных процессов	945
Серегин А.Г., Киричек Р.В. (СПбГУТ) Архитектура программно-аппаратного стенда дистанционного тестирования киберфизических систем	950

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ	954
4.1. Интеллектуальные коммуникационные технологии	954
Ананьев М.А. (СПбГУТ) Обзор методов построения надежной структуры сетей хранения данных	955
Бовшик П.П., Литвинов В.Л. (СПбГУТ) Анализ математических методов глубокого обучения в задачах распознавания объектов на изображении	960
Бондаренко И.Б., Крылов Д.А. (СПбГУТ) Разработка многоагентного подхода для оптимальной защиты многоуровневой промышленной системы	965
Бондаренко И.Б., Миронов П.В. (СПбГУТ) Разработка подхода для защиты информационных систем на основе анализа живучести	970
Григорьева Р.Г, Раковский О.В. (СПбГУТ) Краткий обзор платформ дистанционного обучения	975
Губин А.Н., Михайлова Е.А. (СПбГУТ) Исследование информационной модели оценки уровня подготовки студентов при тестировании	979
Дамдинов Б.Б., Птицына Л.К. (СПбГУТ) Формирование расширений математических формализаций для исследования методов и средств управления крупно-гранулярными процессами	983
Ермолаев Д.А., Иванова В.А., Ковальчук А.В., Птицына Л.К. (СПбГУТ) Planning of research of service-oriented systems with soft architecture	986
Исаенко Д.И., Резников Б.К. (СПбГУТ), Ромانيук Д.Р., Карпов Е.Е. (ИТМО) Основные причины снижения эффективности эксплуатации магистральных сетей передачи данных	990
Красавцева К.А., Раковский О.В. (СПбГУТ) Разработка информационной системы интеллектуального мониторинга микроклимата	994
Кусиков К.С., Птицына Л.К. (СПбГУТ) Анализ влияния коммуникационного взаимодействия на качество функционирования мультиагентных систем умного дома	999
Лакомкина Е.А., Птицына Л.К. (СПбГУТ) Концептуальное моделирование комплексных систем защиты информации с мягкой архитектурой	1002
Леонова Е.А. (СПбГУТ) Обзор методов сегментации изображений	1006
Литвинов В.Л., Яшин А.В. (СПбГУТ) Исследование методов автоматизации логистических центров	1009
Мендус Р.Д. (СПбГУТ) Сравнение структур систем хранения данных, использующих твердотельные накопители	1014
Михаль Г.А., Смородин Г.Н. (СПбГУТ) Оптимизация жизненного цикла разработки программного обеспечения путём внедрения GitOps практик	1018
Панченко А.А., Попонин А.С. (СПбГУТ) Разработка системы нормализации данных для обучения алгоритмов компьютерного зрения	1022
Попонин А.С., Триандафилиди И.И. (СПбГУТ) Повышение управляемости генерации речи в алгоритмах глубокого машинного обучения в области синтеза речи	1027
Склярлов А.А. (СПбГУТ) Метод формализации видеоконтента в среде Python	1032
Соловьев А.С., Птицына Л.К. (СПбГУТ) Прогнозирование достижимости цели при использовании крупно-масштабных сервис-ориентированных систем	1036
Ягунов П.А. (СПбГУТ) Анализ подходов к созданию рекомендательных систем	1039
4.2. Интеллектуальные технологии в автоматизации и цифровых системах управления	1043

Белоус К.В., Кириллова А.К., Кириллова М.К. (СПбГУТ) Управление системой умный дом с использованием dtmf.....	1044
Выжлова А.К. (СПбГУТ) Агентно-ориентированный подход к формированию децентрализованных систем управления.....	1047
Гребешков А.Ю., Пенькова Ю.Е. (СГТУ) Разработка методики оценки эффективности деятельности по управлению научными консорциумами	1050
Елфимов А.В., Косенков В.В. (СПбГУТ) Сравнительный анализ инфраструктурных инструментов Infrastructure as code	1055
Изряднов В.Д. (СПбГУТ) Оценка релевантности ссылок в поисковой системе “Яндекс”	1060
Качуровский Ю.О., Рузманов Е.Ю. (СПбГУТ) Обнаружение аномалий с помощью методов машинного обучения	1064
Корнюшкин Д.А., Крылов А.А (СПбГУТ) Распределенная система управления и защиты от внештатных ситуаций	1068
Кривоногова Е.В., Рябов Г.А. (СПбГУТ) Семантический разбор текстов с помощью искусственных нейросетей.....	1073
Лешукова А.М. (СПбГУТ) Проблемы применения и разработки экспертных систем. Использование экспертных систем в криминалистике	1077
Марзаганов Г.И. (СПбГУТ) Развертывание микросервисной системы управления контентом в системах распределенного реестра.....	1080
Марченко А.А. (СПбГМТУ) Метод увеличения отказоустойчивости системы: Блоки восстановления консенсуса.....	1083
Петров И.В. (СПбГУТ) Использование географических информационных систем в отраслях цифровой экономики	1087
Рожков Г.В. (СПбГУТ) Современные искусственные нейронные сети.....	1090
Соловьев Д.В., Бондаренко И.Б. (СПбГУТ) Разработка программно-аппаратного комплекса дополненной реальности для операторов станков оптоволоконного производства.....	1096
Филиппов Ф.В., Цыварев И.В. (СПбГУТ) Способы решения задачи аутентификации с использованием данных пользователя при взаимодействии с чат-ботами	1101
Юрченко П.В. (СПбГУТ) Способы решения проблемы тематического поиска в библиотечной деятельности.....	1105
4.3. Информационные технологии в дизайне	1110
Андрианов Д.М., Елькин А.А., Федорова А.В. (СПбГУТ) Проектирование визуально-коммуникативной составляющей экотроп с использованием современных цифровых технологий.....	1111
Бояшова Е.П., Мельников М.В. (СПбГУТ) Об использовании программных и аппаратных средств для работы с инфографикой в VR	1114
Джапарова Д.А. (СПбГУТ) Методы визуализации информации с использованием инфографики.....	1118
Диброва О.П., Бояшова Е.П. (СПбГУТ) К вопросу об организации эффективного взаимодействия преподавателя и студента в образовательном процессе вуза.....	1122
Ежов Г.В. (ПГУТИ) Проектирование архитектуры рендерера общего назначения на основе Vulkan API.....	1127
Карпова В.Д., Бояшова Е.П. (СПбГУТ) Разработка концепции приложения для обучения и социальной адаптации детей с особенностями развития	1132
Кучинский Е.С., Шиян А.А. (СПбГУТ) Прогрессивные веб-приложения для бизнеса: какие задачи помогают решать, российский рынок, успешные кейсы.....	1136
Лебедев Д.В., Шиян А.А (СПбГУТ) Виды филаментов для 3D-печати методом послойного наплавления	1141

Лосев А.П., Рогозинский Г.Г. (СПбГУТ) Разработка системы генерации аудиального окружения для моделей виртуальной реальности	1145
Люй Инчжэн (СПбПУ) Область применения и тенденции развития геометрических алгоритмов	1150
Макарова В.В. (СПбГУТ) Разработка пользовательского интерфейса поиска чатов по карте, при помощи существующей дизайн-системы популярного мессенджера.....	1155
Максимова С.В., Мусаева Т.В. (СПбГУТ) Обзор методов управления визуальным восприятием пользователя	1161
Мусаева Т.В., Титов П.А. (СПбГУТ) Искусственный интеллект в дизайне интерфейсов.....	1166
Нефедов Д.И., Сергеев Н.А. (СПбГУТ) Основные проблемы разработки и проектирования современных интерфейсов.....	1171
Онофрийчук Е.И. (СПбГУТ) Исследование методов автоматизации тестирования эргономики веб-интерфейсов.....	1175
Патрухина А.А. (СПбГУТ) Особенности SEO-продвижения сайта автодилера.....	1179
Сергеев Н.А., Нефедов Д.И. (СПбГУТ) Система бронирования рабочих мест, как инструмент для оптимизации офисного пространства	1183
Сметюх Д.В., Шиян А.А. (СПбГУТ) Цифровая метавселенная, возможности ее применения в сфере образования	1187
Урванцев Г.А., Волошинов Д.В. (СПбГУТ) Анализ перспектив применения изображений сгенерированных посредством нейросети Stable Diffusion при формировании личного бренда.....	1192
Ченарани Сасан (СПбПУ) Алгоритмический комплекс для решения задач проектирования интерфейсов для образовательной среды в виртуальной реальности на основе геометрического моделирования	1197
Щербатюк А.Д. (СПбГУТ) Методы визуализации трёхмерных объектов в пространстве и перспективы их применения в художественном образовании	1200
Щур С.Ю. (СПбПУ), Волошинов Д.В. (СПбГУТ) Проектирование объектов генеративного дизайна на основе геометрического моделирования с использованием технологий расширенной реальности	1204

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ, ИННОВАЦИИ, БИЗНЕС 1208

5.1. Цифровая трансформация, инновации, бизнес 1208

Александров Ф.Т., Сидоров Г.К. (СПбГУТ) Основы защиты информации в Biotech-стартапах: правовой и технический аспекты.....	1209
Дороганов Д.В. (СПбГУТ) Анализ эффективности внедрения автоматизированной системы управления нефтебазовым хозяйством.....	1214
Дускаев Д.Д. (СПбГУТ) Цифровая трансформация бизнес-процессов в компании (MDM система).....	1219
Казакова М.С. (ПГУТИ) Цифровой профиль гражданина как элемент профориентации учащихся	1224
Кремлёва Н.А., Папышкова А.В. (ВоГУ) Совершенствование системы предоставления государственных услуг в сфере лесного хозяйства Вологодской области на основе информационных технологий.....	1227
Крещенко Д.С. (КФУ) Цифровая трансформация, инновации и бизнес.....	1232
Миков В.Э. (СПбГУТ) Информационная система как инструмент автоматизации процессов проектирования в проектной организации.....	1235
Митюрева А.В. (СПбГУТ) Разработка модели управления взаимоотношениями с клиентами путем внедрения CRM системы	1240

Михайлов Д.А. (СПбГУТ) Выбор BPM-системы для автоматизации бизнес-процессов крупных интернет провайдеров	1244
Никольский Э.В. (СПбГУТ) Совершенствование модели бизнес-процессов в электросетевой компании (на примере ПАО «Россети Ленэнерго»).....	1248
Свиридов И.В. (СПбГУТ) Эффективность внедрения инновационных икт решений на предприятии.....	1253
Трищенко А.С. (СПбГУТ), Верединский С.Ю. (СПбГУТ) E-COMMERCE. Современные рынки сбыта и маркетинг.....	1256
Хачатрян А.А. (СПбГУТ) Информационная безопасность на рынке ценных бумаг	1260
Хорахордин А.И., Хохлова А.М. (СПбГУТ) Автоматизация процесса управления работы команды на примере проекта Bonch Avalanche Forecast (BAF)	1264
Черепанов Д.А. (СПбГУТ) Классификация «чат-ботов» и анализ жизненного цикла..	1268
ГУМАНИТАРНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА	1272
6.1. Вопросы регионоведения и межкультурных коммуникаций в цифровую эпоху	1272
Бондарь Н.А. (СПбГУТ) Международная деятельность христианских религиозных организаций в Европе	1273
Дукальская И.В. (ПГУТИ) Развитие межкультурной коммуникативной икомпетенции в эпоху цифровизации.....	1278
Жадан Р.А. (СПбГУТ) Ценности в твиттер-блогах премьер-министров великобритании (на примере Т. Мэй и Б. Джонсона)	1283
Лещинский П.В., Неровный А.В. (СПбГУТ) Экологическое сотрудничество ЕС и Западных Балкан	1288
Пуртова Г.М. (СПбГУТ) Адаптация иммигрантов в культурную среду Швеции.....	1291
Сидоренко В.Д. (СПбГУТ) Англицизмы в киберспорте.....	1295
6.2. Реклама и связи с общественностью в цифровом обществе	1300
Андриянов И.А., Кульназарова, А.В.(СПбГУТ) К вопросу использования системы LMS MOODLE в современном образовательном процессе.....	1301
Астафьева-Румянцева И.Е., Аминов С.О. (СПбГУТ) Перспективы и риски использования технологий искусственного интеллекта в интернет-рекламе.....	1305
Астафьева-Румянцева И.Е., Левченко В.В. (СПбГУТ) Анализ студенческих конкурсов в области рекламы и связей с общественностью	1309
Астафьева-Румянцева И.Е. (СПбГУТ), Добычина Я.Г. (Невские новости) «БДТ DIGITAL» как пространство театральной коммуникации.....	1313
Астафьева-Румянцева И.Е., Богданова М.А. (СПбГУТ) Особенности маскотов и их создания для коммерческих брендов	1319
Астафьева-Румянцева И.Е., Щетинина Д.А. (СПбГУТ) Соревнования Worldskills как инструмент формирования имиджа вуза.....	1324
Быстров Р.В., Листвина Н.С. (СПбГУТ) Социальная реклама как инструмент борьбы против использования электронных никотиновых устройств у молодежи в медиапространстве.....	1329
Васильев В.М. (СПбГУТ) Необходимость в исследовании маскотов и их применении учебными организациями.....	1334
Николаев В.Н. (СПбГУТ) Сотрудничество между компаниями деревянного домостроения и профессиональными сообществами на примере АДД	1338
Николаев В.Н. (СПбГУТ) Переговоры как способ развития деревянного домостроения в России.....	1342

Русова А.А., Кульназарова А.В. (СПбГУТ) Факторы узнаваемости бренда.....	1346
Стоноженко К.А. (СПбГУТ) Кинофильм "Брат" режиссера Алексея Балабанова как пример роли медиа в интерпретации периода 90-х годов.....	1350
Ядрышников В.А., Шутман Д.В. (СПбГУТ) Продвижение бренда SNKRS Clean в Telegram.....	1354
Сведения об авторах	1356



всероссийская научно-техническая и научно-методическая конференция магистрантов и их руководителей

ПКМ

**ПОДГОТОВКА ПРОФЕССИОНАЛЬНЫХ КАДРОВ
В МАГИСТРАТУРЕ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ**

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАДИОЭЛЕКТРОНИКИ

Секция 1.1.

Микроволновая техника: материалы, компоненты, устройство

УДК 621.372.543.2
ГРНТИ 47.14.13

УСТРОЙСТВА ЧАСТОТНОЙ СЕЛЕКЦИИ В ОБЪЕМНОМ ИНТЕГРАЛЬНОМ ИСПОЛНЕНИИ

А. В. Грохольский, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассматривается фильтр на основе микрополосковой линии, предлагается оригинальная конструкция устройств. Параллельный колебательный контур представлен в виде классического конденсатора на землю и проинтегрированных в него катушек индуктивности.

микроволновые интегральные схемы, объёмная интегральная схема, метаматериал, устройства частотной селекции, фильтр

Рост частоты телекоммуникационного оборудования усложняет системы радиоэлектроники и требует совершенствования технологий производства.

Создания современной радиоэлектронной аппаратуры (РЭА) невозможно без использования интегральных схем (ИС) СВЧ. Современные гибридные интегральные схемы и перспективные объёмные интегральные схемы СВЧ способны удовлетворить жёсткие требования современной РЭА. Связано это с модернизацией современных технологических процессов и вычислительных систем, позволяющих эффективно моделировать проектируемые устройства на ПК.

Повышение степени интеграции гибридных интегральных схем (увеличение плотности размещения элементов) вынуждает разработчиков искать новые подходы создания ИС СВЧ, так как старые схемотехнические решения и материалы не позволяют достигать требуемых значений коэффициента степени интеграции. Именно поэтому всё чаще применяются объёмные интегральные структуры с использованием метаматериалов, которые являются крайне перспективным решением этой задачи.

Метаматериалы – это искусственно созданные структуры, обладающие эффективными электромагнитными свойствами в том или ином диапазоне частот, выходящими за пределы свойств образующих их компонентов, которые сложно достичь технологически, и которые крайне редко встречаются в природе [1].

Неотъемлемой и одной из важнейших составляющих любого СВЧ устройства являются устройства частотной селекции. В настоящее время они применяются во многих областях радиоэлектроники, среди которых: радиолокация, радионавигация, спутниковая связь, радиобиология, мобильная связь, телевидение, беспроводной доступ в интернет, радиорелейная и космическая системы связи, телеметрия, и многое другое. Применяются фильтры для селекции частоты сигналов, подавления нежелательных помех, выделения полезных сигналов, развязки трактов приёма и передачи [2].

Существует 4 типа фильтров: ФНЧ, ФВЧ, ППФ, ПЗФ. Их характеристики приведены ниже.

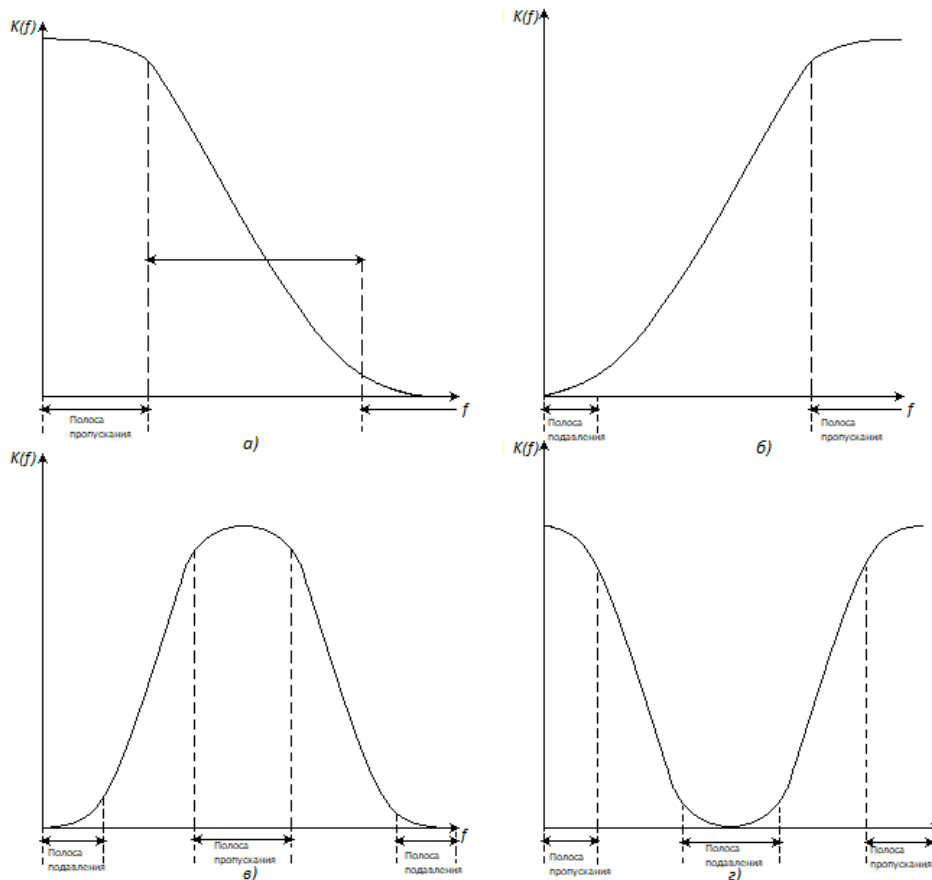


Рис. 1. АЧХ фильтров ФНЧ (а), ФВЧ (б), ППФ (в), ПЗФ (г)

Реализация всех этих характеристик в СВЧ диапазоне невозможна с помощью сосредоточенных элементов, поэтому от схем прототипов мы однозначно переходим к структурам с распределенными параметрами [3]. Обратим внимание читателя на то, что наиболее часто в СВЧ диапазоне используются полосовые фильтры.

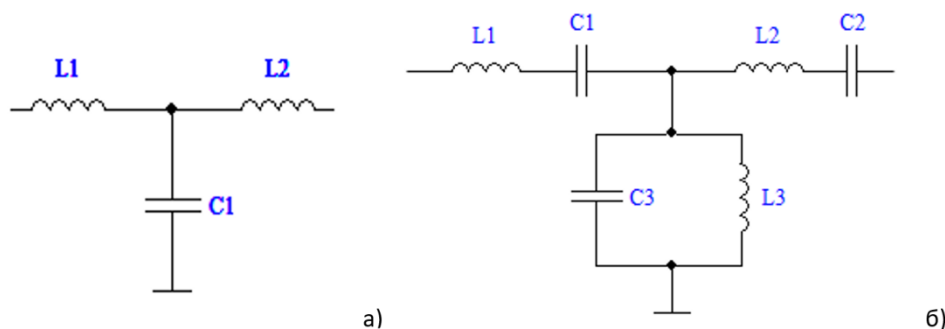


Рис. 2. Преобразование ФНЧ (а) в ППФ (б) [3]

В данном типе фильтров присутствуют параллельные резонансные контура на землю, такие контура обычно изготавливается из двух параллельных элементов (емкости и индуктивности), попытаемся их объединить в один.

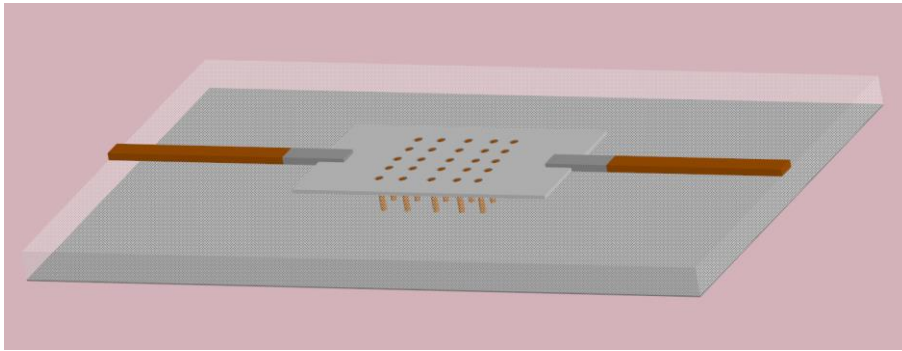


Рис. 3. Совмещённая ёмкость с индуктивностью (3D)

На рис. 3 представлена 3D модель предлагаемой конструкции СВЧ фильтра, разработанная с помощью САПР Компас 3D. Очевидно, что предлагаемый элемент обладает всеми признаками метаматериала.

Проверим его частотные свойства с помощью САПР RFSim. Принципиальная схема устройства приведена на рис. 4.

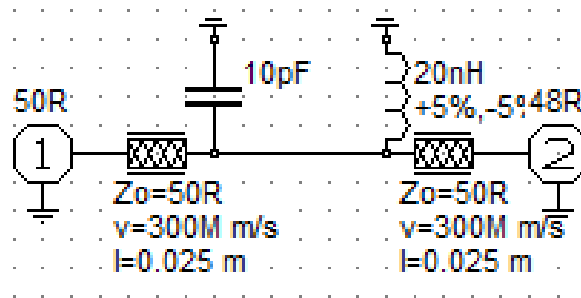


Рис. 4. Принципиальная схема параллельного контура и соединительных линий

Результатом эмуляции является АЧХ устройства (S21) представленная на рис. 5.

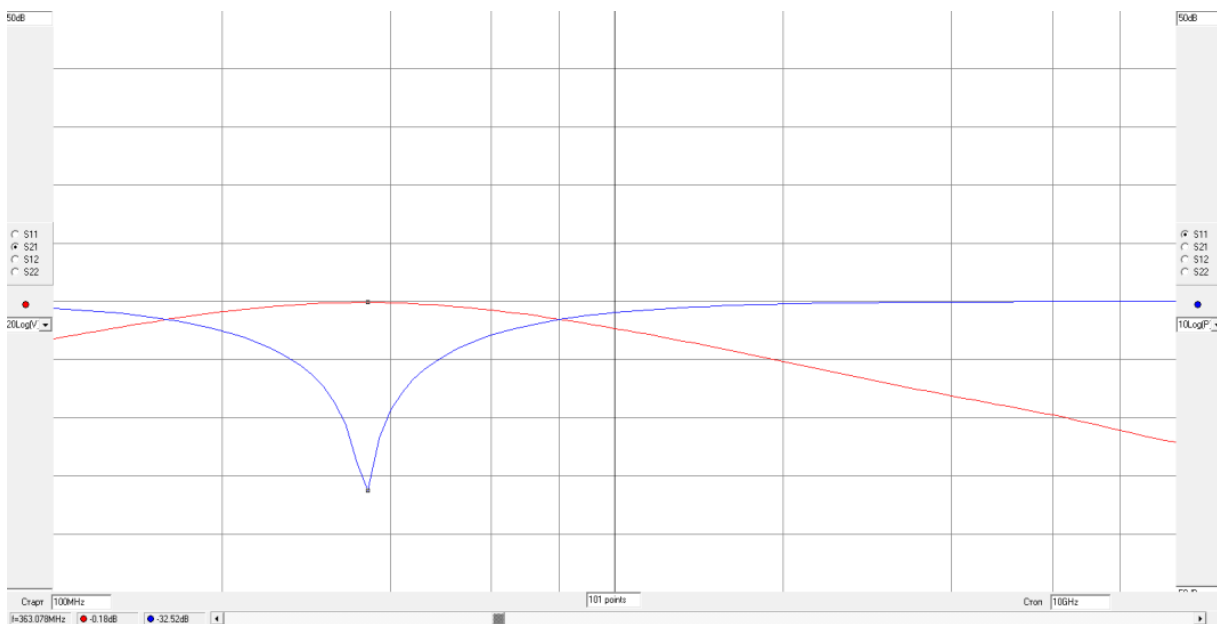


Рис. 5. S21 контура

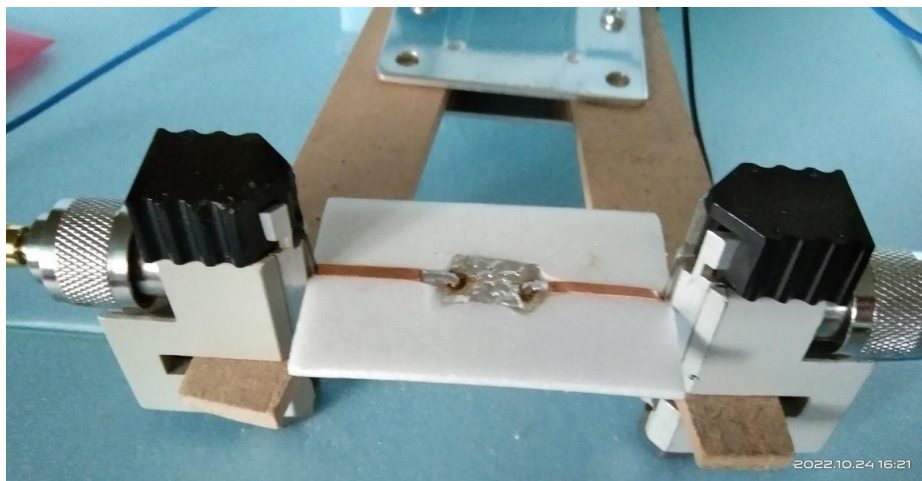


Рис. 6. Масштабный макет предложенного фильтра СВЧ

В результате работы была предложена и исследована конструкция фильтра СВЧ диапазона, включающая в себя параллельный резонансный контур на землю. Создан масштабный макет параллельного колебательного контура «на землю» (рис. 6), проведены его экспериментальные исследования. Результаты эксперимента полностью оправдали наши ожидания. В дальнейшем будет разработана конструкция ППФ нечетного порядка с несколькими такими элементами.

Список используемых источников:

1. Слюсар В. Материалы в антенной технике: основные принципы и результаты // Первая миля. 2010. Выпуск №3-4.
 2. Булатова И. А., Иванова Е. А., Крюков А. Н., Седышев Э. Ю. Шлейфные фильтры СВЧ в объёмном интегральном исполнении // Электроника и микроэлектроника СВЧ : материалы V Всерос. конф., Санкт-Петербург, 2 июня 2016 г. СПб. : СПбГЭТУ «ЛЭТИ», 2016. С. 169.
- Ханзел Г. Е. Справочник по расчету фильтров : пер. с англ. М. : Сов. радио, 1974. С. 23.

Grokholskiy A., Sedyshev E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Frequency selection devices in volumetric integral design.

The paper considers a filter based on a microstrip line, the original design of the devices is proposed. The parallel oscillatory circuit is presented in the form of a classical capacitor to the ground and inductors integrated into it.

Key words: *microwave integrated circuits, volumetric integrated circuit, metamaterial, frequency selection devices, filter.*

УДК 535.417.2
ГРНТИ 47.45.99

ДИЭЛЕКТРИЧЕСКИЕ РЕЗОНАТОРЫ В ИНТЕГРАЛЬНЫХ СХЕМАХ СВЧ

С. А. Жикин, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассматриваются микроволновые резонаторы из диэлектрика различной формы. Оцениваются различные характеристики (добротность, диэлектрическая и магнитная проницаемость, потери) с точки зрения схемотехнического применения. Исследуются возможные способы возбуждения и создания различных устройств (устройства частотной селекции, задающие контура генераторов).

объемный резонатор, диэлектрический резонатор, цилиндрический резонатор, открытый резонатор, гибридная интегральная схема, объемная интегральная схема

Резонаторы используются в широком спектре СВЧ-устройств: усилители, генераторы, передатчики, антенны, фильтры и многое другое [1, 2]. Многообразие форм и материалов резонаторов представляет большой интерес, так как они обладают различными добротностями, рабочими диапазонами частот, диэлектрической и магнитной проницаемостью, размерами. Диэлектрические резонаторы помогают разработчикам СВЧ устройств синтезировать необходимые конструкции с максимальной экономией места и возможностью создания более надежных конструкций, так как твердотельный цилиндр, куб или сфера более прочны, чем полые.

В настоящее время в СВЧ диапазоне больший интерес представляют именно диэлектрические резонаторы, в первую очередь из-за простоты обработки поверхности. У них также меньше размер, масса и выше энергетические показатели, если сравнивать с полыми объемными структурами. По отношению к шлейфам их добротность в разы выше.

В данной работе рассматриваются два вида диэлектрических резонаторов: цилиндрический резонатор с металлизацией стенки (рис. 1.) и диэлектрический цилиндрический резонатор с внутренней полостью (рис. 2.).

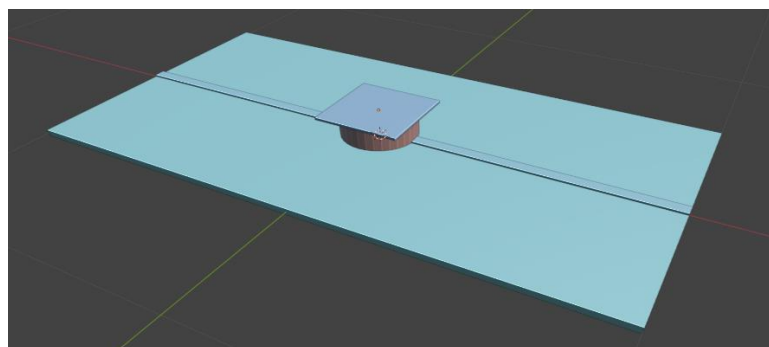


Рис. 1. 3D-модель цилиндрического резонатора с металлизированной поверхностью и возбуждением МПЛ

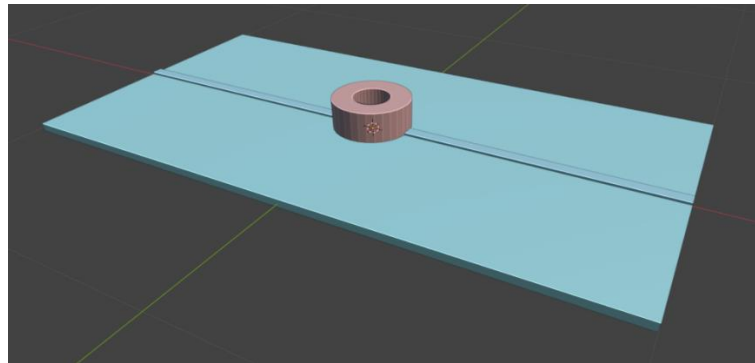


Рис. 2. 3D-модель цилиндрического диэлектрического резонатора с возбуждением МПЛ

На рис. 1 и рис. 2 представлены 3D-модели рассматриваемых резонаторов, сделанных в лицензионной программе. В первом случае конструкция представляет собой цилиндр с тонкими проводящими стенками и “крышкой”, данная конструкция при исследовании дает характеристику с ярко выраженной режекцией, порядка 30 дБ (рис. 3.).

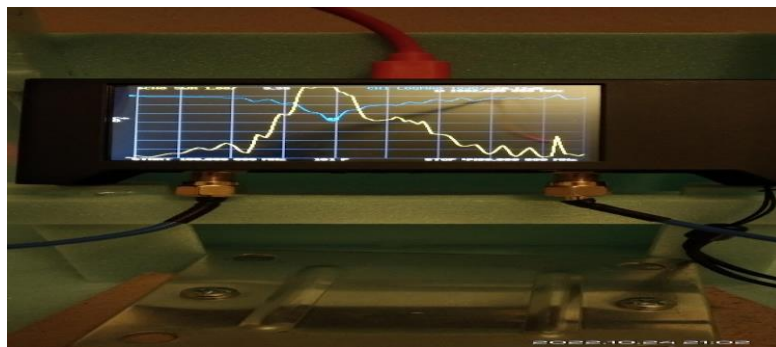


Рис. 3. Осциллограмма S21 цилиндрического резонатора

Второй резонатор представляет собой цилиндр из диэлектрика с воздушным цилиндром внутри [2]. В обоих случаях резонаторы накладываются на проводящую полосковую линию. Результат второго эксперимента приведен на следующем рисунке (рис. 4.).

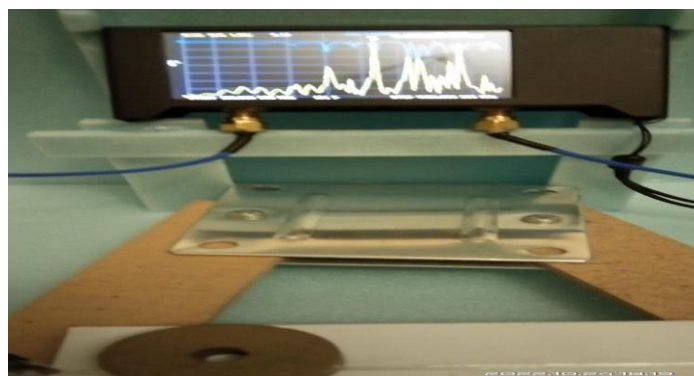


Рис. 4. Осциллограмма S21 цилиндрического резонатора из диэлектрика с воздушной полостью (без металлизации)

Можно увидеть, что у цилиндра с “крышкой” резонанс более чистый, а также ярко выраженный, когда у цилиндра без “крышки” проявляется множество дополнительных резонансных мод.

Рассмотрим эквивалентную схему резонатора, которая представлена на рис. 5, схема представляется собой RLC-контур, где и возбуждаются колебания. Параметры были подобраны таким образом, чтобы в большей степени соответствовать экспериментальным характеристикам цилиндра с “крышкой”. Сама же эквивалентная схема представлена в программном пакете RFSimm. Эмуляционная характеристика представлена на рис. 6.

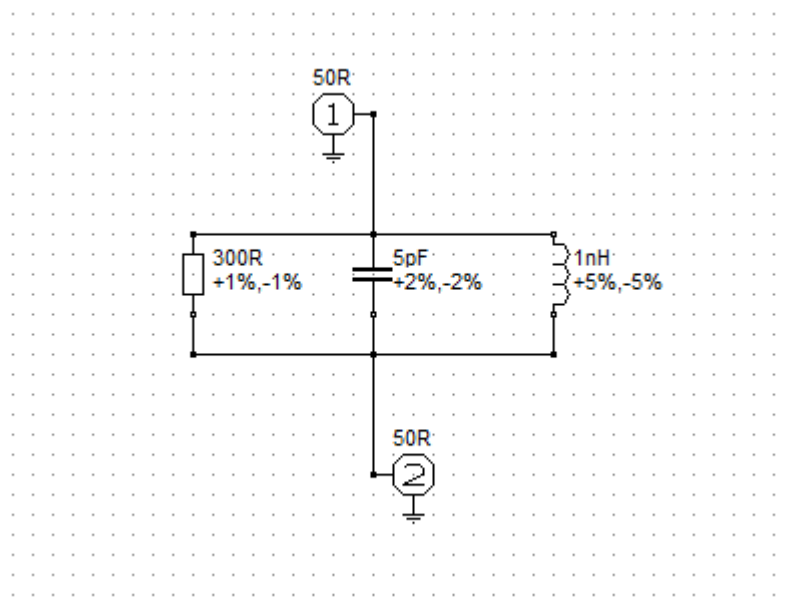


Рис. 5. Эквивалентная схема резонатора

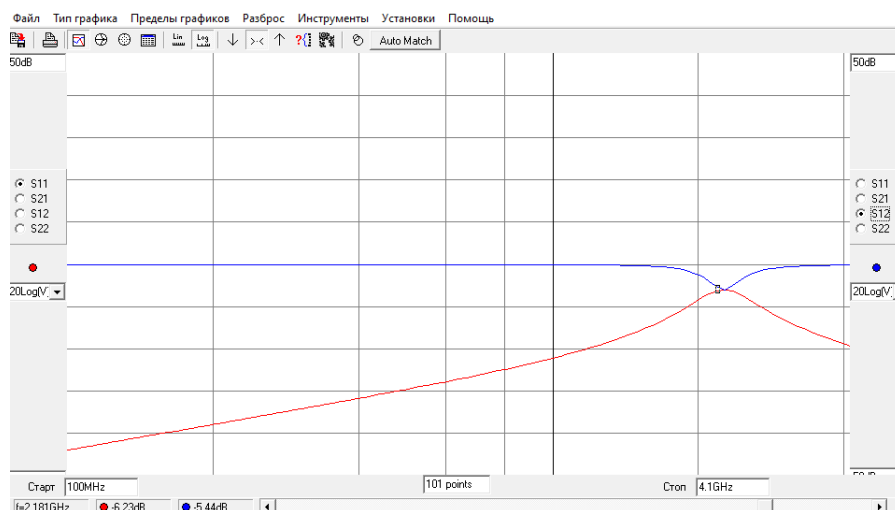


Рис. 6. Характеристики S11, S21 диэлектрического резонатора в виде цилиндра

Характеристика масштабного макета имеет похожий характер, как и та, что получена в программном пакете. Включение резонатора в линию (рис. 1,2) можно попытаться представить обычной принципиальной схемой с традиционным набором элементов. На основе таких масштабных макетов можно создавать промышленные прообразы различных устройств СВЧ [3]. Основной

задачей дальнейшей работы станут поиски способов возбуждения диэлектрических резонаторов, создание на их основе макетов различных устройств (частотной селекции, генераторов), повышение степени интеграции ГИС с диэлектрическими резонаторами.

Список используемых источников:

1. Кондрашова М.А., Седышев Э.Ю. // Эллиптический резонатор на модифицированном компланарном волноводе, СПбГУТ СПб.: Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), 2019, с. 417-419.

2. Кондрашова М. А., Седышев Э. Ю. Синтез компланарного резонатора на цилиндрической поверхности // Актуальные проблемы инфотелекоммуникаций в науке и образовании: материалы VI Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 01-02 марта 2017 г. СПб. : СПбГУТ, 2017. С. 386–391.

Гвоздев В. И., Нефёдов Е. И. Объёмные интегральные схемы СВЧ. М. : Наука. Главная редакция физико-математической литературы, 1985. 256 с.

Zhikin C., Sedyshev E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Dielectric resonators in integrated microwave circuits.

Microwave dielectric resonators of different shapes are considered in this work. Various characteristics (quality factor, dielectric and magnetic permeability, losses) are evaluated. Possible ways of excitation and creation of various devices (frequency selection devices, setting oscillator circuits) are investigated.

Key words: *volume resonator, dielectric resonator, cylindrical resonator, open resonator, hybrid integrated circuit, volume integrated circuit.*

УДК 621.373.52
ГРНТИ 47.45.99

ВОЛНОВОДНЫЙ ГЕНЕРАТОР С ИНТЕГРИРОВАННЫМ РЕЗОНАТОРОМ

Е. И. Книгиницкий, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена рассмотрению некоторых проблем передачи и генерации электромагнитных волн СВЧ диапазона. Обозначаются сферы применения данных микроволновых элементов и устройств. Представлены несколько конструктивных решений генерационных систем, их достоинства и недостатки, в том числе оригинальная конструкция устройства возбуждения колебаний в волноводе. Итогом работы является точная постановка задачи синтеза высокостабильных волноводных генераторов с интеграцией внутрь волновода в качестве задающего элемента объемной интегральной схемы.

объемная интегральная схема, микроволны, генератор, волновод, диод с отрицательным сопротивлением

Развитие информационных технологий приводит к постоянному повышению скорости передачи информации, что в свою очередь вынуждает разработчиков переходить к использованию всё более высоких частот.

Постоянный рост частоты телекоммуникаций приводит к изменению элементной базы устройств генерации и передачи энергии. Тенденции роста частоты обуславливают необходимость перехода от привычных и удобных в эксплуатации коаксиальных кабелей к жестким волноводам. Однако не все устройства адаптированы для работы с волноводными трактами. До сих пор в радиоэлектронике приходилось мириться с высокими потерями коаксиальных кабелей, но альтернативы им порой найти не удавалось. Так, подключение генератора к волноводу осуществляют посредством коаксиального кабеля, вводя энергию в волновод при помощи элементов связи, изображенных на рис. 1 [1]. Такое подключение долгое время было единственно возможным, однако с переходом в сантиметровый диапазон параметры коаксиального кабеля резко ухудшаются, поэтому следует искать новые способы возбуждения колебаний в волноводе.

Сегодня существует множество приложений радиоэлектроники, где использование коаксиальных кабелей серьезно ухудшает показатели устройств и систем в целом. К таким отраслям относятся дальняя космическая связь, устройства управления беспилотными летательными аппаратами и борьбы с ними, радиолокация, радиобиология, ядерные исследования и др.

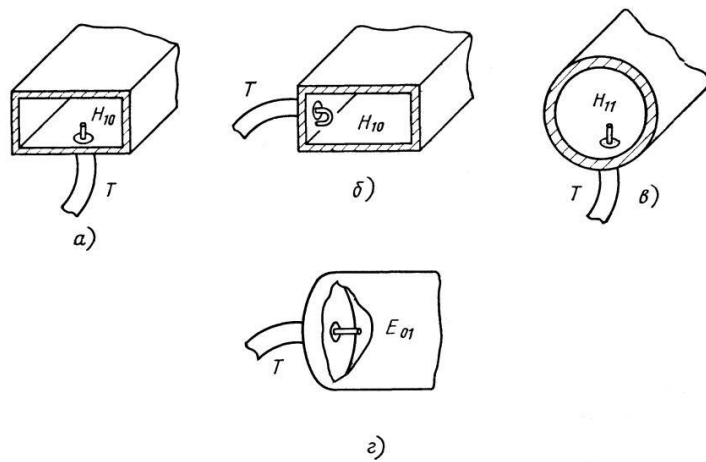


Рис. 1. Элементы связи коаксиального кабеля с волноводом

Основным преимуществом коаксиального кабеля является его гибкость, однако это не позволяет использовать его для типов волн кроме T . Это связано с тем, что критическая длина волны для полей типа H_{11} и E_{01} соизмерима с диаметром кабеля, а при таком соотношении шероховатость гибких стенок кабеля приводит к недопустимому ослаблению распространяющейся волны. Структура поля в коаксиальном кабеле представлены на рис. 2 [1].

Топология поля для коаксиального кабеля и круглого волновода отличаются. Это приводит к изменению типа поля при возбуждении волновода коаксиальным кабелем. Структура поля в круглом волноводе представлена на рис. 3 [1]. Исходя из этого целесообразной будет интеграция устройств возбуждения электромагнитных колебаний напрямую в волновод. Это улучшит показатели тракта передачи энергии и установит неизменную топологию поля.

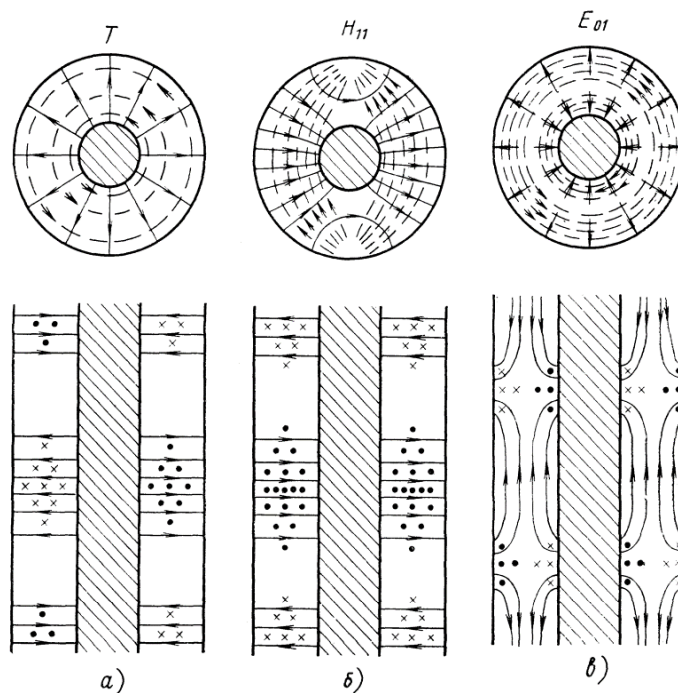


Рис. 2. Волны типа T , H_{11} и E_{01} в коаксиальном кабеле

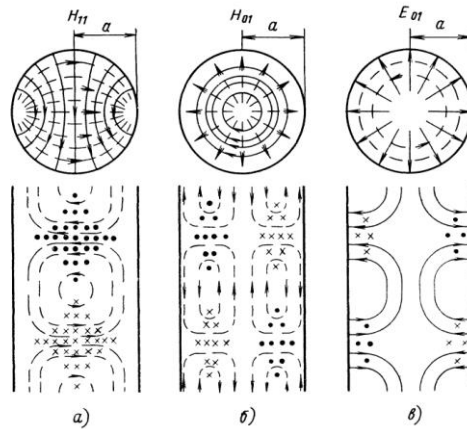


Рис. 3. Структура полей типа H_{11} , H_{01} и E_{01} в круглом волноводе

Комбинация генератора на полусфере [2] и круглого волновода выглядит наиболее логичной в связи с соответствием форм элементов. Кроме того, возможно использование проволочного эквивалента полусферического резонатора, предложенного в работе Е. И. Бочарова, Е. А. Коноваловой и Э. Ю. Седышева [3]. Схематичное изображение модели, представленное в их совместной работе показано на рис. 4. Также допускается использование планарных кольцевых резонаторов [4].

В работе рассматривается конструкции генератора, для которой волновод выполняет не только роль линии, но и содержит интегрированный узел генерации, как показано на рис. 5. Сконструированный таким образом генератор автоматически будет иметь волноводный выход.

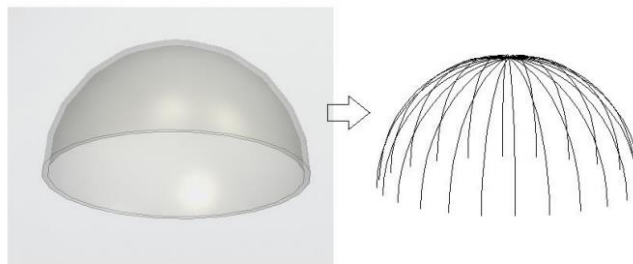


Рис. 4. Модель проволочного эквивалента [3]

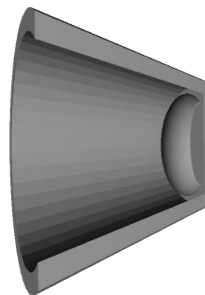


Рис. 5. Упрощенная модель волноводного генератора в сечении

В данной структуре предусмотрен вывод возбужденного в резонаторе микроволнового колебания в волновод через щели между элементами конструкции. В случае использования планарного резонатора, возбуждение может осуществляться спиральной структурой [5].

В связи с тем, что такая конструкция волноводного генератора является новой, для неё требуется создание математической и компьютерной моделей. В качестве основы возможно использование уже имеющихся в смежной области разработок, касающихся сферических резонаторов [6]. В связи с этим остаются нерешенными вопросы соответствия резонансной частоты генератора и критических длин волн круглого волновода. Также под вопросом находится геометрия и размер зазоров для наиболее эффективного вывода энергии из резонатора с сохранением стабильной генерации.

Существует довольно большой ряд конструктивных задач, таких как крепление резонатора с минимальным влиянием на распространяющуюся волну, подключение активного элемента генератора к источнику питания, разделение сегмента с резонатором и собственно волновода связи.

Основным результатом представленного исследования можно считать синтез рабочей модели генератора с монохромным колебанием на выходе круглого (прямоугольного) волновода.

Список используемых источников:

1. Фальковский О. И. Техническая электродинамика : учебник. СПб. : Лань, 2009. 432 с. ISBN 978-5-8114- 0980-8. EDN QMUAZL.
2. Бочаров Е. И., Коновалова Е. А., Седышев Э. Ю. СВЧ генератор на полусфере // Электроника и микроэлектроника СВЧ. 2021. Т. 1. С. 426-429.
3. Бочаров Е. И., Коновалова Е. А., Седышев Э. Ю. Исследование проволочной модели полусферы в качестве резонатора СВЧ // Подготовка профессиональных кадров в магистратуре для цифровой экономики : материалы регион. научно-методич. конф., Санкт-Петербург, 01–03 дек. 2020 г. СПб. : СПбГУТ, 2021. С. 322-325.
4. Сазоненко Н. Ю., Седышев Э. Ю. Устройства частотной селекции на основе кольцевого эллиптического резонатора на микрополосковой линии // Электроника и микроэлектроника СВЧ. 2019. Т. 1. С. 409-411.
5. Глухов Н. И., Лепихин К. А., Седышев Э. Ю. Спиральная структура в качестве питающего элемента круглого волновода // Электроника и микроэлектроника СВЧ. 2021. Т. 1. С. 423-425.
6. Бочаров Е. И., Рынгач Е. В., Седышев Э. Ю. Математическая модель нагруженного сферического резонатора на его резонансных частотах // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы III Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 25–26 фев. 2014 г. СПб. : СПбГУТ, 2014. С. 546-550.

Kniginickii E., Sedyshev E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Microwave generators with integrated resonator.

The article deals with the issues of transmission and initiation of microwave electromagnetic oscillations. The Application areas of the microwave elements and devices with frequency range as well as some generating systems with their advantages and disadvantages are presented. The challenge of synthesis stable waveguide generators with core element as three-dimensional integrated circuit is set.

Key words: volumetric integrated circuit, microwaves, generator, waveguide, diode with negative resistance.

УДК 621.373.52
ГРНТИ 47.45.99

ГЕНЕРАТОР ШУМА СВЧ НА ПОЛУПРОВОДНИКОВОМ ДИОДЕ В ИНТЕГРАЛЬНОМ ИСПОЛНЕНИИ

А. К. Ларионова, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена синтезу генератора шума (ГШ) микроволнового диапазона. Предложена принципиально новая конструкция СВЧ ГШ на полупроводниковом элементе, выполнено моделирование и макетирование устройства. В работе приводятся результаты эксперимента, которые доказывают правильность выдвинутых предположений, а также работоспособность предложенного устройства. В заключении работы сравниваются характеристики генерационного шума в зависимости от напряжения питания.

микроволновый диапазон, СВЧ, генератор, активный двухполюсник, генератор шума

Шум СВЧ диапазона является на сегодняшний день единственным решением проблем понижения мощности передаваемого сигнала с ростом частоты. При правильном выборе типа модуляции (кодирования) шум может стать носителем данных. Все это делает расчет и синтезирование генераторов шума микроволнового диапазона одним из перспективных направлений микроволновой электроники в частности и микроэлектроники в целом.

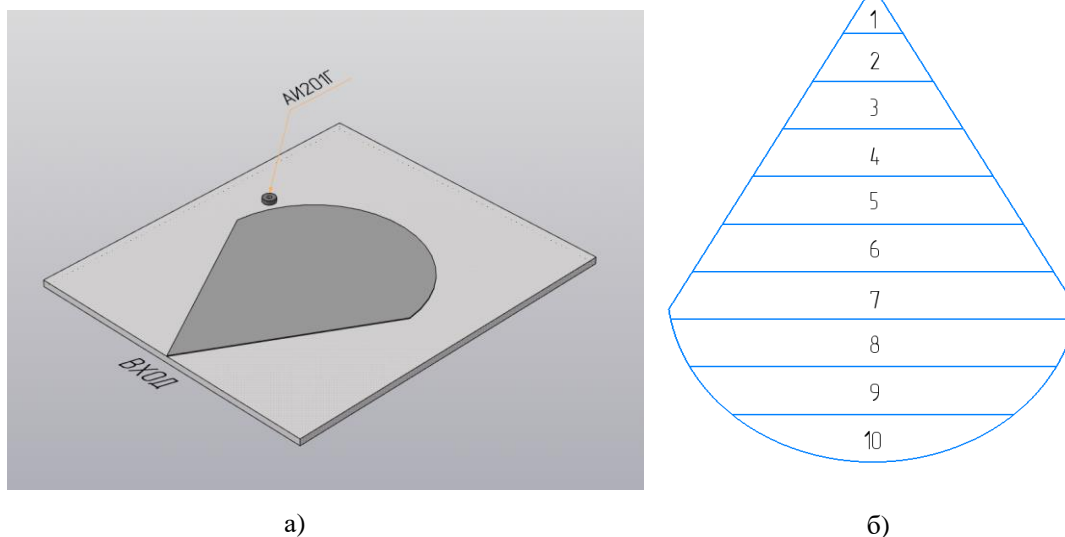


Рис. 1. Предлагаемая конструкция СВЧ генератора шума (а) и его секционная детализация (б)

Конструкция синтезированного генератора представляет собой нерегулярный шлейф в режиме холостого хода и представлена на рис. 1а. Для того, чтобы корректно промоделировать данное устройства было решено использовать принцип декомпозиции. Полученную структуру необходимо

разбить на небольшие участки, которые будут характеризоваться каждый своим волновым сопротивлением (рис. 1б).

В работе «Исследование микроволнового генератора на кольцевом резонаторе» [1] было предложено при моделировании конструкций с активным двухполюсником (а именно туннельным диодом) рассматривать последний с учетом всех его параметров, а не только дифференциальное отрицательное сопротивление. Стоит принять во внимание паразитные емкости диода и индуктивность его корпуса, так как у этих элементов есть свои факторы влияния. Учитывая эквивалентную схему замещения туннельного диода и секционную декомпозицию предложенного шлейфа, была получена принципиальная схема СВЧ генератора. Моделирование производилось в программе RFSim99, результаты приведены на рис. 2.

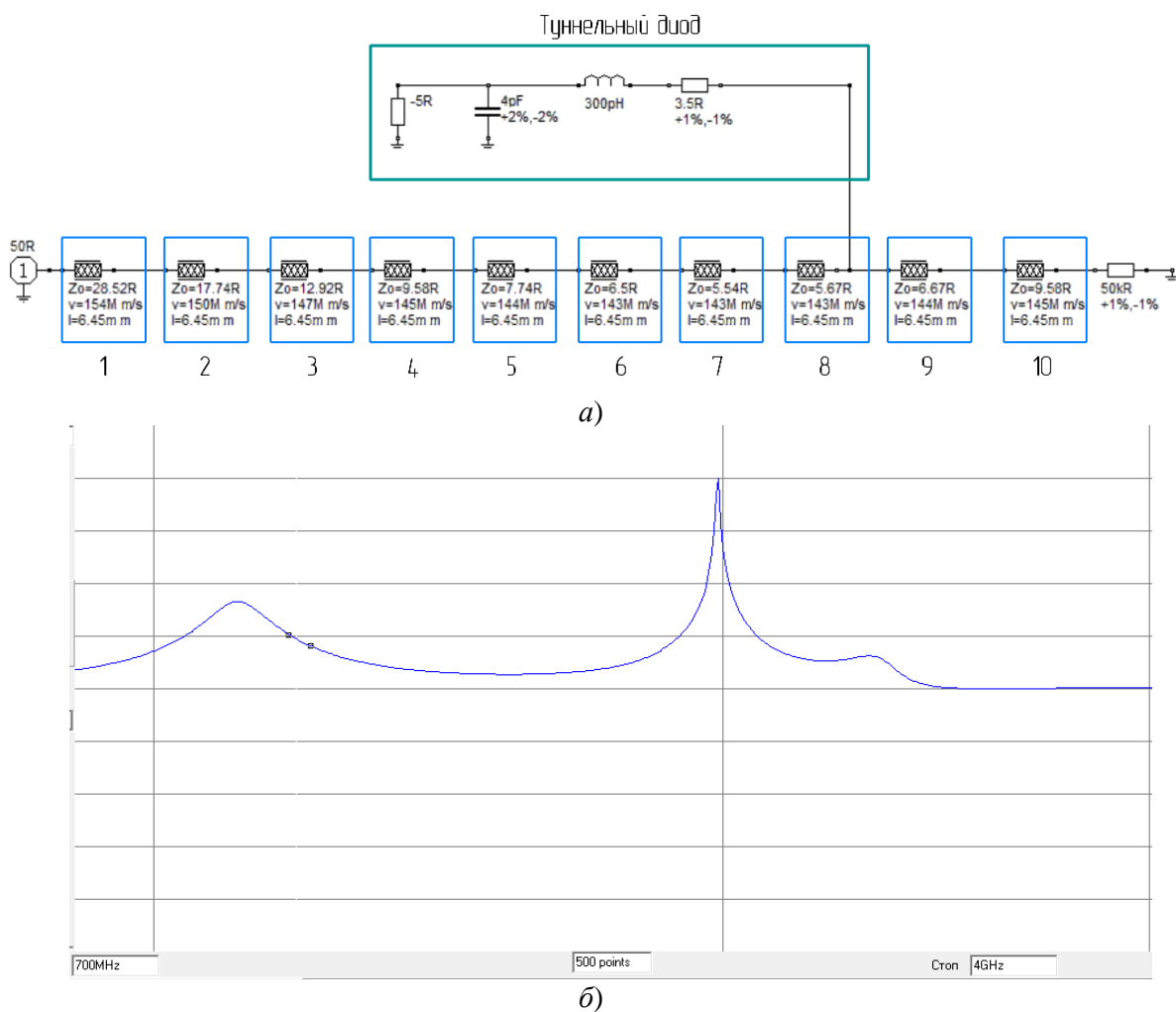


Рис. 2. Прецизионная схема исследуемой структуры (а) и ее АЧХ, полученная в САПР RFSim99(б)

На полученной характеристике можно увидеть шум не во всем, а только в некотором диапазоне частот. В этом заключается принципиальное отличие предложенной конструкции генератора СВЧ, от исследуемых ранее в работе [1], где исследуемые модели представляли собой генераторы шума с шумовыми характеристиками во всем исследуемом диапазоне частот.

По результатам моделирования был изготовлен макет ГШ в Лаборатории синтеза СВЧ устройств СПбГУТ и проведены измерения реальных спектральных характеристик. Результаты макетирования и эксперимента представлены на рис. 3 и 4.

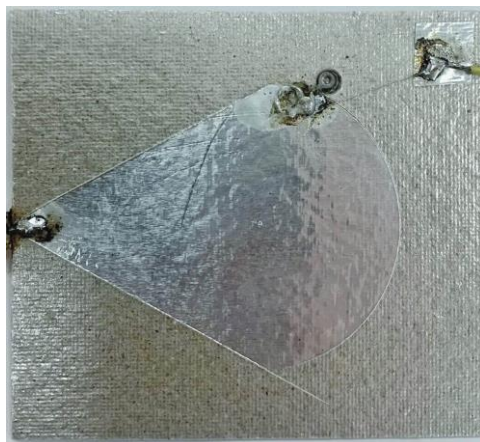


Рис. 3. Исследуемый макет ГШ

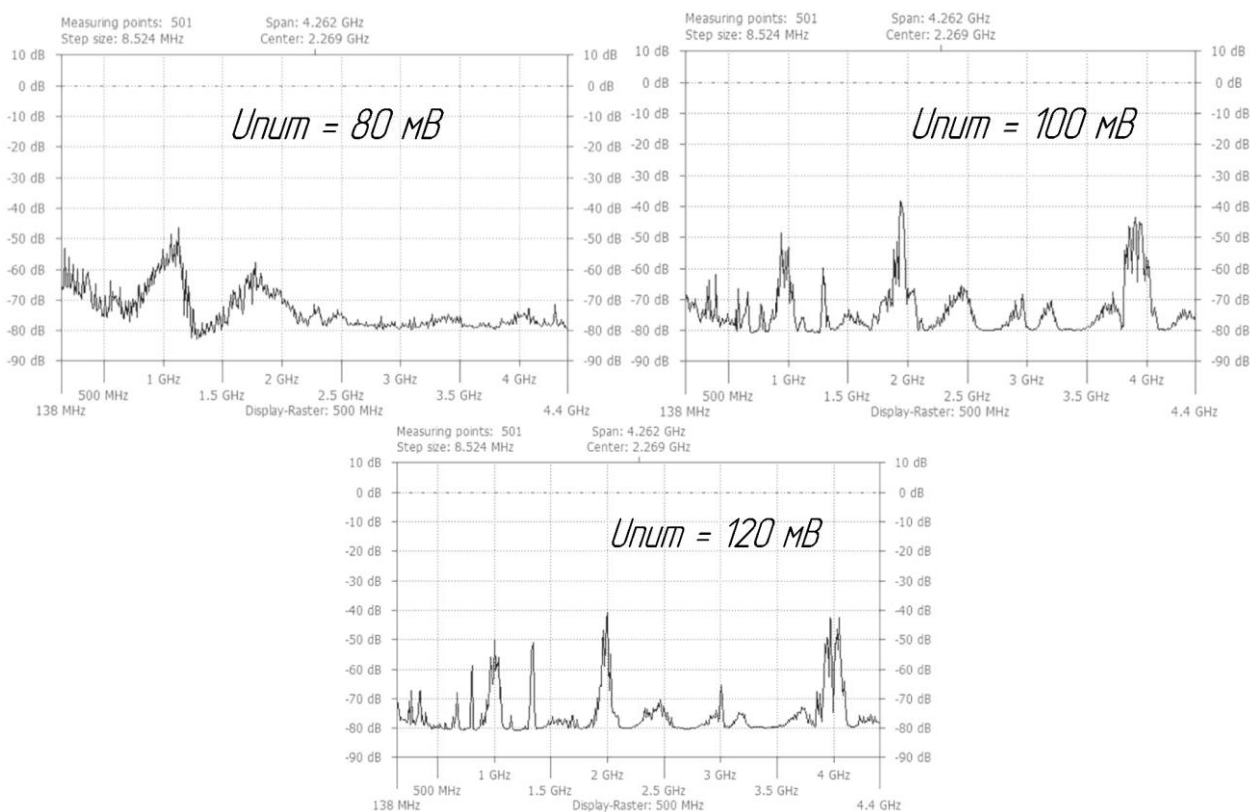


Рис. 4. Экспериментально полученные характеристики исследуемого макета

На основе полученных осциллограмм, можно заметить, как изменяется выходная характеристика при увеличении питающего напряжения ($U_{пит.д}$) туннельного диода. Связано это с вариативностью эквивалентной схемы активного элемента: в зависимости от питающего напряжения, номиналы паразитных составляющих схемы замещения, а также отрицательное

дифференциальное сопротивление диода меняются. Общая эквивалентная схема замещения диода для различных значений $U_{пит.д}$ пока не разработана.

Генератор на эквивалентном двухполюснике можно рассматривать, как усилитель, охваченный положительной обратной связью (ПОС) (рис. 5). В таком режиме коэффициент усиления усилителя стремится к бесконечности, что приводит к самовозбуждению структуры. Таким образом усилительная структура превращается в генерационную. В стандартном случае роль управляющего резонатора автогенератора играет разомкнутая микрополосковая линия (МПЛ). В предложенной конструкции генератора МПЛ является нерегулярной, что влияет на добротность резонатора, а соответственно и на получение шума в диапазоне частот.

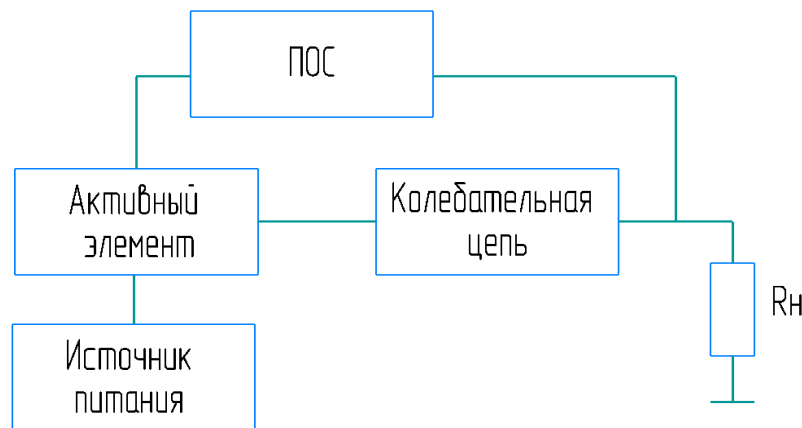


Рис. 5. Структурная схема автогенератора с ПОС

В результате работы синтезирован простой генератор шума, который эффективно генерирует шум в начале СВЧ диапазона. Конструкция отличается простотой и наличием элементов подстройки характеристик выходного шума.

Список используемых источников:

1. Ларионова А. К., Седышев Э. Ю. Исследование микроволнового генератора на кольцевом резонаторе // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы XI междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 15-16 фев. 2022 г. СПб. : СПбГУТ, 2022. С. 645-651.
2. Каткова Т. О., Седышев Э. Ю. Синтез микроволнового генератора на кольцевом эллиптическом резонаторе по рабочим параметрам. // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы XI междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 15-16 фев. 2022 г. СПб. : СПбГУТ, 2022. С. 584-589.
3. Радиопередающие устройства / под ред. О. А. Челнокова, М. : Радио и связь, 1982. с. 212.
4. Отчет о НИР «Разработка принципов построения твердотельных сверхширокополосных источников хаоса микроволнового диапазона повышенной энергоэффективности», Институт радиотехники и электроники им. В. А. Котельникова РАН, 2016г.
5. Мясин Е. А. Генерация шума в одночастотном генераторе на лавинно-пролетном диоде миллиметрового диапазона длин волн под воздействием низкочастотного гармонического колебания // Письма в ЖТФ. 2021. Т. 47. вып. 22. С. 33-36.

Larionova A., Sedyshev E.

The Bonch-Bruевич St. Petersburg State University of Telecommunications

Microwave noise generator on a semiconductor diode in integrated version.

The work is devoted to the synthesis of a noise generator of the microwave range. A fundamentally new design of a microwave noise generator on a semiconductor element is proposed, modeling and layout of the device is performed. The paper presents the results of the experiment, which prove the correctness of the assumptions made, as well as the operability of the proposed device. In conclusion, the characteristics of the generation noise are compared depending on the supply voltage.

Key words: *microwave range, microwave, generator, active bipolar, noise generator.*

УДК 621.372.211
ГРНТИ 47.45.99

УСТРОЙСТВА ЧАСТОТНОЙ СЕЛЕКЦИИ С ВОЗМОЖНОСТЬЮ ПЕРЕРАСПРЕДЕЛЕНИЯ МОЩНОСТИ НА КЭР

А. С. Леонтьев, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена исследованию применений кольцевых эллиптических резонаторов СВЧ диапазона в объёмных интегральных схемах, а также устройств на основе кольцевых эллиптических резонаторов (КЭР). Проанализированы работы последнего времени посвященные применению КЭР в микроволновых устройствах. Целью работы является попытка систематизации материалов посвященных КЭР.

СВЧ, эллиптический резонатор, бегущая волна, кольца, усилители, генераторы, фильтры, делители, сумматоры, МПЛ, КПЛ, КЭР

Для исследования, проектирования и производства современных средств связи всё чаще используются объёмные устройства микроволнового диапазона. В устройствах СВЧ большое значение придается конструктивным элементам интегральных схем (ИС). Конструктивные элементы реализовываются единым технологическим циклом при создании проводящих или диэлектрических пленок (топологии проводников и диэлектриков). Применяемость конкретных топологических решения для конструктивных элементов зависит не только от частотного диапазона, но и от материалов. Одно устоявшееся топологическое решение, может быть, неприменимо в разных частотных диапазонах из-за технических ограничений производства, поэтому поиск новых конструктивных решений в микроволновой технике никогда не прекращается.

В качестве резонансных конструктивных элементов ИС СВЧ часто используются шлейфные резонаторы, представляющие собой отрезки полосковых линий, соединенные с основной линией передачи. Шлейфы используются для создания фильтров разных типов, для настройки и согласования различных элементов, блокировки и развязки различных трактов ИС СВЧ. На их основе создаются устройства распределения энергии за счёт ёмкостной связи между линиями [1, 2]. Привычным типом линии для создания шлейфа является МПЛ, однако такая линия обладает низкой добротностью, что ограничивает возможности её применения, а для достижения требуемых характеристик тех же самых фильтров требуется создавать структуры высокого порядка.

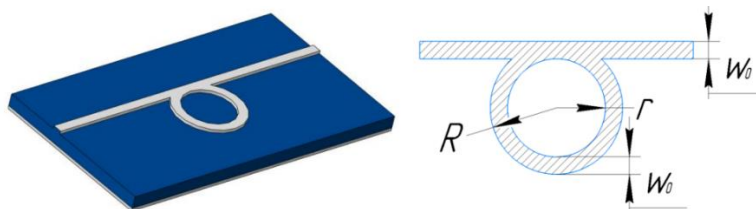


Рис. 1. Модель КЭР на микрополосковой линии

В качестве альтернативы шлейфным резонаторам могут использоваться кольцевые эллиптические резонаторы (КЭР), представляющие собой замкнутые металлизированные полосковые линии, связанные с основной линией передачи (рис. 1). Структура элемента кольцевого эллиптического резонатора проста, что позволяет создавать на его основе множество различных типов конструктивных элементов.

Устройства частотной селекции.

Размер кольца и резонансная частота напрямую зависят друг от друга, зависимость геометрии и резонансной частоты колец ранее была исследована в работе [3]:

$$f_{рез1} = \frac{c}{\lambda\sqrt{\epsilon}}, \tag{1}$$

$$l_{ср} = n\lambda, \tag{2}$$

$$f_{рез2} = \frac{1}{2\pi\sqrt{LC}}, \tag{3}$$

где c – скорость света в вакууме, м/с; λ – длина волны, которая зависит от длины кольца, м; ϵ – диэлектрическая проницаемость подложки, $l_{ср}$ – длина кольца по средней линии, м; $n = 1, 2, 3, \dots$, L – эквивалентные индуктивность и ёмкость эллиптического резонатора, Гн и Ф соответственно.

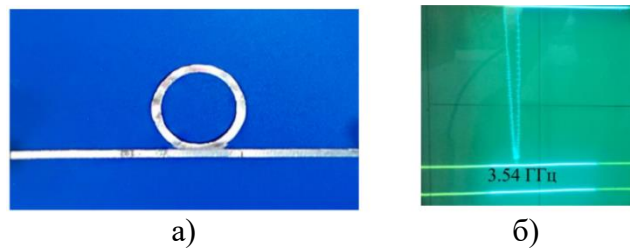


Рис. 2. Макет КЭР на микрополосковой линии (а) и АЧХ резонатора (б)

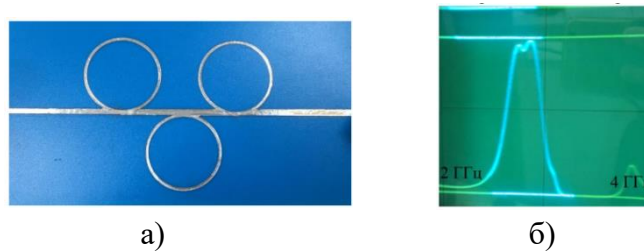


Рис. 3. Макет ППФ на КЭР (а) и АЧХ резонатора (б).

По результатам макетирования (рисунки 2 и 3) были сделаны выводы о работоспособности КЭР и возможности построения на его основе фильтров различных типов.

В работе [4] рассмотрены несколько способов интеграции кольцевых резонаторов в структуры фильтров без прямой гальванической связи (рисунки 4 и 5).

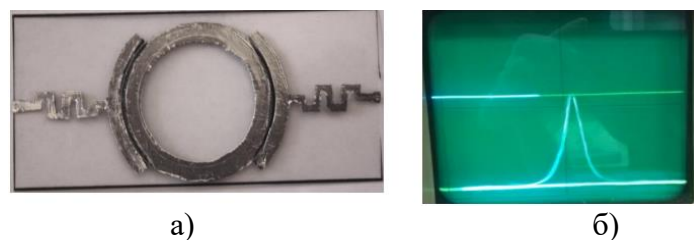


Рис. 4. Макет КЭР на МПЛ (а) и АЧХ резонатора (б)

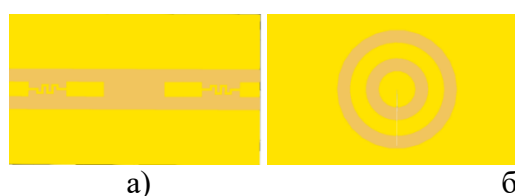


Рис. 5. Модель КЭР на МПЛ нижний (а) и верхний (б) слой.

Данное исследование показало возможность построения КЭР на разных типах линий.

Также рассматривались КЭР на копланарных волноводах (рис. 6) и модифицированных копланарных линиях. (рис. 7) [5-7].



Рис. 6. Модели КЭР на копланарном волноводе с питанием от КПЛ с АЧХ (а, б) и МПЛ с АЧХ (в, г)

В работах [8, 9] была исследована зависимость изменения резонансной частоты от изменений диэлектрической проницаемости и тангенса угла потерь жидкости, проходящей через КЭР, вызванные изменением состава жидкости, а на её основе создан микроволновый датчик для анализа качества масла (рис. 8).



Рис. 7. Макет КЭР на модифицированном копланарном волноводе.

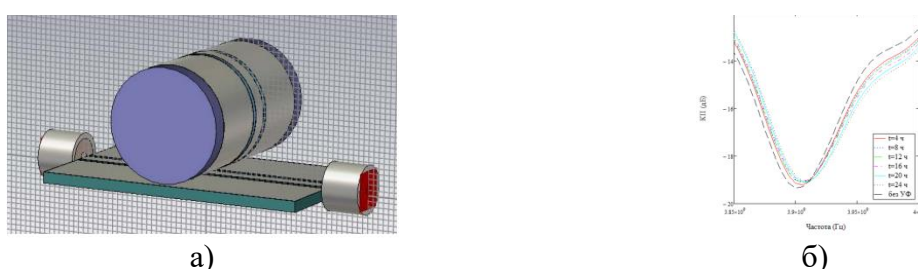


Рис. 8. Модель (а) и зависимость резонансной частоты датчика от качества масла (б)

Результаты этих исследований показывают возможности применения КЭР в разных областях инженерии.

Усиление и сложение мощности активных двухполюсников.

Помимо устройств частотной селекции КЭР нашли применение в качестве элемента для построения усилителей частоты. В работе [10] КЭР объединили с туннельным полупроводниковым диодом, такая конструкция позволила добиться усиления до 14 дБ на требуемой частоте, обеспеченной КЭР (рис. 9).



Рис. 9. Макет усилителя на активном двухполюснике (а) и его АЧХ (б).

Исследованию одновременного включения нескольких активных двухполюсников посвящены работы [11, 12] (рис. 10).

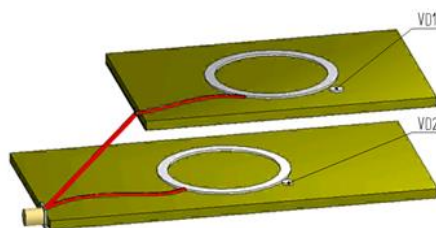


Рис. 10. Модель включения активных двухполюсников для сложения мощности

Главным результатом которых является постановка задачи синхронизации работы активных двухполюсников для повышения эффективности сложения их мощностей.

Генерация СВЧ на КЭР в ОИС.

Резонансный характер АЧХ КЭРа также можно использовать для построения нового типа генераторов на КЭР. Решению этой задачи посвящены работы [13, 14]. В данных исследованиях удалось добиться хорошей сходимости результатов моделирования и эксперимента (рис. 11).

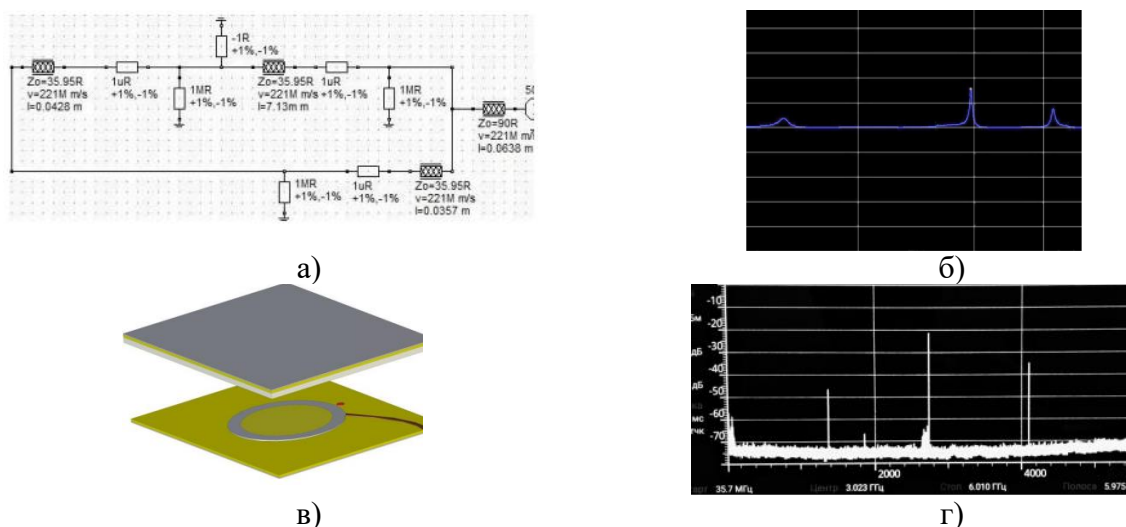


Рис. 11. Модель (а) и расчёт (б) в RFSimm, 3D-модель (v) и результаты эксперимента (г) генератора СВЧ на КЭР в ОИС

Распределение мощности.

Не смотря на узкую полосу рабочей частоты кольцевые резонаторы можно использовать для передачи и распределения мощности между различными каналами в устройстве. Данный способ коммутации описывается в [15], где предлагается совмещать некоторое количество n КЭР разных диаметров друг над другом связывая их, при этом каждое плечо обладает своей АЧХ. При достаточно большом n и малом

расстоянии между КЭР, образуется цилиндрическая волноводная структура со множеством источников ввода и вывода сигнала, как на рис. 12.

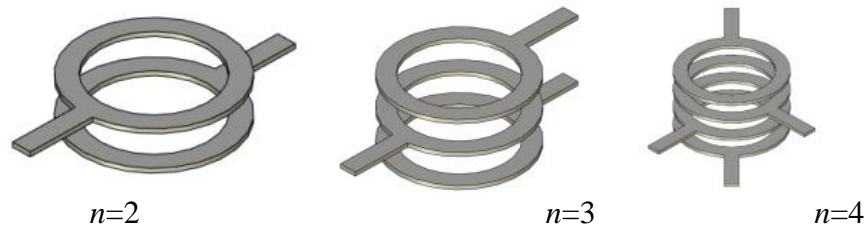


Рис. 12. Эллиптические конструкции с разным количеством n

Для построения КЭР можно выбирать различные типы линий: МПЛ, КПЛ, щелевые линии и т.д. КЭР нашла множество применений в устройствах частотной селекции, конструкции усилителей, генераторов на КЭР, устройств распределения мощности и даже создания невзаимных устройств [16]. Большинство макетов изготовлено аппликационным методом на органических диэлектриках, экспериментально доказана их работоспособность. Применение промышленных материалов и промышленных технологий изготовления однозначно улучшат характеристики устройств на КЭР. Результаты множества исследований и проведенных экспериментов позволяют говорить о дальнейшем развитии целого класса устройств построенных с применением кольцевых эллиптических резонаторов.

Список используемых источников:

1. Леонтьев А.С., Седышев Э.Ю., Синтез устройства частотной селекции на кольцевых эллиптических резонаторах в объёмном интегральном исполнении, материалы Международной научно-технической конференции «Перспективные технологии в средствах передачи информации», Владимирский государственный университет им. А.Г. и Н.Г. Столетовых, г. Владимир, 2021. С. 390-392.
2. Лебедев Л., Наместников Е., Седышев Э. Ю. Синтез широкополосных переходов для объёмных интегральных схем СВЧ // СВЧ электроника. 2019. Т. 2 С. 4-6.
3. Сазоненко Н. Ю., Седышев Э. Ю. Устройства частотной селекции на основе кольцевых эллиптических резонаторов на микрополосковой линии // Электроника и микроэлектроника СВЧ. 2019. Т. 1. С. 409-411.
4. Бочаров Е. И., Рыбалко И. А., Седышев Э. Ю., Селиверстов Л. А., Сикора Г. Р. Микроволновые фильтры на эллиптических резонаторах в объёмном интегральном исполнении // Электроника и микроэлектроника СВЧ. 2017. Т. 1. С. 535-538.
5. Кондрашова М.А., Седышев Э.Ю., Эллиптический резонатор на модифицированном копланарном волноводе // Актуальные проблемы инфо-телекоммуникаций в науке и образовании: сборник научных статей VIII Международной научно-технической и научно-методической конференции АПИНО 2019: в 4 томах. 2019. С. 410-418.
6. Кондрашова М. А., Сазоненко Н. Ю., Селиверстов Л. А., Улитина А. С., Седышев Э. Ю. Частотноселективные устройства на кольцевых эллиптических резонаторах // Электроника и микроэлектроника СВЧ. 2019. Т. 1. С. 417-419.
7. Улитина А. С., Седышев Э. Ю. Синтез кольцевого эллиптического резонатора на несимметричной щелевой линии // Электроника и микроэлектроника СВЧ. 2019. Т. 1. С. 412-416.
8. Коркина А.Р., Микроволновый датчик для анализа примесей в оливковом масле, статья в сборнике трудов конференции // XXV Туполевские чтения (школа молодых ученых): статья в сборнике трудов конференции. Казанский национальный исследовательский технический университет им. А.Н. Туполева. Казань 2021. С. 166-171.
9. Коркина А. Р., Насыбулина А. Р., Фархутдинов Р. В. СВЧ-датчик на основе объёмного копланарного кольцевого резонатора для анализа качества оливкового масла // Взаимодействие сверхвысокочастотного, терагерцового и оптического излучения с полупроводниковыми микро- и наноструктурами, метаматериалами и биообъектами :

сборник статей IX Всерос. науч. школы-семинара. Саратов : Изд-во «Саратовский источник», 2022. С. 360-363.

10. Бочаров Е. И., Подольская М. О., Седышев Э. Ю. Усилитель на активном двухполюснике, интегрированный в кольцевой эллиптический резонатор // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы IX Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 26-27 фев. 2020 г. СПб. : СПбГУТ, 2020. Т. 3. С. 408-412.

11. Седышев Э. Ю., Шомин А. Ю. Исследование возможности одновременного использования нескольких активных двухполюсников при создании СВЧ генераторов // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы IX Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 26-27 фев. 2020 г. СПб. : СПбГУТ, 2020. Т.3. С. 514-519.

12. Ларионова А. К., Седышев Э. Ю. Исследование микроволнового генератора на кольцевом резонаторе с учетом эквивалента активного двухполюсника // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы XI Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 15-16 фев. 2022 г. СПб. : СПбГУТ, 2022. Т.2. С. 645-651.

13. Шомин А. Ю., Седышев Э. Ю. Генератор СВЧ в интегральном исполнении на кольцевом резонаторе // Подготовка профессиональных кадров в магистратуре для цифровой экономики : материалы регион. научно-методич. конф. магистрантов и их руководителей, Санкт-Петербург, 01-03 дек. 2020 г. СПб. : СПбГУТ, 2021. С. 339-343.

14. Каткова Т. О., Седышев Э. Ю. Генератор СВЧ на кольцевом эллиптическом резонаторе в объемном интегральном исполнении // Электроника и микроэлектроника СВЧ. 2021. Т. 1. С. 430-433.

16. Леонтьев А. С., Седышев Э. Ю. Синтез устройства частотной селекции на кольцевых эллиптических резонаторах в объемном интегральном исполнении // Электроника и микроэлектроника СВЧ. 2022. С. 382-386.

17. Vyacheslav Lobekin, Alexandr Tatarenko, Andrei Belyshev, Mirza Bichurin Resonator for microwave magnetoelectric effect, The Yaroslav-the-Wise Novgorod State University, B.St.-Peterburgskaya str., 41, 173003, Veliky Novgorod, Russia

Leontyev A., Sedyshev E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

Frequency selection devices with redistribute power ability based on circle elliptical resonators.

The article is devoted to the study of microwave ring elliptical resonators applications in volumetric integrated circuits and study devices based on circle elliptical resonators (CER). Recent work devoted to the use of CER in microwave devices are analyzed. The purpose of the work is attempted to systematize the materials devoted to CER.

Key words: *microwave, elliptical resonator, running wave, rings, amplifiers, generators, filters, dividers, adders, microstrip line, coplanar, CER.*

УДК 629.072.116
ГРНТИ 47.45.29

ПЕЛЕНГАТОР СВЧ ДИАПАЗОНА В ОБЪЕМНОМ ИНТЕГРАЛЬНОМ ИСПОЛНЕНИИ

А. В. Могилатов, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассматривается пеленгатор кругового обзора в объемном интегральном исполнении. Предлагается оригинальная конструкция устройства на основе микрополосковой патч-антенны.

пеленгатор, круговой обзор, патч-антенна, объемная интегральная схема

В настоящее время системы пеленга находят широкое применение во многих областях человеческой деятельности, например, в:

- станциях мониторинга радиовоздействий;
- системах противодействия несанкционированному доступу беспилотных летательных аппаратов в воздушное пространство охраняемой территории;
- системах радиоэлектронной безопасности;
- радионавигации и радиолокации;
- радиобиологических системах.

Особенно широко применяются устройства пеленгации в охранных системах различных типов. Обеспечение пеленгации подвижных объектов осуществляется путем установки на подвижных устройствах тон-передатчиков, что может позволить точно определять местоположение этих объектов. Также можно с помощью пеленгов создавать системы сигнализации, а именно устанавливая тон-маяк на охраняемом объекте, который начинает посылать сигнал во время «тревоги», в дальнейшем обрабатываемый базовыми станциями.

Предлагаемая структура пеленгующего устройства представляет собой систему из патч-антенн, расположенных по кругу и соединённых с приемником коммутационным устройством.

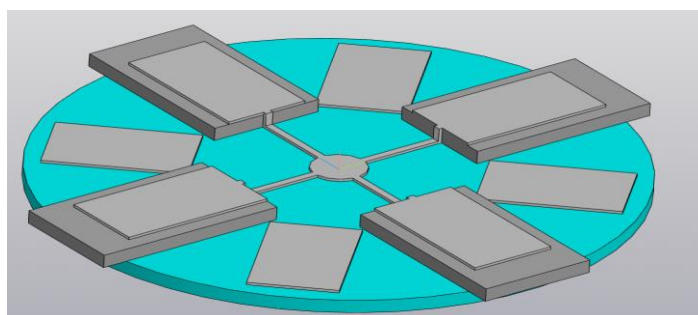


Рис. 1. 3D модель пеленга СВЧ диапазона

На рис. 1 изображена 3D модель предлагаемой структуры, разработанной с помощью лицензированной САПР Компас 3D.

Патч-антенна – разновидность микрополосковой направленной антенны микроволнового диапазона, относящаяся к типу полосковых антенн и изготавливаемая по технологии создания печатных интегральных схем СВЧ. Она представляет собой тонкую плоскую металлическую пластину, расположенную на небольшом расстоянии от плоского металлического экрана (рис. 2). Зазор между излучающим элементом и экраном заполнен слоем диэлектрика. Длина излучающих сторон прямоугольника будет близкой к половине рабочей длины волны [1]. Основными недостатками патч-антенны являются ее узкополосность и небольшой коэффициент усиления [2].

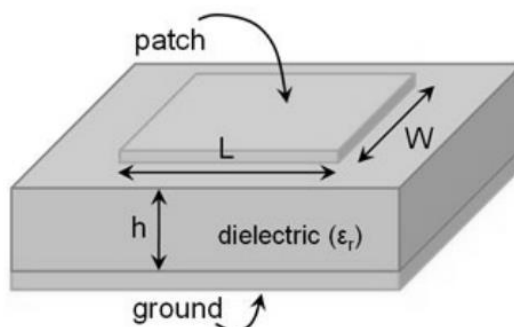


Рис. 2. Устройство патч-антенны

Диаграмма направленности типичной линейно-поляризованной патч-антенны в горизонтальной плоскости представлена на рис. 3, на котором видно, что угол возможного пеленга составляет порядка 65°. Вид диаграммы направленности в вертикальной плоскости практически идентичен. Из этого следует, что для обзора пространственного угла 360 градусов, 4-х излучателей недостаточно. Для кругового обзора пространства потребуется как минимум 6 излучателей, а с учетом небольшого коэффициента усиления, можно использовать и 8 элементов [3]. Таким образом, использование двух одинаковых систем пеленга из 4-х интегрированных излучателей, расположенных в разных плоскостях (уровнях) ОИС, позволит полностью обслуживать весь телесный угол 360 градусов в горизонтальной плоскости.

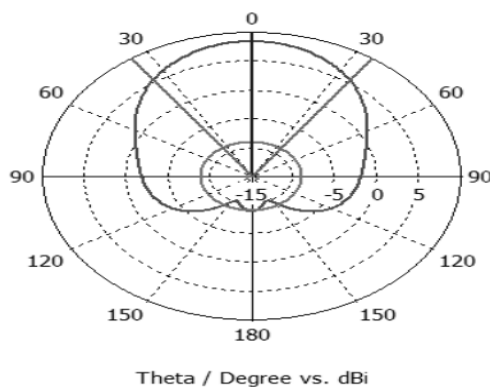


Рис. 3. Диаграмма направленности линейно-поляризованной патч-антенны

Также такое использование патч-антенн позволит исключить влияние соседних антенн, расположенных под углом 45 градусов относительно друг друга (расположение в разных уровнях объемной интегральной схемы уменьшает связь между интегрированными патч-излучателями).

Система может работать в двух режимах: активный пеленг и пассивный. Активный пеленг предполагает собой обнаружение отраженного от цели сигнала. Он реализуется путем установки в центр системы излучающей антенны. Его несомненным достоинством является возможность определения не только направления, но и дистанции до цели.

Пассивным пеленгом называют обнаружение сигналов и шумов, издаваемых иными источниками. Системы пассивного пеленга обладают рядом достоинств по сравнению с активными:

- необходимая дальность действия пассивных пеленгаторов достигается существенно меньшими энергетическими и массогабаритными затратами;
- применение же различных методов обработки обнаруживаемого сигнала позволяет определить ряд параметров обнаруженного объекта;
- большая скрытность.

В ходе работы был создан масштабный макет предложенной структуры (рис. 4).

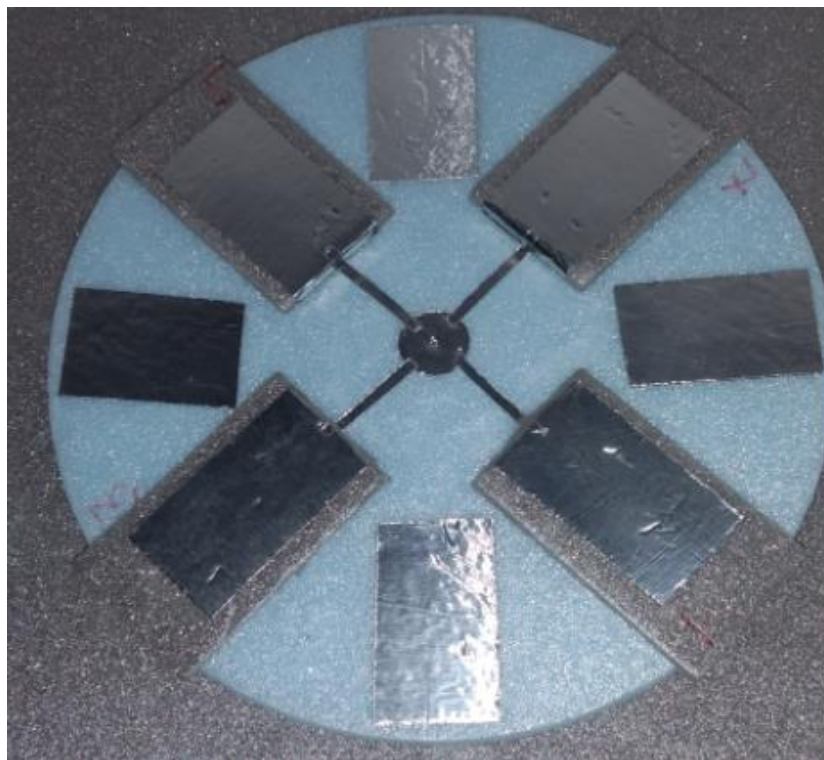


Рис. 4. Масштабный макет предложенной структуры СВЧ пеленгатора

В результате работы была предложена конструкция пеленгатора СВЧ диапазона на основе микро полосковой патч-антенны, создан масштабный макет структуры, определены основные проблемы и задачи синтеза системы в целом.

Список используемых источников:

1. Бочаров Е. И., Ветров В. В., Седышев Э. Ю., Усатова И. А. Планарные излучатели объемных интегральных схем СВЧ // Всероссийская конференция «Электроника и микроэлектроника СВЧ» 3–6 июня 2013. СПб.: Изд-во Санкт-Петербургского гос. унта телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2013, с 1.
2. Стешковой А. С., Туровский А. В. Малогабаритная патч-антенна СВЧ диапазона // Моделирование, оптимизация и информационные технологии. Научный журнал. 2017. С. 2-4.
3. Панченко Б. А., Нефёдов Е. И. Микрополосковые антенны. М. : Радио и связь. 1986. 144 с.

Mogilatov A., Sedyshev E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Direction finder of the microwave range in volumetric integral design.

The article discusses the circular view direction finder in a volumetric integral design. The original design of the device is proposed.

Key words: direction finder, all-round view, patch antenna, volumetric integrated circuit.

УДК 621.396.677.33
ГРНТИ 47.45.29

КОЛЬЦЕВАЯ АНТЕННАЯ РЕШЕТКА СВЧ ДИАПАЗОНА С ДОЛЬФ-ЧЕБЫШЕВСКИМ РАСПРЕДЕЛЕНИЕМ ИЗЛУЧАТЕЛЕЙ

С. Б. Пневский, Э. Ю. Седышев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На сегодняшний день различные устройства используют возможность обмена данными через различные сети связи, включая глобальный интернет. Совершенствуется технология связанной автоматики, все больше сетевых датчиков различного назначения используется во всех сферах жизнедеятельности. Вследствие этого возникает потребность в развитии компактных печатных антенн, возрастают требования к их диаграмме направленности и помехоустойчивости. Одной из перспективных конфигураций антенных систем является микрополосковая кольцевая антенная решетка.

патч-антенна, Wi-Fi, SRD, широкополосная связь

Введение. Микрополосковая кольцевая (патч) антенна давно известна разработчикам систем передачи данных и различных беспроводных устройств небольшого радиуса действия (short-range device, SRD). Теория функционирования одиночной кольцевой антенны достаточно хорошо освещена в литературе [1].



Рис. 1. Модифицированная двойная кольцевая антенна [3]

Однако существует ряд проблем, которые ограничивают применение подобных структур. Одна из таких проблем – способ питания конструкции. Обычно в таких устройствах возбуждается стоячая волна [2].

Попытаться изменить питание, а также улучшить диаграмму направленности (ДН) кольцевой антенны можно с помощью создания специального устройства возбуждения. Для получения в кольце бегущей волны необходимо подвести СВЧ энергию к кольцу либо по касательной, либо с нижних слоев интегральной схемы, а возможно и посредством направленного ответвителя.

На основе кольцевого резонатора бегущей волны можно создать устройство питания фазированной антенной решетки. Рассмотрим целевую антенную решетку, расположив целевые элементарные излучатели вдоль кольца на земляной плоскости.

Одним из способов создания узконаправленной кольцевой решетки является распределение Дольфа - Чебышёва [4]. Расположенные в соответствии с формулой (1) излучатели формируют диаграмму направленности с шириной главного луча в несколько градусов. Также боковые лепестки будут иметь

одинаковый уровень усиления, на несколько порядков меньший главного луча, что позволяет практически полностью избавиться от помех [4].

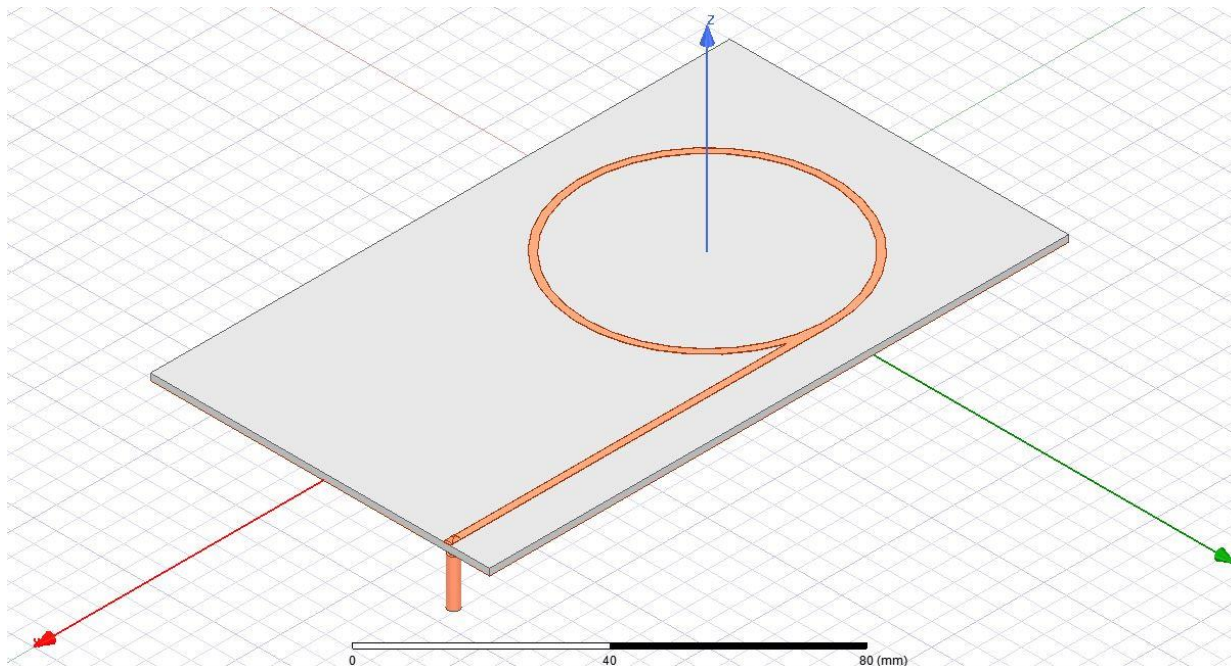


Рис. 2. 3D-модель микрополосковой кольцевой антенны

Моделирование. Моделирование полосковой кольцевой антенны и кольцевой антенной решетки с симметрично расположенными щелевыми излучателями с нижней стороны платы начнем с кольцевого резонатора.

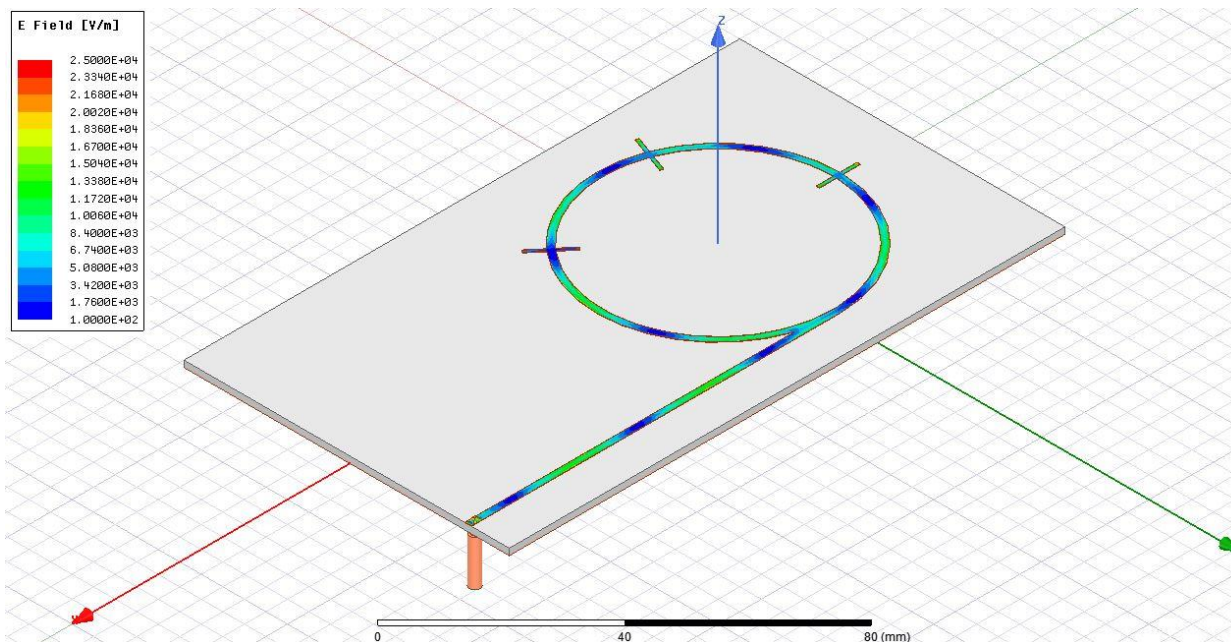


Рис. 3. 3D-модель и распределение E-поля микрополосковой кольцевой антенной решетки с симметричными полосковыми и щелевыми излучателями

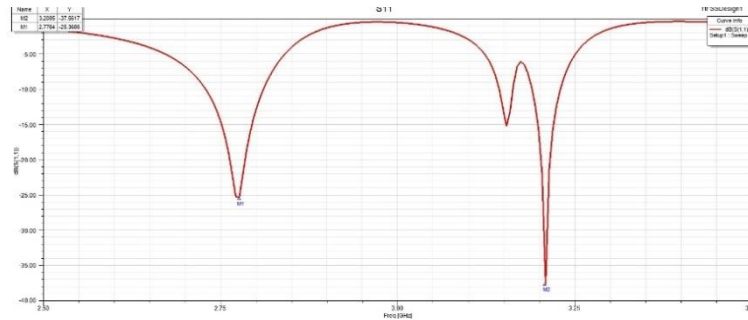


Рис. 4. Частотная зависимость $|S_{11}|$ кольцевой антенны с резонансными частотами $f_1 = 2,7764$ ГГц и $f_2 = 3,2085$ ГГц

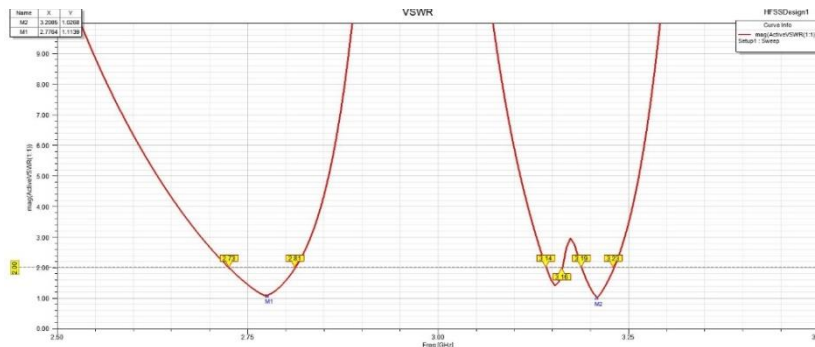


Рис. 5. Частотная зависимость КСВН (VSWR) кольцевой антенны с выделенными диапазонами $K_{СВ} < 2$

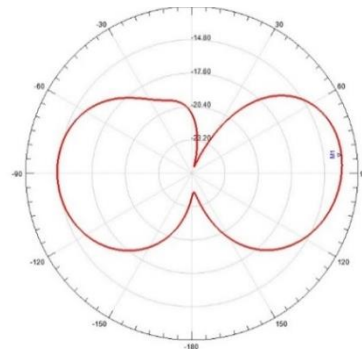


Рис. 6. Диаграмма направленности кольцевой системы вне резонанса на частоте $f = 3$ ГГц

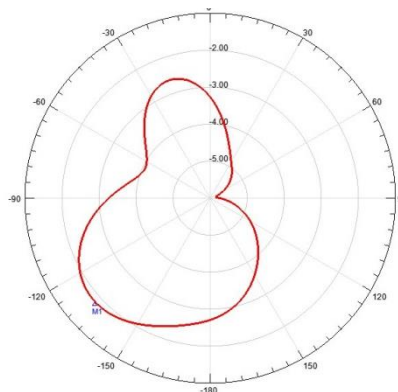
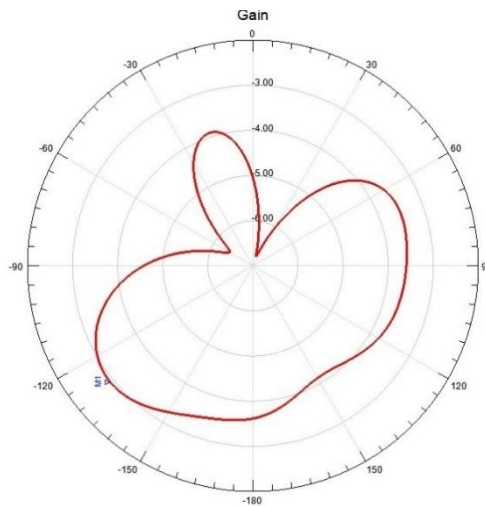


Рис. 7. Диаграмма направленности кольцевой системы на резонансной частоте $f_1 = 2,7764$ ГГц

Name	Theta	Ang	Mag
M1	-129.0000	-129.0000	-2.9199



HFSSDesign1	
Curve Info	max
dB(RealizedGainTotal)	-2.9199
Setup2 - LastAdaptive	
Freq=3.0854GHz	Phi=90deg

Рис. 8. Диаграмма направленности кольцевой системы

Эксперимент. Экспериментальная модель резонатора (рис. 9, 10) была изготовлена из алюминиевой фольги толщиной 100 мкм со следующими размерами – внутренний диаметр 50 мм, ширина полоска 1,5 мм, длина полоска питания 85 мм. Антенна размещена на подложке из органического стекла с диэлектрической проницаемостью $\epsilon = 3,5$ и тангенсом угла диэлектрических потерь $tg\delta = 0,02$.



Рис. 9. Внешний вид кольцевого резонатора на подложке из оргалита



Рис. 10. Габариты кольцевой системы питания

С помощью коаксиально-полоскового перехода типа SMA кольцевая система была подключена к векторному анализатору цепей для определения КСВН (рис. 11). По результатам измерения КСВН на частоте 2,637 ГГц приблизительно равен 4.

Полученные в ходе эксперимента и моделирования характеристики кольцевой системы подчеркивают необходимость создания устройств излучения мощности и переходу к более сложным структурам (рис. 1) излучателей или фазированным кольцевым антенным решеткам.

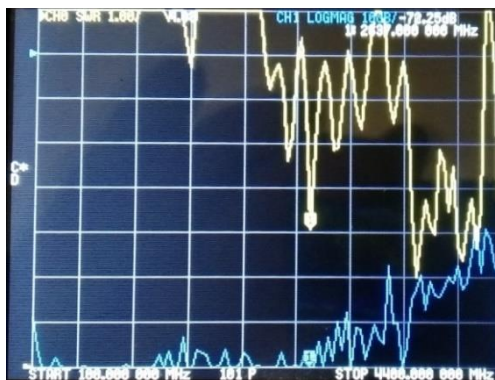


Рис. 11. Частотная зависимость $|S_{11}|$ кольцевого резонатора (желт.)

Заключение. В ходе проверки предположения об использовании кольцевого резонатора для кольцевой антенны с помощью компьютерного моделирования и экспериментального исследования были получены КСВН устройства питания и ДН данного резонатора без излучателей.

В дальнейшем предполагается расположить излучатели по Дольф-Чебышевскому распределению:

$$\Psi(\theta) = \cos \left[M \cdot \arccos[z_0] \cdot \cos \left[\frac{2\pi d}{\lambda} \cdot \sin(\theta) \cdot z_0 \right] \right], \quad (1)$$

где $d = \lambda/2$ – выбранное расстояние между излучателями.

ДН такой решетки (рис.8) имеет характерный узконаправленный главный луч. Еще предстоит создать макет кольцевой антенной решетки и провести эксперимент для проверки теории и результатов моделирования.

Список используемых источников:

1. С.А. Balanis, “Antenna Theory - Analyze and Deign”, Third Edition, A JOHN WILEY & SONS, Inc., Publication, 2005
2. Седышев Э. Ю., Соковых Р. И. Антенная решётка на кольцевом эллиптическом резонаторе // Электроника и микроэлектроника СВЧ. 2021. Т. 1. С. 439-443.
3. Wa'il A., Shaaban R. M., Duffy A. P. Design, simulation, and fabrication of a double annular ring microstrip antenna based on gaps with multiband feature //Engineering Science and Technology, an International Journal. – 2022. – Т. 29. – С. 101033.
4. Вендик О. Г. Антенные решетки Дольфа-Чебышёва // Электроника и микроэлектроника СВЧ. 2018. Т. 1. С. 209-212.

Pnevskiy S., Sedyshev E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

SHF circular ring antenna array with Dolph-Chebyshev distribution radiator.

Nowadays, many devices are able to exchange data via the global Internet, smart home technology is improving, and the number of sensors for various purposes used in technology and in all spheres of life is growing. Consequently, there is a need for the development of compact printed antennas, increasing requirements for their miniaturization and noise immunity. One promising configuration of patch structures is a microstrip ring antenna.

Key words: patch antenna, Wi-Fi, SRD, broadband communication

УДК 621.396.677.7
ГРНТИ 47.45.29

СПУТНИКОВЫЙ АНТЕННЫЙ МОДУЛЬ В ОБЪЕМНОМ ИНТЕГРАЛЬНОМ ИСПОЛНЕНИИ

Э. Ю. Седышев, А. А. Шерстобитов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На данный момент актуальна задача уменьшения габаритов параболических спутниковых антенн. В ходе работы предложен способ решения данной задачи путем использования в качестве облучателя волноводной антенной решетки, рассмотрены основные типы волн, а также создан масштабный макет облучателя, состоящий из двух открытых круглых волноводов.

СВЧ, параболическая антенна, волноводная антенна, антенная решетка

В настоящее время широкое распространение имеют спутниковые антенные модули с диаграммой направленности типа «игла». В основном это параболические зеркальные антенны, данный вид излучателей применяется в космической связи, радиолокации и радионавигации. Параболические зеркала нашли себе место и в спутниковом телевидении, а также в спутниковых системах широкополосного доступа. Примером тут может послужить недавно запущенная в эксплуатацию глобальная спутниковая система Starlink.

Так как параболическая антенна состоит из облучателя и зеркала, формирующего требуемую характеристику направленности, данный вид излучателей характеризуется большими габаритными размерами и довольно сложной конструкцией [1]. Последнее десятилетие ведутся исследования в направлении увеличения компактности таких антенн.

Уменьшение габаритов зеркального типа излучателей, создание компактной спутниковой приемопередающей панели – насущная задача микроволновой микроэлектроники. Идея использования одновременно нескольких облучателей зеркала не нова [2], но создание из этих облучателей антенной решетки на данный момент никем не исследовано. Рассмотрим облучатель, представляющий собой фазированную антенную решетку, которая состоит из двух открытых круглых волноводов.

Облучатель устанавливается напротив зеркала, как и в классической параболической антенне. В теории, при передаче (приеме) сигнала посредством зеркальной антенны данной конструкции, можно увеличить мощность передаваемого (принимаемого) сигнала пропорционально количеству используемых открытых волноводов. Так как в классической параболической антенне мощность передаваемого (принимаемого) сигнала зависит по большей части от диаметра зеркального элемента, использование данного типа облучателя позволит существенно уменьшить диаметр параболы.



Рис. 1. Параболический рефлектор с облучателем

Облучатель из нескольких открытых круглых волноводов должен будет увеличить амплитуду принимаемого сигнала в несколько раз, но сложить сигналы без потерь и в широком диапазоне частот – задача довольно сложная. Обычные сумматоры прим в данном случае применить невозможно. Рассмотрим вначале облучатель из двух элементов. Эскиз облучателя, созданный в программе КОМПАС представлен на рис. 1.

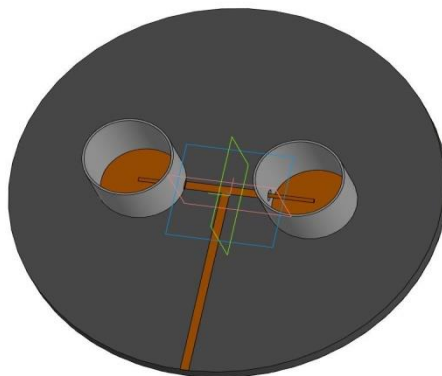


Рис. 2. 3D-модель антенного модуля в программе КОМПАС

Стоит отметить, что существует множество способов возбуждения круглого волновода. Помимо возбуждения штыревой антенной (рис. 2), можно использовать также петлевой элемент (рамку), как показано на рис. 3.

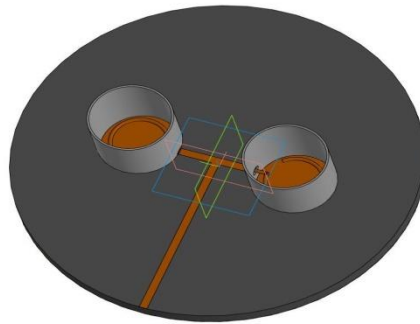


Рис. 3. 3D-модель антенного модуля с использованием рамочного способа возбуждения

Штырь должен быть ориентирован параллельно линиям E поля, рамка же — перпендикулярно линиям H поля [3, 4]. При рамочном способе возбуждения эффективно использовать волну E_{01} . При использовании штыря основным колебанием будет волна H_{11} .

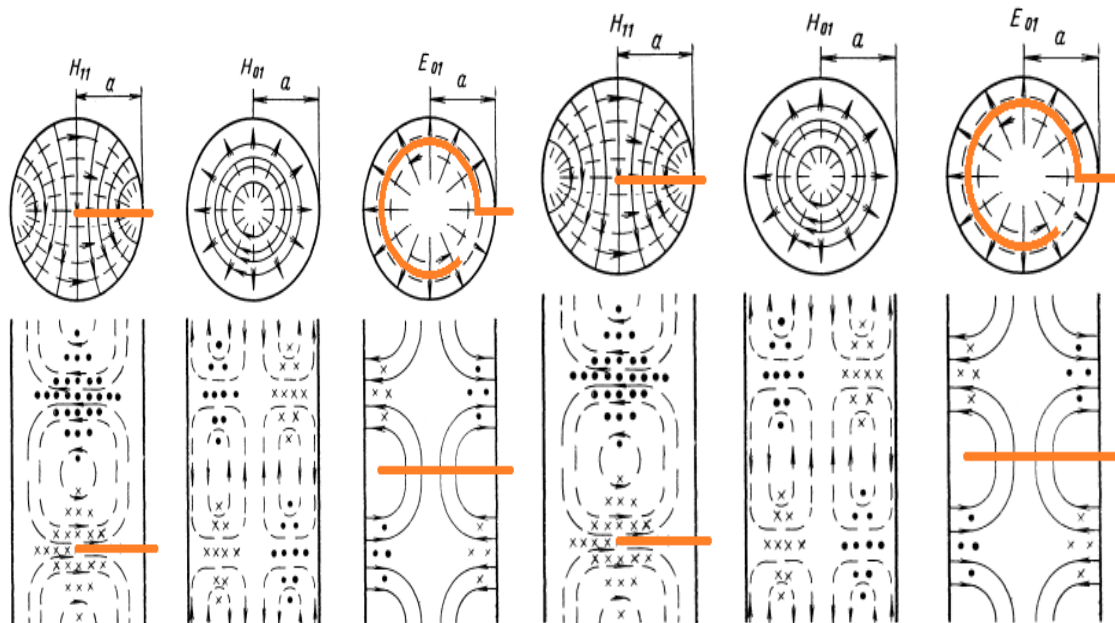


Рис. 4. Структуры волн и способы их возбуждения [1]

Для дальнейшего исследования изготовлен масштабный макет облучателя, состоящий из двух открытых круглых волноводов и подложки. Земля подложки выполнена из меди, нижняя часть волновода также выполнена из меди, а верхняя, регулируемая, — из алюминия. Верхняя часть является подвижной, таким образом можно подбирать длину волновода, а значит регулировать фазовый набег волны.



Рис. 5. Масштабный макет облучателя

В ходе дальнейшего исследования будут решаться задачи, связанные с возбуждением волноводов и суммированием мощности от них. Результатом работы должно стать устройство небольших габаритов (по сравнению с существующими параболическими излучателями), представляющее собой масштабный макет спутникового модуля, работающий в диапазоне частот, удобном для макетирования.

Список используемых источников:

1. Фальковский О. И. Техническая электродинамика : учебник. СПб. : Изд-во «Лань», 2009. 432 с.
2. Саонов Д. М. Антенны и устройства СВЧ : учебник. М. : Высшая школа, 1988. 432 с.
3. Глухов Н. И., Лепихин К. А., Седышев Э. Ю. Спиральная структура в качестве питающего элемента круглого волновода // Электроника и микроэлектроника СВЧ. 2021. Т. 1. С. 423-425.
4. Глухов Н. И., Лепихин К. А., Седышев Э. Ю. Широкополосное возбуждение круглого волновода спиральной структурой // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы X Междунар. научно-технич. и научно-методич. конф., СанктПетербург, 24–25 фев. 2021 г. СПб. : СПбГУТ, 2021. С. 476-482.

Sedishev E., Sherstobitov A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Satellite antenna module in volume integrated version.

At this moment the task of downsizing a parabolic antenna is relevant. In the course of the work, a method for solving this problem was proposed by using a waveguide antenna array as a feed antenna, the main types of waves were considered, and a scale model of the feed antenna, consisting of two open round waveguides, was created.

Key words: *microwave, parabolic antenna, waveguide antenna, antenna array.*

Секция 1.2.
Промышленная электроника

УДК 621.375.026

ГРНТИ 47.41.33

ПРИМЕНЕНИЕ УПРАВЛЯЕМОГО РЕЗОНАНСНОГО ИНВЕРТОРА ТОКА В ДЛИННОВОЛНОВОМ РАДИОНАВИГАЦИОННОМ ПЕРЕДАТЧИКЕ

К. Д. Богатырев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются вопросы генерирования радиоимпульса с заданной формой огибающей в антенне длинноволнового передатчика на основе новой схемы транзисторного управляемого резонансного инвертора тока. Предложена математическая модель исследуемого инвертора.

длинноволновый радионавигационный передатчик, управляемый резонансный инвертор тока, огибающая радиоимпульса

Разработка радионавигационных устройств является неотъемлемой частью развития радиотехники. Однако до недавнего времени длинноволновые (далее – ДВ) наземные радионавигационные передатчики основывались на использовании мощных генераторных ламп, которые обладают высокой мощностью, но имеют большие габариты. Примером таких радионавигационных передатчиков может послужить «Чайка», которая была разработана в 1969 году и является российским аналогом американской системы Loran-C.

Инженер Tim Hardy – руководитель инженерного отдела Nautel Limited, – в 2008 году предложил решение: создание радиоимпульса на схеме мостового ключевого генератора класса D [1], представленной на рис. 1. В отечественной литературе радиотехники такую схему называют классической схемой ключевых генераторов на основе резонансного инвертора напряжения (далее – РИН). В 2008 году в Канаде был построен первый прототип передатчика, использующий новую технологию. Это позволило повысить КПД передачи и уменьшить его габариты. Такой передатчик способен генерировать радиоимпульсы мощностью от 50 кВт до 100 кВт. Первоначальные результаты с использованием схемы генератора класса D оказались благоприятными для компании, исследования показали высокий уровень регулирования амплитуды импульсов и точность синхронизации.

Недостатком схемы генератора класса D является отсутствие амплитудной модуляции. В ней используется ступенчатая модуляция, и для достижения требуемых высоких уровней мощности необходимо объединить некоторое количество усилителей.

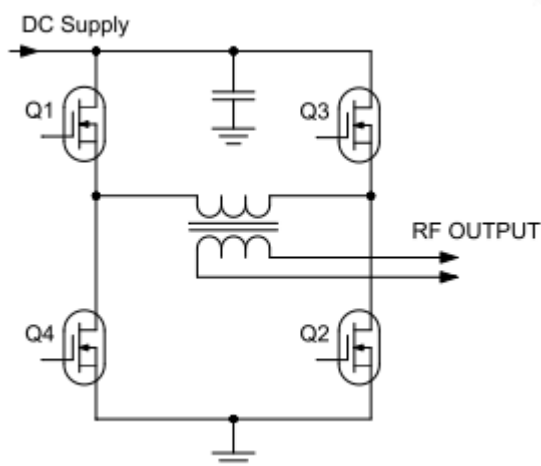


Рис. 1. Схема генератора класса D [1]

В данной статье предложено формирование радиоимпульса ДВ радионавигационного передатчика на схеме управляемого резонансного инвертора тока (РИТ), произведено сравнение схем РИН и РИТ, выделены достоинства, а также рассмотрено компьютерное моделирование схемы управляемого РИТ.

Управляемый РИТ [2], представленный на рис. 2, содержит источник питания, параллельно выходу которого включен фильтровый конденсатор, соединенный с мостовым коммутатором, состоящим из четырех транзисторов, шунтированных обратными диодами, к выходу которого подключен колебательный контур, соединенный с первичной обмоткой трансформатора, во вторичную обмотку которого включена нагрузка, и дроссель, включенный последовательно с мостовым коммутатором и связанный с отрицательным полюсом источника питания. Антенной в данной схеме будет выступать эквивалентный RLC -контур с сосредоточенной постоянной последовательностью. Но этот контур должен обладать правильно подобранной добротностью, так как высокая добротность антенн затрудняет передачу радиоимпульса.

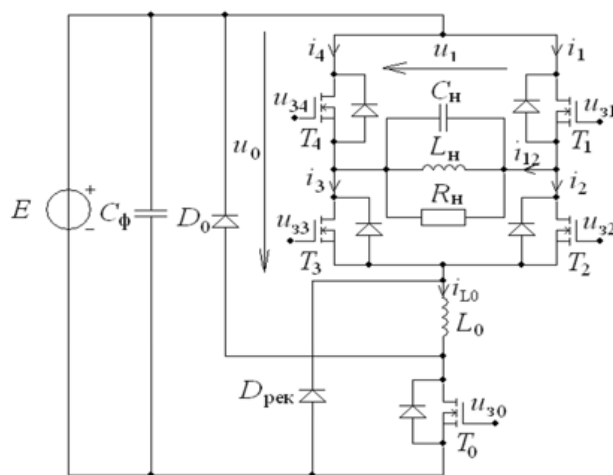


Рис. 2. Схема мостового управляемого резонансного инвертора тока

Управление схемой РИТ осуществляется за счет ШИМ, поэтому такой инвертор тока подходит для применения в радионавигационных датчиках. Введение в схему классического РИТ, управляемого с помощью ШИМ, даёт новое схемотехническое решение для ВЧ управляемого ключевого генератора, способного формировать модулированные колебания с изменяющей огибающей с высоким КПД.

При сравнении РИТ и РИН, к достоинствам РИТ можно отнести то, что скачок напряжения в десятки или в сотни раз меньше напряжения питания и в результате потери на фронтах во много раз снижаются, улучшаются частотные свойства инвертора и повышается КПД. Наличие дросселя обладает фильтрующим действием для тока, что позволяет уменьшить высокочастотную фильтрующую емкость источника питания. Паразитная выходная емкость «сток-исток» на транзисторе учитывается в конденсаторе, который находится в параллельном RLC -контуре.

Модуляционная характеристика схемы ключевого генератора аналитически определена следующим образом:

$$\frac{U_M}{E_0} = 0,5\pi \frac{t_{и}}{T_M}, \quad (1)$$

где U_M – амплитуда ВЧ колебаний в нагрузке;

$t_{и}$ – длительность прямоугольного импульса, отпирающего транзистор ключевого усилителя с ШИМ; E_0 – напряжение источника.

T_M – период повторения этих импульсов.

При изменении $t_{и}$ от 0 до $\frac{2T_M}{\pi}$ амплитуда напряжения на контуре U_M изменяется по линейному закону от 0 до максимального значения равного напряжению питания. На рис. 3 показаны рассчитанная идеальная характеристика и полученная моделированием схемы в программе FASTMEAN 6.0 при изменении коэффициента заполнения импульсов модулятора ШИМ до значения $\frac{2}{\pi} \approx 0,64$.

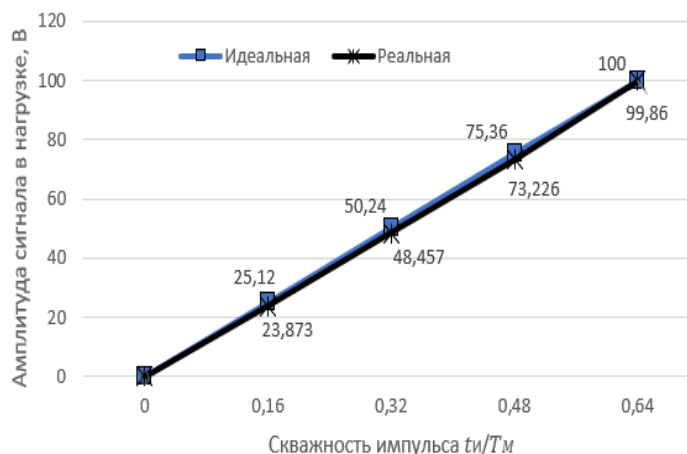


Рис. 3 статическая модуляционная характеристика: а) идеальная (синим цветом); б) реальная (черным цветом)

Компьютерная модель схемы управляемого РИТ в FASTMEAN версии 6.0 примет вид, представленный на рис. 4.

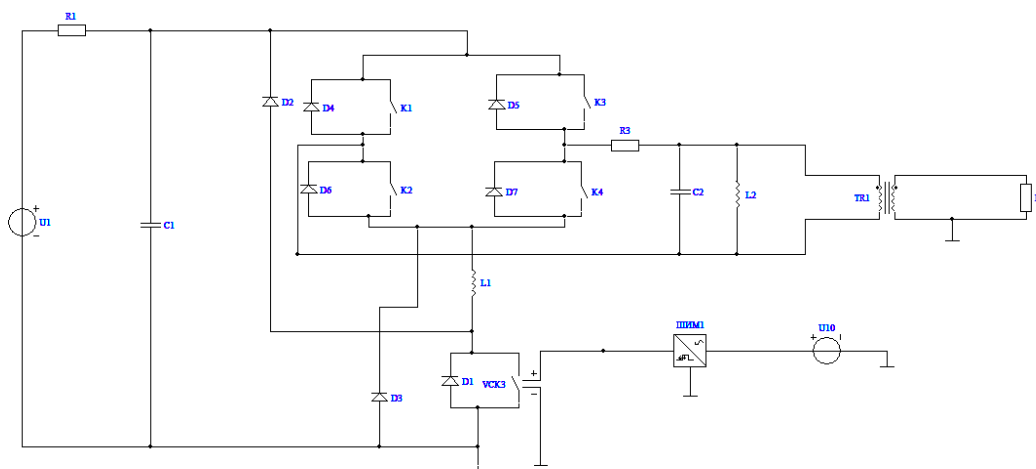


Рис. 4. Компьютерное модель схемы в FASTMEAN 6.0

На вход управляемого РИТ подадим треугольные импульсы, на ШИМ формируется прямоугольные импульсы с разным коэффициентом заполнения. Затем прямоугольные импульсы подаются на транзистор, который представлен в виде ключа VCK3, после чего, фильтруются дросселем, и попадают на РИТ.

По результатам компьютерного моделирования получим переходную характеристику, изображенную на рис. 5, для сигнала на резисторе R2, который представляет собой нагрузку.

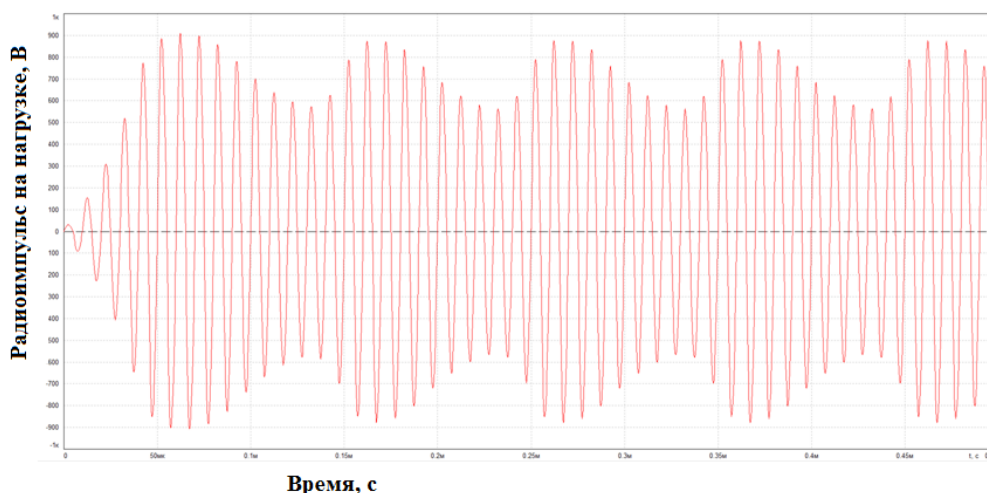


Рис. 5. Результат компьютерного моделирование управляемого РИТ

На рис. 5 изображены радиопульсы, сформированные с помощью управляемого РИТ. Это говорит о том, что данная схема работает правильно и может быть разработан новый ДВ радионавигационный передатчик на базе схемы управляемого РИТ.

В заключении, хотелось бы сказать, что схемотехническое решение управляемого с помощью ШИМ РИТ является новинкой, и имеет существенные достоинства перед схемой на РИН.

Список используемых источников:

1. Next Generation LF Transmitter Technology for (e)LORAN System [Электронный ресурс]. URL: https://www.loran.org/proceedings/Meeting2008/Papers/Hardy_10A3.pdf (дата обращения 01.11.2022).
2. Ганбаев. А. А. Формирование модулированных радиочастотных колебаний с улучшенными спектральными и энергетическими характеристиками в ключевых генераторах на GaN транзисторах : автореф. дис.. д-ра техн. наук : 16.10.20 / Ганбаев А. А. СПб., 2020. 16с.
3. Филин В. А. Управляемый резонансный инвертор тока. Пат. 17207U1 Российская Федерация; заявитель и патентообладатель. Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ)–№172407; заявл. 23.12.16; опубл. 07.07.2017

Bogatyrev K.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Application of a controlled resonant current inverter in a long-wave radio navigation transmitter.

The issues of generating radio pulses with a given envelope shape in the antenna of a DV transmitter based on a new scheme of a transistor controlled resonant current inverter are considered. A mathematical model of the studied inverter is proposed

Key words: long-wave radio navigation transmitter, controlled resonant current inverter, radio pulse envelope.

УДК.621.396.6

ГРНТИ 47.47

ВАРИАНТЫ ПОСТРОЕНИЯ ДЕЛИТЕЛЯ С ДРОБНЫМ КОЭФФИЦИЕНТОМ ДЕЛЕНИЯ

П. В. Воропаев, Ю. А. Никитин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире все чаще и чаще, практически в каждой области, используются устройства, которые подразумевают в своей конструкции синтезатор частот. Точность некоторых приборов позволяет задавать не только целочисленные, но и дробно-переменные деления. Статья предлагает оценку и сравнение разных схемотехнических реализаций делителей с целочисленными и дробными коэффициентами деления.

синтезаторы частот, ДПКД, ДДПКД, делители частот

Синтезаторы частот (СЧ) стали неотъемлемой частью многих отраслей техники, включая микро-наноэлектронную, полупроводниковую, метрологическую и многие другие промышленности. Тенденция и темп развития техники приводит к тому, что необходимо обрабатывать большие объемы информации в том или ином виде, для этого необходимы СЧ.

Одна из важных задач при создании любого синтезатора частот — это обеспечить его быстродействие, стабильность и чистоту спектра. Это приводит к необходимости использовать дорогие компоненты, чего и пытаются избежать, стремясь упростить, например, используя фазовую автоподстройку.

Простейшие структуры являются однопетлевыми, где делитель частоты имеет целочисленный коэффициент деления. Подобная структура приведена на рис. 1. [1] Синтезатор частот включает в себя генератор, управляемый напряжением (ГУН), который настроен на необходимый диапазон. В схему включена отрицательная обратная связь (ООС) через делитель с переменным коэффициентом деления N , фазовый детектор (ФД) и фильтр нижних частот (ФНЧ). На импульсно-фазовый детектор (ИФД) приходит сигнал F_{pd} , частота которого равна заданному шагу сетки. В ИФД формируется сигнал ошибки, который через фильтр нижних частот поступает в ГУН.

Предположим, что необходимо получить сетку с шагом в 2 кГц, при диапазоне 200 ÷ 250 МГц, опорная частота $F_{опор}=2$ МГц. Получается, что $R=1000$, для того, чтобы частота на ИФД была равна 2 кГц. Тогда коэффициент B будет находиться в диапазоне 20000-30000. [2]

Область применения такого делителя очень ограничена, из-за своей простоты он имеет несколько серьезных недостатков, одним из которых являются – помехи с частотой, кратной частоте сравнения в ИФД. Помехи с выхода фазового детектора, поступают в ГУН, вследствие чего в спектре появляются дискретные боковые полосы. Чтобы этого избежать, необходимо корректировать ФНЧ, а именно, его полосу пропускания, что в свою очередь замедляет работу СЧ.

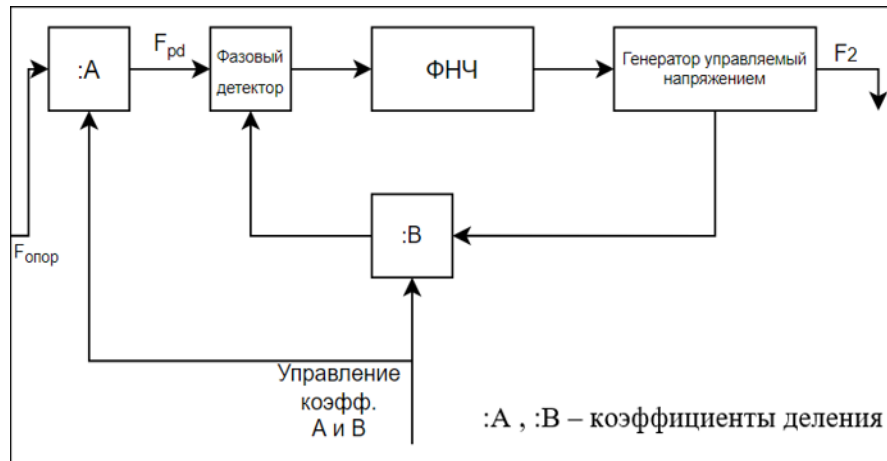


Рис. 1. Простейшая однопетлевая структура

Эту структуру можно улучшить, путем введения в нее смесителя (СМ), рис. 2, при все тех же данных (шаг сетки, выходной диапазон), удастся снизить коэффициент B , из-за которого уменьшится коэффициент усиления помех, подводимых к ИФД. [1] Сигнал $F2-CF_{опор}$ поступает на ПФ и уходит на вход делителя с переменным коэффициентом деления (ДПКД) с коэффициентом деления B . Так же, уменьшая B , мы уменьшаем входную частоту, на которой работает ДПКД, что дает возможность, сделать его дешевле и энергоэффективнее. Недостаток этой схемы в возможности появления в схеме помех, источником которой будут комбинационные помехи на выходе СМ. Из-за этого схема становится очень чувствительной и сложной схемотехнически

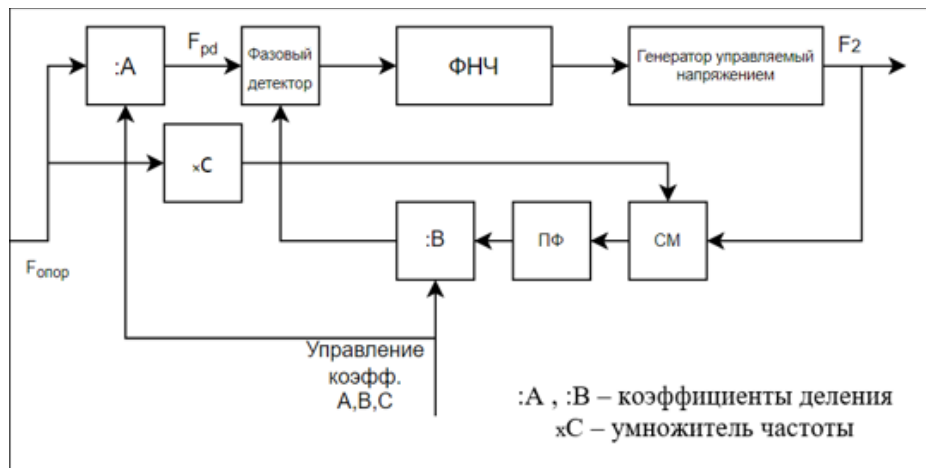


Рис. 2. ДПКД со смесителем на входе

Приведенные выше схемы являются самыми простыми однопетлевыми с целочисленным коэффициентом деления, но с увеличением требуемой точности и расширением полосы частот появилась необходимость создания делителя с дробно-переменным коэффициентом деления (ДДПКД). В большинстве схем используется накапливающий сумматор в качестве аккумулятора, ёмкость которого влияет на шаг сетки моделируемой частоты.

Перейдем к рассмотрению таких схем.

имеющего противоположную фазу, и зачем сложить его с напряжением на ФД. Для этого и служит интегратор.

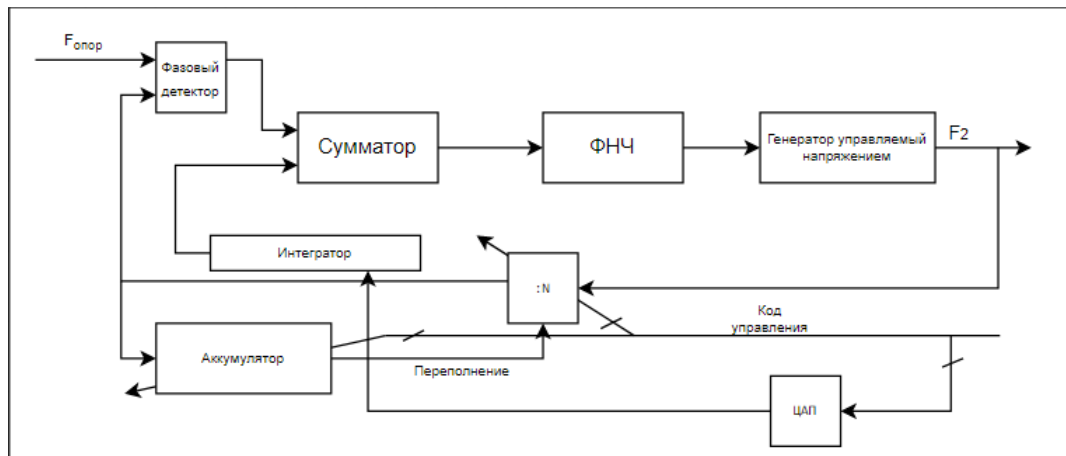


Рис. 5. ДФКД на аккумуляторе с интегратором

Цифро-аналоговый преобразователь используется, как средство управления коэффициентом передачи интегратора. Это получается из-за довольно широкого диапазона значений изменения коэффициента деления. ЦАП, как отдельный блок, может быть использован как питание интегратора и для контроля напряжения посредством внешнего кода управления. На схеме, показанной на рис. 4. возможности контроля напрямую нет, но с помощью еще одного, дополнительного ЦАП можно создать шину, которая будет управляться исходным кодом.

Таким образом, при рассмотрении самых простых однопетлевых схем с целочисленным и дробно-переменным коэффициентом, можно понять принцип работы таких синтезаторов частот, что дает возможность создавать более сложные конструктивно, но в свою очередь более надежные и, при правильном подборе компонентов, коэффициентов деления, количества ветвей обратной связи, недорогие устройства.

Список используемых источников:

1. Козлов В. И. Частотный синтез на основе ФАПЧ. Обзор методов синтеза. Монография. 2022. 210 с.
2. Шахтарин Б. И., Качармина Е. Г., Вельтищев В. В. Анализ синтезатора частот с дробно-переменным коэффициентом деления делителя // Научный вестник МГТУ ГА. 2018. №2.

Voropaev P., Nikitin Yu.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Options for constructing a divisor with a fractional division coefficient.

In the modern world, devices implying a frequency synthesizer in their design are being used more and more often in almost all areas. The accuracy of some devices allows you to set not only integer, but also fractional-variable divisions. The article offers an assessment and comparison of various schematic representations of divisors with integer and fractional division coefficients.

Key words: *frequency synthesizers, fractional division factor, frequency divider.*

УДК 621.311.62
ГРНТИ 47.14.17

ИССЛЕДОВАНИЕ СХЕМЫ ИСТОЧНИКА ПИТАНИЯ ДЛЯ ЭЛЕКТРОННОГО ОБОРУДОВАНИЯ

И. И. Гавриков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Практически в каждом электронном устройстве используются источники питания или стабилизаторы напряжения и тока. Поэтому в работе была рассмотрена и модернизирована типовая схема источника питания, представлены результаты ее компьютерного моделирования и тестирования экспериментального макета. Полученные характеристики созданного макета соответствуют базовым требованиям, предъявляемых к источникам питания электронного оборудования, в т. ч. для измерительной, медицинской и лабораторной техники.

источники питания, стабилизация энергетических параметров, медицинская техника, промышленная электроника

Работа электронной техники и измерительной аппаратуры во многом зависит от надёжности и стабильности питания, также от качественной работы преобразователей энергии при питании от сети переменного напряжения [1 – 3]. В работе рассмотрены базовые схемные решения, представлены результаты компьютерного моделирования проектируемой схемы.

Целью работы является разработка и проектирование лабораторного источника питания выходной мощностью 200 Вт, соответствующего требованиям, предъявляемым к лабораторному и медицинскому оборудованию.

Основными требованиями для универсальных источников питания, применяемых как в высококачественной бытовой технике, так и в лабораторном оборудовании, являются: возможность регулировки напряжения в диапазоне от 0 до 28 В; силы тока – от 0 до 7 А; обеспечение стабилизации по этим параметрам; низкий коэффициент пульсаций (не превышающий 8 %); высокий уровень помехозащищённости.

Для этого был проведён анализ схемотехнических решений импульсных и линейных (трансформаторных) источников питания. Был выбран второй вариант, поскольку трансформаторные источники питания являются более простыми в разработке и характеризуются меньшим уровнем выходных пульсаций напряжения и шумов по сравнению с импульсными стабилизаторами.

Так как линейные стабилизаторы [2] характеризуются высоким уровнем нагрева силовых компонентов [4], в данной работе был проработан вариант решения такого недостатка проектируемой схемы источника. Для этого был применён вентилятор и радиатор в качестве активного и пассивного охлаждения, и коммутатор обмоток для трансформатора, необходимый для повышения КПД.

За основу была взята схема стабилизатора и коммутатора (рис. 1) [5], в которую были внесены изменения для обеспечения требуемых для проекта характеристик.

Подбор компонентной базы был произведен исходя из доступности, дешевизны и небольшого размера печатной платы, благодаря использованию технологий поверхностного монтажа. Для создания лабораторного прототипа был выбран трансформатор ТПП-319, преимуществами которого является низкая стоимость, обеспечение требуемой мощности и работы переключателя обмоток [7].

В выбранной за основу схеме для изменения выходного напряжения используется мощный силовой биполярный транзистор, который рассеивает лишнее напряжение в тепловую энергию. Изменение и стабилизация тока и напряжения реализовано благодаря управляющей части, позволяющей изменять сигнал на базе транзистора в соответствии с выбранным уровнем стабилизированных параметров. Схема управления выполнена на двух операционных усилителях, последовательно включенных в режиме интегратора. Изменение тока происходит путем сравнения опорного напряжения с напряжением датчика тока (и, следовательно, на выходе интегратора), а регулировка напряжения – в результате сравнения части выходного напряжения и сигнала с первого интегратора [4].

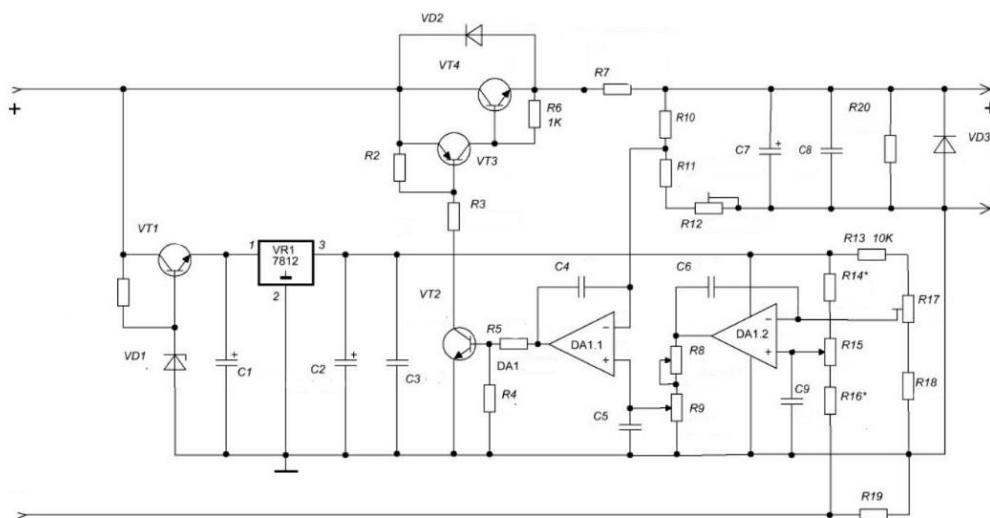


Рис. 1. Схема стабилизатора напряжения и тока [5]

Силовой трансформатор, выбранный для реализации схемы, обладает несколькими вторичными обмотками, что позволяет внедрить в схему так называемый, "коммутатор обмоток" [7]. Принцип его работы заключается в следующем: при превышении выходного напряжения стабилизатора напряжения и тока [5] до некоторого значения (например, 15 В), происходит пробой стабилитрона, и на базе транзистора (, работающего в ключевом режиме [2]), относительно земли появляется положительный потенциал. Благодаря этому, один из выводов катушки коммутирующего реле подтягивается к минусовому проводу. Это приводит к последовательному подключению второй обмотки к

первой, вследствие чего увеличивается напряжение на входе силового транзистора (на входе стабилизатора). Благодаря этому, уменьшается разность потенциалов на его выводах. Данное схемотехническое решение позволяет повысить КПД устройства и уменьшить степень нагрева проектируемой схемы.

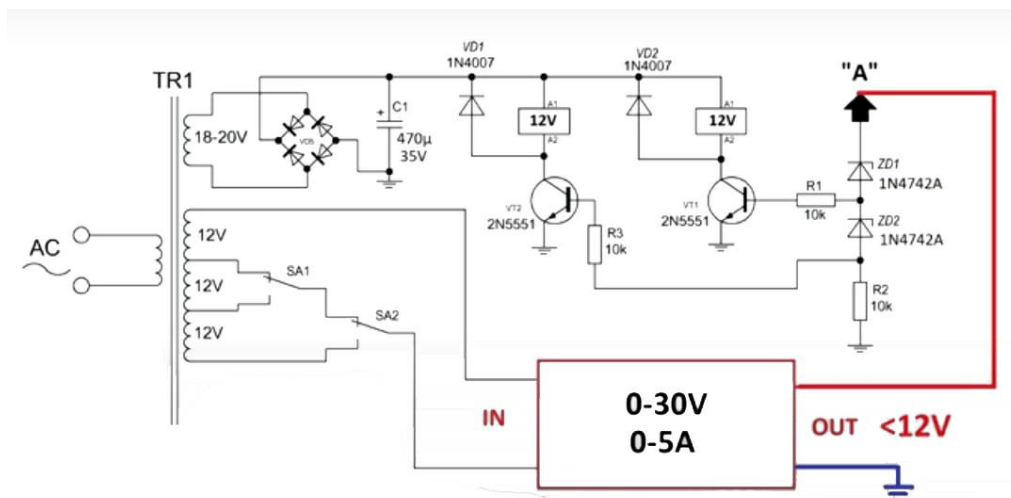


Рис. 2. Схема переключателя обмоток [7]

В модернизированной схеме применён регулятор скорости оборотов вентилятора, который автоматически изменяет степень активного охлаждения, пропорционально уровню нагрева силовых компонентов. Механизм такой регулировки режима работы вентилятора основан на изменении напряжения на терморезисторе, влияющим на частоту импульсов, подаваемых непосредственно на вентилятор.

Для уменьшения уровня шумовых помех была проработана схема соединения заземляющего проводника с корпусом сборочного макета и на общий провод схемы через пленочный конденсатор. Ёмкость в данном случае применена для гальванической развязки [4], что позволяет нейтрализовать поражение электрическим током пользователя.

Прототип схемы был промоделирован в компьютерной программе LTspice, предназначенной для моделирования аналоговых электронных схем на базе SPICE, выпускаемая производителем полупроводников Analog Devices. Это бесплатное, наиболее широко распространенное программное обеспечение SPICE, используемое при проектировании схем электронной техники [6]. По результатам проведенного компьютерного моделирования модернизированной схемы были получены следующие параметры:

Коэффициент пульсаций при ток $I = 7 \text{ A}$ равен 4%;

Максимальная мощность на выходе составила примерно $P \approx 196 \text{ Вт}$;

Напряжение уменьшилось на 50 мВ при увеличении тока от 0 до 2 А.

По итогам проведенных измерений на сборочном макете, получили следующие параметры:

Коэффициент пульсаций при ток $I = 7 \text{ A}$ составил 7%;

5. Схема стабилизатора и регулятора напряжения и тока [Электронный ресурс] URL: <https://forum.cxem.net/index.php?topic/76820-%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B9-%D0%B8-%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BD%D1%8B%D0%B9-%D0%B1%D0%BF-050%D0%B2/>. (Дата обращения: 30.03.2022)

6. Сайт программного обеспечения для компьютерного моделирования электрических схем LTspice. URL: <https://www.analog.com/en/design-center/design-tools-and-calculators/ltspice-simulator.html>. (Дата обращения: 30.03.2022)

7. Схема переключателя обмоток [Электронный ресурс] URL: <https://vip-schema.org/index.php/home/bloki-pitaniya/407-kommutator-obmotok-dlya-laboratornogo-bloka-pitaniya>. (Дата обращения: 30.03.2022)

Gavrikov I.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Investigation of the power supply circuit for electronic equipment.

Power sources or voltage and current stabilizers are used almost in every electronic device. Therefore, a typical power supply circuit was considered and modernized in the paper; the results of its computer modeling and testing of an experimental model are presented. The obtained characteristics of the created electric circuit correspond to the basic requirements for power sources of electronic equipment, including for measuring, medical and laboratory equipment.

Key words: *power supplies, stabilization of energy parameters, medical equipment, industrial electronics.*

УДК 621.391, 621.382.2/.3

ГРНТИ 47.01.05

ВАРИАНТ НОНИУСНОГО ЦИФРОАНАЛОГОВОГО ПРЕОБРАЗОВАНИЯ

А. Э. Гиниятуллин, Ю. А. Никитин, В. А. Юрова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Создание высокоточных и быстродействующих цифро-аналоговых преобразователей (ЦАП) достаточно сложный и трудоемкий процесс, который требует больших затрат по ресурсам, чтобы соответствовать всем требованиям к технологии. Однако ЦАП, построенные по нониусной технологии, обладают достаточно высоким быстродействием и позволяют увеличивать разрядность без потерь этого быстродействия.

цифроаналоговый преобразователь, арифметический сумматор, аналоговый сумматор, нониус, управляющий код, промышленная электроника

Современные цифровые технологии, облают большими возможностями по обработке, хранению и передачи больших объемов информации. Они активно внедряются в самые разные сферы человеческой деятельности, даже там где раньше в основном использовались аналоговые методы. Сейчас, пожалуй, уже сложно найти сферу деятельности, где не используются цифровые технологии [1 – 2].

Чтобы произвести обработку какой-либо аналоговой величины, необходимо эту величину сначала преобразовать в цифровой код, произвести необходимые математические операции и преобразовать полученный в цифровом виде результат обратно в аналоговую величину. И точность такой цепочки преобразований не должна быть хуже точности аналоговой обработки исходного сигнала. Также, нередко, необходимо результаты цифровых процессов предоставить в виде аналоговой величины с высокой степенью точности [3 – 5]. Если необходимой точности при таких преобразованиях достичь не удастся, то вся мощь современной вычислительной техники окажется бесполезной.

Выпускаемые серийно АЦП и ЦАП в большинстве своем имеет ряд недостатков, накладывающих ограничения на создание быстродействующих многоразрядных систем [5 – 8]. Одним из главных недостатков является то, что для увеличения числа разрядов, приходится жертвовать скоростью преобразования. И наоборот, чтобы получить более высокую скорость преобразования, нужно уменьшать число разрядов. В ином случае будет страдать точность преобразования, что критично для многоразрядных систем.

Одним из косвенных методов, на основе которого могут создаваться скоростные и одновременно высокоточные приборы, является нониусный метод. Этот метод имеет определенные перспективы. Его привлекательность обусловлена сочетанием высокого быстродействия и точности.

Решением приведенной выше проблемы служит цифро-аналоговый преобразователь (ЦАП), построенный по нониусной технологии [9 – 10]. Суть нониусного метода (рис. 1) состоит в том, что используются два ЦАП меньшей разрядности, но в конечном итоге они в сумме позволяют достичь более точного результата на выходе и за меньшее время в отличие от использования одного ЦАП большой разрядности, так как каждый ЦАП по отдельности обрабатывает отведенные ему биты независимо друг от друга [8, 11]. На вход такого ЦАП подается входной код X , который делится на две примерно равные группы, а именно так называемые старшие M длиной α и младшие разряды N длиной β , которые будут обрабатываться двумя независимыми друг от друга цифро-аналоговыми преобразователями. После преобразования старших разрядов M в ЦАП 1, мы получим аналоговый сигнал Z_1 , который будет пропорционален управляющему слову $Q = M \pm N$, которое получаем, прогнав старшие и младшие разряды M и N через арифметический сумматор 1, где над этими кодами производится операция сложения или вычитания. Параллельно этому происходит преобразование N младших разрядов управляющего слова в аналоговый сигнал Z_2 в ЦАП 2, однако непосредственно перед преобразованием управляющее слово длиной α подвергается цифровому умножению в a раз. На входы ЦАП 1 и ЦАП 2 должны подаваться соответственно опорные аналоговые сигналы Y_1 и Y_2 , причем $Y_2 = Y_1(1 \mp a^{-\alpha})$ (отличие на единицу младшего разряда), где a – основание системы счисления, которую мы используем для управляющего слов X . Далее уже аналоговые сигналы Z_1 и Z_2 поступают на входы аналогового сумматора 2, где подвергаются операции вычитания или сложения в зависимости от той операции, которую мы использовали в арифметическом сумматоре 1, если там было вычитание, значит используем сложение и наоборот, если было сложение, то выполняет операцию вычитание. На выходе аналогового сумматора 2 мы получим аналоговый сигнал Z_0 .

В параллельных цифроаналоговых преобразователях (ЦАП) из опорного сигнала Y формируют эталонные сигналы, соответствующие значениям (весам) разрядов входного управляющего кода X , которые затем суммируют и образуют дискретные значения выходной аналоговой величины Z .

$$Z = Y \cdot \frac{X}{a^\psi} \quad (1)$$

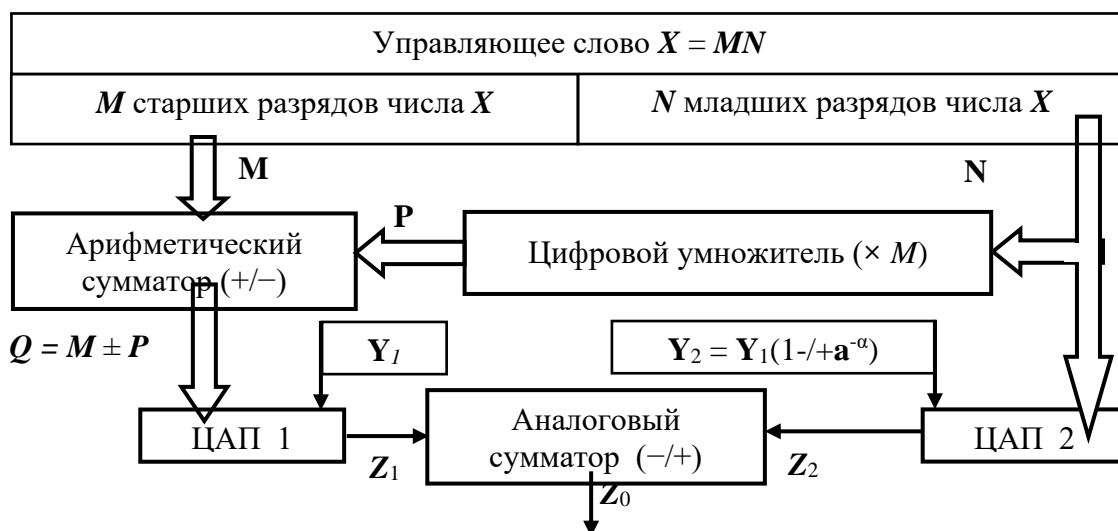


Рис. 1. Принципиальная схема работы нониусного ЦАП

Принцип нониусного преобразования отражается следующей формулой:

$$Z_0 = Z_1 - Z_2 = \frac{Y_1 \cdot (M \pm N) \mp Y_2 \cdot N}{a^{(\alpha + \beta)}} \quad (2)$$

где Z_0 – аналоговый сигнал преобразования входного кода X

$$X = M + N \cdot a^{-\alpha} \quad (3)$$

M – код старшей группы разрядов α ,

N – код младшей группы разрядов β ,

Z_1 – аналоговый сигнал суммы кодов M и N ,

Z_2 – аналоговый сигнал кода N ,

Y_1 – опорное напряжение для ЦАП суммы кодов групп $(M + N)$,

Y_2 – опорное напряжение для ЦАП кода N группы младших разрядов β ,

a – основание системы счисления.

Опорные напряжения обоих ЦАП связаны формулой:

$$Y_2 = Y_1 \cdot (1 \pm a^{-\alpha}) \quad (4)$$

Если подставить выражение (4) в (2) с учетом (3), получим

$$\begin{aligned} Z_0 = Z_1 - Z_2 &= \frac{Y_1 \cdot (M \pm N) \mp Y_2 \cdot N}{a^{(\alpha + \beta)}} = \frac{Y_1 \cdot (M \pm N) \mp Y_1 \cdot (1 \pm a^{-\alpha}) \cdot N}{a^{(\alpha + \beta)}} = \\ &= \frac{Y_1 \cdot (M \pm N \mp N + a^{-\alpha} \cdot N)}{a^{(\alpha + \beta)}} = \frac{Y_1 \cdot (M + a^{-\alpha} \cdot N)}{a^{(\alpha + \beta)}} = \frac{Y_1 \cdot X}{a^\psi}; \end{aligned} \quad (5)$$

Формула (5) совпадает с формулой (1), т. е. соответствует простому цифро-аналоговому преобразованию.

Вывод: Предложенный выше ЦАП за счет параллельного преобразования старших и младших разрядов почти не теряет быстродействия, но имеет разрядность $2n - 2$, чем исходные n -разрядные ЦАП с тем же быстродействием.

Список используемых источников:

1. Аверченков О. Е. Основы схемотехники аналого-цифровых устройств : учеб. пособие. М. : ДМК Пресс, 2012. 80 с.
2. Волович Г. И. Схемотехника аналоговых и аналого-цифровых электронных устройств. М. : ДМК Пресс, 2015. 528 с.
3. Гутников В. С. Интегральная электроника в измерительных устройствах. Л. : Энергоатомиздат. Ленингр. отд-ние, 1988. 304 с.
4. Кестер У. Проектирование систем цифровой и смешанной обработки сигналов : пер. с англ. М. : Техносфера, 2010. 328 с.
5. Микросхемы АЦП и ЦАП. Справочник. М. : ИД Додэка-Х, 2005. 422 с.
6. Федорков Б. Г. Микросхемы ЦАП и АЦП: функционирование, параметры применение. М. : Энергоатомиздат, 1990. 320 с.
7. Шило В. Л. Популярные цифровые микросхемы. М. : Радио и связь, 1987. 352 с.
8. Жан М. Р., Ананта Ч., Боривож Н.. Цифровые интегральные схемы. Методология проектирования = Digital Integrated Circuits : пер. с англ. М. : Вильямс, 2007. 912 с.
9. Топильский В. Б. Схемотехника аналого-цифровых преобразователей. М. : ТЕХНОСФЕРА, 2014. 288 с.
10. Микроэлектронные цифро-аналоговые и аналого-цифровые преобразователи информации / под ред. В. Б. Смолова. Л. : Энергия, 1976. 336 с.

Giniyatullin A., Nikitin Yu., Yurova V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

A variant of vernier digital-to-analog conversion.

The creation of high-precision and high-speed digital-to-analog converters (DACs) is a rather complex and time-consuming process that requires a lot of resources to meet all the requirements for the technology. However, DACs constructed with vernier technology have a sufficiently high speed and allow increasing bitrates without loss of this speed

Key words: *digital-to-analog converter, arithmetic adder, analog adder, vernier, control code, industrial electronics*

УДК 538.9
ГРНТИ 47.29.37

МАСС СПЕКТРОМЕТР И ЕГО ИСПОЛЬЗОВАНИЕ ПРИ ИССЛЕДОВАНИИ ЭФФЕКТА ПОЛЕВОЙ ЭМИССИИ.

В. В. Гришин, А. Г. Колосько

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Сегодня иметь возможность наблюдать поверхность наноструктур является жизненно необходимой. Приборы на основе эффекта полевой эмиссии позволяют это сделать, однако для получения оптимальных характеристик процесса требуется исследование внешних факторов, влияющих на испускание электронов. Одним из подходящих для этого приборов является масс-спектрометр.

полевая эмиссия, масс-спектрометрия, состав остаточной атмосферы, адсорбция

Масс-спектрометром называется устройство, позволяющее определить состав вакуума, газа, жидкого вещества и даже твёрдых тел на атомном уровне. Делается это благодаря тому, что молекулы различных веществ имеют различные соотношения масса/заряд.

В независимости от того, какого типа масс-спектрометр, принцип работы является следующим:

- ионизация атомов вещества
- ускорение заряженных ионов электрическим полем
- разделение ионов на «пакеты»
- фиксация «пакетов» детектором.

При исследовании газообразного вещества свободные атомы существуют априори, поэтому переход к процессу их ионизации не составляет труда. Если же необходимо анализировать твёрдую или жидкую среду на её состав, то предварительно переводят материал в состояние атомного пара; для этих целей применяют атомизатор, преимущественно термического или электротермического типа.

После процесса образования свободных атомов происходит ионизация вещества. Для этого используется термокатод, в результате нагрева которого осуществляется электрический разряд. Из-за ударов электронов, возникших при разряде, по атомам среды происходит ионизация вещества. В итоге образуются положительно заряженные ионы, которые под действием выталкивающего импульса электрического поля начинают своё движение в сторону анода. Этот импульс создаётся при участии отражателя, который выступает в качестве анода. Когда же частицы пролетают отражатель, то на него подаётся обратное напряжение, заставляющее их двигаться в обратном направлении, где они в последствие улавливаются детектором.

Детектор, принимая пакет ионов, преобразует его в электрический ток, причём вследствие дискретности потока частиц ток будет не постоянным, а

импульсным. Амплитуда импульсов тока пропорциональна количеству принятых детектором ионов.

Важным моментом является наличие одинакового импульса частиц, но не скорости, из-за различия которой и происходит деление на «пакеты».

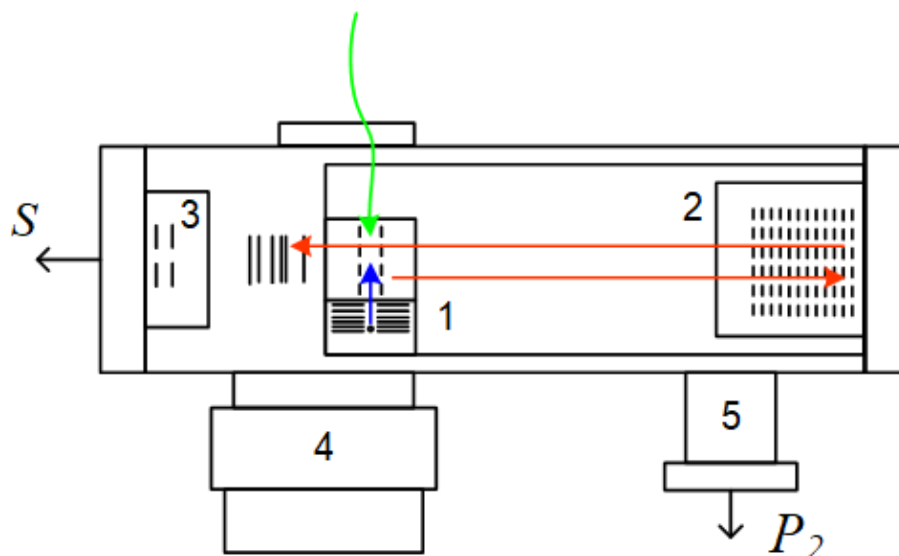


Рис. 1. Схема работы масс-спектрометра, где 1) Ионизатор и термокатод; 2) Отражатель; 3) Детектор; 4) Вакуумный насос, необходимый для поддержания чистоты процесса; 5) Датчик давления.

В ходе работы детектора получается зависимость силы импульсного тока от времени, которая с помощью несложных математических преобразований трансформируется в зависимость от массы частиц.

Время и масса в масс-спектрометре связаны следующим образом:

$$t = A * \sqrt{m} + B$$

где A и B – постоянные. Отсюда масса выражается как:

$$m = \left(\sqrt{m_1} + \frac{t - t_1}{t_2 - t_1} * (\sqrt{m_2} - \sqrt{m_1}) \right)^2$$

Здесь массы и моменты времени с индексами 1 и 2 – значения для уже известных нам элементов таблицы Менделеева. Удобнее всего использовать H_2 и CO . После замещения времени массой на графике получается масс-спектр остаточной атмосферы [1], т.е. зависимость пиков силы тока от массы вещества (см. рис. 2).

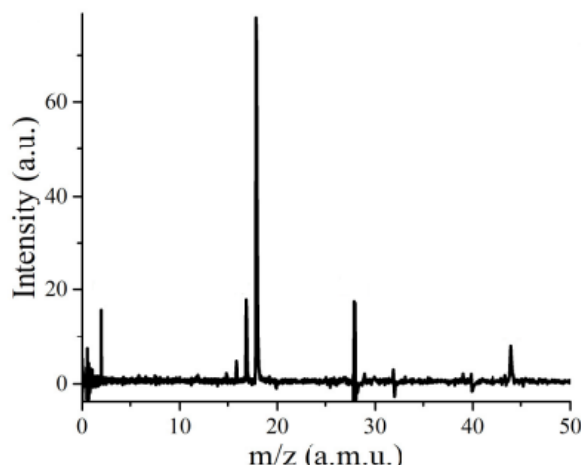


Рис. 2. Пример полученного масс-спектра; исходя из графика можно сделать вывод, что в среде преобладает вода, водород и азот (атомные массы 18, 2 и 28 соответственно)

Масс-спектрометрия активно применяется в исследовании физических принципов работы полевых катодов, поскольку наличие летучих веществ может напрямую сказаться на свойствах излучателя.

Связано это с тем, что катод имеет свойство адсорбировать некоторые атомы вещества извне. Исходя из теории квантовой физики, присоединённый атом изменяет форму энергетической зоны поверхности анода, что влечёт за собой изменение вероятности туннелирования электрона сквозь запрещённую зону [2].

В зависимости от вида адсорбента электрону становится либо тяжелее покинуть эмиссионный центр, либо наоборот проще за счёт эффекта «резонансного туннелирования» [3]. В этом случае адсорбент играет роль остановки на пути в вакуум, что, однако, приводит к уменьшению работы выхода вещества. Эффект возможен при переходах между одинаковыми энергетическими уровнями в эмиттере и атоме вещества.

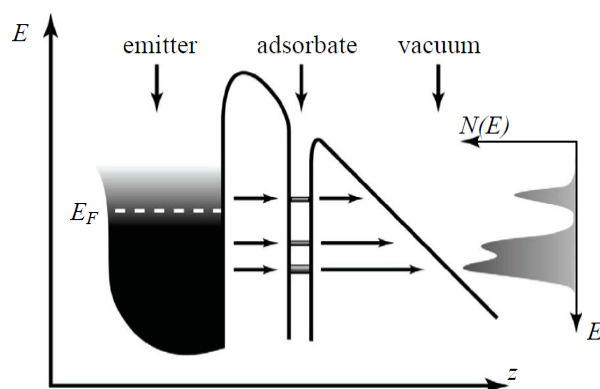


Рис. 3. Энергетическая диаграмма вещества при резонансном туннелировании

С течением времени может произойти обратный процесс – десорбция, после чего уже новый атом может осесть на освободившееся место. В результате непрерывных адсорбционно-десорбционных процессов на поверхности

многоострийного полевого катода происходят флуктуации эмиссионного тока, что вызывает шум и приводит к нестабильности общего тока и, в частности, к перегреву катода и переходу его в режим термо-эмиссии, который может закончиться саморазрушением.

Таким образом, масс-спектрометр является неотъемлемой частью исследования эффекта полевой эмиссии при использовании многоострийных катодов.

Список используемых источников:

1. Ануфриев Г. С., Болтенков Б. С., Рябинков А. И. Масс-спектры высокого разрешения остаточного газа в металлической вакуумной системе // Журнал технической физики. 2006, Т. 76, Вып. 1. С. 105-113.

2. Eugeni O. Popov, Anatoly G. Kolosko, Sergey V. Filippov, Igor L. Fedichkin, and Pavel A. Romanov. Mass-spectrum investigation of the phenomena accompanying field electron emission: : Journal of Vacuum Science & Technology B 33, 03C109 (2015), С. 3-5.

3. Gadzuk J. W., Resonance Tunneling of Field Emitted Electrons Through Adsorbates on Metal Surfaces, Special Publication (NIST SP), v. 958, 2001.

Grishin V., Kolosko A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication.

Mass-spectrometer and it's use in the study of the field emission effect. Today, all electronics strives to reduce the size of the elements to achieve speed of impact and compactness. In such conditions, being able to observe the surface of nanostructures is vital. Devices based on the field emission effect allow this to be done, however, in order to obtain optimal process characteristics, an investigation of external factors affecting the emission of electrons is required. One of the devices suitable for this is a mass spectrometer.

Key words: *field emission, mass spectrometry, residual atmosphere composition, adsorption.*

УДК 66.071.6
ГРНТИ 44.01.11

ПРОИЗВОДСТВО ВОДОРОДА В МИРЕ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

Р. С. Гуляев, С. Р. Кузенов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

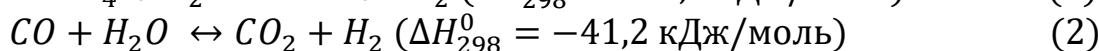
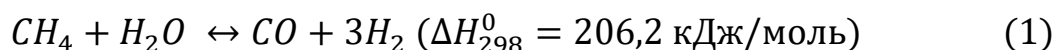
Водород – самый распространённый элемент во Вселенной. Водород рассматривается как перспективный энергоноситель вместо существующих жидких и газообразных углеводородных топлив. В работе представлены кратко представлены основные способы получения водорода, существующие на сегодняшний день.

получение водорода, цвета водорода, водородный топливный элемент

В свободном состоянии водород на Земле практически нигде не встречается, он находится в связанном состоянии либо в молекулах воды, либо в молекулах углеводородов, спиртов и т. д. Поэтому одной из важнейшей задачей водородной энергетики является получение водорода из существующих в природе водородсодержащих соединений.

Целью работы было определение особенности и основных параметров особенностей современных методов производства водорода и их энергетической эффективности. Для этого был проведён анализ основных методов производства водорода, применяемых в производстве в настоящее время, сравнить экономическую стоимость различных способов получения водорода. Для этого были проведены анализ научной и специализированной литературы по теме исследования, сопоставление и оценка данных по особенностям технологий и их эффективности.

Получение водорода. В настоящее время до 90 % водорода в мире получают из ископаемых топлив [1], причем 48 % производства водорода осуществляется за счет парового риформинга природного газа, более 20 % – из легких фракций нефти, 18 % – за счет газификации угля и только 4 % – за счет электролиза, из-за все еще высокой себестоимости производства водорода этим способом [2, 3]. Риформинг углеводородных топлив происходит в специальных химических реакторах – риформерах. Наиболее часто используемым сырьем являются природный газ и другие легкие углеводороды. Рассмотрим реакцию парового риформинга метана, который в промышленности обычно проводят в две стадии:



Первая реакция (1) является обратимым эндотермическим процессом и в промышленности ее проводят при температурах 700-900 °С и давлениях 2-3 МПа и называется реакцией парового риформинга метана (ПРМ). Вторая реакция (2) является экзотермической, целью данной реакции является увеличение выхода

водорода при реакции ПРМ, данная реакция именуется в англоязычной литературе WGS- реакция, которая протекает при температурах 250-400°C. Таким образом, при реакции ПРМ на выходе имеется газовая смесь, состоящая в основном из CO_2 и H_2 , и в меньшей степени CO с условием проведения реакции (2). В последние годы интенсивно развивается технология получения водорода путем газификации биомассы, однако себестоимость данного процесса достаточно высока по сравнению с конверсией ископаемых топлив [4].

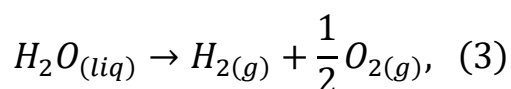
Для извлечения водорода из этой смеси существуют несколько способов, самыми распространенными из которых являются сорбционный и мембранный [5].

В сорбционном способе очистки водорода от газовых примесей используется принцип разделения газов, основанный на разной скорости их адсорбции на промышленных адсорбентах. Легко адсорбируемые примеси достаточно быстро поглощаются адсорбентом, для слабо адсорбируемых примесей требуется большее время адсорбции. Регенерация (десорбции примесей) происходит путем снижения давления после процесса адсорбции, т.е. адсорбция происходит при высоком давлении, десорбция при существенно более низком. На таком принципе работают установки короткоциклового адсорбции (КЦА), применяемые в промышленности для получения чистого водорода. Современные установки КЦА способны выделять до 400000 м³/ч водорода чистотой до 99,9999 % из продуктов конверсии углеводородных топлив [6].

Применение мембранных технологий для выделения водорода из газовых смесей экономически более целесообразно для установок производительностью менее 1000 м³/час. Мембранный способ разделения водорода является одностадийным, по сравнению с сорбционными технологиями, мембранный метод обладает более низким энергопотреблением, мембранные установки по сравнению с установками КЦА имеют меньшие габариты [5].

Как уже было ранее сказано, около 4% водорода в мире получают из воды путем электролиза. Электролиз воды является наиболее известным и изученным методом получения водорода и один из самых простых технологических способов получения чистого водорода (99.5-99.99%), который непрерывно может производиться в одну технологическую ступень [8].

В настоящее время наибольшее распространение получили три типа электролизера: щелочные, твердополимерные и твердооксидные. Первые два типа электролизеров относятся к низкотемпературным, последний тип - к высокотемпературным. Реакцию разложения воды при $T = 298$ К (25°C) и давлении 1 бар можно описать уравнением:



При термонеutralном напряжении ($\approx 1,48$ В при температуре ниже 100°C) разложение воды в реакции (3) происходит только за счет подводимой электрической энергии, без выделения или поглощения теплоты и для

осуществления реакции разложения воды при комнатной температуре требуется подвод значительного количества электроэнергии.

Расход электроэнергии можно уменьшить, если проводить электролиз при более высоких температурах, т.е. проводя реакцию с подводом тепла. Такой способ используется в высокотемпературных твердооксидных электролизерах, которые имеют самый высокий термодинамический КПД при условии подвода высокопотенциального тепла (800-900°C) [9].

Экономический анализ получения водорода. Экономика процессов получения водорода детально исследована в работе [7] и представлена в таблице 1.

ТАБЛИЦА 1. Экономические оценки основных методов получения водорода

Процесс	Источник энергии	Сырье	Стоимость водорода, \$/кг	Капитальные затраты, млн \$
ПРМ с улавливанием CO ₂	Ископаемое топливо	Природный газ	2,3	227
ПРМ без улавливания CO ₂	Ископаемое топливо	Природный газ	2,0	181
Ветровой электролиз	Ветер	Вода	5,9 – 6,0	499 – 505
Атомный термоэлектролиз	Атомная энергия	Вода	2,2 – 2,6	≈ 2100
Солнечный электролиз	Солнце	Вода	8,0 – 8,4	5,7 – 16
Электролиз с помощью ГЭС	Вода	Вода	3,2	≈ 2500

Результаты: В соответствии с данными таблицы 1, наиболее привлекательным с финансовой точки зрения способом получения водорода является паровой риформинг метана. Атомные термохимические циклы вполне могут конкурировать с ископаемым топливом и биомассой по цене; а в случае проведения электролиза с использованием силы ветра или солнечной энергии себестоимость получаемого водорода оказывается самой высокой.

Из данных таблицы 1 следует, что на протяжении почти 50 лет самым предпочтительным способом получения водорода является ПРМ. В настоящее время подавляющее большинство водорода в мире получают с применением технологий ПРМ + КЦА без улавливания и хранения CO₂. С точки зрения выбросов парниковых газов водород, полученный путем конверсии углеводородного сырья без предварительного улавливания CO₂, является «грязным» и его именуют «серым» водородом. Однако в связи с развитием «зеленой» энергетики в мире (электроэнергия из ВИЭ), а также с интенсивным исследованием новых материалов для создания высокопроизводительных и

относительно дешевых электролизеров в последние годы наблюдается увеличение доли производства зеленого водорода.

Водород, полученный путем электролиза, называется «зеленым» водородом. При получении водорода электролизом отсутствует проблема утилизации CO_2 и это является главным достоинством данного метода.

В последние десятилетия ведутся интенсивные исследования и разработки материалов для электролизеров с максимальным КПД, которые способны работать в течение длительного времени без существенного снижения производительности. На сегодняшний день наиболее перспективными электролизерами являются низкотемпературные электролизеры с твердополимерными электролитами, обладающими высоким КПД, малым временем пуска/остановки и низкой температурой эксплуатации. Например, компания Hysata [10] разработала водородный электролизёр с рекордным КПД, равным 95 %.

В последние десятилетия интенсивно развивается направление атомно-водородной энергетики, в которой одним из предложений является использование избыточного высокопотенциального тепла, отводимого из ядерных реакторов для работы высокотемпературных электролизных установок. Водород, получаемый с помощью такой технологии, называется «желтым» («оранжевым») водородом [11]. К сожалению, на сегодняшний день из-за высоких температур эксплуатации существующие высокотемпературные электролизеры не способны работать в течение длительного времени.

При извлечении водорода из газовой смеси, образуемой в реакции ПРМ, с помощью сорбционных или мембранных технологий, возникает проблема утилизации CO_2 . Активно ведутся разработки технологий улавливания и хранения CO_2 , и водород, получаемый из углеводородного сырья, одновременно с утилизацией CO_2 называется «голубым» водородом. В настоящее время стоимость «голубого» водорода заметно превышает стоимость «серого» водорода [7].

Выводы: Выяснены и объяснены основные способы получения водорода, проанализированы стоимость водорода и капитальные затраты каждого из способов, проведен анализ по изучению основных способов получения водорода, представлено подробное описание получения «серого» водорода (получается из ископаемых топлив) доля которого является основным на сегодняшний день. В связи с интенсивным развитием в мире сектора ВИЭ, а также с возрастающим числом исследований, посвященным разработкам новых материалов для высокоэкономичных электролизеров, «зеленый» водород в перспективе может заметно уменьшить долю «серого» водорода в спектре «цветов» получаемого в мире водорода.

Список используемых источников:

1. Decourt B., Lajoie B., Debarre R., Soupa O. Hydrogen-Based Energy Conversion, More Than Storage: System Flexibility; SBC Energy Institute: France. 2014, - 48 p.
2. Wang Z., Roberts R., Naterer G., Gabriel K. Comparison of thermochemical, electrolytic, photoelectrolytic and photochemical solar-to-hydrogen production technologies. Int. J. Hydrogen Energy, 2012. Pp. 16287–16301.

3. El-Shafie M., Kambara S., Hayakawa Y. Hydrogen Production Technologies Overview. J. Power Energy Eng, 2019. Pp. 107–154.
4. Moate J. R., LeVan M. D. Temperature swing adsorption compression: Effects of nonuniform heating on bed efficiency. Applied Thermal Engineering, 2010. Pp. 658-663
5. Ямпольский Ю.П. Новые полимерные материалы газоразделительных мембран. Высокомолекулярные соединения. (1993) Т.35. №1. С. 51-62.
6. Сайт химической компании по производству технических газов Air Liquide. URL: <https://www.engineering-airliquide.com/ru/adsorbtsiya-pri-peremennom-davlenii-psa-ochistka-vodoroda> (Дата обращения: 02.10.2022)
7. Kayfeci M. et al. Hydrogen production in Solar Hydrogen Production. [Электронный ресурс]. 2019. URL: <https://www.sciencedirect.com/topics/engineering/hydrogen-production-cost> (Дата обращения^ 21.10.2022).
8. Schug C.A. Operational characteristics of high-pressure, high-efficiency water-hydrogen-electrolysis. Int. J. Hydrogen Energy. 1998. N 23. Pp. 1113.
9. Rosa V.M., Santos M.B.F., Da Silva E.P. New Materials for Water Electrolysis Diaphragms. Int. J. Hydrogen Energy. 1995. N. 20. Pp. 697.
10. New Atlas. URL: <https://newatlas.com/energy/hysata-efficient-hydrogen-electrolysis/> (Дата обращения: 16.03.2022).
11. Пономарев-Степной Н.Н., Столяревский А.Я. Атомно-Водородная энергетика. М. : Энергоатомиздат, 2008. – 107 с.

Gulyaev R., Kuzenov S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Hydrogen production in the world: current state and prospects.

Hydrogen is the most common element in the universe. Hydrogen is considered as a promising energy carrier instead of existing liquid and gaseous hydrocarbon fuels. The paper briefly presents the main methods of producing hydrogen that exist today.

Key words: production of hydrogen, hydrogen colors, hydrogen fuel cell.

УДК 621.355.9
ГРНТИ 47.59.39

ОСОБЕННОСТИ ЗАРЯДА И РАЗРЯДА ЛИТИЕВЫХ БАТАРЕЙ. НЕДОСТАТКИ ПАССИВНЫХ И АКТИВНЫХ БАЛАНСИРОВ

А. И. Кучерявый, Е. Ю. Передистов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье разобраны особенности заряда и разряда многоячеестых литиевых аккумуляторных батарей. Описаны принципы работы самых распространённых методов зарядки одиночных аккумуляторов и многоячеестых батарей, их основные преимущества и недостатки при различных условиях эксплуатации. Описаны условия проявления этих недостатков.

литиевые аккумуляторы, системы зарядки, активные балансиры, пассивные балансиры

Литиевые аккумуляторы на сегодняшний день встречаются повсеместно. Сборки из литиевых аккумуляторов являются основным источником энергии для электротранспорта. Для увеличения ёмкости аккумуляторной батареи литиевые аккумуляторы соединяют параллельно, а для увеличения напряжения их соединяют последовательно. Сборку из аккумуляторов соединённых последовательно в составе батареи называют аккумуляторной ячейкой. Зарядка одной аккумуляторной ячейки является тривиальной задачей. Для её решения существует огромное количество различных микросхем, самые распространённые из которых: tp4056, xl4005e1, ip2312 и т.д. В это же время зарядка батарей состоящих из нескольких ячеек – сложная задача.

Существует три основных способа заряда многоячеестых литиевых батарей. Первый – использование балансиров. Второй – использование зарядных устройств с гальванической развязкой выходов. Третий – перекоммутация ячеек с последовательной схемы в параллельную схему с дальнейшей зарядкой батареи, как одноячеестой. Самым распространённым на сегодняшний день способом является первый. Его реализуют либо с помощью встроенного в устройство активного или пассивного балансира, обычно входящего в плату BMS (Battery Management System), тогда для зарядки к устройству подключают источник питания с постным напряжением и ограничением по току, либо с помощью внешнего балансира, встроенного в зарядное устройство. На рис. 1 показана плата BMS с встроенным в неё пассивным балансиром, предназначенная для установки непосредственно в устройство и зарядное устройство IMAX B6 MINI с пассивным балансиром внутри.



Рис. 1. Пассивный баланси́р в плате BMS и зарядное устройство с встроенным баланси́ром

При встроенном в устройство баланси́ре увеличивается его массогабаритные характеристики, что может быть критично для некоторых устройств, таких как квадрокоптеры, поэтому часто в них и баланси́р и систему защиты батареи не используют, подключая батарею непосредственно к потребителю энергии. Использование внешнего баланси́ра встроенного в зарядное устройство решают эту проблему, но остается ряд недостатков свойственных всем баланси́рам без исключения.

Все эти проблемы возникают из-за несколько отличающихся по ёмкости последовательно соединённых ячеек батареи. Эти отличия невозможно устранить, возможно только минимизировать отличия путем индивидуальной проверки каждой из ячеек, а также сборки батареи из ячеек максимально близких по характеристикам. Однако даже в этом случае двух одинаковых батарей не подобрать, всегда есть небольшие отличия в состоянии заряда батарей, саморазряда, емкости, сопротивлении и температурных характеристиках; даже если речь идет о батареях одинаковых типов, от одного производителя и одной производственной партии [1]. В свою очередь внешние факторы, например неравномерный нагрев батареи из-за близлежащих источников тепла в устройстве, еще больше увеличивают разброс параметров последовательно соединенных ячеек [2].

Баланси́ры бывают пассивные и активные. Пассивные баланси́ры при полной зарядке любой из ячеек замыкают её на резистор, и большая часть тока заряда идет через него, превращаясь в тепло. Типичная схема такого подключения изображена на рис. 2. Процесс происходит до тех пор, пока все ячейки не зарядятся [3]. Главными недостатками пассивных баланси́ровка являются большой нагрев и малый ток баланси́ровки, который даже в мощных баланси́рах редко превышает 400 мА, что в свою очередь может увеличить время заряда в разы. Если заряжается очень ёмкая батарея или если, по какой-либо причине, одна или несколько ячеек разряжены или заряжены существенно больше, чем другие. Продолжением этой проблемы является перезаряд уже заряженных ячеек при длительной баланси́ровке. Хотя батареи и шунтируются резистором, часть тока продолжает протекать через уже заряженную ячейку. При продолжительной баланси́ровке, напряжение на самых малоёмких ячейках

может добираться до критических 4.25 В, после чего зарядка всей батареи практически останавливается.

Если зарядка остановилась из-за уже заряженных ячеек и если зарядились крайние ячейки, дозарядить оставшиеся можно как отдельную батарею, исключив заряженные. Однако это увеличивает и усложняет процесс заряда для внешних систем балансировки, а для встроенных этот метод и вовсе недоступен. При этом если проблема возникла с центральными ячейками, то дозарядить их придется и вовсе по отдельности.

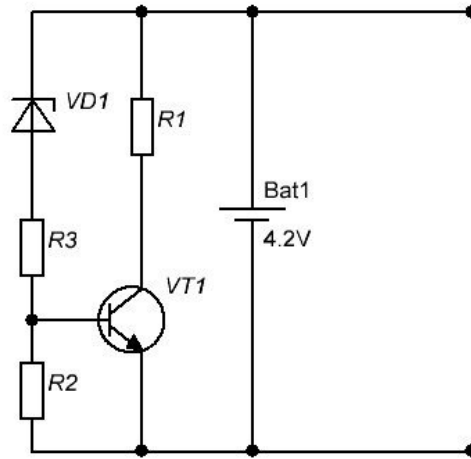


Рис. 2. Схема шунтирования заряженной батареи

С этой проблемой столкнулся автор при использовании зарядного устройства iMAX b6 при зарядке 3s4r батареи ёмкостью 10 Ач из литий-ионных аккумуляторов. Даже при том, что батареи собраны из аккумуляторов одной партии, ёмкость последовательно соединенных ячеек отличалась. Вследствие чего при зарядке батареи током 4.6 А, после полной зарядки третьей ячейки, устройство зарядки перешло в режим балансировки. В этом режиме ток балансировки устройства составляет 200 мА, скорость зарядки при этом упала до 0.1–0.3 А т.е. в десятки раз, рис. 3. Поэтому недозапряжённые ячейки постоянно приходится заряжать по отдельности, что в разы дольше и доставляет неудобство.



Рис. 3. Замедлившаяся зарядка после третьей ячейки аккумулятора

При всем этом при использовании пассивного балансира общая емкость аккумулятора оказывается не больше, чем у ячейки аккумулятора с минимальной емкостью [4].

Активные балансиры лишены этих недостатков. Вместо рассеивания всей избыточной энергии в тепло через резистор, энергию из самой заряженной батареи с помощью конденсатора или индуктивности передают в менее заряженные ячейки, рис. 4. Это позволяет существенно увеличить токи балансировки, сократить нагрев и время заряда. При этом, если активный балансир встроен в устройство, то в процессе эксплуатации самые ёмкие батареи будут подзаряжать менее ёмкие, что в теории может сделать общую ёмкость батареи большей, чем ёмкость ячейки с наименьшей ёмкостью. Этот эффект тем заметнее, чем менее интенсивно происходит разряд батареи. Однако когда время разрядки мало, а ток разрядки велик этот эффект практически незаметен, что снижает целесообразность использования активного балансира.

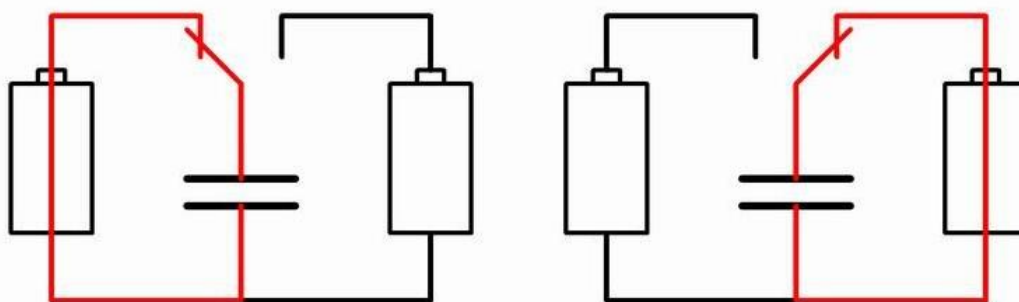


Рис. 4. Принцип работы активного балансира с использованием конденсатора

Главными недостатком активных балансиров являются дороговизна компонентов, затраты времени и средств на проектирование и изготовление. А также заметное потребление тока активными балансиром на холостом ходу.

Таким образом, хоть балансиры и выполняют свою функцию и используются повсеместно, в некоторых случаях их недостатки заставляют задуматься над другими методами балансировки батарей.

Список используемых источников:

1. Сихуа Вэн. Выравнивание параметров секций аккумулятора обеспечивает дополнительное время работы и увеличивает срок службы аккумуляторных батарей // Компоненты ТП: Бюллетень научно-технической информации. — 2011. — Вып. 2 (30). — С. 44-48.
2. Рыкованов А., Беляев С. Активные и пассивные системы баланса li-ion аккумуляторных батарей // Компоненты и технологии. 2014. N 3. С. 121–124.
3. Кучерявый А. И. Разработка зарядного устройства литиевых аккумуляторов с гальванической развязкой заряжаемых ячеек // Студенческая весна – 2022 : вуз. сб. науч. тр. / Под ред. Е. Ю. Передистова. Санкт-Петербург : Изд-во Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2022. С. 83–88.
4. Мельничук О., Фетисов В. Особенности заряда и разряда литиевых аккумуляторных батарей и современные технические средства управления этими процессами // Электротехнические и информационные комплексы и системы. 2016. N 2. С. 41–48.

Kycheryavyi A., Peredistov E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Features of charging and discharging lithium batteries. Disadvantages of passive and active load balancers.

The article analyzes the characteristics of the charge and discharge of multi-cell lithium batteries. The principles of operation of the most common methods of charging single batteries and multicellular batteries are described. Their main advantages and disadvantages under various operating conditions are considered. The conditions for the manifestation of these shortcomings are described.

Key words: *lithium batteries, charging systems, active balancers, passive balancers.*

УДК 004.383.3
ГРНТИ 50.43.15

ПРИМЕНЕНИЕ МИКРОКОНТРОЛЛЕРОВ ОБЩЕГО НАЗНАЧЕНИЯ В DC-DC ПРЕОБРАЗОВАТЕЛЯХ НАПРЯЖЕНИЯ

Н. Е. Скороходов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Любой современный преобразователь напряжения постоянного тока имеет в своем составе петлю обратной связи, позволяющую значительно расширить его возможности и улучшить характеристики. В простейшем случае петля обратной связи состоит из операционного усилителя и управляемого генератора сигнала широтно-импульсной модуляции. Использование цифрового устройства управления позволяет не только организовать надежную обратную связь, но и обеспечить работу сложных схем с большим количеством синхронных ключей. При этом все необходимые устройства для регуляции работы преобразователя будут расположены на одном единственном кристалле интегральной микросхемы. Преимуществом использования вычислителей именно с программным управлением является их небольшая цена, а также скорость и простота разработки и отладки программного обеспечения.

DC-DC преобразователь, микроконтроллер, цифровая обратная связь

Как известно, в преобразователях напряжения постоянного тока зависимость уровня выходного напряжения от величины входного напряжения может быть устранена с помощью введения петли обратной связи. В общем случае сигнал обратной связи подается на усилитель ошибки, который сравнивает фактический уровень выходного напряжения с неким опорным значением, регулируя выходное напряжение так, чтобы привести его к заданному значению. Поскольку регулировка осуществляется в противофазе по отношению к отклонению (если выходное напряжение слишком высоко, то действие направлено на его уменьшение, а если оно слишком низко, то на его увеличение), такая обратная связь называется отрицательной. Если же петля обратной связи окажется положительной, то любые ошибки будут усиливаться и выходное напряжение либо будет пульсировать, либо быстро установится на минимальном или максимальном возможном для нее значении. Обеспечение такого режима, при котором во время переходных процессов условия для положительной обратной связи никогда бы не возникали, является одним из самых сложных аспектов разработки петли регулирующей обратной связи [1].

Петля обратной связи должна обеспечивать как компенсацию всех изменений входного напряжения, так и любых изменений, вызванных изменением нагрузки на преобразователь. На рис. 1 представлена схема понижающего преобразователя напряжения с двумя ключами, работающими в противофазе. Здесь поделенное выходное напряжение подается на инвертирующий вход операционного усилителя, работающего по схеме усилителя ошибки. Разность входных напряжений порождает пропорционально большое выходное напряжение операционного усилителя, которое призвано

регулировать рабочий цикл ШИМ-генератора, что в свою очередь влияет на значение выходного напряжения. Таким образом выходное напряжение можно задать путем подбора номиналов резисторов R_1 и R_2 . Стоит также отметить, что для исключения зависимости выходного напряжения от входного необходимо подобрать амплитуду управляющего ШИМ-сигнала в зависимости от статических характеристик транзисторного ключа.

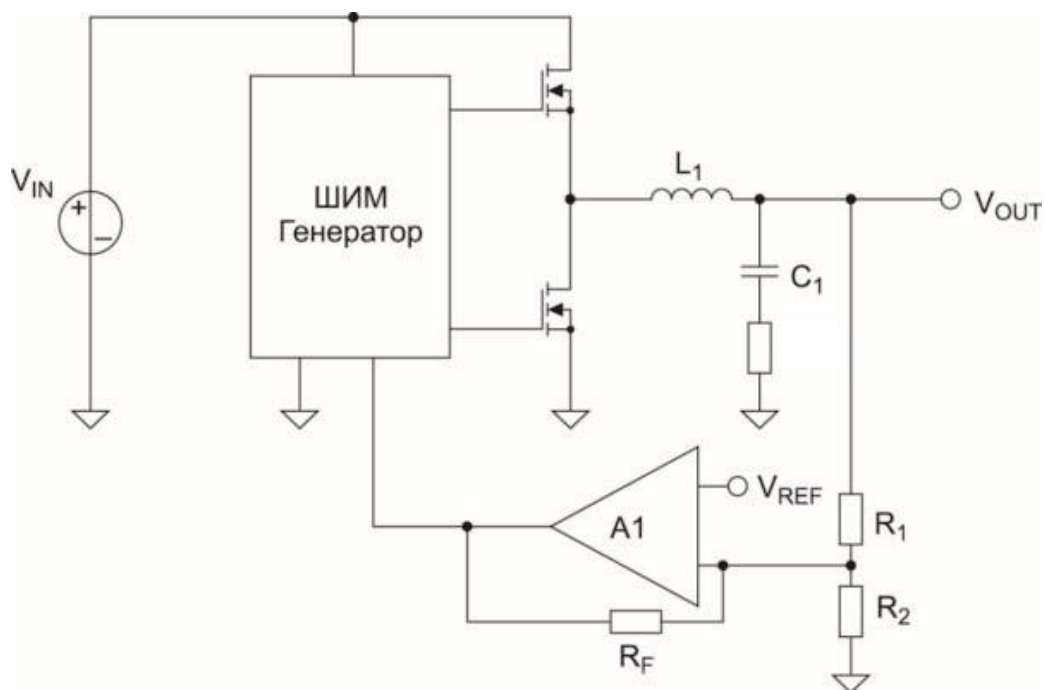


Рис. 1. Схема понижающего преобразователя напряжения с функцией стабилизации

Использование высокоинтегрированных устройств с программируемой логикой, таких как ПЛИС, сигнальные процессоры и микроконтроллеры, позволяет управлять более сложными схемами DC-DC преобразователей. При этом в разы сокращается занимаемое полезное пространство по сравнению со схемами с аналоговым управлением. В случае использования программно-управляемых вычислителей, процессы выбора элементной базы и разработки устройства будут значительно ускорены.

Микроконтроллеры широко применяются в системах управления источниками питания, причем, в зависимости от требуемой частоты работы силовых ключей, либо весь регулятор строится на основе контроллера, либо он работает в связке с аналоговым ШИМ-контроллером. На рис. 2 представлена упрощенная схема мостового преобразователя напряжения с фазовым сдвигом, выполненная на базе микроконтроллера. Наличие нескольких модулей ШИМ в составе микроконтроллера позволяет управлять как самим мостовым преобразователем, так и его выходным синхронным выпрямителем. При помощи встроенного аналого-цифрового преобразователя (АЦП) производится слежение за входным и выходным напряжениями, а также осуществляется контроль температуры и слежение за значением выходного тока. В зависимости от состава

микроконтроллера также могут использоваться встроенные операционные усилители.

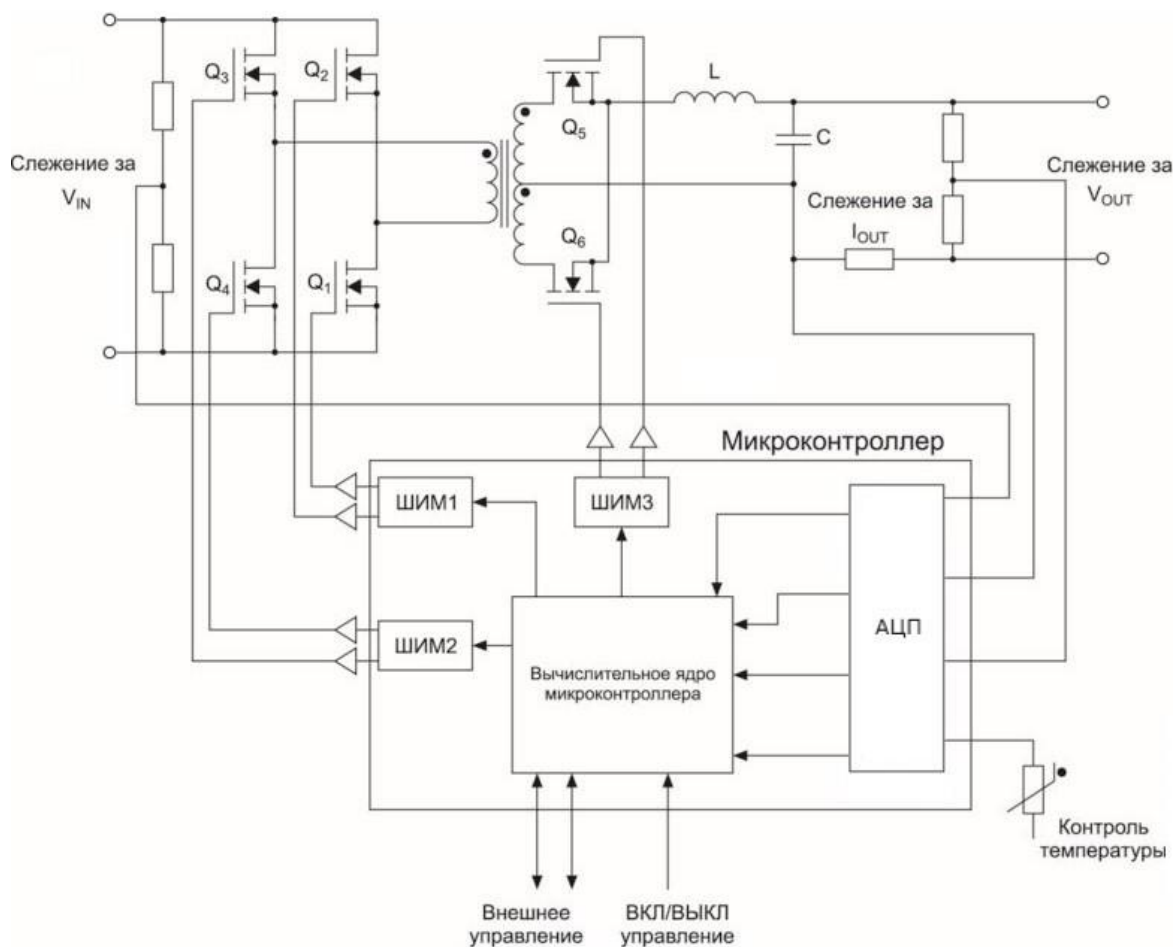


Рис. 2. Схема мостового преобразователя на основе микроконтроллера

На основе сигналов обратной связи и управляющего воздействия вычисляется отклонение или ошибка выходной величины. После цифровой коррекции и с помощью модулей ШИМ на основе счетчиков-таймеров формируются выходные импульсные последовательности, которые через формирователи импульсов или драйверы управляют работой силовых ключей.

Управление входным напряжением позволяет осуществлять как контролируемый пуск, так и программируемую блокировку с адаптивным гистерезисом при питании преобразователя от недопустимо низкого входного напряжения.

Контроль температуры может осуществляться как внутри самого DC-DC преобразователя, так и во внешней нагрузке. Последующая реакция в случае чрезмерного повышения температуры программируется в соответствии с техническими требованиями устройства. Например, для снижения тепловыделения может быть использована остановка с защелкой, отключение и автоматический перезапуск системы после охлаждения, а также ограничение мощности.

Внешнее управление позволяет реализовать такие условия работы, которые будут обновляться в реальном времени. Сигналы внешнего управления поступают в микроконтроллер от внешнего датчика, либо через один из входов АЦП, либо через один из коммуникационных интерфейсов (SPI, I²C, UART, и др.), в случае дистанционного управления. Кроме того, использование интерфейсов позволяет сигнализировать об ошибках и уведомлять вышестоящее устройство об обновлении состояния [2].

Для организации цифровой регуляции в современных DC-DC преобразователях микроконтроллер должен иметь развитую систему ШИМ-модулей, быстродействующий АЦП и высокую скорость выполнения базовых математических операций [3]. Перечисленными качествами обладают практически все современные микроконтроллеры общего назначения.

В таблице 1 представлены характеристики распространенных семейств микроконтроллеров, которые благодаря своим функциональным возможностям могут быть использованы для решения задач цифрового управления.

ТАБЛИЦА 1. Сравнение характеристик микроконтроллеров различных производителей

Семейство	Разрядность, бит	Тактовая частота, МГц	Память программ, Кбайт	ОЗУ, Кбайт	Напр. питания, В	Хар-ки АЦП	Кол-во выходов ШИМ
PIC24F GC	16	16	64-128	8	3-3,6	4 шт., 16 кан., 12 бит	12
dsPIC33F	16	40-50	64-256	8-16	3-3,6	1-2 шт., 18-32 кан., 10/12 бит	16
STM32	32	48-550	16-2056	8-512	1,7-3,6	1-3 шт., 16-24 кан., 12 бит	2-10
V850ES/Sx2	32	0.032-320	384-640	32-48	2,8-3,6	12-16 кан., 10 бит	9x16 12x16

В заключение стоит добавить, что вычислительные ядра микроконтроллеров семейств STM и PIC обладают низкой устойчивостью к воздействию сильных электромагнитных полей, характерных для силовой электроники. Это связано с тем, что команды для выполнения загружаются в память типа RAM, физической особенностью которой является низкая помехоустойчивость [3]. Поэтому с целью защиты от сбоя следует применять экранирование. Микроконтроллеры V850 являются более стабильными, поскольку команды исполняются непосредственно из Flash-памяти.

Список используемых источников:

1. Steve Roberts. DC/DC Book of Knowledge: Practical tips for the User. Second Edition, 2015. – 234 p.
2. Ice C., Kankanala R. Digital Control Brings More Efficiency to DC/DC Converters // Power Electronics Europe. – 2011. – № 5. – P. 17-19.

3. Буркин Е.Ю., Горюнов Г.А. Применение 32-разрядных микроконтроллеров NEC семейства V850ES/Sx2 в схемах источников электропитания // Компоненты и Технологии. – 2006. – № 6. – С. 78-81.

Skorokhodov N.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Application of General Purpose Microcontrollers in DC/DC Voltage Converters.

Any of modern DC/DC converters incorporates a feedback loop, which allows you to significantly expand its capabilities and improve performance. In the simplest case, the feedback loop consists of an operational amplifier and a controlled PWM signal generator. The use of a digital control device allows not only to organize reliable feedback, but also to ensure the operation of complex circuits with a large number of synchronous switches. In this case, all the necessary devices for regulating the operation of the converter are located on a single IC. The advantage of using software controlled chips is their low cost, as well as the speed and ease of development and debugging of software.

Key words: DC/DC converter, microcontroller, digital feedback loop.

РАДИОТЕХНОЛОГИИ СВЯЗИ

2.1. Медиа-технологии и телерадиовещание

УДК 006.86
ГРНТИ 84. 13. 53

ОЦЕНКА ПАРАМЕТРОВ ИЗЛУЧЕНИЙ ПЕРЕДАТЧИКОВ РАДИО ВЕЩАТЕЛЬНОЙ СЛУЖБЫ СРЕДСТВАМИ РАДИОКОНТРОЛЯ

Б. М. Антипин, А. К. Терновая

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Целью работы является анализ требований к допустимым отклонениям частоты, предъявляемых к передатчикам радиовещательной службы нормативными документами и нахождение методов их проверки.

радиовещательная служба, средства радиоконтроля, анализатор спектра, частотомер, допустимые отклонения частоты

Требования на допустимые отклонения частоты (ДОЧ) радиопередатчиков всех категорий гражданского применения устанавливаются Государственной комиссией по радиочастотам в Нормах 17-13, здесь же дается определение ДОЧ. Допустимое отклонение частоты – максимальное допускаемое отклонение средней частоты полосы частот излучения от присвоенной частоты или характерной частоты излучения от относительной частоты [1].

Выполнение измерений частоты радиопередатчика выполняется в соответствии с методиками (методами) измерений, аттестованными в установленном порядке. Погрешность измерения частоты должна составлять не более 0,1 от нормы допустимого отклонения частоты [1].

Допустимые отклонения частоты радиопередатчиков всех категорий гражданского применения не должны превышать значений, приведённых в таблице 1.

Допустимые отклонения частоты радиопередатчиков выражаются в миллионных долях относительно присвоенной частоты,

$$\frac{|f_u - f_n|}{f_n} \leq N \cdot 10^{-6}, \quad (1)$$

или в значениях абсолютного отклонения частоты в герцах от присвоенной частоты:

$$|f_u - f_n| \leq N_{abs}, \quad (2)$$

где N и N_{abs} указаны в таблице 1. N – норма допустимого относительного отклонения частоты радиопередатчика, выраженная в миллионных долях относительно присвоенной частоты; N_{abs} – норма допустимого абсолютного отклонения частоты радиопередатчика от присвоенной частоты, выраженная в герцах; f_n – присвоенная частота радиопередатчика; f_u – измеренная рабочая частота.

Присвоенная частота – средняя частота полосы частот, присвоенной станции.

ТАБЛИЦА 1. Требования на допустимые отклонения частоты радиопередатчиков

Полоса частот (исключая нижний и включая верхний пределы) и категории станций	Допустимое отклонение частоты	
	$\pm N \cdot 10^{-6}$	$\pm N_{\text{абс}} \text{ Гц}$
Полоса: 29,7-100 МГц		
Радиовещательные станции (кроме телевизионных)		
Станции аналоговые звукового радиовещания	0,5	
Полоса: 100-470 МГц		
Станции аналоговые звукового радиовещания	0,5	
Для передатчиков со средней мощностью 50 Вт или меньше		3000
Передатчики цифрового телевизионного вещания стандарта DVB		100
Полоса: 470-2400 МГц		
Радиовещательные станции (кроме телевизионных)	10	
Передатчики цифрового телевизионного вещания стандарта DVB		100

Целью измерения ДОЧ является обеспечение электромагнитной совместимости. Измерения проводятся средствами радиоконтроля без уведомления оператора или владельца средства, что накладывает определенные ограничения.

Погрешность измерения ДОЧ складывается из двух составляющих: погрешности средства измерения (СИ) и систематической погрешности. При измерении ДОЧ частотно-модулированных колебаний средствами радиоконтроля возникает систематическая погрешность, обусловленная конечным значением девиации частоты, так как средства радиоконтроля измеряют ДОЧ в штатном режиме работы передатчика.

$$\delta f_{\Sigma} = \delta f_{\text{СИ}} + \delta f_{\text{сист}}, \quad (3)$$

$$\Delta f_{\Sigma} = \Delta f_{\text{СИ}} + \Delta f_{\text{сист}}, \quad (4)$$

Оценить систематическую погрешность можно следующим образом:

$$\Delta f_{\text{сист}} = \frac{\Delta f_{\text{и max}} - \Delta f_{\text{и min}}}{2}, \quad (5)$$

где $\Delta f_{\text{и max}}$ – максимальное измеренное значение отклонения сигнала; $\Delta f_{\text{и min}}$ – минимальное измеренное значение отклонения сигнала.

Согласно требованиям норм ГКРЧ измерения ДОЧ следует проводить с помощью анализатора спектра или частотомера.

Для определения ДОЧ с помощью частотомера требуется провести множество измерений $n \geq 10$

$$\Delta f_{\text{cp}} = \frac{1}{n} \sum_{i=1}^n |f_{\text{и}i} - f_{\text{п}}|, \quad (6)$$

где $f_{и}$ - значение рабочей частоты радиопередатчика, полученное при i -ом измерении, Гц; $f_{п}$ - значение присвоенной частоты радиопередатчика, Гц.

Относительную погрешность измерения ДОЧ при использовании частотомера вычисляют следующим образом:

$$\delta_{f_{\text{част}}} = \left(\delta_0 + \frac{1}{\Delta t_0 \cdot f_{и}} \right), \quad (7)$$

где δ_0 – погрешность опорного генератора; Δt_0 – время счета в секундах; $f_{и}$ – измеряемая частота в герцах.

Тогда абсолютная погрешность

$$\Delta f = f_{и} \cdot \delta_{f_{\text{част}}}, \quad (8)$$

Для определения ДОЧ с помощью анализатора спектра требуется, прежде всего определить значение присвоенной полосы частот. Вычисляют значение присвоенной полосы частот $B_{п}$ радиопередатчика по формуле:

$$B_{п} = B_{н} + (2 \times N_{\text{абс}}), \quad (9)$$

где $B_{н}$ – значение необходимой ширины полосы частот, Гц; $N_{\text{абс}}$ – норма на допустимое отклонение частоты радиопередатчика.

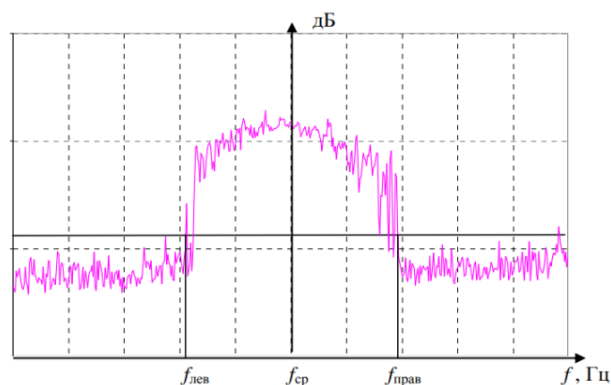
На спектрограмме, отображенной на экране анализатора спектра, находят две точки, лежащие на пересечении выбранного уровня с составляющими спектра сигнала, превышающими этот уровень, и имеющих минимальную $f_{\text{лев}}$ и максимальную $f_{\text{прав}}$ частоты. Проводят n измерений $f_{\text{лев}}$ и $f_{\text{прав}}$. Тогда разность значений $f_{\text{прав}} - f_{\text{лев}}$ можно принять за оценку $B_{п}$.

Определяют среднюю частоту присвоенной полосы частот $f_{\text{ср},i}$ и её отклонение $\Delta f_{\text{ср},i}$ от присвоенной частоты по формулам [2]:

$$f_{\text{ср},i} = 0,5 \times (f_{\text{лев},i} + f_{\text{прав},i}) \quad (10)$$

Тогда отклонение измеренной частоты

$$\Delta f_{и,i} = |f_{\text{ср},i} - f_{и}| \quad (11)$$


 Рис. 1. Иллюстрация метода определения $f_{ср}$

Погрешность измерения ДОЧ рассчитывается как сумма погрешностей, перечисленных в техническом описании анализатора. К ним относятся погрешность опорной частоты, погрешность установки полосы обзора и погрешность установки центральной частоты полосы разрешения.

$$\Delta f_{АС} = f_{и} \cdot \delta_0 + \Delta f_{по} + \Delta f_{цч}, \quad (12)$$

δ_0 – относительная погрешность опорного генератора; $\Delta f_{по}$ – погрешность установки полосы обзора; $\Delta f_{цч}$ – погрешность установки центральной частоты полосы разрешения.

Рассчитаем ДОЧ для аналогово радиовещания

$$\delta = 0,5 \cdot 10^{-6} \text{ – по таблице 1.}$$

$$\Delta f = 0,5 \cdot 10^{-6} \cdot 10^8 = 50 \text{ Гц}$$

Погрешность измерения ДОЧ

$$\Delta f_{доч} = 0,1 \cdot \Delta f = 5 \text{ Гц}$$

На основании вышеприведенных данных был выбран следующий частотомер: Частотомер электронно-счетный VM0401.

При использовании модуля кварцевого генератора VM2202 $\delta_0 = \pm 1 \cdot 10^{-9}$ за 24 ч и $\pm 1 \cdot 10^{-7}$ за 12 месяцев. Для расчета воспользуемся формулой 7.

$$\delta_{f_{част}} = \left(10^{-8} + \frac{1}{10^8} \right) = 2 \cdot 10^{-8}$$

$$\Delta f = f \cdot \delta_{f_{част}} = 2 \text{ Гц}$$

Анализатор радиосвязи MT8820C обладает следующей погрешностью опорного генератора:

$$\delta_0 = \pm 2 \cdot 10^{-8}$$

Следовательно, абсолютная погрешность вычисляется следующим образом (согласно формуле 12):

$$\Delta f_{\text{доч}} = 100 \cdot 10^{-6} \cdot 2 \cdot 10^{-8} + 1 + 0,5 = 4,5 \text{ Гц}$$

В ходе данной работы были проанализированы требования норм ГКРЧ 17-13 к значениям ДОЧ.

Были рассмотрены частотомеры и анализаторы спектра, с помощью которых могут быть определены ДОЧ и получены оценки погрешностей вносимые данными приборами.

В ходе работы установлено, что для оценки погрешности измерения ДОЧ необходимо учитывать как погрешность, вносимую СИ, так и систематическую составляющую погрешности измерения. Несмотря на то, что абсолютная погрешность измерения частотомера меньше, чем анализатора спектра, необходимо учитывать влияние также систематической составляющей погрешности, которая в измерении с помощью анализатора спектра отсутствует.

Список используемых источников:

1. Решение Государственной комиссии по радиочастотам при Минкомсвязи России от 24 июня 2013 г. № 13-18-03 «Об утверждении Норм 17-13. Радиопередатчики всех категорий гражданского применения. Требования на допустимое отклонение частоты.»
2. Приложение № 1 к решению ГКРЧ от 1 июля 2016 г. № 16-37-02

Ternovaya A., Antipin B.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Estimation of the radio broadcasting service transmitters' radiation by the radiocontrol means. The goal of the paper is to analyze the tolerance frequency deviation in the radio broadcasting service transmitters regarding the standard documentation and developing verification methods.

Key words: radio broadcasting service, radiocontrol means, spectrum analyzer, frequency counter, tolerance frequency deviation.

УДК 654.195.6
ГРНТИ 49.43.35

ИССЛЕДОВАНИЕ РАБОТЫ СРЕДСТВ РАДИОВЕЩАНИЯ НА ОБЪЕКТЕ РТПС В Н. П. МИХАЙЛОВКА

А. В. Вербицкий, М. А. Швец

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В цехе Михайловка “Волгоградского ОРТПЦ” филиала ФГУП РТПС заканчивается ресурс несущей способности мачты. Необходимо исследовать работу средств радиовещания для дальнейшей оптимизации места на мачте, которое в будущем будет занято оборудованием новых радиостанций и оборудованием сотовых операторов.

радиостанция, схема подачи сигнала, зона уверенного приёма

На радиотелевизионной станции (РТС) “Волгоградского ОРТПЦ” Российской телевизионной и радиовещательной сети (РТПС), в населённом пункте Михайловка, по заключению комиссии филиала заканчивается ресурс несущей способности мачты. В ходе исследования были поставлены следующие задачи:

1. изучить работающие на объекте радиостанции (РС) и используемое для этого оборудование;
2. рассчитать зоны уверенного приёма для действующих РС.

Сначала была изучена документация по имеющимся радиостанциям и схема расположения оборудования на мачте, а также были опрошены сотрудники предприятия после чего была составлена схема подачи сигнала [1,2,3,4].

Сигнал радиостанции “Радио России” поступает на объект со спутника на спутниковую тарелку, после чего сигнал через делитель сигналов поступает на основной и резервный спутниковые приёмники. Для резервирования используется отличный от основного приёмник, что позволяет избежать остановки вещания федеральной радиостанции. Далее сигнал с двух приёмников поступает на коммутатор, где происходит автоматическое переключение между приёмниками в случае аварии. После чего сигнал поступает на УКВ ЧМ передатчик мощностью 4 кВт, вещающий на частоте 106.5 МГц. С передатчика сигнал поступает по фидеру $RFA\ 1\ 5/8$ ” длиной 168 метров и потерями 1.124 дБ на антенную систему $BLR-2DBA \times 8$ [5], расположенную на высоте 133 метра с максимальной вмещающей мощностью 10 кВт.

Для радиостанций “Ретро ФМ” и “Новая волна” схема подачи сигнала одинакова. Сигнал поступает на объект со спутника на спутниковую тарелку. После чего сигнал подаётся на спутниковый приёмник и далее идёт на компьютер для обработки и его контроля. Далее сигнал поступает на УКВ ЧМ передатчик. В случае “Ретро ФМ” передатчик вещает на частоте 103.9 МГц и мощностью 0.5 кВт. Далее сигнал поступает по фидеру $RFA\ 7/8$ ” длиной 175 метров и потерями 1.96 дБ на антенную систему $BLR-2DBA \times 8$ с максимальной мощностью 10 кВт, расположенную на высоте 148 метров. В случае

радиостанции “Новая волна” передатчик вещает на частоте 102.9 МГц и мощностью 0.1 кВт. Далее сигнал поступает по фидеру *RFA 7/8* длиной 180 метров и потерями 2.016 дБ на антенную систему *BLR-2DBAx8* с максимальной мощностью 6 кВт, расположенную на высоте 150 метров.

Для радиостанций “Радио Апрель” и “Радио День” схема подачи сигнала также одинакова. Сигнал поступает на объект от вещателя сразу на УКВ ЧМ передатчик. У радиостанции “Радио Апрель” передатчик вещает с частотой 102.4 МГц и мощностью 1 кВт. После чего сигнал поступает по фидеру *RFA 1 5/8* длиной 240 метров и потерями 1.606 дБ на антенную систему *BLR-2DBAx8* с максимальной мощностью 2.5 кВт расположенную на высоте 194.125 метра. У радиостанции “Радио День” передатчик вещает с частотой 105.3 МГц и мощностью 0.5 кВт. После чего сигнал поступает по фидеру *RFA 7/8* длиной 148 метров и потерями 1.717 дБ на антенную систему *BLR-2DBAx8* с максимальной мощностью 2.5 кВт, расположенную на высоте 102 метра.

ТАБЛИЦА 1. Параметры имеющихся радиостанций

Название РС	Частота, МГц	Мощность передатчика, кВт	Мощность антенны, кВт	Высота подвеса антенны, м
Ретро ФМ	103,9	0.5	10	148
Новая волна	102,9	0.1	6	150
Радио России	106,5	4	10	133
Радио Апрель	102,4	1	2.5	194,125
Радио День	105,3	0.5	2.5	102

В таблице 1 представлены параметры всех радиостанций, вещающих с объекта. На рис. 1 представлена действующая схема подачи сигнала всех радиостанций, вещающих с объекта. В ходе изучения документации было выявлено, что радиостанция «Новая волна» является собственником всего оборудования, использующегося у этой радиостанции. Было направлено письмо собственнику оборудования с предложением оптимизировать вещание их РС, на что был получен отказ. В случае остальных четырёх РС всё оборудование принадлежит филиалу РТРС [6].

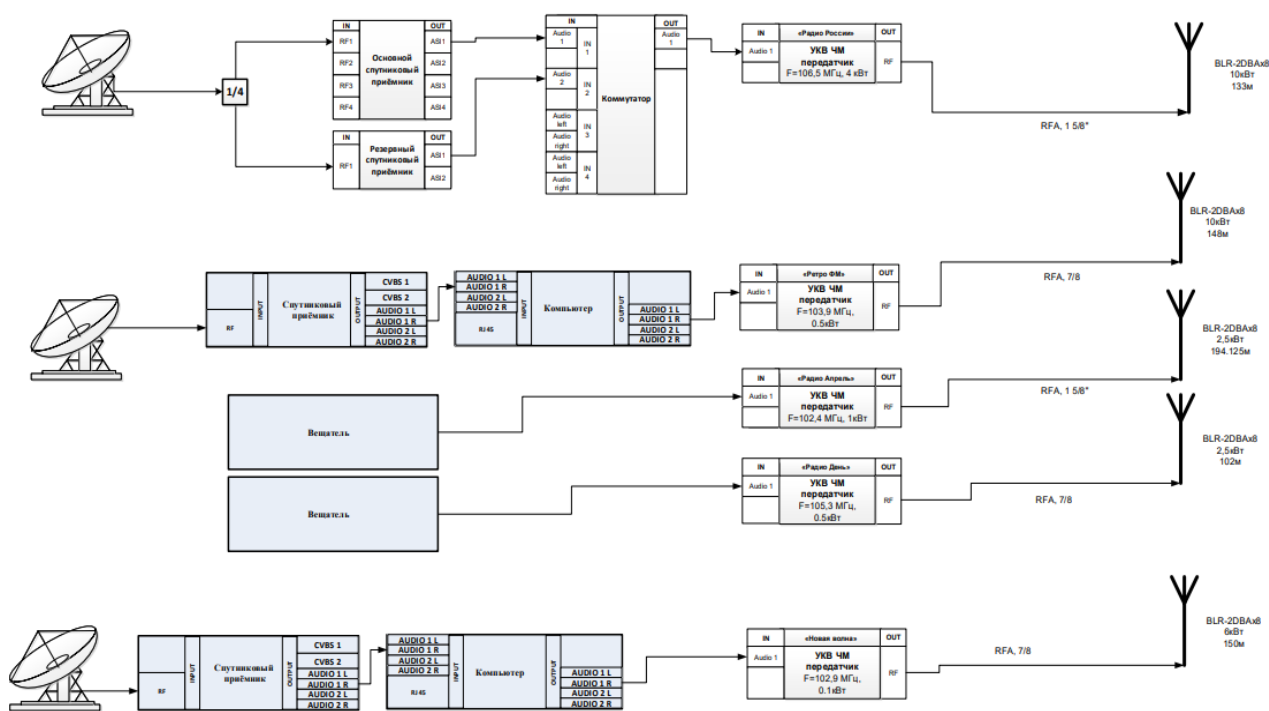


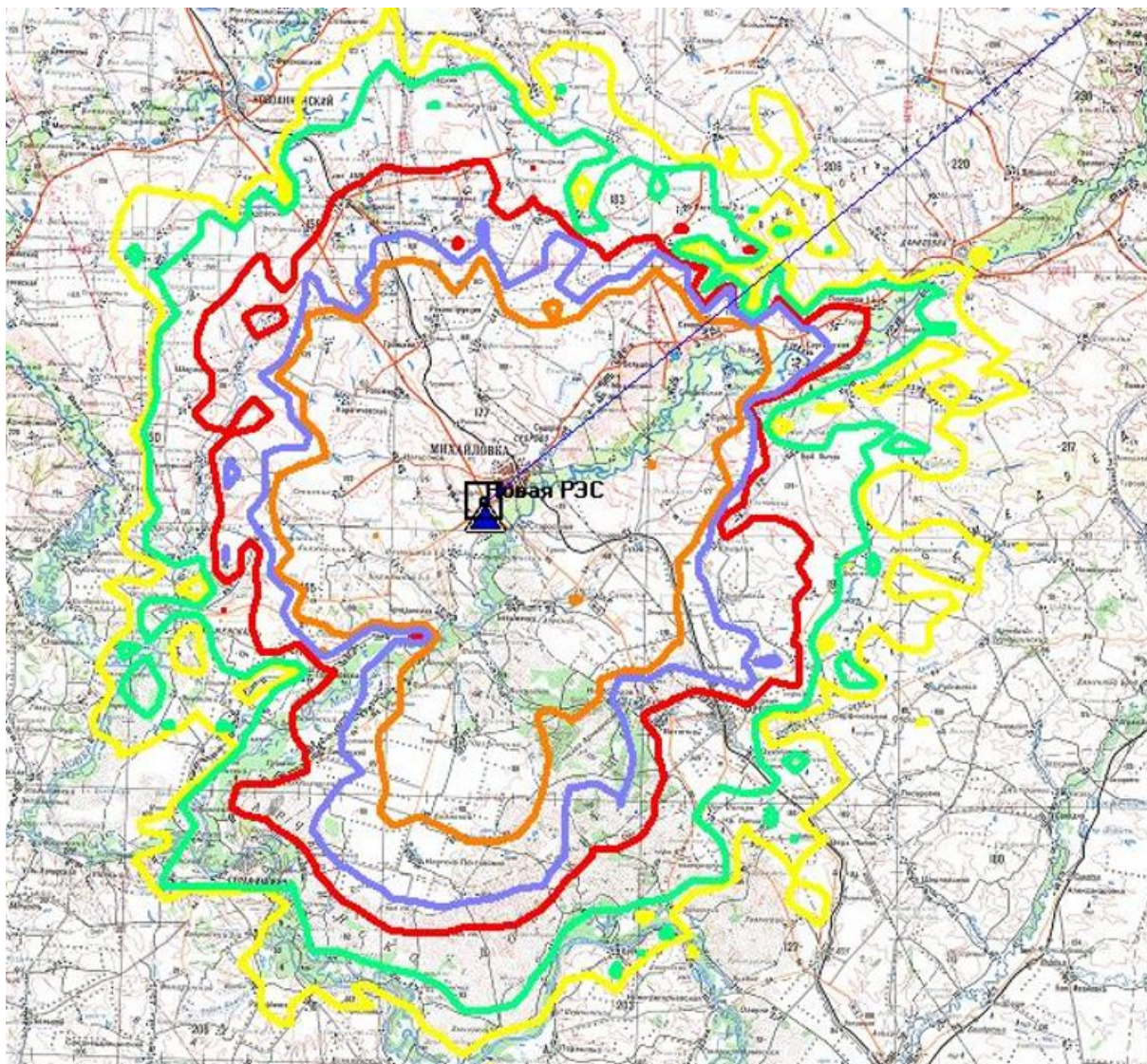
Рис. 1. Действующая схема подачи сигнала

Для расчёта был выбран пакет программ ПИАР. Данный пакет программ поставлялся централизованно и используется во всех филиалах РТРС. Проводимые в программе расчёты довольно точно совпадают с реальными натурными измерениями. Для расчётов в программе необходимо указать высоту антенны (м), мощность (Вт), азимут (град), вертикальный угол (град), потери в фидере (дБ), тип антенны, частоту (МГц) и географические координаты объекта.

В данной программе были рассчитаны зоны уверенного приёма сигналов для каждой радиостанции действующей схемы подачи сигнала. На рис. 2 представлены границы зон уверенного приёма всех радиостанций, вещающих на объекте.

ТАБЛИЦА 2. Результаты расчёта зон уверенного приёма в ПИАР

На данный момент						
Частота, МГц	Высота, м	Протяженность, м	Площадь, км ²	Ср.радиус, км	Население	Нас. пункты
103,9	148	514136	6443,26	45,287	103408	108
102,9	150	373046	3418,94	32,989	89826	56
106,5	133	1162663	11982,38	61,758	181846	204
102,4	194,125	861777	9346,46	54,544	170831	160
105,3	102	494768	4547,72	38,047	93164	70



- Радио России
- Ретро ФМ
- Новая волна
- Радио Апрель
- Радио День

Рис. 2. Границы зон уверенного приёма всех радиостанций

В таблице 2 приведены результаты расчёта программного пакета ПИАР для всех антенных систем, действующих на данный момент на объекте. На основе данных из этой таблицы в будущем необходимо будет оптимизировать работу средств радиовещания на данном объекте, так как нецелесообразно вещать всем радиостанциям со своих отдельных антенн.

Таким образом в ходе исследования средств радиовещания на объекте были изучены РС, работающие на объекте. В соответствии с этим были произведены расчёты зон уверенного приёма всех радиостанций. В дальнейшем необходимо

разработать схему подачи сигнала для этих радиостанций, которая позволит оптимизировать работу средств радиовещания на данном объекте.

Список используемых источников:

1. Закон “О связи” от 07.07.2003 № 126-ФЗ
2. Решение Государственной комиссии по радиочастотам при Министерстве информационных технологий и связи РФ от 15.12.2009 № 09-05-05 “Об утверждении Положения о порядке рассмотрения материалов, проведения экспертизы и принятия решения о выделении полос радиочастот для радиоэлектронных средств и высокочастотных устройств”
3. Постановление Правительства РФ от 12.10.2004 № 539 “О порядке регистрации радиоэлектронных средств и высокочастотных устройств”
4. Приказ Минкомсвязи РФ от 26.08.2014 № 258 “Об утверждении Требований к порядку ввода сетей электросвязи в эксплуатацию”
5. BLR-2DBA. — Текст: электронный // НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ “КАБЕЛЬНЫЕ СЕТИ”: [сайт]. — URL: <http://kseti.spb.ru/catalog/aerial-feeder-equipment/fm-peredayushchie-antenny-blr-/39-blr-2dba.html> (дата обращения: 07.11.2022).
6. Бунчук В. Россия в радиоэфире. Контент-аналитическое исследование двух радиостанций (“Эхо Москвы”, “Радио России”). Москва, 2008.

Verbitsky A., Shvets M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Investigation of the operation of radio broadcasting facilities at the RTPS facility in the locality of Mikhailovka.

In the Mikhailovka workshop of the Volgograd RRTTC branch of the FSUE RTRN, the bearing capacity of the mast is running out. It is necessary to study the operation of radio broadcasting facilities to further optimize the space on the mast, which in the future will be occupied by the equipment of new radio stations and the equipment of cellular operators.

Key words: *radio station, signaling scheme, reliable reception area.*

УДК 534.83
ГРНТИ 29.37.33

ИССЛЕДОВАНИЕ МЕТОДОВ АКТИВНОГО ШУМОПОДАВЛЕНИЯ

М. Н. Григорьев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире количество источников шума растёт. Автомобили, промышленные предприятия, толпы людей и т.д. являются неотъемлемым атрибутом современной городской жизни. Для борьбы с данной проблемой люди используют наушники в сочетании с музыкой высокой громкости, но такой метод является небезопасным для здоровья слуха. Решением данной проблемы являются наушники с системой активного шумоподавления.

шумоподавление, шум, цифровая обработка сигнала, звук

Уровень шума является важным параметром при определении качества окружающей среды. Шум относится к числу факторов, которые могут вызывать дискомфорт, раздражение и приводить к головной боли и усталости. Более того, шумы с высоким уровнем могут вызвать потерю слуха [1].

В данной работе шумом считаются акустические колебания, излучаемые сторонними источниками. Шумы различаются по характеру спектра (широкополосный, тональный), частоте (низкочастотный, среднечастотный, высокочастотный), и временным характеристикам (стационарный и нестационарный).

В настоящее время системы шумоподавления активнее всего используются в наушниках, но могут быть использованы и в более сложных системах [2].

Системы шумоподавления делятся на активные и пассивные. В пассивных системах используются материалы, изолирующие ухо от внешних источников шума, в активных – электрические схемы, обрабатывающие шумовой сигнал.

Активные системы шумоподавления делятся на:

- Аналоговые

Звуковой шумовой сигнал проходит через инвертирующее звено и складывается с общим звуковым сигналом. Данный метод прост и недорог. Недостатками данной системы является задержки при прохождении шумового сигнала через инвертирующее звено, что вызывает неполное удаление нежелательного шума. Примеры реализации данной системы представлены ниже на рис. 1 и рис. 2.

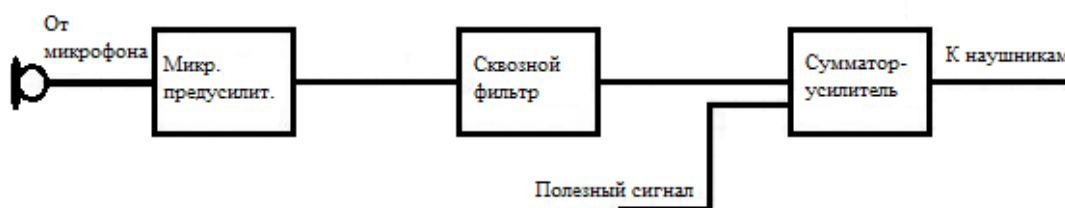


Рис. 1. Схема аналоговой системы шумоподавления

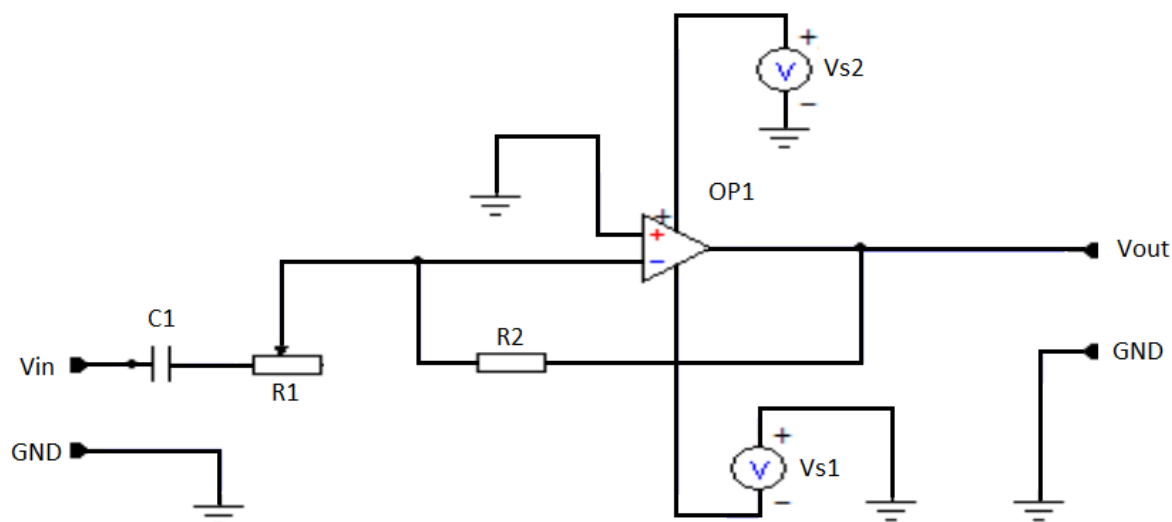


Рис. 2. Пример реализации электрической схемы аналогового шумоподавления

● Цифровые

Аудиосигналы преобразуются в последовательности битов и обрабатываются при помощи микроконтроллеров. Это позволяет получить большую свободу в выборе различных алгоритмов для оптимального шумоподавления, но требует высокой производительности вычислительных элементов для минимизации задержек.

Один из примеров такого алгоритма – метод спектрального вычитания. Он используется для подавления аддитивных стационарных шумов и состоит из 4 этапов:

1. Разложение сигнала с помощью кратковременного (оконного) преобразования Фурье (STFT)
2. Составление вычитаемого слепок шума (noise footprint). Слепок шума получается усреднением по времени амплитуд спектра, взятых из подготовленного участка шума, не содержащего полезного сигнала
3. "Вычитание" амплитудного спектра шума из амплитудного спектра сигнала
4. Обратное преобразование STFT - синтез результирующего сигнала [3].

● Гибридные

Данные системы включают в себя части из двух предыдущих. Аналоговая часть позволяет системе быть более устойчивой к изменениям внешних факторов, а цифровая – выполнять более совершенные алгоритмы.

Важно понимать, что в реальном применении алгоритмов шумоподавления можно рассчитывать лишь на приближенное воспроизведение шума в противофазе, так как инверсия фазы сложных сигналов должна учитывать

задержки на прохождение шумов и рассчитывать сигнал защиты от шума так, чтобы он поступал к пользователю одновременно с шумом. Это приводит к неполному устранению шума, а лишь к его ослаблению.

Также, для стационарных систем сложность представляет геометрия помещения, в котором подавляется посторонний шум и которым определяется характер его распространения. Решением данной проблемы является разработка и настройка системы для конкретной данной области, но для массового применения системы активного шумоподавления должны быть куда более универсальны и меньше зависеть от помещения. Кроме того, на практике шумоподавление может, наоборот, усилить сторонние шумы в некоторых областях помещения, даже сравнительно простой формы [4].

Стоит отметить, что аналоговая система шумоподавления без дополнительных технических решений имеет ряд недостатков. Наиболее значимыми из них являются узкий диапазон, в котором происходит шумоподавление, и сравнительно высокое энергопотребление предусилителя и инвертирующего элемента, что приводит к сниженной автономности переносных устройств.

Цифровые системы активного шумоподавления потребляют меньшее количество энергии для своей работы, могут работать в более широком диапазоне и способны использовать гораздо больше алгоритмов для максимальной эффективности. Так, например, с помощью микропроцессоров возможна реализация трёх типов шумоподавления: с обратной связью, без обратной связи и гибридная. Система без обратной связи имеет один внешний микрофон, который отслеживает шум. О данном методе и его недостатках было упомянуто ранее. Система с обратной связью имеет один внутренний микрофон, который отслеживает суммарный аудиосигнал. С помощью данного алгоритма, происходит сравнение всего поступающего звука с источником аудио, что позволяет выявить и устранить шум. Недостатками данной системы является сложность разработки устойчивой системы без самовозбуждения и возможное искажение музыкального полезного сигнала. Гибридное решение использует внешний микрофон для отслеживания шума и внутренний микрофон контроля суммарного аудиосигнала. Данное решение усложняет конструкцию, но является наиболее эффективным.

Системы активного шумоподавления подверглись значительному усовершенствованию за последние десятилетия. В современном мире их широко применяют в разных областях: от промышленности до аудиоаппаратуры.

Список используемых источников:

1. ГОСТ 12.1.003-2014 Система стандартов безопасности труда (ССБТ). Шум. Общие требования безопасности. – 2 с.
2. Википедия [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/Шум> (дата обращения 01.11.2022).
3. Алексей Лукин. Введение в цифровую обработку сигналов (Математические основы). Методическое пособие, 2002, 44 с.
4. Ходунова О.А. Адаптивное устройство активного шумоподавления // Материалы IV Всерос. молодеж. науч.-техн. конф. с междунар. участием «Россия молодая: передовые

технологии – в промышленность!» (Омск, 15-17 нояб. 2011 г.). В 2-х кн. Кн. 2. Омск : ОмГТУ, 2011. С. 134-137.

Grigorev M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Active Noise Cancellation.

In the modern world, the number of noise sources is increasing. Cars, industrial enterprises, crowds of people are an essential part of modern urban life. To deal with this problem, people use headphones in combination with music at high volume, but this is unsafe for hearing. The solution to this problem is headphones with an active noise reduction system.

Key words: noise reduction, noise, digital signal processing, sound.

УДК 654.1
ГРНТИ 49.43.01

НОРМИРОВАНИЕ ЗВУКОВЫХ СИГНАЛОВ В ТЕЛЕРАДИОВЕЩАНИИ

Д. Н. Дудевич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлена разработка физической модели автоматического регулятора уровня громкости, пригодной для решения проблемы перепадов уровня звука в телерадиовещании. Научная новизна исследования заключается в разработке собственной схемы устройства для автоматической регулировки уровня громкости. Представлена схема разработанной модели и принцип ее работы.

звуковой сигнал, уровень громкости, перепады громкости, нормализация громкости, автоматический регулятор уровня (APU)

Телерадиовещание является самым распространенным средством массовой информации для населения. В нынешнее время происходит слияние средств вещания, телекоммуникаций и компьютерных технологий в едином информационном пространстве [1].

Изображение на экране телевизора передает весьма большой объем информации, но общее понимание о телевизионной программе зависит не только от качества увиденного изображения, но и от качества звукового сопровождения передачи. Даже технически совершенное изображение может не заинтересовать зрителя, если оно будет сопровождаться некомфортным для восприятия звуком.

Одной из главных проблем телевизионного вещания являются неожиданные «скачки» звука в транслируемом контенте, особенно ярко они проявляются в переходе контента на рекламные ролики. В нашей стране существует федеральный закон от 13.03.2006 N 38-ФЗ (ред. от 14.07.2022) "О рекламе", в котором говорится, что «при трансляции рекламы уровень громкости ее звука, а также уровень громкости звука сообщения о последующей трансляции рекламы не должен превышать средний уровень громкости звука прерываемой рекламой телепрограммы или телепередачи» [2]. Уровень громкости – это субъективное ощущение звукового давления, которое позволяет располагать все звуки по шкале от тихих до громких. Громкость звука главным образом зависит от уровня сигнала и распределения энергии звуковых колебаний по шкале частот, выражается в единицах громкости LUFS (LUFS эквивалентно LKFS, используемой в ITU-R BS. 1770). Единица LKFS эквивалентна децибелу, поскольку увеличение уровня сигнала на 1 дБ приведет к увеличению показателя громкости на 1 LKFS [3].

Обеспечение постоянного уровня громкости и предотвращения возникновения резких перепадов громкости ложится на плечи вещателей, но бывают и случаи, когда этого недостаточно и звук, подвергаясь помехам и искажениям в тракте, на выходе все равно получается неравномерным.

Решением данной проблемы может стать автоматическая регулировка уровня на стороне слушателя, пример реализуемой схемы представлен на рис. 1.

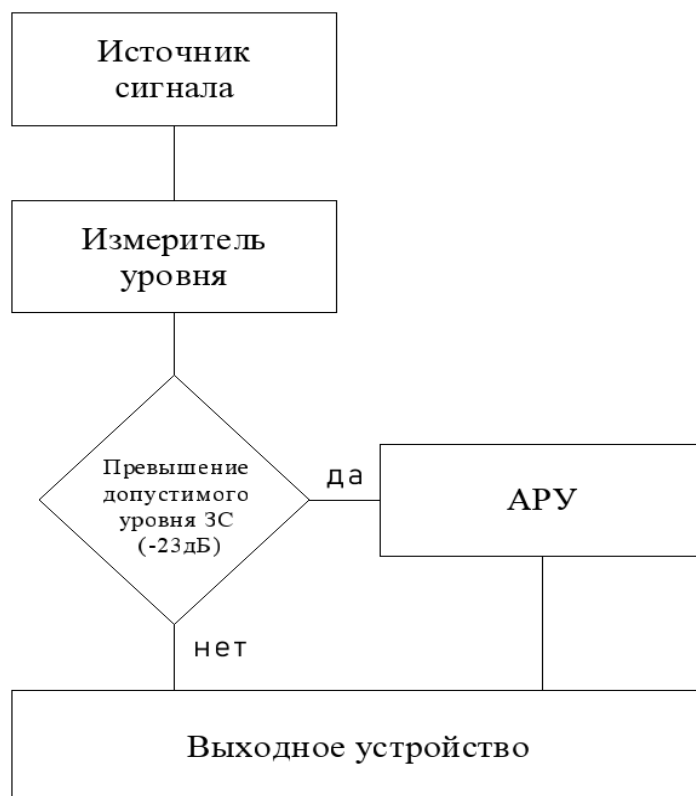


Рис. 1. Алгоритм работы модели

На входе системы располагается блок измерителя уровня ЗС. Он состоит из буфера, накапливающего отсчёты ЗС на промежутке 50 мс, среднеквадратического значения ЗС (RMS ЗС) и среднее значения уровня ЗС на интервале 1,5 сек. Формулы расчёта среднеквадратического уровня ЗС представлены ниже.

Для начала рассчитывается среднеквадратическое значение уровня сигнала на промежутке 50 мс (формула 1):

$$X(n) = 20 \log (u) = \frac{\sqrt{a_1^2 + a_2^2 + \dots + a_n^2}}{u_0}, \quad (1)$$

где $X(n)$ – среднеквадратическое значение уровня ЗС в дБ, a_n – амплитуда значения отсчёта ЗС, n – номер отсчёта ЗС.

Затем эти значения усредняются на промежутке 1,5 с по формуле 2:

$$N_{RMS} = \frac{x(1) + x(2) + \dots + x(n)}{n}, \quad (2)$$

где N_{RMS} – усреднённое на заданном промежутке среднеквадратическое значение уровня ЗС в дБ, $X(n)$ – среднеквадратическое значение уровня ЗС, n – номер усредняемого среднеквадратического значения уровня ЗС.

Полученный уровень сигнала сравнивается с пороговым, который был принят равным минус 23,5 дБ LUFS [4]. Когда этот порог превышает, на выход подаётся сигнал, компенсированный автоматическим регулятором уровня (АРУ). Время задержки сигнала учитывается при его прохождении через тракт, и учитывается в буфере сразу после источника сигнала.

На сегодняшний день разработан прототип устройства, для подключения к компьютеру, представляющее из себя плату Arduino Nano [5], размещённую в корпус, напечатанный на 3D принтере (рис. 2а), который работает в совокупности с программным кодом на языках Arduino и Python.

Корпус представляет собой пластиковую болванку, внутри которой располагается отладочная плата Arduino Nano, подключенная к пину с АЦП. На внешней стороне корпуса разъёмы: mini jack 3,5мм и type-C. Физический вариант устройства представлен на рис. 2б. Подключение устройства возможным образом: со стороны компьютера задействуется COM-порт (Usb-порт) и аудиовыход, ответными портами на устройстве служат разъем type-C и mini jack 3,5мм соответственно; в качестве выходного устройства может служить любая аппаратура для воспроизведения аудио с mini jack 3,5мм.

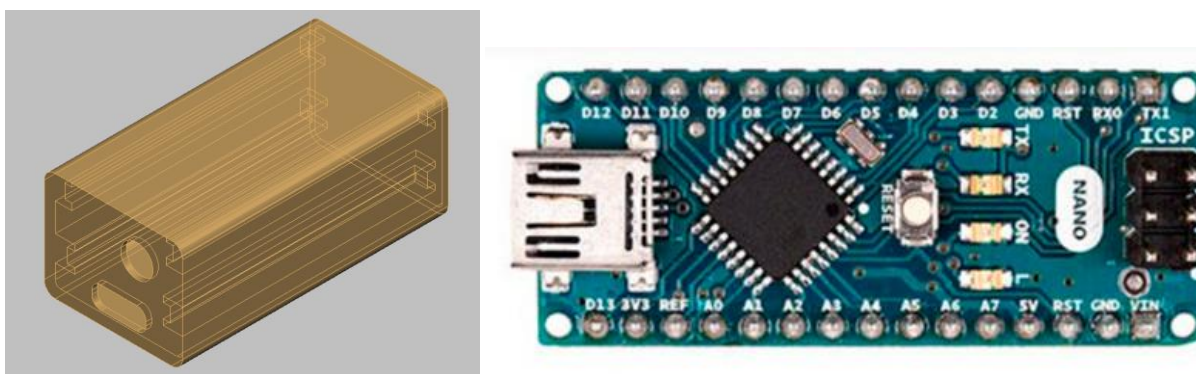


Рис. 2а. Модель корпуса и используемая плата



Рис. 2б. Реализованное АРУ

Со стороны пользователя, на компьютере реализуется программный код для отображения интерфейса управления устройством (рис. 3). На всплывающем окне расположены регуляторы, выпадающий список и соответствующие кнопки для активации заданных параметров.

«Максимальная регулируемая громкость» — уровень, до которого АРУ сможет менять свое значение (по умолчанию равна максимуму, т.е. 100%).

«Минимальная регулируемая громкость» — уровень, до которого АРУ сможет менять свое значение (ноль является критическим значением, т.к. в некоторых моментах регулятор может полностью заглушить звук).

«Коэффициент k для экспоненциального фильтра» — весовая функция (чем ближе коэффициент к нулю, тем плавнее происходит регулирование, но уменьшается быстродействие).

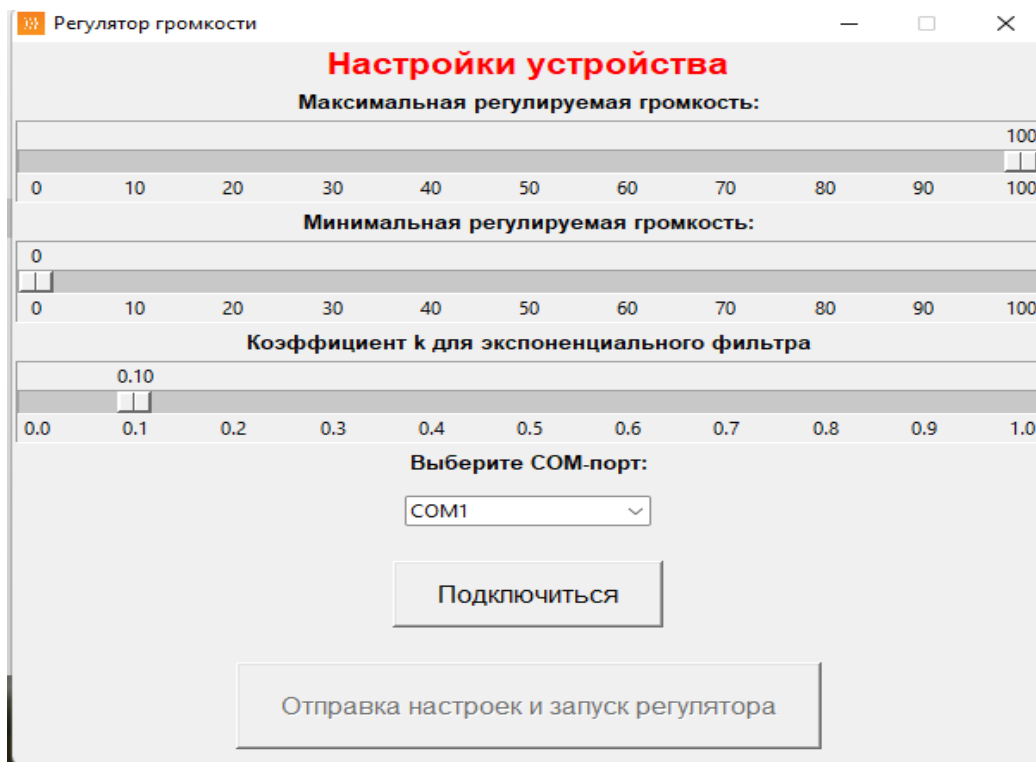


Рис. 3. Интерфейс управления

После успешной активации работы программы можно провести два независимых исследования разработанной модели.

Первое исследование представляет с собой изучение и анализ графиков, выводимых программой (рис. 4). На графике по оси абсцисс откладываются отчеты времени, по оси ординат — уровень громкости, при условии, что максимумом транслируемого аудио контента является 100%. Наблюдаются следующие кривые: максимальный уровень (допустимый уровень громкости, который изначально был задан пользователем в пределах от 0 до 100); уровень громкости исходного сигнала; уровень сигнала после прохождения экспоненциального фильтра; изменение максимального уровня громкости (данный показатель отвечает за итоговый уровень сигнала на выходе, т.е. при возникновении громких периодов максимальный уровень сигнала будет уменьшаться, тем самым транслируя на выход меньшую громкость).



Рис. 4. Работа устройства в графическом виде

Второе исследование нацелено на изучение эффективности работоспособности разработанного устройства путем субъективной экспертизы. Испытательной группе будет предложено прослушать аудиодорожки с резкими «скачками» звука (отрывок видеофильма с громким взрывом, музыкальный отрывок симфонического оркестра и отрывок с человеческой речью, в которой присутствуют резкие перепады громкости) и без них (аудио дорожки сглаживаются при помощи разработанного устройства). После прослушивания шести отрывков участникам следует оценить восприятие контента по различным параметрам.

Устройство и программный код находится в стадии доработки, на данный момент осуществляется работа над увеличением быстродействия.

Конечной целью является внедрение устройства в систему воспроизведения аудиовизуального контента.

Список используемых источников:

1. Карякин В. Л. Цифровое телевидение : учебное пособие. М. : СОЛОН-ПРЕСС, 2012. 448 с.
2. Федеральный закон от 13.03.2006 N 38-ФЗ (ред. от 14.07.2022) "О рекламе" (с изм. и доп., вступ. в силу с 13.10.2022). Статья 14. 2006г.
3. Рекомендация МСЭ-R BS.1770-4 (10/2015) – 24 с.
4. Приказ Минкомсвязи России «Об утверждении Рекомендаций в области нормирования звуковых сигналов в телерадиовещании» – Май 2015 – 31с.
5. Описание платы Arduino Nano: [Электронный ресурс] // [arduino-nano.ru](http://arduino-nano.ru/#desc) М., 2014-2018. URL: <http://arduino-nano.ru/#desc>. (Дата обращения 10.11.2022).

Dudevich D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Rationing of audio signals in broadcasting.

The article presents the development of a physical model of an automatic volume control suitable for solving the problem of sound level fluctuations in broadcasting. The scientific novelty of the research lies in the development of its own device circuit for automatic volume control. The scheme of the developed model and the principle of its operation are presented.

Key words: sound signal, volume level, volume drops, volume normalization, automatic level control (AGC).

УДК 654.739
ГРНТИ 49.33.29

ПРОЦЕСС РАБОТЫ СОВРЕМЕННОГО ТЕЛЕВИДЕНИЯ: ОСОБЕННОСТИ РАЗВИТИЯ СИСТЕМ ГИБРИДНОГО ВЕЩАНИЯ

А. П. Молчанов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В мире ранее принятый подход к телевидению и радио как к исключительно линейному вещанию, ограниченному определенными техническими способами (наземное эфирное вещание, кабельное вещание, спутниковое вещание), сменяется подходом к регулированию совокупности аудиовизуальных медиасервисов. Переход к новым моделям передачи данных обусловлен изменением структуры потребления аудио и видео контента и развитием таких технологий телерадиовещания, как IPTV и Интернет-вещание, которые позволяют реализовывать новую модель потребления. И здесь необходимо отталкиваться от того, что даже несмотря на появление новых видов СМИ, сегодня именно телевидение является одним из самых популярных средств доставки информации. Согласно стратегии развития телерадиовещания на территории Российской Федерации на 2020 – 2025 годы одним из направлений развития является обеспечение роста качества изображения и звука внедрением телевидения высокой четкости. В их числе и гибридное широкоэмитательное широкополосное телевидение, которое и даст телерадиовещанию новую жизнь.

вещание, интернет, гибридное телевидение

Hybrid Broadcast Broadband Television, HbbTV или гибридное широкоэмитательное ТВ – цифровое телевидение с поддержкой системы «Интернет», международный стандарт, который позволяет телезрителю получать интерактивные сервисы на экране Smart TV поверх исходного телевизионного сигнала [1]. Для HbbTV существует стандарт, разработанный и одобренный Европейским институтом стандартов телекоммуникаций – (ETSI) TS 102 796 V1.6.1 (2021-04). В процессе работы есть возможность пользователям принимать участие в том, что происходит на экране. Здесь можно привести пример и обратить внимание на то, что можно принимать участие в голосованиях, опросах и даже в самой прямой эфирной трансляции. Например, если смотреть футбольный матч, то с помощью HbbTV можно получить данные об игроках, статистику их активности на поле, посмотреть повтор эпизодов игры, а также выбирать самим удобные камеры для обзора трансляции. Данная опция уже доступна в России при трансляции спортивных событий [1]. Тест данной системы также запланирован и на концертных мероприятиях.

Главные особенности HbbTV заключаются в следующем:

- Интерактивная информация в телевизоре;
- Возможность заказа товаров во время просмотра рекламы;
- Просмотр повтора понравившихся телепередач;
- Выбор ракурса просмотра;
- Получение дополнительной информации о ведущим [2].

Вообще самое внедрение интерактивного телевидения пошло от технологии ОТТ (Over The Top) – в переводе означает «поверх остального сигнала», когда слушатель или зритель может сам может принимать участие или изменить ход прямой трансляции программы. ОТТ-сервисы сейчас фактически не отличаются от IPTV, но имеют преимущества, так как доступны любому пользователю интернета (в IPTV контент распределяется только пользователям в сети ПД одного оператора связи, минуя интернет, и чтобы гарантировать качество, в IPTV использует протоколы восстановления потерянных IP-пакетов). К недостаткам ОТТ-сервисов можно отнести задержку, что, впрочем, несущественно для видео [3].

Гибридное широкоэмитательное широкополосное телевидение начали прорабатываться еще в 2009 году за рубежом после появления телевизоров с возможностью подключения к интернету. Для того, чтобы функции гибридного ТВ начали работать дома необходимы:

- Цифровой тюнер;
- Стабильное подключение к Интернету (для работы и интерактивности).
- Поддержка HbbTV самим телевизором (или купить специальную приставку) [1].

Технология HbbTV также может быть реализуема в рамках развития стандарта DVB-I. Одна из основных задач нового стандарта — позволить вещателям уйти от системы приложений, которые им сейчас приходится использовать в интернет-среде для доставки услуг потребителям. Одна из задач DVB-I — регламентировать требования к приемнику, который среди прочего позволит формировать единый список доступных услуг. Однако существует отличия между HbbTV и DVB-I. Гибридное телевидение ориентировано на предоставление гибридных услуг, в которых линейное ТВ передается по вещательному каналу, а нелинейные сервисы и интерактивные приложения — по IP-сети [4]. HbbTV не используется в отрыве от вещательной сети, и в стандарте много внимания отводится синхронизации услуг, передаваемых по вещательному и IP-каналам.

В России данную систему начали тестировать и применять с 2018 года. Из российских каналов в 2022 году пользоваться функцией HbbTV можно на Первом канале, телеканалах «Матч ТВ», «НТВ», «СТС», «Домашний» «ТВ-3» и «ТНТ». О том, как распространяется сигнал на территории страны представлено на рис. 1.

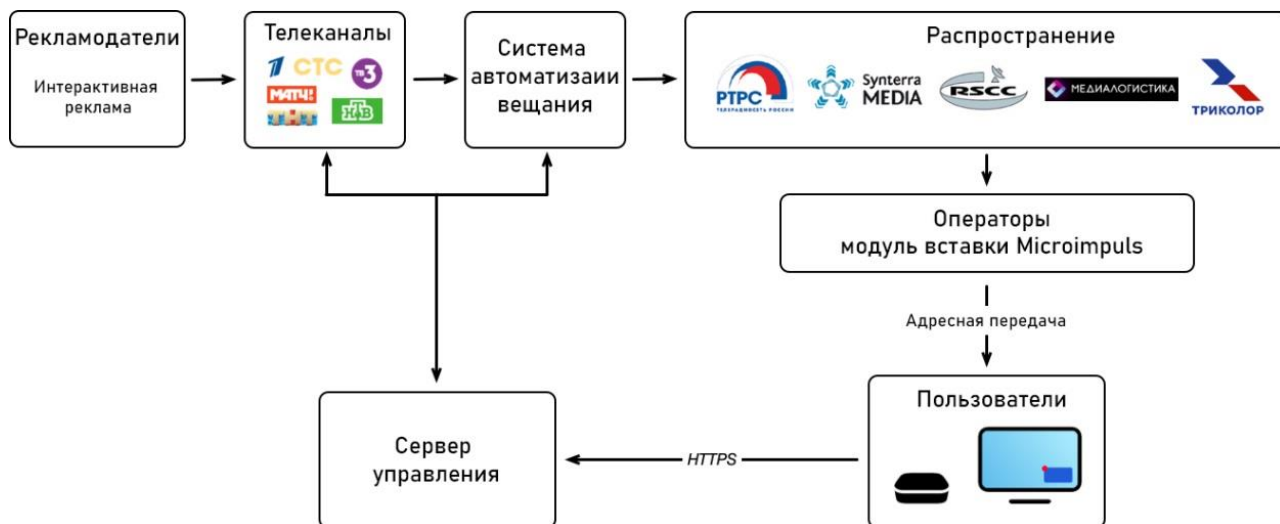


Рис. 1. Распространение и работа гибридного телевидения на территории России

Согласно концепции развития телерадиовещания на 2020 – 2025 года, для более широкого внедрения технологии HbbTV на территории России необходимо решить несколько важных задач [5]:

- обязательная продажа на территории Российской Федерации телевизоров и приставок с поддержкой указанного функционала и активация устройств HbbTV производителями в настройках «по умолчанию»;

- создание организации для координации развития технологии HbbTV, поскольку для ускорения развития HbbTV телевещателям важно начать взаимодействие по стандартизации и продвижению. Кроме того, должна быть определена единая организация, осуществляющая функции оператора технологии HbbTV, предоставляющая соответствующие услуги всем вещателям;

- повышение информированности телезрителей о наличии и возможностях интерактивного телевидения;

- обеспечение единообразного пользовательского опыта, в том числе единообразных вариантов организации подключения к HbbTV;

- распространение принципа неизменности телеканалов первого и второго мультиплекса при их трансляции на любую дополнительную информацию, включаемую вещателем в предназначенный для распространения телевизионный сигнал. Поскольку технология HbbTV позволяет распространять совместно с телеканалом дополнительную информацию, определенную вещателем, повышающую потребительскую ценность доставляемого телезрителю видеоконтента, на операторов связи должно возлагаться обязательство по обеспечению неизменности не только телеканала как совокупности телепрограмм при его трансляции, но и любой иной информации, сопровождающей трансляцию телеканала. Возможность предоставления интерактивных сервисов позволит замедлить отток зрителей линейного телевизионного вещания, а также создаст условия для предоставления дополнительных платных услуг и будет способствовать росту доходов телевещателей [5].

HbbTV объединило в себе функции интернета и телевидения одновременно и здесь существуют новые задумки и планы по работе над технической составляющей всего телевидения в целом, так как работа гибридного телевидения и современно, и технологично. А также может принести современным телеканалам еще больше популярности, что сегодня важно для российских вещателей.

Список используемых источников:

1. Зачем рекламодателям и телеканалам HbbTV: возможности и кейсы. Российский опыт. Какие перспективы [Электронный ресурс]. URL: <https://adindex.ru/publication/opinion/internet/2018/10/8/174778.phtml> (дата обращения: 07.11.2022)
2. Кабакчи Д. Технология гибридного телевидения HbbTV в России уже 1,5 года: что изменилось за это время? [Электронный ресурс]. URL: <https://www.cableman.ru/blog/tekhnologiya-gibridnogo-televideniya-hbbtv-v-rossii-uzhe-15-goda-chto-izmenilos-za-eto-vremya> (дата обращения: 07.11.2022)
3. Михайлов Н. OTT TV. Матчасть [Электронный ресурс]. URL: <https://www.cableman.ru/article/ott-tv-matchast> (дата обращения: 10.11.2022)
4. Бителева А. Стандарт DVB-I [Электронный ресурс]. URL: <https://telesputnik.ru/materials/tsifrovoe-televidenie/article/standart-dvb-i>
5. Концепция развития телерадиовещания в Российской Федерации на 2020 – 2025 годы : офиц. текст. М. : Телеспутник, 2021. 69 с.

Molchanov A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

The process of operation of modern Hybrid Broadcast Broadband Television. Television and radio were treated as narrow-line broadcasting, limited use of technical means (terrestrial broadcasting, cable broadcasting, satellite broadcasting), the approach to regulating audiovisual media services is changing. The transition to a new data transmission depends on the structure of audio and video consumption and, potentially, broadcasting technologies such as IPTV and Internet broadcasting, which allow a new consumption model to be realized. And here it is necessary to build on the fact that even the emergence of new types of media today has to be specially looked at from the most popular means of information delivery. According to the development of the television broadcasting strategy on the territory of the Russian Federation for 2020-2025, the provision of high image and sound quality is ensured by high definition. Including hybrid broadcast broadband television, which will give broadcasting a new life.

Key words: broadcasting, internet, hybrid broadcast broadband television.

УДК 654.172
ГРНТИ 49.40.49

СТАБИЛИЗАЦИЯ ВИДЕО

Е. А. Морозова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Получение качественного видео с помощью ручной камеры — это сложная задача. Нежелательные движения наших рук, как правило, размывают изображение и создают рывки в записанном видео. Эта проблема усугубляется при использовании объектива переменного фокусного расстояния или цифрового изменения фокусного расстояния. Для решения этой проблемы было разработано множество методов стабилизации видео. Оптические подходы измеряют дрожание камеры и контролируют дрожание, воздействующее на объектив или датчик CCD/ CMOS. Методы цифровой стабилизации видео используют только информацию, полученную из изображений, и не требуют дополнительных аппаратных средств.

стабилизация видео, цифровая стабилизация видео, оптическая стабилизация видео, оценка движения, искажение изображения

В последнее десятилетие мультимедийные устройства (КПК, мобильные телефоны и т. д.) получили широкое распространение. Более того, увеличение их вычислительной производительности в сочетании с более высокой емкостью памяти позволяет им обрабатывать большие объемы данных. Эти устройства, как правило, маленькие и тонкие, обычно имеют возможность захвата видео. Однако создание стабильного видео с помощью этих устройств является очень сложной задачей, особенно при использовании зум-объектива или цифрового зума. Из-за дрожания рук пользователя записываемые видео страдают раздражающими искажениями. Такая же проблема возникает при наличии камер, размещенных на мобильных опорах (автомобиль, самолет) или стационарных камер, работающих на открытом воздухе. Атмосферные условия (например, ветер) и вибрации, создаваемые проезжающими транспортными средствами, делают записанное видео нестабильным.

Стабилизация видео позволяет снимать видеофрагменты без рывков, устраняя нежелательные движения камеры. Затем качество видео улучшается, и алгоритмы более высокого уровня, присутствующие в устройстве (сегментация, отслеживание, распознавание), также могут работать должным образом. Более того, из стабилизированного видео можно получить более высокое сжатие битрейта по сравнению с нестабильным.

Разработано множество подходов к стабилизации. Некоторые методы, использующие механические или электронные инструменты, измеряют дрожание камеры, а затем контролируют дрожание, воздействующее на объектив (OIS – оптическая стабилизация изображения) или на датчик CCD/ CMOS. В этих подходах оба шага применяются до получения изображения, что позволяет избежать каких-либо вычислений после обработки и деформации изображения со стоимостью некоторых дополнительных механических или

оптических устройств. OIS не требует вычислительной сложности (все шаги выполняются в объективе перед съемкой), но требует дорогих оптических систем и достаточного пространства вокруг объектива камеры, что затрудняет интеграцию в очень маленькие и тонкие системы, такие как телефоны для обработки изображений.

С другой стороны, методы цифровой стабилизации видео используют только информацию, полученную из анализа видео для оценки физического движения камеры без каких-либо дополнительных механических устройств, но с некоторыми дополнительными вычислительными затратами и риском деформации изображения. Однако, эти подходы могут быть легко реализованы как в системах реального времени, так и в системах постобработки.

Алгоритмы стабилизации цифрового видео в целом состоят из трех этапов (рис. 1): оценка движения, обнаружение нежелательного движения и искажение изображения.

Первый этап посвящен нахождению параметров относительно преобразования, произошедшего между соседними кадрами. Трансляционная, подобие и аффинная являются наиболее распространенными моделями движения.

Второй шаг отличает преднамеренное движение (например, панорамирование) от нежелательного движения (дрожания). Обычно в этом процессе учитываются соображения плавности движения (джиттер – это высокочастотный сигнал). Последний шаг состоит из реконструкции стабилизованного изображения посредством надлежащего деформирования. Для этого захваченные последовательности должны быть больше, чем итоговое видео.

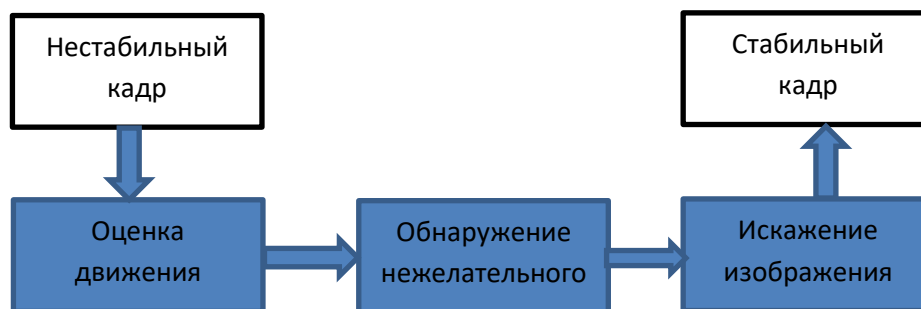


Рис. 1. Алгоритм стабилизации видео

Проблема оценки движения/регистрации изображения широко исследовалась и было предложено множество решений. Существующие подходы можно разделить на две категории: прямые методы и методы, основанные на признаках. Первые методы заключаются в восстановлении неизвестных параметров с помощью глобальных критериев минимизации на основе прямой информации об изображении. Некоторые допущения (например, постоянство яркости) обычно используется в качестве отправной точки. Другие же подходы, основанные на признаках, сначала определяют надежные признаки

на изображении, а затем оценивают параметры движения с учетом их соответствия.

В области стабилизации видео используется множество моделей межкадрового преобразования. Из-за ограничений реального времени встроенных устройств многие подходы рассматривают только двумерную трансляционную модель. Эта модель связывает точку (x_i, y_i) в кадре I_n с точкой (x_f, y_f) в кадре I_{n+1} следующим преобразованием:

$$\begin{aligned}x_f &= x_i + T_x \\y_f &= y_i + T_y\end{aligned}$$

где T_x и T_y смещения по осям x и y соответственно.

Точность этих подходов ограничена простотой модели, однако, они, как правило, дешевы, и их можно сделать надежными без особых усилий. Более того, шаг компенсации может быть реализован тривиально (это простая обрезка) без выполнения какой-либо интерполяции.

В последнее время, благодаря возрастающим вычислительным ресурсам встроенных устройств, стали рассматриваться более продвинутые модели. Двумерная модель подобия была принята как хороший компромисс между сложностью и вычислительными затратами:

$$\begin{aligned}x_f &= x_i \lambda \cos \theta - y_i \lambda \sin \theta + T_x \\y_f &= x_i \lambda \sin \theta + y_i \lambda \cos \theta + T_y\end{aligned}$$

где λ – параметр масштабирования, θ – угол поворота, T_x и T_y смещения по осям x и y соответственно.

Эта модель позволяет получить лучшие характеристики с точки зрения точности: учитывается дрожание вращения. Кроме того, она стабильна при наличии масштабирования или перемещения пользователя вперед (параметр масштаба отсутствует в простой 2D- трансляционной модели). Однако разработка быстрых и надежных подходов — нетривиальная задача. Компенсация движения должна выполняться посредством интерполяции.

Какая бы модель ни использовалась, алгоритмы оценки движения должны иметь возможность работать с критическими условиями. Очень часто в реальном видео возникает множество условий, которые ухудшают работу алгоритмов стабилизации видео, если ими не управлять должным образом. При наличии однородных областей (рис. 2(a)), периодических закономерностей (рис. 2(b)) и быстрых изменений освещенности, локальные оценки движения иногда дают неправильные векторы. Объекты в сцене (рис. 3) могут ввести в заблуждение при оценке глобального вектора движения, хотя их векторы рассчитаны правильно, они не описывают движения камеры. Наконец, масштабирование и движение вперед пользователя могут создать некоторые проблемы, если они не учитываются в модели движения (например, поступательная модель движения).

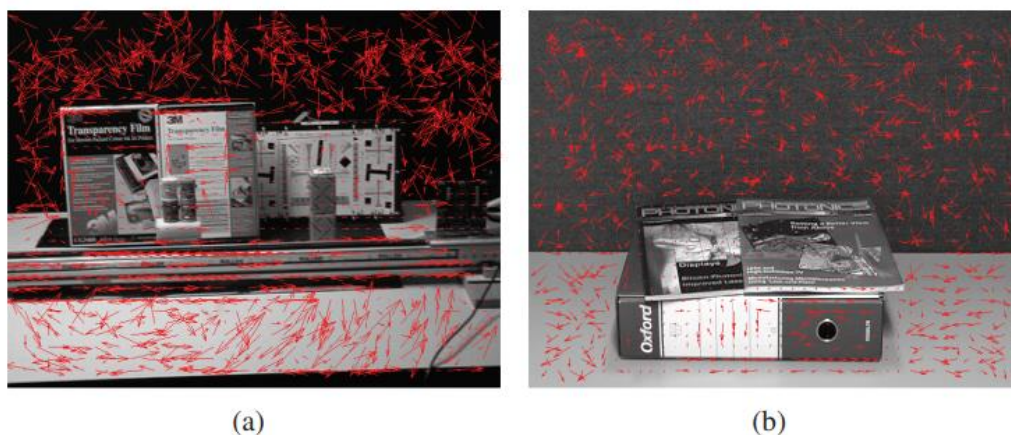


Рис 2. Локальная оценка движения иногда дает сбой: при наличии однородных областей (а), периодических закономерностей (б)

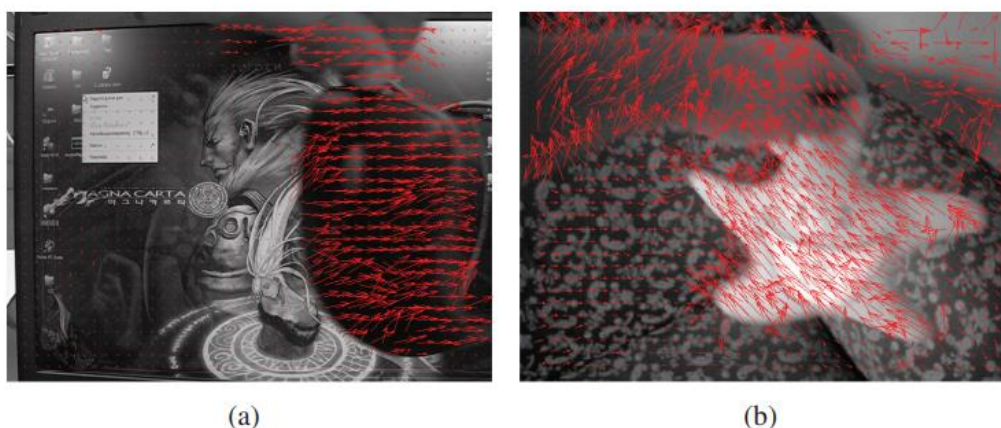


Рис 3. Векторы движения, соответствующие движущимся объектам, мыши (а) и мягкой звезде (б)

Оптическая стабилизация: дрожание измеряется с помощью гироскопа и акселерометра, и затем изменяется путь световых лучей в камере. Выполняются либо в объективе, либо на матрице. Каждая компания запатентовала свою технологию оптической стабилизации, отчего в области возникла некоторая путаница с названиями, например выделяют Vibration Reduction (VR), Image Stabilizer (IS), AntiShake (AS), IBIS, Optical SteadyShot (OSS), MegaOIS, PowerOIS, SteadyShot (SS), Super SteadyShot (SSS), SteadyShot INSIDE (SSI), Optical Stabilization (OS), Vibration Compensation (VC), Shake Reduction (SR), PureView, UltraPixel. Как видно, некоторые из названий совпадают с целым классом технологий. В таком виде, как класс, в дальнейшем их и следует понимать. Все эти технологии объединяет то, что изображение стабилизируется до того, как изображение с сенсора будет преобразовано в цифровые данные. Можно выделить:

- Стабилизирующий элемент объектива, подвижный ортогонально оптической оси, по команде с сенсоров отклоняется так, чтобы проекция изображения полностью компенсировала колебания.
- Сервоприводы, перемещают грани заполненной жидкостью призмы, расположенная на пути света, и, как следствие, изменяется положение

изображения на матрице[4]. (например, применялось в Canon XL1, Sony VX1000).

– Матрица смещается так, чтобы противодействовать движению камеры. Когда камера поворачивается, вызывая угловую ошибку, матрица смещается, чтобы поддерживать проекцию изображения на плоскости матрицы, также используются данные о фокусном расстоянии объектива (впервые применялось в Dimage A1 в 2003 г., технология называлась «Anti-Shake»). Преимущество заключается в возможности использовать различные объективы, в том числе без встроенной стабилизации

Такие способы стабилизации позволяют снимать видеоряды без рывков.

Список используемых источников:

1. Mercenaro L., Vernazza G., Regazzoni C., “Image stabilization algorithms for video-surveillance application,” in Proceedings of International Conference on Image Processing (ICIP-01), pp. 349–352, Thessaloniki (Greece), 2001.

2. S. Battiato and R. Lukac, Encyclopedia of Multimedia, ch. Video Stabilization Techniques, pp. 941–945. Springer-Verlag, October 2008.

3. Ялов А. Л. Распознавание движения со стационарной и поворотной камер видеонаблюдения // Процессы управления и устойчивость: Труды 44-й международной научной конференции аспирантов и студентов под ред. Н. В. Смирнова, Т. Е. Смирновой. СПб.: Издат. Дом С.-Петербур. гос. ун-та, 2013. С. 508–512.

Morozova E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Video stabilization.

To make a high-quality video with a hand-held camera is a very difficult task. The unwanted movements of our hands typically blur and introduce disturbing jerkiness in the recorded video. Moreover, this problem is amplified when a zoom lens or a digital zoom is used. To solve this problem many video stabilization techniques have been developed. Optical based approaches measure camera shake and control the jitter acting on lens or on the CCD/CMOS sensor. On the other hand digital video stabilization techniques make use only of information drawn from images and do not need any additional hardware tools.

Key words: *video stabilization, digital video stabilization, optical video stabilization, motion estimation, image warping.*

УДК 004.946
ГРНТИ 28.17.33

ТЕХНОЛОГИИ ИММЕРСИВНОЙ РЕАЛЬНОСТИ

Д. С. Сидоркина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящий момент технологии оказывают влияние на жизнь человека во всех областях, что дает способность каждому активно использовать новейшие технические тенденции. Сегодня, благодаря развитию иммерсивных технологий, воображение и материальность соединяются друг с другом, создавая тонкий мост между виртуальным и реальным миром. Наиболее известными представителями иммерсивной реальности являются VR (Virtual Reality) и AR (Augmented Reality). В данной статье рассматриваются иммерсивные технологии, представленные на современном рынке. Приводится краткое описание основных составляющих технологий: 360°, VR, AR, MR, XR.

иммерсивные технологии, 360°, VR, AR, MR, XR

Что такое иммерсивная реальность? Понятие иммерсивности происходит от англ. «immersion», означающем «глубокое погружение». Иммерсивность в ряде исследований понимается как создание эффекта «присутствия» за счет комплекса ощущений человека, находящегося в искусственно созданной среде [1,2]. Данные технологии являются эффективным инструментом, который усиливает реальность пользователя, накладывая цифровые изображения на реальное окружение человека.

Иммерсивные технологии, более известные как технологии расширенной реальности. В их список входят виртуальная реальность, дополненная реальность, смешанная реальность, расширенная реальность и технология 360° [3]. Они имитируют эффект, полного или частичного погружения в альтернативное пространство, тем самым изменяя взаимодействие с пользователем в совершенно разных областях и выводя его на новый уровень. Далее рассматриваются основные иммерсивные технологии.

Технология 360°

Это самая фундаментальная и, вероятно, самая известная иммерсивная технология. В наши дни контент в формате 360° можно увидеть практически везде в Интернете. Этот первоначальный формат дает создателям контента больше пространства для работы и предоставляет пользователям свободу выбора материала, смотря в любом направлении [4].

Виртуальная реальность (VR)

Полностью смоделированная реальность с применением современных технологий. Основной целью VR является развитие у потребителя восприимчивых ощущений, сопровождаемых в некоторых случаях зрением, осязанием, слухом, обонянием или даже вкусом, в отличие от AR и MR (рис. 1) [8]. Определение "виртуальный" – это приближенный, а реальность – это то, что воспринимает или чувствует пользователь. Таким образом, термин "виртуальная реальность" в основном означает "приближенную реальность". Виртуальная

реальность относится к созданию виртуального мира или проекции, которая создает реалистичное ощущение, не существующее в реальности. Это виртуальный опыт, который пользователь может наблюдать, слушать и взаимодействовать с ним, но при этом не может потрогать [5].

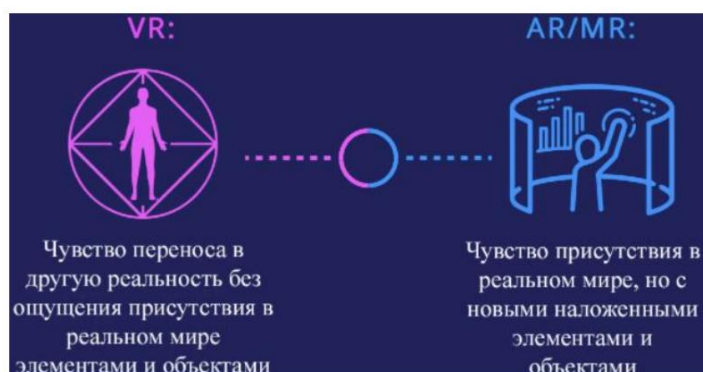


Рис. 1. Главное отличие VR от AR и MR

Виртуальная реальность (VR) – это смоделированное пространство, которое доступно с помощью иммерсивных устройств, таких как шлемы, перчатки и наушники (рис. 2). Тщательно проработанная локация в VR может полностью имитировать реальный мир с помощью звуков и пейзажей, создавая ощущение полного присутствия и погружения.



Рис. 2. Наиболее популярные VR-гарнитуры

Дополненная реальность (AR)

Это технология, которая сочетает в себе элементы виртуальной реальности и реального мира. AR наблюдается, когда определенный элемент, объект или устройство, присутствует в реальности, но на самом деле не существует в реальном мире. Вместо того чтобы перемещать пользователя в виртуальный мир, AR расширяет реальность с помощью виртуального сюжета (рис. 3). Новая виртуальная среда создается путем наложения запрограммированных виртуальных объектов на видеосигнал с камеры и становится интерактивной благодаря использованию специальных маркеров. В течение многих лет дополненная реальность используется в таких областях, как медицина, промышленность, реклама, армия и игровая индустрия [8].



Рис. 3. Особенности технологий AR, и VR/MR

Можно выделить три основные области, в которых может развиваться данная технология:

«Безмаркерная» технология AR – данная технология использует специальный алгоритм распознавания для размещения виртуальной "сетки" поверх ландшафта, снятого камерой. На этой сетке программный алгоритм находит особые опорные точки и использует их для определения точного места "привязки" виртуальной модели. Преимущество этой техники заключается в том, что маркером становится сам реальный объект, и нет необходимости создавать для реального объекта специальный визуальный идентификатор.

AR «технология на основе маркеров» – технология с использованием специальных маркеров или меток полезна тем, что они позволяют легко распознать точность и по ним можно более достоверно определить местоположение виртуальной модели. Эта технология более надежна, чем «безмаркерная», и работает практически безошибочно.

«Пространственная» технология – в дополнение к "безмаркерным" и "маркерным" технологиям существуют технологии дополненной реальности, которые основаны на пространственном позиционировании объектов. При этом используются данные GPS/ГЛОНАСС, гироскопа и компаса, встроенные в мобильный телефон. Положение виртуального объекта определяется его координатами в пространстве. Программа дополненной реальности активируется, когда координаты в программе совпадают с координатами пользователя [6].

Смешанная реальность (MR)

Это объединение или сочетание дополненной реальности и виртуальной реальности. MR – это сочетание физического и цифрового миров, которое позволяет взаимодействовать между людьми, компьютерами и окружающей средой. Реализация этих технологий стала возможной благодаря развитию систем компьютерного зрения, обработки графики, технологий отображения, систем ввода и вывода информации, а также облачных вычислений [9].

В 1994 году термин «Смешанная реальность» впервые появился в документе под названием «Таксономия визуальных дисплеев для смешанной реальности», опубликованном Полом Милграмом. Этот документ объяснил концепцию виртуального континуума и классификацию визуальных дисплеев.

Впоследствии смешанная реальность стала относиться не только к дисплеям, но и ко всему, что выполняет следующие функции:

- понимание рабочей среды: пространственное сопоставление и референция;
- понимание человека: отслеживание рук, взгляда и голосового ввода;
- позиционирование и местоположение в физическом и виртуальном пространстве;
- совместная работа с 3D-материалами в пространствах смешанной реальности [7].

Расширенная реальность (XR)

Это обобщающий термин для дополненной реальности (AR), виртуальной реальности (VR), смешанной реальности (MR) и всего, что между ними (рис. 4).

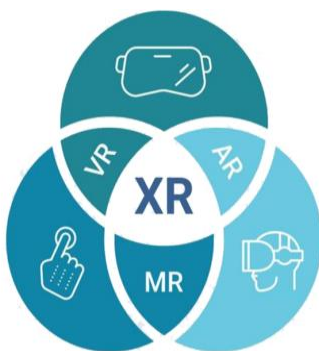


Рис. 4. Составляющие XR

Под аббревиатурой XR следует понимать, как набор технологий и решений, объединенных на основе ранее установленных определений виртуальной реальности и дополненной реальности. Это говорит о том, что данные технологии обладают способностью расширять границы физического пространственно-временного континуума, позволяя цифровым инструментам воздействовать на человеческое восприятие. В настоящее время XR служит средством переноса людей из их реального местоположения в искусственно созданный мир. Иммерсивные решения на основе VR/AR и различных вспомогательных технологий являются одними из наиболее перспективных направлений XR, практикуемых в настоящее время во многих отраслях [9].

Область применения иммерсивных технологий весьма обширна: начиная от индустрии цифровых развлечений и заканчивая здравоохранением и образованием. Практически везде можно найти способ применения данных технологий: в промышленности VR и AR позволяет контролировать качество процессов, в области розничной торговли данная технология позволяет виртуально продемонстрировать продукт.

Наличие такого разнообразия технологий показывает высокий интерес пользователей к данным продуктам, а также демонстрируют высокий потенциал развития этой области информационных технологий. Все это, безусловно, толкает как отдельных разработчиков, так и крупных игроков рынка усердно работать и развивать данную сферу.

Список используемых источников:

1. Корнилов Ю. В., Попов А. А. К вопросу о терминологии и классификации иммерсивных технологий в образовании // Проблемы современного педагогического образования. 2020. N 68. С.171-174.
2. Авербух Н. В. Психологические аспекты феномена присутствия в виртуальной среде // Вопросы психологии. 2010. С. 105 – 113.
3. Luis Muñoz-Saavedra, Lourdes Miró-Amarante and Manuel Domínguez-Morales / Augmented and Virtual Reality Evolution and Future Tendency. 2020.
4. Vijeta Kumawat. Evolution of Immersive Technology: Journey of Computational Reality. 2020.
5. Lawrence J. Rosenblum. Virtual and Augmented Reality: [Электронный ресурс] // Researchgate.net. 2020. URL: <https://clck.ru/32fys4> (Дата обращения 25.10.2022).
6. Соснило А. И. Применение технологий виртуальной реальности (VR) в менеджменте и образовании // Управленческое консультирование. 2021. N 6. С. 158-163.
7. Steven M. LaValle. VIRTUAL REALITY: [Электронный ресурс] // University of Illinois. Cambridge University Press. 2017. URL: <http://vr.cs.uiuc.edu> (Дата обращения 27.10.2022)
8. Gordon Wetzstein. A personalized VR/AR system that adapts to the user is crucial to deliver the best possible experience – 2016.
9. Смолин А. А., Жданов Д. Д., Потемин И.С. Системы виртуальной, дополненной и смешанной реальности. СПб. : Университет ИТМО, 2018. 60 с.

Sidorkina D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Immersive Reality Technologies.

At the moment, technology has an impact on human life in all areas, which gives everyone the ability to actively use the latest technical trends. Today, thanks to the development of immersive technologies, imagination and materiality connect with each other, creating a thin bridge between the virtual and real world. The most famous representatives of immersive reality are VR (Virtual Reality) and AR (Augmented Reality). This article discusses immersive technologies presented on the modern market. A brief description of the main components of the technology is given: 360°, VR, AR, MR, XR.

Key words: Immersive technologies, 360°, VR, AR, MR, XR.

УДК 621.397
ГРНТИ 81.83.20

РАЗВИТИЕ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ОБОРУДОВАНИЕМ ТЕЛЕРАДИОПЕРЕДАЮЩЕГО ЦЕНТРА

Я. Г. Сушко, С. Л. Федоров

Санкт-Петербургский государственный университет телекоммуникаций им проф. М. А. Бонч-Бруевича

Рассмотрены возможности системы дистанционного мониторинга СДК-5 от «НПП Триада-ТВ». Приведены мониторируемые основные параметры передающего и приемного оборудования. Представлена схема системы мониторинга цифровых передатчиков СДК-5. Указаны достоинства данной системы, а также представлены варианты оптимизации управления оборудованием передающего центра.

СДК-5, система мониторинга, VSAT, удаленный доступ

В настоящее время в Российской Федерации полностью организована система цифрового эфирного телерадиовещания. Для этого к концу 2019 г. было закончено строительство передающих объектов 1-го и 2-го мультиплексов. По данным ФГУП «Российская телевизионная радиовещательная сеть» охват эфирным цифровым вещанием составляет 98-99 % населения Российской Федерации. Для обеспечения населения стабильным цифровым телерадиосигналом осуществляется постоянный мониторинг параметров состояния приемного и передающего оборудования. Например, в Мурманской области был организован филиал РТРС «Мурманский ОРТПЦ» цех Кандалакша для осуществления круглосуточного контроля за состоянием оборудования на удаленных передающих станциях. В России были составлены правила технической эксплуатации (ПТЭ) средств цифрового телерадиовещания стандарта DVB-T2, которые описывают условия эксплуатации оборудования, находящегося на обслуживаемых и необслуживаемых объектах цифрового наземного телевизионного вещания (ЦНТВ).

В соответствии с ПТЭ в филиалах РТРС для организации системы мониторинга используется оборудование СДК-5.3 отечественного производителя «НПП Триада ТВ». Данная система позволяет оперативно определить, на какой передающей станции возникла неисправность, в каком именно узле связи и по какой причине. Так же система оповещает оператора, сигнализируя о неисправности. На рис. 1 представлена структурная схема системы мониторинга. Все данные о состоянии оборудования передающего центра поступают на центральный сервер, к которому подключены персональные компьютеры операторов, наблюдающих за состоянием сети вещания. Операторы получают доступ через веб-интерфейс, то есть для управления системой мониторинга требуется только устройство с доступом к веб-браузеру.



Рис. 1. Схема системы мониторинга цифровых передатчиков СДК-5

Система мониторинга на базе оборудования СДК-5 позволяет контролировать такие параметры как:

1. Передатчики:

- Выходные параметры падающей мощности
- Параметры отраженной мощности
- КСВН
- Общие состояния передатчика, усилителей, источников питания, входа, ВЧ-сигнала

2. Приемники:

- Состояние захвата сигнала
- Состояние работы демодулятора
- Уровень E_b/N_0 , дБ
- Уровень C/N , дБ
- Запас устойчивости
- Уровни $\log(PER)$, $\log(BER)$

Блок СДК разработан «НПП Триада-ТВ» специально для контроля состояния удаленных передающих станций через сети связи с низкоскоростными неустойчивыми каналами *VSAT* или *GPRS*. Система СДК-5 позволяет осуществлять не только наблюдение, но и производить управление блоками связи. Таким образом есть возможность изменять мощность передатчиков, осуществлять резервирование сигнала передающего оборудования, выполнить обновление программного обеспечения, активировать либо деактивировать замещение *PLP* в реплейсере, изменять параметры приема спутникового сигнала, и многое другое. Но *VSAT* или *GPRS* не обладают стабильным каналом связи, что вносит невозможность оперативного реагирования на технические неисправности. При выполнении операций через *VSAT* могут происходить сбои соединения, задержки выполнения операций, как следствие устранение неисправностей затягивается. Так же данная система не позволяет управлять системой кондиционирования и электропитания удаленного объекта через веб-

интерфейс, так как они не обладают возможностью управления через систему общего доступа, а только лишь индуцируют информацию о своем состоянии.

Исходя из вышеперечисленных недостатков системы СДК-5, целесообразно осуществить подключение блока мониторинга по оптоволоконной сети через местного оператора связи. А также ввести в систему блоки управления кондиционированием и электропитанием через реле с удаленным контролем.

Для обеспечения стабильного подключения, следует внедрить в объекты ЦНТВ оптоволоконное приемное оборудование оператора связи с последующим подключением WAN выхода СДК-5.3 к маршрутизатору *Cisco 1121* (рис. 2), осуществить настройку маршрутизации сети доступа.



Рис. 2. Маршрутизаторы *Cisco 1121*

Для осуществления коммутации оборудования без возможности управления через веб-интерфейс можно использовать выходные одно реле и четыре оптореле. Они представляют собой пары контактов с возможностью дистанционного замыкания по команде пользователя. Данные контакты могут быть внедрены в различные электрические цепи в соответствии техническими параметрами реле и оптореле. Представленные коммутационные устройства имеют гальваническую развязку как друг с другом, так и с корпусом. Ниже приведена таблица 1 с электрическими характеристиками.

Управление реле имеет только один режим и может быть переключен пользователем через веб-интерфейс. В свою очередь оптореле имеют четыре режима: один – ручной и три – автоматических.

ТАБЛИЦА 1. Электрические характеристики реле и оптореле

Наименование	Переменный ток		Постоянный ток	
	Макс. напряжение, В	Макс. ток, А	Макс. напряжение, В	Макс. ток, А
Реле	250	5	50	5
Оптореле 1-4	50	1	50	1

Таким образом, предлагаемые усовершенствования существующей системы мониторинга приведут к улучшению эксплуатационных характеристик системы цифрового наземного телевизионного вещания.

Список используемых источников:

1. Пищин, О. Н. Дополнительная система мониторинга цифрового эфирного телевидения (ЦЭТВ) в Астраханской области / О. Н. Пищин, А. А. Иванов. — Текст: непосредственный // Молодой ученый. — 2020. — № 27 (317). — С. 100-104.
2. Блок системы дистанционного контроля «СДК-5.3» [Электронный ресурс] / ООО «НПП Триада-ТВ» г. Новосибирск – URL: <https://triadatv.ru/> (дата обращения 05.11.2022).
3. Отечественный разработчик мирового уровня / Константин Быструшкин и Артем Абросимов // «Теле-Спутник» — октябрь 2017. — №10(264). — Режим доступа : <https://old.telesputnik.ru/archive/pdf/264/60.pdf> (06.11.2022).

Sushko Y., Fedorov S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Development of the system of control and management of the equipment of the broadcasting center.

Capabilities of the SDK-5 remote monitoring system by "SPE Triada-TV" are considered. Monitored basic parameters of transmitting and receiving equipment are given. The scheme of the monitoring system of digital transmitters SDK-5 is presented. Advantages of this system are indicated, as well as options for optimizing the management of the transmitting center equipment are described.

Key words: *SDK-5, monitoring system, VSAT, remote access.*

УДК 004.946
ГРНТИ 28.17.33

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ГРАФИКЕ

Д. А. Татаренков, А. С. Горцуева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время нет такой сферы, которую бы не затрагивал искусственный интеллект. При этом также нет области деятельности, в которой бы не было графической составляющей, поэтому тема пересечения этих технологий является очень интересной и неоднозначной, но достаточно перспективной. На сегодняшний день есть множество направлений развития искусственного интеллекта и машинного обучения в области обработки изображений и графики в целом.

искусственный интеллект, нейросети, обработка изображений, графика, машинное обучение

Современный мир невозможно представить без графики, поскольку она окружает нас повсеместно: фильмы, видеоролики в интернете, реклама, фото в социальных сетях и так далее. Мы живем в то время, когда человек все больше процессов делегирует компьютеру, и это достаточно неоднозначно трактуется обществом. Некоторые люди воспринимают то, что нейронные сети способны рисовать всевозможные изображения покорить новые вершины в своей профессии и открыть что-то новое благодаря большой вычислительной мощности и интересной генерации новых идей, а другие боятся данной технологии, видят в этом этическую проблему. Несмотря на неоднозначность проблемы, в данном исследовании хотелось бы рассмотреть возможности, открываемыми перед людьми в сфере применения искусственного интеллекта в графике.

Задачи, которые позволяет решить искусственный интеллект в графике можно разделить на 3 больших группы: видео, изображения и 3D-графика. Классификация применимости ИИ представлена на рис. 1.

Как можно заметить, это далеко не все примеры применения нейросетей в графике, поскольку узких областей, в которых они используются огромное множество. При этом новые инструменты по большей части должны решать старые задачи, но быстрее, дешевле и эффективнее [1].

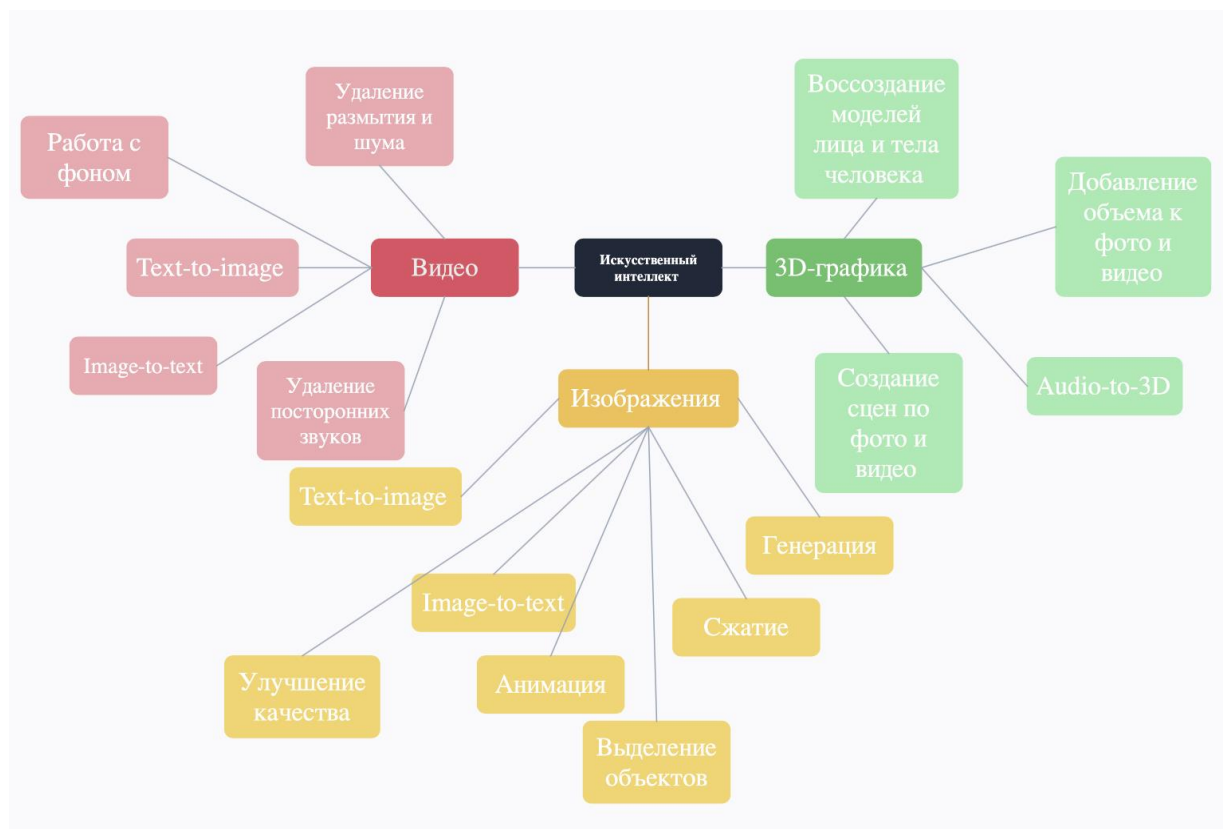


Рис. 1. Применимость искусственного интеллекта в графике

В области медиатехнологий с каждым днем появляется все больше технологий и инструментов, упрощающих работу с фотографиями, анимацией, видео и рисунками. Машинное обучение становится все более доступным для обычного пользователя. Практически каждый сталкивался с генеративно-состязательной нейросетью 2018 года StyleGAN, которая создавала удивительно похожие на реальные фотографии человеческих лиц изображения. Первая и последующие версии данной модели в связке с другими обученными нейросетями позволяют создать неповторимые картины и анимации, тем самым делая прорыв в искусстве, доступном каждому.

Далее хотелось бы поговорить о Text-to-image-модели, то есть модели генерирующей изображения по введенному пользователем тексту.

В апреле 2022 года была опубликована статья High-Resolution Image Synthesis with Latent Diffusion Model, в которой авторы описали принцип работы модели глубокого обучения со скрытой диффузией [2]. В этом же году на основе принципов, описанных в этой статье была построена и обучена модель Stable Diffusion [3], преобразующая текст в изображение, а также изображение в новый рисунок. Данная модель имеет открытый исходный код, любой желающий может запустить ее на своем компьютере и создавать невероятные картины. Такой синтез рисунков позволяет более широкой аудитории визуализировать свои идеи и снижает порог вхождения для художников и дизайнеров. Результат преобразования текста «Television and metrology department» в картинку в модели Stable Diffusion представлен на рис. 2.

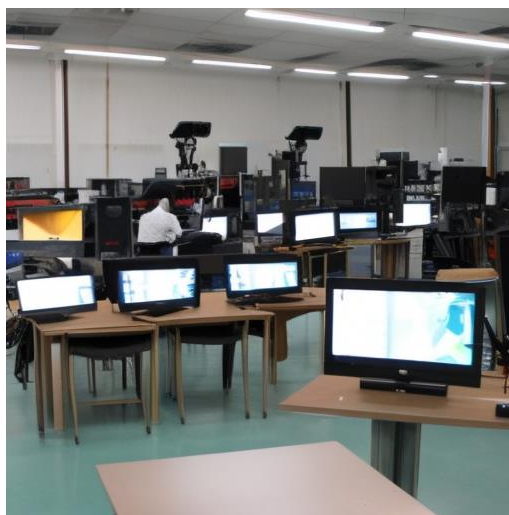


Рис. 2. Результат генерации «Television and metrology department»

Рассмотрим устройство данной модели машинного обучения. На рис. 3 представлена общая схема работы нейросети.

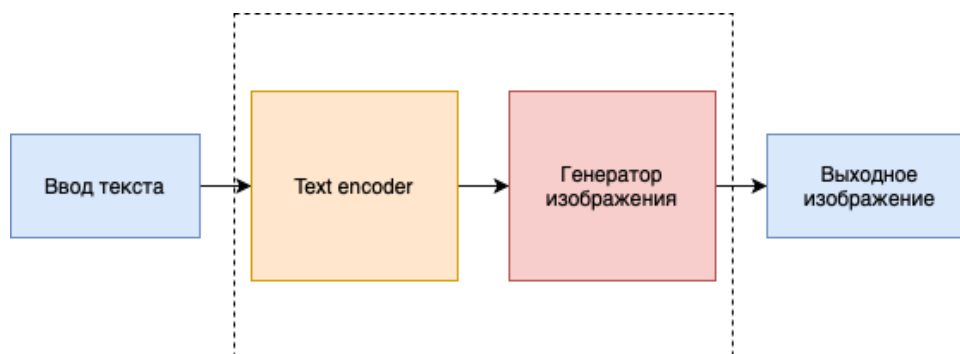


Рис. 3. Схема работы модели text-to-image

Текстовая информация подается на блок кодирования, на выходе которого образуется некоторый вектор, представленный в виде чисел. Далее полученный вектор поступает на Image Generator, состоящий из пары звеньев, выполняющих функции по созданию диффузированного изображения, а после – его декодирования в готовый рисунок высокого качества.

Если рассматривать операции по вычислению, производимыми моделью, то внутренние процессы, то есть блоки текстового кодировщика и генератора изображений (рис. 3) будут выглядеть так, как представлено на рис. 4.

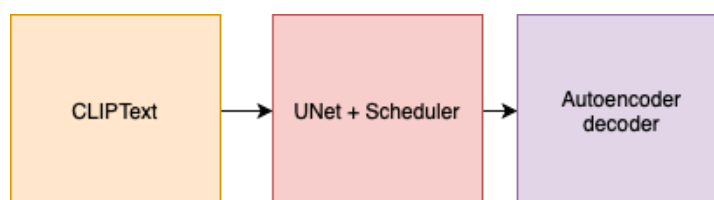


Рис. 4. Схема работы нейросетей внутри модели Stable Diffusion

Обучение CLIP происходит следующим образом: на вход кодировщика подается библиотека изображений и подписей к ним. Схожесть выходных результатов оценивается на основании косинусного коэффициента, в итоге

необходимо получить возможность оценивать степень корреляции описания и изображения.

В блоке UNet+Sheduler происходит поэтапное распознавание изображения из шумового вектора. На этапе обучения для данной операции нейросети представляется обратный процесс: к изображению добавляется шум до тех пор, пока картинка не станет нераспознаваемой, после чего модель должна уметь производить обратный процесс. При этом кодер и декодер обучаются вместе с применением скрытого пространства для ускорения внутренних процессов, поскольку это позволяет работать не с полноразмерными изображениями, а с их представлением меньшей размерности, встраиваемых в сжатый код. Данный метод сжатия кодировщиком позволяет модели сосредоточиться на семантике изображения, а не затрачивать вычислительную мощность на чтение всей информации об изображении. Именно использование скрытого пространства выделяет Stable Diffusion на фоне аналогичных моделей, таких как GLIDE.

Помимо генерации изображений модель Stable Diffusion хорошо работает в области сжатия изображений с потерями. Она сжимает изображение гораздо лучше, чем JPG или WebP. В качестве кодека Stable Diffusion сохраняет больше аспектов изображения, даже зернистость, однако на сжатие влияют артефакты и мелкие детали могут изменяться. Самым большим преимуществом можно выделить хорошее визуальное качество.

Кроме вышеизложенного нейросети позволяют повысить качество изображения вплоть до 4k (SuperResolution [4]), интерполировать/достроить дополнительные кадры (SuperSloMo [5]), рендерить физически сложные объекты (такие как облака), переносить стиль из одного изображения в другое, а также генерировать материалы. И это далеко не все сферы применения искусственного интеллекта.

Таким образом, несмотря на наличие этических проблем и споров в данной области, сфера применения искусственного интеллекта достаточно широка и является крайне перспективной, особенно в области медиатехнологий. Быстрое развитие моделей машинного, а в частности глубокого обучения, поможет совершить большой прорыв в обработке изображений и видео. Касаемо технологий, используемых в Stable Deffusion, они несомненно внесут большой вклад в развитие всевозможных сфер применения. Особо стоит отметить важность решения задачи по применению кода данной модели применительно к обработке и генерации изображений большей четкости, например, с явно распознаваемым текстом на них, поскольку из тестов модели видно, что в данной области на сегодняшний день существуют проблемы.

Список используемых источников:

1. Об интеллекте / Вильямс – Москва-Санкт-Петербург-Киев; 2007 – С. 128.
2. Robin Rombach, Andreas Blattmann, Dominik Lorenz, Patrick Esser, Bjorn Ommer /High-Resolution Image Synthesis with Latent Diffusion Models – 22.04.2022
3. dreamstudio.ai [Электронный ресурс]. URL: <https://beta.dreamstudio.ai/dream> (дата обращения 28.10.2022)
4. AMD Radeon [Электронный ресурс]. URL: <https://www.amd.com/en/technologies/radeon-super-resolution> (дата обращения 28.10.2022)

5. Huaizu Jiang / Super SloMo: High Quality Estimation of Multiple Intermediate Frames for Video Interpolation – 13.07.2018

Gortsueva A., Tatarenkov D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Artificial Intelligence application in graphics.

Currently, there is no area that is not affected by artificial intelligence. There is also no field of activity that does not have a graphic component, so the topic of the overlap between these technologies is very interesting and ambiguous, but very promising. Today there are many directions for the development of artificial intelligence and machine learning in the field of image processing and graphics in general.

Key words: artificial intelligence, neural networks, image processing, graphics, machine learning.

УДК 004.946
ГРНТИ 28.17.33

СРАВНЕНИЕ БИБЛИОТЕК ДЛЯ УПРАВЛЕНИЯ АДРЕСНЫМИ СВЕТОДИОДАМИ

Д. А. Татаренков, А. В. Чеботарева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире большое количество оформленного светового пространства включает в себя использование светодиодных панелей, лент, вывесок и экранов. Их используют как для маркетинговых мероприятий, так и для сценического искусства. Статья посвящена устройству и принципу работы адресных светодиодов. Также в данной статье производится сравнение существующих библиотек для работы с адресными светодиодами.

адресные светодиоды, FastLED, NeoPixel

В настоящее время, для оформления светового пространства все большее применение получают разного рода светодиодные панели, вывески, ленты и экраны. Яркое и красочное изображение, которое позволяют получить светодиоды, выигрышно смотрится на фоне, и привлекает внимание. Таким образом, данный вид визуализации информации широко используется для рекламы, формирования сценических композиций и для декора помещений.

Адресные светодиоды представляют собой модуль с тремя светодиодами красного, зеленого и синего цветов (RGB), которыми управляет контроллер. В зависимости от реализации модуль может быть оснащён только одним контроллером (WS2811), в таком случае оттенок будет одинаков для каждой триады. В случае, когда каждый трёхкомпонентный светодиод управляется собственным контроллером (WS2812B), есть возможность управлять оттенком и яркостью каждого элемента отдельно.

Каждый модуль имеет 4 вывода: два для вывода данных (DI – digital input, DO – digital output, например) и два для вывода питания (5V и GND, например). Адресные светодиоды подключаются по цепочке через выводы данных, тем самым имея возможность передавать информацию дальше.

Принцип работы цепочки из адресных светодиодов, следующий: команда приходит на вход первого модуля в виде последовательности 24 битов (по 8 на каждый светодиод), первый модуль сохраняет их в своей памяти, а остальные биты передает следующему модулю. Когда данные перестают поступать дольше 50 мкс, светодиоды выводят цвета, согласно сохраненной информации [1].

Биты данных в адресный светодиод передаются в виде прямоугольных импульсов высокого и низкого уровня, длительность которых зависит от значения. Длительность каждого бита равна 1,25 мкс. Длительность высокого уровня логического «0» равна 0,4 мкс, а логической «1» – 0,85 мкс. Между последовательностями данных необходимо выдерживать паузу в 50 мкс. Если данные не передаются дольше 100 мкс, то контроллер воспринимает это как окончание передачи данных.

Внешнее управление такими адресными светодиодными цепочками осуществляется с помощью контроллеров. Они позволяют пользователю управлять всей конструкцией, получая данные от устройства. Так, например, контроллер ESP32 позволяет получать данные через канал Wi-Fi как с компьютера, так и с мобильного устройства.

Для управления адресными светодиодными цепочками на программном уровне, в основном используют две популярные библиотеки: FastLED и NeoPixel.

Библиотека NeoPixel была разработана компанией Adafruit Industries и предназначалась для работы со светодиодными лентами и кольцами, которые продавала эта компания. Поддерживает все виды плат прототипирования Arduino на процессоре Atmel. Библиотека основана на таких языках как C, Assembler и Wiring. Она позволяет:

- устанавливать цвета для каждого светодиода,
- выбирать различные режимы работы светодиодных лент и панелей,
- управлять яркостью свечения светодиода.

Библиотека FastLED была разработана Даниэлем Гарсиа и Марком Кригсманом в 2010-2013 годах. Написана на языке C и работает с Arduino и множеством других плат, включая микроконтроллеры на базе AVR и ARM. Возможности данной библиотеки намного шире, в отличие от прошлой, которая базируется только на основных необходимых функциях. Так, например, одной из возможностей данной библиотеки является поддержка цветовой палитры HSV.

Скорость работы каждой из библиотек зависит от количества светодиодов в цепочке. Данные приведены в таблице 1 [2].

ТАБЛИЦА 1. Скорость работы библиотек в зависимости от количества светодиодов

Количество светодиодов	FastLED, Гц	NeoPixel, Гц
512	59	55
400	74	71
300	95	95
256	108	110
200	133	142
144	182	196
100	220	283
60	300	469
30	400	822
16	400	1261
8	400	1813

Для удобства данные были переведены в график, изображенный на рис. 1.

Как можно заметить на графике, скорость работы с библиотекой NeoPixel выше, особенно при небольшом количестве светодиодов. Если же использовать большое количество светодиодов, то скорость с FastLED немного больше.

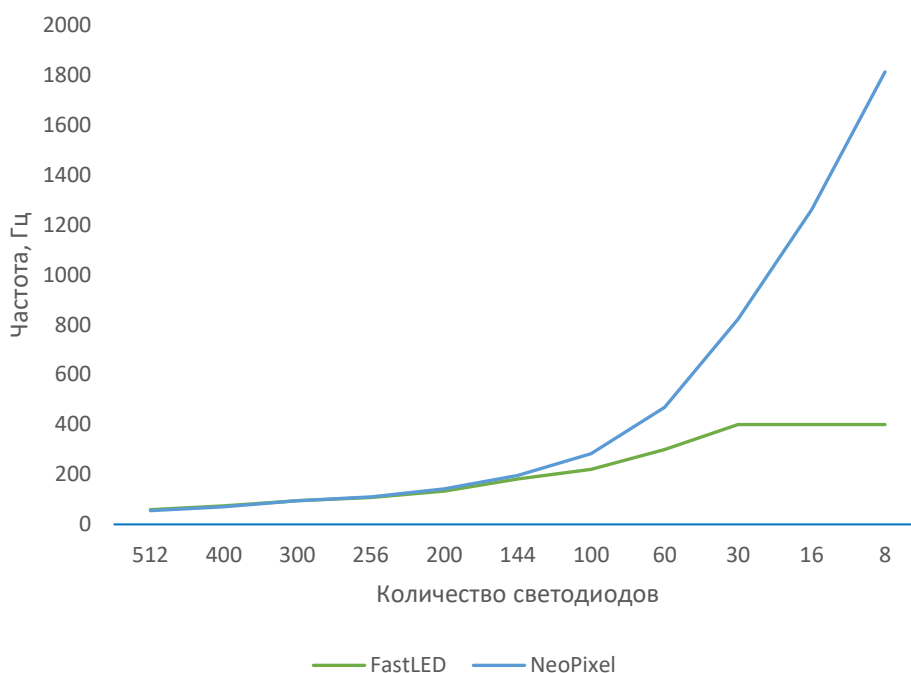


Рис. 1. График зависимости частоты от количества светодиодов

Приведенные библиотеки различаются также объемами занимаемой памяти. Библиотека NeoPixel требует меньше, чем FastLED [2].

Таким образом, можно сделать вывод, что библиотека NeoPixel находится в более выигрышном положении за счет лучшей скорости работы, меньшим количеством занимаемой памяти и всем необходимым функционалом работы. Возможности данной библиотеки являются базовыми, поэтому сложность работы с ней минимальна. Однако, если необходимо использовать большое количество светодиодов и/или необходимы более продвинутые функции, лучшим вариантом будет использование FastLED.

Список используемых источников:

1. Адресные светодиоды, модули NeoPixel. [Электронный ресурс] // URL: <https://wiki.iarduino.ru/page/adresnye-svetodiody-moduli-neopixel/> (дата обращения 10.11.2022).
2. Кто быстрее, FastLED или NeoPixel? [Электронный ресурс] // URL: https://alexgyver.ru/fastled_vs_neopixel/ (дата обращения 10.11.2022).

Tatarenkov D., Chebotareva A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

In the modern world, a large amount of decorated light space includes the use of LED panels, ribbons, signage and screens. They are used both for marketing events and for performing arts. The article is devoted to the device and the principle of operation of address LEDs. This article also compares existing libraries for working with address LEDs.

Key words: addressable LEDs, Fast LED, NeoPixel.

УДК 528.854.4
ГРНТИ 28.23.15

АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ РАСПОЗНАВАНИЯ ЭМОЦИЙ ЧЕЛОВЕЧЕСКОГО ЛИЦА

Д. В. Тяжев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Автоматическое распознавание выражения лица — сложная тема, которая в последние годы вызвала интерес у многих исследователей. В связи с этим имеет смысл рассмотреть существующие системы распознавания эмоций человеческого лица и провести сравнительный анализ.

FER, распознавание эмоций человека, FACS, TFLearn, сверточная нейронная сеть, CNN

Человеческое лицо имеет важные и отличительные характеристики, которые помогают в распознавании выражений лица. FER (автоматическое распознавание эмоций по лицу) определяется как изменение выражения лица, вызванное внутренним эмоциональным состоянием человека. Оно используется в широком спектре приложений взаимодействия человека с компьютером, таких как обработка изображений лиц, видеонаблюдение и анимация лиц, а также в областях компьютерного зрения, цифровой обработки изображений и искусственного интеллекта. Автоматическое распознавание выражения лица — сложная тема, которая в последние годы вызвала интерес у многих исследователей. В FER критической является стадия выделения признаков. Ученые обнаружили, что выражения лица являются наиболее важным способом выражения информации о человеческих эмоциях. Информация о выражении эмоций составляет около 55 % информации, передаваемой экспериментаторами, голосовая информация — 38 %, а языковая информация — всего 7 % всей информации [1].

У людей есть базовый набор эмоций, которые передаются через универсальные и базовые выражения лица. Автоматическая идентификация эмоций на изображениях и видео станет возможной, если будет разработан алгоритм, который идентифицирует, извлекает и оценивает эти выражения лица в режиме реального времени. В социальной среде выражение лица является мощным инструментом для передачи личных чувств и намерений. Они играют важную роль в социальных взаимодействиях людей. Восприятие лица в контексте ситуаций, в которых его видят, дает важную контекстуальную информацию для обработки выражений лица. Способность обнаруживать и передавать человеческие эмоции имеет решающее значение в межличностных отношениях. С незапамятных времен автоматическое обнаружение эмоций было спорным научным предметом.

Система кодирования лицевых движений.

Система кодирования лицевых движений (FACS) выявляет небольшие изменения черт лица. Этот широко используемый в психологии метод основан на наблюдении человека и состоит из 44 блоков действия, связанных с напряжением групп лицевых мышц для обнаружения эмоций лица (рис. 1) [2]. Кроме того, используются так называемые Action Units (AU) (рис. 2). FACS часто

рассматривается вручную опытными специалистами, которые изучают замедленные видеозаписи сокращений лицевых мышц, прежде чем кодировать и маркировать их. В последние годы было предпринято много попыток автоматизировать эту процедуру. Чтобы оценить эмоции с использованием данных FACS, данные FACS должны быть сначала преобразованы в систему, способную это делать. Такое поведение моделируется системой эмоциональных лицевых действий (EMFACS) [2].

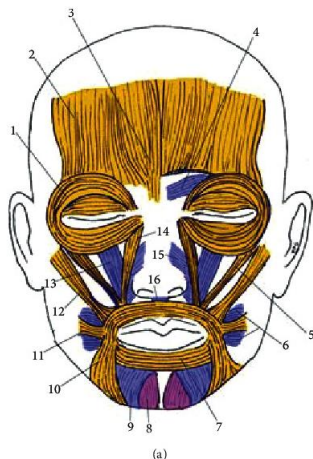


Рис. 1. Мимические мышцы лица






























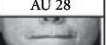
Upper Face Action Units					
AU 1	AU 2	AU 4	AU 5	AU 6	AU 7
					
Inner Brow Raiser	Outer Brow Raiser	Brow Lowerer	Upper Lid Raiser	Cheek Raiser	Lid Tightener
*AU 41	*AU 42	*AU 43	AU 44	AU 45	AU 46
					
Lid Droop	Slit	Eyes Closed	Squint	Blink	Wink
Lower Face Action Units					
AU 9	AU 10	AU 11	AU 12	AU 13	AU 14
					
Nose Wrinkler	Upper Lip Raiser	Nasolabial Deepener	Lip Corner Puller	Cheek Puffer	Dimpler
AU 15	AU 16	AU 17	AU 18	AU 20	AU 22
					
Lip Corner Depressor	Lower Lip Depressor	Chin Raiser	Lip Puckerer	Lip Stretcher	Lip Funneler
AU 23	AU 24	*AU 25	*AU 26	*AU 27	AU 28
					
Lip Tightener	Lip Pressor	Lips Part	Jaw Drop	Mouth Stretch	Lip Suck

Рис. 2. Action Units

На сегодняшний день существует множество готовых алгоритмов распознавания эмоций человека по изображению. Однако не все они могут похвастаться высокими показателями точности и скорости. В качестве примера был проведен аналитический анализ существующих систем распознавания эмоций:

- Emotion recognition using Deep Convolutional Neural Network [4]
 - Face classification and detection from the B-IT-BOTS robotics team [3]
- Emotion recognition using Deep Convolutional Neural Network.

Для задачи классификации эмоций было выбрано решение, представляющее собой обученную многослойную сверточную нейронную сеть. На вход которой в реальном времени подается видеопоток, анализируя который нейронная сеть распознает эмоции на человеческом лице. Для построения нейронной сети была выбрана библиотека TFlearn для языка программирования Python, которая основана на фреймворке TensorFlow для машинного обучения разработанная компанией Google [6]. Работа с данным фреймворком упрощается за счет того, что для разработки нейронной сети необходимо только описание самих слоев, в отличие от других алгоритмов, где требуется описание каждого нейрона по-отдельности. Также существенным достоинством данного фреймворка считается упрощенная система обучения сети и вывод обратной связи процесса в реальном времени и точности обучения. Более того, библиотека позволяет сохранять результат натренированной модели и использовать её при дальнейших исследованиях. Схематическая модель итоговой нейронной сети представлена на рис. 3.

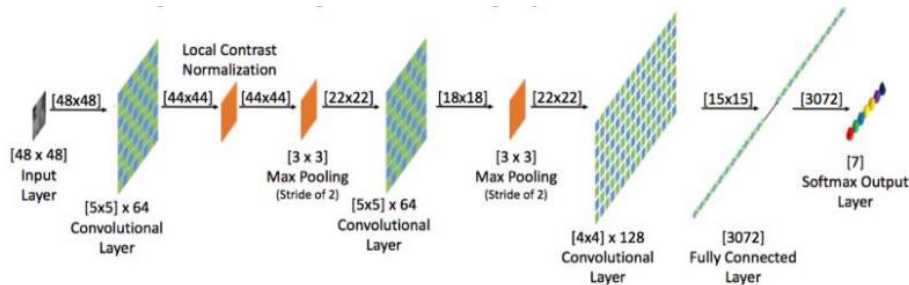


Рис. 3. Схематическая модель нейронной сети.

Начинается анализ с попытки распознавания на кадре видеопотока человеческого лица. Происходит это при помощи библиотеки OpenCV [5]. После распознавания лица, изображение обрезается до размеров 48 на 48 пикселей, таким образом чтобы лицо располагалось по центру. Только на данном этапе изображение попадает на вход нейронной сети. Благодаря этому получается оптимизированное ПО, которое существенным образом сокращает нагрузку, создаваемую на нейронную сеть. Для обучения сети был выбран набор изображений FERC-2013 [7], насчитывающего около 35887 черно-белых изображений, содержащих примеры проявления следующих эмоций: гнев, страх, счастье, грусть, удивление, безразличие и отвращение. Плотность распределения эмоций в данном наборе изображений отражена на рис. 4.

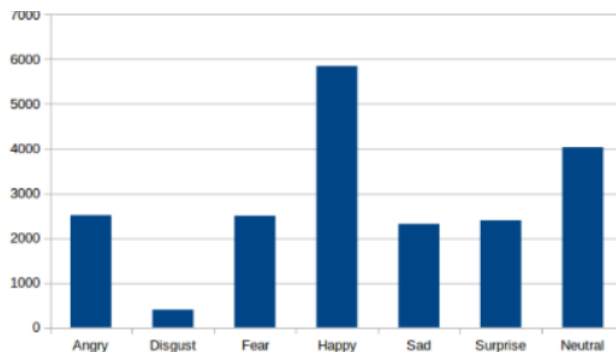


Рис. 4. Распределение выражаемых эмоций в датасете FERC-2013

После 26 эпох обучения нейронной сети точность определения эмоций на тренировочной выборке составила порядка 86,4% (рис. 5).

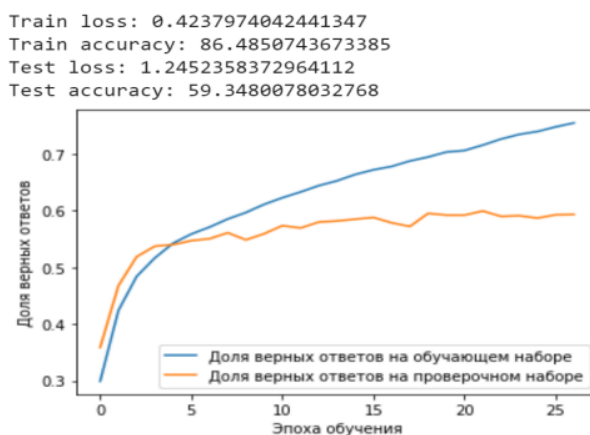


Рис. 5. Результат работы нейронной сети после 26 циклов обучения.

Face classification and detection from the B-IT-BOTS robotics team.

В данной работе для классификации человеческих эмоций был выбран также алгоритм основывающийся на сверточной нейронной сети и открытой библиотеки распознавания лиц openCV [5]. Модель нейронной сети была реализована при помощи библиотеки с открытым исходным кодом Keras. Отличительной особенностью библиотеки Keras является возможность использования GPU или CPU. Для обучения данной модели использовали другой датасет IMDB, состоящий из 460723 RGB изображений распределение выражаемых эмоций в датасете IMDB представлено на рис. 6 [3].

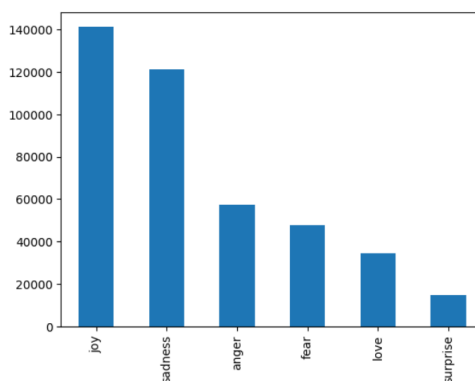


Рис. 6. Распределение выражаемых эмоций в датасете IMDB

При обучении на датасете IMDB после 26 циклов обучения была достигнута максимальная точность распознавания 96%. Также для получения сравнительных анализов двух систем было проведено обучение нейронной сети на датасете FER-2013 [7], включающие в себя 35,887 черно-белых изображений. Однако на данном датасете была достигнута максимальная точность в 66%.

В заключении можно сказать, что задачи по распознаванию эмоций человека хоть и пользуются огромной популярностью среди исследователей, которые ищут различные подходы для решения данной задачи, но все же еще не была сформирована идеальная модель для 100% распознавания человеческих эмоций. Однако стоит учесть, что основным средством реализации являются сверточные нейронные сети различных архитектур и обученные на датасетах доступных в открытом доступе.

Список используемых источников:

1. Как технологии распознают наши эмоции и почему это так перспективно [Электронный ресурс]. – URL: <https://rb.ru/opinion/tehnologii-i-emptsii/>. – (Дата обращения: 5.11.2022).
2. Methods for Facial Expression Recognition with Applications in Challenging Situations / Anil Audumbar Pise, Dimitrios A. Karras [Электронный ресурс]. – URL: <https://www.hindawi.com/journals/cin/2022/9261438/>. – (Дата обращения: 10.11.2022).
3. About facereader [Электронный ресурс]. – URL: <https://www.noldus.com/facereader/measure-your-emotions>. – (Дата обращения: 10.11.2022).
4. Correa, E. Emotion Recognition using Deep Convolutional Neural Network / E. Correa, A. Jonker, M. Ozo, R. Stolk [Электронный ресурс]. – URL: https://github.com/isseu/emotionrecognition-neural-networks/blob/master/paper/Report_NN.pdf – (Дата обращения: 11.11.2022).
5. Библиотека обработки изображений OpenCV [Электронный ресурс]. – URL: <http://opencv.org> (13.11.2022).
6. Библиотека для глубокого обучения TFlearn [Электронный ресурс]. – URL: <http://tflearn.org/> (07.10.2022).
7. FER-2013 [Электронный ресурс]. – URL: <https://www.kaggle.com/datasets/msambare/fer2013> – (Дата обращения: 09.11.2022).

Tyazhev D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of existing methods for recognizing human facial emotions.

Automatic facial expression recognition is a complex topic that has attracted the interest of many researchers in recent years. In this regard, it makes sense to consider the existing systems for recognizing the emotions of a human face and conduct a comparative analysis.

Key words: FER, Human Emotion Recognition, FACS, TFlearn, Convolutional Neural Network, CNN.

УДК 654.172
ГРНТИ 49.45.29

ЭВОЛЮЦИЯ ТВЕРДОТЕЛЬНЫХ ТЕЛЕВИЗИОННЫХ ПРЕОБРАЗОВАТЕЛЕЙ СВЕТ-СИГНАЛ

С. Л. Федоров, А. И. Волкова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются твердотельные преобразователи свет-сигнал технологий: приборы с зарядовой связью (ПЗС) и комплиментарный металл-оксид-полупроводник (КМОП). Отмечается, что современное вещание с использованием форматов телевидения высокой четкости и телевидения сверхвысокой четкости невозможно без технологии КМОП. Приводится развитие КМОП-технологии.

КМОП, ПЗС, ТВ вещание, форматы ТВЧ и ТСВЧ

Эпоха вакуумных телевизионных преобразователей свет-сигнал завершилась с появлением их твердотельных аналогов. В начале 1970-х гг. появились первые приборы с зарядовой связью (ПЗС), а относительно недавно на смену ПЗС технологии пришла другая – КМОП (металл-оксид-полупроводник), которая привела к появлению так называемых «видеосистем на кристалле» - интеграция на одном кристалле фотоприёмников, устройств развёртки, оцифровки и цифровой обработки видеосигналов.

Матрица преобразователя на основе ПЗС представляет собой устройство последовательного считывания, работа которого состоит из двух основных процессов: накопление зарядов в МОП-структурах (или обратносмещенных фотодиодах) и перенос зарядов в определенном направлении путем последовательной подачи фазных напряжений на соответствующие электроды с выводом зарядов через выходное устройство, формирующее сигнал изображения. Процесс переноса зарядов зависит от организационной структуры матрицы. Так в телевизионных и видеокамерах нашли применение матрицы трех типов: с кадровым, строчным и кадрово-строчным переносом.

За время существования преобразователей с ПЗС технологией произошли значительные их усовершенствования, которые привели практически к идеальному преобразователю по эксплуатационным характеристикам. Однако появление телевидения высокой четкости (ТВЧ), не говоря уже о сверхвысокой четкости (ТСВЧ), заставило задуматься о новой специфике построения твердотельных телевизионных преобразователей свет-сигнал.

Переход к форматам ТВЧ и ТСВЧ предусматривает повышение пропускной способности выходного устройства преобразователя на основе ПЗС-технологии (таблица 1), которую обеспечить достаточно сложно [1].

ТАБЛИЦА 1. Зависимость роста пропускной способности выходного устройства от увеличения количества пикселей

Формат	Пропускная способность
SD	15 МГц
HD и 1080i50	55 МГц
HD и 1080p50	110 МГц
HD и 1080p150	330 МГц

Одно из самых больших различий между ПЗС и формирователями изображения КМОП - ПЗС передают сигнал от пикселя к пикселю к выходному узлу в области заряда, в то время как формирователи изображения КМОП преобразуют сигнал из заряда в напряжение в каждом пикселе и выводят сигналы напряжения когда они выбираются по строке и столбцу, то есть у каждого пикселя есть собственный выходной усилитель (рис. 1). Это означает, что требования пропускной способности, предъявляемые к данному выходному усилителю, связаны только с количеством считываний в секунду [2].

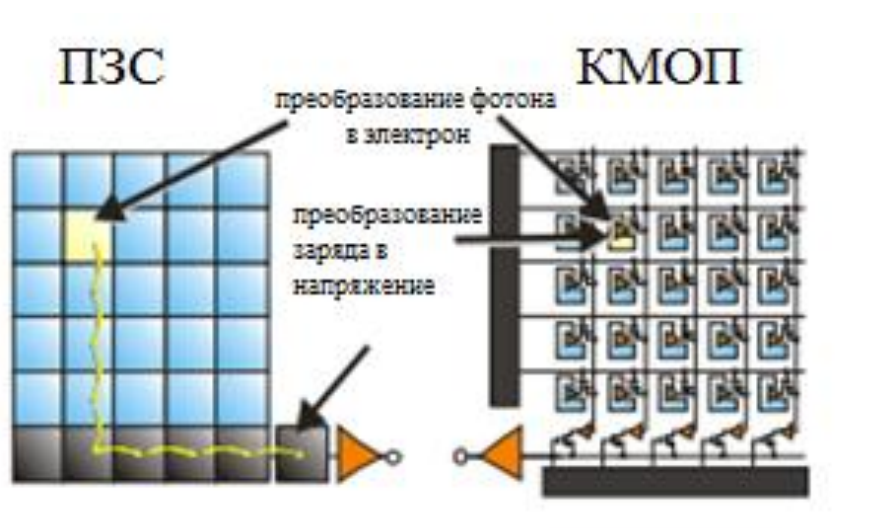


Рис. 1. Основное различие между ПЗС и КМОП

Также как ПЗС, КМОП-матрица состоит из фотодиодов, но роль «хранителя» заряда выполняет конденсатор. Рядом с фотодиодом располагаются транзисторы. Первый в качестве электронного ключа открывающего цепь «фотодиод — конденсатор», второй для установки конденсатора в «начальное» состояние. Как принято, «начальным» состоянием у конденсатора КМОП-матрицы будет заряженное состояние, а фотодиод будет разряжать его.

КМОП-сенсоры имеют ряд преимуществ перед ПЗС: повышенную чувствительность (КМОП: чувствительность не снижается, ПЗС: 1-1,5 деления диафрагмы теряется), сниженное энергопотребление (напряжение питания КМОП: +3В, +5,5В; ПЗС: от +12В до +15В), меньшее тепловыделение (КМОП: 35°C; ПЗС: 40°C), расширенный динамический диапазон и цифровую природу самого сенсора, благодаря чему в камере отпадает необходимость в аналоговой части тракта. В итоге – потенциально более высокое разрешение, расширенный динамический диапазон и увеличенная кадровая частота [1]. Динамический

диапазон может быть еще более расширен с возможностью создания внутрикамерного HDR.

КМОП-технология развивается до сих пор. Первым поколением КМОП-сенсоров были сенсоры с пассивным пикселем (Passive Pixel Sensor, PPS). Их особенностью является наибольшая связь с породившими их микросхемами динамической или статической памяти [3]. Данный вид сенсора, помимо матрицы фотодиодов содержит: регистр, осуществляющий выбор строки; ключевые полевые транзисторы, осуществляющие коммутацию фотодиодов выбранной строки к вертикальным видеошинам; аналоговый мультиплексор, осуществляющий подключение видеосигнала с выбранного фотодиода к выходному усилителю, что представлено на рис. 2.

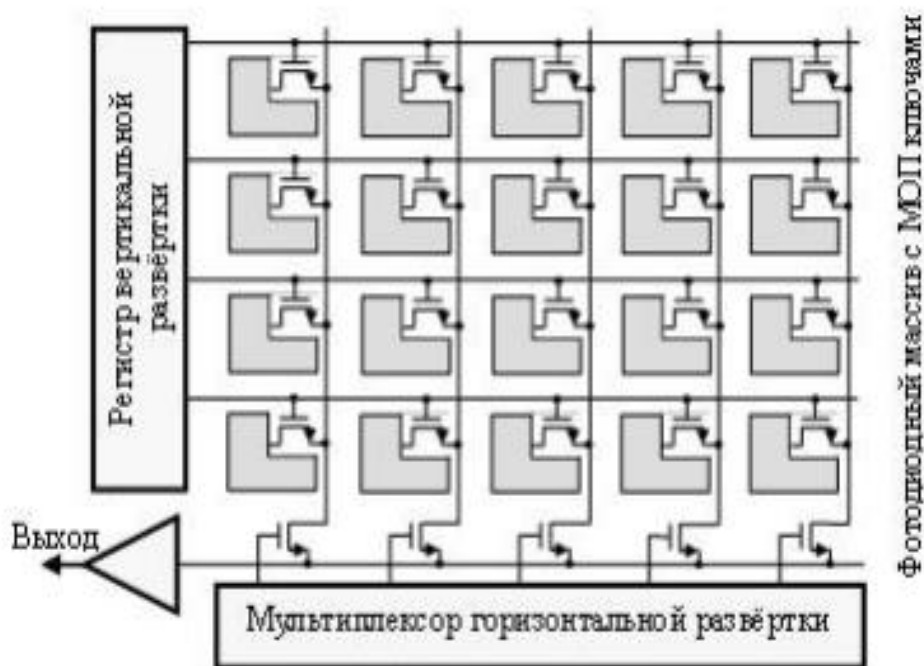


Рис. 2. КМОП-сенсор с пассивным пикселем

Вторым поколением КМОП-сенсоров являются сенсоры с цифровым пикселем (Digital Pixel Sensor, DPS). Особенностью этих преобразователей является интеграция в каждый пиксел не только активного усилителя, но и непосредственно АЦП (рис. 3). При этом частота преобразования АЦП становится равной кадровой частоте фотоприемника, а полоса частот видеосигнала уменьшается до минимальных значений [3]. В настоящее время известны КМОП сенсоры с цифровым пикселем размером $9,8 \times 9,8$ мкм, при технологии 0,18 мкм, содержащие в каждом пикселе АЦП, состоящий из 37 транзисторов.



Рис. 3. КМОП-сенсор с цифровым пикселем

В 2019 году и ранее слой оксида никеля, блокирующий электроны, использовался для предотвращения инжекции электронов с пиксельного электрода в схему считывания сигнала КМОП в слой кристаллического селена, что приводило к точечному шуму на изображении, и были разработаны методы улучшения качества изображения [4].

В 2020 году научные лаборатории Японии провели исследования одночипового цветного устройства формирования с использованием органических фотопроводящих пленок (органических пленок) с целью создания компактных цветных камер высокого разрешения. Был создан прототип трехслойного цветного устройства формирования изображения с двумя типами органической пленки, наложенной на датчик изображения КМОП. Также началась разработка твердотельного устройства формирования изображения КМОП, которое использует фотопроводящую пленку из кристаллического селена с функцией умножения заряда (умножающая пленка) для реализации высокочувствительных камер 8K Ultra-High Definition [5].

За счет того, что КМОП-матрицы имеют более низкое энергопотребление в статическом состоянии, их применяют в камерах мобильных телефонов. Преобразователи VD6853 и VD6803 с разрешением 3,15 Мп (2048×1536 пикселей) компании STMicroelectronics, разработанные в 2009 г., предназначены специально для мобильных устройств, смартфонов, игровых консолей. Датчики имеют встроенные средства регулировки глубины резкости, что наряду с малыми размерами пикселя (1,75 мкм), позволяют получать изображение отличного качества при фокусном расстоянии менее 15 см. Размер модуля составляет 6,5×6,5 мм.

К 2022 году развитие технологии КМОП для мобильных устройств достигло того, что появилась линейка 8- и 13-мегапиксельных КМОП-матриц с задней подсветкой с размером пикселей 1,12 микрона. Также компания Toshiba Electronics Europe (ТЕЕ) представила новую 20-мегапиксельную КМОП-

матрицу с размером пикселей 1,12 мкм, предназначенную для мобильных телефонов и смартфонов класса High-End с разрешением 1080p. Оптический размер в 1/2,4 дюйма матрицы Т4КА7 позволяет создавать модули камер толщиной не более 6 мм, чтобы удовлетворить потребительский спрос на сверхтонкие и сверхлегкие мобильные устройства.

Требования к качеству изображения с каждым годом повышаются, прогнозируется появление новых форм визуального вещания. Технология ПЗС показала себя с наилучшей стороны, но ее время подходит концу, в части преобразователей свет-сигнал. Настоящее и ближайшее будущее преобразователей свет-сигнал, несомненно, связано с КМОП-технологией и усовершенствованием эксплуатационных характеристик телевидеокамер.

Список используемых источников:

1. Вебер К. КМОП: готов к телевещанию уже сегодня // Белая книга. 2012. С. 1, 4, 9-10
2. DALSA Digital Cinema. Image Sensor Architectures for Digital Cinematography // С. 5-7
3. Манцетов А.А., Цыцулин А.К. Телекамеры на КМОП фотоприемниках // Вопросы радиоэлектроники, сер. Техника телевидения. 2006. С. 1-12
4. MITANI Kohji. Anuall report // NHK Science & Technology Research Laboratories. 2019
5. MITANI Kohji. Anuall report // NHK Science & Technology Research Laboratories. 2020

Volkova A., Fedorov S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Voluion of solid state TV light-signal converters.

Solid-state light-to-signal technology converters are considered: charge-coupled devices (CCD) and complementary metal-oxide-semiconductor (CMOS). It is noted that modern broadcasting using high-definition television and ultra-high-definition television formats is impossible without CMOS technology. The development of CMOS technology is given.

Key words: CMOS, CCD, TV broadcast, HDTV and UHD TV formats.

УДК 621.397
ГРНТИ 49.45.29

ВОЗМОЖНОСТЬ ИМПОРТОЗАМЕЩЕНИЯ ОБОРУДОВАНИЯ ЦИФРОВОГО ЭФИРНОГО ТЕЛЕВИЗИОННОГО ВЕЩАНИЯ СТАНДАРТА DVB-T2 НА ПРИМЕРЕ ВЕЩАНИЯ ПАКЕТА РТРС-1

А. Р. Элежбиев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Вопрос импортозамещения для Российской Федерации является сейчас актуальным как никогда ввиду сложившейся санкционной обстановки и отказа поставки как оборудования, так и запасных частей к нему. Данная ситуация не обошла стороной такую важную область как телекоммуникации (телевидение). В данной статье будет предложено решение возникшей проблемы путем прямого замещения импортного оборудования оборудованием, производимым в РФ.

телевизионное вещание, импортозамещение, приемник, передатчик

В процессе эксплуатации существующего импортного оборудования неизбежно возникают проблемы сбоя программного обеспечения (ПО) и выхода целых узлов из строя. Учитывая сложность такого оборудования, решение остается одно, переустановка (ПО) или замена вышедшего узла новым. И то, и другое производители оборудования отказываются поставлять, что в дальнейшем ведет к неполноценной эксплуатации и полного отсутствия возможности вообще эксплуатировать данное оборудование.

В одночастотной сети Чеченской Республики для первого мультиплекса используются кодеры, модуляторы и усилители одного производителя «*Rohde&Schwarz*», приемники-декодеры от компании «*Harmonic Inc.*».

В данной работе вместо существующего оборудования будут использованы:

Вместо приемника *Harmonic Proview 7100* производства Израиль будет использован приемник-декодер *RTM TRK-575* от производителя «ОАО Юрьев-Польский Завод «Промвязь»». Спутниковый приемник *RTM TRK-575* предназначен для приема двух транспондеров в формате *DVB-S/S2* с деинкапсуляцией в *T2-MI* и выводом транспортных потоков *ASI* на любой из четырех выходных портов [1].

Достоинства приемника *RTM TRK-575* наличие двух отдельных декодеров в одном корпусе. Наличие четырех независимых выходов с возможностью отдельной настройки. Например, с первого выхода можно снимать сигнал первого мультиплекса, со второго выхода сигнал второго мультиплекса, с третьего и четвертого сигнал выделенного пакета разных мультиплексов, данная возможность отсутствует в приемнике *Harmonic Proview 7100*.

Вместо оборудования «*Rohde&Schwarz*», кодер, модулятор, усилитель будет использован передатчик *Микротек-TTUD250*, который состоит из двух блоков: возбудитель и усилитель мощности. Достоинства передатчика Микротек это наличие кодера и модулятора в одном корпусе.

Собранная стойка для РТРС-1 с использованием отечественного оборудования представлена на рис. 1.



Рис. 1. Стойка вещания пакета RTPC-1, собранная исключительно из отечественного оборудования

Проверив правильность подключения, следует настроить оборудование и провести измерение.

Для исследования используется анализатор *R&S®ETC* производства фирмы «*Rohde&Schwarz*». Анализатор *R&S®ETC* предназначен для анализа телевизионных сигналов, а также для проведения спектрального и скалярного анализа цепей и измерений мощности [2].



Рис. 2. Сигнальное созвездие принимаемого сигнала пакета RTPC-1

Режим измерений сигнального созвездия *CONSTELLATION DIAGRAM* показывает значения демодулированных *I/Q* квадратурных компонент в прямоугольной системе координат совместно с основными параметрами измерений и настроек прибора. Сигнал передается без видимых искажений и шумов (см. рис. 2).

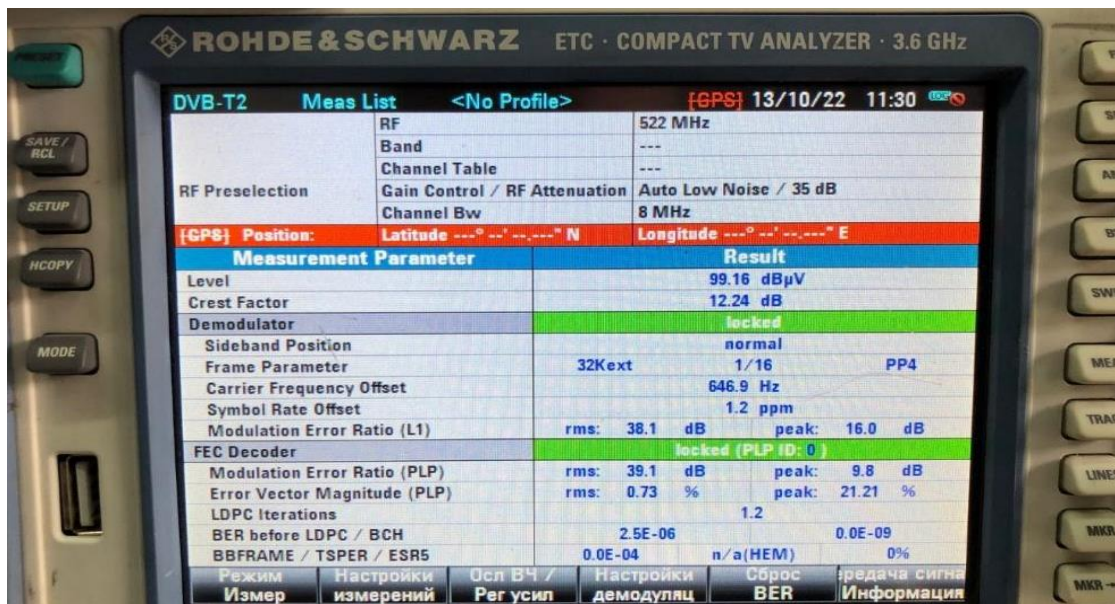


Рис. 3. Основные параметры сигнала пакета RTPS-1

Исходя из данных показателей, мы видим частоту, которая установлена, ширину полосы, при наличии *GPS* антенны координаты точки проведения измерений, уровень сигнала, захват модуляции, синхронизацию, количество битовых ошибок.

Измерения $MER(k)$ показывают распределение величины MER по модулированным поднесущим *OFDM* сигнала (k) (см. рис. 4).



Рис. 4. Распределение величины MER

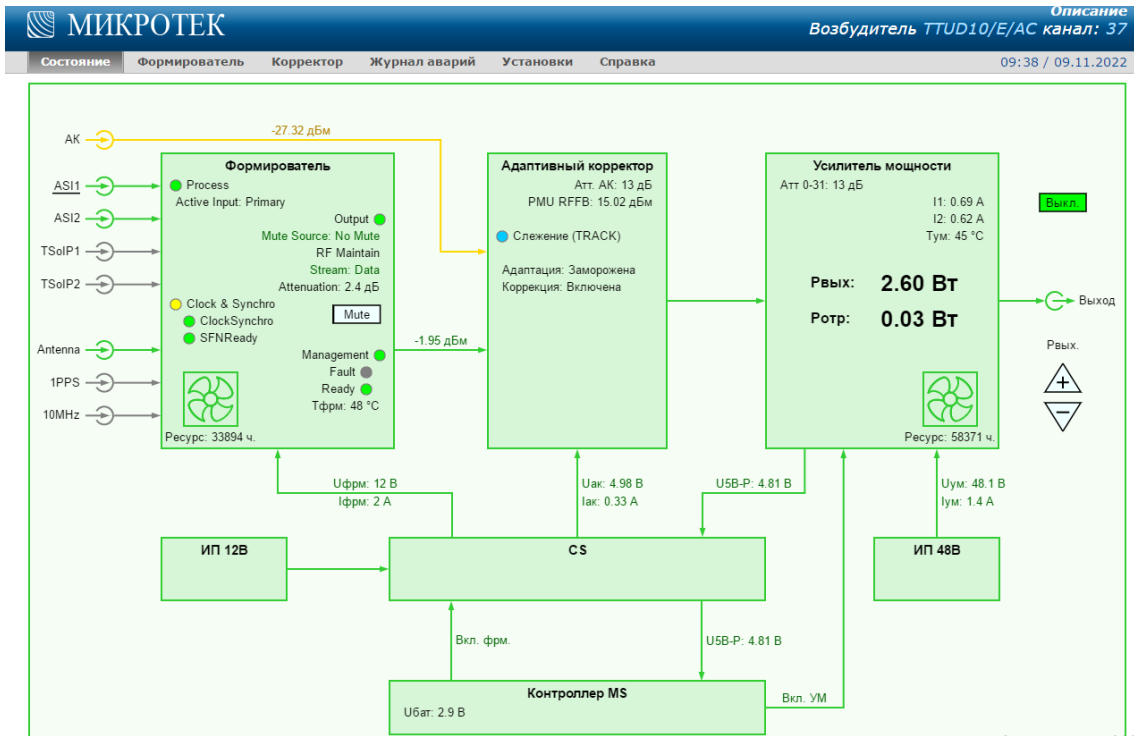


Рис. 5. Рабочее окно состояния (работы) передатчика

Окно состояния передатчика простое и понятное, отображает в реальном времени состояние внешних и внутренних узлов. Позволяет в реальном времени дистанционно или локально просмотреть подробно или изменить интересующие параметры. Меняя параметры меню настроек передатчика, есть возможность в реальном времени просматривать изменения в рабочем окне. (см. рис. 5 и б).

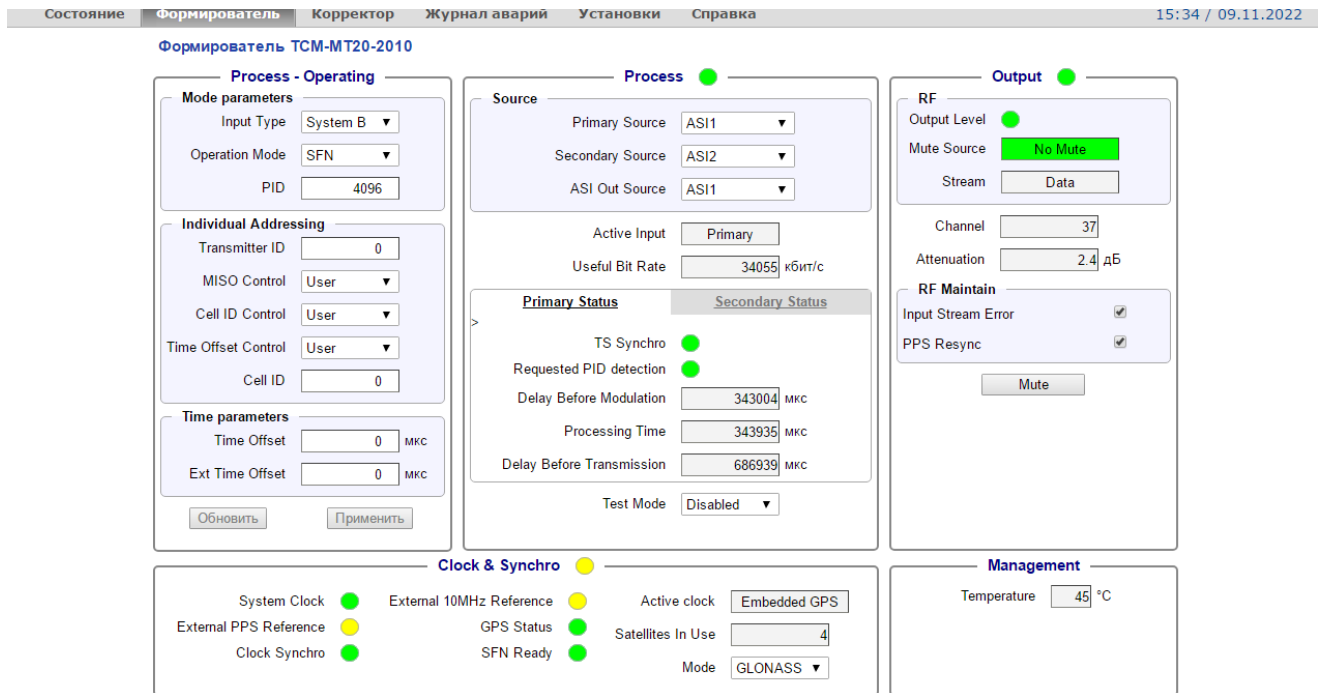


Рис. 6. Меню настроек передатчика

Настройка TTUD10/E/AC 18124/1

[Начать заново](#) | [Сокращенная настройка](#)

Монтаж и сочленение разъемов изделия проверены?	Да	Пропустить			
Включите изделие. Установите напряжение 48В	Готово	Пропустить			
Установите напряжение 12В	Готово	Пропустить			
Напряжение в КТ 48±0,5В?	48.0	Да	Пропустить		
Напряжение в КТ 12±0,1В?	12.0	Да	Пропустить		
Выберите код изделия	TTUD10/E/AC	Корректор AC-6 (SC1894)	RS-485 Водущий	Готово	Пропустить
Введите конструктивную версию	1.0	Готово	Пропустить		
Введите заводской номер	18124/1	Готово	Пропустить		
Введите дату и время	Дата: 09-11-2022	Время: 15:36:19	Системные	Готово	Пропустить
Введите пароль доступа к корректировке параметров	1234567	Готово	Пропустить		
Скорректируйте IP-адрес формирователя (192.168.*.141)	192.168.250.23	Готово	Пропустить		
Запустите ControlCast, обновите ПО формирователя	Готово	Пропустить			
Выберите режим DVB (Т/Н, Т2) (ТС)	Готово	Пропустить			
Установите режимы формирователя по умолчанию (ТС)	Готово	Пропустить			
Установите номер радиоканала	37	Готово	Пропустить		
Введите Rном макс, Вт	5.50	Рвых: 2.62	Атт: 13	Готово	Пропустить
Установите Рвых максимально близко к Rном	Рвых: 2.62	-	+	Готово	Пропустить
Амплитудная калибровка датчика Р пад. Введите реальную Рпад, Вт	Рвых: 2.62	Готово	Пропустить		
Подбор коэффициента передачи. Введите Rном макс, Вт	Рвых: 2.62	Атт: 13	Готово	Пропустить	
Установите Рвых равную Rном	Рвых: 2.62	-	+	Готово	Пропустить
Калибровка датчика Ротр. Откройте нагрузку	Готово	Пропустить			
Калибровка датчика Ротр. Введите Ротр равную Рпад, Вт	Ротр: 0.03	Рпад: 2.62	Готово	Пропустить	
Подсоедините нагрузку	Готово	Пропустить			
Коэффициенты		К1		К2	
	Рпад, Вт	100.0	-	+	290
	Ротр, Вт	100.0	-	+	111
		Нормировать		Записать	

Рис. 7. Пример меню настроек

Из выше представленных соображений становится понятным, что рано или поздно имеющееся оборудование импортного производства постепенно будет выходить из строя, а отсутствие возможности ремонта или замен вышедших из строя узлов станет невозможным ввиду отсутствия запчастей и ПО к ним. Представленное решение является наиболее актуальным и быстро реализуемым. Так как ПО и запчасти к отечественному оборудованию поставляются самим производителем.

Так же необходимо отметить одно из достоинств отечественного тюнера *RTM-575*, что в нем реализованы сразу два отдельных приемных декодера в одном корпусе, а также четыре независимых *ASI-выхода*, которые настраиваются отдельно, что значительно повышает удобство эксплуатации и возможности различных конфигураций для подключения.

Отечественное оборудование может конкурировать с импортным. По параметрам работы они аналогичны. А вот по цене они более привлекательны.

Список используемых источников:

1. RTM TRK-575 - описание и инструкция по эксплуатации.
2. Руководство по эксплуатации ТВ анализатора R&S ETC.

Elezhibiev A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunications

The possibility of import substitution of digital terrestrial television broadcasting equipment of the DVB-T2 standard on the example of broadcasting of the RTRS-1 package. Nowadays the issue of import substitution in Russian Federation is more relevant than ever because of the current Impact of sanctions on the Russian economy. Telecommunications has not spared the problem of supplying the necessary equipment. This article will propose a solution to the problem by directly replacing imported equipment with equipment manufactured in the Russian Federation.

Key words: *television broadcasting, import substitution, receiver, transmitter.*

УДК 621.396.99
ГРНТИ 47.53.99

ВОЗМОЖНОСТИ ИССЛЕДОВАНИЯ БЕСПРОВОДНЫХ ПРОТОКОЛОВ СВЯЗИ С ПОМОЩЬЮ SDR НА ПРИМЕРЕ ОБРАТНОЙ РАЗРАБОТКИ УСТРОЙСТВ, РАБОТАЮЩИХ В ДИАПАЗОНЕ LPD433

Д. М. Юраков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье показан вариант использования программно определяемого радио для выполнения обратной разработки. Последовательность решения задач по обратной разработке продемонстрирована на примере простого протокола взаимодействия между пультом дистанционного управления и радиоуправляемым реле.

USRP B210, GNU Radio, программно определяемое радио, LPD433, обратная разработка

Программно определяемая радиосистема – это концепция, согласно которой радиочастотная связь осуществляется посредством использования программного обеспечения (или прошивки) для выполнения задач обработки сигналов. Владея базовыми знаниями программирования и теории связи, можно собирать анализаторы эфира, системы передачи данных, системы вещания, а также производить обратную разработку протоколов и многое другое.

Рассмотрим обратную разработку на примере пульта дистанционного управления радиоуправляемого реле Орбита ОТ-НОС05 [1]. Производителем в характеристиках заявлено, что устройство работает на частоте 433 МГц. Предполагается, что за данной формулировкой стоит диапазон радиочастот для маломощных устройств, входящий в международную сетку промышленных, научных и медицинских частот - LPD433 [2].

В качестве программно определяемого радио для дальнейшей разработки используется USRP B210 [3], а для выполнения задач обработки сигналов выбирается объектно-ориентированная среда программирования GNU Radio [4].

Для выполнения анализа эфира требуется схема из двух блоков UHD: USRP Source, который используется в качестве связи с аппаратным обеспечением и блок QT GUI Sink. Данный блок многофункционален и имеет в наборе спектроанализатор, график водопад, осциллограф и график созвездия.

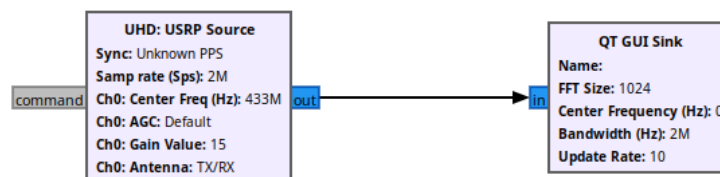


Рис. 1. Блок диаграмма для анализа эфира

Для анализа всего диапазона устанавливается центральная частота приёмника 434 МГц и `samp_rate` (переменная частоты дискретизации в программе) равный 2 МГц, чтобы захватить весь диапазон целиком. Далее

выполняется запуск программы и переключение на график водопада. Происходит нажатие на кнопку пульта дистанционного управления. На рис. 2 наблюдается, что центральная частота настройки совпала с рабочей частотой пульта ДУ радиуправляемого реле. Перейдя в просмотр графика осциллографа наблюдается использование амплитудной модуляции.

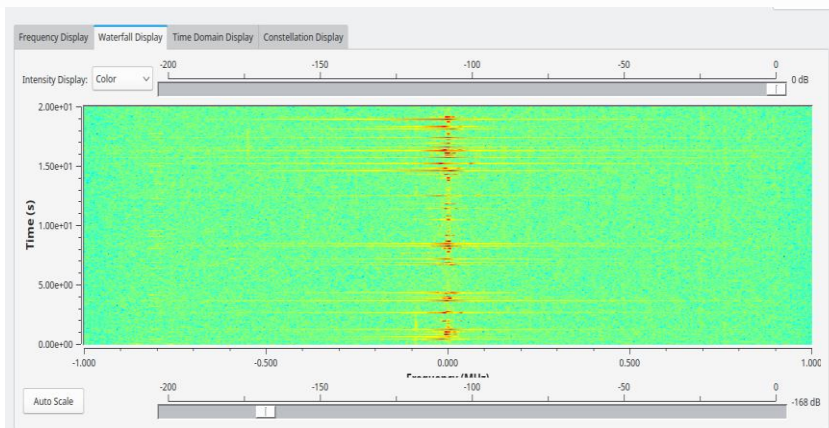


Рис. 2. Дисплей водопада (кнопка дистанционного пульта нажималась)

Для дальнейшей обработки добавляется блок Complex to Mag, который оставит только реальную составляющую. Далее выполняется запуск программы и переключение на график осциллографа (рис. 3).

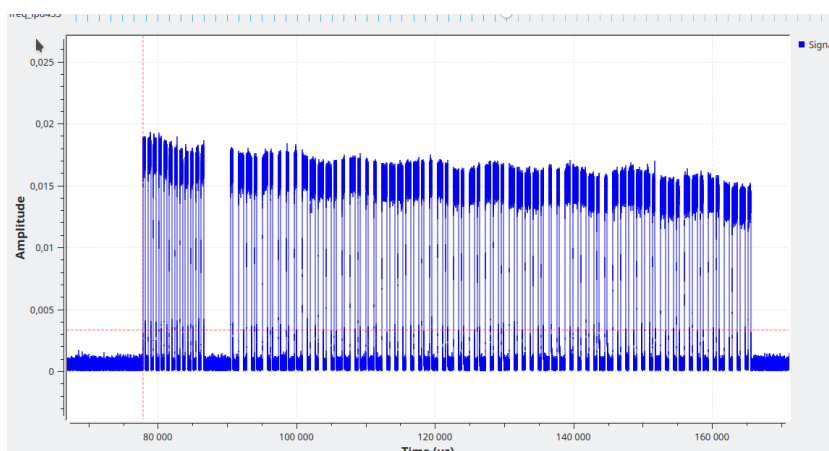


Рис. 3. Сигнал сообщения в эфире

Проанализировав несколько пакетов, делается вывод, что сообщение никак не изменяется и всегда постоянно, а следовательно шифрование не применяется. Также на осциллограмме заметен стартовый заголовок сообщения, который состоит из единиц и нулей, а после стартовый ноль для синхронизации. За ним следует само сообщение, где короткий импульс — это бит “1”, длинный два бита “1”, а короткое отсутствие импульса — это бит “0”, длинное два бита “0”. Длительность одного символа составляет 400 мкс. Длинный стартовый ноль соответствует длительности 9 бит. Если частота дискретизации равна 1 МГц, не сложно посчитать сколько отсчетов приходится на каждый бит. На рис. 4 представлена программа для демодуляции сообщения.

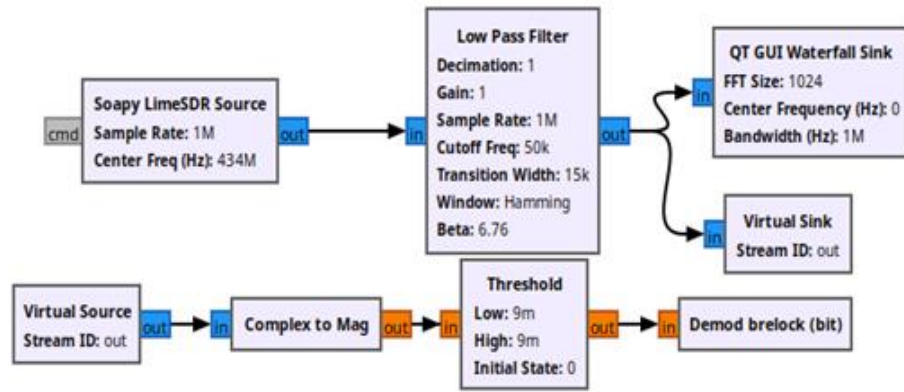


Рис. 4. Программа демодулятора сообщения

Блок Threshold при значении на входе больше порога выводит 1, меньше порога 0. Это требуется для упрощения написания демодулятора. Блок Demod brelock (bit) рукописный блок, который по количеству отсчётов не прерывающихся 1 или 0 определяет набор бит сообщения и выводит их в командную строку. Вывод блока примерно такой:

Заголовок: 1010101010101010101010

Тишина: 00000000

Пакет: 11010011010010011010011011011010011011011010010011011011011
 01001101001001101001010010010010011011011010011011011011010010010011
 01101101101001001101101101101101001101101001101101001101001101101101

Проверив сообщение побитово утверждается, что демодулятор справился с задачей безошибочно. Следующим шагом требуется написать программу генератора сигнала, которая представлена на рис. 5.

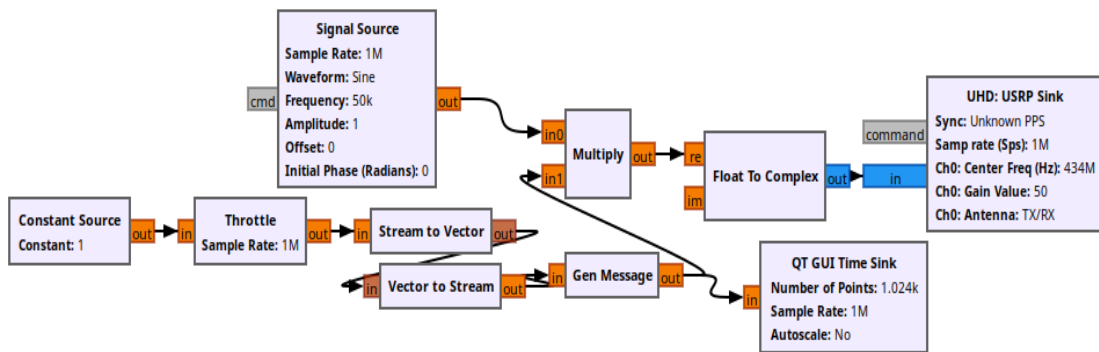


Рис. 5. Блок схема программы генератора сигнала

Выходной сигнал генератора представлен на рис. 6, что в точности соответствует исходному сигналу. После данный сигнал перемножается с источником синусоидальной волны, а результат выводится на блок UHD: USRP Sink. Воспроизведя данный сигнал в эфире, наблюдается отклик радиоуправляемого реле.

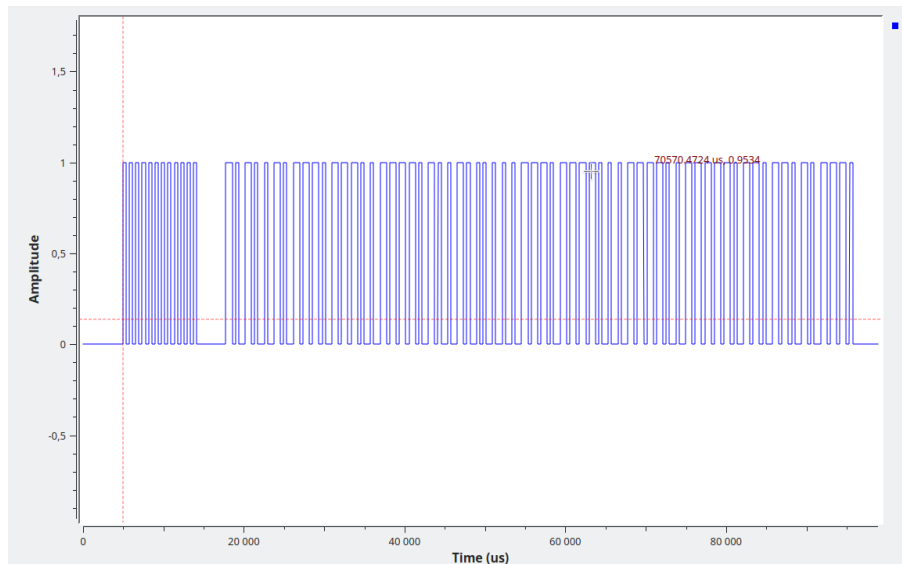


Рис. 6. Сгенерированный сигнал из битовой последовательности

В рамках данной статьи был показан процесс обратной разработки на физическом уровне одного из протоколов для сигнала в диапазоне LPD433. Для других протоколов в различных диапазонах концепция обратной разработки будет довольно схожа, и в некоторых случаях намного сложнее так как протокольная часть у каждого стандарта связи разная и эта тема за рамками обзорной статьи. В демонстрационных целях был взят простейший протокол без шифрования данных, где имелась возможность проверить работоспособность модели.

В дальнейшем по результатам данной работы планируется разработка методических материалов исключительно в образовательных целях.

Список используемых источников:

1. Орбита ОТ-HOS05 [Электронный ресурс]. URL: <https://str-mobile.ru/orbita-ot-hos05-radioupravlyаемое-rele-s-pultom-1-kanal12v/> (дата обращения 15.11.2022).
2. LPD433 [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/LPD433> (дата обращения 15.11.2022).
3. USRP B210 [Электронный ресурс]. URL: <https://www.ettus.com/all-products/ub210-kit/> (дата обращения 15.11.2022).
4. GNU Radio [Электронный ресурс]. URL: <https://wiki.gnuradio.org/index.php?title=Tutorials> (дата обращения 15.11.2022).

Yurackov D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Possibilities of researching wireless communication protocols using SDR on the example of reverse engineering of devices operating in the LPD433 band.

This paper shows a variant of using a software-defined radio to perform reverse engineering. The problem-solving sequence for reverse engineering is demonstrated using a simple interaction protocol between a remote control and a radio controlled relay as an example.

Key words: *USRP B210, GNU Radio, software defined radio, LPD433, reverse engineering.*

**Секция 2.2.
Подвижная связь и радиодоступ**

УДК 621.396
ГРНТИ 49.43.29

PROSPECTS FOR THE INTRODUCTION OF eSIM BY MOBILE OPERATORS

O. V. Glazacheva, A. A. Zaichenko, E. P. Zheltova

The Bonch-Bruевич Saint Petersburg State University of Telecommunications

This article provides outlooks for eSIM technology being gradually introduced in mobile communications. eSIM is a standard that allows you to store multiple carrier profiles on one integrated electronic device (chip) and allows you to connect devices to cellular communications without physical SIM cards. At the same time, subscriber profiles of specific telecom operators can be uploaded to eSIM via the network (Internet). The implementation of the eSIM standard simplifies the process of connecting devices such as smartphones, smart watches, portable healthcare systems and other devices to the cellular network..

eSIM, subscribers, network, mobile operators, MVNO, IoT, M2M service

Currently, almost every adult citizen of our country is a customer of a mobile operator. At the same time, there has not been a significant increase in the number of subscriber devices in the last few years. The main increase in the subscriber base of the operator companies is due to the IoT segment (Internet of Things - Internet of Things) [1]. The latter circumstance has led to an increase in the interest of mobile operators in eSIM technology, which is necessary for users of smart devices and has become popular with gadget users.

To authenticate subscribers in the mobile network, a SIM card is used (Subscriber Identification Module - subscriber identification module). However, using a familiar physical SIM card implemented in the form of a separate module is not always convenient, so the transition to eSIM (embedded SIM - embedded SIM) is currently underway. eSIM is a programmable module integrated into the chip of the device. While not all devices support this technology, however, it presents many opportunities to both end users and vendors.

The purpose of this paper is to review recent research in the field of study, to highlight a problem and controversy of introduction of eSIM by mobile operators and to establish the importance of the topic for telecommunication specialists.

One of the main advantages that many mobile operators have already implemented is the ability to get an eSIM without visiting the office. This is available to persons who have a qualified electronic signature or a simple electronic signature, the key to which was obtained during a personal appearance, as well as identified in a Single biometric system. This opportunity appeared after the amendments to the law "On Communications" came into force on June 1, 2021 [2]. Currently, especially in the context of a pandemic that has not yet ended, this advantage is very relevant. In addition, it makes more accessible the use of mobile communication services by persons with disabilities. eSIM is also convenient for end users, as it cannot be lost or broken.

The introduction of eSIM contributes to the development of competition in the mobile communications market, as a result improving the quality of service in general. The use of eSIM contributes to the emergence of MVNO (Mobile Virtual Network Operator – virtual mobile operators), as it reduces the cost of entering the market due to the absence of costs for the manufacture of a physical SIM card and logistics.

Subsequently, it is planned to implement the connection of one eSIM module to different telecom operators through the use of MEP (Multiple Enabled Profiles) technology [3].

In addition, using eSIM is an opportunity to reduce costs while roaming as the eSIM profile is much easier to replace than replacing a physical SIM card. This opens up many opportunities not only for users of smartphones, tablets, laptops, etc., but also for the development of IoT (Internet of Things). For example, IoT monitoring systems for freight transport are becoming increasingly popular. The work of GPS trackers is directly related to movement. Changing a physical SIM card in the process of moving is expensive and labor-intensive, sometimes even impossible. This problem is solved by using eSIM.

IoT implementation is a necessary and natural process. Many sectors of the economy today can no longer be imagined without the use of smart devices. In the future, their use will only increase. The concept of a smart city, which is currently developing, is based on the use of smart devices that interact using radio technologies, including IoT. Physical M2M (Machine-to-Machine – Machine-to-machine interaction) SIM cards are usually made of more expensive materials than conventional SIM cards due to the requirements for thermal and vibration loads. Installing SIM cards in a large number of devices is a time-consuming and expensive process. This problem is also solved by using eSIM. In addition, the eSIM module is more compact than the slot for a physical SIM card, so the use of eSIM makes it possible to produce more compact models. In addition, it simplifies the task of producing a sealed case.

When using eSIM in gadgets, a PULL model is used (loading the eSIM profile on the initiative of the client, as a rule, after scanning the QR code). When configuring M2M eSIM, a PUSH model is used. Figure 1 shows the architecture of interaction between the server and the device when adding an eSIM profile [4].

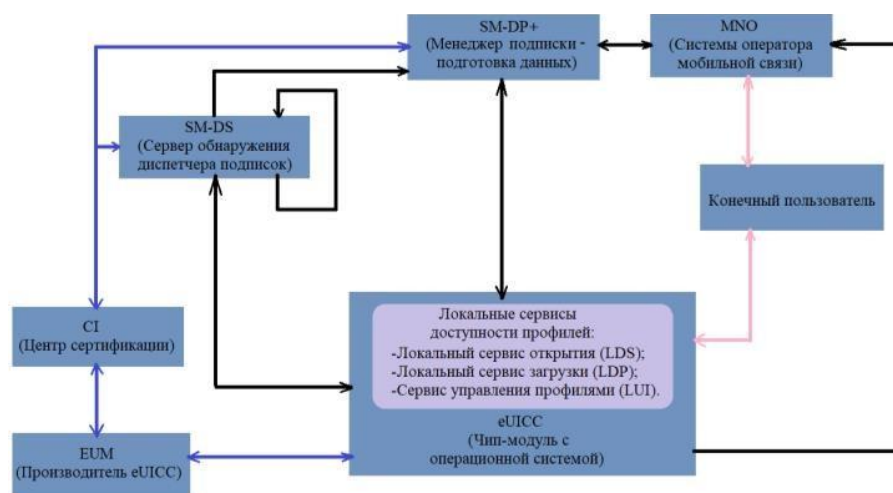


Fig. 1. Architecture of the PULL model

Despite the fact that eSIM is already available to customers of many telecom operators, this technology still has disadvantages that need to be solved for comfortable use of the technology. For example, at the time of downloading the eSIM profile, the device must be connected to the Internet. When using technology in a gadget, this does not seem to be a significant problem the user can connect to a Wi-Fi network, use the Internet from another SIM card in the device, etc. When connecting a large number of IoT devices, moving the device into the Wi-Fi network coverage area (or deploying a Wi-Fi network to the location of IoT devices) can be difficult or even impossible.

Currently, to eliminate this difficulty, as a rule, the first connection of the device to the mobile network is made at the factory, at the time of manufacture, then, after the configuration is completed, the device switches to bootstrap mode (i.e. boot mode in which the device is ready to receive eSIM M2M service commands) [5]. Connecting even before the device is sold has a positive effect on the quality of the final product it minimizes the number of defective devices on the market, but limits competition among mobile operators the user will have to conclude an agreement with the operator company with which the vendor signed the contract.

According to the general opinion of telecommunication specialists in Russia, the introduction of this promising technology will lead to the evolution of mobile communications in general [5] as it is gradually replacing physical plastic SIM cards in this country and it is spreading fast due to its easy shopping, security possibilities, etc. Switching to eSIM significantly enhances the security of online banking, instant messengers and other data. This might simplify the users' life, because this new technology enables not to visit the offices of cellular companies in order to switch between networks of different operators. On the other hand, how to fix or register the SIM card number in the Russian Federation remains unclear [5].

At the moment, all well-known operators have already implemented eSIM connectivity as a service. In the online application or in the offline store, the eSIM connection service is offered to clients free of charge. The transition process takes no more than 15 minutes. It is worth noting that after activating the eSIM, the standard SIM card is no longer active.

For the above mentioned reasons, the emergence of new opportunities for the production of devices, the technology has stimulated an increase in competition due to the cheaper entry of new mobile operators (virtual operators) into the market. Originally developed for use in smart devices, the technology is not only successfully used in the M2M segment simplifying operation and maintenance, allowing for more compact devices, solving the problem of using devices in roaming, but has also found application in gadgets. Besides, eSIM technology makes it possible to make both economic and social spheres more comfortable by making it possible to conclude a contactless contract with a telecom operator (previously this was impossible not only because of the difficulty of identifying the client, but also because of the need to obtain a physical SIM card).

Thus, eSIM technology has significant potential to enhance communication process, making it more efficient and smooth. Therefore, it requires further consideration and highly qualified specialists.

Reference:

1. Statistika otrasli: Ministerstva tsifrovogo razvitiya, svyazi i massovykh kommunikatsiy RF. URL: <https://digital.gov.ru/ru/pages/statistikaotrasli/> (access date: 16 Oct., 2022).
2. Maya Goraib. eSIM Development: A revolution in connectivity. Inside Telecom International Telecoms Business Magazine. Oct 07 2022. URL: <https://insidetelecom.com/the-rise-of-esim-connectivity-revolution-2/> (access date: 10 Nov., 2022).
2. Supporting multiple enabled profiles on single embedded subscriber identity module (eSIM) chip. URL: <https://uspto.report/patent/grant/10,708,761> (access date: 19.10.2022).
3. RSP Architecture Version 3.0 28 March 2022 – GSM Association Official Document SGP.21, 2022, 144 p.
4. eSIM. Copyright 2022 GSM Association. URL: <https://www.gsma.com/esim/> (access date: 21 Oct., 2022).
5. How Russian operators treat eSIM. URL: <https://24gadget.ru/1161067393-kak-rossiyskie-operatory-otnosyatsya-k-esim.html> (access date: 10 Nov., 2022).

Глазачева О. В., Зайченко А. А., Желтова Е. П.

*Санкт-Петербургский Государственный университет телекоммуникаций им. проф.
М. А. Бонч-Бруевича*

Перспективы внедрения eSIM мобильными операторами.

В данной статье описывается потенциал технологии eSIM, постепенно внедряемой в мобильную связь. eSIM – это стандарт, который позволяет хранить несколько профилей операторов связи на одном интегрированном электронном устройстве (чипе) и позволяет подключать устройства к сотовой связи без физических SIM-карт. В то же время профили абонентов конкретных операторов связи могут быть загружены в eSIM через сеть (Интернет). Внедрение стандарта eSIM упрощает процесс подключения к сотовой сети таких устройств, как смартфоны, умные часы, портативные медицинские системы и другие устройства.

Ключевые слова: *eSIM, абоненты, сеть, мобильные операторы, MVNO, IoT, M2M service*

УДК 621.391.1
ГРНТИ 49.43.29

АНАЛИЗ ПРИНЦИПОВ РАБОТЫ ФУНКЦИОНАЛА ANR В СЕТЯХ LTE С ПОДДЕРЖКОЙ SON

М. Т. Аскеров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время важным направлением в области мобильной связи является разработка отечественных решений как в части радиооборудования LTE, так и в части софта. В связи с этим становится актуальной задача анализа принципов функционирования существующих решений зарубежных вендоров и разработки соответствующих алгоритмов и методов, которые впоследствии могут быть реализованы отечественными производителями оборудования.

SON, ANR, LTE, мобильные сети, eNB, 3GPP, NRT, PCI

Самоорганизующаяся сеть (SON – Self Organizing Network) – это автоматизированная адаптивная сеть, способная выполнять набор функций с минимальным вмешательством человека [1]. Согласно концепции 3GPP технические решения для сетей SON можно разделить на три категории по решаемым задачам [2]:

- самоконфигурирование сети (SELF-Configuration);
- самооптимизация сети (SELF-Optimisation);
- самовосстановление сети (SELF-Healing).

В данной работе рассматривается одна из ключевых функций сетей SON – автоматическое управление взаимодействием с соседними сотами (ANR – Automatic Neighbor Relations), которая обеспечивает уменьшение ручной работы технического персонала оператора сети LTE при настройке списка соседних сот во вновь развернутых eNB и при оптимизации радиосети [3].

Модуль ANR автоматизирует все операции добавления и удаления соседей. ANR настраивает список соседей вновь развернутого eNB и периодически обновляет его при дальнейшем функционировании базовой станции в составе сети. Этот вариант использования относится к двум категориям SON: самоконфигурация и самооптимизация (рис. 1 [4]).



Рис. 1. Функции ANR

На рис. 2 представлен алгоритм автоматического формирования связей между соседними сотами реализуемый функцией Automatic Neighbor Relations (ANR) в сетях LTE с поддержкой SON.

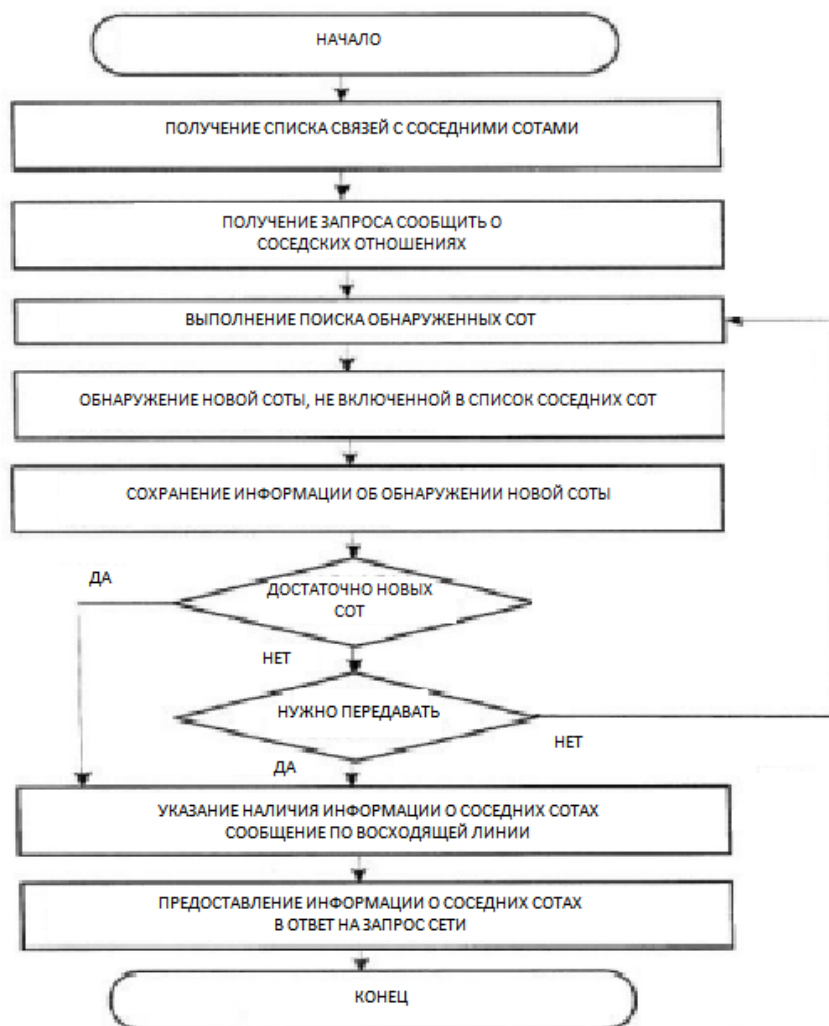


Рис. 2. Алгоритм автоматического формирования связей между соседними сотами

Основные понятия, связанные с ANR:

- Список соседних сот (NCL – Neighboring cell list).

NCL eNodeB содержат информацию о внешних сотах, которые обслуживаются окружающими базовыми станциями, отличными от этого eNodeB. eNodeB имеет NCL intra-RAT (для внутрисистемного хэндовера) и NCL inter-RAT (для межсистемного взаимодействия сот). В современных гетерогенных сетях обычно применяются следующие intra-RAT списки соседних сот: NCL GERAN, NCL UTRAN, NCL CDMA2000 (FDD) или NCL NG-RAN.

NCL intra-RAT:

- NCL E-UTRAN: включает глобальные идентификаторы сот E-UTRAN (ECGI – E-UTRAN cell global identifier) внешних сот E-UTRAN, идентификаторы физических сот (PCI – physical cell identifier) и частоты E-UTRAN.

NCL Inter-RAT:

- NCL GERAN: включает глобальные идентификаторы сот (CGI) внешних сот GERAN, идентификационные коды базовых приемопередающих станций (BSIC) и частоты GERAN.
- NCL UTRAN: включает CGI внешних сот UTRAN, коды скремблирования и частоты UTRAN.
- NCL NG-RAN: включает CGI внешних сот NG RAN, коды скремблирования и частоты NG-RAN.
- NCL CDMA2000 (FDD): включает CGI внешних сот CDMA2000, PnOffset и частоты CDMA2000.

Функционал ANR может автоматически добавлять внешние соты в NCL, удалять внешние соты из NCL или обновлять информацию о внешних сотах в NCL.

- Таблица отношений соседей (NRT – Neighboring Relation Table).

NRT содержит информацию о соседских отношениях сот. Пример записи основной информации в intra-RAT NRT приведен в таблице 1 [5].

ТАБЛИЦА 1. Пример записи основной информации в intra-RAT NRT

SN	LCI	Target Cell PLMN	eNodeB ID	Cell ID	No Remove	No HO
1	LCI#1	46001	eNodeB ID#1	Cell ID#1	FORBID_R MV_ENUM	FORBID_H O_ENUM
2	LCI#1	46001	eNodeB ID#2	Cell ID#2	PERMIT_R MV_ENUM	PERMIT_H O_ENUM
3	LCI#1	46001	eNodeB ID#3	Cell ID#3	FORBID_R MV_ENUM	FORBID_H O_ENUM

В данной таблице показаны следующие параметры: идентификатор локальной соты (LCI); PLMN целевой соты – идентифицирует наземную сеть мобильной связи общего пользования (PLMN) оператора, которому принадлежит целевая сота; ID eNodeB – идентифицирует eNodeB, который обслуживает целевую соту, Cell ID – идентифицирует целевую соту; No Remove – указывает, может ли ANR удалить соседские отношения из NRT; No HO – указывает, можно ли использовать отношения соседства для передачи обслуживания.

Ключевые параметры ANR в реализации Huawei представлены в таблице 2 [5].

ТАБЛИЦА 2. Ключевые параметры ANR

ID	Описание	Диапазон значений; Рекомендованное значение
NcellHoStat Num	Пороговое значение общего количества попыток передачи обслуживания в соседнюю соту для удаления соседских отношений из NRT на основе успешного хэндовера	1~10000; 20

StatisticPeriod	Период измерения успешности хэндовера для удаления соседских отношений.	1~10080; 1440 мин
FastAnrRprt Amount	Количество периодических отчетов об измерениях, отправляемых для быстрого ANR.	r1, r2, r4, r8, r16, r32, r64, Infinity; r4(4)
FastAnrRprt Interval	Интервал периодических отчетов об измерениях, отправляемых для быстрого ANR	120 мс, 240 мс, 480 мс, 640 мс, 1024 мс, 2048 мс, 5120 мс, 10240 мс, 1 мин, 6 мин, 12 мин, 30 мин, 60 мин
FastAnrCheck Period	Таймер быстрой проверки ANR. Когда таймер истекает, eNodeB автоматически проверяет, следует ли отключить быстрое ANR.	1~10080; 60 мин
FastAnrRsrpThd	Пороговое значение RSRP intra-RAT быстрого ANR для автоматического добавления внешней соты eNodeB.	-130~-70; -102 дБм
FastAnrIntraRat MeasUeNum	Максимально допустимое количество UE, выполняющих intra-RAT измерения быстрого ANR.	1~200; 5
FastAnrInterRat MeasUeNum	Максимально допустимое количество UE, выполняющих inter-RAT измерения быстрого ANR.	1~200; 5
FastAnrIntraRat UeNumThd	Пороговое значение, при превышении которого eNodeB входит в состояние мониторинга intra-RAT быстрого ANR.	1~10000; 20
FastAnrInterRat UeNumThd	Пороговое значение, при превышении которого eNodeB входит в состояние мониторинга inter-RAT быстрого ANR.	1~10000; 20
StatisticPeriod ForNRTDel	Период оценки удаления взаимосвязи соседства intra-RAT, в течение которого eNodeB собирает статистику о том, была ли соседняя сота intra-RAT обнаружена UE, и о количестве хэндоверов в соседнюю соту intra-RAT.	1~50400; 1440 мин
StatisticNum ForNRTDel	Пороговое значение общего количества хэндоверов от локальной соты ко всем соседним сотам intra-RAT для удаления соседских отношений из полной intra-RAT NRT или периодического удаления	1~10000; 50
StatPeriodCoeff	Количество последовательных периодов оценки, заданных параметром StaPeriodForIRatNRTDel или StatisticPeriodForNRTDel, для удаления избыточных взаимосвязей соседей.	1~20; 4

Данные, полученные в результате анализа принципов работы функционала ANR, позволяют разработать алгоритмы, которые могут быть использованы

отечественными производителями при создании программного обеспечения для сетей мобильной связи LTE. Дальнейшие исследования в данном направлении будут посвящены разработке блока имитационной модели сети LTE, реализующего функционалы SON.

Список используемых источников:

1. Maria Gonzalez, «Self-Organizing Networks», June 2018, pp. 3-9.
2. 3GPP TS 32.500 «Telecommunication management; Self-Organizing Networks (SON); Concepts and requirements»
3. 3GPP TS 32.511 «Automatic Neighbour Relation (ANR) management; Concepts and requirements»
4. Pradeepa Ramachandra, Kristina Zetterberg, Fredrik Gunnarsson, Reza Moosavi, Sakib Bin Redhwan, Stefan Engström, Ericsson, «Automatic Neighbor Relations (ANR) in 3GPP NR», 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW): 7th International Workshop on Self-Organizing Networks (IWSON), pp. 125-129.
5. Huawei technologies co., LTD, eRAN15.1 Draft A (2019-01-05), «ANR Management Feature Parameter Description»

Askerov M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of the principles of ANR functionality in LTE networks with SON support. Currently, an important direction in the field of mobile communications is the development of domestic solutions both in terms of LTE radio equipment and in terms of software. In this regard, the task of analyzing the principles of functioning of existing solutions of foreign vendors and developing appropriate algorithms and methods that can subsequently be implemented by domestic equipment manufacturers becomes urgent.

Key words: SON, ANR, LTE, mobile networks, eNB, 3GPP, NRT, PCI.

УДК 621.396.99
ГРНТИ 49.43.29

ПРИНЦИП ПОСТРОЕНИЯ СИСТЕМЫ СВЯЗИ ДЛЯ РОБОТЕХНИЧЕСКИХ КОМПЛЕКСОВ, ФУНКЦИОНИРУЮЩИХ В УСЛОВИЯХ ИНТЕНСИВНЫХ ПОМЕХ

М. С. Бабенко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время в приграничных районах РФ наблюдаются нарушения работы систем связи БПЛА гражданского назначения, вызванные интенсивными преднамеренными помехами, создаваемыми комплексами военного назначения.

Традиционные методы повышения помехозащищенности не позволяют добиться необходимого уровня помехоустойчивости системы связи. Предлагаемый метод параллельной передачи пакетов по нескольким каналам обмена данными, построенный на основе комбинирования различных радиотехнологий, в отличие от традиционных методов повышения помехозащищенности позволяет повысить устойчивость системы к преднамеренным помехам и обеспечить возможность управления полетами БПЛА в сложной помеховой обстановке.

система связи, помехи, помехозащищенность, БПЛА

Существует достаточно большое количество методов повышения помехозащищенности радиоканалов (рис. 1) [1], [2].

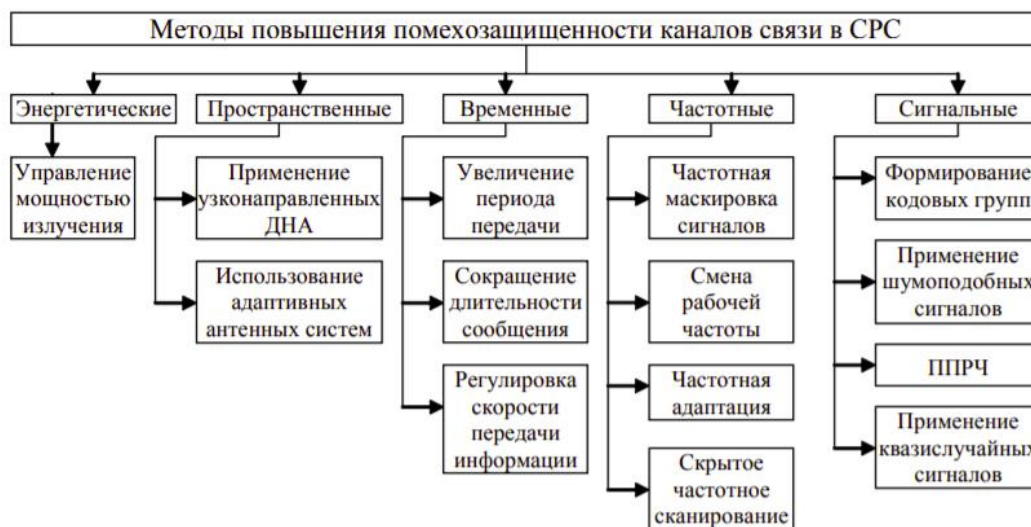


Рис. 1. Основные методы повышения помехоустойчивости в системах связи

Определение конкретного метода, который необходимо использовать при передаче данных по радиоканалу в каждом конкретном случае определяется с учётом сложности реализации задач, а также доступных технических возможностей. Чаще всего наибольшей эффективностью обладают системы связи, использующие несколько методов повышения помехозащищенности.

Анализ результатов применения традиционных методов помехоустойчивости, показывает, что они позволяют снизить порог отношения сигнал/шум (SNR) на несколько дБ (рис. 2) [3].



Рис. 2. Сравнение помехоустойчивости систем связи, с применением и без применения помехоустойчивых кодов

На рис. 3 приведена зависимость отношения сигнал/шум от вероятности ошибки для различных типов помехоустойчивых кодов [3].

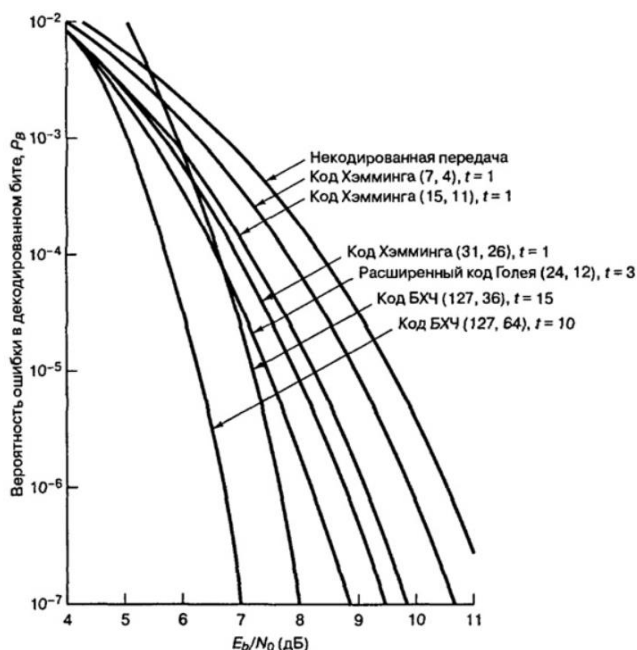


Рис. 3. Зависимость отношения сигнал/шум от вероятности ошибки для различных типов помехоустойчивых кодов

Все помехоустойчивые коды могут исправлять только ограниченное количество ошибок t . Однако в реальных системах связи часто возникают

ситуации сгруппированных ошибок, когда в течение непродолжительного времени количество ошибок превышает t . Но, даже каскадное применение различных кодов, в сочетании с глубоким перемежением не способно обеспечить работу канала связи при отрицательных значениях SNR. Вместе с тем, применение преднамеренных помех выводит SNR в канале к глубоко отрицательным значениям, достигающим -20 дБ.

Таким образом, становится актуальной задача разработки практически реализуемой структуры системы связи, способной работать при наличии интенсивных преднамеренных помех, действующих одновременно, в нескольких диапазонах частот.

Рассмотрим типовую структуру системы связи для обеспечения управления несколькими БПЛА с наземного или воздушного (корабельного) пункта управления (ПУ).

Информация от БПЛА к пункту управления – параметры полета, состояние различных узлов и агрегатов, подтверждение принятой от пункта управления информации, небольшой объем данных с полезной нагрузки передается по узкополосному каналу связи (НСОД – низкоскоростная система обмена данными). Большой объем данных от полезной нагрузки (например, фото и видео) передаются с помощью широкополосного канала (ВСОД – высокоскоростная система обмена данными). От пункта управления к БПЛА передаются команды управления БПЛА и полезной нагрузки и изменения полетного задания [4].

Чаще радиоканал является дуплексным или полудуплексным, может быть широкополосным и узкополосным. Архитектура радиоканала может быть разнообразной – от «точка-точка» до «mesh». Также иногда для управления БПЛА используют системы сотовой связи.

Для кардинального повышения помехоустойчивости системы связи предлагается модернизировать действующую систему связи следующим образом (рис. 4).

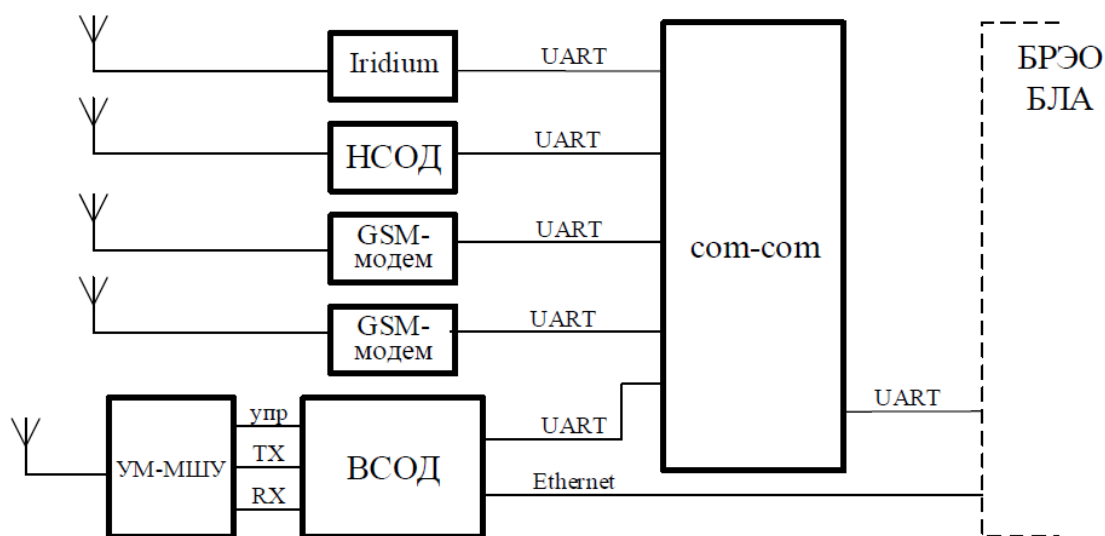


Рис. 4. Архитектура перспективной системы связи

В каждом направлении осуществляется распараллеливание передаваемых пакетов и добавление к каждому пакету уникального номера

Далее, пакеты передаются одновременно и независимо по каждому из каналов. В случае отключения или подавления одного из каналов – передача осуществляется по сохранившимся.

На приемной стороне осуществляется контроль целостности принятых пакетов и сшивка исходной последовательности, согласно порядку уникальных номеров пакетов.

Т.к. в системе используются разнородные каналы связи, работающие в различных диапазонах электромагнитного спектра, их одновременное подавление представляется проблематичным.

Система будет работать до тех пор, пока хотя бы в одном канале отношение сигнал/шум сохраняется выше порога.

В данной работе описаны методы повышения помехоустойчивости систем радиосвязи, выполнен анализ характеристик существующей системы связи и предложен метод модернизации системы передачи данных за счет параллельной передачи пакетов по нескольким каналам обмена данными, который позволяет повысить устойчивость системы к преднамеренным помехам.

Актуальность задачи исследования и последующей модернизации системы связи в первую очередь обусловлена следующими факторами:

- как с экономической, так и с технической точки зрения более разумным является модернизация системы с целью улучшения ее характеристик, чем построение новой системы с нуля;

- улучшенная система связи позволит выполнять задачи, решение которых с использованием существующей системы невозможно или затруднительно;

- разработанные в ходе работы модели и алгоритмы в дальнейшем можно использовать в других существующих системах или при разработке новых.

Список используемых источников:

1. Варгаузин В., Цикин И. Методы повышения энергетической и спектральной эффективности цифровой радиосвязи. — СПб.: БХВ- Петербург, 2013. — 352 с.

2. Борисов В.И. Помехозащищенность систем радиосвязи: основы теории и принципы реализации / В.И Борисов. – М.: Наука, 2009. – 358 с.

3. Теоретические основы цифровой связи. Учебные материалы ОКСО 210000. Электронная техника, радиотехника и связь. Лекции для преподавателей и студентов ВУЗ. URL:<https://siblec.ru/telekommunikatsii/teoreticheskie-osnovy-tsifrovoj-svyazi> (дата обращения: 14.11.2022).

4. Применение беспилотных летательных аппаратов в гражданских целях [Электронный ресурс] URL: http://www.uav.ru/articles/civil_uav_th.pdf (дата обращения: 14.11.2022).

5. Боев Н.М, Шаршавин П.В., Нигруца И.В. Построение систем связи беспилотных летательных аппаратов для передачи информации на большие расстояния // Известия ЮФУ. Технические науки. 2014. №3 (152). URL: <https://cyberleninka.ru/article/n/postroenie-sistem-svyazi-bespilotnyh-letatelnyh-apparatov-dlya-peredachi-informatsii-na-bolshie-rasstoyaniya> (дата обращения: 14.11.2022).

Babenko M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Principle of building a communication system for robotic complexes operating in conditions of intense interference

Currently, in the border areas of the Russian Federation, there are violations of the communication systems of civilian UAVs caused by intense intentional interference created by military complexes. Traditional methods of increasing noise immunity do not allow to achieve the necessary level of noise immunity of the communication system. The proposed method of parallel transmission of packets over several data exchange channels, built on the basis of combining various radio technologies, unlike traditional methods of increasing noise immunity, makes it possible to increase the system's resistance to intentional interference and provide the ability to control UAV flights in a complex interference environment.

Key words: *UAV, communication system, interference, noise immunity.*

УДК 623.746.4-519

ГРНТИ 49.03.03

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИСТЕМ СВЯЗИ OCUSYNC И LIGHTBRIDGE, ПРИМЕНЯЕМЫХ В БПЛА КОМПАНИИ DJI

Е. В. Бабурин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В рамках данной работы выполнен сравнительный анализ систем передачи данных Lightbridge и Ocusync, используемых беспилотными летательными аппаратами компании DJI. Проведен анализ программно-аппаратных решений и определены параметры радиоканалов, с целью дальнейшего исследования их помехозащищенности.

БПЛА, DJI, Ocusync, Lightbridge

Признанным лидером по производству и продаже легких беспилотных авиационных систем является частная китайская компания DJI, в 2022 году доля её продаж на мировом рынке составила около 72–75% [1]. Поскольку на территории РФ БПЛА DJI активно используются для решения различных задач гражданского и военного назначения, представляет интерес исследование помехозащищенности систем передачи данных Lightbridge и Ocusync, применяемых этими БПЛА. На первом этапе данного исследования необходимо определить параметры данных систем, а также их потенциальные возможности.

Ключевые особенности систем передачи данных Ocusync и Lightbridge.

OcuSync и Lightbridge – это более надежные альтернативы системам связи на основе Wi-Fi, применяемым в так называемых «БПЛА потребительского класса».

Lightbridge – это программно-аппаратное решение. При разработке аппаратной части изначально применялись ПЛИС (FPGA). Позже DJI перешла на использование заказных микросхем (ASIC). Разработка ASIC требует более высоких начальных инвестиций, чем применение FPGA, при этом затраты ресурсов на разработку с использованием FPGA ниже, чем при использовании ASIC. Таким образом, компания старалась снизить себестоимость модулей связи при большом объеме производства, однако из-за этого возможность обновления существенно ограничилась. Следствием данного подхода к разработке является проблема совместимости – покупатель БПЛА одного поколения производства, как Phantom 3 и Inspire 1 может использовать одно и то же мобильное приложение DJI GO для подключения к пульту управления и дальнейших полетов. Но, для управления, например, Inspire 2, оператор должен установить другое приложение DJI GO4, которое привязано к новой аппаратной части БПЛА.

Ocusync – технология, основанная исключительно на уникальном программном обеспечении. Аппаратная часть этой системы связи (по сути SDR – Soft Defined Radio) является универсальной для целого ряда моделей БПЛА, что позволяет DJI снизить затраты на оборудование и обеспечить возможность

периодического обновления ПО при выявлении проблем с текущей версией или появлении новых функциональностей.

Сравнение характеристик систем связи БПЛА компании DJI.

Характеристики систем передачи данных OcuSync и Lightbridge на примере наиболее распространенных БПЛА DJI приведены в таблице 1 [3].

ТАБЛИЦА 1. Сравнение характеристик систем связи БПЛА DJI

	Mavic 2	Mavic 3	Inspire 2	Phantom 4 Advanced
Системы передачи видео	OcuSync 2.0	OcuSync 3.0	Lightbridge 2	Lightbridge
Частота, ГГц	2,4	2,4 и 5,8	2,4 и 5,8	2,4
Модуляция	OFDM	OFDM	OFDM	COFDM
Ширина полосы, МГц	10/20	10/20/40	10/20	10/20
Скорость передачи, Мбит/с	12	50	12	30-100
Дальность передачи, м / Мощность передатчика (ЭИИМ), дБм	FCC: 7000 / 26 CE: 4000 / 20 SRRC: 4000 / 20 MIC: 4000 / 200	FCC: 15000 / 26 CE: 8000 / 20 SRRC: 8000 / 20 MIC: 8000 / 20	FCC: 7000 / 23 CE: 3500 / 17 SRRC: 4000 / 20	FCC: 7000 / 23 CE: 3500 / 17 SRRC: 4000 / 20
Качество трансляции, р	ПУ: 720/1080 Очки DJI Goggles: 720/1080 Очки DJI Goggles RE: 720/1080	ПУ: 1080	-	-
Кадров в секунду	30	30/60	30 при 720р	60 при 1080р
Макс. битрейт трансляции, Мбит/с	100	5,5 (Пульт RC-NI) 15 (Пульт DJI RC Pro) 80 (Wi-Fi 6)	100	100
Задержка сигнала, мс	120-130	120-130	220	160-220

Примечание: CE (Европа, Россия в том числе), SRRC (континентальный Китай), FCC (США), MIC (Япония) – это стандарты сертификации конкретного региона, в соответствии с которыми программно ограничивается максимальная выходная мощность передатчиков в зависимости от геолокации БПЛА.

Анализ спектра Ocusync.

Как и Lightbridge, Ocusync использует OFDM-сигнал (Orthogonal frequency-division multiplexing – мультиплексирование с ортогональным частотным разделением каналов) для передачи видео и псевдослучайную перестройку

рабочей частоты (ППРЧ) (англ. FHSS – frequency-hopping spread spectrum) для канала управления в одном и том же частотном диапазоне. На рис. 1 приведена спектральная картина, которую можно наблюдать от момента включения БПЛА и до момента обнаружения «чистого» канала.

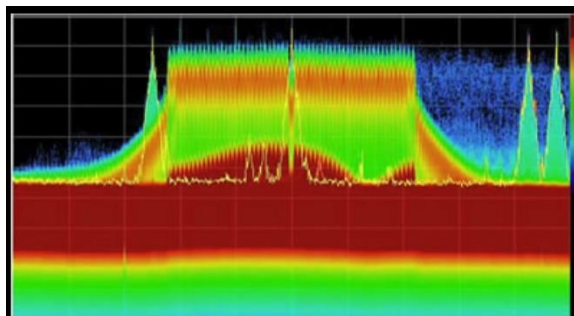


Рис. 1. Спектрограмма, полученная на этапе синхронизации системы *Ocusync*

Несущая OFDM – это множество маленьких поднесущих в центре. Видео останавливается на этом канале и остается там на протяжении всего полета БПЛА. Смещение несущей, возможно лишь в двух случаях: при наличии помех или если пользователь сменит канал вручную [2]. Однако, при нормальных условиях БПЛА выберет один канал при запуске и будет оставаться на нём в течении всего полета. Вокруг видео-сигнала OFDM отображается сигнал управления ППРЧ.

На рис. 2 изображено спектральное представление постоянных пакетов данных канала управления, которые перескакивают через всю полосу спектра.

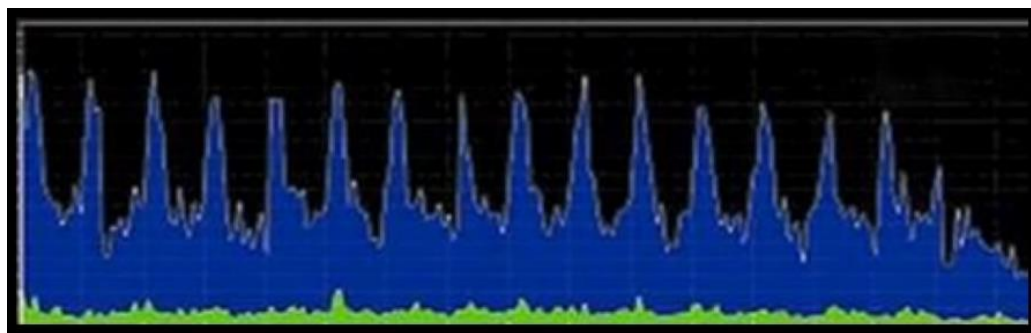


Рис. 2. Сигнал управления (ППРЧ)

Синие пики – это исторические положения сигнала, а зеленые пики – текущее положение несущей. Перестройка происходит случайным образом, поэтому предугадать частоту сигнала управления невозможно.

Сигнал управления постоянно перемещается вокруг и поверх видео-сигнала OFDM. Как и *Ocusync*, так и в *Lightbridge* системы передачи данных и сигналов управления объединены.

Если посмотреть на спектр *Ocusync*, то можно увидеть красную массу OFDM в центре (рис. 3).

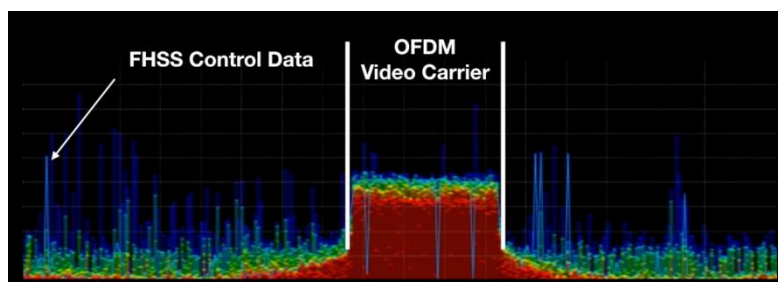


Рис. 3. Полихромная диаграмма спектра *Ocusync* (полученная в режиме накопления данных)

Это основная несущая, которая передает HD-видеосигнал от БПЛА на наземный пульт управления.

На рис. 3 синие пики, которые находятся вокруг основной несущей OFDM – это сигналы ППРЧ, которые «прыгают» вокруг канала управления. Светло-синие пики – это текущие положения сигнала, а темно-синие – предыдущие положения, где находилась несущая до перестройки частоты.

Можно заметить, что иногда сигнал ППРЧ перескакивает через основной канал, на котором идет передача видео. Но это не имеет критического значения, потому что смена частоты происходит так быстро, что даже если информация не будет получена, сигнал уже перейдет на следующую позицию, и этот пакет будет принят пультом дистанционного управления или дроном (в зависимости от направления передачи).

Сравнение спектра *Ocusync* и *Lightbridge*.

На рис. 4 показаны спектры сигналов *Ocusync* и *Lightbridge*.

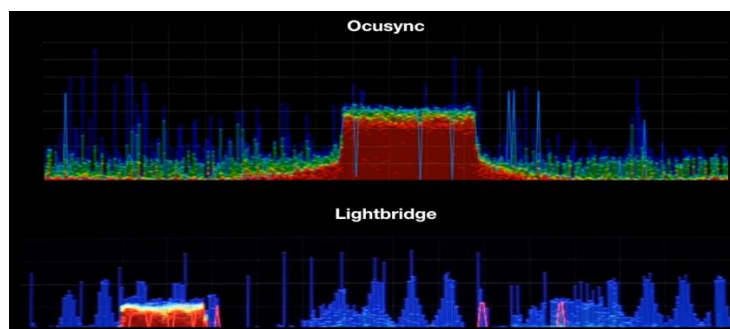


Рис. 4. Полихромная диаграмма спектра *Ocusync* и *Lightbridge* (полученная в режиме накопления данных)

Визуально спектры очень похожи. Поэтому можно сделать вывод об использовании в данных системах очень похожих радиосигналов и скорее всего основная разница между системами заключается в используемых протоколах, которые являются проприетарными.

Проведенный анализ параметров оборудования, принципов построения системы связи и спектров сигнала показал, что системы передачи данных *Ocusync* и *Lightbridge* очень похожи. С точки зрения аппаратно-программной реализации система *Ocusync* дешевле и обладает меньшими габаритами. Тем не менее система *Lightbridge* до сих пор применяется в более крупных и дорогостоящих БПЛА. Такие БПЛА показывают практически идентичную

производительность, меньшую задержку и большую дальность передачи сигнала [4]. Вопрос помехозащищенности рассмотренных систем требует отдельного изучения, этому будет посвящена дальнейшая работа в данном направлении.

Список используемых источников:

1. Новый проект [Электронный ресурс] Главная страница – URL: <https://newprospect.ru/news/articles/drony-idut-na-vzlet> (дата обращения 13.11.2022).
2. Боев Н.М. Адаптивное изменение параметров цифровых систем связи комплексов беспилотных летательных аппаратов// 22-я Международная Крымская конференция "СВЧ-техника и телекоммуникационные технологии", 10–14 сент., 2012 г.: материалы конф.: в 2 т. Т.1.
3. DJI [Электронный ресурс] Главная страница – URL: <https://www.dji.com/ru> (дата обращения 13.11.2022).
4. IEEE Communication magazine, Wireless Communication Using Unmanned Aerial Vehicles (UAVs): Optimal Transport Theory for Hover Time Optimization, September 2017.

Baburin E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Comparative analysis of oculusync and lightbridge communication systems used in DJI UAVs. As part of this work, a comparative analysis of the Lightbridge and Ocusync data transmission systems used by DJI unmanned aerial vehicles has been performed. The analysis of software and hardware solutions was carried out and the parameters of radio channels were determined in order to further study their noise immunity.

Key words: UAV, DJI, Ocusync, Lightbridge.

УДК 654.165
ГРНТИ 49.43.29

ОЦЕНКА РАДИОПОКРЫТИЯ СЕТЕЙ 5G С ЦИФРОВЫМИ МОДЕЛЯМИ МЕСТНОСТИ В СРЕДЕ MATLAB

О. П. Добрая

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича.

Мир развивается, появляется всё больше технологий, потребности пользователей мобильной связи растут и, соответственно, для реализации настоящих и будущих внедрений требуется введение надлежащих средств для обслуживания данных сервисов, такой технологией на данный момент является сеть 5 поколения.

eMBB, сотовая связь, URLLC, mMTC, 5G, радиопокрытие, GMTEd2010, Matlab

Текущие сети 4G не выдерживают требований, выдвигаемых новыми сценариями применения. Кроме плотности подключений и пропускной способности, задержки в сетях 4G довольно велики.

На смену 4G приходит 5G (от англ. fifth generation — пятое поколение).

Основные услуги, которые будут реализованы благодаря внедрению нового поколения [1]:

1. eMBB (enhanced Mobile Broadband) - сверхширокополосная мобильная связь;
2. URLLC (Ultra-Reliable Low Latency Communication) - сверхнадежная связь с низкими задержками;
3. mMTC (Massive Machine-Type Communications), массовая межмашинная связь.

Отсюда вытекают требования к сетям 5G [1]:

1. Пропускная способность сети до 20 Гбит/сек по линии "вниз" (т.е. к абоненту); и до 10 Гбит/с в обратном направлении.
2. Поддержка одновременного подключения до 1 млн. устройств/км².
3. Сокращение временной задержки на радиointерфейсе до 0,5 мс (для сервисов Сверхнадежной межмашинной связи URLLC) и до 4 мс (для сервисов Сверхширокополосной мобильной связи eMBB).

Рост скорости передачи информации в основном возможен за счет расширения полосы используемых частот и требования, предъявляемые к сетям передачи информации поколения 5G, возможно реализовать лишь в миллиметровом диапазоне (ММД) частот.

Использование миллиметровых волн требует сверхплотное территориальное распределение образующих их устройств радиодоступа – базовых станций BS (Base Station) и подвижных пользовательских устройств UE (User Equipment) с плотностью до одного устройства на 1 м² [3]. Чтобы достичь определенного успеха в развертывании сетей 5G, требуется обширное планирование и анализ многочисленных данных и факторов, влияющих на

потери в радиолинии, на основании чего в дальнейшем происходит оптимизация проектируемой сети.

Для оценки радиопокрытия сетей 5G отлично подходил такой ресурс цифровых карт, как GMTED 2010. GMTED 2010 обеспечивает возможность совместного использования с программой MatLab для оценки дальности связи, оценки потерь и примерного покрытия радиосвязи.

Улучшенная глобальная модель высот «Global Multi-resolution Terrain Elevation Data 2010» (GMTED2010) была совместно разработана Геологическая служба США (USGS) и Национальным агентством геопространственной разведки (NGA) [2].

GMTED2010 основан на данных, полученных из 11 растровых источников высот. Основным исходным набором данных для GMTED2010 являются цифровые данные о высоте местности NGA SRTM (DTED). Существенным преимуществом использования данных цифровых карт является открытый доступ к ресурсу.

Для наглядности, на рис. 1. приведен пример рельефа местности в среде Matlab с использованием цифровых карт GMTED2010. На данной иллюстрации рассмотрен рельеф местности, характеристиками которого является широта, долгота, высота рельефа и цветом помечены энергетические уровни соответствующих высот.

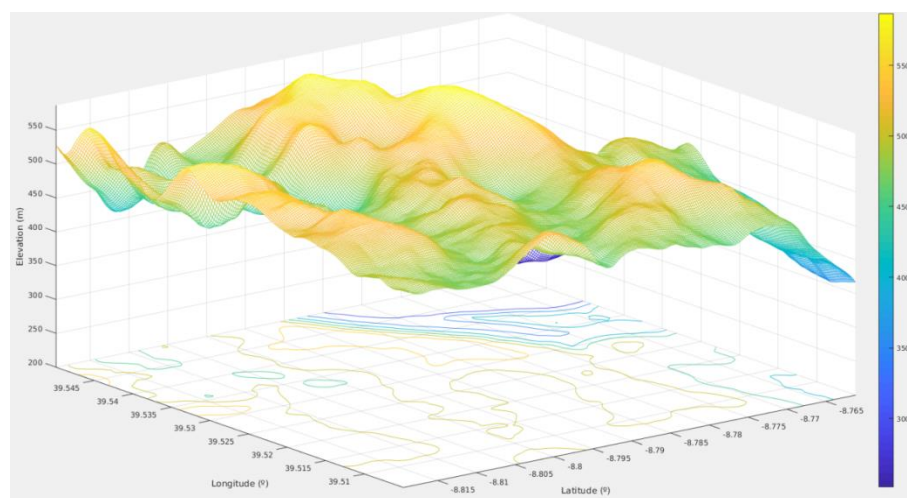


Рис. 1. Пример рельефа местности в среде Matlab

В качестве примера рассмотрим ЖК Кантемировский, Калининский район, г. Санкт-Петербург.

Для более точного расчета были подключены 3D модели построек с помощью ресурса OpenStreetMap. Данные о рельефе местности: источник ДЗЗ GMTED2010; Разрешение 7,5 угловых секунд (приблизительно 250 метров).

Создадим БС (базовая станция) с характеристиками: тип антенны – изотропная, частота – 20ГГц, высота подвеса – 30 м, мощность – 1Вт, угол наклона – 0 градусов.

Также создадим три приемные станции высотами 1.5 м. Каждый приемник представляет собой место, на котором размещен стационарный беспроводной терминал пользователя.

На рис. 2. показано размещение передающей станции – красный цвет и приемных станций – голубой цвет.

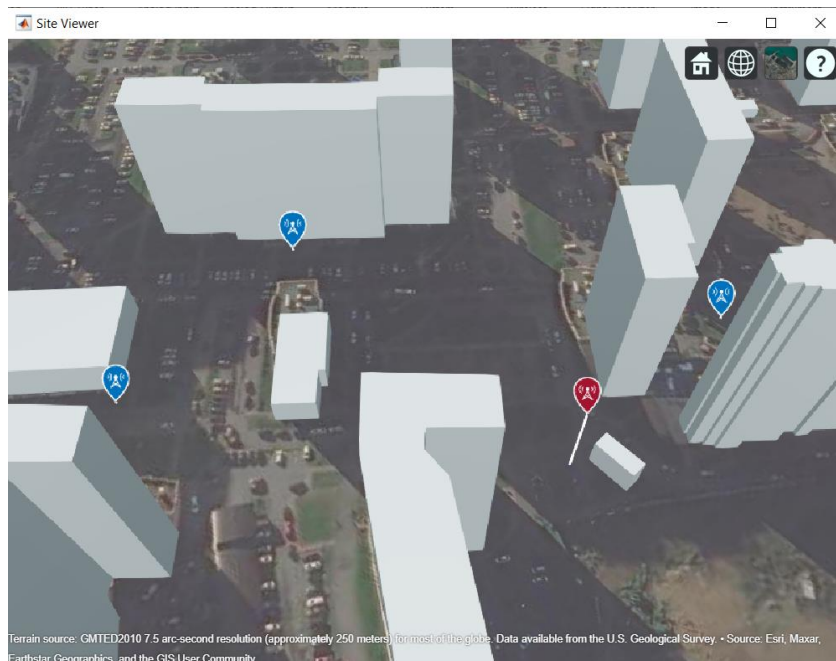


Рис. 2. Размещение BS и приемных устройств

Для оптимальных условий распространения требуется прямая видимость. На рис. 3 показана общая картина каналов связи между передающей и приемными станциями, можно заметить, что прямая видимость отсутствует с одним из приемных устройств (линия помечена красным цветом). Расчет прямой видимости включает местность, но не другие препятствия, в данном случае происходит потери за счет затухания в виде препятствующего здания.

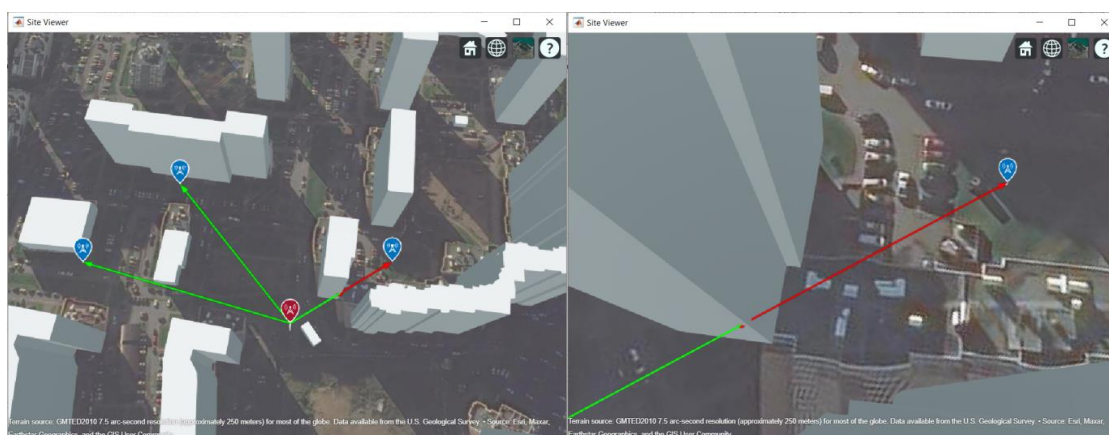


Рис. 3. Установление канала связи между BS и приемными устройствами

Далее проводим оптимизацию, за счет смещения приемника удается достичь прямой видимости.

Для оценки радиопокрытия сети проведем анализ сигнал/помеха. Как видно, SINR варьируется от 20 дБ до -5 дБ (рис. 4.). Часть района не покрывается из-за высокой плотности застройки.

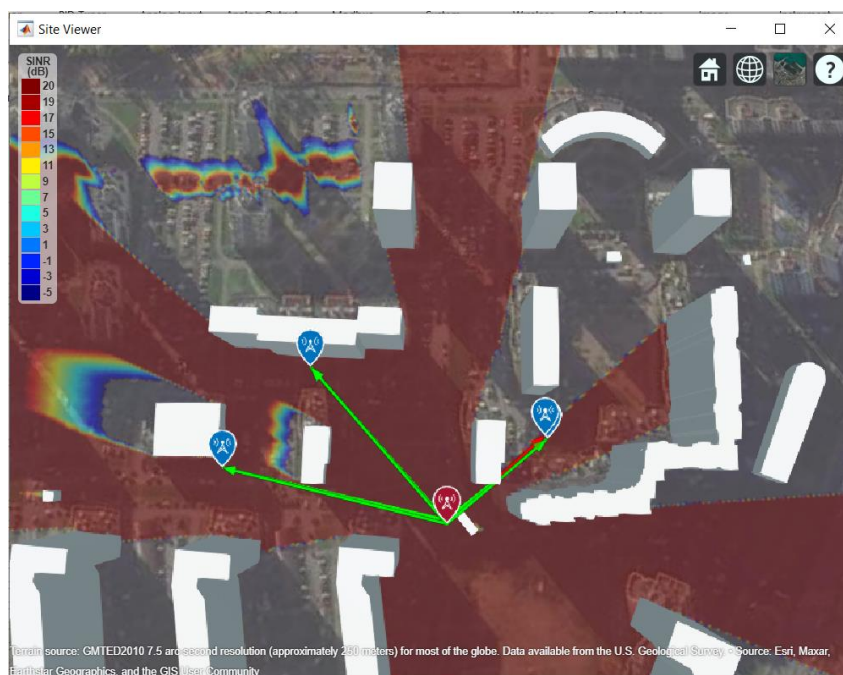


Рис. 4. Отношение сигнал/помеха

Также в Matlab мы можем оценить карту покрытия для сильных и слабых сигналов. Допустим, максимальный уровень сигнала -50 дБм, а минимальный уровень сигнала -90 дБм. На рис. 5 мы видим покрытие сети, вблизи БС покрытие значительно лучше, дальность максимального уровня доходит до 115 м.

Вычисляем уровни сигналов рассматриваемых приемных устройств: $RX1 = -52.7084$ дБ, $RX2 = -53.6315$ дБ, $RX3 = -48.7029$ дБ.

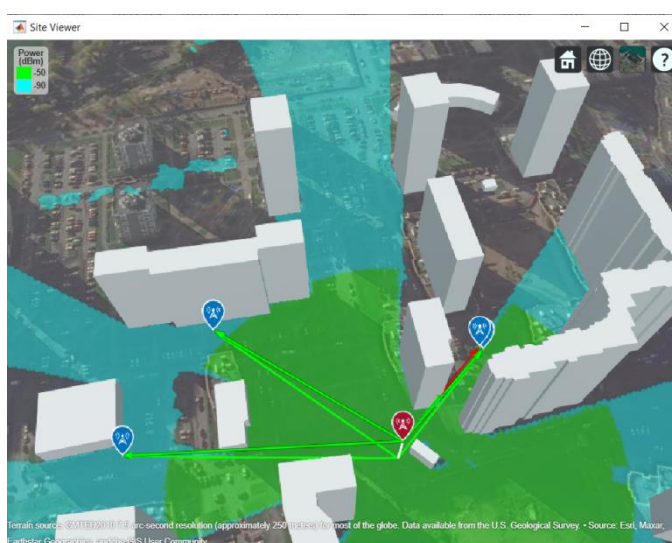


Рис. 5. Карта покрытия

Таким образом, рассмотренный метод оценки радиопокрытия с цифровыми моделями местности является отличным вариантом для первичного

планирования сетей 5G, поскольку функционал MatLab позволяет проанализировать достаточно информации для того, чтобы предварительно оценить распространение сигнала, его мощность, отношение сигнал/помеха и покрытие.

Список используемых источников:

1. Портал о современных технологиях мобильной и беспроводной связи [Электронный ресурс]. URL: <http://1234g.ru/5g> (дата обращения 02.11.2022).
2. Danielson, J.J., and Gesch, D.B., 2011, Global multi-resolution terrain elevation data 2010 (GMTED2010): U.S. Geological Survey Open-File Report 2011–1073, 26.
3. Фокин Г. А. Оценка помех в сверхплотных сетях радиодоступа 5G с диаграммообразованием // Информационные технологии и телекоммуникации. 2020. Том 8. №4. С. 35–59. DOI 10.31854/2307-1303-2020-8-4-35-59.

Dobraya O.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Evaluation of radio coverage of 5g networks with digital terrain models in the Matlab environment.

The world is developing, more and more technologies are emerging, the needs of mobile users are growing and, accordingly, for the implementation of current and future implementations, the introduction of appropriate means for servicing these services is required, such a technology is currently the 5th generation network.

Key words: eMBB, mobile communication, URLLC, mMTC, 5G, radio coverage, GMTED2010, Matlab.

УДК 621.396.99
ГРНТИ 49.43.29

АНАЛИЗ ПРОБЛЕМЫ ОБСЛУЖИВАНИЯ АБОНЕНТОВ СЕТЕЙ МОБИЛЬНОЙ СВЯЗИ В ВЫСОКОСКОРОСТНЫХ ПОЕЗДАХ

А. А. Зайченко, Т. А. Чичко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Для комфортного использования любого вида транспорта необходимо обеспечить возможность оказания пассажирам услуг, которыми они привыкли пользоваться в повседневной жизни. Благодаря высокой скорости передачи данных и низкой задержке сети стандарта LTE являются наиболее перспективным решением для обеспечения связью пассажиров железных дорог. Однако существующая конфигурация этих сетей не позволяет обеспечить необходимую надежность и качество связи при высокоскоростном перемещении абонента. Таким образом, существует задача разработки технических предложений по размещению радиооборудования сетей LTE, использованию специализированных опций и настройке сетевых параметров с учетом высокой скорости движения абонентов.

LTE, высокоскоростное перемещение абонентов, успешность хэндоверов, согласованная многоточечная передача (CoMP)

Основные проблемы, из-за которых снижается качество соединения и прерывается передача данных в мобильной связи при высокоскоростном перемещении, вызваны следующими причинами: доплеровский сдвиг, чрезмерно частые жёсткие хэндоверы и потери при проникновении. Наиболее частой причиной ухудшения качества связи являются неуспешные хэндоверы – с одной стороны, задержка передачи обслуживания при жёстком хэндовере достаточно велика, подвижный объект проходит зону перекрытия двух базовых станций так быстро, что процедура передачи не может быть выполнена своевременно; с другой стороны, из-за высокой скорости перемещения абонентское устройство может пропустить оптимальный момент для начала хэндовера, что тоже снижает вероятность его успеха [1].

Уже не первый год во многих странах проводятся исследования по обеспечению надлежащего качества мобильной связи для железнодорожных путей. Например, в работах по оптимизации сети GSM-R были разработаны алгоритмы для быстрой передачи обслуживания выделенной пассажирской линии, путем установки нового списка соседей [2]. Впоследствии было предложено использование оптоволоконных линий для концепции MEC (Moving Extended Cell), которая использует механизм реструктуризации виртуальной зоны с несколькими ячейками, так что группа виртуальных антенн перемещается вместе с мобильным пользователем [3]. Позже для этой концепции ввели реле в процесс передачи обслуживания в сотовых сетях, чтобы улучшить производительность передачи обслуживания [4].

Учитывая обязательства операторов мобильной связи по обеспечению сплошного покрытия сетями LTE территорий РФ в ближайшие годы, наиболее

целесообразным вариантом для обеспечения связи в высокоскоростных поездах является применение технологии CoMP (Coordinate Multiple Point transmission) [5]. Согласованная многоточечная передача позволяет географически разделенным базовым станциям совместно отправлять данные на одно устройство и совместно получать данные с него же. Рассмотрим подробнее сеть с использованием CoMP, которая позволяет решить описанные выше проблемы [6].

Так как сегменты сети мобильной связи, обеспечивающие покрытие вдоль железных дорог, имеют линейную топологию, базовые станции имеют двухсекторную конфигурацию. Поскольку в LTE используется мультиплексирование OFDM (Orthogonal Frequency-Division Multiplexing), основным источником интерференции являются межсотовые помехи. Во избежание возникновения данного негативного явления можно использовать распределение частот, как показано на рис. 1. Всю полосу частот делят на две части. При движении объекта в одном направлении (из точки А в точку Б) обслуживание производится на одной частоте F1, при движении в противоположном направлении используется вторая частота F2.

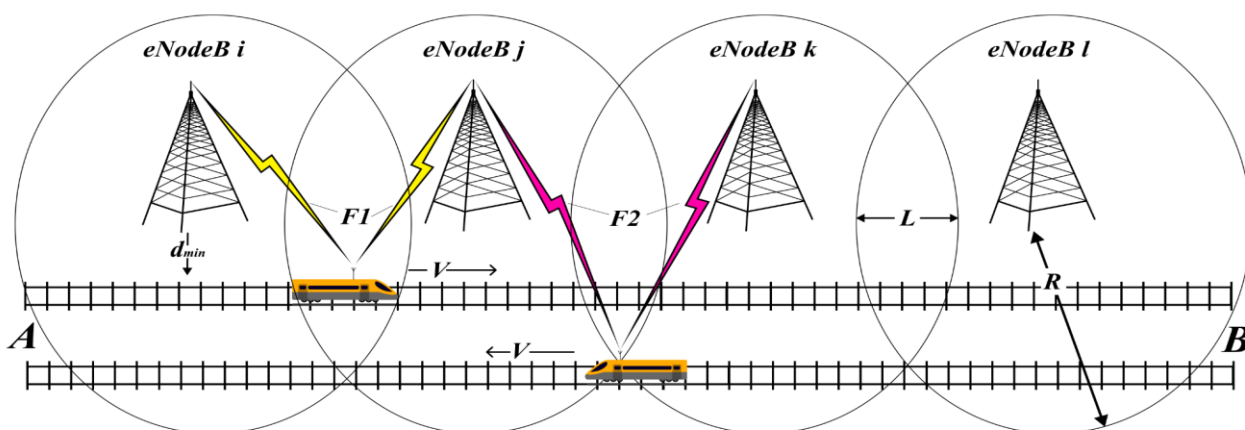


Рис. 1. Распределение частот на железнодорожных путях, где d_{min} – минимальное расстояние между базовой станцией и железнодорожными путями, V – скорость движения объекта, L – зона перекрытия, R – радиус соты

Для уменьшения потерь проникновения целесообразно использовать для приёма и передачи сигнала между движущимся транспортным средством и базовой станцией наружные антенны и центральный узел управления пико-сотой (CCS – Central Control Station), находящейся внутри высокоскоростного объекта. Предпочтительно использование 2 наружных антенн, расположенных в начале и в конце транспортного средства, чтобы использовать преимущества распределённой передачи – это позволит уменьшить влияние задержек передачи в канале связи (структура предлагаемой схемы расположения оборудования радиодоступа в подвижном объекте представлены на рис. 2).

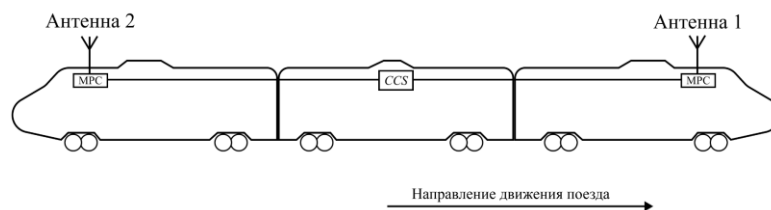


Рис. 2. Структурная схема расположения оборудования радиодоступа в подвижном объекте, где МРС – мобильная ретрансляционная станция, ССС – центральный узел управления

Также двухантенная схема предпочтительна для успешного совершения хэндоверов – когда антенна 1 входит в зону перекрытия, базовая станция 1, которой обслуживается подвижное транспортное средство, активирует режим совместной передачи (cooperative transmission set – CTS), при котором с транспортным средством взаимодействуют и текущая базовая станция 1, и новая базовая станция 2, в зону обслуживания которой переместилась антенна 1. (рис. 3). Активация режима совместной передачи происходит на основании измерений уровней сигналов, принимаемых антеннами 1 и 2, а также информации о местоположении, предоставляемой системой управления поездом. Как только режим совместной передачи активирован, базовая станция 1 передаёт данные пользовательской плоскости базовой станции 2 по интерфейсу X2 – обе соседние базовые станции используют один и тот же частотный ресурс для связи с поездом. Сигналы от базовых станций накладываются по фазе с помощью предварительного кодирования, что обеспечивает усиление разнесения и усиление мощности. Когда транспортное средство полностью входит в область перекрытия зон обслуживания соседних базовых станций, и антенна 1, и антенна 2 принимают сигналы от обеих базовых станций, но информация о результатах измерений передаётся только на базовую станцию 1. Решение о начале хэндовера без прерывания передачи пользовательских данных принимает базовая станция 1 на основании полученных результатов измерений и информации от RRM (radio resource management – центр управления радиоресурсами) целевой базовой станции 2. После начала хэндовера режим совместной передачи отключается, обслуживание переходит к целевой базовой станции 2.

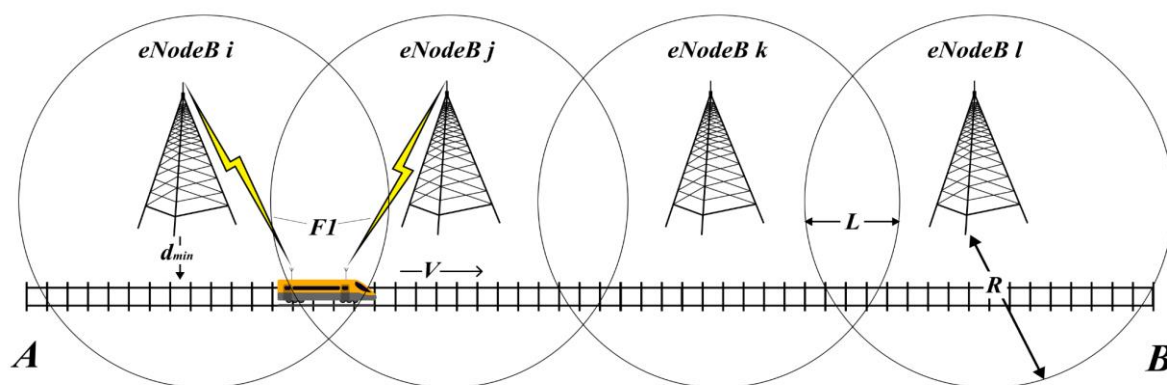


Рис. 3. Схема мягкой передачи обслуживания на основе CoMP

При использовании технологии CoMP увеличивается вероятность успешного выполнения хэндоверов. Без использования технологии согласованной многоточечной передачи успешность выполнения хэндоверов не превышает 89% процентов, с использованием CoMP достигает 99% [7]. Однако производительность сети с использованием CoMP в условиях высокоскоростного передвижения абонентов пока не была установлена. Для оценки производительности сети на следующем этапе исследований планируется разработать имитационную модель, схема которой представлена на рис. 4.

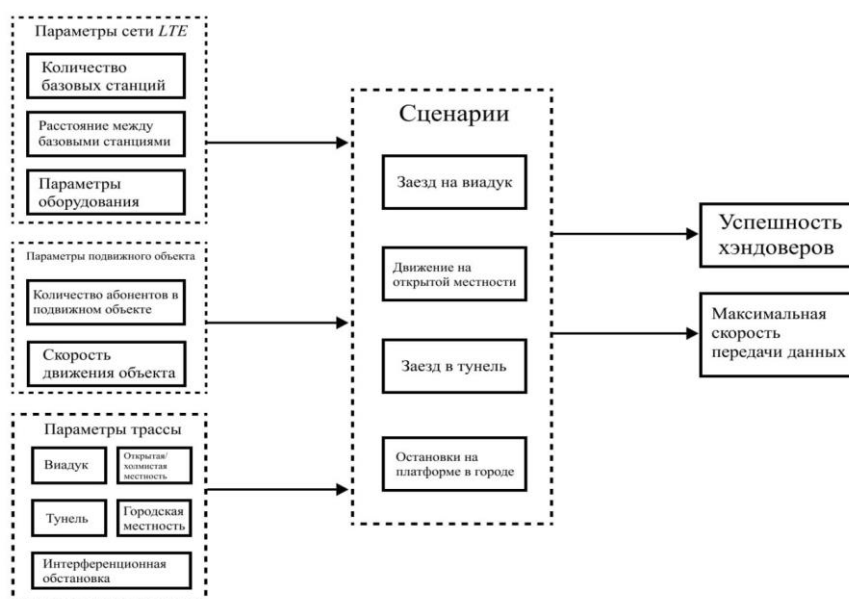


Рис. 4. Схема имитационной модели сети LTE с CoMP для высокоскоростных поездов

Итак, для улучшения качества мобильной связи для абонентов в высокоскоростных подвижных объектах необходимо уменьшить вероятность совершения неуспешных хэндоверов. Использование технологии согласованной многоточечной передачи позволяет увеличить вероятность совершения успешных хэндоверов. Для развития и внедрения данной технологии необходимо исследовать производительность сети с CoMP в условиях высокоскоростного передвижения абонентов.

Список используемых источников:

1. Putri H., Novianti A., Damayanti T. N. Timer Decision Algorithm for Ping-Pong Handover Control on High-Speed Train in LTE Networks 1800 MHz //Journal of Hunan University Natural Sciences. – 2021. – Т. 48. – №. 8;
2. Источник: Zhong Z. D. et al. Key Issues for GSM-R and LTE-R //Dedicated Mobile Communications for High-speed Railway. – Springer, Berlin, Heidelberg, 2018. – С. 19-55;
3. S Jeon, S Lee, A relay-assisted handover technique with network coding over multihop cellular networks. IEEE Commun Lett. 11, 252–254 (2007);
4. R Pabst, BH Walke, DC Schultz, Relay-based deployment concepts for wireless and mobile broadband radio. IEEE Commun Mag. 42, 80–89 (2004)

5. 3GPP TR 36.819; Coordinated multi-point operation for LTE physical layer aspects;
6. РЫЖКОВ А. Е. Сети стандарта LTE. Развитие технологий радиодоступа: [монография] / А. Е. РЫЖКОВ, М. А. Сиверс, А. С. Бабкин, А. М. Пыленок, А. П. Трофимов; СПбГУТ. – СПб., 2014. – 256 с;
7. Luo W., Zhang R., Fang X. A CoMP soft handover scheme for LTE systems in high speed railway //EURASIP Journal on wireless Communications and Networking. – 2012. – Т. 2012. – №. 1. – С. 1-9.

Zaichenko A., Chichko T.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of the problem of servicing subscribers of mobile communication networks in high-speed trains.

For the comfortable use of any transport system, it is necessary to ensure the possibility of providing passengers with services that they are used to using in everyday life. Due to the high data transfer rate and low latency, LTE networks are the most promising. However, the existing configuration of these networks does not allow providing the necessary reliability and quality of communication during high-speed subscriber movement. There is a task of developing technical proposals for the placement of LTE radio equipment, the use of specialized options and the configuration of network parameters taking into account the high speed of subscribers.

Key words: *LTE, high speed mobile mover, handover success, coordinate multiple point transmission (CoMP).*

УДК 621.396.61
ГРНТИ 47.47.29

ОСОБЕННОСТИ МОДЕЛИРОВАНИЯ РАДИОПЕРЕДАТЧИКА СВЕРХШИРОКОПОЛОСНЫХ СИГНАЛОВ НА ОСНОВЕ ХАОТИЧЕСКИХ РАДИОИМПУЛЬСОВ

Е. А. Измestьева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе представлена имитационная модель радиопередающего устройства сверхширокополосных сигналов на основе хаотических радиоимпульсов. Рассмотрены преимущества использования сверхширокополосных сигналов, а также особенности моделирования передатчика, при которых преимущества этих сигналов не теряются. При этом в системе также обеспечиваются необходимые помехоустойчивость и помехозащищенность.

сверхширокополосные сигналы, моделирование передатчика, хаотические радиоимпульсы

В современном мире объём информации, передаваемой по радиоканалу, растёт постоянно. Связано это и с увеличением количества пользователей, и с потребляемым ими количеством трафика, что приводит к необходимости увеличения пропускной способности радиоканалов. Добиться увеличения можно более привычными способами, такими как уплотнение информационных потоков в один по различным параметрам, однако другим способом является переход на системы, использующие сверхширокополосные (СШП) сигналы. В данный момент регулирует СШП системы, работающие в диапазоне 3,1...10,6 ГГц.

СШП сигналы позволяют обеспечивать повышенную скорость передачи, надёжность и помехозащищенность каналов передачи за счёт того, что верхняя граница полосы частот в 2 и более раз превышает нижнюю границу полосы частот. В итоге получается достаточно широкая полоса пропускания, из-за чего увеличивается пропускная способность канала. Безопасность же повышает то, что спектральная плотность мощности уменьшается из-за повышения полосы пропускания, а поэтому сигнал без специального приёмника будет сложнее обнаружить за шумами.

Моделирование передатчиков и приёмников СШП сигналов отличается от привычных приёмно-передающих устройств узкополосных сигналов, однако принцип построения у них совпадает. В работе делается акцент на передатчиках, и их структурная схема представляется на рисунке 1.



Рис. 1. Структурная схема передатчика СШПС

Имитационная же модель радиопередатчика СШП сигналов на основе хаотических импульсов представляется на рисунке 2 [1].

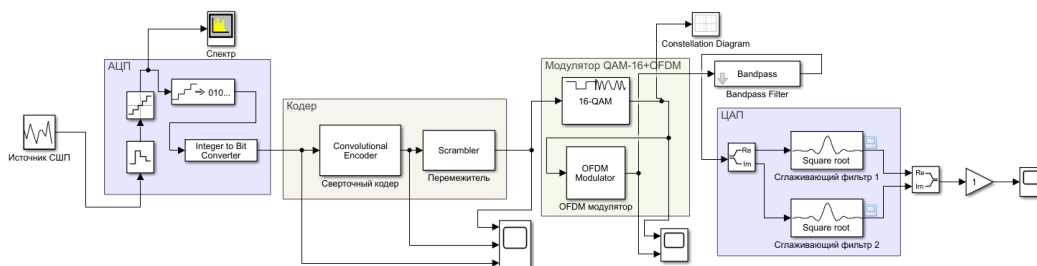


Рис. 2. Имитационная модель передатчика СШПС в Simulink

В работе исследуется передатчик, СШП сигналы которого формируются хаотическими радиоимпульсами [2]. Такой сигнал позволяет использовать возможности хаотических сигналов на пользу СШП сигналам. Главное полезное свойство хаоса – широкополосность, которая почти не зависит от длины импульса [3]. У самого сигнала есть параметры, которые являются случайными функциями времени; в имитационной модели это дисперсия. Аналоговый сигнал идёт на АЦП и после оцифровки можно наблюдать спектр, характеризующий СШПС (рис. 3). Параметры данного генератора: дисперсия – 1,1; среднее значение выборки – 0; полоса пропускания – 500 МГц.

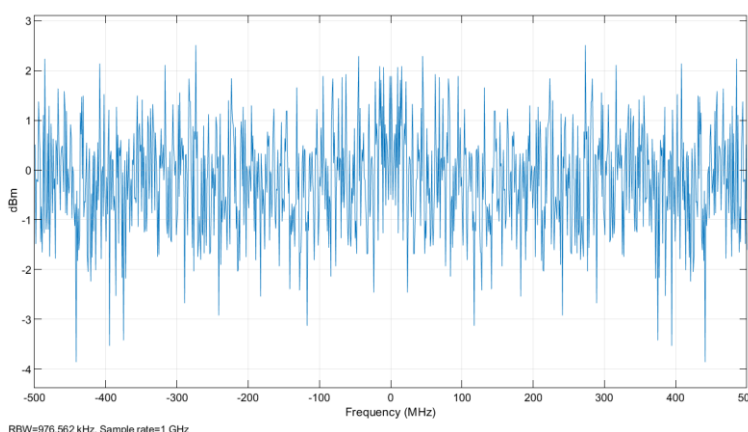


Рис. 3. Спектр полезного СШП сигнала

Для дальнейшей коррекции ошибок, возникающих при передаче в среде, возможно использование сверточного кодера и перемежителя [4]. В таком случае преобразованный СШП сигнал (рис. 4) на выходе кодера будет иметь следующий вид (рис. 5).

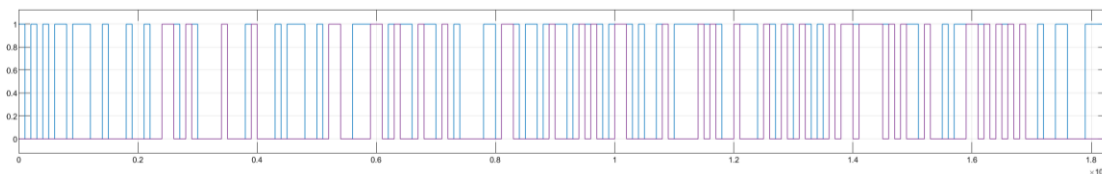


Рис. 4. Цифровой СШП сигнал

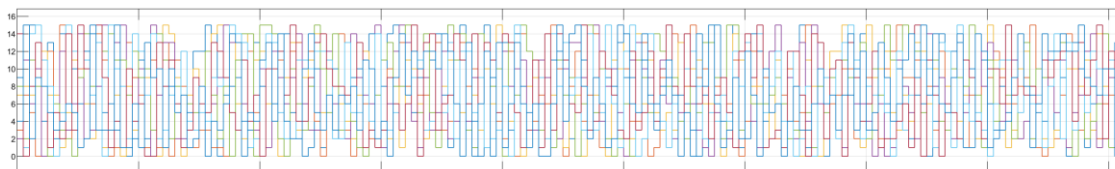


Рис. 5. СШП сигнал на выходе кодера

Блок с модулированием сигнала в СШП передатчиках может отсутствовать, так как его особенность и заключается в том, что он шумоподобный, однако использование модулятора QAM-16 позволяет увеличить скорость передачи данных [5]. В итоге пропускная способность канала будет увеличиваться не только за счёт применения широкой полосы СШП сигнала, но и за счёт применения модулирующей схемы. OFDM модулятор же позволяет бороться с негативными явлениями, возникающими при многолучевой передаче сигнала: межсимвольными помехами и интерференцией между поднесущими.

На выходе модулятора получается сигнал, представленный на рисунке 6, где различными цветами показаны параллельные потоки.

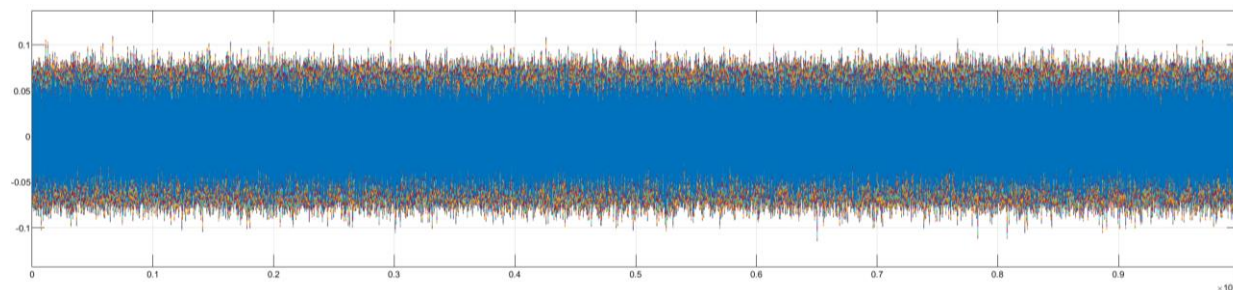


Рис. 6. Модулированный СШП сигнал

В результате проведённых манипуляций получается достаточно широкополосный сигнал, который необходимо подвергнуть фильтрации для дальнейшей передачи. В качестве фильтра используется полосовой – он позволяет подавить ненужные частоты, оставляя только 500 МГц для обработки и передачи.

Через канал передаётся аналоговый сигнал, поэтому, как и узкополосные сигналы, СШП сигнал нуждается в блоке ЦАП. Особенностью является только то, что необходимо два ЦАПа, так как после модулятора сигнал будет иметь две части: реальную и мнимую [6]. На антенну, предназначенную для передачи СШП сигналов, будет передаваться уже комплексный сигнал (рис. 7).

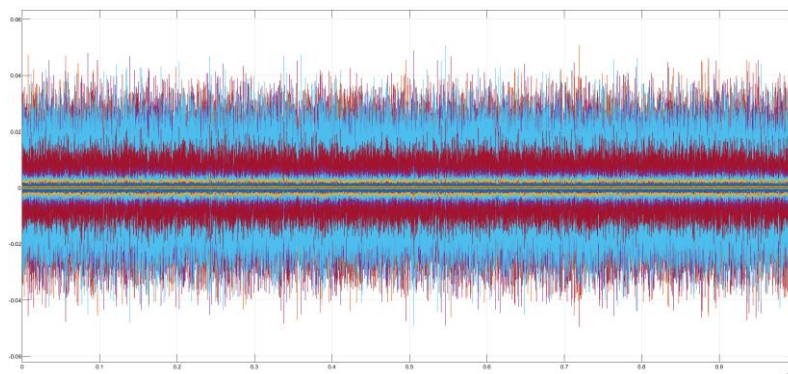


Рис. 7. СШП сигнал на выходе передатчика

В заключение можно сказать, что данная имитационная модель является только одним из вариантов генерации и передачи СШП сигналов. Помимо хаотических импульсов существует ещё множество других моделей. Однако устройства связи на основе хаотических импульсов достаточно просты в реализации.

Список используемых источников:

1. Солонина А. И. Цифровая обработка сигналов. Моделирование в Simulink. СПб.: БХВ-Петербург, 2012. 432 с.
2. Лазоренко О. В., Черногор Л. Ф. Сверхширокополосные сигналы и физические процессы. 1. Основные понятия, модели и методы описания // Радиоп физика и радиоастрономия. 2008, т. 13, №2, с. 166-194.
3. Дмитриев А. С. и др. Сверхширокополосная беспроводная связь на основе динамического хаоса // Радиотехника и электроника. 2006, Т. 51, №10.
4. Torben Brack, Matthias Alles, Timo Lehnigk-Emden, Frank Kienle, Norbert Wehn. A Survey on LDPC Codes and Decoders for OFDM-based UWB Systems // Conference: Proceedings of the 65th IEEE Vehicular Technology Conference, VTC Spring 2007, 22-25 April 2007, Dublin, Ireland.
5. Косичкина Т. П. Исследование и разработка методов передачи и приема информации сверхширокополосными сигналами в системах радиодоступа : автореф. дис. ... канд. техн. наук : 10.02.2015 / Косичкина Татьяна Павловна, Москва, 2004, 24 с.
6. DAC implementation in OFDM [Электронный ресурс]. URL: <https://dsp.stackexchange.com/questions/23064/dac-implementation-in-ofdm> (дата обращения 10.11.2022).

Izmesteva E. A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Features of modeling a radio transmitter of UWB signals based on chaotic radio pulses. Simulation model of a radio transmitter of UWB signals based on chaotic radio pulses has been presented in the research. The advantages of using UWB signals are considered, as well as the features of modeling the transmitter in which the advantages of these signals are not lost. At the same time, the system also provides the necessary noise immunity.

Key words: *UWB signals, modeling a transmitter, chaotic radio pulses.*

УДК 654.165
ГРНТИ 49.33.29

АНАЛИЗ РЕАЛИЗАЦИИ ПРОТОКОЛА УПРАВЛЕНИЯ РАДИОРЕСУРСАМИ RRC В ИМИТАЦИОННОЙ МОДЕЛИ СЕТИ LTE В СИМУЛЯТОРЕ NS-3

Е. Е. Каранова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На сегодняшний день наиболее распространенным подходом при разработке оборудования и программного обеспечения сетей мобильной связи является использование современных средств имитационного моделирования. Данная работа посвящена симулятору NS3 – мощному инструменту моделирования телекоммуникационных систем и распространяемому под лицензией GNU GPLv2. В работе представлен анализ возможностей модуля, реализующего протокол управления радиоресурсами RRC в имитационной модели сети LTE в симуляторе ns-3.

мобильные сети, LTE, RRC, моделирование

В данной работе основное внимание уделяется вопросу моделирования протоколов сигнализации управления, в частности протокола RRC. Протокол управления радиоресурсами – это протокол уровня 3 (сетевого уровня), используемый между UE и базовой станцией. Этот протокол указан 3GPP в TS 36.331 [1] для LTE. Сообщения RRC передаются по RDCP-протоколу. В реальных системах LTE протокол RRC обеспечивает функциональные возможности передачи и получения системной информации, управления соединением, настройки мобильности и измерений.

Модель RRC обеспечивает следующие функции: передача (eNB) и получение (пользователем UE) информации о системе; процедура установления соединения RRC; процедура реконфигурации RRC, поддерживающая варианты использования установки однонаправленного радиоканала данных, реконфигурации режима PHY TX (для поддержки MIMO) и индекса конфигурации SRS, а также передачи обслуживания.

Архитектура модели RRC.

Модель RRC в NS-3 разделена на следующие компоненты:

- объекты RRC `LteUeRrc` и `LteEnbRrc`, которые реализуют конечные автоматы объектов RRC соответственно в UE и eNB;

-SAP RRC `LteUeRrcSapProvider`, `LteUeRrcSapUser`, `LteEnbRrcSapProvider`, `LteEnbRrcSapUser`, которые позволяют объектам RRC отправлять и получать сообщения RRC и информационные элементы;

-классы протокола RRC `LteUeRrcProtocolIdeal`, `LteEnbRrcProtocolIdeal`, `LteUeRrcProtocolReal`, `LteEnbRrcProtocolReal`, которые реализуют две разные модели передачи сообщений RRC.

В «идеальной» модели сообщения RRC не потребляют никаких радиоресурсов и доставляются с нулевой задержкой, а «реальная» модель включает реализацию кодирования информационных элементов ASN.1 [2].

Конечный автомат UE RRC.

Конечный автомат, представленный на рис. 1 реализован в объекте RRC UE. Следует отметить, что большинство состояний являются переходными, то есть,

как только UE переходит в одно из состояний CONNECTED, оно никогда не переключится обратно в какое-либо из состояний IDLE. Этот выбор сделан из-за того, что в модели LTE-EPC основное внимание уделяется режиму CONNECTED. В частности, отказ радиоканала не моделируется, поэтому UE не может перейти в режим ожидания из-за отказа радиоканала, более того, освобождение соединения RRC в настоящее время не инициируется ни EPC, ни NAS. Наличие состояния IDLE облегчает реализацию выбора соты в режиме ожидания [3].

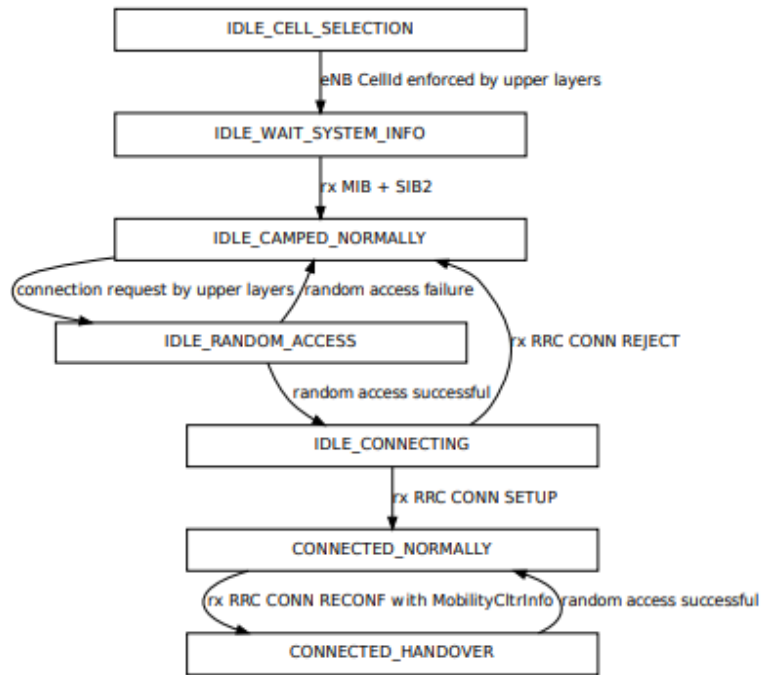


Рис. 1. Конечный автомат RRC UE

Конечный автомат eNB RRC.

Конечный автомат eNB RRC поддерживает состояние для каждого UE, подключенного к соте. В данной модели состояние каждого UE содержится в экземпляре класса UeManager. Конечный автомат представлен на рис. 2.

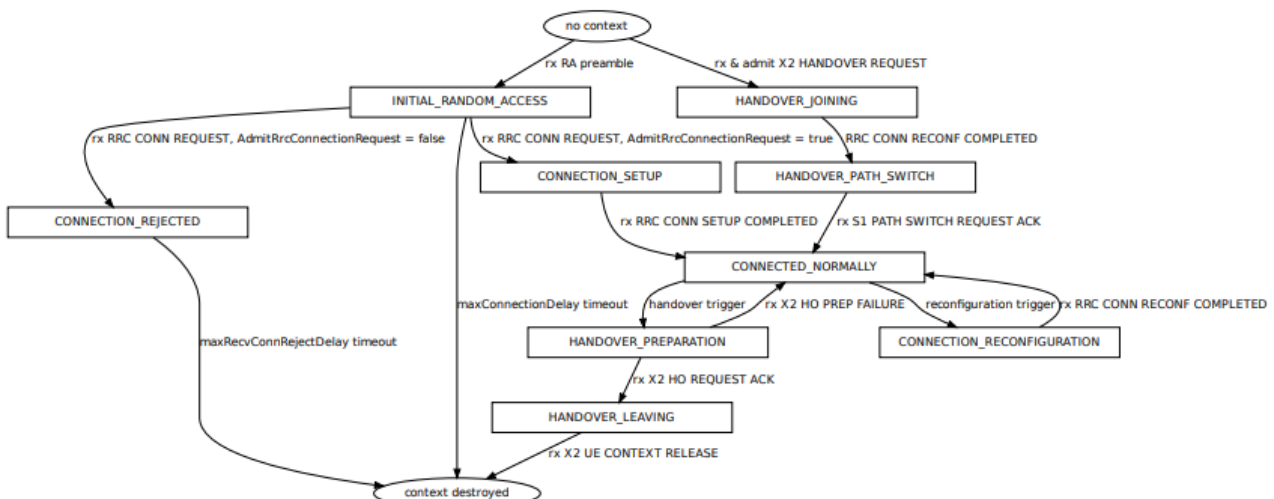


Рис. 2. Конечный автомат eNB RRC для каждого UE

Управление доступом к радиоканалу.

Управление доступом к радио поддерживается за счет наличия ответа RRC eNB на сообщение RRC CONNECTION REQUEST, отправленное UE, либо с сообщением RRC CONNECTION SETUP, либо с сообщением RRC CONNECTION REJECT, в зависимости от того, должно ли быть допущено новое UE. В текущей реализации поведение определяется логическим атрибутом ns3::LteEnbRrc::AdmitRrcConnectionRequest.

Кроме этого, в модели объект RRC UE обеспечивает поддержку измерений:

- поддерживаются только внутрочастотные измерения E-UTRA;
- пропуски измерений не моделируются, так как они не нужны для внутрочастотных измерений;
- поддерживаются только измерения, управляемые событиями; другой тип измерений не поддерживается;
- время срабатывания не поддерживается, т. е. всегда предполагается значение времени срабатывания, равное нулю;
- фильтрация уровня 3 предполагает, что периодичность измерений, о которых сообщает RHY, равна 200 мс;
- в отчетах об измерениях всегда предполагается, что reportQuantity имеет значение «оба», т. е. всегда сообщаются как RSRP, так и RSRQ, независимо от триггерного количества.

В модели объект RRC eNB реализует следующие параметры конфигурации и процедуры:

- конфигурируются только внутрочастотные измерения E-UTRA, поэтому в качестве объекта измерения конфигурируется только несущая частота нисходящей линии связи обслуживающей соты;
- параметр reportInterval настроен на 480 мс, поэтому после запуска событий UE будет отправлять отчеты об измерениях с этой периодичностью;
- параметр filterCoefficientRSRQ настроен на fc4, что является значением по умолчанию, указанным в спецификации протокола [3];
- параметры hysteresis и timeToTrigger настроены равными нулю.

Для проверки правильного функционирования функций данной модели моделирования, а также для проверки результатов моделирования разработаны и интегрированы с тестовой средой ns-3 несколько наборов тестов. Набор тестов LTE-RRC проверяет правильную функциональность следующих аспектов: произвольный доступ MAC, сбор системной информации RRC, установление соединения RRC, реконфигурация RRC.

Тестирование.

Набор тестов рассматривает тип сценария с одним eNB и несколькими UE, которым предписано подключиться к eNB. Каждый тестовый пример реализует экземпляр этого сценария с конкретными значениями следующих параметров:

- количество UE;
- количество активных однонаправленных радиоканалов данных, которые должны быть активированы для каждого UE;
- время t_0^c , в которое первое UE получает указание начать подключение к eNB;

- интервал времени d^i между началом соединения UE n и UE n+1, таким образом, время, в течении которого подключается пользователь n, определяется как $t_n^c = t_0^c + nd^i$;

- логический флаг, указывающий, используется ли идеальная или реальная модель протокола RRC.

Каждый тест проходит успешно, если условие «UE подключено к eNB» оценивается положительно для каждого UE после задержки d^e с момента начала подключения к eNB. Задержка d^e определяется по следующей формуле:

$$d^e = d^{si} + d^{ra} + d^{ce} + d^{cr} \quad (1)$$

- Максимальная задержка, необходимая для получения системной информации определяется как d^{si} ;

- d^{ra} – задержка для процедуры произвольного доступа (RA) MAC. Это зависит от коллизий преамбулы, а также от доступности ресурсов для выделения гранта UL. Общее количество необходимых попыток RA зависит от коллизий преамбулы и неудач при распределении разрешения UL из-за нехватки ресурсов. Количество коллизий зависит от количества UE, которые пытаются получить доступ одновременно.

- d^{ce} – задержка, необходимая для передачи сообщения RRC CONNECTION SETUP, за которым следует сообщение RRC CONNECTION SETUP COMPLETED. В частности, рассматривается двусторонняя задержка, равная 10 мс плюс $[2n/4]$, учитывая, что должны быть переданы 2 пакета RRC и что за один TTI может быть передано не более 4 таких пакетов;

- d^{cr} – задержка, необходимая для необходимых транзакций RRC CONNECTION RECONFIGURATION. Необходимое количество транзакций – 1 для каждой активации канала-носителя. Аналогично тому, что сделано для d^{ce} , для каждой транзакции учитывается задержка в оба конца, равную 10 мс плюс $[2n/4]$. задержка 20 мс.

Таким образом, условие «UE подключено к eNB» оценивается как положительное, если выполняются следующие условия:

- eNB имеет контекст UE (идентифицированный значением RNTI, извлеченным из RRC UE);

- состояние RRC UE в момент eNB ПОДКЛЮЧЕН НОРМАЛЬНО;

- состояние RRC на UE: НОРМАЛЬНО СОЕДИНЕНО;

- UE конфигурируется с CellId, DIBandwidth, UIBandwidth, DIEarfcn и UIEarfcn eNB;

- количество активных однонаправленных радиоканалов данных является ожидаемым, как в соответствии с контекстной информацией как в UE, так и в eNB;

- для каждого однонаправленного радиоканала данных идентификаторы EPS однонаправленного канала, идентификатор DRB и LCID согласованы между UE и eNB.

Как для LTE, так и для 3G сообщения и задержки конфигурации могут плохо взаимодействовать с определенными моделями состояния сети. Актуальная информации о состоянии RRC влияет на производительность и играет важную роль для операторов связи и разработчиков приложений.

Процедура перехода между состояниями в LTE обеспечивает гораздо лучшую среднюю производительность, чем в 3G, в основном из-за меньшего количества сигналов уровня управления, необходимых для передачи данных или изменения состояний RRC. Задержки в LTE в первую очередь связаны с плохим взаимодействием между некоторыми сообщениями уровня управления и процессом понижения состояния. Влияние состояний RRC на передачу трафика является сложным и сильно зависит от деталей реализации. Рассмотренная модель состояния RRC позволит разработчикам оборудования лучше определять влияние состояний RRC на шаблоны трафика приложений.

Список используемых источников:

1. Network Simulator (LENA) [Электронный ресурс] // URL: <http://iptechwiki.cttc.es/LTEEPC> (дата обращения 25.10.2022).
2. G. Piro, L. A. Grieco, G. Boggia, and P. Camarda. A Two-level Scheduling Algorithm for QoS Support in the Downlink of LTE Cellular Networks. In Proc. of European Wireless, EW2010, Apr. 2010. (дата обращения 20.10.2022).
3. Сетевой симулятор NS-3 [Электронный ресурс] // URL: <https://www.nsnam.org/> (дата обращения 20.10.2022).

Karanova E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of the implementation of the radio resource control protocol rrc in the simulation model of the lte network in the ns-3 simulator.

To date, the most common approach in the development of equipment and software for mobile communication networks is the use of modern simulation tools. This work is devoted to the NS3 simulator, a powerful tool for modeling telecommunication systems and distributed under the GNU GPLv2 license. The paper presents an analysis of the capabilities of the module that implements the RRC radio resource control protocol in the simulation model of the LTE network in the ns-3 simulator.

Key words: *mobile networks, LTE, RRC, simulation.*

УДК 629.127
ГРНТИ 55.45.31

СПОСОБЫ СВЯЗИ С ПОДВОДНЫМИ ОБЪЕКТАМИ

Т. В. Киселёв

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Связь с подводными объектами, когда они находятся в погруженном состоянии – достаточно серьезная техническая задача. Основная проблема состоит в том, что электромагнитные волны с частотами, используемыми в традиционной радиосвязи, сильно ослабляются при прохождении через толстый слой проводящего материала, которым является соленая вода.

подводная связь, КНЧ, ОНЧ, НЧ

Связь с подводными объектами – это область связи, которая представляет технические трудности и требует специальных технологий. Поскольку радиоволны плохо распространяются через соленую воду, подводные объекты отключены от радиосвязи на обычных радиочастотах.

Диапазон очень низких частот (ОНЧ: от 3 кГц до 30 кГц) имеет приличное проникновение в морскую воду, возможно, на глубину до 20 метров. Идя еще дальше вниз по частотному диапазону, сигналы в диапазоне низких частот (НЧ: от 30 Гц до 300 Гц) и чрезвычайно низких частот (КНЧ: от 3 Гц до 30 Гц) способны проникать в морскую воду на глубину сотни метров, что достаточно глубоко для того, чтобы любая подводная лодка могла сохранять свою скрытность [1].

Общая информация об используемых волнах для связи с подводными объектами.

Радиоволны ОНЧ (3–30 кГц) могут проникать в морскую воду на несколько десятков метров, и подводная лодка на небольшой глубине может использовать их для связи. Более глубокое судно может использовать буй, оборудованный антенной на длинном тросе. Буй поднимается на несколько метров ниже поверхности и может быть достаточно маленьким, чтобы оставаться незамеченным вражеским гидролокатором и радаром. Однако эти требования к глубине ограничивают подводные лодки короткими периодами приема, и технологии противолодочной войны могут обнаруживать подводную лодку или антенный буй на этих малых глубинах.

Электромагнитные волны в диапазоне частот НЧ и КНЧ могут проникать в морскую воду на глубину в сотни метров, что позволяет передавать сигналы подводным лодкам на их рабочих глубинах. Создание передатчика КНЧ является сложной задачей, поскольку они должны работать на невероятно длинных волнах [2]. Для связи с подводными лодками ВМФ РФ используют объект радиосвязи “ЗЕВС”

Существует множество методов подводной связи, которые используются/разрабатываются.

Методы военной подводной связи.

Объект радиосвязи “ЗЕВС”.

Это объект радиосвязи ВМФ России для передачи сообщений подводным лодкам, находящимся в погружённом состоянии в океанских глубинах или под арктическими льдами. Расположен на Кольском полуострове. Передача сообщений осуществлялась на несущей частоте 82 Гц.

Объект включает в себя два разнесённых на 10 км радиопередающих модуля — основной и резервный, каждый со своей антенной особой конструкции. Антенны расположены параллельно, в направлении с запада на восток. К антенному устройству относятся два больших заземляющих электрода, проникающих глубоко в землю, и подключённая к этим электродам антенная линия, подобная воздушной линии электропередачи, длиной около 60 км [3].

В наши дни объект представляет собой развитый комплекс радиопередающих устройств различного назначения в диапазоне частот от ультракоротких до сверхдлинных волн, что позволяет не только передавать сигналы боевого управления на подводные лодки, находящиеся на глубине, но и осуществлять руководство всеми силами ВМФ.

Акустическая передача.

Акустическая передача состоит в размещении под водой ретранслирующих станций «подводных модемов», имеющих надводные радиоантенны. Предположим, что такая станция преобразует радиосигналы в акустические колебания и транслирует их под водой, а лодка “принимает звук”, находясь на большой глубине. Акустическая подводная связь, в теории, работает на расстояниях, измеряемых десятками километров. Однако весь океан такими станциями не застроишь, их можно разместить только вдоль традиционных районов патрулирования.

Подобным способом можно организовывать как двустороннюю, так и конференц-связь. При этом акустический сигнал доносит голос или цифровую информацию на расстояние до 35 километров и на глубину до шести километров [4].

Стандартная радиотехнология.

Для связи могут использоваться специальные буи, поднимаемые с лодки, находящейся в подводном положении. Такой буй, начинённый радиосистемами, привязанный к лодке и обменивающийся с ней информацией, может всплыть на поверхность, а может и оставаться на небольшой глубине.

Вспомогательные подводные лодки.

В 1970-х годах в СССР был разработан проект модификации подводных лодок проекта 629 для использования их в качестве ретрансляторов сигнала и обеспечения связи кораблей из любой точки мира с командованием ВМФ. По проекту было модифицировано три субмарины.

Самолеты.

Для связи с подводными лодками в ВМФ РФ используется самолёт-ретранслятор Ту-142МР «Орёл». В нижней части фюзеляжа установлен барабан с выпускной буксируемой тросовой антенной длиной 8,6 км. Тросовая антенна данной длины позволяет самолету за счет своего размера держать связь с находящимися на глубине в сотни метров субмаринами [5].

Прочие методы подводной связи.

Мобильный радиокomплекс беспроводной подводной связи IVA S/W

Российская компания IVA Technologies сообщила о выпуске обновленной версии мобильного радиокomплекса подводной связи IVA S/W. Усовершенствованный радиокomплекс прошел успешные испытания в акватории Баренцева моря с участием боевых пловцов воинской части специального назначения Военно-морского флота (ВМФ) России.

В ходе испытаний группе водолазов с устройствами IVA S/W удалось установить стабильную голосовую связь высокой четкости на дальности до 2 тыс. м и на глубине до 26 м. Из сфер применения можно отметить Освоение Арктики, исследование флоры и фауны акваторий, Ремонт, тех. обслуживание и модернизация стационарных подводных сооружений и так далее [6].

Aqua-fi.

Разработанная технология Aqua-Fi позволяет передавать видео в формате HD в водной среде при помощи лазеров. Принцип работы основан на трансляции данных полученных при подводной съемке, например с использованием смартфона помещенного в водонепроницаемый защитный чехол, при помощи традиционных радиоволн на промежуточное устройство, закрепленное на воздушных баллонах аквалангиста. На следующем этапе микрокомпьютер преобразует данные в световые импульсы, кодирующиеся в двоичный код и отправляющиеся на приемник с использованием 520-нанометрового лазера либо массива зеленых светодиодов [7].

Применение лазера более перспективно при трансляции данных на большие расстояния. Однако использованием светодиодов требует гораздо меньше энергии. Закодированные данные передаются на приемник, размещенный на днище судна, где они расшифровываются и преобразуются в обычные фото или видео материалы с использованием компьютерных дешифраторов. В дальнейшем полученные фото можно традиционным образом передавать в интернет с помощью спутников.

Таким образом, были рассмотрены различные типы связи как с любительскими, научно-исследовательскими, так и военными подводными объектами.

Достоинства и недостатки методов связи предоставлены в таблице 1.

ТАБЛИЦА 1. Преимущества и недостатки различных методов подводной связи

Технология	Преимущества	Недостатки
Объект радиосвязи “ЗЕВС”	Связь с подводными лодками на глубине сотен метров; Связь с подводными лодками на любом расстоянии	Очень низкая скорость передачи (несколько знаков в минуту); Большое потребление мощности (порядка 20-30 МВт)
Акустическая передача	Высокая скорость передачи	Связь только в области союзные вод
Стандартная радиотехнология	Простота реализации; При нахождении буя на поверхности воды возможна спутниковая связь	Ограничение скорости лодки; Небольшое время автономной работы; Нахождение лодки на строго заданной глубине
Вспомогательные подводные лодки	Устойчивая радиосвязь с другими подводными лодками	Моральное и техническое устаревание технологии
Самолеты	Связь с подводными лодками на глубине сотен метров	Односторонняя связь
IVA S/W	Глубина связи до 60 м; Возможность обхода препятствий для распространения сигнала	Дальность связи до 2000м
Aqua-fi	Высокие скорости передачи (2 Мбит/с)	Приемо- передающие устройства должны быть в прямой видимости друг от друга;

Список используемых источников:

1. Дударев, Д. С. Распространение радиоволн в океане [Электронный ресурс] / Д. С. Дударев, К. С. Дударев, Н. К. Теренина. — Текст : непосредственный // Юный ученый. — 2019. — № 1 (21). — С. 13-18. — URL: <https://moluch.ru/young/archive/21/1332/> (дата обращения: 12.11.2022)

2. Катанович А.А., Рочев А.М., Цыванюк В.А. О проблемах связи с подводными лодками [Электронный ресурс] // Журнал Военная мысль: электрон. научн. журн. 2020. N 7. С 102-109. URL: <https://cyberleninka.ru/article/n/o-problemah-svyazi-s-podvodnymi-lodkami> (дата обращения 12.11.2022)

3. Велихов И.П., Войтеховский Ю.Л., Жамалетдинов А.А. Взаимодействие электромагнитных полей контролируемых источников СНЧ диапазона с ионосферой и земной корой: Материалы Всероссийского (с международным участием) научно-практического семинара. В 2 т. [Электронный ресурс] / Рос. акад. наук, Отд. наук о Земле, Кольский научный центр, Геологический институт; гл. ред. академик РАН Е.П. Велихов, зам. гл. редактора д.г.-м.н. Ю.Л. Войтеховский. – Апатиты, 2014. – Т. 1. – 206 с. URL: <http://geoksc.apatity.ru/index.php/conferences/236-vzaimodejstvie-elektromagnitnykh-polej-knch-snch-diapazona-s-ionosferoj-i-zemnoj-koroj> (дата обращения 12.11.2022)

4. Литовкин Д.В., Рамм А.М. Военные моряки развернули подводный интернет [Электронный ресурс] // Журнал Известия электрон. новостн. Журн 2016. URL: <https://iz.ru/news/652775> (дата обращения 13.11.2022)
5. Затучный А.М., Ригмант В.Г., Синеокий П.М. «Турбовинтовые самолеты Ту-95/Ту-114/Ту-142/Ту-95МС» [Электронный ресурс] Журнал Полигон-пресс, 2017, 600 стр., цв. Ил. URL: <http://www.polygonpress.ru/portfolio-category/2016-2019/> (дата обращения 12.11.2022)
6. Власов А.А., Родионов А.Ю. Перспективы использования систем подводной коммуникации на основе магнитной индукции [Электронный ресурс] // Журнал Вестник инженерной школы Дальневосточного федерального университета, 2021. — № 2. — С. 45-46. URL: <https://cyberleninka.ru/article/n/perspektivy-ispolzovaniya-sistem-podvodnoy-kommunikatsii-na-osnove-magnitnoy-induktсии-obzor> (дата обращения 12.11.2022)
7. Micael Koziol. Aqua-Fi is a Wi-Fi system for watery environments where radios typically struggle [Электронный ресурс] // Журнал – IEEE Spectrum: электрон. научн. журн. 2020. URL: <https://spectrum.ieee.org/researchers-lasers-bring-internet-underwater> (дата обращения 12.11.2022)

Kiselev T.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Methods of communication with underwater objects.

Communication with underwater objects when they are submerged is a rather serious technical problem. The main problem is that electromagnetic waves with frequencies used in traditional radio communication are greatly attenuated when passing through a thick layer of conductive material, which is salt water.

Key words: underwater communication, ELF, VLF, LF.

УДК 378.162.33
ГРНТИ 49.34.06

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ РЕФАРМИНГА С ТОЧКИ ЗРЕНИЯ ВЛИЯНИЯ НА ЗОНЫ ПОКРЫТИЯ СЕТИ

В. Е. Коротин, В. С. Вторых

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время рефарминг спектра — это экономичный способ увеличить пропускную способность сети за счет существующих диапазонов 2G/3G/LTE без необходимости покупки операторами новых диапазонов частот. В связи с этим имеет смысл исследовать существующие решения в области рефарминга радиочастот, существующую на данный момент законодательную базу в данной области, а также провести моделирование для оценки потерь при распространении в условиях рефарминга спектра.

сотовая связь, рефарминг, частотный спектр, LTE, GSM, UMTS

С появлением радиосвязи радиочастотный спектр все больше и больше переполняется различными технологиями. Различные системы радиосвязи были разработаны для различных целей, и многие участники проявили интерес к использованию этих систем в одно и то же время. Поэтому неизбежно встает вопрос регулирования использования радиочастотного спектра.

Государственный регулирующий орган (в РФ это ГКРЧ) высвобождает какую-либо полосу от занятия устаревшей технологией, и вместе с тем разрешает операторам сотовой связи использовать данный диапазон для более новых и перспективных технологий [1]. Ключевыми решениями ГКРЧ по вопросам рефарминга являются:

1) В 2013 году на заседании ГКРЧ было принято решение о “технологической нейтральности”. Согласно решению, операторы сотовой связи стали иметь право на рефарминг частот внутри своего частотного спектра (протокол № 13-22) [2].

2) На частотном спектре стандарта GSM-900 и GSM-1800 по решению ГКРЧ от 2016 года возможно проводить рефарминг (протокол № 16-37) [3].

3) В 2017 году принято решение разрешающее создание сетей связи стандарта LTE и последующих его модификаций в полосе частот UMTS-2100 (решение ГКРЧ № 17-44) [4].

Теперь, когда разобрана юридическая составляющая вопроса необходимо понять, почему рефарминг частот так актуален, то есть что является предпосылками для его проведения. Можно выделить следующие ключевые факторы:

1. Стремительное обновление парка устройств
2. Увеличение объемов потребляемого трафика
3. Терминалы высокого класса требуют более широкую частотную полосу в LTE чем доступна оператору (требуется довести до 3x20 МГц и выше)
4. Переход на более эффективные технологии, с лучшим сервисом:
Например, качество сервиса передачи пакетных данных и голосового трафика выше в сети LTE (VoLTE), чем в сети GSM/UMTS
5. Создание достаточного уровня сервиса (покрытия сети)

Технологическая составляющая может быть реализована различными методами, что обусловлено многообразием физических эффектов при возникновении помехового влияния между РЭС, а также сложностью законов распространения радиоволн и алгоритмов работы радиооборудования. Именно технологическая составляющая требует отдельного рассмотрения и согласования в рамках регулирования радиочастотного спектра при реализации технологической нейтральности [1].

Классификация систем рефарминга в разных источниках указывается по-разному, но в целом можно выделить два подхода: “статический” и “динамический” рефарминг [5, 6].

Основная идея динамического использования спектра (DSR) заключается в том, что соты LTE развернуты в спектре GSM, но подавляют передачу всех сигналов, включая опорные сигналы, в некоторых конкретных физических блоках, соответствующих части несущих GSM, для обеспечения полного покрытия GSM. Хотя концептуально это просто, это может включать в себя сложное частотное планирование. Что еще более важно, такой подход не позволяет операторам полностью “отдать” GSM-спектр для LTE [7]. Тем не менее, именно такое решение и используется при рефарминге GSM-спектра операторами в России. Соответственно необходимо проверить эффективность такого подхода.

Для этой цели была создана имитационная модель в MATLAB и произведен расчет потерь на трассе (Pathloss Estimation) в зависимости от расстояния между базовой станцией и абонентским устройством. Результаты представлены на рис. 1-3.

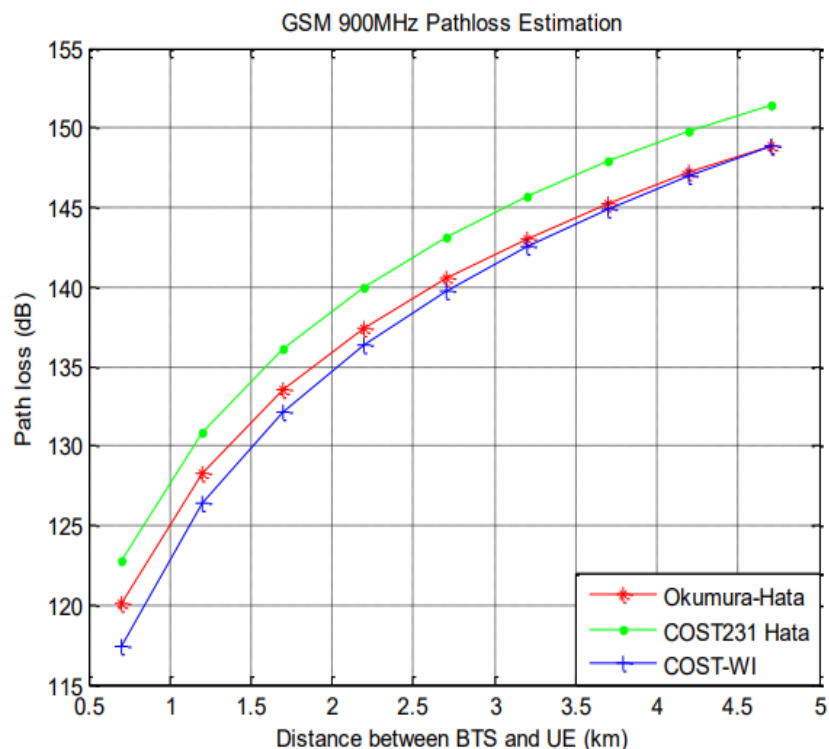


Рис. 1. Оценка потерь в тракте GSM-900

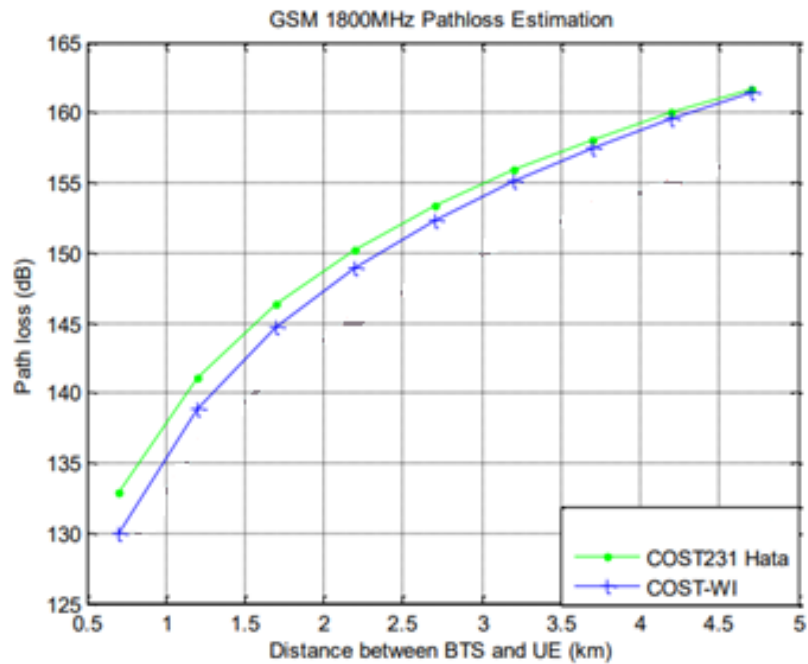


Рис. 2. Оценка потерь в тракте GSM-1800

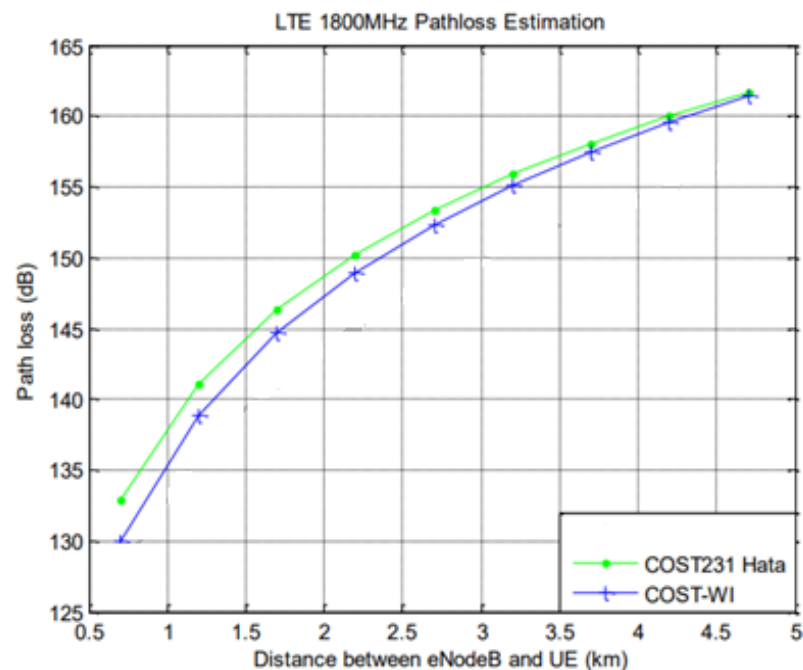


Рис. 3. Оценка потерь в тракте LTE-1800

Как показано на рис. 1, GSM обеспечивает максимальные потери на пути передачи 152 дБ при COST 231 Hata. На рис. 2 показан диапазон GSM-1800 МГц с максимальными потерями на пути примерно 162 дБ. Это показывает, что полоса 900 МГц имеет меньшие потери при распространении, что характерно для низких частот. На этой частоте также характерен более широкий охват. Полоса 1800 МГц не так интенсивно используется GSM, как полоса 900 МГц, она имеет большую пропускную способность и приводит к большему повторному использованию частот, подходящему для городских центров, когда трафик данных высок. Как показано на рис. 3, при развертывании LTE в диапазоне 1800 МГц максимальные потери на пути передачи составляют 162 дБ,

как и в GSM 1800 МГц. Следовательно, LTE сама по себе не обеспечивает увеличения покрытия.

С точки зрения покрытия результаты показывают, что операторы могут развернуть LTE 900/1800 МГц, используя существующие GSM-сайты.

Список используемых источников:

1. Коротин В. Е., Павлов Т. А.. Современные подходы к рефармингу в интересах 4-5 поколений мобильной связи и интернета вещей. 2020. – с. 4.
2. Решение Государственной комиссии по радиочастотам при Минкомсвязи России от 11 декабря 2013 г. № 13-22-01 "Об установлении условий использования полос радиочастот радиоэлектронными средствами сухопутной подвижной радиослужбы гражданского назначения при оказании услуг связи в населенных пунктах Российской Федерации" // URL: <https://files.stroyinf.ru/Data2/1/4293774/4293774843.htm>. (дата обращения: 15.11.2022)
3. Заседание ГКРЧ от 1 июля 2016 года (протокол №16-37) // URL: https://digital.gov.ru/ru/documents/5138/?utm_referrer=https%3a%2f%2fwww.google.com%2f. (дата обращения: 15.11.2022)
4. Заседание ГКРЧ от 28 декабря 2017 года (протокол №17-44) // URL: <https://digital.gov.ru/ru/documents/5875/>. (дата обращения: 15.11.2022)
5. Lin, Xingqin & Viswanathan, Harish. (2013). Dynamic Spectrum Refarming with Overlay for Legacy Devices. IEEE Transactions on Wireless Communications. 12. 10.1109/TWC.2013.092313.130227.
6. Lin, Xingqin & Viswanathan, Harish. (2013). Dynamic Spectrum Refarming of GSM Spectrum for LTE Small Cells. 10.1109/GLOCOMW.2013.6825068.
7. Francis Idachaba, Adeyemi Alatishe. Refarming 1800MHz GSM Spectrum to LTE: The Effects on Coverage Based on Pathloss Estimation

Korotin V., Vtorykh V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Research the efficiency of refarming from the point of the impact on the network coverage. Currently, spectrum refarming is a cost-effective way to increase network capacity from existing 2G/3G/LTE bands without the need for operators to purchase new frequency bands. In this regard, it makes sense to study the existing solutions in the field of radio frequency refarming, the current legislative framework in this area, and also to conduct simulations to estimate propagation losses in the conditions of spectrum refarming.

Key words: communications, refarming, frequency spectrum, LTE, GSM, UMTS.

УДК 004.716
ГРНТИ 49.37.33

ВИРТУАЛИЗАЦИЯ УЗЛОВ ЯДРА СЕТИ СОТОВОЙ СВЯЗИ

М. Н. Косьянов, О. В. Воробьев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящей работе рассматриваются способы и особенности виртуализации ядра сети сотовой связи на примере ядра сети 2G GSM. Представлена структурная схема организации связи с помощью виртуальных компонентов. Рассмотрена возможность развертывания виртуального ядра сети на персональном компьютере. В заключении приводится результат работы виртуального ядра, подключенного к действующему оборудованию.

2G, core network, виртуальное ядро, базовая станция

Структурная схема организации связи с помощью виртуальных элементов выглядит следующим образом:

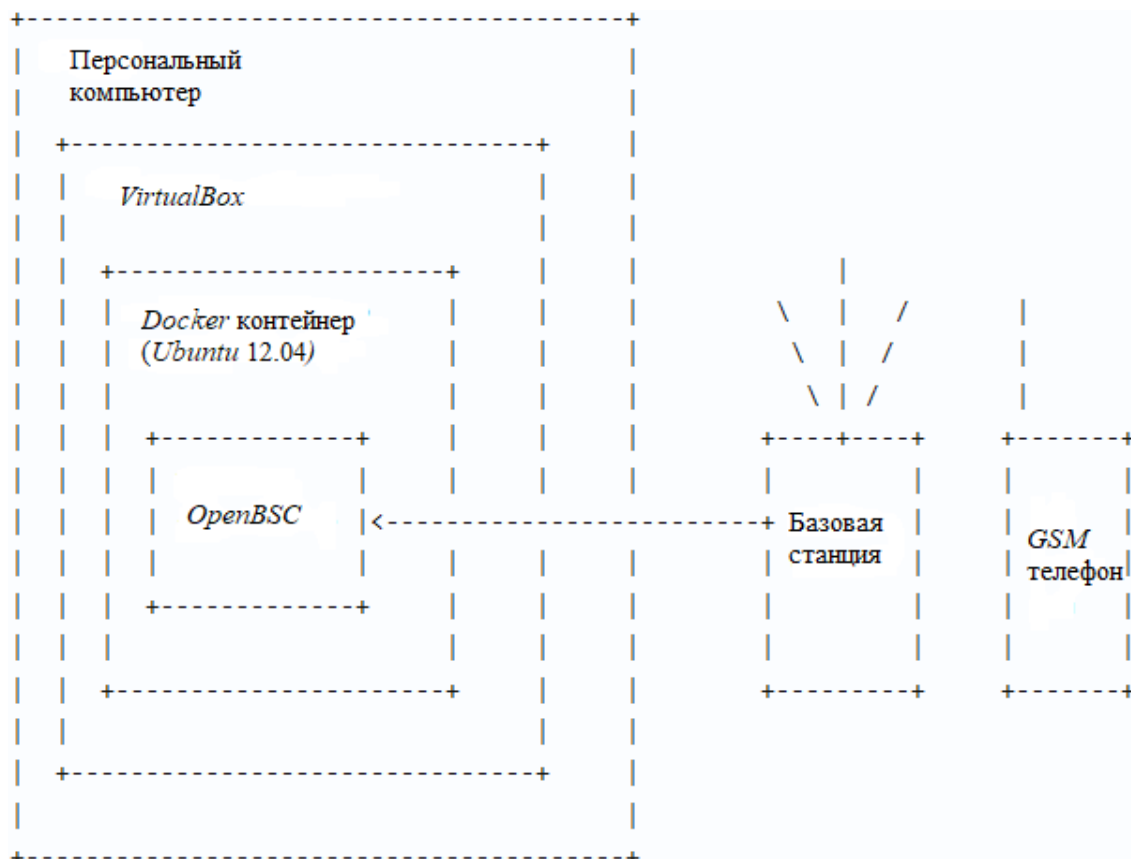


Рис. 1. Структурная схема виртуальной сети GSM

Первым компонентом данной схемы (рис. 1) является персональный компьютер, на его основе разворачивается наша виртуальная сеть. Следующим представлен *VirtualBox*, необходимый для дальнейшей установки виртуальной операционной системы (*Ubuntu 12.04*), с помощью которой происходит настройка, управление и редактирование сети GSM. Центром данной системы

является *OpenBSC*. Этот компонент включает в себя весь функционал физической *BSC*. Дальнейшая схема является стандартной для *2G GSM* и включает в себя базовую станцию и оконечное абонентское устройство с поддержкой *GSM* [1].

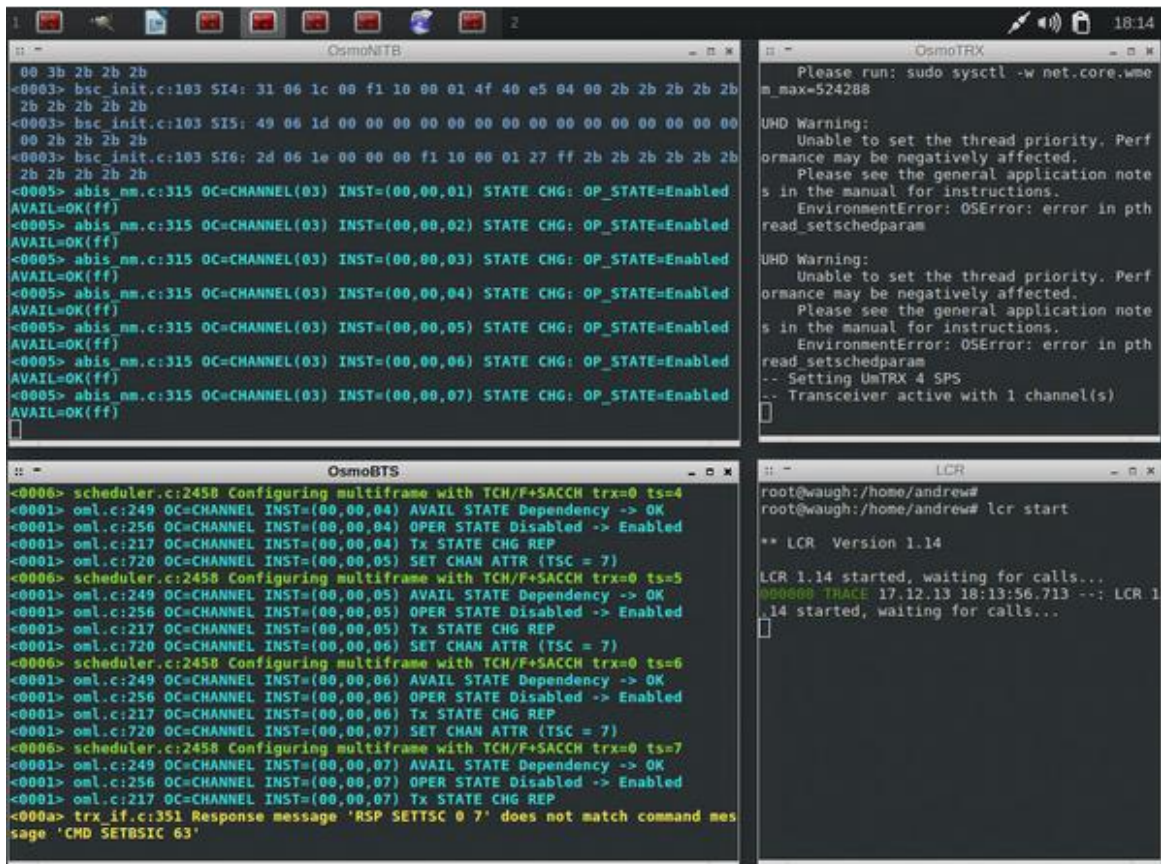
Построим сеть *2G GSM* на частоте 1800 МГц. Нам необходимо установить *ARFCN* в соответствии с фактическими частотами, также рекомендуется изменить политику аутентификации на закрытую, чтобы предотвратить вход в сеть неавторизованных телефонов. В дальнейшем можно изменить *MCC* и *MNC* [2].

Используемое мной программное обеспечение *Osmocom* может быть настроено для использования следующих технологий:

1. *GSM400*;
2. *GSM850*;
3. *GSM900*;
4. *DCS1800*;
5. *PCS1900*.

Диапазон устанавливается на уровне *BTS* и настраивается как в *OsmoBTS*(*osmo-bts.cfg*), так и в *OpenBSC*(*open-bsc.cfg*).

Начало работы:



```

OsmoNTB
00 3b 2b 2b 2b
<0003> bsc_init.c:103 SI4: 31 06 1c 00 f1 10 00 01 4f 40 e5 04 00 2b 2b 2b 2b
2b 2b 2b 2b
<0003> bsc_init.c:103 SI5: 49 06 1d 00 00 00 00 00 00 00 00 00 00 00 00 00
00 2b 2b 2b 2b
<0003> bsc_init.c:103 SI6: 2d 06 1e 00 00 00 f1 10 00 01 27 ff 2b 2b 2b 2b
2b 2b 2b 2b
<0005> abis_nm.c:315 OC=CHANNEL(03) INST=(00,00,01) STATE CHG: OP_STATE=Enabled
AVAIL=OK(ff)
<0005> abis_nm.c:315 OC=CHANNEL(03) INST=(00,00,02) STATE CHG: OP_STATE=Enabled
AVAIL=OK(ff)
<0005> abis_nm.c:315 OC=CHANNEL(03) INST=(00,00,03) STATE CHG: OP_STATE=Enabled
AVAIL=OK(ff)
<0005> abis_nm.c:315 OC=CHANNEL(03) INST=(00,00,04) STATE CHG: OP_STATE=Enabled
AVAIL=OK(ff)
<0005> abis_nm.c:315 OC=CHANNEL(03) INST=(00,00,05) STATE CHG: OP_STATE=Enabled
AVAIL=OK(ff)
<0005> abis_nm.c:315 OC=CHANNEL(03) INST=(00,00,06) STATE CHG: OP_STATE=Enabled
AVAIL=OK(ff)
<0005> abis_nm.c:315 OC=CHANNEL(03) INST=(00,00,07) STATE CHG: OP_STATE=Enabled
AVAIL=OK(ff)

OsmoBTS
<0006> scheduler.c:2450 Configuring multiframe with TCH/F+SACCH trx=0 ts=4
<0001> oml.c:249 OC=CHANNEL INST=(00,00,04) AVAIL STATE Dependency -> OK
<0001> oml.c:256 OC=CHANNEL INST=(00,00,04) OPER STATE Disabled -> Enabled
<0001> oml.c:217 OC=CHANNEL INST=(00,00,04) Tx STATE CHG REP
<0001> oml.c:720 OC=CHANNEL INST=(00,00,05) SET CHAN ATTR (TSC = 7)
<0006> scheduler.c:2450 Configuring multiframe with TCH/F+SACCH trx=0 ts=5
<0001> oml.c:249 OC=CHANNEL INST=(00,00,05) AVAIL STATE Dependency -> OK
<0001> oml.c:256 OC=CHANNEL INST=(00,00,05) OPER STATE Disabled -> Enabled
<0001> oml.c:217 OC=CHANNEL INST=(00,00,05) Tx STATE CHG REP
<0001> oml.c:720 OC=CHANNEL INST=(00,00,06) SET CHAN ATTR (TSC = 7)
<0006> scheduler.c:2450 Configuring multiframe with TCH/F+SACCH trx=0 ts=6
<0001> oml.c:249 OC=CHANNEL INST=(00,00,06) AVAIL STATE Dependency -> OK
<0001> oml.c:256 OC=CHANNEL INST=(00,00,06) OPER STATE Disabled -> Enabled
<0001> oml.c:217 OC=CHANNEL INST=(00,00,06) Tx STATE CHG REP
<0001> oml.c:720 OC=CHANNEL INST=(00,00,07) SET CHAN ATTR (TSC = 7)
<0006> scheduler.c:2450 Configuring multiframe with TCH/F+SACCH trx=0 ts=7
<0001> oml.c:249 OC=CHANNEL INST=(00,00,07) AVAIL STATE Dependency -> OK
<0001> oml.c:256 OC=CHANNEL INST=(00,00,07) OPER STATE Disabled -> Enabled
<0001> oml.c:217 OC=CHANNEL INST=(00,00,07) Tx STATE CHG REP
<000a> trx_if.c:351 Response message 'RSP SETTSC 0 7' does not match command mes
sage 'CMD SETBSIC 63'

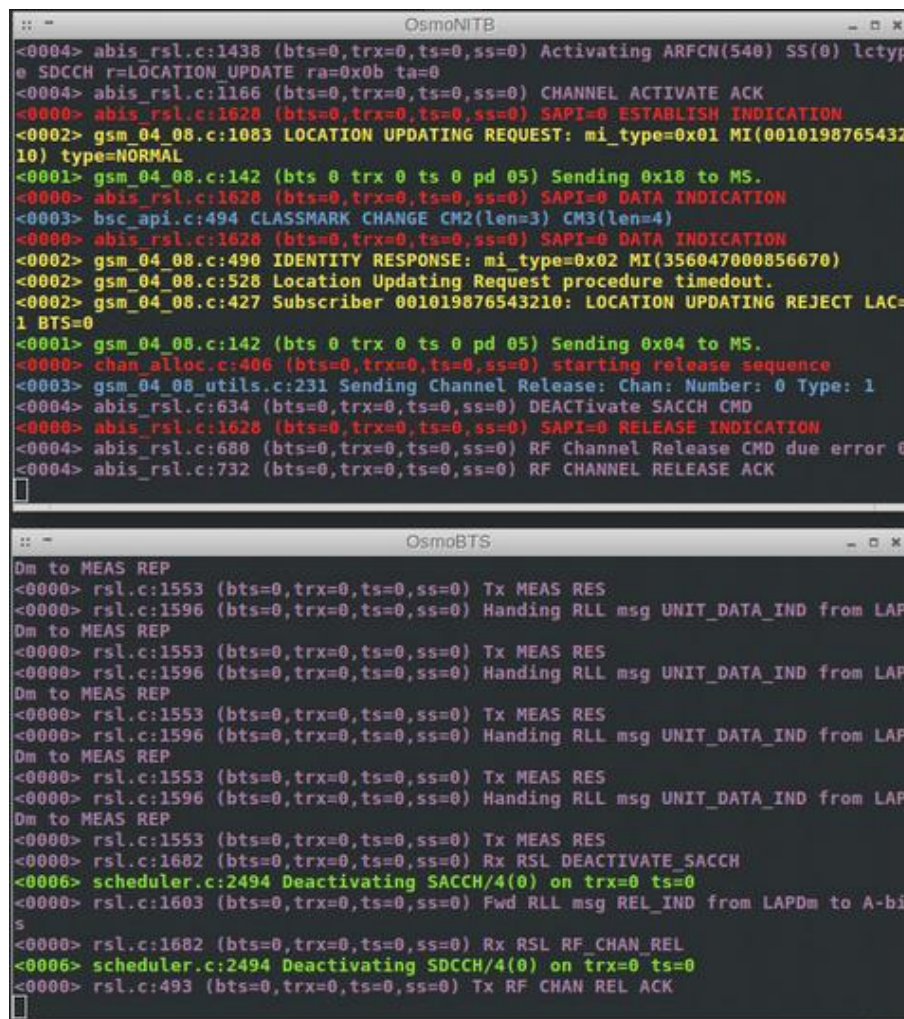
LCR
root@waugh:/home/andrew#
root@waugh:/home/andrew# lcr start
** LCR Version 1.14
LCR 1.14 started, waiting for calls...
000000 TRACE 17.12.13 18:13:56.713 --: LCR 1
.14 started, waiting for calls...
    
```

Рис. 2. Запуск *OsmoBTS*, *LCR*, *OsmoNTB*, *OsmoTRX*

Запуск каждого компонента в своей собственной оболочке облегчает мониторинг активности и отладку любых проблем.

Авторизация абонента:

Для начала нужно удостовериться, что пользователи зарегистрированы в *open-bsc.cfg*, так как в нашем случае политика авторизации установлена в закрытом режиме, запросы об обновлении местоположения от незарегистрированных абонентов будут отклонены и им не будет предоставлен сетевой сервис.



```

OsmoNITB
<0004> abis_rsl.c:1438 (bts=0,trx=0,ts=0,ss=0) Activating ARFCN(540) SS(0) lctyp
e SDCCH r=LOCATION_UPDATE ra=0x0b ta=0
<0004> abis_rsl.c:1166 (bts=0,trx=0,ts=0,ss=0) CHANNEL ACTIVATE ACK
<0000> abis_rsl.c:1628 (bts=0,trx=0,ts=0,ss=0) SAPI=0 ESTABLISH INDICATION
<0002> gsm_04_08.c:1083 LOCATION UPDATING REQUEST: mi_type=0x01 MI(0010198765432
10) type=NORMAL
<0001> gsm_04_08.c:142 (bts 0 trx 0 ts 0 pd 05) Sending 0x18 to MS.
<0000> abis_rsl.c:1628 (bts=0,trx=0,ts=0,ss=0) SAPI=0 DATA INDICATION
<0003> bsc_api.c:494 CLASSMARK CHANGE CM2(len=3) CM3(len=4)
<0000> abis_rsl.c:1628 (bts=0,trx=0,ts=0,ss=0) SAPI=0 DATA INDICATION
<0002> gsm_04_08.c:490 IDENTITY RESPONSE: mi_type=0x02 MI(356047000856670)
<0002> gsm_04_08.c:528 Location Updating Request procedure timedout.
<0002> gsm_04_08.c:427 Subscriber 001019876543210: LOCATION UPDATING REJECT LAC=
1 BTS=0
<0001> gsm_04_08.c:142 (bts 0 trx 0 ts 0 pd 05) Sending 0x04 to MS.
<0000> chan_alloc.c:406 (bts=0,trx=0,ts=0,ss=0) starting release sequence
<0003> gsm_04_08_utils.c:231 Sending Channel Release: Chan: Number: 0 Type: 1
<0004> abis_rsl.c:634 (bts=0,trx=0,ts=0,ss=0) DEACTIVATE SACCH CMD
<0000> abis_rsl.c:1628 (bts=0,trx=0,ts=0,ss=0) SAPI=0 RELEASE INDICATION
<0004> abis_rsl.c:680 (bts=0,trx=0,ts=0,ss=0) RF Channel Release CMD due error 0
<0004> abis_rsl.c:732 (bts=0,trx=0,ts=0,ss=0) RF CHANNEL RELEASE ACK

OsmoBTS
Dm to MEAS REP
<0000> rsl.c:1553 (bts=0,trx=0,ts=0,ss=0) Tx MEAS RES
<0000> rsl.c:1596 (bts=0,trx=0,ts=0,ss=0) Handing RLL msg UNIT_DATA_IND from LAP
Dm to MEAS REP
<0000> rsl.c:1553 (bts=0,trx=0,ts=0,ss=0) Tx MEAS RES
<0000> rsl.c:1596 (bts=0,trx=0,ts=0,ss=0) Handing RLL msg UNIT_DATA_IND from LAP
Dm to MEAS REP
<0000> rsl.c:1553 (bts=0,trx=0,ts=0,ss=0) Tx MEAS RES
<0000> rsl.c:1596 (bts=0,trx=0,ts=0,ss=0) Handing RLL msg UNIT_DATA_IND from LAP
Dm to MEAS REP
<0000> rsl.c:1553 (bts=0,trx=0,ts=0,ss=0) Tx MEAS RES
<0000> rsl.c:1596 (bts=0,trx=0,ts=0,ss=0) Handing RLL msg UNIT_DATA_IND from LAP
Dm to MEAS REP
<0000> rsl.c:1553 (bts=0,trx=0,ts=0,ss=0) Tx MEAS RES
<0000> rsl.c:1596 (bts=0,trx=0,ts=0,ss=0) Handing RLL msg UNIT_DATA_IND from LAP
Dm to MEAS REP
<0000> rsl.c:1553 (bts=0,trx=0,ts=0,ss=0) Tx MEAS RES
<0000> rsl.c:1602 (bts=0,trx=0,ts=0,ss=0) Rx RSL DEACTIVATE SACCH
<0006> scheduler.c:2494 Deactivating SACCH/4(0) on trx=0 ts=0
<0000> rsl.c:1603 (bts=0,trx=0,ts=0,ss=0) Fwd RLL msg REL_IND from LAPDm to A-bi
s
<0000> rsl.c:1602 (bts=0,trx=0,ts=0,ss=0) Rx RSL RF_CHAN_REL
<0006> scheduler.c:2494 Deactivating SDCCH/4(0) on trx=0 ts=0
<0000> rsl.c:493 (bts=0,trx=0,ts=0,ss=0) Tx RF_CHAN_REL ACK
    
```

Рис. 3. Запрос на обновление местоположения

Выше мы видим, что полученный запрос на обновление местоположения был отклонен. Так как это первый запрос от *MS* с момента инициализации базы данных, абоненту был присвоен *ID 1*.

При следующей попытке запроса обновления местоположения мобильный телефон был принят.


```

<0003> bsc_api.c:494 CLASSMARK CHANGE CM2(len=3) CM3(len=4)
<0000> abis_rsl.c:1628 (bts=0,trx=0,ts=0,ss=0) SAPI=0 DATA INDICATION
<0002> gsm_04_08.c:490 IDENTITY RESPONSE: mi_type=0x02 MI(356047000856670)
<0002> gsm_04_08.c:454 -> LOCATION UPDATE ACCEPT
<0001> gsm_04_08.c:142 (bts 0 trx 0 ts 0 pd 05) Sending 0x02 to MS.
<0002> gsm_04_08.c:796 -> MM INFO
<0001> gsm_04_08.c:142 (bts 0 trx 0 ts 0 pd 05) Sending 0x32 to MS.
<0002> gsm_subscriber.c:361 Subscriber 1019876543210 ATTACHED LAC=1
<0003> gsm_04_08.c:1215 TX APPLICATION INFO id=0x00, len=4
<0001> gsm_04_08.c:142 (bts 0 trx 0 ts 0 pd 06) Sending 0x38 to MS.
<0000> abis_rsl.c:1628 (bts=0,trx=0,ts=0,ss=0) SAPI=0 DATA INDICATION
<0002> gsm_04_08.c:1099 TMSI Reallocation Completed. Subscriber: 1019876543210
<0000> chan_alloc.c:406 (bts=0,trx=0,ts=0,ss=0) starting release sequence
<0003> gsm_04_08_utils.c:231 Sending Channel Release: Chan: Number: 0 Type: 1
<0004> abis_rsl.c:634 (bts=0,trx=0,ts=0,ss=0) DEACTivate SACCH CMD
<0000> abis_rsl.c:1628 (bts=0,trx=0,ts=0,ss=0) SAPI=0 DATA INDICATION
<0004> bsc_api.c:659 Got data in non active state(RELEASE REQUESTED), discarding
.
<0000> abis_rsl.c:1628 (bts=0,trx=0,ts=0,ss=0) SAPI=0 RELEASE INDICATION
<0004> abis_rsl.c:680 (bts=0,trx=0,ts=0,ss=0) RF Channel Release CMD due error 0
<0004> abis_rsl.c:732 (bts=0,trx=0,ts=0,ss=0) RF CHANNEL RELEASE ACK
    
```

Рис. 4. Подключение мобильного телефона

Приведенный алгоритм действий позволяет развернуть собственную 2G сеть у себя дома [3]. Нужно помнить, что для проведения, что проводить подобные эксперименты необходимо либо в клетке Фарадея, в этом случае весь радиочастотный спектр в вашем распоряжении и можно указать любую пару чисел в диапазоне от 512 до 885 с разнице примерно в 10 каналов, либо проводить эксперимент в присутствии специалиста, который поможет вам найти пару неиспользованных каналов [4].

Список используемых источников:

1. Falih M. D. et al. Implementation of GPRS Service on Mobile Network Based OSMOCOM //2019 IEEE Conference on Sustainable Utilization and Development in Engineering and Technologies (CSUDET). – IEEE, 2019. – С. 276-280.
2. Paudel S. Investigation, Analysis and Implementation of Open Source Mobile Communication Software : дис. – NTNU, 2016.
3. Welte H., Markgraf S. Running your own GSM stack on a phone //27C3. Berlin, CCC. <http://events.ccc.de/congress/2010/Fahrplan/events/3952.en.html>. – 2010.
4. Lu F. et al. A virtualization-based cloud infrastructure for IMS core network //2013 IEEE 5th International Conference on Cloud Computing Technology and Science. – IEEE, 2013. – Т. 1. – С. 25-32.

Kosyanov M., Vorobev O.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Core network virtualization.

In this present work, the methods and features of virtualization of cellular network core on the example of 2G GSM network core. It presents a structural diagram of the organization of communication using virtual components. The possibility of deploying a virtual network core on a personal computer. In conclusion, the result of the virtual core connected to the existing equipment.

Key words: 2G, core network, consciousness, base station.

УДК 621.396.99
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ПАРАМЕТРОВ РАДИОКАНАЛА ДЛЯ ПЕРЕДАЧИ ТРАФИКА В СЕТЯХ СТАНДАРТА NEW RADIO

А. А. Кузьмин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича

Представлены основные различия сетей четвертого поколения (LTE) и пятого поколения (NR). Рассмотрены варианты размещения сигналов демодуляции в частотной и временной областях радиоканалов NR. Представлены результаты расчетов максимальных скоростей передачи данных без MIMO и дополнительной агрегации частотных полос при передаче вниз и вверх для сетей NR.

сеть NR, каналный ресурс, опорные сигналы DM-RS, пропускная способность

Появление стандарта NR обусловлено возрастающими требованиями к общей пропускной способности сети мобильной связи и быстрым развитием сетей интернета вещей. Сети стандарта New Radio имеют существенные отличия от сетей LTE.

Одним из значимых отличий является ширина полосы радиоканала. В LTE она может достигать 20 МГц, а в стандарте NR 100 МГц или 400 МГц в зависимости от частотного диапазона.

Основным различием является то, что в структуре NR каналный ресурс выделяется в виде ресурсных блоков на слот. В нисходящем канале PDSCH и восходящем канале PUSCH для синхронизации приема и для работы систем MIMO используются опорные сигналы демодуляции DM-RS, которые многовариантны как в частотной области, так и во временной области. Для передачи вниз и вверх в частотной области возможны 2 конфигурации размещения сигналов демодуляции – это конфигурация типа 1 и конфигурация типа 2. Конфигурация типа 1 приведена на рис. 1 (слева) [1]. При данной конфигурации внутри ресурсного блока номера поднесущих, на которых расположены опорные сигналы демодуляции DM-RS, определяются формулой [1]:

$$k = 4n + 2k' + \Delta,$$

где $n = 0; 1; 2$, $k' = 0; 1$, а Δ – в режиме MIMO определяется числом активных антенн. Конфигурация типа 2 показана на рис. 1 (справа). При данной конфигурации в ресурсном блоке будут только 4 опорных сигнала демодуляции, позиции которых задаются формулой:

$$k = 6n + k' + \Delta,$$

где $n = 0; 1$; $k = 0; 1$, а Δ – в режиме MIMO определяется числом активных антенн. Выбор конфигурации зависит от предоставляемой услуги и условий передачи трафика. Это является одной из задач, решаемых планировщиком на базовой станции.

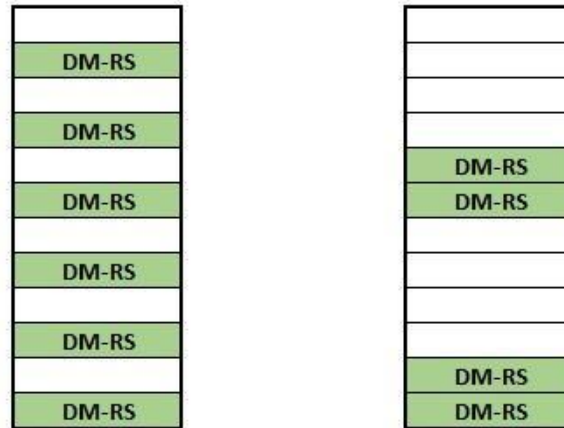


Рис. 1. Конфигурация типа 1 и 2

Во временной области расположение опорных сигналов демодуляции зависит от структуры канала PDSCH, который может быть двух типов: «А» и «В». Два вышеперечисленных типа специфицированы в [1], позиции сигналов DM-RS приведены в таблице 1, где для канала типа «А» $l_0 = 3$ и $l_1 = 11$, а для канала типа «В» $l_0 = 0$.

ТАБЛИЦА 1. Расположение DM-RS во временной области в канале PDSCH

Число OFDM-символов в	Позиции DM-RS							
	PDSCH тип А				PDSCH тип В			
	Дополнительные позиции DM-RS				Дополнительные позиции DM-RS			
	Поз. 0	Поз. 1	Поз. 2	Поз. 3	Поз. 0	Поз. 1	Поз. 2	Поз. 3
2	-	-	-	-	l_0	l_0	l_0	l_0
3	l_0	l_0	l_0	l_0	l_0	l_0	l_0	l_0
4	l_0	l_0	l_0	l_0	l_0	l_0	l_0	l_0
5	l_0	l_0	l_0	l_0	l_0	$l_0, 4$	$l_0, 4$	$l_0, 4$
6	l_0	l_0	l_0	l_0	l_0	$l_0, 4$	$l_0, 4$	$l_0, 4$
7	l_0	l_0	l_0	l_0	l_0	$l_0, 4$	$l_0, 4$	$l_0, 4$
8	l_0	$l_0, 7$	$l_0, 7$	$l_0, 7$	l_0	$l_0, 6$	$l_0, 3, 6$	$l_0, 3, 6$
9	l_0	$l_0, 7$	$l_0, 7$	$l_0, 7$	l_0	$l_0, 7$	$l_0, 4, 7$	$l_0, 4, 7$
10	l_0	$l_0, 9$	$l_0, 6, 9$	$l_0, 6, 9$	l_0	$l_0, 7$	$l_0, 4, 7$	$l_0, 4, 7$
11	l_0	$l_0, 9$	$l_0, 6, 9$	$l_0, 6, 9$	l_0	$l_0, 8$	$l_0, 4, 8$	$l_0, 3, 6, 9$
12	l_0	$l_0, 9$	$l_0, 6, 9$	$l_0, 5, 8, 11$	l_0	$l_0, 9$	$l_0, 5, 9$	$l_0, 3, 6, 9$
13	l_0	l_0, l_1	$l_0, 7, 11$	$l_0, 5, 8, 11$	l_0	$l_0, 9$	$l_0, 5, 9$	$l_0, 3, 6, 9$
14	l_0	l_0, l_1	$l_0, 7, 11$	$l_0, 5, 8, 11$	-	-	-	-

Канал типа «В» – это канал для вариантов, когда для передачи пользовательского трафика не требуется выделение целого слота. В канале типа «А» тоже может быть выделена только часть слота, но в отличии от канала типа

«В», где для этого требуется наличие хотя бы двух OFDM-символов, для этого необходимо наличие как минимум трех OFDM-символов.

Сигналы DM-RS могут размещаться в одном, двух, трех или четырех ресурсных блоках. Все зависит от объема ресурсных блоков в слоте и качества канала. На рис. 2 приведены варианты размещения сигналов DM-RS в канале типа «А».

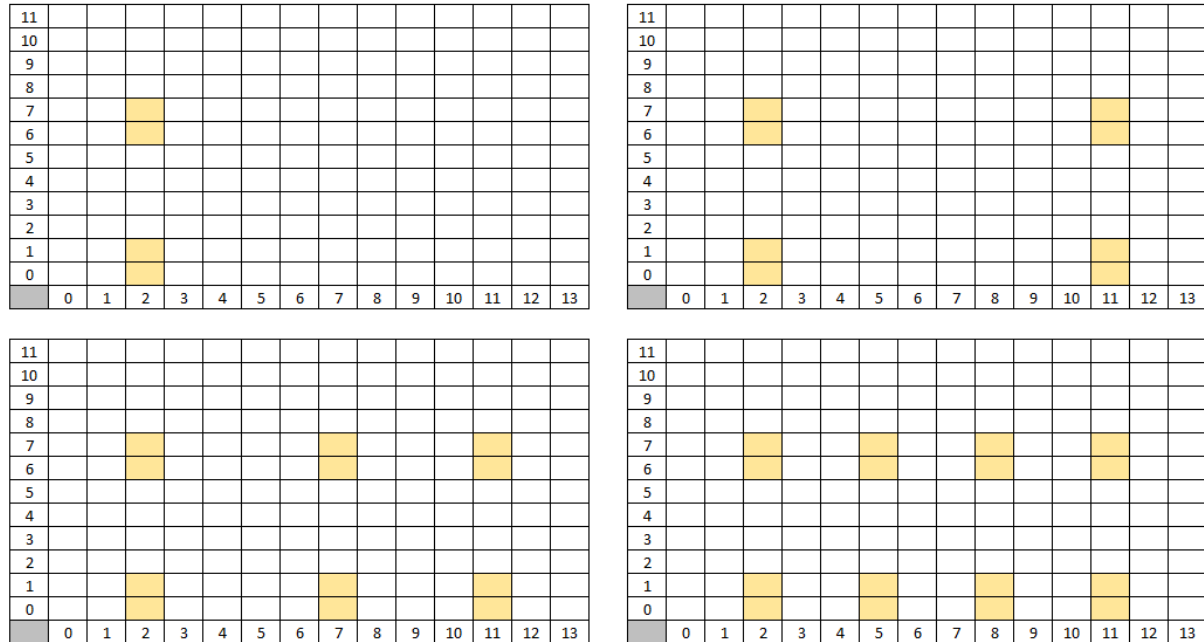


Рис. 2. Варианты размещения сигналов DM-RS в PDSCH типа «А»

Канал передачи вверх PUSCH так же может быть двух типов: «А» и «В». Два этих типа специфицированы в [1], размещение символов DM-RS приведено в таблице 2, где для канала типа «А» l_0 задается параметром dmrs-TypeA-Position, а для канала типа «В» $l_0 = 0$.

ТАБЛИЦА 2. Расположение DM-RS во временной области в канале PUSCH

Число OFDM-символов в	Позиции DM-RS							
	PUSCH тип А				PUSCH тип В			
	Дополнительные позиции DM-RS				Дополнительные позиции DM-RS			
	Поз. 0	Поз. 1	Поз. 2	Поз. 3	Поз. 0	Поз. 1	Поз. 2	Поз. 3
<4	-	-	-	-	l_0	l_0	l_0	l_0
4	l_0	l_0	l_0	l_0	l_0	l_0	l_0	l_0
5	l_0	l_0	l_0	l_0	l_0	$l_0, 4$	$l_0, 4$	$l_0, 4$
6	l_0	l_0	l_0	l_0	l_0	$l_0, 4$	$l_0, 4$	$l_0, 4$
7	l_0	l_0	l_0	l_0	l_0	$l_0, 4$	$l_0, 4$	$l_0, 4$
8	l_0	$l_0, 7$	$l_0, 7$	$l_0, 7$	l_0	$l_0, 6$	$l_0, 3, 6$	$l_0, 3, 6$
9	l_0	$l_0, 7$	$l_0, 7$	$l_0, 7$	l_0	$l_0, 6$	$l_0, 3, 6$	$l_0, 3, 6$
10	l_0	$l_0, 9$	$l_0, 6, 9$	$l_0, 6, 9$	l_0	$l_0, 8$	$l_0, 4, 8$	$l_0, 3, 6, 9$
11	l_0	$l_0, 9$	$l_0, 6, 9$	$l_0, 6, 9$	l_0	$l_0, 8$	$l_0, 4, 8$	$l_0, 3, 6, 9$
12	l_0	$l_0, 9$	$l_0, 6, 9$	$l_0, 5, 8, 11$	l_0	$l_0, 10$	$l_0, 5, 10$	$l_0, 3, 6, 9$
13	l_0	$l_0, 11$	$l_0, 7, 11$	$l_0, 5, 8, 11$	l_0	$l_0, 10$	$l_0, 5, 10$	$l_0, 3, 6, 9$
14	l_0	$l_0, 11$	$l_0, 7, 11$	$l_0, 5, 8, 11$	l_0	$l_0, 10$	$l_0, 5, 10$	$l_0, 3, 6, 9$

Сигналы DM-RS размещаются в одном, двух, трех или четырех ресурсных блоках, но их размещение во временной области отлично от размещения сигналов DM-RS в канале PDSCH. На рис. 3 приведены варианты размещения сигналов DM-RS в канале типа «B».

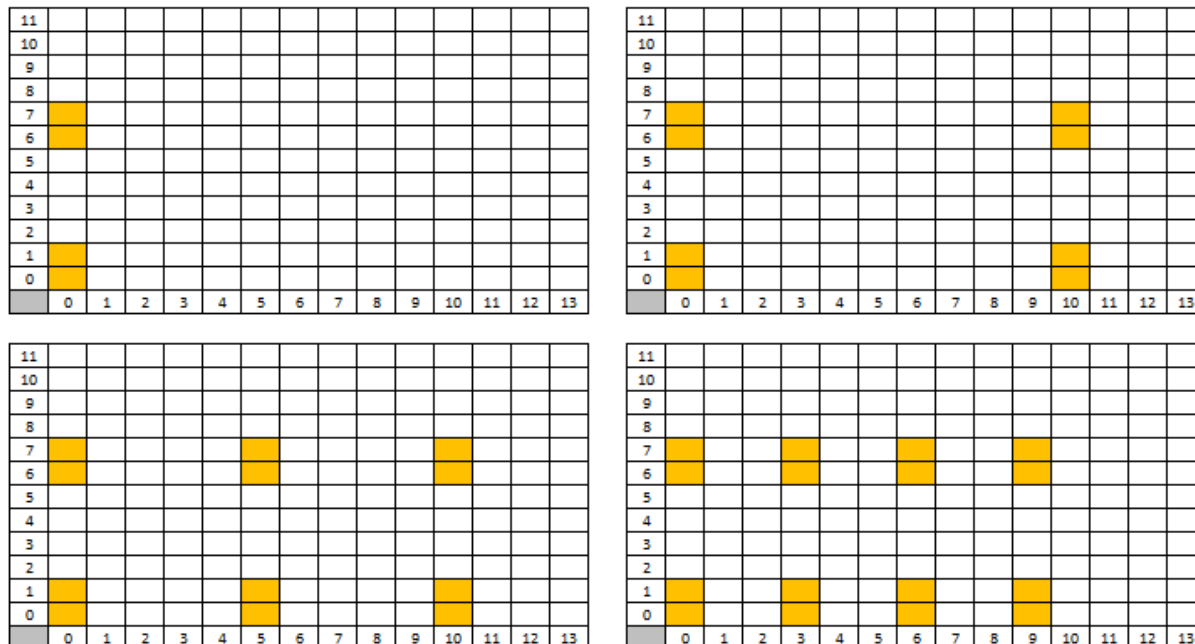


Рис. 3. Варианты размещения сигналов DM-RS в PUSCH типа «B»

Оценим скорости передачи вниз и вверх в сетях пятого поколения. При расчете скоростей передачи вниз для стандартов LTE и NR виден значительный прирост скоростей при увеличении ширины полосы частот. В сетях LTE с максимальной полосой 20 МГц без агрегации частотных полос и MIMO максимальные скорости достигают порядка 110 Мбит/с. Для стандарта NR с такой же полосой и при таких же условиях максимальные скорости схожие, но при увеличении полосы до 50 МГц и 100 МГц скорости значительно возрастают. При расчетах учтено наличие канала управления, на который необходимо около 10% от общей пропускной способности как вниз, так и вверх.

Например, при использовании модуляции 256-QAM, скорости избыточного кодирования 0,948 в полосе 50 МГц при размещении символов DM-RS в 2 ресурсных блоках получаем:

- при разnose поднесущих в 15 кГц $V_{инф} = 295$ Мбит/с.
- при разnose поднесущих в 30 кГц $V_{инф} = 291$ Мбит/с

При модуляции 256-QAM, скорости избыточного кодирования 0,948 в полосе 100 МГц при размещении символов DM-RS в 2 ресурсных блоках и разnose поднесущих в 30 кГц $V_{инф} = 596$ Мбит/с.

При расчете скоростей передачи вверх используются полосы 20, 50 и 100 МГц.

Если используем модуляцию 64-QAM и скорость избыточного кодирования 0,853 при размещении символов DM-RS в 2 ресурсных блоках получаем:

- в полосе 20 МГц при разnose поднесущих в 15 кГц $V_{инф} = 78$ Мбит/с.

- в полосе 20 МГц при разносе поднесущих в 30 кГц $V_{инф} = 75$ Мбит/с.
- в полосе 50 МГц при разносе поднесущих в 15 кГц $V_{инф} = 199$ Мбит/с.
- в полосе 50 МГц при разносе поднесущих в 30 кГц $V_{инф} = 196$ Мбит/с.
- в полосе 100 МГц при разносе поднесущих в 30 кГц $V_{инф} = 402$ Мбит/с.

Также возможен вариант использования модуляции 256-QAM и скорости избыточного кодирования 0,948, но на реально действующей сети такой вариант маловероятен. При использовании полосы 20, 50 и 100 МГц получаем следующие скорости передачи:

- в полосе 20 МГц при разносе поднесущих в 15 кГц $V_{инф} = 116$ Мбит/с.
- в полосе 20 МГц при разносе поднесущих в 30 кГц $V_{инф} = 111$ Мбит/с.
- в полосе 50 МГц при разносе поднесущих в 15 кГц $V_{инф} = 295$ Мбит/с.
- в полосе 50 МГц при разносе поднесущих в 30 кГц $V_{инф} = 291$ Мбит/с.
- в полосе 100 МГц при разносе поднесущих в 30 кГц $V_{инф} = 596$ Мбит/с.

Список используемых источников:

1. 3GPP TS 38.211 V17.3.0. NR; Physical channels and modulation. 2022. 136p.

Kuzmin A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Study of radio channel parameters for traffic transmission in New Radio networks.

The main differences between fourth generation (LTE) and fifth generation (NR) networks are presented. Options for placing demodulation signals in the frequency and time domains of NR radio channels are considered. The results of calculations of maximum data rates without MIMO and additional aggregation of frequency bands for down and up transmission for NR networks are presented.

Key words: *NR network, channel resource, DM-RS reference signals, throughput.*

УДК 621.396.94
ГРНТИ 49.37.29

ДИНАМИЧЕСКОЕ УПРАВЛЕНИЕ ЧАСТОТНО-ОРБИТАЛЬНЫМ РЕСУРСОМ НИЗКООРБИТАЛЬНЫХ СПУТНИКОВЫХ СИСТЕМ

А. Ю. Ларионов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Принципиально новый уровень гибкости и масштабируемости спутниковых сетей связи следующего поколения требует создания новых алгоритмов управления частотными ресурсами. Важно иметь возможность динамично управлять ими и иметь возможность быстро адаптировать их к условиям передачи и текущим потребностям пользователей сети, избегая при этом интерференции при передаче.

спутниковая связь, телекоммуникации, частотный ресурс, низкоорбитальные системы

Особенностью нового этапа развития сетей спутниковой связи является быстрое увеличение количества мобильных пользователей, таких как маломощные подвижные абонентские терминалы, самолёты, корабли. Сложностью при обслуживании таких пользователей является то, что необходимо минимизировать пространственно-временную неопределенность, возникающую из-за задержек при передаче сигнала, а также частого изменения местоположения и траектории движения абонента. Учитывая, что мобильные пользователи составляют важный сегмент рынка, спутниковым операторам важно использовать современные гибкие стратегии распределения частотного ресурса, устойчивого к динамическому изменению текущей обстановки.

Традиционные спутниковые системы как правило размещаются на геостационарной орбите и используют широкие лучи для покрытия больших областей, при этом рассеивая доступные мощностные и частотные ресурсы. Спутниковые системы следующего поколения заполняют собой негеостационарные орбиты и имеют возможность создания точечного луча для обслуживания конкретных сравнительно небольших областей и абонентских терминалов [1]. Эти более узкие точечные лучи имеют гораздо более острую направленность и, следовательно, выше коэффициент усиления передачи и приема, что позволяет использовать пользовательское оборудование меньшего размера, требует меньше энергозатрат, а также использовать схемы модуляции высокого порядка для увеличения скорости передачи данных [2]. Также при этом появляется возможность управления лучами, повторно использовать частотные ресурсы и перераспределять мощность между конкретными лучами согласно текущим потребностям.

Использование этих дополнительных возможностей, особенно перераспределение частотных ресурсов в режиме реального времени, имеет решающее значение для повышения эффективности системы связи, улучшения качества обслуживания пользователей, а также появления возможности применения новых вариантов сервиса для абонентов.

Далее будут предложены ограничения, позволяющие избежать интерференции при многолучевой передаче. Предположим, что все спутники идентичны и имеют доступ к одному и тому же частотному ресурсу, разделенному на N_{ch} частотных каналов, и каждый спутник при этом имеет N_r вариантов наборов частот с повторным использованием и N_p вариантов поляризации. Конкретные комбинации повторного использования частот и поляризации также называются группами ресурсов.

На рис. 1 представлен частотный план в виде сетки с $N_r \cdot N_p$ строк (групп ресурсов) и N_{ch} столбцов (частотных каналов).

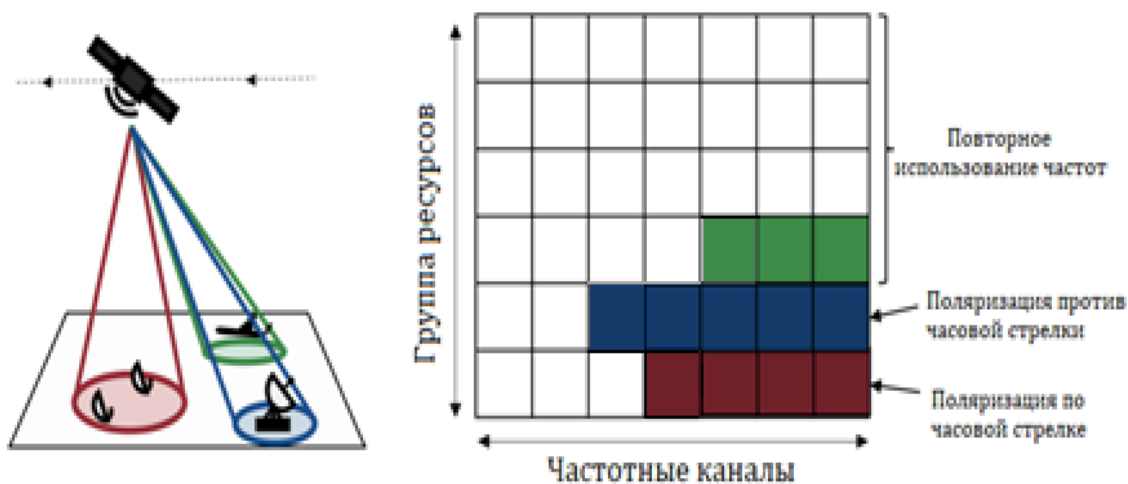


Рис. 1. Пример частотного плана

Основная задача состоит в том, чтобы верно задать характеристику A для каждого из лучей:

$$A = \{ \alpha_i = (f_i, b_i, g_i, p_i, e_i) \} \forall i \{ 1, \dots, N_{b_u} + N_{b_g} \} \quad (1)$$

где f_i - начальная частота луча i , b_i - количество частотных каналов луча i , g_i - повторное использование групп частот, p_i - поляризация луча i , e_i - флаг активности луча i .

Флаг активности позволяет деактивировать лучи, для которых на данный момент невозможно найти допустимое значение частоты, а также все другие лучи, связанные с ним [3]. Например, если пользовательскому лучу не удастся назначить частотный ресурс, то связанные с ним ресурсы шлюза также могут быть деактивированы.

Для каждого луча можно определить минимальное число $b_{min,i}$ и максимальное число $b_{max,i}$ частотных каналов, которые необходимы для удовлетворения его потребностей с учетом самого высокого и самого низкого значения спектральной эффективности системы. Если $b_i < b_{min,i}$ потребности абонента не будут удовлетворены и нужны дополнительные ресурсы, а если $b_i > b_{max,i}$, то излишние частоты могут быть назначены другому лучу, так как потребность текущего абонента может быть удовлетворена за счет меньшего количества частотных каналов.

Переменные частотного присвоения определяются как:

$$\begin{aligned}
 0 &\leq f_i \forall i \\
 f_i + b_i &\leq N_{ch} \forall i \\
 b_{min,i} &\leq b_i \leq b_{max,i} \forall i \\
 0 &\leq g_i \leq N_r \forall i \\
 0 &\leq p_i \leq N_p \forall i \\
 f_i, b_i, g_i, p_i &\in Z \forall i
 \end{aligned} \tag{2}$$

Присвоение частот зависит от двух основных факторов: помехового воздействия, а также ограничений на повторное использования частоты, кодируемых с использованием двоичных переменных α_{ij} и β_{ij} [4]. Ограничение на повторное использование частот гарантирует, что любые два луча, назначенные одному и тому же спутнику, в некоторый момент $\beta_{ij} = 1$ ($\beta_{ij} = 0$ в противном случае) не используют одновременно один и тот же частотный канал. Это ограничение гарантирует, что мы не назначаем одновременно одни и те же ресурсы частотные ресурсы нескольким лучам, учитывая информацию о передвижении мобильной станции. Следовательно, чтобы правильно применить данное ограничение, необходимо принять во внимание время начала и окончания обслуживания абонента, данные об изменении местоположения мобильной станции, а также данные об используемом им шлюзовом луче от сервера к спутнику.

Ограничение помехового воздействия гарантирует, что два луча, излучаемых одним и тем же спутником, и проходящие в непосредственной близости друг о друга, не подвергаются интерференции. Ограничение интерференции основано на величине углового расстояния $\gamma_{ij}(t)$ между лучами i и j . Этот угловой разнос зависит от положения лучей в момент времени t . Таким образом, хотя величина минимального углового разноса изменяется со временем, интерференционные ограничения между лучами не должны зависеть от положения спутника относительно абонента. Два луча считаются расположенными достаточно близко, чтобы создавать интерференционное воздействие $\alpha = 1$, если $\gamma_{ij}(t) < \alpha_{min} \forall t$, где α_{min} представляет собой минимальный угол разноса, за который принята величина, равная двойной ширине луча.

С учётом данных требований могут быть сформулированы следующие ограничения при формировании лучей:

$$\begin{aligned}
 e_i = 0 \text{ or } e_j = 0 \text{ or } e_i = 0 \text{ or } \beta_{ij} = 0 \text{ or } g_i \neq r_j \text{ or } p_i \neq p_j \\
 \text{or } f_i + b_i \leq f_i \text{ or } f_j + b_j \leq f_i
 \end{aligned} \tag{3}$$

$$\begin{aligned}
 e_i = 0 \text{ or } e_j = 0 \text{ or } e_i = 0 \text{ or } \beta_{ij} = 0 \text{ or } \alpha_{ij} = 0 \text{ or } p_i \neq p_j \\
 \text{or } f_i + b_i \leq f_i \text{ or } f_j + b_j \leq f_i
 \end{aligned} \tag{4}$$

Уравнение 3 гарантирует, что любые два активных луча излучающихся одновременно с одного спутника в любой момент имеют или разные группы повторного частотного использования, или поляризацию, или непересекающиеся частотные каналы.

Уравнение 4 гарантирует, что если два активных луча назначены на один и тот же спутник и географически близки в какой-то момент времени, то они имеют либо разную поляризацию, либо неперекрывающиеся частотные каналы.

Таким образом, можно сделать вывод о том, что предложенные выражения позволят избежать интерференции при работе спутников низкоорбитальной группировки со множеством направленных лучей. Выражения справедливы как для нисходящей, так и для восходящей линии связи. При этом предполагается что спутник имеет возможности и достаточную производительность для оперативной обработки текущих характеристик абонента и канала передачи. Выражения также справедливы для спутниковых систем с прямой ретрансляцией сигнала.

Список используемых источников:

1. Мырова Л. О. и др. Низкоорбитальные спутниковые системы связи StarLink и OneWeb //Труды Научно-исследовательского института радио. – 2021. – №. 2. – С. 36-45.
2. Андронов С. И. и др. Модель влияния основных факторов на временную задержку распространения радиосигналов спутниковых линий связи //Научная мысль. – 2018. – Т. 3. – №. 1. – С. 41-46
3. Kim H. W. et al. SAT-OFDM: a satellite radio interface for the IMT-advanced system //International Journal of Satellite Communications and Networking. – 2015. – Т. 33. – №. 4. – С. 295-314.
4. He Y. et al. Evaluation of system performance for the BMSat //International Journal of Satellite Communications and Networking. – 2015. – Т. 33. – №. 4. – С. 315-328.

Larionov A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Dynamic management of the frequency-orbital resource of low-orbit satellite systems. A fundamentally new level of flexibility and scalability of next-generation satellite communication networks requires the creation of new algorithms for managing frequency resources. It is important to be able to dynamically manage them and be able to quickly adapt them to transmission conditions and the current needs of network users, while avoiding interference during transmission.

Key words: *satellite communications, telecommunications, frequency resource, low-orbit systems.*

УДК 621.391.81
ГРНТИ 49.37.29

РАЗРАБОТКА ТЕХНОЛОГИЧЕСКОЙ СЕТИ ДЛЯ РОССЕТЕЙ

В. А. Марковец

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

Появляются все больше различных идей по внедрению новых технологий в привычные для нас сферы жизни. Особенно это касается сфер, которые хочется автоматизировать для упрощения работы. В данной статье представлен обзор на требования и вариант реализации технологической сети для большого предприятия на технологии NB-IoT.

технологическая сеть, цифровые технологии, автоматизация управления, NB-IoT

Технологическая сеть.

Появляются особенно актуальные услуги для пользователей, связанные с дистанционным управлением или же передачей данных. Можно реализовать технологическую сеть внутри существующей сети компании. Для современных компаний должно быть важно технологическое и инновационное развитие и цифровая трансформация, а так же обеспечение информационной и технологической безопасности их предприятия.

Приоритетными направлениями в области устойчивого развития для компаний являются: создание достойных и безопасных условий труда, а также совершенствование операционной деятельности. Цифровые технологии оптимизируют информационные потоки и позволят повысить эффективность принимаемых решений и заметно улучшат показатели эффективности на: затраты, безопасность, удовлетворённость клиентов.

Технологическая сеть связи представляет собой сеть, предназначенную для обеспечения производственной деятельности организаций и управления технологическими процессами в производстве [1].

Особыми предпосылками для развертывания технологических сетей стали:

1. Разнородные и устаревшие комплексы управления в диспетчерских пунктах
2. Ручная обработка и анализ событий сети
3. Отсутствие возможности удалённого управления оперативным переключениям, в том числе управления
4. основным оборудованием
5. Отсутствие возможности текущего наблюдения изменений эксплуатационного состояния

Технологическую сеть можно применить для упрощения получения данных с приборов учета различных ресурсов, которые предоставляет компания населению, а также для четкой, безопасной и бесперебойной работы всей сети. Затрагивая сферу электроэнергетики, речь идет о большом количестве различных датчиков и счетчиков, с которых необходимо быстро и своевременно собирать

необходимую для качественной работы информацию для соответствующего оказания услуг пользователям. Нужно учитывать счетчики электро и водоснабжения в домах, потребление энергии насосами, данные потребления энергии с ЛЭП и мачт, счетчики в трансформаторных подстанциях, датчики влажности и температуры на трансформаторных подстанциях, датчики движения, датчики дыма и воды, датчики обрыва, а так же связь сотрудников и мониторинг транспорта. Требуется мониторить состояние параметров, необходимых для непрерывной работы всей сети, таких как информация потребления по фазам на кабелях, состояние системы мониторинга и управления, датчики на проникновение в помещения и на трансформаторные подстанции, состояние кабелей на обрыв линий .

Будет происходить передача информации в небольшом количестве, но с большого количества мест. С разных мест мониторинг передачи информации будет происходить с разными интервалами времени, данные с внутридомовых счетчиков достаточно получать 1 раз в месяц как и с центральной подстанции, но требуется постоянная передача информации с датчиков потребления, с датчиков на проникновение. Требуется регулярный мониторинг сети на обрыв линий электропередачи, чтобы при обрыве или аварии можно было оперативно восстановить целостность сети. Ведь важно спроектировать технологическую сеть и поддерживать ее в хорошем состоянии долгое время для безопасного использования.

Также необходимо, чтобы данная сеть работала с наименьшим электро и энергопотреблением, высокой скоростью передачи данных, надо чтобы была возможность управления сетью дистанционно и большим радиусом действия, и недорогой стоимостью развертывания сети и длительным сроком работы конечных устройств. Для дистанционного управления сетью, можно использовать узловые автоматы, для необходимости срочного включения и выключения сети.

Обзор требований.

Так как рассматриваем технологическую сеть относительно существующей компании необходимо познакомиться с уже установленными требованиями касающимися разработки и установки оборудования и самой сети.

Требования к технологиям и комплексным системам, установленные в Положении ПАО «Россети» [2].

1) Для цифровой подстанции необходимо, чтобы выполнялись требования относительно таких параметров, как:

- высокий уровень автоматизации управления оборудованием и системами с применением автоматизированных систем управления;
- дистанционная управляемость всеми технологическими процессами в режиме единого времени и дистанционная наблюдаемость параметров и режимов работы оборудования и систем;
- цифровой обмен данными между всеми технологическими системами в едином формате;

2) Исходя из целей создания цифровой подстанции, важно обеспечение наблюдаемости параметров функционирования ЛЭП, оборудования и устройств подстанции.

3) Для автоматизированных систем технологического управления, важны требования к дистанционному управлению электросетевыми объектами с блокировкой недопустимых команд, и к мониторингу и ведению электронного журнала состояния сети, оборудования и ЛЭП.

4) Для оперативного контроля и управления объектами электросетевого комплекса в автоматизированных системах технологического управления должно быть предусмотрено:

- дистанционное управление коммутационным аппаратом;
- телесигнализация положения коммутационным аппаратом;
- телеизмерения режимных параметров (ток, напряжение, мощность, частота);

5) Функции автоматизированных систем, должны производить: измерение, преобразование, сбор аналоговой и дискретной информации о текущих технологических режимах и состоянии.

6) Для оперативного контроля и управления объектами электросетевого комплекса в автоматизированных системах технологического управления должно быть предусмотрено дистанционное управление коммутационным аппаратом, где очень важную роль играют задержки по времени. Для разных процедур они разные, но колеблются от 0.5мс - до 2с.

NB-IoT.

По совокупности требований к технологической сети, будет рассмотрена сеть на технологии NB-IoT на стандарте связи LTE. NB-IoT то есть узкополосный Интернет вещей, разработанный для обеспечения широкого спектра новых устройств и услуг интернета вещей, имеет: длительный срок работы конечных устройств; экономичность и простоту внедрения решений; отличную масштабируемость за счет практически неограниченного количества подключаемых датчиков. NB-IoT значительно повышает пропускную способность системы и эффективность использования спектра, особенно при глубоком покрытии. Срок службы батареи более 10 лет может поддерживаться для широкого спектра случаев использования. Этот стандарт передачи данных, разработан для работы устройств в сетях операторов мобильной связи.

Поддерживаемый всеми основными производителями мобильного оборудования, чипсетов и модулей, NB-IoT может сосуществовать с мобильными сетями 2G, 3G и 4G. Также извлекает выгоду из всех функций безопасности и конфиденциальности мобильных сетей, таких как поддержка конфиденциальности идентификации пользователя, аутентификации объектов, конфиденциальности, целостности данных и идентификации мобильного оборудования. NB-IoT обеспечивает максимальную скорость загрузки 250 кбит/с и скорость восходящей линии связи 250 кбит/с при многотональной передаче или 20 кбит/с при однотоновой. Технология NB-IoT использует сигналы с

низкой пропускной способностью для связи в рамках существующих технологий LTE [3].

Специально разработанные устройства и датчики являются основными компонентами в системах NB-IoT. Эти устройства собирают информацию из своего окружения и передают ее на базовые станции NB-IoT или узлы передачи. Отдельные базовые станции подключены к шлюзу Интернета вещей и серверам облачных приложений Интернета вещей для централизованного мониторинга и анализа данных. Данный стандарт передачи данных основывается на использовании существующей инфраструктуры мобильных сетей общего пользования. Для исключения перегрузки сети связи при передаче данных «Интернета вещей» полоса частот ограничена по сравнению с обычным доступом в глобальную сеть, что позволяет одной базовой станции обслуживать десятки тысяч счетчиков без ущерба для основных функций. Дополнительное снижение стоимости достигается за счет того, что NB-IoT не требуется физически существующая SIM-карта. Услуги NB-IoT в России предоставляют все операторы «большой четверки».

Учитывая то, что NB-IoT работает в лицензионных частотах, необходим дорогой и труднодоступный радиоресурс, Ростелеком готов предоставить частоты 450 МГц для реализации на них технологической сети для компании «Россети». NB-IoT идеально подходит для развертывания технологической сети учитывая все требования и запросы

Сравнивая LPWA технологии, NB-IoT является маломощной технологией глобальной сети, созданной для устройств с низким энергопотреблением, имеет меньшие задержки по сравнению другими технологиями из-за более высокой выходной мощности устройства, что может обеспечить более высокие скорости передачи данных. Также NB-IoT имеет высокую дальность связи до 3км, и невысокое энергопотребление, но это не критично, по сравнению ко всем плюсам данной технологии.



Рис. 1. Сравнение технологий по энергопотреблению и дальности передачи [4]

Список используемых источников:

1. Технологическая сеть связи, [Электронный ресурс]
URL:<https://controleng.ru/teoriya/tehnologicheskaja-set-svjazi/>
2. Положение ПАО «Россети» «О единой технической политике в электросетевом комплексе»
3. Linda Rosencrance / NB-IoT Электронный ресурс: techtarget
URL:<https://www.techtarget.com/whatis/definition/narrowband-IoT-NB-IoT>
4. Стандарт NB-IoT Low-Power and Wide-Area, LPWA:Tadviser[Электронный ресурс].
URL:https://www.tadviser.ru/index.php/Статья:Стандарт_NB-IoT_Low-Power_and_Wide-Area,_LPWAN

Markovets V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunications

Development of a technological network for Rossets.

There are more and more different ideas for introducing new technologies into the spheres of life familiar to us. This is especially true for areas that you want to automate to simplify your work. This article provides an overview of the requirements and the implementation option of a technological network for a large enterprise based on NB-IoT technology.

Key words: technological network, digital technologies, control automation, NB-IoT.

УДК 654.165
ГРНТИ 49.33.29

АНАЛИЗ МОДЕЛИ ИНТЕРФЕЙСА X2 В СИМУЛЯТОРЕ NS-3

Е. А. Мартынова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На сегодняшний день вопрос о разработке отечественного оборудования и построении на его основе сетей LTE является очень актуальным. Моделирование является наиболее надежным подходом для разработки сетей мобильной связи. В данной работе представлено описание модели интерфейса X2 стандарта сети LTE. Он является неотъемлемой частью для выполнения процедуры хэндовера, а также реализации функций сетей SON.

интерфейс, LTE, SON, моделирование

Одной из важнейших особенностей сетей LTE по сравнению с предыдущими поколениями является наличие сигнального интерфейса X2, который обеспечивает соединение «точка-точка» между двумя базовыми станциями eNodeB (рис. 1) [1]. Данный интерфейс используется для организации внутрисистемных хэндоверов, балансировки трафика, а также для реализации функций SON, COMP и ряда других. В связи с этим моделирование интерфейса X2 является одной из главных задач при построении имитационной модели сети LTE. Это соединение должно быть осуществлено даже при отсутствии физического прямого соединения между двумя базовыми станциями.

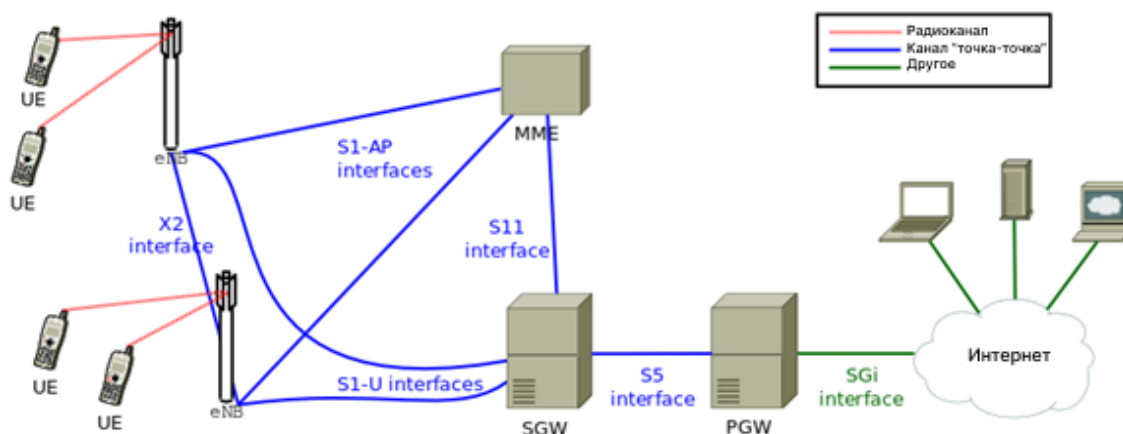


Рис. 1. Имитационная модель пакетного ядра сети LTE

Интерфейс X2, реализованный в симуляторе, обеспечивает выполнение следующих команд [1]:

- сообщение Handover Request
- сообщение Handover Request Acknowledgement
- сообщение SN Status Transfer
- сообщение UE Context Release (завершение процедуры хэндовера)

Эти команды участвуют в процессе реализации хэндовера на основе интерфейса X2. Стоит отметить, что модель симулятора в настоящее время поддерживает только мягкий хэндовер.

Приведенная ниже диаграмма [1] показывает последовательность процедуры хэндовера в симуляторе на основе интерфейса X2. Серые прямоугольники указывают на момент, когда UE или eNodeB переходят в другое состояние RRC.

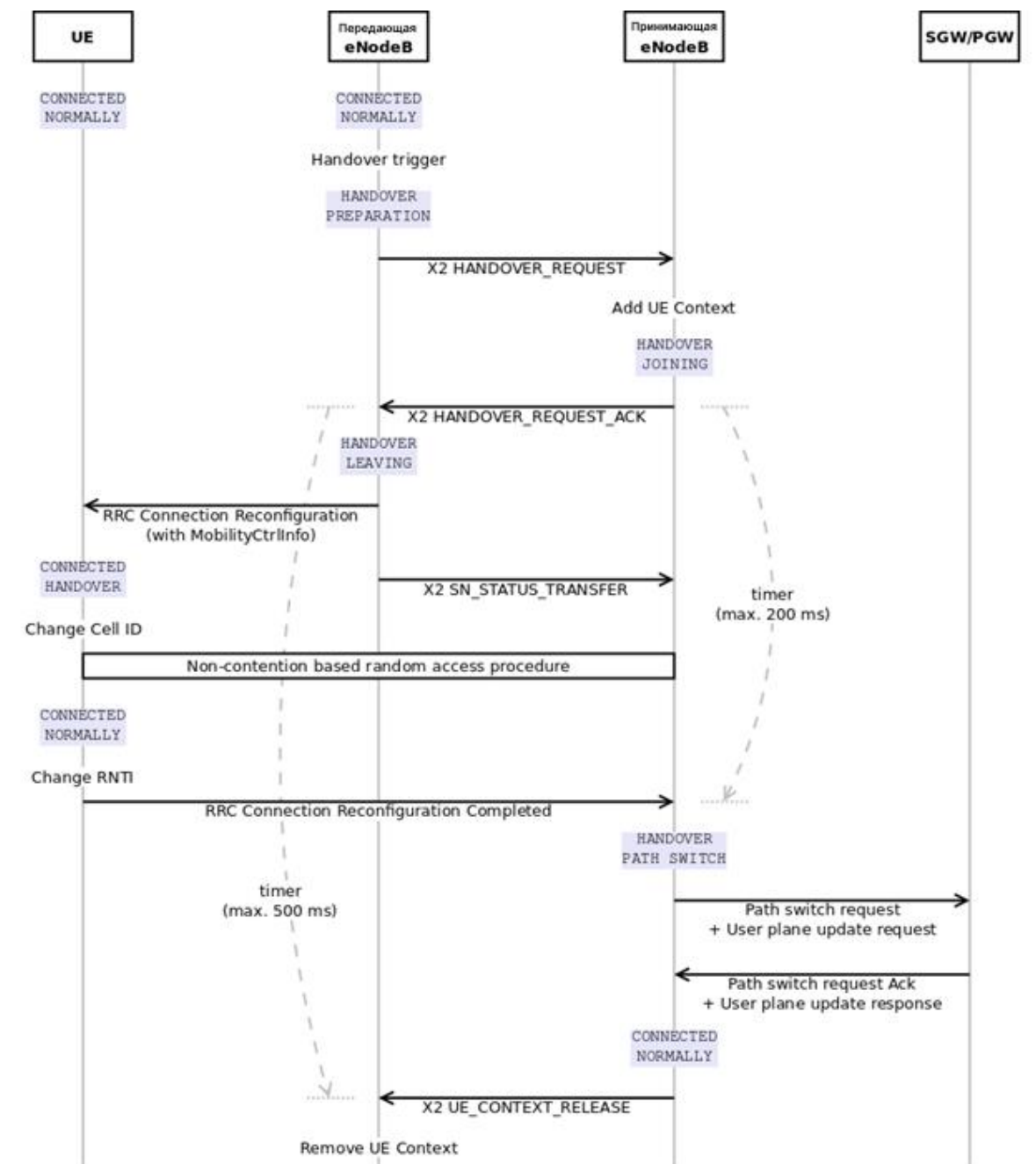


Рис. 2. Последовательность процедуры хэндовера

На диаграмме также показаны два таймера, которые участвуют в процедуре хэндовера:

- Handover leaving – таймер отключения от процедуры хэндовера (поддерживается передающим eNodeB)

- Handover joining – таймер подключения к процедуре хэндовера (поддерживается получающим eNodeB)

В симуляторе NS-3, длительность таймеров может быть настроена с помощью атрибутов HandoverLeavingTimeoutDuration и HandoverJoiningTimeoutDuration. По истечении таймеров процедура хэндовера считается неудавшейся. В симуляторе на данный момент не предусмотрена корректная обработка сорвавшихся передач, поэтому рекомендуется настраивать модель таким образом, чтобы избежать непредвиденных ошибок в работе.

Интерфейсы X2

Модель содержит два интерфейса:

Интерфейс X2-C. Он является управляющей частью интерфейса X2 и используется для передачи X2AP, (X2 application protocol) т.е. элементарных процедур, таких как подготовка к передаче, передача статуса, управление мобильностью.

Интерфейс X2-U. Определяется между eNB, которые обеспечивают туннелирование GTP-U для каждой пользовательской плоскости. Он используется для пересылки данных во время передачи обслуживания по инициативе X2. При отправке через этот интерфейс пакеты данных инкапсулируются через GTP /UDP /IP [2].

На рис. 3 показаны стеки протоколов интерфейса X2-U и интерфейса X2-C, реализованные в симуляторе [1].

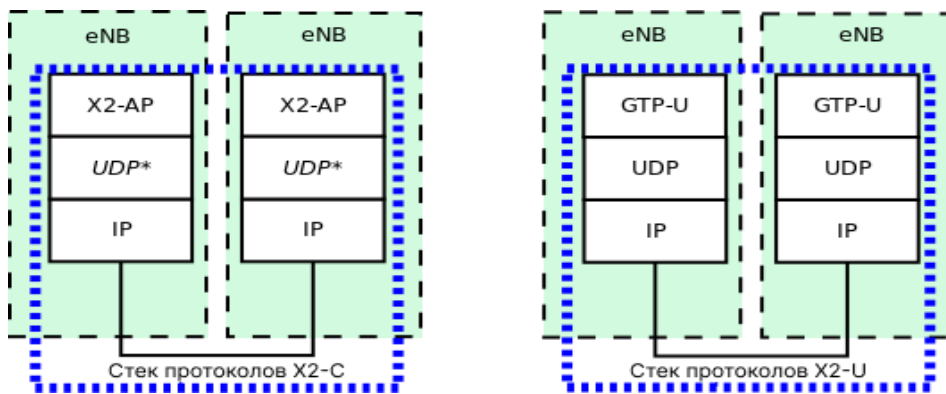


Рис. 3. Стеки протоколов интерфейса X2

В исходном стеке протоколов в качестве транспортного протокола используется протокол SCTP, но в настоящее время в симуляторе NS-3 нет возможности его смоделировать, поэтому в данном случае в качестве протокола, ориентированного на дейтаграммы, используется протокол UDP

В модели интерфейса X2 также могут быть использованы примитивы для реализации самоорганизующейся сети (SON- Self-Organized Network), изучение алгоритмов которой планируется в дальнейшем:

-Load information

-Resource status update

Стоит отметить, что они не настроены по умолчанию в модели. Их используют для того, чтобы была возможность разработать дополнительные алгоритмы.

В качестве примера рассмотрим, как можно использовать примитив Resource status update. Предположим, что LteEnbRrc (LTE Radio Resource Control entity at the eNB) настроен и готов для включения новой переменной:

```
EpcX2Sap::CellMeasurementResultItem m_cmri;
```

Ссылаемся на файл epc-x2-sap.h и на ссылки документации doxygen, для получения подробной информации об этом типе переменной и настройки ее значения. Далее добавляем следующий код для отправки примитива Resource status update:

```
EpcX2Sap::ResourceStatusUpdateParams params;  
params.targetCellId = cellId;  
params.cellMeasurementResultList.push_back (m_cmri);  
m_x2SapProvider->SendResourceStatusUpdate (params);
```

Метод eEnbRrc::DoRecvResourceStatusUpdate будет вызван, когда принимающая станция eNB получит сообщение об обновлении статуса.

В данной статье рассмотрены принципы функционирования интерфейса X2 в сетях мобильной связи стандарта LTE и особенности его реализации при моделировании сетей LTE в симуляторе NS-3. Полученные результаты могут быть использованы при разработке и модернизации алгоритмов хэндовера, а также моделировании функционалов SON.

Список используемых источников:

1. NS-3 design documentation <https://www.nsnam.org/docs/models/html/lte-design.html#fig-epc-topology> (дата обращения 25.10.2022).
2. RF Wireless World [Электронный ресурс] // URL: <https://www.rfwireless-world.com/Tutorials/LTE-system-interfaces.html> (дата обращения 25.10.2022).

Martynova E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of the X2 interface model in the NS-3 simulator.

Nowadays the issue of developing domestic equipment and building LTE networks based on is really relevant. Modeling is the most reliable approach for the development of mobile communication networks. This article presents a description of the X2 interface model of the LTE network standard. It is an integral part for performing the handover procedure and for implementing the functions of SON networks.

Key words: *interface, LTE, SON, modeling.*

УДК 621.396.9
ГРНТИ 49.33.29

РЕАЛИЗАЦИЯ ВЫСОКОСКОРОСТНОГО МОБИЛЬНОГО ИНТЕРНЕТА ВЕЩЕЙ В СЕТЯХ NEW RADIO

В. Е. Науменко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича

Представлена ключевая особенность стандарта NR – услуги URLLC. Описаны способы уменьшения задержек при передаче сообщения в услугах URLLC в ядре сети NR и в логических уровнях L1 и L2 радиointерфейса. Приведены результаты расчетов пропускной способности сетей NR при реализации услуг URLLC в зависимости от выделяемого канального ресурса при использовании различных модуляционно-кодирующих схем.

сеть NR, URLLC, пропускная способность

Предпосылкой к появлению стандарта NR (New Radio, 5G) является увеличение требований к общей пропускной способности сети мобильной связи и быстрое развитие сетей мобильного интернета вещей.

Одним из важных преимуществ пятого поколения над четвертым заключаются в том, что NR имеет более высокую скорость передачи данных, высокую плотность сети, низкие задержки, что вкуче повышает производительность сети и увеличивает количество устройств, которые могут быть одновременно подключены к ней.

URLLC (Ultra-Reliable-Low-Latency-Communication) – сверхнадежная связь с гарантированной скоростью, критичной к задержкам, которая является ключевой особенностью стандарта NR.

Услуги URLLC предназначены для поддержки вариантов использования со строгими требованиями к чрезвычайно низкой задержке (например, 1 мс) и высокой надежности (например, 99,999%) передачи данных. Данные технологии активно применяют в системах общественной безопасности, удаленной диагностики/хирургии, при реагировании на чрезвычайные ситуации, внедряются в системы автономного вождения. К этому можно добавить такие разные приложения, как управление в энергетическом секторе, в том числе умными сетями энергетики и организация развлечений (игр) в реальном времени [1].

Для обеспечения требуемой надежности необходимо увеличивать число повторов сообщений от десятка до сотни раз.

Более сложным является процесс уменьшения задержек при передаче сообщений. Для обеспечения малой задержки на сквозном соединении должна быть снижена задержка в ядре сети 5G и уменьшены задержки в логических уровнях L1 и L2 радиointерфейса.

Для снижения задержки в ядре сети используют краевые вычислительные облачные структуры (КВС). Последние 3 года этой проблеме уделяется большое внимание.

Для уменьшения задержек на логическом уровне L2 необходимо использовать расщепление сети радиодоступа на данном уровне. На рис. 1 показаны подуровни логического уровня L2: PDCP, RLC, MAC, а также процессорная обработка передаваемых сообщений на физическом уровне.

Частично или полностью обработку на подуровнях логического уровня L2 производят в централизованном устройстве CU (Central Unit), который обслуживает группы базовых станций. На рис. 1 представлены результаты машинного моделирования задержек в зависимости от того, какая часть обработки на подуровнях L2 выполняется централизованно, а какая часть – непосредственно в приемо-передатчике [2]. Как следует из данного рисунка, при увеличении объема вычислительных функций в CU задержка снижается от единиц миллисекунд до сотых долей миллисекунд.

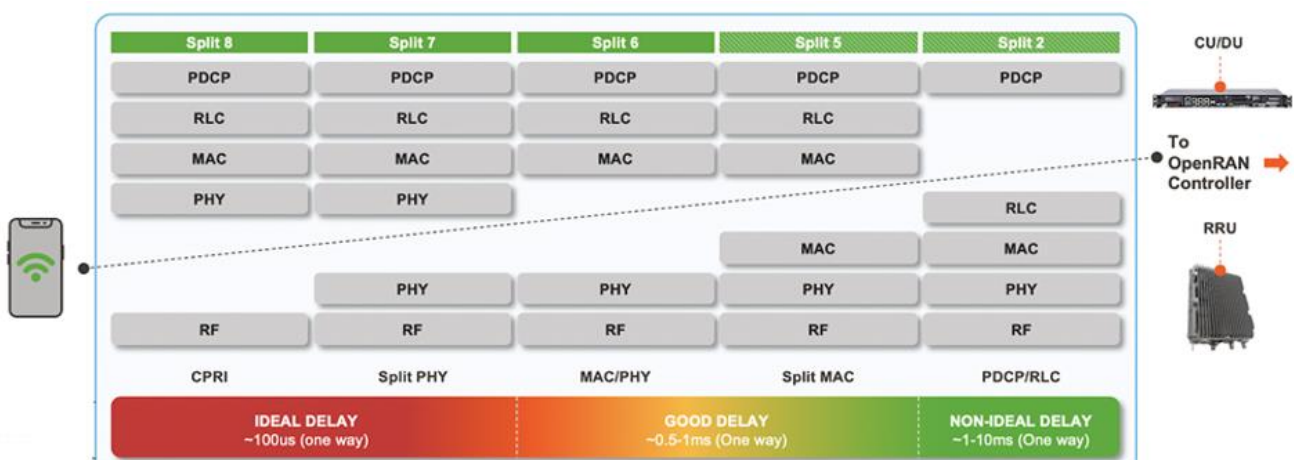


Рис. 1. Расщепление сети радиодоступа на логическом уровне L2

Что касается уменьшения задержек на логическом уровне L1 радионтерфейса, то как было сказано ранее, вычисления, связанные с кодированием и перемежением информации, могут быть выполнены как в приемо-передатчике, так и в централизованном устройстве. Реальное время передачи сообщения по радиointерфейсу определяет скорость передачи в радиоканале. Поскольку скорость передачи в радиоканале зависит от выделенной полосы радиочастот, то реализация услуг URLLC требует использования широкополосных каналов. Предполагается, что это будут каналы шириной 10 МГц, 20 МГц и более [2].

Для оценки пропускной способности сети стандарта NR следует задаваться модуляционно-кодирующими схемами. Как и в стандарте LTE, в спецификациях стандарта NR приведены характеристики транспортных блоков при различных вариантах модуляции и кодирования. Для того, чтобы представить результаты расчетов в более компактном виде, воспользуемся вместо таблиц транспортных блоков таблицами CQI, которые определяют реперные уровни модуляционно-кодирующих схем.

Произведём расчет числа передаваемых пакетов в сетях New Radio для услуг URLLC при передаче вверх для $SCS = 15$ кГц с полосой 10 МГц, 20 МГц

и 50 МГц, а также для $SCS = 30$ кГц с полосой 20 МГц, 50 МГц и 100 МГц. При этом рассматриваем три варианта передаваемых сообщений, размером в 1 байт, 2 байта и 4 байта.

Сообщению предшествуют заголовки по IP и TCP протоколам. Заголовки составляют 3 байта. При передаче по радиointерфейсу сообщение обрабатывается на трех подуровнях: PDCP, RLC, MAC. На каждом подуровне добавляют 1 байт, таким образом, минимальный размер передаваемого сообщения составляет 7 байт. При передаче сообщений размером в 2 и 4 байта размер на радиointерфейсе будет составлять 8 и 10 байт соответственно. Структура передаваемого сообщения проиллюстрирована рис. 2 [2].

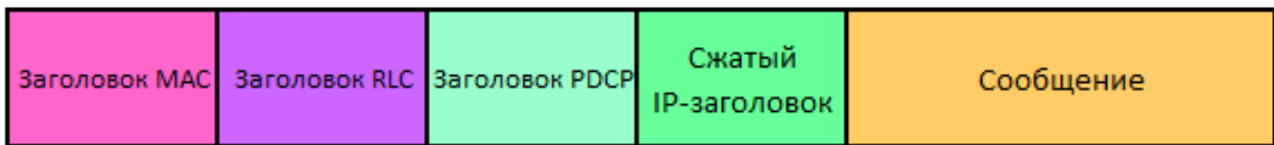


Рис. 2. Структура передаваемого сообщения

Для выполнения расчетов возможного числа передаваемых сообщений зададимся следующими данными. Будем производить расчеты для одного варианта выделения канального ресурса в канале PUSCH тип В [3]. В выбранном варианте выделяется один РБ при расстоянии между поднесущими $SCS = 15$ кГц, что по длительности передачи соответствует выделению двух РБ при $SCS = 30$ кГц (рис. 3).

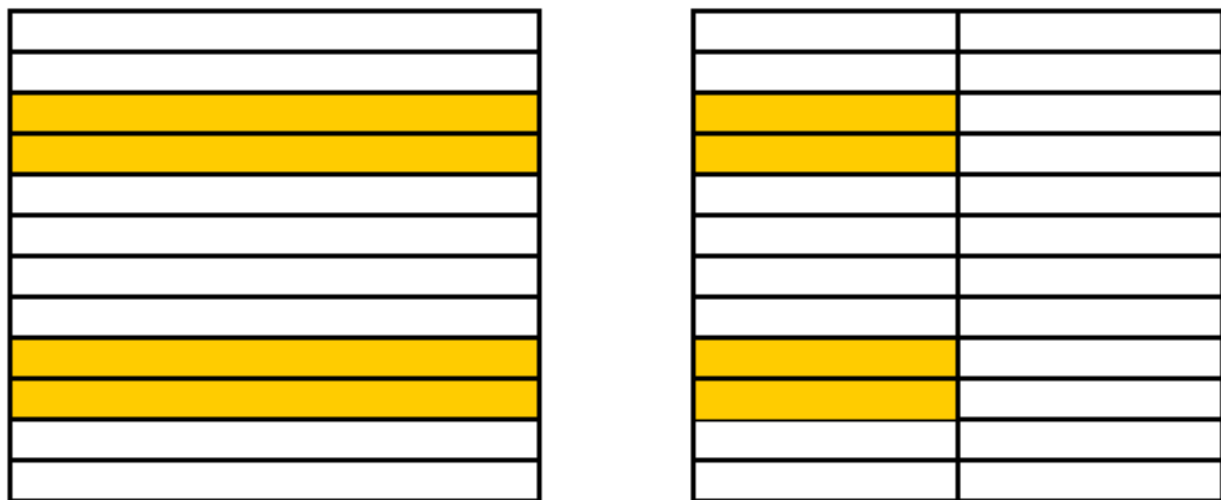


Рис. 3. Выделение канального ресурса для передачи сообщений URLLC

В таблицах 1 и 2 приведены расчеты числа передаваемых пакетов в URLLC. Варианты модуляционно-кодирующих схем выбираем по таблице 1 приведенной в [4]. При этом расчеты начинаем с $CQI = 5$, поскольку варианты с 1 по 4 имеют очень низкую эффективность.

ТАБЛИЦА 1. CQI

CQI индекс	Модуляция	Скорость кодирования \times 1024	Эффективность
5	4-ФМ	0,19	0.3770
6	4-ФМ	0,30	0.6016
7	4-ФМ	0,44	0.8770
8	4-ФМ	0,59	1.1758
9	16-КАМ	0,37	1.4766
10	16-КАМ	0,48	1.9141
11	16-КАМ	0,6	2.4063
12	64-КАМ	0,46	2.7305
13	64-КАМ	0,55	3.3223
14	64-КАМ	0,65	3.9023
15	64-КАМ	0,75	4.5234

 ТАБЛИЦА 2. Результаты расчетов с выделением одного ресурсного блока
 $SCS = 15$ кГц

			$SCS = 15$ кГц Полоса 10 МГц			$SCS = 15$ кГц Полоса 20 МГц			$SCS = 15$ кГц Полоса 50 МГц		
			$N_{RB} = 52$			$N_{RB} = 106$			$N_{RB} = 270$		
			Число переданных пакетов								
CQI I	Модуляция	Rкод	1 байт	2 байта	4 байта	1 байт	2 байта	4 байта	1 байт	2 байта	4 байта
5	4-ФМ	0,19	2	2	1	5	5	4	14	12	10
6	4-ФМ	0,30	4	3	3	9	7	6	23	20	16
7	4-ФМ	0,44	6	5	4	13	11	9	33	29	23
8	4-ФМ	0,59	8	7	6	17	15	12	45	39	31
9	16-КАМ	0,37	10	9	7	22	19	15	57	49	40
10	16-КАМ	0,48	14	12	9	28	25	20	73	64	51
11	16-КАМ	0,6	17	15	12	36	31	25	92	81	64
12	64-КАМ	0,46	20	17	14	41	36	28	105	92	73
13	64-КАМ	0,55	24	21	17	50	44	35	128	112	89
14	64-КАМ	0,65	29	25	20	59	51	41	151	132	105
15	64-КАМ	0,75	33	29	23	68	59	47	174	153	122

ТАБЛИЦА 3. Результаты расчетов с выделением двух ресурсных блоков
 $SCS = 30$ кГц

			$SCS = 30$ кГц Полоса 20 МГц			$SCS = 30$ кГц Полоса 50 МГц			$SCS = 30$ кГц Полоса 100 МГц		
			$N_{RB} = 51$			$N_{RB} = 133$			$N_{RB} = 273$		
			Число переданных пакетов								
CQ I	Модуляция	Rкод	1 байт	2 байта	4 байта	1 байт	2 байта	4 байта	1 байт	2 байта	4 байта
5	4-ФМ	0,19	6	6	4	17	15	12	36	32	25
6	4-ФМ	0,30	10	9	7	28	25	20	58	51	41
7	4-ФМ	0,44	16	14	11	41	36	29	85	74	59
8	4-ФМ	0,59	21	18	15	55	48	39	115	100	80
9	16-КАМ	0,37	26	23	18	70	61	49	144	126	101
10	16-КАМ	0,48	34	30	23	90	79	63	187	163	131
11	16-КАМ	0,6	43	38	30	114	100	80	244	205	164
12	64-КАМ	0,46	49	43	34	130	113	90	266	233	186
13	64-КАМ	0,55	60	52	42	156	137	109	321	281	225
14	64-КАМ	0,65	71	62	49	185	162	129	380	332	266
15	64-КАМ	0,75	81	71	57	213	187	149	438	383	307

Из приведенных расчетов видно, что при переходе от варианта $SCS = 15$ кГц к варианту $SCS = 30$ кГц получаем прирост пропускной способности сети примерно в 20%.

Список используемых источников:

1. Wan Lei, Anthony C. K. Soong, Liu Jianghua, Wu Yong, Brian Classon, Weimin Xiao, David Mazzaresse, Zhao Yang, Tony Saboorian. 5G System Design An End to End Perspective, 2020. 408p.
2. Sassan Ahmadi. 5G NR Architecture, Technology, Implementation, and Operation of 3GPP New Radio Standards, 2019. 1020 p
3. 3GPP TS 38.214 V17.1.0. NR; Physical channels and modulation. 2022. 130p.
4. 3GPP TS 38.214 V17.1.0. NR; Physical layer procedures for data. 2022. 226p.

Naumenko V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Implementation of high-speed Internet of Things in New Radio networks.

The key feature of the standard NR – URLLC services is presented. The methods of reducing delays in the transmission of a message in URLLC services in the core of the NR network and in the logical levels L1 and L2 of the radio interface are described. The results of calculations of the bandwidth of NR networks in the implementation of URLLC services depending on the allocated channel resource using various modulation-coding schemes are presented.

Key words: NR network, URLLC, bandwidth.

УДК 621.396.677
ГРНТИ 47.45.29

ИСПОЛЬЗОВАНИЕ МЕТОДА НАИМЕНЬШИХ КВАДРАТОВ (LMS) В ЗАДАЧАХ ЦИФРОВОГО ДИАГРАММООБРАЗОВАНИЯ В СЕТЯХ 5G

И. А. Никитин, У. И. Прилуцкая

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе исследуются возможности алгоритма наименьших квадратов (Least Mean Square) в задачах адаптивного диаграммообразования, актуальных для сетей 5G за счёт перехода в диапазон миллиметровых волн и развития многоантенных систем. Рассмотрен принцип работы и математическая модель алгоритма. Построена имитационная модель MATLAB на основе линейной антенной решётки и продемонстрированы результаты её работы в виде рассчитанных весовых коэффициентов антенной решётки, а также сформированных диаграмм направленности.

5G, диаграммообразование, адаптивные антенные решётки, смарт-антенны, MIMO, LMS

Отличительной чертой развёртываемых сетей пятого поколения 5G является сверхплотное территориальное распределение образующих их устройств радиодоступа – базовых станций и пользовательских устройств с плотностью до 1 млн устройств на 1 км², в следствие этого сильно увеличивается уровень внутрисистемных помех [1]. Для их компенсации в сетях 5G предусмотрен множественный доступ с пространственным разделением благодаря применению методов адаптивного диаграммообразования (ДО), реализованных на антенных решётках (АР).

Приём сигнала с помощью многоэлементных адаптивных АР является одним из основных методов решения сложных задач обнаружения и оценивания, поскольку данный тип антенн, в отличие от фазированных АР, позволяет осуществлять формирование не только максимума диаграммы направленности (ДН), но и провалов в произвольных направлениях, вследствие чего происходит максимальное подавление помех при минимальных искажениях полезного сигнала. Способность к адаптации делает работу систем с антенными решётками более гибкой и позволяет повысить эффективность приёма и передачи [2].

Увеличение числа элементов АР в задачах цифрового ДО в сетях 5G обусловило необходимость поиска компромисса между известными подходами аналогового и цифрового ДО, которое материализовалось в методах гибридного ДО. Основные архитектуры ДО представлены на рис. 1.

Используя технические возможности методов цифрового и гибридного ДО, рассмотрим далее модели пространственной фильтрации полезного SOI (Signal of Interest) и мешающего SNOI (Signal Not of Interest) сигналов в сценариях функционирования сверхплотных сетей 5G [3].

В данной работе будет проанализирована линейная АР с целью продемонстрировать основные принципы использования АР в сценариях сверхплотного распределения устройств в сетях 5G.

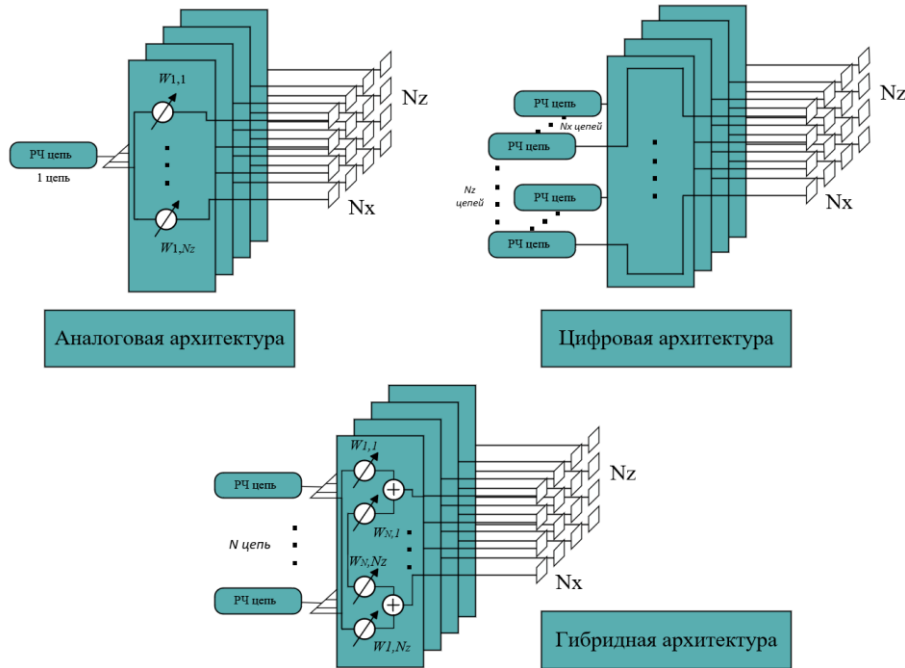


Рис. 1. Варианты архитектуры ДО

Антенный фактор линейной решётки с одинаковым разнесением элементов, расположенных симметрично вдоль оси y , определяется выражением [4]

$$(AF)_M = \sum_{n=1}^{M/2} w_n \cos \cos [(2n - 1)\psi_n], \quad (1)$$

где

$$\psi_n = \frac{\pi d}{\lambda} \sin\theta \sin\phi + \beta_n.$$

где w_n и β_n представляют собой амплитудные и фазовые коэффициенты отдельных элементов АР. Коэффициенты амплитуды w_n , в первую очередь, определяют форму диаграммы направленности и уровень лепестков, в то время как фазовые коэффициенты определяют сканирующие возможности решётки.

Существуют алгоритмы ДО, которым не требуется информация о направлении прихода сигналов. Одним из таких является алгоритм наименьших квадратов LMS (Least Mean Square), который использует обучающую последовательность для регулировки амплитуд и фаз, чтобы соответствовать временным задержкам, создаваемым приходящим на решётку сигналам, и не требует памяти [4]. По сути, это требует решения линейной

системы уравнений. Основная причина, по которой обычно нежелательно решать уравнения напрямую, заключается в том, что сигнальная среда постоянно меняется.

Рассмотрим аналитический пример, в котором необходимо определить комплексные веса двухэлементной линейной АР для приёма полезного сигнала SOI с направления $\theta_0 = 0^\circ$ и подавить помеху SNOI с направления $\theta_1 = 30^\circ$. Допустим, элементы АР, представленные на рис. 2, изотропные, а принимаемые сигналы представляют собой синусоиды. Сначала анализируется выходной сигнал АР $y(t)$, сформированный полезным сигналом $p(t)$ и помеховый сигнал $n(t)$. Таким образом, выходной сигнал $y(t)$ можно представить как:

$$y(t) = P e^{j\omega_0 t} (\dot{w}_1 + \dot{w}_2)$$

Чтобы выходной сигнал $y(t)$ был эквивалентен только полезному сигналу $p(t)$, необходимо, чтобы выполнялось условие

$$\dot{w}_1 + \dot{w}_2 = 1$$

С другой стороны, выходной сигнал $y(t)$, сформированный помехой $n(t)$, задаётся как

$$y(t) = N e^{j(\omega_0 t - \frac{\pi}{4})} \dot{w}_1 + N e^{j(\omega_0 t + \frac{\pi}{4})} \dot{w}_2$$

где $-\frac{\pi}{4}$ и $+\frac{\pi}{4}$ обусловлены, соответственно, задержкой и опережением по фазе относительно средней точки решётки, что отображено на рис. 2.

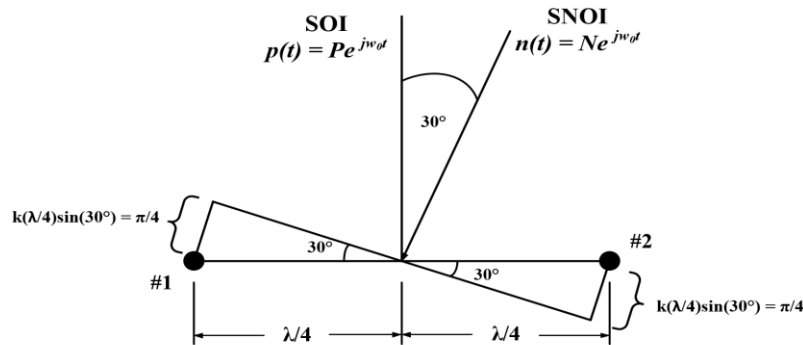


Рис. 2. Двухэлементная АР. Вычисление фазовой задержки и опережения $n(t)$

Так как

$$e^{j(\omega_0 t - \frac{\pi}{4})} = \frac{e^{j\omega_0 t}}{\sqrt{2}} (1 - j)$$

$$e^{j(\omega_0 t + \frac{\pi}{4})} = \frac{e^{j\omega_0 t}}{\sqrt{2}} (1 + j)$$

выходной сигнал $y(t)$ может быть представлен как

$$y(t) = Ne^{j\omega_0 t} \left[\frac{\sqrt{2}}{2} (1-j)\dot{w}_1 + \frac{\sqrt{2}}{2} (1+j)\dot{w}_2 \right]$$

Из тождеств

$$e^{j(\omega_0 t - \frac{\pi}{4})} = \frac{e^{j\omega_0 t}}{\sqrt{2}} (1-j)$$

$$e^{j(\omega_0 t + \frac{\pi}{4})} = \frac{e^{j\omega_0 t}}{\sqrt{2}} (1+j)$$

следует, что выходной сигнал $y(t)$ может быть представлен как

$$y(t) = Ne^{j\omega_0 t} \left[\frac{\sqrt{2}}{2} (1-j)\dot{w}_1 + \frac{\sqrt{2}}{2} (1+j)\dot{w}_2 \right]$$

Следовательно, для того, чтобы выходной $y(t)$ был равен нулю (т.е. полностью исключалась помеха), необходимо выполнение условия

$$\frac{\sqrt{2}}{2} (1-j)\dot{w}_1 + \frac{\sqrt{2}}{2} (1+j)\dot{w}_2 = 0$$

Антенный фактор в зависимости от угла прихода, полученный средствами имитационного моделирования, представлен на рис. 3.

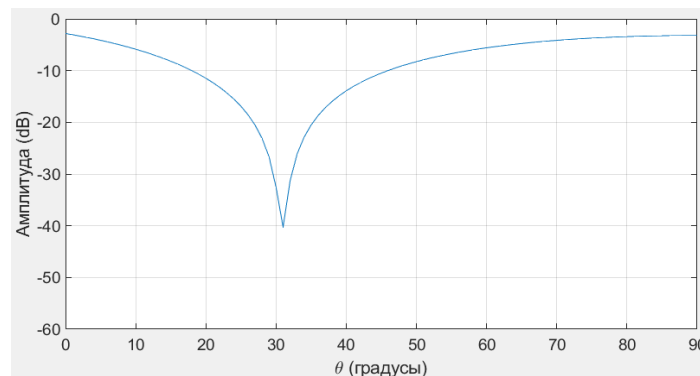


Рис. 3. Антенный фактор (SOI $\theta_0 = 0^\circ$ и SNOI $\theta_1 = 30^\circ$)

Если сигнальная среда стационарна, веса AP вычисляются путём решения уравнений (1). Однако на практике среда в сценариях сверхплотных сетей является динамической и изменяющейся во времени, и поэтому веса необходимо вычислять с помощью адаптивных методов [4].

Далее решим пример с применением LMS. Алгоритм вычисляет весовые коэффициенты итеративно

$$w_{k+1} = w_k + 2\mu x_k (d_k - x_k^T w_k)$$

Чтобы обеспечить сходимость весов w_k , размер шага μ ограничен условием

$$0 < \mu < \frac{1}{\lambda_{max}},$$

где λ_{max} - максимальное собственное значение ковариационной матрицы R_{xx} . Основным недостатком алгоритма является то, что он имеет тенденцию медленно сходиться, особенно в зашумлённой среде.

С помощью имитационной модели (ИМ) линейной АР построим ДН. Рассчитанная за 500 итераций ДН двухэлементной АР приведена на рис. 4. Сформированная ДН отвечает желаемому требованию иметь провал в направлении SNOI $\theta_1 = 30^\circ$, однако излучение в направлении SOI недостаточно сконцентрировано. Для лучшей концентрации мощности в направлении SOI увеличим количество элементов до 8 и снова рассчитаем весовые коэффициенты.

Сформированная ДН представлена на рис. 5. Видно, что в сформированная ДН удовлетворяет требованию иметь максимум при $\theta_0 = 0^\circ$ и провал в направлении помехи $\theta_1 = 30^\circ$.

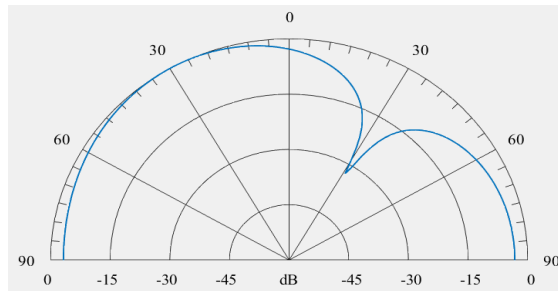


Рис. 4. Сформированная ДН двухэлементной АР (SOI $\theta_0 = 0^\circ$ и SNOI $\theta_1 = 30^\circ$)

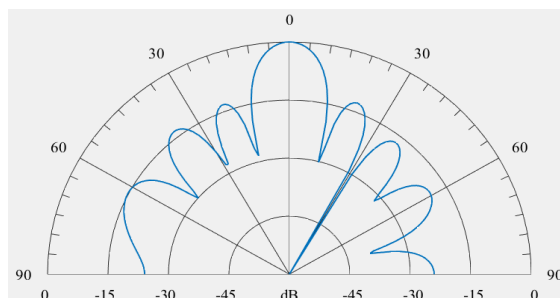


Рис. 5. Сформированная ДН восьмиэлементной АР (SOI $\theta_0 = 0^\circ$ и SNOI $\theta_1 = 30^\circ$)

В работе описаны принцип формирования весовых коэффициентов АР и принцип работы алгоритма наименьших квадратов (LMS). Результаты имитационного моделирования показали существенное усиление полезного сигнала SOI и подавление помехи SNOI, а также увеличение разрешающей способности алгоритма с ростом числа элементов АР. В результате моделирования продемонстрировано, что при адаптивном диаграммообразовании с применением алгоритма LMS уровень подавления помехи относительно полезного сигнала может достигать десятки дБ. Направлением дальнейших исследований является моделирование набора сценариев работы SOI и SNOI устройств в составе сверхплотных сетей 5G.

Список используемых источников:

1. Рекомендация МСЭ-R М.2083. Видение ИМТ - Структура и общие цели будущего развития ИМТ на период до 2020 года и далее. 2015. С. 22.
2. Фокин Г. А. Оценка помех в сверхплотных сетях радиодоступа 5G с диаграммообразованием // Информационные технологии и телекоммуникации. 2020. Том 8. № 4. С. 35–59. DOI 10.31854/2307-1303-2020-8-4-35-59
3. Фокин Г.А. Комплекс моделей и методов позиционирования устройств в сетях пятого поколения: дис. ...д-ра техн. наук : 30.06.21 / Фокин Григорий Алексеевич. СПб., 2021. 499 с.
4. Balanis C. Antenna Theory: Analysis and Design. 4th Ed. Wiley, 2016. 1104 P

Nikitin I., Prilutskaya U.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Application of Least Mean Square algorithm for 5G network Beamforming purpose.

This article investigates possibilities of Least Mean Square algorithm in beamforming issues relevant to 5G networks due to transition to mmWave range and development of multiple antenna systems. The basis and mathematical model of the algorithm are considered. A MATLAB simulation model based on a linear antenna array is created and the results of its computation are presented in the form of calculated weights of antenna array, as well as generated radiation patterns.

Key words: 5G, Beamforming, Adaptive Antenna Array, Smart-Antenna, MIMO, LMS.

УДК 654.93
ГРНТИ 47.49.33

КОНФИГУРАЦИЯ И АЛГОРИТМ РАБОТЫ НАЗЕМНЫХ СТАНЦИЙ СИСТЕМЫ МНОГОПОЗИЦИОННОГО НАБЛЮДЕНИЯ

П. Ф. Рекель

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время все больше увеличивается количество авиатранспорта, а, следовательно, и количество авиaperелетов. В этих условиях плотность заполнения воздушных магистралей резко возрастает, также, как и возрастает сложность управления воздушными судами с земли. Для облегчения задачи навигации применяются различные методы. Одним из решений является многопозиционная система наблюдения, которая позволяет определять точные координаты, высоту и скорость самолета.

МПСН, алгоритм работы, система наблюдения, зона покрытия, базовая станция

Общая конфигурация базовых станций МПСН.

МПСН предназначена для обеспечения в зоне ее действия [1]:

- наблюдения за ВС, оборудованными ответчиками АТС RBS;
- наблюдения за ВС, оборудованными ответчиками режима S;
- наблюдения за ВС, оборудованными бортовой аппаратурой автоматического зависимого наблюдения АЗН-В 1090ES;
- выдачи информации наблюдения в комплекс средств автоматизации управления воздушным движением (КСА УВД)

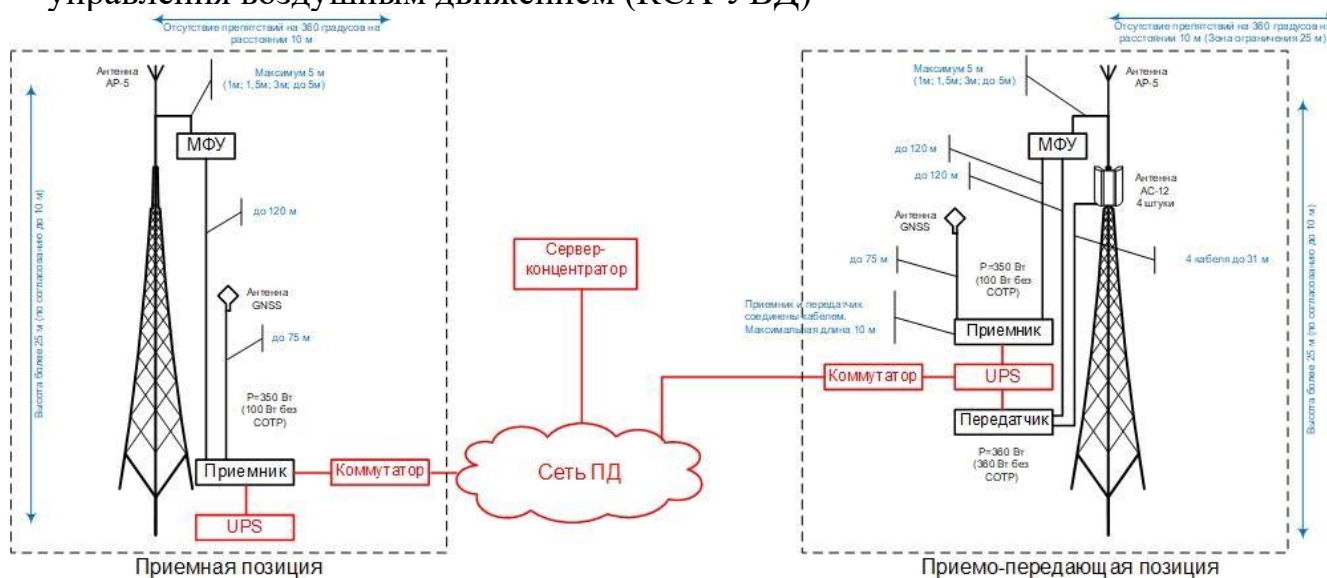


Рис. 1. Общий принцип построения системы МПСН

Из рисунка 1 видно, что на топе антенно-мачтового сооружения устанавливается приемная антенна. Эта антенна является всенаправленной. Ниже располагаются 4 передающие секторные антенны. Как правило, разнос по высоте между приемной и передающей антенной устанавливают равным одному

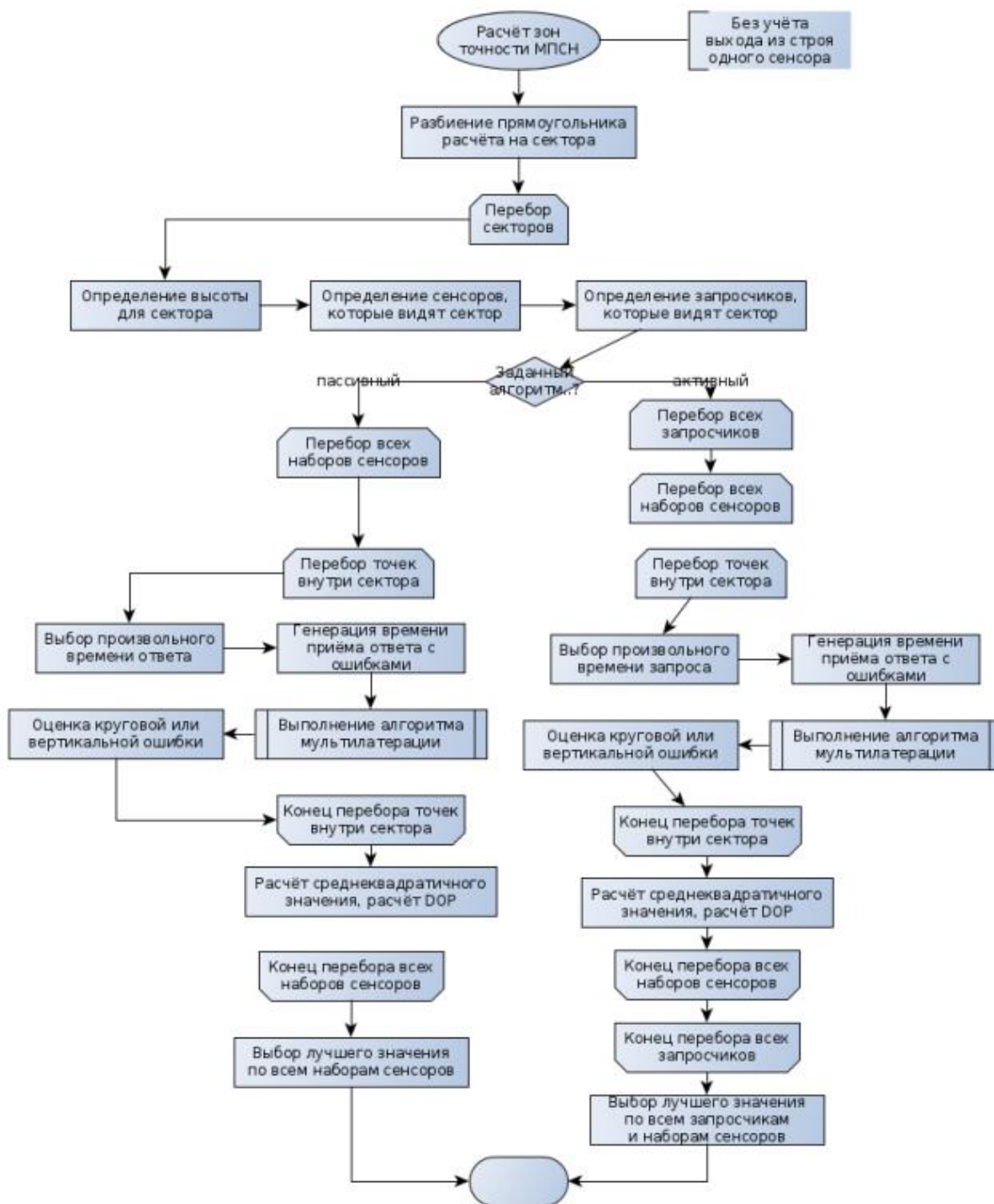


Рис. 3. Алгоритм работы системы многопозиционного наблюдения

На рис. 3 приведен общий алгоритм работы МПСН без учета выхода из строя одного сенсора. Данный алгоритм использует принцип мультилатерации. Конечным итогом выполнения алгоритма является нахождение рассчитанных координат воздушного судна [2].

Выполнение алгоритма мультилатерации (для пассивных алгоритмов). Задача пассивной мультилатерации может быть описана системой уравнений [3]:

$$\{\sqrt{(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2} = c(toa_i - tor), i = 1..N\},$$

где x, y, z – искомые неизвестные координаты воздушного судна, x_i, y_i, z_i – координаты сенсора i

c – скорость распространения электромагнитной волны в воздухе,

N – число сенсоров в алгоритме

toa_i – время приема ответа с учетом параметра ошибок

tor – произвольное время

Выполнение алгоритма мультилатерации (для активных алгоритмов).
Задача активно мультилатерации может быть описана системой уравнений:

$$\sqrt{(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2} = c(tor - toi),$$

где toi – произвольное время запроса

Практические результаты применения алгоритма.

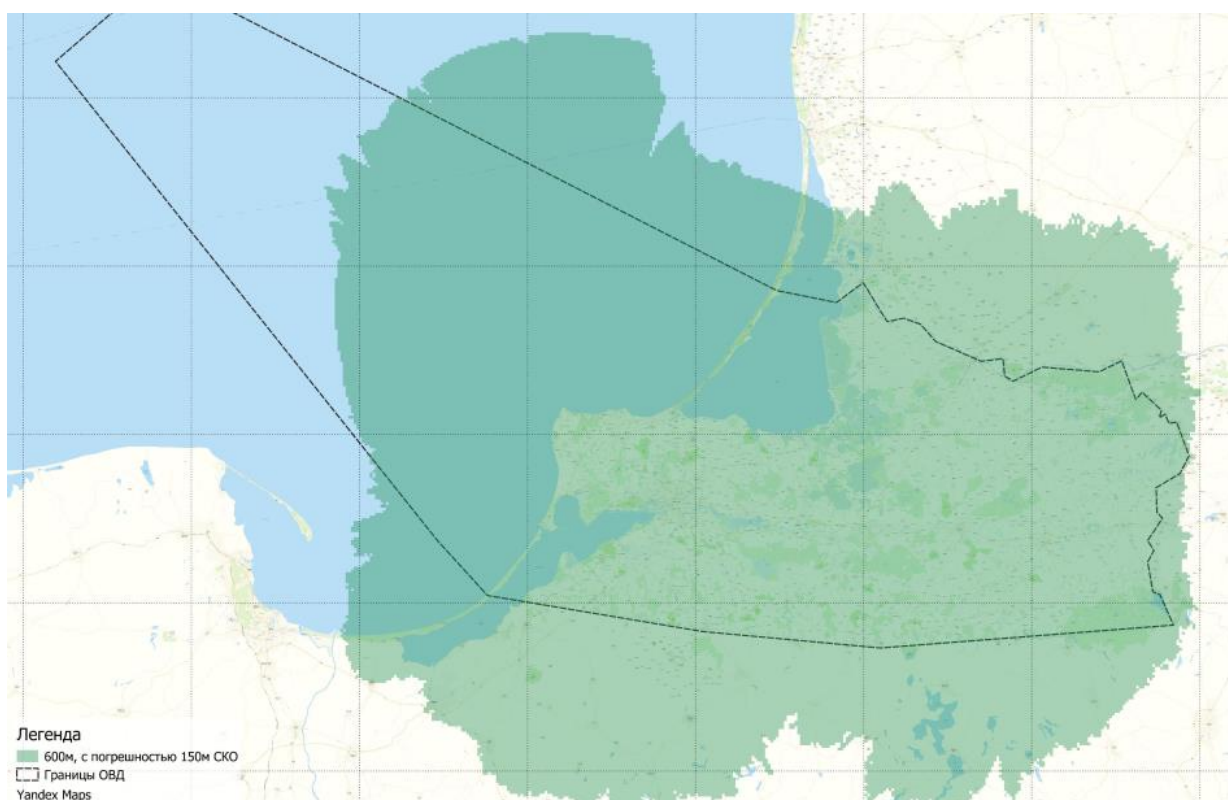


Рис. 4. Зона покрытия МПСН на высоте 600 метров



Рис. 5. Зона покрытия МПСН на высоте 12000 метров

На рис. 4 и 5 приведено математическое моделирование зоны покрытия МПСН на разных высотах. Из рисунков видно, что с увеличением высоты значительно увеличивается зона покрытия, но также увеличивается и погрешность определения положения воздушного судна, со 150 метров до 350 метров по горизонтальной плоскости, что не является критическим [2].

Список используемых источников:

1. МПСН для удаленного диспетчерского обслуживания [Электронный ресурс]. URL: <https://innovation.mintrans.ru/upload/iblock/db4/db4b489d55e1166d52014b426f6bbea5.pdf> (Дата обращения: 10.11.2022)
2. Проектная документация ПАО "Гипросвязь"
3. СЕРТИФИКАЦИОННЫЕ ТРЕБОВАНИЯ (БАЗИС) к широкозонным и аэродромным многопозиционным системам наблюдения

Rekel P.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Multilateration system.

A properly designed multilateration system allows you to cover a large area of airspace while meeting all the requirements for the quality and reliability of coverage.

Key words: *multilateration, quality of coverage, cover a large area.*

УДК 621.3.052
ГРНТИ 49.31.01

ВЫБОР УЗЛА ЦИФРОВОЙ ОБРАБОТКИ ПРИ МНОГОКАНАЛЬНОЙ ПЕРЕДАЧЕ

К. А. Родина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В связи с увеличением числа абонентов появляется потребность в организации многоканальной передачи. При построении сети с параллельной передачей по нескольким каналам разработчику необходимо определиться с выбором устройств, которые смогут справиться с такими задачами как модуляция, фильтрация и объединение каналов. Более качественно с подобного рода задачами поможет справиться современное цифровое решение – системы на кристалле.

многоканальная передача, системы на кристалле, цифровая система, микропроцессор, программируемые логические интегральные схемы

В основе современных систем передачи сообщений лежит разработка систем и методов, которые позволяют одновременно передавать по одной физической цепи большое число независимых сообщений, то есть организация многоканальной связи. Это целесообразно, в первую очередь, с экономической точки зрения: так как из всех элементов системы связи наибольший процент стоимости приходится на линии связи [1], а многоканальные системы позволяют «уплотнить» радиоканал, группируя несколько сообщений согласно разным методам разделения канала. Структурная схема многоканальной системы передачи представлена на рис. 1.

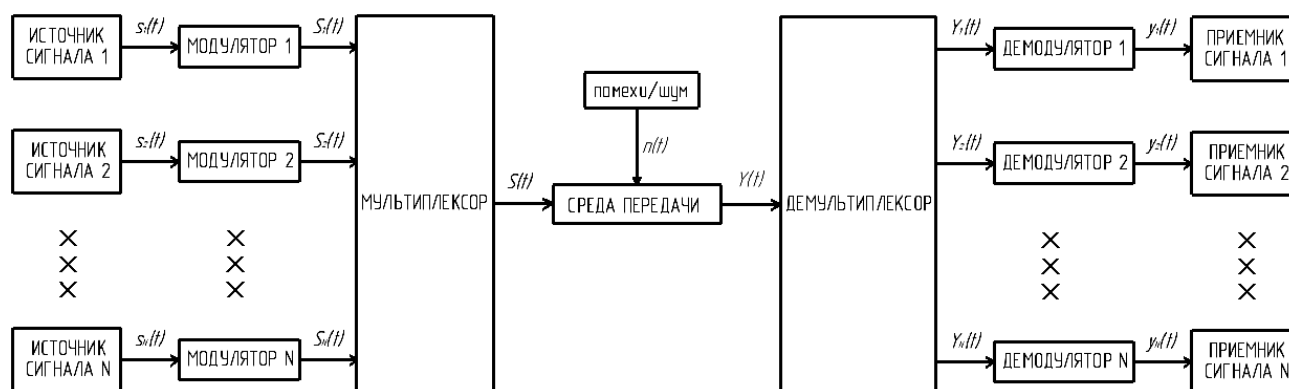


Рис. 1 Структурная схема многоканальной передачи

Несколько источников передают информационные сигналы, каждый из которых поступает на соответствующий модулятор для того, чтобы в дальнейшем можно было бы выделить каждый сигнал из группы. Для обеспечения переноса в среде передаче нескольких канальных сигналов используется мультиплексор, после которого в среду передачи поступает групповой сигнал. В тракте объединенная последовательность претерпевает различного характера искажения, поэтому передаваемую последовательность

необходимо отфильтровать. Для выделения из среды передачи отдельных сигналов служит демультимплексор. Демодулятор позволяет выполнить обратное преобразование, в соответствии с используемой модуляцией.

Примером многоканального передатчика может выступать базовая станция. Абонентские терминалы передает сигнал на антенную решетку базовой станции в пределах зоны обслуживания, которой они находятся. Согласно технологии организации множественного доступа, запросы от абонентов распределяются по группам. Самыми распространенными технологиями множественного доступа являются: множественный доступ с частотным разделением – выделенный для определенной системы спектр делится на полосы частот, в которых осуществляется передача канальной информации от разных абонентов, множественный доступ с временным разделением – выделенная полоса частот предоставляется на определенный короткий промежуток времени, выстраивая очередь и множественный доступ с кодовым разделением – сигналы, принятый от абонентов шифруются и передаются одновременно. В качестве примера можно рассмотреть систему с частотным разделением: с антенны сигнал поступает на микросхему передатчика, где преобразуется в цифровой сигнал, и передается на модулятор, осуществляющий перенос на одну из выделенных несущих частот. Следует отметить, что количество передатчиков, входящий в состав базовой станции, должно соответствовать количеству выделенных частотных каналов. После перестроения все сигналы суммируются и передаются по радиотракту, после которого необходимо осуществить обработку с помощью фильтров с конечной импульсной характеристикой. Далее спектр отчищенной группы сигналов разделяется на несколько каналов согласно количество несущих частот и перестраивается на первоначальную несущую частоту с помощью демодулятора. Каждый из канальных сигналов передается абоненту, которому было адресовано сообщение.

Чтобы описанную систему с параллельной передачей по нескольким каналам, одной из важных задач является выбор управляющего устройства, которое будет объединять в себе функции: модулятора, мультиплексора, демультимплексора, демодулятора, а также фильтра, который необходим, чтобы отчистить сигнал от шума. В качестве такого устройства можно использовать микропроцессор или программируемые логические интегральные схемы (ПЛИС). При решении данной задачи необходимо ознакомиться с преимуществами и недостатками каждого. Сравнительная характеристика микропроцессора и ПЛИС представлен в таблице 1.

ТАБЛИЦА 1. Сравнительный анализ микропроцессора и ПЛИС

	Микропроцессоры	ПЛИС
Обработка	Последовательная	Параллельная
Выполнение операций с плавающей запятой	Возможно	Возможно, однако требует больше времени и ресурсов
Выполнение арифметических операций	Быстро справляется, более точный результат	В зависимости от сложности, может быть недостаточно точный и требовать больше времени

Потребление/скорость	Низкое	Высокое
Стоимость	Высокая	Низкая
Аппаратный дизайн	Простой	Сложный

Микропроцессоры имеют преимущество при выполнении последовательных или насыщенных циклами алгоритмов, а также при реализации сложных алгоритмов, требующих вычислений с плавающей точкой.

ПЛИС может создавать самые разные электронные схемы – от простых комбинаторных схем, например, сумматора или мультиплексора, до сложных систем управления роботизированными комплексами [2], а также решить задачи обработки сигналов, где требуется больше вычислительной мощности для обработки данных. Задачи ПЛИС также предполагают решение задачи с наименьшим возможным временем при минимальном потреблении ресурсов и мощности.

Оптимальным решением, который позволит объединить в себе преимущества ПЛИС и микропроцессора являются системы на кристалле, микросхема, которая способна выполнять функции нескольких отдельных устройств, построенных на одном кристалле.

Таким образом, с помощью систем на кристалле можно построить цифровую систему, которая позволит передавать данные от нескольких абонентов быстро и с наименьшими искажениями. Такое устройство может объединять в себе ПЛИС, которая будет выполнять мультиплексирование каналов, модуляцию, и процессора, который лучше справиться с очищением сигнала от помех.

Список используемых источников:

1. Абилов А.В. А15 Лекции по курсу «Многоканальные системы передачи». – Ижевск: Изд-во ИжГТУ, 2001. – 130 с.
2. Д.С. Смирнов, И.Г. Дейнека, А.С. Алейник, И.А. Шарков. Основы разработки встраиваемых систем на ПЛИС с использованием процессора NIOS® II. Учебное пособие. – СПб: Университет ИТМО, 2019. – 95 с.

Rodina K.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Choosing a digital processing node for multichannel transmission.

Due to the increase in the number of subscribers, there is a need to organize multi-channel transmission. When building a network with parallel transmission over several channels, the developer needs to decide on the choice of devices that can cope with tasks such as modulation, filtering and channel unification. A modern digital solution – systems on a chip - will help to cope with such tasks more efficiently.

Key words: *multichannel transmission, systems on a chip, digital system, microprocessor, programmable logic integrated circuits.*

УДК 621.396.99
ГРНТИ 49.33.01

ОБЗОР РАДИОПАРАМЕТРОВ В СЕТЯХ ПОДВИЖНОЙ СВЯЗИ

Р. С. Рощинский

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современной жизни людей весомую роль играет мобильная связь – по всему миру насчитывается несколько миллиардов уникальных пользователей. Однако для того, чтобы обеспечить всех людей связью, необходимо проводить комплекс работ: разработка и производство оборудования, планирование и установка произведенных устройств, их эксплуатация, а также проверка качества работ. С этими работами связаны весьма важные элементы – радиопараметры.

сотовая связь, мобильная связь, радиопараметры

В настоящее время важную и неотъемлемую роль несет мобильная связь. Центральным вопросом в обеспечении связи является определение и выявление необходимых радиопараметров. Они важны во всех аспектах: создание, сертификация и испытание оборудования, планирование радиосети, оценка качества услуг и работы связи.

Консорциум 3GPP, разрабатывающий спецификации для мобильной телефонии, в своих релизах определяют требования для стандарта. Создается техническая спецификация TS (Technical Specifications), либо технические отчеты TR (Technical Reports) [1]. На основании этих документов можно определить, к примеру, диапазон рабочих частот, того или иного стандарт подвижной связи. В таблице 1 показан пример рекомендаций [2].

ТАБЛИЦА 1. Поддерживаемые диапазоны частот LTE

Номер рабочей полосы частот	Диапазон восходящего направления, МГц	частот	Диапазон нисходящего направления, МГц	частот
1	1920 – 1980		2110 – 2170	
2	1850 – 1910		1930 – 1990	
3	1710 – 1785		1805 – 1880	
4	1710 – 1755		2110 – 2155	
5	824 – 849		869 – 894	
7	2500 – 25700		2620 – 2690	

Таким образом, для существующих технологий подвижной связи (GSM, UMTS и LTE) можно классифицировать и выделить основные радиопараметры, применяемые в различных задачах.

Рассмотрим первый вариант применения радиопараметров, относящихся к созданию базовых станций. В данном случае рассматривается стандарт связи GSM. На примере приказа от 12 апреля 2007 года №45 министерства

информационных технологий и связи РФ [3] выделяются следующие радиопараметры:

1. Требования по частотному диапазону. Для стандарта связи используются два основных диапазона частот – GSM900 и GSM1800. Для каждого из них есть свои требования по количеству частотных каналов, по соседним каналам, а также по частотному разнесу между несущими.

2. Следующим немаловажным параметром является скорость передачи информации. при передаче голосовой информации в виде цифрового потока с полной (13 кбит/с) или половинной (6,5 кбит/с) скоростью; при передаче данных - до 9,6 или 14,4 кбит/с. Для данного стандарта также используются разные модуляционно-кодирующие схемы, которые тоже можно отнести к радиопараметрам и которые могут значительно повлиять на качество сети.

3. Требования к параметрам фазовой ошибки. В зависимости от модуляции, которая выбирается для работы БС, выдвигаются требования для фазовой ошибки, которые не должны превышать установленных норм.

4. Требования к параметрам выходной мощности передатчика БС. В зависимости от класса мощности БС, выбираются различные выходные мощности. Все они также разделяются для различных частотных диапазонов.

Приведенные выше требования предъявляются для каждого поколения подвижной связи, однако значения, к примеру у технологий GSM и LTE значительно отличаются.

В процессе планирования радиосети, необходимо учитывать еще больше радиопараметров. Помимо учета приведенных требований и параметров, появляются новые требования к базовым станциям – например правила по использованию, ограничениям для антенн и фидерных устройств, который описаны в приказе министерства информационных технологий и связи РФ от 23 ноября 2006 г. №153 [4]. К этим параметрам относят пункты:

1. Коэффициент усиления антенны
2. Значение коэффициента защитного действия
3. Значения коэффициента стоячей волны
4. Волновое сопротивление антенны

Последний выделенный аспект, это оценка качества сети. Данный пункт основывается на проверке всего созданного и установленного оборудования. В зависимости от выбранного измерительного комплекса оборудования и тестируемого стандарта связи, будут выбираться радиопараметры для оценки качества каналов связи. Если производится тестирование оборудования, которое работает на базе технологии LTE, то производится проверка по параметрам, указанных в таблице 2.

ТАБЛИЦА 2. Радиопараметры технологии LTE

Радиопараметры	Пояснение
EARFCN	E-UTRA Absolute Radio Frequency Channel Number - номер канала в сети LTE. Он обозначает центральную частоту.
RSSI	Received Signal Strength Indicator -Значение мощности сигнала, поступающего на антенны устройства
Phy Cell ID	Физический идентификатор соты. Он используется смартфоном для переключения между сотами
RSRP	Reference Signal Received Power - оценка мощность на основе пилотных сигналов

Однако при работе с указанными выше параметрами, могут возникнуть ошибки из-за шумов, помех, искажений или битовых рассинхронизаций. Для их определения и работы с ними ввели, к примеру - BER (Bit Error Rate) - частота возникновения ошибок, Block Error Rate (BLER) - отношение числа блоков, содержащих ошибку, к суммарному числу блоков, принятых в цифровой сети. К каждому из них, по приказам и правилам вводят свои ограничения и рекомендации [5].

В заключении статьи необходимо уточнить, что в тексте приведены далеко не все ключевые радиопараметры, которые необходимо учитывать в работе с подвижной связью, но даже все параметры, которые были приведены выше, необходимо сверять с приказами и правилами, которые устанавливают для стандартов связи.

Список используемых источников:

1. Константинов А. С. Методы тестирования радиооборудования сети LTE
2. 3GPP TS 36.101 version 12.7.0 release 12. Evolved universal terrestrial radio access; user equipment radio transmission and reception.
3. Приказ от 12 апреля 2007 года N 45 «Об утверждении Правил применения базовых станций и ретрансляторов систем подвижной радиотелефонной связи. Часть II. Правила применения подсистем базовых станций и ретрансляторов сетей подвижной радиотелефонной связи стандарта GSM 900/1800»
4. Приказ от 23 ноября 2006 г. N 153 "Об утверждении Правил применения антенн и фидерных устройств"
5. Приказ от 06 июня 2011 г. №128 «Об утверждении Правил применения абонентских терминалов сетей подвижной радиотелефонной связи стандарта LTE».

Roschinskiy R.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Review of radio parameters in mobile networks.

Mobile communications play a significant role in people's lives today - there are several billion unique users worldwide. However, in order to provide all people with communications, it is necessary to carry out a set of works: design and manufacture of equipment, planning and installation of manufactured devices, their operation, as well as checking the quality of the work. There are very important elements associated with this work: radio parameters.

Key words: *cellular communications, mobile communications, radio parameters.*

УДК 621.396.969
ГРНТИ 47.49.31

ИСПОЛЬЗОВАНИЕ SDR-ТЕХНОЛОГИИ ДЛЯ ЗАДАЧ СЕТЕВОГО ПОЗИЦИОНИРОВАНИЯ. ФОРМИРОВАНИЕ ИНФОРМАЦИОННОГО БЛОКА MIB

К. Е. Рютин, Г. А. Фокин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Задача позиционирования пользовательских устройств (UE – User Equipment) в сети мобильной связи LTE приобрела высокую актуальность в последние годы, особенно в контексте наличия препятствий, неблагоприятных для устойчивого приёма сигналов ГНСС в среде с плотной городской застройкой. Объектом настоящего исследования является SDR-демонстратор технологии позиционирования в сети LTE, разработанный для апробации новых технических решений по повышению точности определения местоположения устройств UE в существующих сетях 4G LTE и в перспективных сетях 5G NR. Целью данного исследования является разработка и проверка формирователя главного информационного блока MIB (Master Information Block), необходимого UE, в частности, для извлечения параметра ширины полосы пропускания во время позиционирования в сети LTE. Результатом настоящего исследования является реализация и экспериментальная апробация формирователя блока MIB стандарта LTE на стенде SDR-демонстратора технологии сетевого позиционирования.

4G, LTE, SDR, MIB, PBCH, позиционирование

Сегодня на базе лаборатории программно-конфигурируемого радио (SDR – Software-Defined Radio) в СПбГУТ уже существует прототип (демонстратор) [1] программно-аппаратной реализации передатчика и приёмника системы позиционирования в сети LTE, представляющий собой прототипы базовой станции eNB и пользовательского устройства UE, соответственно. Настоящая статья является продолжением серии работ, посвящённых описанию и экспериментальной апробации разработанного SDR-демонстратора.

Для выполнения первичных измерений местоположения существующий демонстратор реализует передачу и приём таких сигналов, как сигналы синхронизации (PSS – Primary Synchronization Signal и SSS – Secondary Synchronization Signal), а также опорных сигналов (CRS – Cell-Specific Reference Signal и PRS – Positioning Reference Signal).

В настоящий момент для приёма перечисленных выше сигналов и сбора первичных измерений, необходимо вручную выставлять и контролировать параметры нисходящего канала связи DL на стороне приёмника (UE).

Следовательно, первым шагом к автоматическому согласованию параметров нисходящего канала связи DL между прототипами eNB и UE является реализация передачи главного информационного блока MIB (Master Information Block).

Объектом настоящего исследования является SDR-демонстратор технологии позиционирования в сети LTE, разработанный для апробации новых технических решений по повышению точности ОМП UE в существующих сетях 4G LTE и в перспективных сетях 5G NR. Корректное функционирование UE во время приёма опорных сигналов сети LTE, необходимых для решения задачи позиционирования, требует обработки различных блоков служебной информации, передаваемых базовой станцией eNB. Целью данного исследования является разработка и проверка формирователя блока MIB, необходимого UE для извлечения параметра ширины полосы пропускания во время позиционирования в сети LTE. Результатом настоящего исследования является реализация и экспериментальная апробация формирователя блока MIB стандарта LTE на стенде SDR-демонстратора технологии сетевого позиционирования.

Кодирование главного информационного блока MIB. Для использования в задачах сетевого позиционирования более широкополосных по сравнению с PSS и SSS опорных сигналов CRS пользовательскому устройству UE необходимо определить ширину полосы частот принимаемого из радиоэфира «на лету» сигнала LTE. Параметр ширины полосы частот вместе с числом передающих антенн содержится в блоке MIB, который декодируется UE в первую очередь. Блок системной информации MIB транслируется в физическом вещательном канале PBCH и содержит 24 бита закодированных данных [2]:

1) Ширина полосы канала DL: задаётся в количестве ресурсных блоков, может равняться 6, 15, 25, 50, 75 и 100;

2) Конфигурация канала PHICH (Physical channel HybridARQ Indicator Channel): длительность PHICH (может быть нормальной или расширенной) и ресурсы PHICH (могут быть 1/6, 1/2, 1 и 2);

3) Номер кадра: eNB передаёт значение SFN (System Frame Number) в канале PBCH; UE может синхронизировать SFN на основании этого значения.

Блок MIB кодируется и передается на 4 последовательных символах во втором слоте кадра; данные блока MIB не занимают ресурсные элементы, выделенные для передачи опорных сигналов. Рис. 1 иллюстрирует процедуры кодирования блока MIB согласно [3].

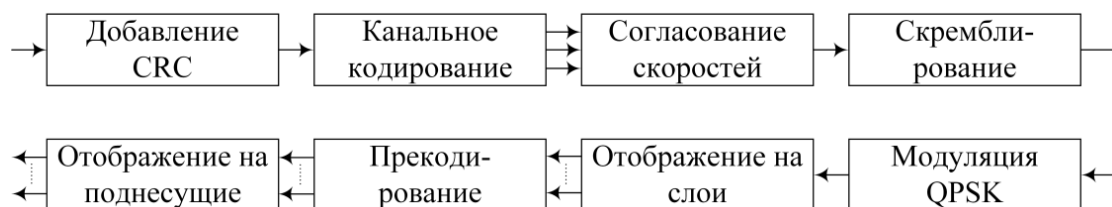


Рис. 1. Процедуры кодирования блока MIB

Лабораторные испытания. Лабораторный стенд (рис. 2) состоит из:

1. Средства объективного контроля, а именно – векторный анализатор сигналов Agilent 89600 Vector Signal Analyzer;

2. ПК с предустановленным СПО Agilent 89600 Vector Signal Analyzer [4] для работы с данным анализатором. Анализатор подключён к этому ПК по интерфейсу FireWire;

3. Ноутбук с предустановленным СПО MATLAB, на котором запущены скрипты формирователя рассматриваемых сигналов;

4. Передающая SDR-плата Ettus USRP B210 [5], подключенная к ноутбуку, в СПО которого формируются сигналы;

5. Коаксиальный кабель (1 м), соединяющий передающий антенный порт SDR-платы с входным портом анализатора.

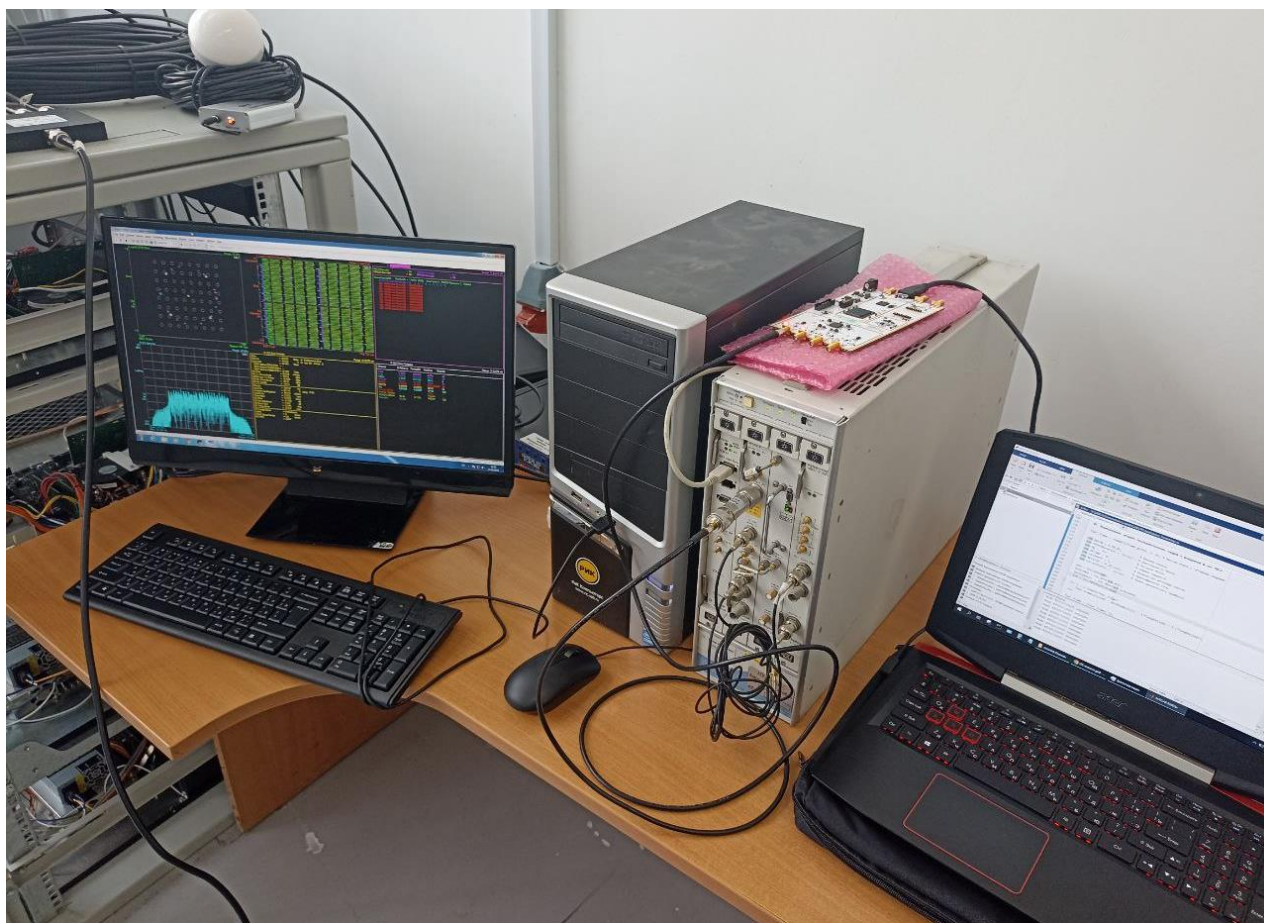


Рис. 2. Лабораторный стенд

Лабораторные испытания заключались в анализе ресурсной сетки OFDM-сигнала на предмет наличия в ней сформированного канала РВСН, а также в контроле правильности декодирования пакета МІВ при различных заранее заданных параметрах полей этого пакета.

В разработанной программе для формирования пакета МІВ предусмотрена структура `env` параметров нисходящего канала связи.

Также, для формирования сигналов синхронизации и опорных сигналов, был задан идентификатор соты Cell ID, равный 9. Идентификатор соты $N_{ID}^{cell} = 3N_{ID}^{(1)} + N_{ID}^{(2)}$ однозначно определяется числом $N_{ID}^{(1)}$ в диапазоне от 0 до 167,

которое определяет идентификатор группы сот, и числом $N_{ID}^{(2)}$, находящимся в пределах от 0 до 2 и определяющим идентификатор соты в пределах группы.

Вместе со всем перечисленным, была задана нормальная длина циклического префикса.

В рамках испытаний проводилось произвольное изменение параметров данной структуры с последующим контролем декодированной информации в программе, работающей с векторным анализатором сигналов Agilent 89600 Vector Signal Analyzer. Окно данной программы целиком показано на рис. 3.

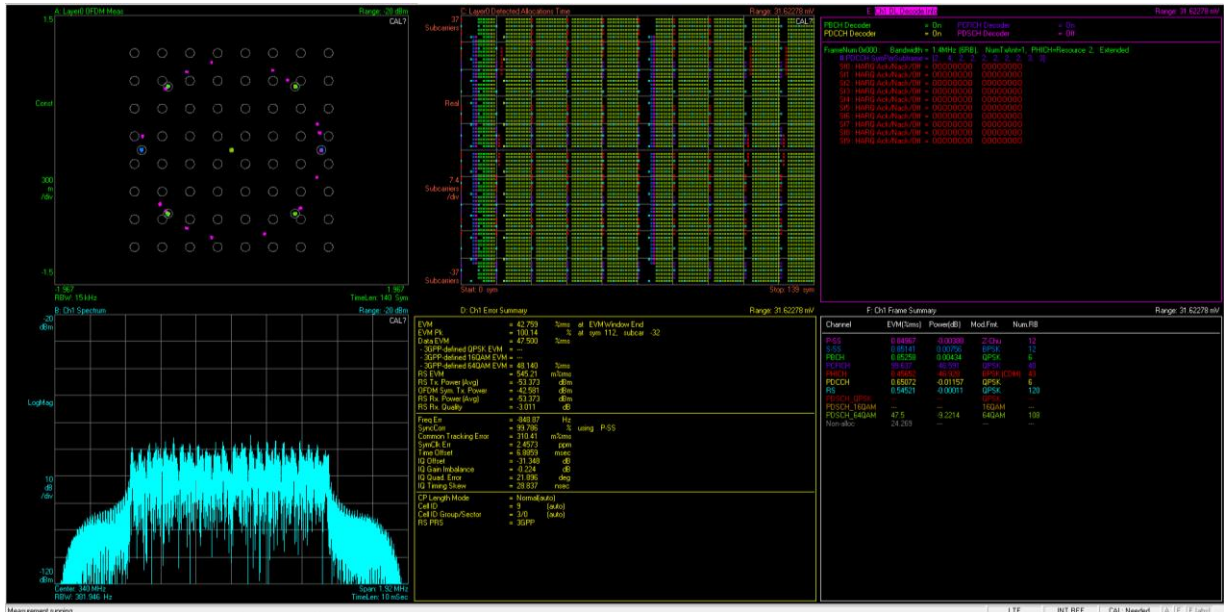


Рис. 3. Окно программы Agilent 89600 Vector Signal Analyzer

В качестве примера проверки корректности работы формирователя на скриншотах ниже (рис. 4 и рис. 5) представлена часть окна программы Agilent 89600 Vector Signal Analyzer, в которой показана декодируемая информация из канала РВСН. В данном примере производилось изменение такого параметра, как длительность РНІСН с расширенной (Extended) на нормальную (Normal), а также производилось изменение группового множителя НІСН с 2 на 1.

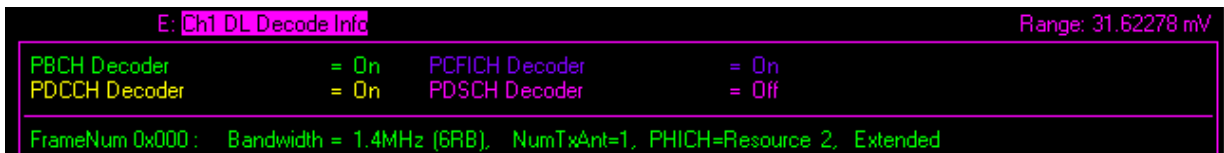


Рис. 4. Декодированный пакет MIB при задании расширенной длительности РНІСН и группового множителя НІСН, равным 2

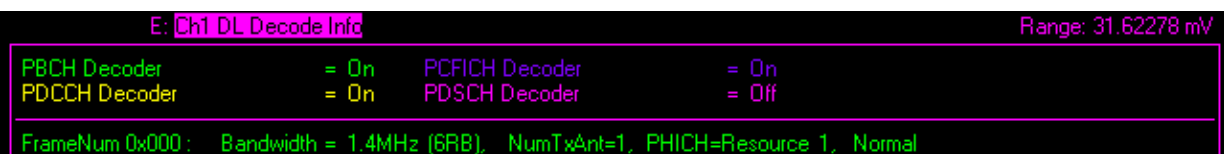


Рис. 5. Декодированный пакет MIB при задании нормальной длительности РНІСН и группового множителя НІСН, равным 1

В той части окна программы, в которой указан идентификатор соты (рис. 6), видно, что Cell ID равен 9. Это значение совпадает с установленным предварительно. Более того, видно, что совпадают $N_{ID}^{(1)}$ и $N_{ID}^{(2)}$, равные 3 и 0, соответственно. Также наблюдается корректное декодирование длины циклического префикса (Normal) и соответствие опорных сигналов позиционирования PRS спецификации.

```
CP Length Mode      = Normal(auto)
Cell ID             = 9          (auto)
Cell ID Group/Sector = 3/0      (auto)
RS PRS             = 3GPP
```

Рис. 6. Декодированное значение Cell ID

Анализируя полученные результаты работы средства объективного контроля, можно заключить, что испытания показали корректность формирования широкополосного канала PBCH, в котором передаются пакеты MIB. Кроме того, можно сделать вывод о корректности формирования сигналов синхронизации (PSS и SSS) и опорных сигналов (CRS и PRS).

В результате данного исследования был реализован и апробирован формирователь главного информационного блока MIB стандарта LTE. Реализованный на SDR-демонстраторе формирователь блока MIB позволяет извлекать параметр ширины полосы пропускания и проводить дальнейшие испытания процедур приёма опорных сигналов CRS макетом пользовательского устройства в полевых условиях. Направлением дальнейших исследований является реализация полученного кодера главного блока служебной информации MIB на ПЛИС, а также реализация декодера блоков MIB средствами СПО MATLAB.

Список используемых источников:

1. Фокин Г.А., Волгушев Д.Б., Харин В.Н. Использование SDR технологии для задач сетевого позиционирования. Формирование опорных сигналов LTE // Т-Comm: Телекоммуникации и транспорт. 2022. Том 16. №5. С. 28-47;
2. 3GPP TS 36.331 V17.1.0 (2022-03) Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification (Release 17);
3. 3GPP TS 36.212 V17.1.0 (2022-03). Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and channel coding (Release 17);
4. Agilent 89600 Vector Signal Analyzer. [Электронный ресурс]. URL: <https://www.keysight.com/us/en/products/software/pathwave-test-software/89600-vsa-software.html> (Дата обращения 11.11.2022);
5. USRP B210 (Board Only). Ettus Research. [Электронный ресурс]. URL: <https://www.ettus.com/all-products/ub210-kit/> (Дата обращения 11.11.2022).

Ryutin K., Fokin G.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

SDR Network Positioning Technology Design. MIB Transceiver Development.

The problem of positioning of user equipment (UE) using LTE mobile communication network has become highly relevant in recent years, especially for GNSS denied environment. The object of this research is a software-defined radio (SDR) LTE network positioning technology prototype design for testing new technical solutions to improve the accuracy of UE location estimation in existing LTE and emerging 5G NR networks. The purpose of this research is development and validation of the Master Information Block (MIB) transmission and reception for bandwidth acquisition on-the-fly during UE positioning in LTE network. The contribution of this research is MIB software realization and its experimental validation in laboratory conditions.

Key words: positioning, software-defined radio, LTE, master information block, MIB.

УДК 004.7
ГРНТИ 49.29.14

МОДЕЛИРОВАНИЕ РАДИОПОКРЫТИЯ СЕТЕЙ РАДИОДОСТУПА С ИСПОЛЬЗОВАНИЕМ ТРАССИРОВКИ ЛУЧЕЙ

С. А. Скрылев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе представлена модель трассировки лучей для распространения волн на миллиметровых частотах, которые будут применяться в будущих беспроводных коммуникациях 5G. Поскольку затухание и блокирование распространения миллиметровых волн в городских условиях гораздо более серьезное, чем на микроволновых частотах, лучи прямой видимости и отраженные лучи вне прямой видимости должны быть главными механизмами распространения.

В этой статье представлено моделирование трассировки лучей на открытом воздухе на частотах 28 ГГц.

трассировка лучей, 5G, миллиметровые волны, 3D-модель

Сети связи пятого описаны стандартами подвижной связи следующего поколения, определяемые международным союзом электросвязи. IMT-2020 (5G) описывает системы, компоненты и связанные с ними элементы, поддерживающие расширенные возможности, превосходящие возможности систем IMT-2000 (3G) и IMT-Advanced (4G).

Подробное описание концепции дальнейшего развития IMT на период до 2020 года и далее содержится в Рекомендации ITU-R M.2083-0 [1], в которой обозначены общие тенденции развития сетей связи, такие как:

- технологический прогресс гетерогенных сетей;
- подключения большого количества устройств и как следствие рост
- глобального трафика IMT (в период с 2020 по 2030 год в 10–100 раз);
- расширение и поддержка различных сценариев использования.

Все эти тенденции предполагают под собой совершенствование параметров сетей связи, для обеспечения приемлемого качества обслуживания QoS (Quality of Services).

Новое поколение сотовой связи будет первым, использующим миллиметровые волны для обеспечения связи в сетях доступа, т. е. в каналах связи между базовыми станциями и мобильными пользователями. В частности, 3GPP в релизе 15 определил первые частотные полосы для строительства 5G. Все полосы радиочастот 3GPP для 5G разделил на два блока FR1 - частоты до 6ГГц и FR2 - частоты свыше 6ГГц или mmWave (миллиметровые волны) [2]. Из последних опубликованных версий стандарта 3GPP в следующей таблице перечислены указанные полосы частот [3], [4].

ТАБЛИЦА 1. Диапазон частот 5G

Блок радиочастот	Радиочастотный диапазон
FR1	450 МГц – 6000 МГц
FR2	24250 МГц – 71000 МГц

Частоты mmWave, действительно, имеют большие участки неиспользованной полосы пропускания, которые могут увеличить скорость передачи данных, что позволяет удовлетворить требования пятого поколения к сверхвысокой пиковой пропускной способности (20 Гбит/с) [1]. Однако характеристики распространения радиочастотных сигналов в этих полосах частот усложняют проектирование надежных систем связи. Во-первых, высокие потери при распространении ограничивают зону покрытия базовых станций mmWave. Кроме того, сигналы mmWave могут быть легко заблокированы, например, транспортными средствами, зданиями, препятствующими прямой видимости. Учитывая сочетание этих явлений, канал mmWave представляется чрезвычайно нестабильным для мобильных пользователей, качество работы которых может быть низким, если не будет принято правильное планирование сети.

Поскольку экспериментальные платформы и испытательные стенды в mmWaves все еще находятся на ранней стадии разработки, анализ и моделирование играют фундаментальную роль в оценке производительности новых решений для сетей mmWave. Трассировка лучей считается многообещающей стратегией моделирования для 5G и обеспечивает точные результаты [5]. Ожидается, что для повышения уровня достоверности на симуляторах, 3D-модели должны быть максимально точными. Например, в сценариях на открытом воздухе требуются конкретные детали, включая точные размеры, материалы и формат зданий, хорошее распределение количества транспортных средств и людей. Важно подчеркнуть, что реалистичность объектов пропорциональна количеству содержащихся в них граней, что приводит к большему количеству взаимодействий, следовательно, больше вычислительных затрат. Чтобы смягчить последствия увеличения количества граней, в этом докладе были использованы оптимизированные модели. В качестве первого шага необходимо выбрать область исследования, рис. 1.



Рис. 1. Карта местности и ее 3D модель

Для импорта 3D модели использовался сайт OpenStreetMap. В этой работе областью исследования был выбран район г. Санкт-Петербурга, возле метро Улица Дыбенко, как городская среда, в которой могут быть плотные бетонные здания, где прямой путь между передатчиком и приемником невозможен. Следующим шагом является установка всех базовых настроек в симуляторе трассировки лучей, таких как, место установки базовой и мобильной станции, высота подвеса, частота работы, мощность антенны, и другие.



Рис. 2. Карта покрытия

На рис. 2 показано местоположение базовой станции 5G работающей на частоте 28 ГГц и ее характеристики. Высота антенны 10м, высота поверхности 9м, широта и долгота 59.90277 и 30.48325 соответственно. Создана модель карты покрытия сигнала, а также установленная мобильная станция вне зоны прямой видимости на расстоянии 110м.

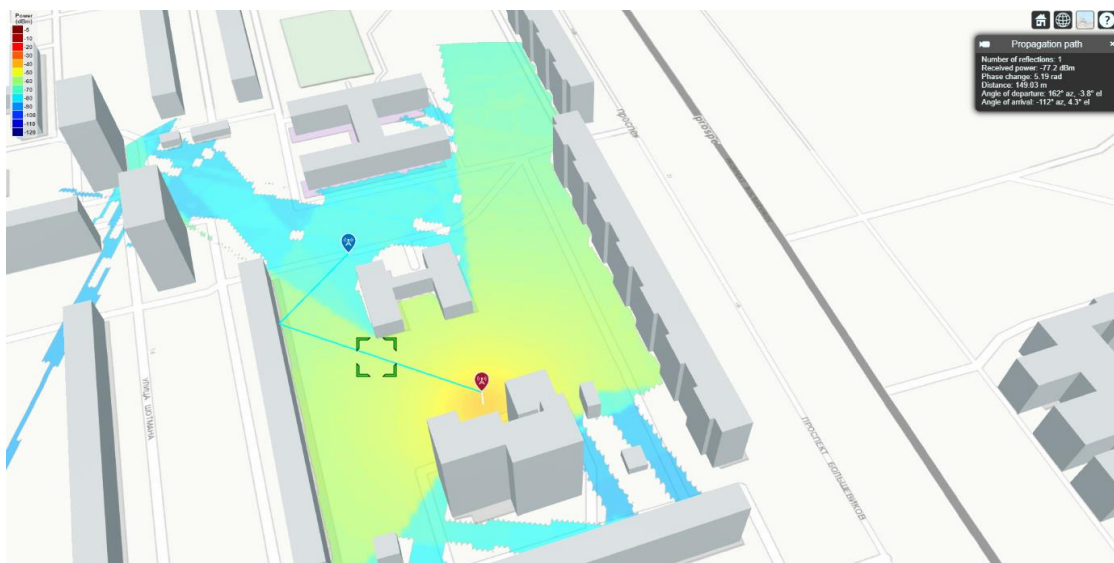


Рис. 3. Карта покрытия с одним отражением

На рис. 3 построена траектория распространения сигнала с одним отражением, учитывающая влияние погодных условий и реалистичные материалы зданий, от базовой до мобильной станции, показаны характеристики данной траектории, которые включают принимаемую мощность -77.2 дБм, изменение фазы 5.19 рад, длину 149 м и углы отправления 162° по азимуту, -3.8° по элевации и прибытия -112° по азимуту, 4.3° по элевации. Также смоделирована карта покрытия сигнала с учетом одного отражения.

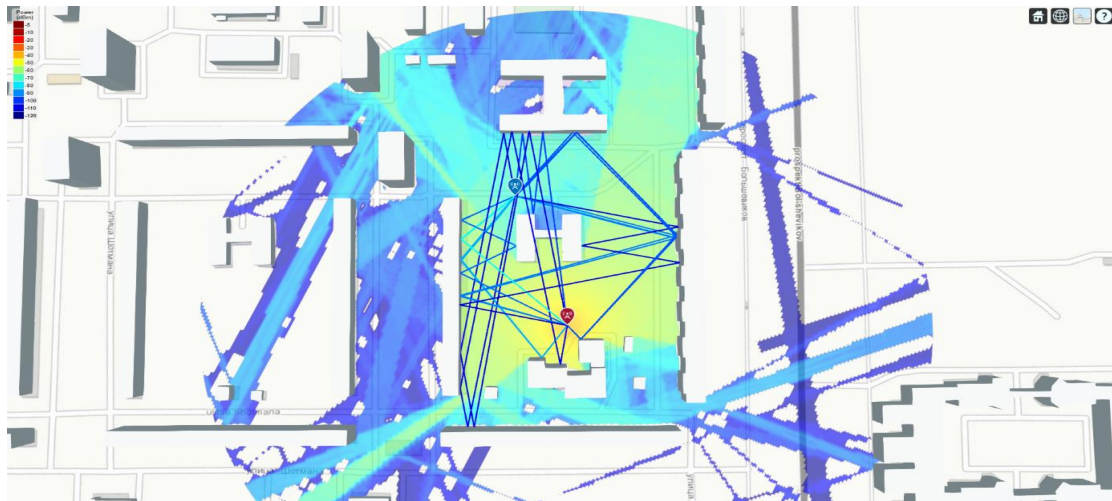


Рис. 4. Карта покрытия с четырьмя отражениями

На рис. 4 построены траектории распространения сигнала с четырьмя отражениями, создана модель покрытия сигнала.

Все измерения, показанные до сих пор, были проведены с использованием изотропной антенны, установленной на базовой станции. Используя отчет ITU-R M.2412 [6], создаем антенну с собственной диаграммой направленности. Теперь можно использовать электронное управление лучом, чтобы улучшить передаваемую мощность в определенном направлении.



Рис. 5. 3D диаграмма направленности антенны от базовой станции в направлении к мобильной станции

Зная угол отклонения для одного отражения из вычислений выше, ориентируем антенну в оптимальное положение для достижения более высокой принимаемой мощности, как представлено на рис. 5. Из характеристик построенной траектории видно, что принимаемая мощность увеличилась с -77.2 дБм до -54.6 дБм по сравнению с такой же траекторией отражения построенной на рис. 3 с использованием изотропной антенны.

Таким образом, в этой работе использовался симулятор трассировки лучей для моделирования связи и покрытия в городской среде. Моделирование показывает, эффективность метода трассировки лучей для миллиметрового диапазона волн, повышая качество и область покрытия.

Список используемых источников:

1. Recommendation ITU-R M.2083-0. IMT Vision - Framework and overall objectives of the future development of IMT for 2020 and beyond. ITU-R, Sep 2015.
2. 3GPP. NR and NG-RAN Overall Description - Rel. 15. TS 38.300, 2018.
3. 3GPP. User Equipment (UE) radio transmission and reception; Part 1: Range 1 Standalone – Rel.17. TS 38.101-1, 2022.
4. 3GPP. User Equipment (UE) radio transmission and reception; Part 2: Range 2 Standalone – Rel.17. TS 38.101-2, 2022.
5. F. Fuschini, E. M. Vitucci, M. Barbiroli, G. Falciasecca, V. Degli-Esposti, “Ray tracing propagation modeling for future small-cell and indoor applications: A review of current techniques,” May 2015.
6. Report ITU-R M.2412-0. Guidelines for evaluation of radio interface technologies for IMT-2020. ITU-R, Oct 2017.

Skrylev S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Simulation of radio coverage of radio access networks using ray tracing.

The paper presents a ray tracing model for wave propagation at millimeter frequencies, which will be used in future 5G wireless communications. Since the attenuation and blocking of the propagation of millimeter waves in urban conditions is much more serious than at microwave frequencies, line-of-sight rays and reflected rays outside the line of sight should be the main propagation mechanisms. This article presents a simulation of ray tracing in the open air at frequencies of 28 GHz.

Key words: *ray tracing, 5G, mmWave, 3D model.*

УДК 621.371.31
ГРНТИ 47.43.17

АНАЛИЗ ОСОБЕННОСТЕЙ РЕАЛИЗАЦИИ MASSIVE MIMO ДЛЯ УМЕНЬШЕНИЯ ПОМЕХОВОЙ ОБСТАНОВКИ

А. А. Страшнов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье проведен анализ технологии крупномасштабных антенных систем. Считается, что данная технология подходит только для миллиметровых волн, работает в средах с высоким уровнем рассеяния сигнала, а высокая производительность может быть достигнута только с помощью методов формирования луча в открытом контуре, но на практике существуют методы, позволяющие избежать данных проблем. Показано, что на современном этапе развития технология крупномасштабных антенных систем может быть использована только с активными антенными модулями, использование предварительного линейного кодирования, объединение по принципу максимального отношения, комбинирования с нулевым форсированием и комбинированием с минимальной среднеквадратичной ошибкой.

massive MIMO, AAU, Zero-Forcing

Беспроводная связь – является одной из самых успешных технологий человечества. Учитывая тенденцию роста беспроводного трафика, которая будет продолжаться благодаря инновационным технологиям и приложениям. Например: интернет вещей, дополненная реальность, искусственный интеллект. Данный рост нуждается в увеличении обработки большего количества трафика данных, что является проблемой для систем прошлого поколения связи. Решением данной кризисной ситуации является технология много антенных систем. Однако, данная технология столкнулась с некоторыми разногласиями в коммуникационном сообществе, о чем свидетельствуют следующие замечания относительно данной системы: «Технология Massive MIMO может использовать почти неограниченное количество антенн высокого качества на базовых станциях. Имея по крайней мере на порядок больше антенн, чем активных терминалов, можно использовать асимптотическое воздействие, характерное для некоторых специальных видов беспроводных каналов. На первый взгляд эта технология выглядит прекрасно, но, к сожалению, сложность обработки сигналов запредельна, а антенные решетки будут настолько огромными, что ее можно реализовать только в миллиметровом диапазоне волн» [1].

Massive MIMO – режим, когда число антенн на базовой станции больше, чем число антенн на мобильном терминале, при использовании единого тракта сигнализации. В таком режиме использование частотного ресурса гораздо более эффективно. При этом также значительно повышается число устройств, которые могут быть обслужены на одном частотном и временном канале внутри одной соты, по сравнению с современными системами 4G, что представлено на рис. 1.


 Рис. 1. Системы 4G и *mMIMO*

Данная технология имеет большие перспективы в сфере сотовых систем связи, высокоскоростных локальных вычислительных сетях, *IoT* и многих других сферах. Этот режим имеет множество преимуществ, к которым можно отнести:

- Увеличение скорости передачи
- Значительное повышение количества абонентских устройств
- Эффективное использование частотного ресурса
- Обеспечивает более надежные сетевые услуги

Но существует и отрицательный момент в *Massive MIMO*. Чем выше порядок *MIMO* – тем больше излучающих элементов в антенне, следовательно, и тем больше кабелей нужно подключать со стороны радиомодулей. Поэтому для технологии *Massive MIMO* нужны не просто антенны, а специальные активные антенные модули (*AAU*) – антенны объединённые с радиомодулем [2]. Цена данных модулей до недавних пор была огромной, но с развитием технологического процесса стала снижаться, что крайне важно для мобильных операторов. И хотя *Massive MIMO* можно использовать и в сетях 4G, пока операторы не спешат внедрять эту технологию.

Поскольку данная технология начала набирать популярность в 2017 году, исследована не до конца. Так же многие терминалы и абонентские устройства еще не имеют поддержки данной технологии, на чем основано большое количество “мифов” относительно данной технологии.

Передача полезной нагрузки в *Massive MIMO* основана на линейной обработке в *BS*. В *Uplink BS* имеет M результатов канала множественного доступа от K терминалов. *BS* применяет линейное комбинирование (сложения с равными весовыми коэффициентами и сложения максимизирующего отношения сигнал/шум), чтобы отличить сигнал передаваемый каждым терминалом, от помех. Простейшим методом является объединение по принципу максимального отношения (*MR*), которое использует оценку канала, для максимизации силы сигнала этого терминала посредством когерентного сложения составляющих

сигнала. Это приводит к тому, что сигнал становится наиболее эффективным, так как мелкомасштабные замирания усредняются по массиву, в результате чего их дисперсия уменьшается с ростом числа M . Это называют укреплением канала и является следствием закона больших чисел. Поскольку в системах TDD каналы восходящей и нисходящей линий связи являются двусторонними, существует тесная связь между объединением приема в восходящей линии связи и предварительным кодированием передачи в нисходящей линии-это известно, как дуализм восходящей и нисходящей линий связи. Линейное предварительное кодирование, основанное на принципах MR, ZF или MMSE, может быть применено для усиления.

Альтернативным вариантом является *Zero-Forcing* (комбинирование с нулевым форсированием) [3], которое подавляет интерференцию между сотами ценой уменьшения коэффициента усиления массива, и *MMSE* (комбинирование с минимальной квадратичной ошибкой), которое обеспечивает баланс между усилением сигналов и подавлением интерференции, путем умножения сигналов на комплексный вес и последующих их суммированием. Объединение приемов создает один эффективный скалярный канал на терминал, где предполагаемый сигнал усиливается и/или подавляется помеха. Любое разумное объединение приемов будет становиться лучше при добавлении дополнительных антенн БС, поскольку имеется больше возможностей для использования наблюдений за каналом. Оставшиеся помехи обычно рассматриваются как дополнительный аддитивный шум, поэтому можно применять стандартные алгоритмы борьбы с ним:

- Смена рабочих частот и используемых для связи сигналов.
- Выбор и использовании полосы частот, в которых помехи минимальны.
- Использование широкополосных (шумоподобных) сигналов.
- Внедрение в аппаратуру схемы ШОУ (Широкополосный усилитель, Ограничитель, Узкополосный фильтр).
- Кодирование по методу Блоха-Харкевича.

Другая задача – сосредоточить каждый сигнал на требуемом терминале (и, по возможности, ослабить помехи для остальных терминалов).

В результате анализа можно сделать вывод, что для, для лучшей работы данная технология нуждается в использовании различных методов кодирования, комбинирования и использования новейших антенных систем.

Список используемых источников:

1. Emil Bjornson, Erik G. Larsson, and Thomas L. Marzetta. Massive MIMO: Ten Myths and One Critical Question//IEE Communications Magazine. 2016 N 54. С. 114-123.
2. HUAWEI TECHNOLOGIES CO., LTD.// Huawei Antenna & Antenna line Products Catalogue [Электронный ресурс] 2017 С. 1-410. URL: <http://www.jemsdata.com/wp-content/uploads/2019/01/HuaweiAAUAntennaLineProductsCatalogue2017-2018.pdf>.
3. Rainer Strobel, Andreas Barthelme, Wolfgang Utschick. Zero-Forcing and MMSE Precoding for G.fast//IEE Global Communication Conference 2015 С. 6-10.

Strashnov A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of Massive MIMO implementation features to reduce interference.

The article analyzes the technology of large-scale antenna systems. It is believed that this technology is suitable only for millimeter-wave, works in environments with high levels of signal scattering, and high performance can only be achieved using open-loop beamforming techniques, but in practice there are methods to avoid these problems. It is shown that at the present stage of development of large-scale antenna systems technology can only be used with active antenna modules, the use of pre-linear coding, combining on the principle of maximum ratio, combining with zero forcing and combining with minimum RMS error.

Key words: *Massive MIMO, AAU, Zero-Forcing.*

УДК 621.376.6
ГРНТИ 49.29.14

ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К РАДИОКАНАЛУ ДЛЯ СВЯЗИ С БПЛА НА ДАЛЬНИЕ РАССТОЯНИЯ

В. С. Тимофеев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире все чаще и чаще требуется аппаратный комплекс, способный проводить мониторинг объектов на дальних расстояниях. В связи с этим появилась потребность организации радиоканала с широкой полосой пропускания. Для решения подобной задачи нужно сформировать требования.

беспилотный летательный аппарат, наземный пульт управления, радиоканал

На данный момент область применения беспилотных летательных аппаратов (далее БПЛА) динамично расширяется. Развитие происходит на качественно другом уровне не только беспилотных аппаратов, а также технологий считывания информации, комплексной оценки опасностей, мониторинга обстановки, угроз дистанционного радиационного, химического и биологического мониторинга. Для реализации мониторинга на труднодоступных объектах инфраструктуры, предотвращения ЧП, а также для исследования и поиска новых месторождений, в силу огромных размеров нашей страны, особенно актуально увеличение дальности устойчивой связи с БПЛА.

Линия радиосвязи летательного аппарата (ЛА) и наземного пункта управления (НПУ) обеспечивает в общем случае двухсторонний обмен информацией между бортовой и наземной аппаратурой. Основными задачами, решаемыми указанной линией связи, являются:

в направлении НПУ-ЛА – передача командной информации для осуществления управления полетом ЛА и работой целевого бортового оборудования;

в направлении ЛА-НПУ – передача телеметрической информации, передача информации, полученной с помощью целевого оборудования (фотоснимки, ТВ изображения и др.).

В рамках постановки задачи, чтобы реализовать радиоканал управления с НПУ к БПЛА и радиоканал передачи информации с БПЛА к НПУ, следует учитывать особенности частотных диапазонов. От частоты радиосигнала зависят следующие параметры: величина пропускной способности (ширина радиоканала); дальность связи (в силу затухания); способность огибать препятствия; проникающая способность.

Также нужно принять во внимание постановление Правительства Российской Федерации от 18 сентября 2019 г. № 1203-47 “Об утверждении Таблицы распределения радиочастот между радиослужбами Российской Федерации и признании утратившими силу некоторых постановлений Правительства Российской Федерации”.

Потери радиосигнала на трассе рассчитываются по формуле:

$$L = 20 \log \left(\frac{4\pi D}{\lambda} \right),$$

где L – потери на распространение в свободном пространстве, дБ; D – расстояние между приемником и передатчиком, м; λ – длина волны, м.

Из рис. 1 видно, что чем выше частота, тем выше затухание сигнала, соответственно меньше дальность устойчивой радиосвязи. Частоты ниже 700-500 МГц не подходят для реализации радиоканала от БПЛА к НПУ, так как должна быть обеспечена необходимая пропускная способность для передачи информационного трафика, а также антенны для такого частотного диапазона по массогабаритным характеристикам могут быть установлены только на крупных (длина от 1.5м) БПЛА. Соответственно нужно найти компромиссное решение, которое удовлетворит требованиям к дальности устойчивой связи и пропускной способности. Также необходимо проверить доступность данного частотного ресурса в таблице ГКРЧ [1].

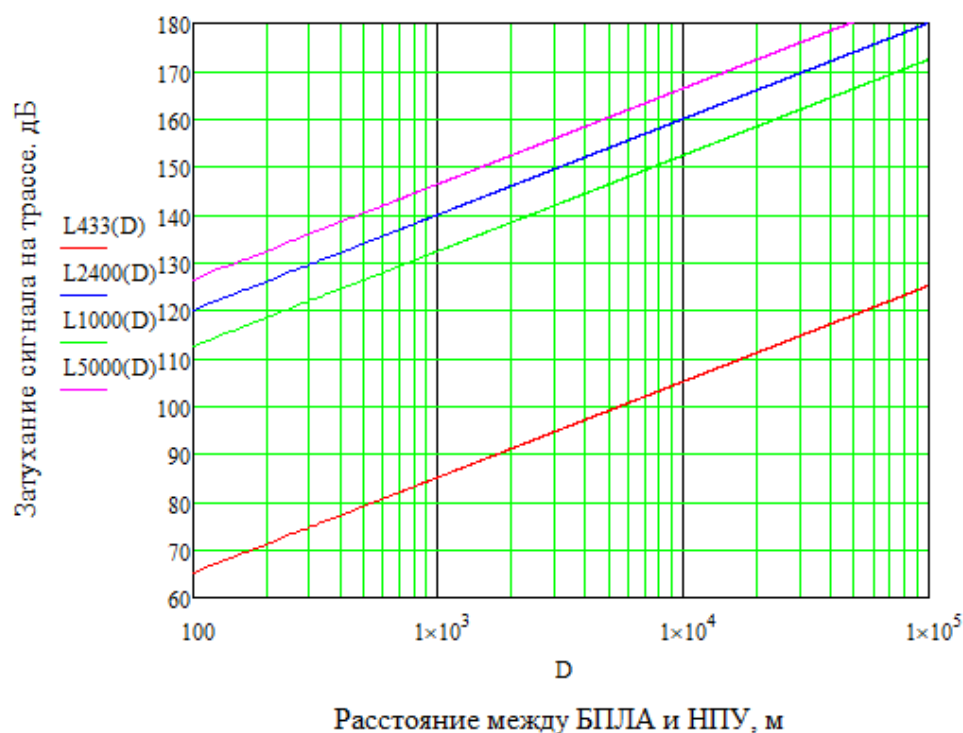


Рис. 1. Затухание сигнала на трассе в зависимости от расстояния между БПЛА и НКУ для двух разных частот

Исследовав график (рис. 1), следует проанализировать таблицу частотного распределения ГКРЧ и проверить наиболее подходящий частотный ресурс в радиослужбах ГКРЧ. В ходе анализа было установлено, что есть возможность на получение лицензии на работу в подходящем частотном диапазоне – 960-1164 МГц или 1164-1215 МГц.

Далее следует рассмотреть вопрос выбора вида модуляции сигнала в приемеопередатчике.

При сравнении различных видов модуляции пользуются критериями спектральной и энергетической эффективности [2]. При этом энергетическая эффективность определяется как энергия, которую необходимо затратить на передачу одного бита информации с заданной достоверностью, а спектральная эффективность определяется как полоса частот, которая необходима для передачи информации с определенной скоростью. Основным требованием при создании системы связи с БПЛА является обеспечение возможности передачи данных с заданной скоростью и вероятностью ошибки при больших расстояниях между ЛА и НКУ. Целесообразным является полное использование разрешенного частотного диапазона с применением расширяющих спектр методов (прямое расширение спектра, расширение спектра методом псевдослучайной перестройки несущей частоты). Для обеспечения максимальной дальности связи в этом случае необходимо использовать наиболее энергетически эффективные методы модуляции. На рис. 2 показано сравнение энергетической эффективности некоторых видов модуляции.

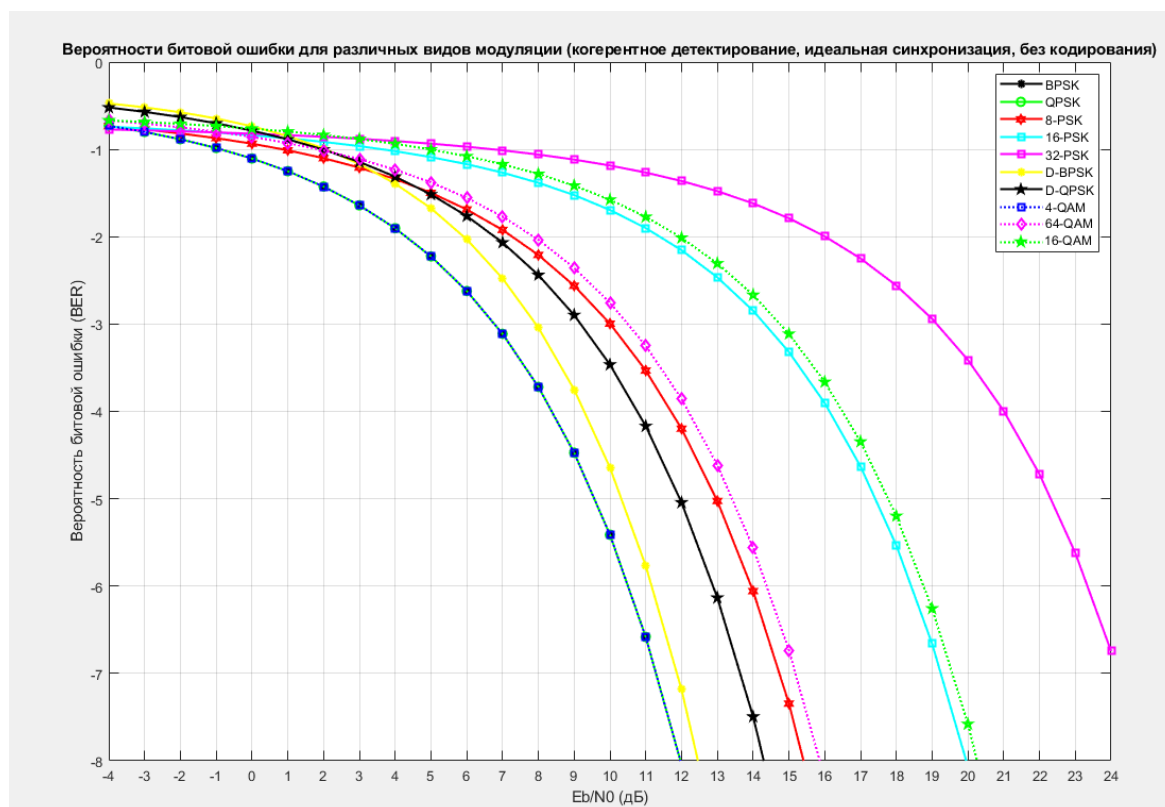


Рис. 2. Вероятности битовой ошибки для различных видов модуляции (когерентное детектирование, идеальная синхронизация, без кодирования)

Как видно из рисунка 2, с увеличением позиционности модуляции вероятность битовой ошибки увеличивается, т. е. для поддержания заданного уровня битовой ошибки необходимо увеличивать ОСШ на входе приемника. Поэтому целесообразным является использование многопозиционной модуляции только при малых расстояниях между ЛА и НКУ. Для обеспечения

максимальной дальности связи необходимо использовать энергетически наиболее выгодные виды модуляции – такие как двоичная фазовая манипуляция (BPSK) и квадратурная фазовая манипуляция (QPSK) (рис. 2). При изменении расстояния между ЛА и НКУ в широких пределах мощность сигнала на входе приемника будет изменяться на ~50 дБ (рис. 1, при изменении расстояния от 500 м до 100 км), что позволяет использовать энергетический запас при малых расстояниях для передачи большего объема информации без изменения ширины полосы частот.

Реализация данного подхода требует создания алгоритмов адаптивного изменения вида модуляции цифровой системы связи в зависимости от обстановки.

Далее следует рассчитать минимально-возможную ширину радиоканала, чтобы была возможность передачи видео и данных с датчиков. Исходя из информации в источнике [3], для передачи изображения в качестве 480p без эффекта HDR, необходимо получить скорость не менее 2,5 Мбит/с. Также нужно учесть помехоустойчивое кодирование, которое увеличивает требование к пропускной способности приблизительно в 2 раза, соответственно требование к скорости передачи данных в радиоканале – не менее 5 Мбит/с.

При подсчёте пропускной способности по теореме Найквиста [4] учитываем, что для максимальной дальности в энергетически более выгодных видах модуляции 2 уровня. Отсюда следует, что необходимую скорость в 5Мбит/с можно получить при ширине канала 2.5 МГц. Также, если при малых расстояниях будет использована QAM-16, то получим скорость 10 Мбит/с, что позволит передавать изображение в формате 720p без эффекта HDR, что значительно улучшит восприятие полученной информации.

В дальнейшем планируется моделирование полного радиоканала с БПЛА.

Список используемых источников:

1. Таблица распределения полос радиочастот между радиослужбами Российской Федерации [Электронный ресурс]. URL: <https://grfc.ru/grfc/zayav/radio-frequency-band-distribution-table/> (дата обращения 10.11.2022).
2. Построение систем связи беспилотных летательных аппаратов для передачи информации на большие расстояния [Электронный ресурс]. URL: <https://uav-siberia.com/news/postroenie-sistem-svyazi-bespilotnykh-letatelnykh-apparatov-dlya-peredachi-informatsii-na-bolshie-ra/#:~:text=%D0%91%D0%B5%D0%B7%20%D1%83%D1%87%D0%B5%D1%82%D0%B0%20%D1%80%D0%B5%D1%84%D1%80%D0%B0%D0%BA%D1%86%D0%B8%D0%B8%20%D0%B2%20%D0%B0%D1%82%D0%BC%D0%BE%D1%81%D1%84%D0%B5%D1%80%D0%B5,%D0%B4%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8F%D1%85%20%D0%B4%D0%BE%20200%E2%80%93300%20%D0%BA%D0%BC.> / (дата обращения 10.11.2022).
3. Оптимальная скорость интернета для просмотра видео в 4K [Электронный ресурс]. URL: https://club.dns-shop.ru/blog/t-326-internet/52706-optimalnaya-skorost-interneta-dlya-prosmotra-video-v-4k/?utm_referrer=https%3A%2F%2Fwww.google.com%2F/ (дата обращения 10.11.2022).

4. Взаимосвязь пропускной способности канала и его полосы пропускания [Электронный ресурс]. URL: <https://studfile.net/preview/9013637/page:3/> (дата обращения 10.11.2022).

Timofeev V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Formation of radio channel requirements for long-distance communication with UAVs.

In the modern world, more and more often a hardware complex is required that is capable of monitoring objects over long distances. In this regard, there was a need to organize a radio channel with a wide bandwidth. To solve such a problem, you need to create requirements.

Key words: UAV, radio channel, GCP, modulation.

УДК 654.165
ГРНТИ 49.43.29

АНАЛИЗ ТРЕБОВАНИЙ К ИНТЕРФЕЙСАМ ТРАНСПОРТНОЙ СЕТИ В ДЕЙСТВУЮЩИХ И ПЕРСПЕКТИВНЫХ СЕТЯХ МОБИЛЬНОЙ СВЯЗИ

В. А. Ушакова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время наблюдается повышенный интерес к сетям пятого поколения. Очевидно, что внедрение этих сетей на территории Российской Федерации будет поэтапным и требует серьезных изменений инфраструктуры оператора мобильной связи. В статье рассматриваются требования к интерфейсам транспортной сети со стороны сети радиодоступа и возможность использования существующей транспортной сети на раннем этапе внедрения технологии.

eCPRI, мобильная связь, сеть радиодоступа, интерфейс.

Скорость передачи данных в сетях мобильной связи зависит не только от возможностей радиооборудования, но и от параметров транспортной сети. От выбранного интерфейса транспортной сети зависит максимальная скорость передачи данных, количество обслуживаемых абонентов и другие важные характеристики. В действующих сетях мобильной связи радиомодуль (RRU – Remote Radio Unit), который располагается рядом с антенными системами или в более современных реализациях интегрирован в саму антенну, и блок управления (BBU – Baseband Unit) соединены между собой оптическим или медным кабелем, а их взаимодействие реализуется с помощью интерфейса CPRI (Common Public Radio Interface).

Внедрение технологии 5G NR требует изменения архитектуры сети радиодоступа. В связи с непрерывным ростом трафика и увеличением числа устройств, подключаемых к сети, для использования 5G была предложена облачная архитектура сети радиодоступа Cloud-RAN. В C-RAN определен транспортный сегмент, получивший название Fronthaul, практическая реализация которого ограничена из-за его высокой стоимости. Новый интерфейс – eCPRI (Enhanced-CPRI), специально разработанный для сетей Fronthaul, предъявляет строгие требования к задержкам, которые могут быть удовлетворены с помощью оптических линий связи. Но значительная стоимость внедрения Fronthaul является препятствием для использования облачной сети радиодоступа. Чтобы решить данную проблему, было предложено передавать потоки eCPRI через каналы Ethernet, что значительно снижает капитальные и эксплуатационные расходы на развертывание C-RAN.

На рис. 1 представлены три транспортных сегмента сети пятого поколения: Fronthaul, Middlehaul и Backhaul [2].

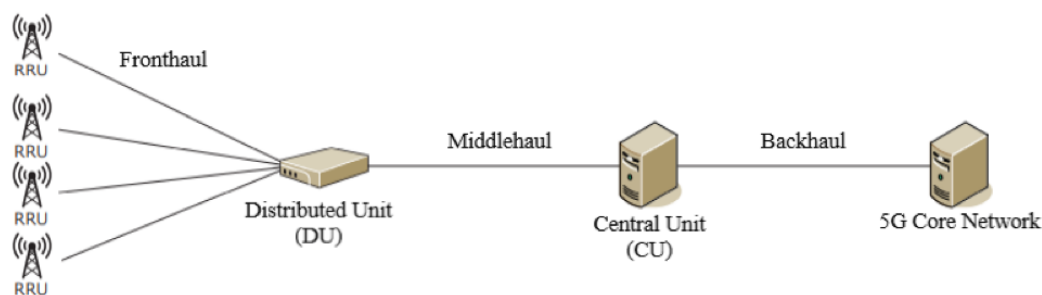


Рис. 1. Топология транспортной сети 5G/IMT-2020

Поскольку 5G требует большого расширения полосы пропускания, только вариант скорости CPRI 10, новый стандарт традиционного интерфейса, может соответствовать этому требованию. Однако данная вычислительная мощность достигла максимального предела, что вызывает сомнения в том, можно ли стабильно использовать CPRI в 5G. Более того, его способность поддерживать расширенные сетевые функции ограничена по сравнению с основными стандартами пакетной передачи. Учитывая такую ситуацию, новый интерфейс был создан для непосредственного устранения скоростных ограничений CPRI. Характеристики интерфейсов представлены в таблице 1.

ТАБЛИЦА 1. Сравнительная таблица требований к транспортному оборудованию Fronthaul [2]

Требование к транспортному оборудованию Fronthaul	Допустимые значения при использовании CPRI	Допустимые значения при использовании eCPRI	
Допустимая двусторонняя задержка	От 50 до 250 мкс, в зависимости от пользовательского устройства	100 мкс – 100 мс в зависимости от класса трафика	
Допустимая ошибка времени	± 16 нс	± 10 нс (± 1.36 мкс в зависимости от класса трафика)	
Точность установки частоты	50 ppb	16 ppb	
Поддержка интерфейсов	CPRI1	0.614 Гбит/с	10 Гбит/с 25 Гбит/с
	CPRI2	1.2288 Гбит/с	
	CPRI3	2.4576 Гбит/с	
	CPRI4	3.0720 Гбит/с	
	CPRI5	4.9152 Гбит/с	
	CPRI6	6.1440 Гбит/с	
	CPRI7	9.8304 Гбит/с	
	CPRI8	10.1376 Гбит/с	
	CPRI9	12.1651 Гбит/с	
	CPRI10	24.3302 Гбит/с	

При реализации eCPRI первичная обработка сигнала осуществляется непосредственно в RRU, снижая требования к пропускной способности (почти в 10 раз). В eCPRI пользовательские данные передаются по сети в виде обычных

Ethernet-пакетов. Для обеспечения функции синхронизации предлагается использовать существующие протоколы, а именно RTP (Precision Time Protocol) и SyncE (Synchronous Ethernet). Информация контроля и управления также будет передаваться по обычно используемым протоколам. При этом требуемая пропускная способность может гибко масштабироваться в соответствии с трафиком пользователя, уменьшая задержку при высоком приоритете. В то же время рабочая полоса увеличивается в 5 раз и составляет 100 МГц, а расстояние между поднесущими остаётся прежним – 15 кГц [1]. Кроме того, eCPRI имеет возможность разделения функций внутри слоя PHY (Physical Layer), которая сохраняет большинство функций в BBU. Это уменьшает количество радиооборудования и позволяет быстрее внедрять расширенные функции без замены уже существующего оборудования.

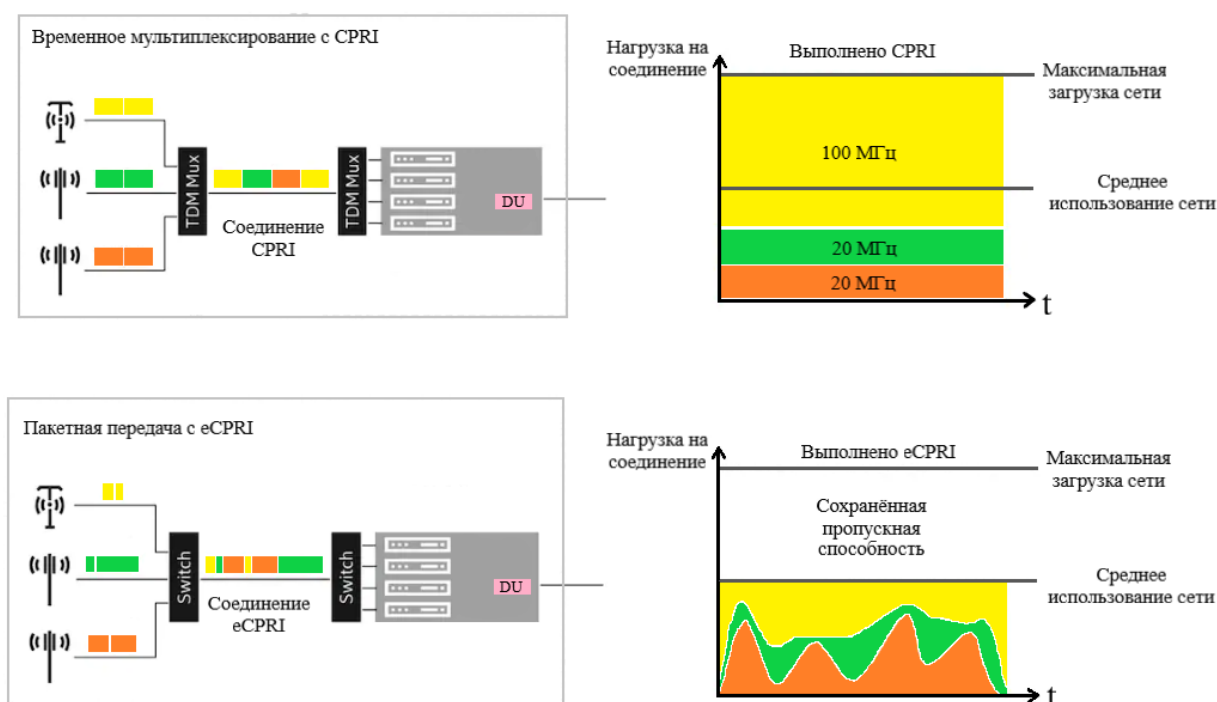


Рис. 2. Разница передачи данных с помощью CPRI и eCPRI

Другим заметным изменением является применение пакетной передачи в eCPRI вместо мультиплексирования с временным разделением (Time Division Multiplexing, TDM) в CPRI (рис. 2). Главным недостатком TDM является неэффективное использование ресурсов основной полосы. При реализации eCPRI статическое мультиплексирование обеспечивает переменный битрейт, изменяющийся в зависимости от нагрузки пользовательского трафика, и тем самым ослабляет требования к пропускной способности [3].

Данные, представленные в таблице 2, отражают требования к ошибке выравнивания по времени (TAE – Time Alignment Error) с учётом выбранной категории.

ТАБЛИЦА 2. Требования к ошибке выравнивания по времени (ТАЕ) в зависимости от выбранной категории [1]

Категория	Область применения	Требования к ошибке выравнивания по времени (ТАЕ)
А+	Использование ММО или разнесённая передача на каждой несущей частоте	65 нс
А	Внутриполосная агрегация соседних несущих с ММО или разнесённой передачей (или без разнесения)	130 нс
В	Внутриполосная агрегация несмежных несущих с ММО или разнесённой передачей (или без), и внутриполосная агрегация несущих с ММО или разнесённой передачей (или без разнесения)	260 нс
С	3GPP LTE TDD	3 мкс

Таким образом, новый интерфейс в отличие от CPRI больше подходит для транспортного сегмента Fronthaul. Внедрение eCPRI обеспечивает наиболее низкие задержки при передаче данных по сравнению с традиционным интерфейсом, что крайне важно для реализации услуг 5G. Не смотря на то, что в ближайшее время внедрение технологий 5G повсеместно в России невозможно, модернизация оборудования под сети ИМТ-2020 неизбежна.

В данной работе было показано, что возможности интерфейса CPRI достигли максимального предела. В то же время внедрение интерфейса eCPRI предполагает внесение значительных изменений в архитектуру RAN. Вследствие этого возникает проблема актуальности применения CPRI в сетях пятого поколения, что будет решено посредством оценки и сравнительного анализа двух интерфейсов.

Список используемых источников:

1. eCPRI Transport Network V1.0, “ Common Public Radio Interface: Requirements for the eCPRI Transport Network”, 2017.
2. Богданова Е. // Транспортная сеть 5G/ ИМТ-2020 – 2019. – №. 4. – С. 40-42.
3. Ericsson. Packet fronthaul – design choices towards versatile RAN deployments [Электронный ресурс] Главная страница URL: <https://www.ericsson.com> (дата обращения 05.11.2022).

Ushakova V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of requirements for transport network interfaces in existing and future mobile communication networks.

Currently, there is an increased interest in fifth-generation networks. It is obvious that the introduction of these networks on the territory of the Russian Federation will be phased and requires major changes in the infrastructure of the mobile operator. The article discusses the requirements for transport network interfaces from the radio access network and the possibility of using the existing transport network at an early stage of technology implementation.

Key words: eCPRI, mobile communication, radio access network, interface.

УДК 628.058
ГРНТИ 47.49.31

ПРИЕМ МЕТКИ ГНСС С ПОМОЩЬЮ GPS/GLONASS-ПРИЕМНИКА

И. Г. Ушкова, Г. А. Фокин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящей работе рассматриваются особенности функционирования устройства приема сигнала глобальных навигационных спутниковых систем (ГНСС) GlobalSat BU-353 GLONASS (далее BU-353G), а также формат метки глобальных спутниковых систем навигации типа nmea. Представлено описание драйвера устройства BU-353G, а также проанализирован формат и содержимое метки принятой ГНСС. В заключении формулируются сценарии использования данной метки в задачах разработки демонстратора технологии сетевого позиционирования.

BU-353G, NMEA, GPS, GLONASS, ГНСС приемник

Устройство BU-353G является навигационный приемник с интерфейсом USB, встроенной активной антенной и способно принимать сигналы GPS (Global Positioning System) и GLONASS (Global Navigation Satellite System) [1].



Рис. 1. Вид устройства BU-353G

Данный приемник (рис. 1) построен на высокопроизводительном чипсете MTK MT3333, поддерживающем обновление местоположения и возможность приема в некоторых условиях городской застройки. BU-353G имеет магнитное основание; длина интерфейсного кабеля составляет около полутора метра.

Приемник работает на частотах $L1$ GPS и $L1$ GLONASS; частота $L1$ означает, что принимается сигнал пониженной точности. Частота $L1$ для GPS изменяется от 1602,56 до 1615,5 МГц, а для GLONASS она равна 1575,42 МГц. Скорость по умолчанию составляет 4800 б/с, а частота обновления данных о местоположении равна 1 Гц, данные параметры можно изменить в программе *SiRF Demo*, частоты изменяют с целью увеличения объема полученных навигационных измерений, а скорость увеличивают для исключения вероятности потери пакетов [2]. Приемник нужен основан на чипсете MTK MT3333, которому предоставляется встраиваемое ПО, которое поддерживает выдачу потока данных в формате NMEA (National Marine Electronics Association). Протокол NMEA имеет достаточно удобное представление, поэтому получил распространение не только в морской навигационной аппаратуре, но и в геодезических, бытовых и авиационных GPS приемниках.

Для анализа принимаемых меток устройством BU-353G воспользуемся прилагаемыми драйверами с официального сайта [GlobalSat](https://www.globalstar.com). После установки драйверов, необходимо подключить устройство к свободному USB-порту ПК. При подключении к ПК устройство получает свое название (рис. 2):

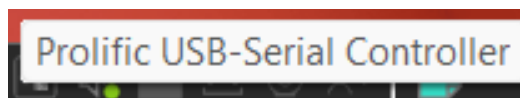


Рис. 2. Название устройства при подключении к ПК

Для приема меток ГНСС можно использовать приложение [GPSInfo](https://gpsinfo.com), или терминал в предустановленной ОС Linux. Далее рассмотрим прием метки ГНСС через терминал. Непрерывный процесс приема метки ГНСС иллюстрирует рис. 3.

```

aniri@aniri-virtual-machine: ~
tcp://localhost:2947  NMEA0183>
Time: 2022-10-28T15:38:12.000Z  Lat: 59 52.645500' N  Lon: 30 28.569100' E
Cooked TPV
-----
GNGLL  GNGSA  GNRMC  GPRVTG  GPZDA  GPGGA  GPGSV  GLGSV
Sentences
-----
SVID  PRN  Az  El  SN  HU  Time: 153812.000  Time: 153813.000
GP 7 7 100 10 24 Y Latitude: 5952.6455 N Latitude: 5952.6455
GP 14 14 112 69 30 Y Longitude: 03028.5691 E Longitude: 03028.5691
GP 17 17 140 23 41 Y Speed: 0.00 Altitude: 14.1
GP 30 30 105 42 34 Y Course: 189.27 Quality: 2 Sats: 6
GL 3 67 193 30 23 Y Status: A FAA:D HDOP: 2.55
GL 23 87 109 9 35 Y MagVar: RMC Geoid: 18.0
GP 5 5 229 11 21 N
GP 8 8 28 14 0 N
GP 10 10 350 7 0 N Mode: A3 Sats: 7 14 17 + UTC: RMS:
GP 13 13 213 67 20 N DOP H=2.55 V=0.94 P=2.71 MAJ: MIN:
GP 15 15 275 52 21 N TOFF: 0.925398058 ORI: LAT:
GP 19 19 163 1 20 N PPS: N/A LON: ALT:
v GSV GSA + PPS GST
(50) $GNGSA,A,3,14,17,30,07,,,,,,,,,2.71,2.55,0.94*10
(46) $GNGSA,A,3,87,67,,,,,,,,,2.71,2.55,0.94*19
(72) $GNRMC,153812.000,A,5952.6455,N,03028.5691,E,0.00,189.27,281022,,D*7C
(39) $GPRVTG,189.27,T,M,0.00,N,0.00,K,D*3D
(35) $GPZDA,153812.000,28,10,2022,*53
(70) $GPGSV,4,1,14,14,69,112,30,13,67,213,20,15,52,275,21,30,42,105,34*75
(66) $GPGSV,4,2,14,17,23,140,41,23,22,323,,40,18,152,36,08,14,028,*77
(68) $GPGSV,4,3,14,24,12,278,15,05,11,229,21,07,10,100,24,21,10,056,*78
(42) $GPGSV,4,4,14,10,07,350,,19,01,163,20*73
(68) $GLGSV,2,1,08,77,66,061,,68,59,261,21,78,51,251,16,67,30,193,23*6F
(64) $GLGSV,2,2,08,69,29,327,,85,19,002,,76,16,066,,87,09,109,35*66
(80) $GPGGA,153813.000,5952.6455,N,03028.5691,E,2,6,2.55,14.1,M,18.0,M,0000,0000
*60
(51) $GNGLL,5952.6455,N,03028.5691,E,153813.000,A,D*44
(50) $GNGSA,A,3,14,17,30,07,,,,,,,,,2.71,2.55,0.94*10
(46) $GNGSA,A,3,87,67,,,,,,,,,2.71,2.55,0.94*19
    
```

Рис. 3. Прием метки с помощью устройства

Из рис. 3 видно, что сигналы, принятые устройством, имеют формат *NMEA*, а именно: заголовок сообщения состоит из 5 символов, из которых 2 первых определяют тип сообщения («*GP*» - *GPS*; «*GL*» - *GLONASS*; «*GN*» - *GLONASS+GPS*), а три оставшихся – его название [3]. В зависимости от названия сообщения, они могут передавать следующие типы стандартных сообщений: *GGA* – информация о местоположении; *GLL* – информация о географических координатах; *GNS* – данные местоположения *GNSS*; *GSA* – информация о геометрическом факторе ухудшения точности и активные спутники; *GSV* – информация о видимых спутниках; *RMC* – минимальный рекомендованный набор данных; *VTG* – скорость и курс относительно Земли; *ZDA* – время и дата. Структура стандартных сообщений показана на рис. 4.

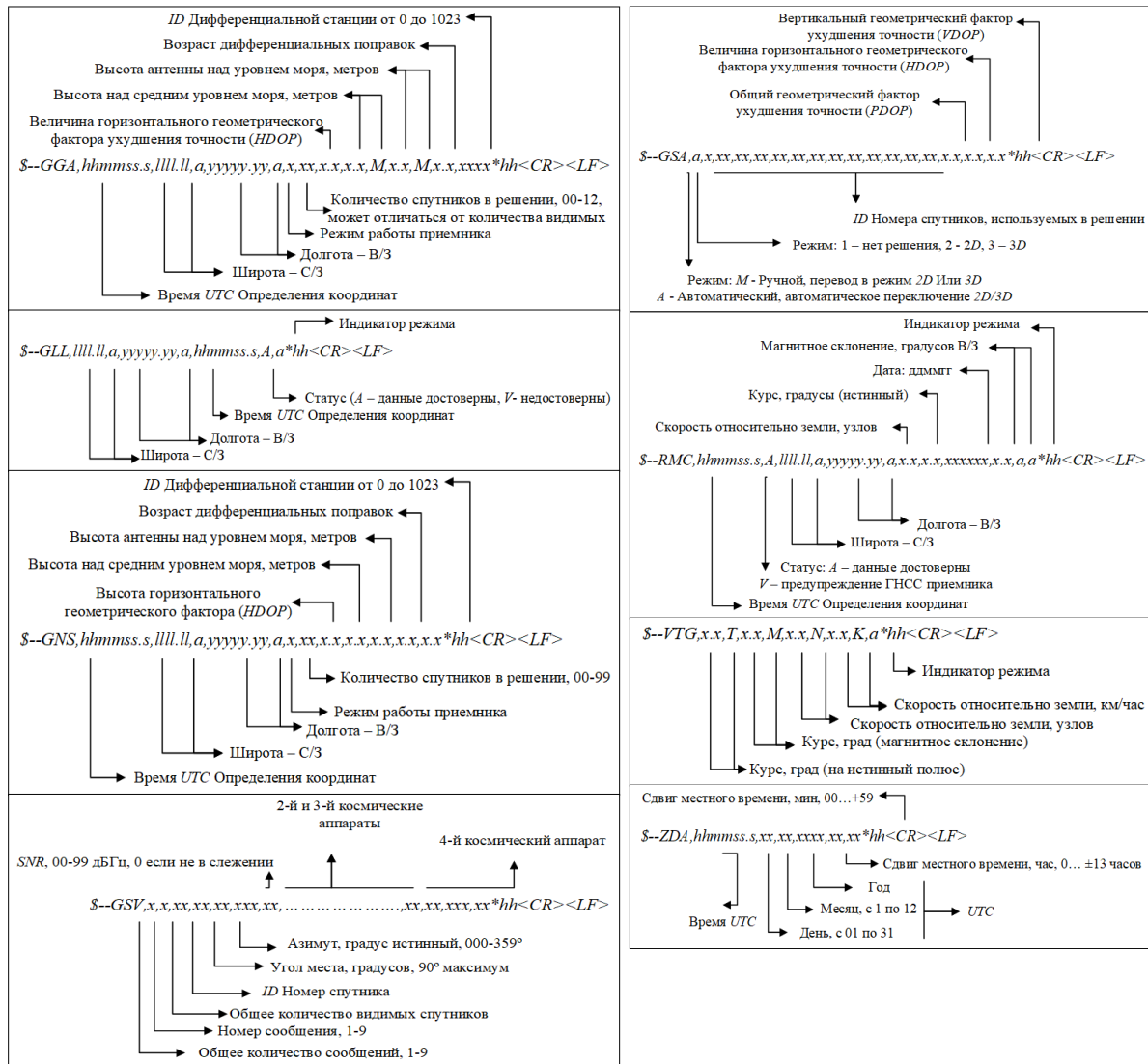


Рис. 4. Структура стандартных сообщений

При запуске приема метки ГНСС, создается файл, который графически отображает расположение спутников (рис. 5). В графе *Skyview* показано расположение спутников, относительно точки местоположения, из которой были произведены измерения. Для каждого спутника указан его номер, а также его условное обозначение: круг обозначает спутники США – *GPS*; ромб обозначает спутники России – *GLONASS*; квадрат обозначает *SBAS (Satellite Based Augmentation System)* – спутниковые системы функционального дополнения); является дополнением для *GPS*. Так же можно заметить, что все обозначения имеют свой цвет, который говорит о качестве сигнала: красный (низкое качество), желтый (среднее качество) и зеленый (высокое качество); а белый цвет говорит о том, что для него отношение сигнал/шум равно 0 дБ, т.е. спутник не отслеживается в данный момент. В графе *Satellite List* описаны параметры для спутников: его принадлежность к системе, *svid* показывает номер спутника в системе, *PRN (PseudoRandom Noise)* показывает *PRN* номер спутника, *elev* показывает высоту над уровнем моря в градусах, *azim* показывает азимут в градусах к истинному северу, *SNR (Signal to Noise Ratio)* показывает отношение сигнал/шум, параметр *used* показывает используется ли спутник в данный момент.

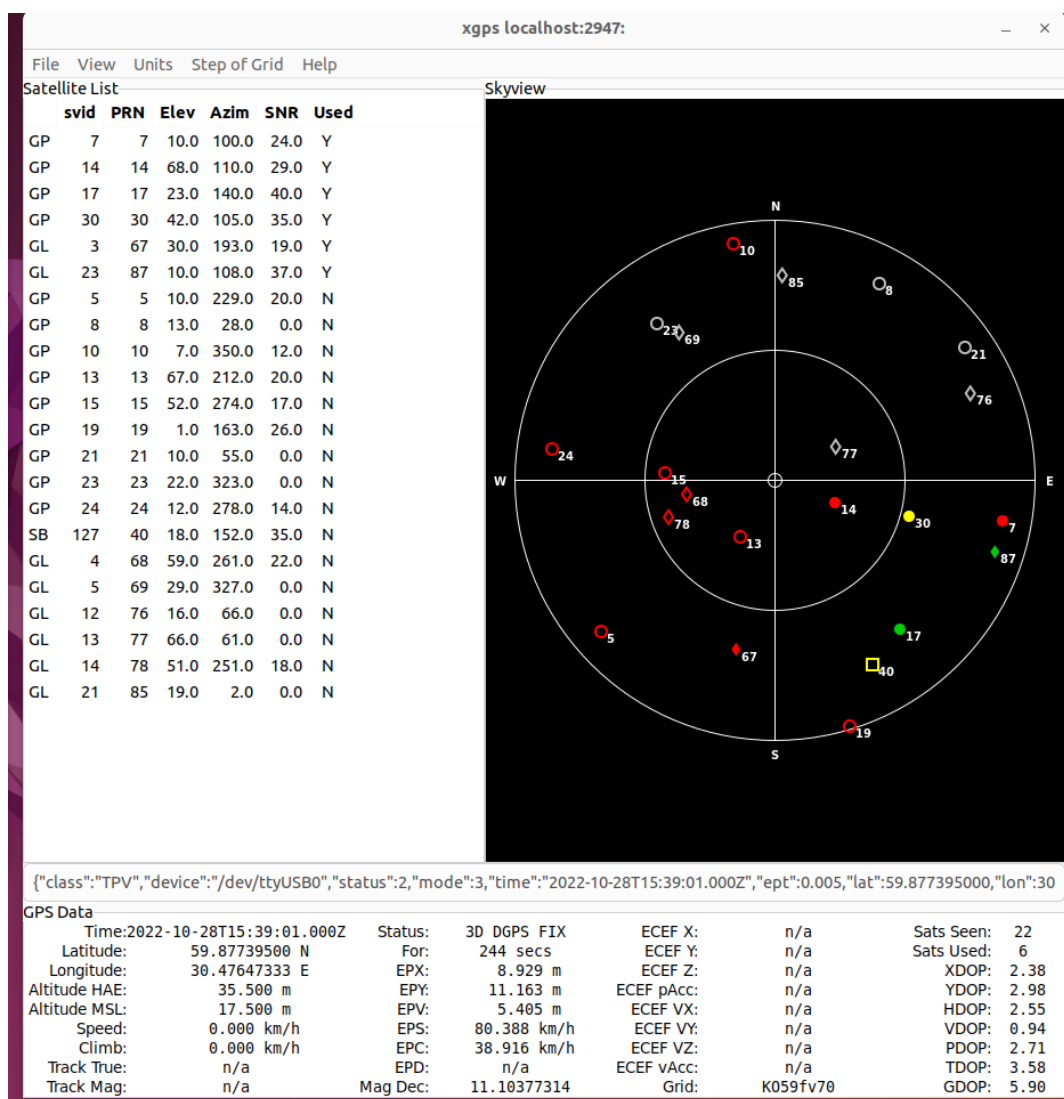


Рис. 5. Графическое представление расположения спутников

Пункт *GPS Data* показывает данные о местоположении/времени/скорости *GNSS (Global Navigation Satellite System)* и местоположение доступных спутников. Также представлены следующие параметры: *Latitude* и *Longitude* показывают местоположение устройства во время измерений; *Altitude HAE (High Altitude Endurance)* показывает высоту, относительно эталонного эллипсоида, на которой производились измерения в метрах; *Altitude MSL (Mean Sea Level)* показывает высоту относительно среднего уровня океанов и морей; *Status: 3D DGPS FIX* говорит о том, что устройство работает корректно и определяет координаты *GPS*, параметр «*DGPS*» говорит о получении более точных данных с точностью до 7,6 метров, а *For* показывает время измерений; *Speed* и *Climb* являются скоростями по движению прямо и на подъем, так как измерения проводились в одной точке, то они равны 0; *Track True* и *Track Mag* показывают правильность записанной информации со спутников, в градусах на истинный поток и в градусах, относительно магнитного склонения, соответственно; *EPX*, *EPY*, *EPV*, *EPS*, *EPC* являются расчетными ошибками по: долготе, широте, вертикали (в метрах), скорости, восхождению (в км/час), соответственно, с доверительным интервалом 95%, это означает с вероятностью 95% данные имеют разницу в 8,929 метров; *ECEF (Earth-Centered, Earth-Fixed)* –

геоцентрическая система координат, где $x/y/z$ – широта/долгота/высота. Представляет местоположение вблизи Земли, в данном случае неактивна; *Sats Seen* показывает количество спутников, которые были в зоне видимости, а параметр *Sats Used* показывает количество используемых спутников, на момент измерения. Последний параметр показывает фактор понижения точности *DOP*, он делится на: «X» - в северном направлении, «Y» - в восточном направлении, «H» - горизонтальный, «V» - вертикальный, «P» - позиционный, «T» - временной, «G» - геометрический. При значениях меньше 1, данные имеют максимально возможную точность, при 2-3 точность является отличность, 4-6 – точность хорошая, 7-8 – точность средняя, 9-20 – точность ниже среднего (могут использоваться для грубого приближения), 21-50 – точность плохая, такие результаты отбрасывают.

Рассмотренные форматы представления оценок координат по спецификации NMEA являются стандартизированными и рекомендуются к использованию для создания аппаратно-программного комплекса системы интеллектуальной навигации на основе сети технологической радиосвязи.

Список используемых источников:

1. GPS-приемник GlobalSat BU-353 GLONASS. Руководство пользователя. ООО «ГлобалСат», 2018. 8 с.
2. Изменение частот и скорости обмена GPS-приемников GlobalSat ND-105C/BU-353s4, BU-353 GLONASS. Руководство. ООО «ГлобалСат», 2016. 8с.
3. Модули ГеоС. NMEA протокол обмена. Версия 3.0. М. : ООО ДЦ «ГеоСтар навигация», 2016. 30 с.
4. Протокол обмена NMEA (IEC 61162). ТДЦК.460951.002 Д11. Литера «О», 2004. 20 с.

Ushkova I., Fokin G.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Receiving a GNSS tag using a GPS/GLONASS receiving

In the present work features of the GlobalSat BU-353G GLONASS (further BU-353G) Global Navigation Satellite Systems (GNSS) signal receiver, as well as the format of nmea-type Global Navigation Satellite Systems tags are considered. A description of the BU-353G device driver is presented, and the format and contents of the accepted GNSS tag are analyzed. Finally, scenarios for the use of this tag in the development tasks of the demonstrator of network positioning technology are formulated.

Key words: BU-353G, NMEA, GPS, GLONASS, GNSS, receiver.

УДК 621.396.946
ГРНТИ 49.33.29

АНАЛИЗ СВЕРХШИРОКОПОЛОСНЫХ ИМПУЛЬСОВ

Н. И. Шайхлеева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе проводится анализ основных существующих форм сверхширокополосных импульсов. Приведены математические модели для реализации сверхширокополосных сигналов. Выявлены основные преимущества тех или иных моделей.

СШП, импульс Гаусса, импульс Релея

В конце 20 – начале 21 века во многих областях науки возник интерес к применению новых нетрадиционных видов сигналов, обладающих, по сравнению с узкополосными и широкополосными сигналами, большими возможностями. Данные возможности следуют из принципа работы сверхширокополосных (СШП) технологий, который заключается в том, что импульс кратковременен. Длительность сигнала не превышает несколько наносекунд, при это ширина спектра достигает от 3,1 – 10 ГГц [1].

Сверхширокополосными сигналами принято считать сигналы с относительной полосой $\mu \geq 0,2 \dots 0,25$. Показатель широкополосности (коэффициент широкополосности):

$$\mu = \frac{\Delta f}{f_0} = 2 \cdot \frac{f_{max} - f_{min}}{f_{max} + f_{min}} \quad (1)$$

Где:

$\Delta f = f_{max} - f_{min}$ – ширина полосы частот сигнала;

$f_0 = \frac{f_{max} - f_{min}}{2}$ – средняя (центральная) частота функции спектральной плотности мощности одномерного преобразования Фурье (ОПФ);

$f_{max} = f_0 \cdot \left(1 + \frac{\mu}{2}\right)$ – максимальная частота спектральная плотность мощности (СПМ);

$f_{min} = f_0 \cdot \left(1 - \frac{\mu}{2}\right)$ – минимальная частота СПМ;

$\tau_s = 1/\Delta f \approx 2 \cdot (\mu \cdot f_0)$ – длительность СШП сигнала.

Уровень излучения СШП-систем должен соответствовать самым жестким законодательным нормам на нежелательные излучения. Для этого необходимо, чтобы спектральная плотность мощности (СПМ) СШП систем не превышала некоторых значений, определенных ГКРЧ (рис. 1):

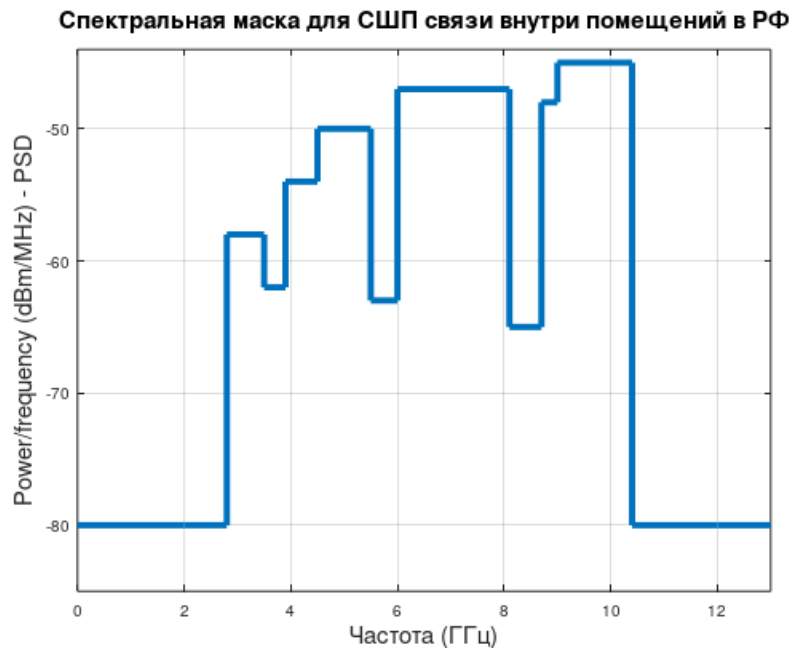


Рис. 1. Спектральная маска для СШП связи внутри помещений Российской Федерации

$$P_{UWB}(f) \leq P_{ГКРЧ}(f) \tag{2}$$

Где $P_{ГКРЧ}(f)$ – СПМ маски ГКРЧ, $P_{UWB}(f)$ – СПМ СШП импульса.

Рассмотрим импульс, основанный на производных Релея, поскольку они характеризуются непрерывностью в области существования (3), финитностью во временной области и удовлетворяют теореме Парсеваля, обеспечивающей эффективность излучения импульса.

$$\int_0^{\infty} s_{opt}(t)dt = S(f)|_{f=0} = 0 \tag{3}$$

На рис. 2 изображен СШП импульс на базе функции Релея. Коэффициенты форм импульсов подобраны так, чтобы правый и левый фронты СПМ не нарушали границ маски ГКРЧ, то есть выполнялось условие (2).

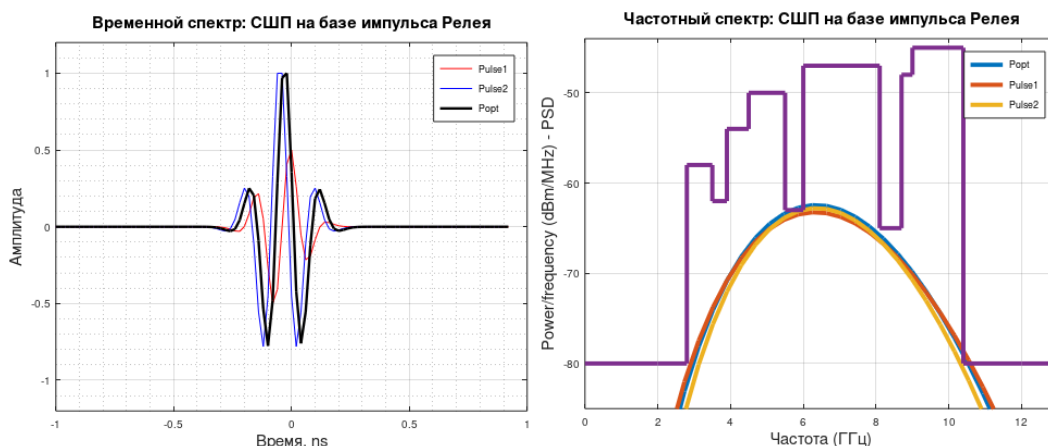


Рис. 2. Спектр СШП сигнала на основе импульса Релея

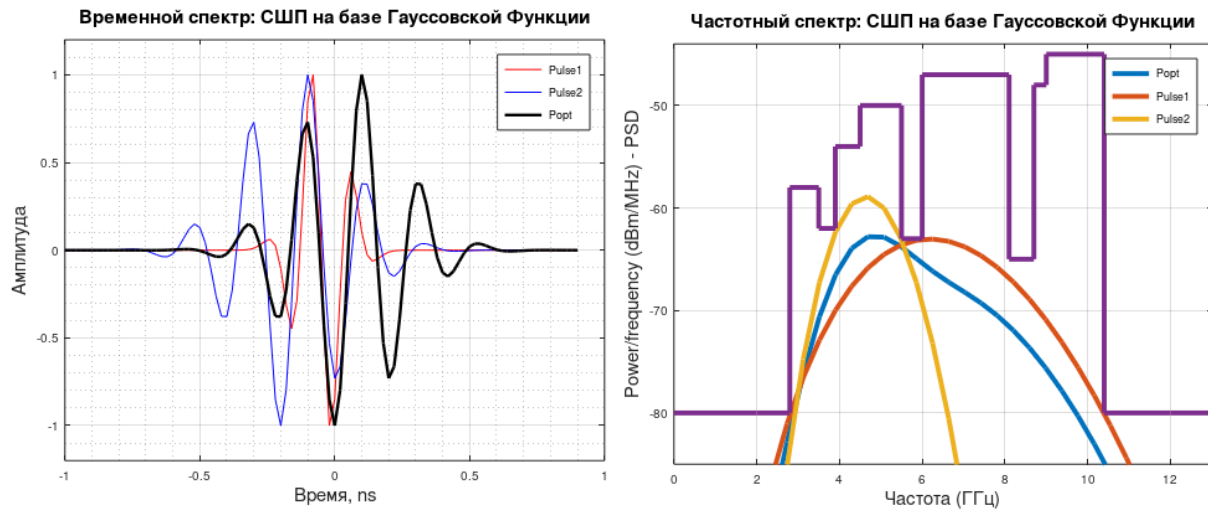


Рис. 3. Спектр СШП сигнала на основе импульса Гауссовской функции

Рассмотрим форму СШП сигнала в частотной и временной областях (рис. 3) на базе функции Гаусса.

Аналогичным образом был осуществлен подбор параметров (таблица 1), как и в случае импульса Релея. Производные импульса Гаусса характеризуются большим уровнем мощности по сравнению с первым случаем, однако их полоса рабочих частот существенно уменьшается.

ТАБЛИЦА 1. Параметры импульсов

Название	Аналитическая форма	Выполнение условия (2)	Параметры импульса
Импульс Рэля [2]	$s(t) = \frac{4 \cdot \pi \cdot t}{\sigma^2} \cdot e^{-\frac{2 \cdot \pi \cdot t^2}{\sigma^2}}$ $s_{opt}(\sigma, t) = s_1(\sigma_1, t) + s_2(\sigma_2, t)$	$s_1 = \frac{d^4 s(t)}{dt^4}$ $s_2 = \frac{d^5 s(t)}{dt^5}$ $\sigma_1 = 0,195;$ $\sigma_2 = 0,212.$	σ (ns)
Импульс Гаусса [3]	$s(t) = \frac{A}{\sigma \cdot \sqrt{2 \cdot \pi}} \cdot e^{-\frac{t^2}{2 \cdot \sigma^2}}$ $s_{opt}(\sigma, t) = w_1 \cdot s_1(\sigma_1, t) + w_2 \cdot s_2(\sigma_2, t)$	$s_1 = \frac{d^5 s(t)}{dt^5}$ $s_2 = \frac{d^{15} s(t)}{dt^{15}}$ $\sigma_1 = 0,056;$ $\sigma_2 = 0,131.$	σ (ns) w – весовой коэффициент

Рассмотренные импульсы, а также подобранные параметры позволяют максимально использовать выделенный диапазон частот. Полученные СШП импульсы могут способствовать повышению дальности канала или увеличению производительности СШП систем.

Список используемых источников:

1. Лазаренко О. В., Черногор Л. Ф. Сверхширокополосные сигналы и физические процессы //Радиофизика и радиоастрономия. – 2008. – С. 270-322.

2. Грахова, Е.П. Моделирование СШП радиоимпульсов на основе производных Гаусса и Рэлея с учетом спектральной маски ГКРЧ / Е.П. Грахова, В.Х. Багманов, И.Л. Виноградова, И.К. Мешков // Электротехнические и информационные комплексы и системы. – 2014. – т.10. №3. – с. 62-69;

3. Абдрахманова Г. И., Багманов В. Х. Сверхширокополосная система связи на основе новых моделей импульсов и антенн //Вестник Уфимского государственного авиационного технического университета. – 2013. – Т. 17. – №. 4 (57). – С. 151-158.

Shaikhleeva N.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunications

Analysis of UWB pulses.

In this paper, the analysis of the main existing forms of ultra-wideband pulses is carried out. Mathematical models for the implementation of ultra-wideband signals are presented. The main advantages of certain models are revealed.

Key words: *UWB, Gauss pulse, Rayleigh pulse.*

УДК 621.398
ГРНТИ 47.14.17

РАЗРАБОТКА КРОСПЛАТФОРМЕННОГО МИКРОВОЛНОВОГО ИОТ РАДАРА ДЛЯ INDOOR-ПОЗИЦИОНИРОВАНИЯ

И. А. Шойтов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе приведен пример разработки и реализации кроссплатформенного микроволнового IoT радара для indoor-позиционирования на базе датчика MICRADAR R60AMP1 и периферийного оборудования на базе гибридных технологий проводных и беспроводных сетей с использованием таких протоколов как Modbus, WI-Fi, Bluetooth, LoRa и ZigBee. Произведен выбор оборудования, приведены проектные решения, разработка схемы и разводка печатной платы. Показано, что реализация системы indoor-позиционирования с использованием микроволнового радара позволяет обеспечить гибкую, функциональную и не менее надежную систему, чем решение с использованием классических систем INDOOR позиционирования.

умный дом, IoT, WI-Fi, Bluetooth, LoRa, indoor-позиционирование

Система внутреннего позиционирования (англ. Indoor positioning system, IPS) – локальная система нахождения местоположения внутри зданий и закрытых сооружений, где практически недоступна спутниковая система навигации. Как любая другая система позиционирования, она состоит из набора базовых узлов (базовые станции и активной метки). Принцип работы данных систем заключается в отслеживании базовыми станциями координат меток различными методами (трилатерация, мультилатерация, триангуляция). В «классических» систем Indoor-позиционирования используются технологии инфракрасного, ультразвукового, механического и радиочастотного позиционирования.

Главной проблемой в системах Indoor-позиционирования на данный момент является необходимость использования активных меток непосредственно на отслеживаемых объектах, что существенно ограничивает возможность применения данных систем в рамках домашнего использования [1].

Одним из вариантов решения данной проблемы является использование технологии микроволнового позиционирования, отличающегося от классических систем отсутствием необходимости в применении активных меток.

Принцип действия микроволнового позиционирования заключается в работе на основе эффекта Доплера (рис. 1), в результате которого посылаемая радаром электромагнитная волна изменяет свою частоту при малейших движениях объекта (дыхании человека, сердцебиение и другое).

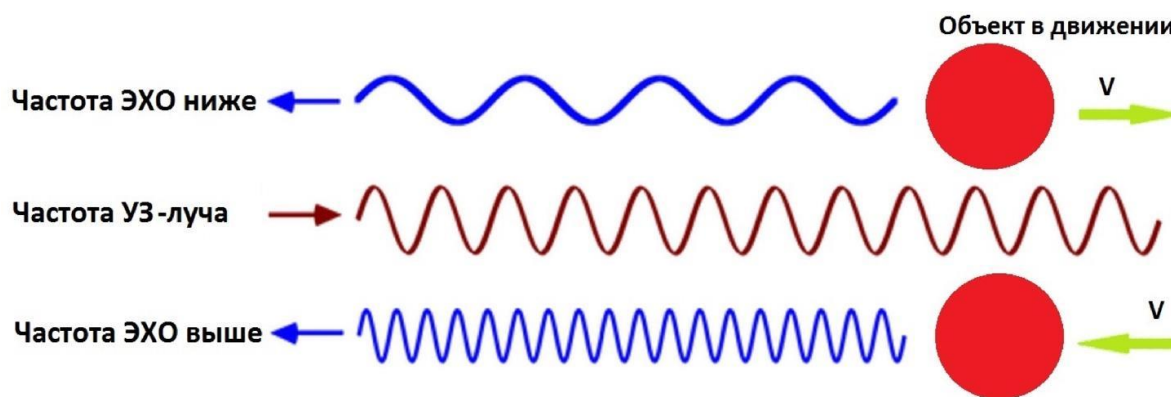


Рис. 1. Графическое представление эффекта Доплера в системе позиционирования

Для проектируемого устройства были определены следующие технические требования:

- возможность использования различных протоколов передачи данных для интеграции в системы *IOT*: *Modbus*, *WI-Fi*, *Bluetooth*, *LoRa* и *ZigBee*;
- низкое энергопотребление: до 3 Вт;
- количество отслеживаемых объектов (людей): от 5 шт;
- компактные габариты финального устройства: до 10 на 10 см;
- широкий угол зоны отслеживания объектов: от 80° по горизонтали и 80° по вертикали.

В качестве базы для разрабатываемого радара был выбран датчик *MICRADAR R60AMP1*, обладающих следующими характеристиками [2]:

- рабочая частота: 60-61,5 ГГц;
- мощность передачи: 6 дБм;
- угол раскрытия: 100° по горизонтали, 100° по вертикали;
- дальность обнаружения: 10 метров;
- максимальное количество отслеживаемых объектов: 10;
- напряжение питания: 5 В/93 мА;
- интерфейс вывода данных: *Uart*.

Для подключения радара к системам *IoT* выбраны следующие и модули:

- *ESP32-WROVER-1* (*WI-Fi*, *Bluetooth*)
- *CC2538* (*ZigBee*)
- *SX1278* (*LoRa*)
- *MAX485* (*Modbus*)

Была разработана схема подключения устройств, в соответствии с технической документацией к каждому модулю (рис. 2) [3],[4],[5].

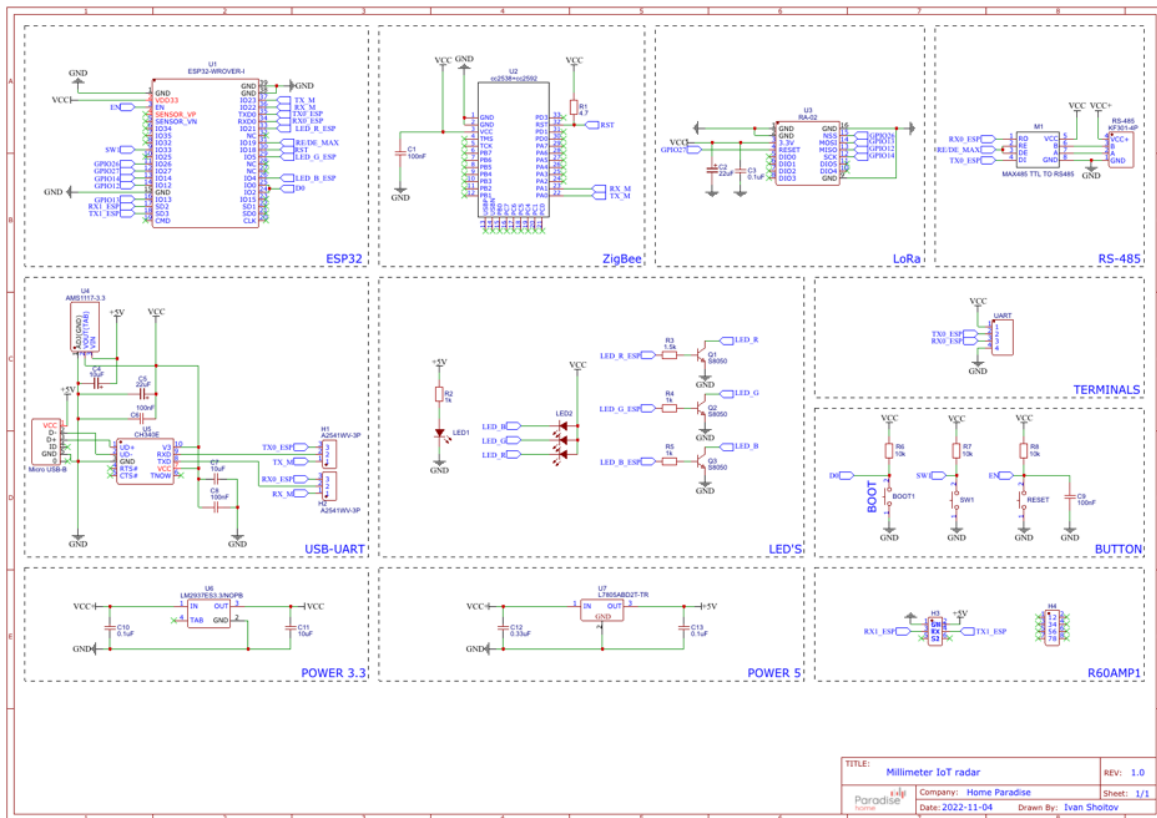


Рис. 2. Схема разрабатываемого устройства

На основе данной схемы была разведена печатная плата (представлена на рис. 3).

Плата обладает следующими особенностями:

- двухслойное строение;
- толщина стеклотекстолита: 1 мм;
- толщина токопроводящих дорожек: 18 мкм;
- размер 80 на 80 мм.

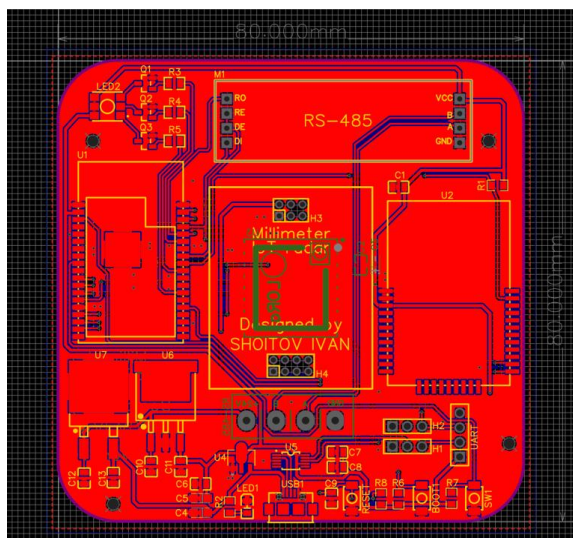


Рис. 3. Изображение разведенной платы радара

На рис. 4 представлено концептуальная трехмерная модель прототипа проектируемого устройства, разработанная на основе разведенной печатной платы. Данная модель необходима для дальнейшего проектирования корпуса устройства.

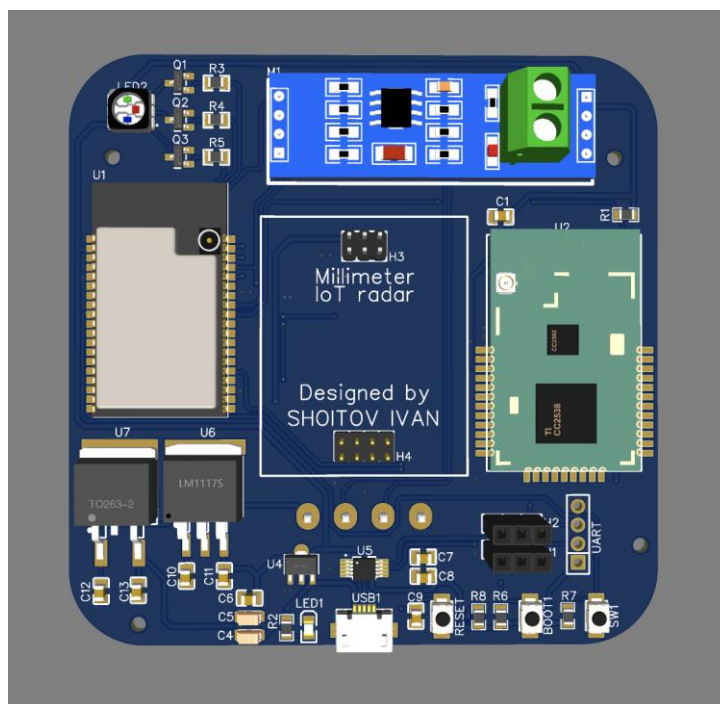


Рис. 4. Трёхмерная модель радара

В результате проделанной работы был спроектирован первый прототип разрабатываемого устройства (*Proof of Concept*), готовый к дальнейшему производству и тестированию.

Список используемых источников:

1. Indoor positioning system / [Электронный ресурс] // Wikipedia: [сайт]. — URL: https://en.wikipedia.org/wiki/Indoor_positioning_system (дата обращения: 10.11.2022).
2. MicRadar Technology (Shenzhen) Co.,LTD R60AMP1-Multi-person trajectory radar Datasheet / MicRadar Technology (Shenzhen) Co. ,LTD [Электронный ресурс] // micradar.cn:[сайт].— URL: <http://www.micradar.cn/uploads/soft/20220801/1659342110.pdf> (дата обращения: 10.11.2022).
3. Espressif Systems Copyright ESP32 Series Datasheet / Espressif Systems Copyright [Электронный ресурс] // espressif.com: [сайт]. — URL: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf (дата обращения: 10.11.2022).
4. Texas Instruments CC2538 Powerful Wireless Microcontroller System-On-Chip / Texas Instruments [Электронный ресурс] // ti.com: [сайт]. — URL: https://www.ti.com/lit/ds/symlink/cc2538.pdf?ts=1668370855224&ref_url=http%253A%252F%252Fwww.ti.com%252Fproduct%252FCC2538 (дата обращения: 10.11.2022).
5. Texas Instruments SX1278/SX1276 Wireless Module / Texas Instruments [Электронный ресурс] // ebyte.com: [сайт]. — URL: <https://www.micros.com.pl/mediaserver/info-rf%20e19-868m20s.pdf> (дата обращения: 14.11.2022)

Shoitolov I.

The Bonch-Bruевич St. Petersburg State University of Telecommunications

Development of a cross-platform microwave IOT radar for indoor positioning.

This paper provides an example of the development and implementation of a cross-platform microwave IoT radar for indoor positioning based on the MICRADAR R60AMP1 sensor and peripheral equipment based on hybrid technologies of wired and wireless networks using protocols such as Modbus, WI-Fi, Bluetooth, LoRa and ZigBee. The choice of equipment was made, design solutions were given, the development of the circuit and the wiring of the printed circuit board. It is shown that the implementation of an indoor positioning system using a microwave radar makes it possible to provide a flexible, functional and no less reliable system than a solution using classical INDOOR positioning systems.

Key words: *smart home, IoT, WI-Fi, Bluetooth, ZigBee, LoRa, indoor-positioning.*

Секция 2.3.
Проектирование и технология радиоэлектронных средств

УДК 621.396.67
ГРНТИ 47.45.29

ТЕХНОЛОГИИ МЕТАЛЛИЗАЦИИ НАПЕЧАТАННЫХ ПЛАСТИКОВЫХ ДЕТАЛЕЙ ПРИ БЫСТРОМ ПРОТОТИПИРОВАНИИ УСТРОЙСТВ СВЧ ДИАПАЗОНА

Н. П. Дунаев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

3D печать пластиком повсеместно применяется для прототипирования различных изделий сложной формы. В том числе корпусов радиоэлектронных средств, СВЧ-устройств и антенн. В устройствах СВЧ диапазона деталь из пластика может быть не только частью несущей конструкции, но и функциональным узлом, свойства которого зависят от электрических характеристик материала (диэлектрической проницаемости, тангенса угла диэлектрических потерь...). Одной из сложностей является металлизация изделий из пластика. В статье будет рассмотрено несколько подходов к решению этой задачи и приведены экспериментальные результаты применения токопроводящей краски как экрана в СВЧ-устройстве.

быстрое прототипирование, аддитивные технологии, металлизация, токопроводящие материалы, антенны, СВЧ устройства

Аддитивные технологии заняли ведущее место в прототипировании и быстрой реализации различных изделий [1-4]. Этому способствует удешевление комплектующих и расходных материалов для 3D принтеров. Изготовленные детали обладают достаточной прочностью, чтобы, в некоторых случаях, заменить оригинал из пластика или металла. У данной технологии есть и свои минусы, например, скорость производства одной детали, малое количество изготовленных деталей за одну итерацию работы станка, а также сложность металлизации изделия.

Для металлизации изделия, изготовленного с помощью аддитивных технологий, возможны два пути:

Первый способ – внедрение в филамент (пластиковая нить) металлических структур. При этом нет гарантии получения достаточной проводимости так как связующий материал – пластик, не проводит ток. Если же увеличить количество внедряемых структур возможно получение проводимости, но так как связующего компонента меньше, уменьшается и прочность.

Второй способ – покрытие готового изделия проводящим слоем. При этом способе возможно получить проводящий слой не нарушая структуру исходного изделия. В некоторых случаях необходимо покрывать не все изделие, а только необходимую часть.

Нанесение покрытий возможно с помощью различных токопроводящих красок, фольги или химическими методами. Рассмотрим два первых способа, поскольку известные реализации химических методов возможны только в условиях производства и плохо сочетаются с быстрым прототипированием.

Металлизация поверхностей с помощью медной или алюминиевой фольги с клейким основанием не требует специальных навыков и приспособлений. В

качестве примера на рис. 1 приводится волноводный трансформатор, распечатанный на 3D принтере. Покрытие фольгой осуществлялось с внутренних стенок, затем углы покрывались внахлест что бы закрыть возможные щели.

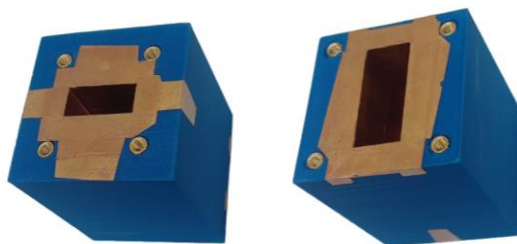


Рис. 1. Волноводный трансформатор

Следующий пример – двухгребневая широкополосная рупорная антенна. После расчета модель была разделена на простые элементы для упрощения печати, покрыта медью поэлементно и собрана как показано на рис. 2.



Рис. 2. Двухгребневая широкополосная рупорная антенна

Оба примера показывают, что полная металлизация нужна не во всех случаях, лишь для формирования необходимых граничных условий.

Другим способом покрытия проводящим слоем, как сказано выше, является токопроводящая краска. Покажем эффективность применения на примере делителя мощности.

Сравнение будет проводится с помощью замены экрана на делителе мощности. После измерения параметров делителя мощности снимем медный экран, как показано на рис. 3.

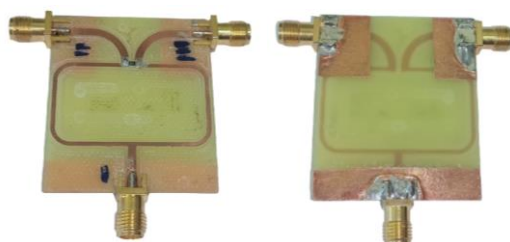


Рис. 3. Делитель мощности без экрана

Измерим параметры полученного устройства и нанесем электропроводящую краску ЗИПСИЛ 910 КЭП в один слой, как показано на рис. 4.

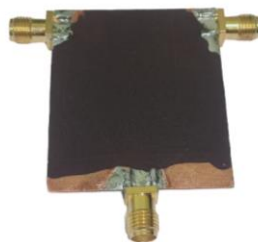


Рис. 4. Делитель мощности с экраном из электропроводящей краски

На рис. 5-8 представлены КСВН, ослабление и затухание делителя мощности с медным экраном, без экрана и экраном из электропроводящей краски.

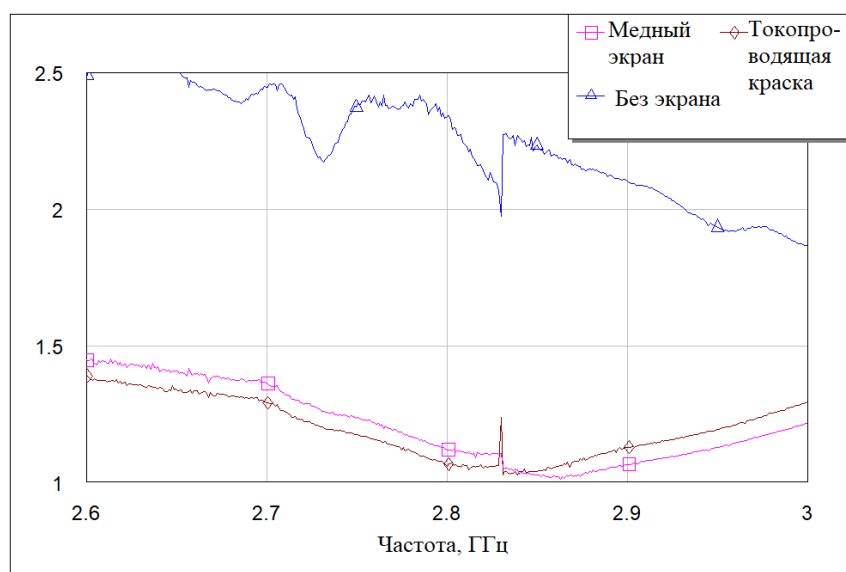


Рис. 5. КСВН делителя мощности

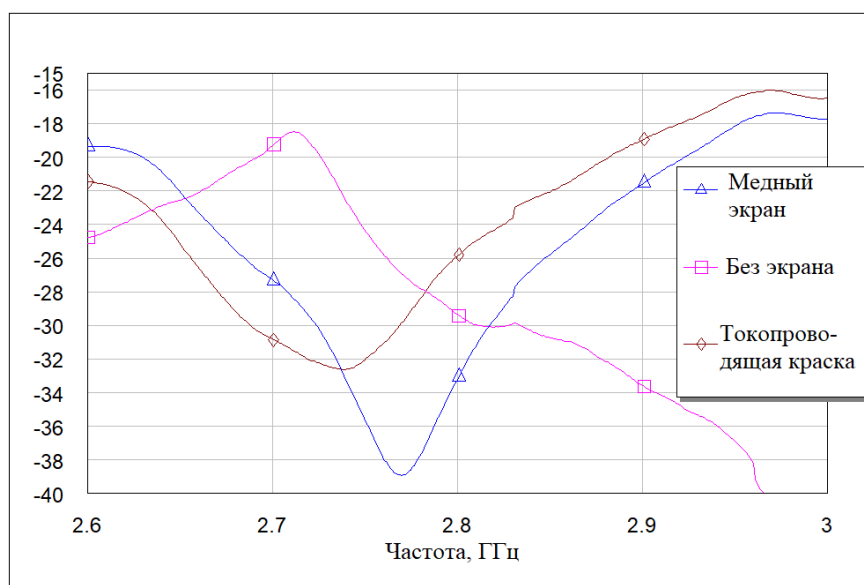


Рис. 6. Затухание делителя мощности

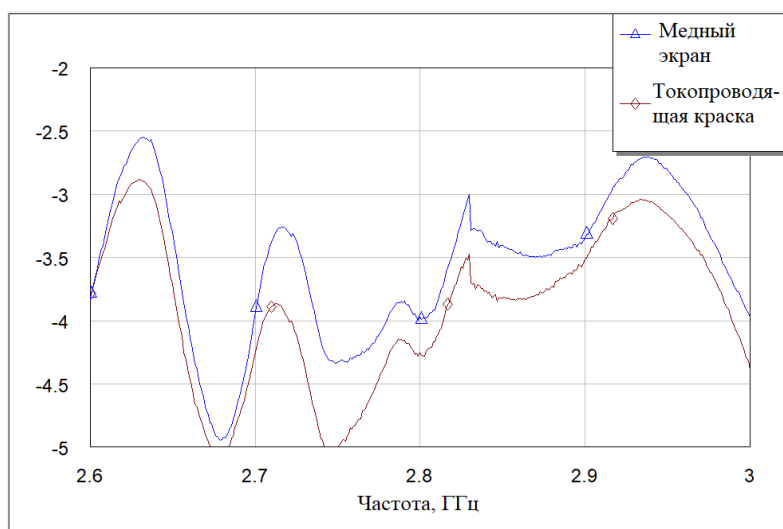


Рис. 7. Ослабление делителя мощности

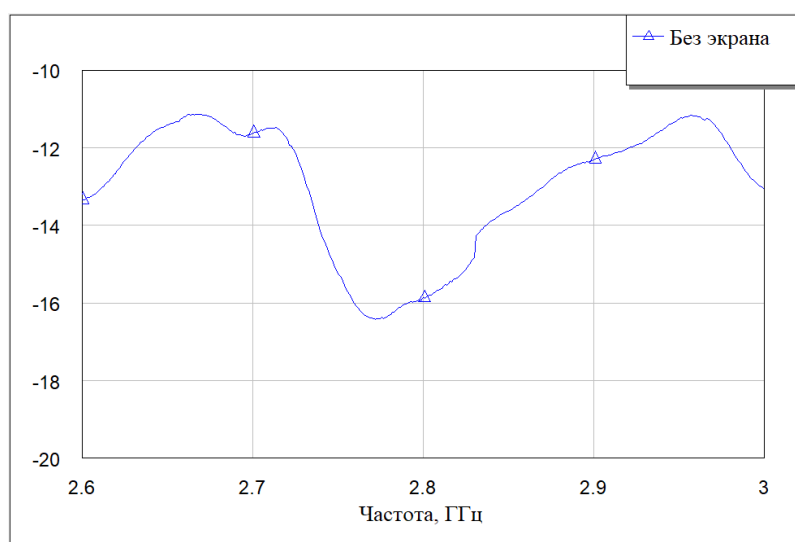


Рис. 8. Ослабление делителя мощности без экрана

Для металлизации отверстий, или реализации качественного крепежа в глухом отверстии, рекомендуется применение латунных впадных гаек [6]. Для установки требуется нагреватель (например, паяльник). Нагретая гайка вставляется в отверстие расплавляя пластик. Остывший пластик удерживает гайку за боковые насечки, при этом повышая прочность области вокруг, так как слои лучше соединяются между собой. На рис. 9 представлен тестовый образец для отработки выбора посадочных мест для гаек.



Рис. 9. Тестовый образец установки впадных гаек

Приведённые способы металлизации позволяют ускорить прототипирование устройств СВЧ диапазона. Использование

электропроводящей краски в качестве экрана может обеспечить приемлемые характеристики прототипов СВЧ-устройств.

Список используемых источников:

1. Демиденко Е.В., Кузьмин С.В., Кирик Д.И. 3D печать антенно-фидерных устройств с использованием полимерных материалов // Электроника и микроэлектроника СВЧ. 2018. Т. 1. С. 491-495.
2. Харалгин С.В., Войтович М.И. Исследование диэлектрических характеристик материалов, изготавливаемых с применением аддитивных технологий // Российский технологический журнал. 2021. Т. 9. № 2 (40). С. 57-65.
3. Балашов А.Ю., Гюльмагомедов Н.Х., Ермилов А.С. Применение 3d-печати при разработке конструкций, обладающих радиопрозрачными свойствами // Аддитивные технологии: настоящее и будущее : материалы VII Междунар. конф., Москва, 7-8 окт. 2021. М. : ВИАМ НИЦ «Курчатовский институт», 2021. С. 180-189.
4. Кузиков А.А., Орехов Р.С., Саломатов Ю.П., Сугак М.И. Исследование печатной цилиндрической линзы люнеберга // Электроника и микроэлектроника СВЧ. 2018. Т. 1. С. 426-430.
5. Куроптев П.Д., Фатеев А.В. Широкополосная рупорная антенна диапазона 0,8- 30 ГГц // Электронные средства и системы управления: материалы XI междунар. научно-практич. конф., Томск, 25-27 нояб. 2015 г. Томск : В-Спектр, 2015. 141- 146 с.
6. Вплавляемая гайка: [Электронный ресурс]. URL: https://robotparts.ru/catalog/mekhanika_i_ustanovochnye_izdeliya/krepyezh/gayki/vplavlyаемая_gayka_m3x4_2x5/ (дата обращения: 02.11.2022).

Dunaev N.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Technologies of metallization of printed plastic parts for rapid prototyping of microwave devices.

3D printing with plastic is widely used for prototyping various products of complex shape. Including buildings of radio-electronic means, microwave devices and antennas. In microwave devices, a plastic part can be not only a part of the supporting structure, but also a functional node, the properties of which depend on the electrical characteristics of the material (permittivity, loss tangent e.t.). One of the difficulties is the metallization of plastic products. The article will consider several approaches to solving this problem and provide experimental results of using conductive paint as a screen in a microwave device.

Key words: *rapid prototyping, additive manufacturing, Metallizing, conductive materials, antennas, microwave devices.*

УДК 621.396.13
ГРНТИ 47.14.17.

ИССЛЕДОВАНИЕ ПОДХОДОВ ПО КОНВЕРСИИ ИЗДЕЛИЙ ДВОЙНОГО ПРИМЕНЕНИЯ

Р. М. Есенбеков, Д. И. Кирик

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена вопросам исследования методов конверсии изделий двойного назначения. В работе приводится анализ зарубежных моделей конверсии. В работе подчеркивается важность поиска методов конверсии изделий двойного назначения для телекоммуникационного оборудования для повышения безопасности важнейших элементов критической информационной инфраструктуры страны, а также выполнения задачи импортозамещения на отечественном рынке телекоммуникационного оборудования.

изделия двойного назначения, телекоммуникационное оборудование, информационная безопасность, импортозамещение

Оборонно-промышленный комплекс (ОПК) любой промышленно развитой страны базируется на современных технологиях, поэтому чрезвычайно важен вопрос использования двойных технологий [4], т.е. применимых в производстве продукции как военного, так и гражданского назначения. Хотя производство вооружений, военной и специальной техники является важнейшим общественным благом, обеспечивающим безопасность страны, производимая военная продукция не используется в дальнейшем ни в процессе потребления домашних хозяйств, ни в качестве средств производства предприятиями. Вкладывая инвестиции в их производство, мы «замораживаем» часть доступных экономике страны ресурсов, и нагрузка военных расходов на бюджет может стать излишне большой – как это имело место в позднем СССР. Использование двойных технологий позволяет найти коммерческое применение военным разработкам и за счет прибыли от применения технологии в производстве гражданской продукции снизить военную нагрузку на бюджет.

В современном мире потребность в скорейшем обмене информацией важна как никогда. Для успешной работы предприятию необходимы сети передачи информации. Гарантом их качественной бесперебойной работы является телекоммуникационное оборудование, которое используется для передачи аудио и видеосигнала или другой информации, а также для установления связи между различными типами устройств.

Разнообразное профессиональное оборудование, как: телекоммуникационное оборудование, IT-оборудование; центры обработки данных; промышленные компьютеры; оборудование промышленной автоматизации; оборудование систем оповещения; профессиональное видеооборудование и оборудование систем видеонаблюдения; профессиональное управляющее оборудование, требует качественной и бесперебойной связи.

Безопасность важнейших элементов критической информационной инфраструктуры Российской Федерации должна обеспечиваться за счет разработки и внедрения компонентной базы и изделий электроники российского производства с последующим импортозамещением. Особенно значимыми направлениями для импортозамещения являются телекоммуникационное оборудование, вычислительная техника, системы автоматизированного и интеллектуального управления [1].

Сегодня, на рынке представлено множество различного телекоммуникационного оборудования. Практически к любому техническому средству (ТС) можно подобрать аналог со схожими техническими характеристиками. В условиях сильной конкуренции, даже минимальное преимущество имеет значение. Поставленная задача исследования методов конверсии изделий двойного назначения с учётом мирового опыта, с последующим выпуском телекоммуникационной продукции, не уступающей по техническим характеристикам импортным аналогам, отвечает потребностям страны. Кроме улучшения потребительских качеств телеком оборудования важным является вопрос уменьшения себестоимости изделий, а также временных затрат на его разработку.

Отечественный опыт.

Холдинг «Росэлектроника» вывел на рынок станции тропосферной связи «Гроза» [3]. Технология 50-х годов прошлого века, активно используемая в «оборонке», получила новую жизнь на гражданском рынке. Станции тропосферной связи позволяют организовать мобильную связь и доступ в Интернет со скоростью до 25 Мбит/с на расстоянии до 210 км, в зонах, где отсутствует покрытие спутниковой связи, размещение радиорелейной связи или оптического волокна затруднительно и дорого.

Кроме того, тропосферная связь имеет высокую экономическую эффективность по сравнению со спутниковой связью за счет отсутствия расходов на абонентскую плату за аренду спутникового ресурса. Станция тропосферной связи будет стоить дороже, чем терминал спутниковой связи, однако за 1–2 года эксплуатации инвестиции в приобретение аппаратуры окупятся, поскольку пользователь не платит за аренду спутникового канала и не несет никаких других дополнительных расходов.

Для изучения подходов по конверсии изделий двойного назначения был проведен сравнительный анализ подобных решений иностранных производителей.

Зарубежный опыт.

Стратегия правовой инфраструктуры процессов передачи в гражданский сектор двойных технологий в США базируется на следующих принципах:

- Поощрение конкуренции и свободы предпринимательства;
- Защита интересов национальной безопасности США в процессе передачи технологий;
- Охрана авторских прав и интеллектуальной собственности.

При этом государство не имеет правовых механизмов регулирования передачи двойных технологий, разработанных фирмами самостоятельно. Для активизации этого процесса оно использует различные меры экономического стимулирования.

Важным шагом в развитии технологической политики явилось выдвижение специальной Национальной технологической инициативы, главная цель которой состояла в стимулировании использования новейших технологий американской промышленностью для укрепления национальной экономики и повышения ее конкурентоспособности на мировом рынке. Задачами этой инициативы были следующие: увеличение масштабов использования новых технологий, разработанных как в государственном, так и в частном секторе; создание большего числа высокооплачиваемых рабочих мест; установление новых контактов и кооперационных связей по разработке и внедрению перспективных технологий в гражданском секторе.

Национальный центр передачи технологий.

В рамках НАСА в 1989 г. был создан Национальный центр передачи технологий [2]. В рамках программы передачи технологий ежегодно выделяется около 1600 новых технологий самого различного применения.

Многие из них нашли своё место в современной мире:

– Камеры телефонов: цифровые камеры всех смартфонов восходят к сенсору, разработанному в 1965 году инженером НАСА Ю. Лэлли. Его изобретение позволило конвертировать фотоны в электроны, чтобы делать снимки. Изначально технология применялась на спутниках, а затем лицензия на нее была предоставлена производителям мобильных телефонов.

– Солнцезащитные очки: стекло, рассеивающее ультрафиолет, было разработано, чтобы защитить сотрудников НАСА от вспышек, лазерного и сварочного излучения на Земле и в космосе

– Аппарат ИВЛ: когда разразилась пандемия COVID-19, инженеры из Лаборатории реактивного движения НАСА разработали локально доступную технологию искусственной вентиляции легких (VITAL). НАСА бесплатно передало лицензию на эту технологию 36 компаниям.

Таким образом, роль государства в ускорении процесса трансфера технологий может состоять в следующем:

- Сокращение до разумного предела сроков секретности технологий;
- Создание нормативной базы с целью взаимовыгодной для всех сторон реализации этого процесса;
- Поддержка государства как собственника разработчиков технологий (государственных учреждений) и потенциальных их покупателей (госкорпораций ОПК);
- Формирование структур, аналогичных американскому Национальному центру передачи технологий.

Список используемых источников:

1. Распоряжение Правительства РФ от 17.01.2020 № 20-п "Об утверждении Стратегии развития электронной промышленности Российской Федерации на период до 2030 года" [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_343384/ (дата обращения: 02.11.2022).
2. Передача технологий НАСА: с небес на землю [Электронный ресурс]. – URL: https://www.wipo.int/wipo_magazine/ru/2022/02/article_0005.html (дата обращения: 04.11.2022).
3. Система тропосферной связи Гроза [Электронный ресурс]. – URL: <https://katalog-rek.ru/catalog/99/1729/> (дата обращения: 03.11.2022).
4. Товары двойного назначения [Электронный ресурс]. – URL: <https://minprom.ru/uslugi/eksportnyj-kontrol-i-tovary-dvojnogo-naznacheniya/tovary-dvojnogo-naznacheniya/> (дата обращения: 02.11.2022).

Esenbekov R., Kirik D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Study of approaches to the conversion of dual-use products.

The work is devoted to the research of methods for the conversion of dual-use products. The paper provides an analysis of foreign conversion models. The paper emphasizes the importance of finding methods for the conversion of dual-use products for telecommunications equipment to improve the security of the most important elements of the country's critical information infrastructure, as well as to fulfill the task of import substitution in the domestic market of telecommunications equipment.

Key words: dual-use products, telecommunications equipment, information security, import substitution.

УДК 620.162.2
ГРНТИ 55.24.29

ИССЛЕДОВАНИЕ ЗАВИСИМОСТИ ПРОЧНОСТНЫХ ХАРАКТЕРИСТИК ИЗДЕЛИЯ ОТ ПАРАМЕТРОВ 3D-ПЕЧАТИ И ИСПОЛЬЗУЕМОГО МАТЕРИАЛА

А. С. Литвинов¹, С. В. Балабанов²

¹Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

²ФГБУН Ордена Трудового Красного Знамени Институт химии силикатов им. И. В.Гребенщикова РАН

Для производства деталей различного назначения могут применяться различные технологии, в том числе – 3D-печать методом послойного наплавления пластика. Детали, производимые таким способом, имеют свои достоинства и недостатки; открытым остаётся вопрос прочности готового изделия. Она зависит от множества настроек, которые можно изменять перед отправкой на печать.

3D-печать, прочность изделий из пластика, PET-G пластик, производство

В настоящее время в связи с обстановкой в мире во многих отраслях производства наблюдается проблема с поставкой запасных частей для оборудования и не только. В ситуации, когда поставка оригинальных деталей невозможна или занимает слишком длительный срок, например, поставка какого-либо кронштейна, критически необходимого для работы МРТ-аппарата, необходимо иметь возможность изготовить деталь самостоятельно. Зачастую, к деталям выставляются дополнительные требования, например: работа в сложных климатических условиях (с большой амплитудой температур, с низкими / высокими температурными минимумами и максимумами), работа в средах с сильными магнитными полями и прочее [1].

Все особенности необходимо учитывать при разработке и производстве деталей. В настоящее время широкое распространение получила технология послойного наплавления пластика - *Fused Deposition Modeling* или *FDM*-печать. Она подразумевает подачу определённого количества пластика с помощью блока, называемого экструдером и последующий нагрев в специальном блоке (хотэнде), что приводит к выталкиванию материала на поверхность стола печати (*hot-bed* или *bed*) – рис. 1. Пластик выдавливается в выставленных пользователем в программе (слайсере) координатах. Постепенно, слой за слоем, деталь «растёт» в высоту. Для уменьшения количества затраченного пластика внутренняя часть модели заполняется пластиком не полностью, а частично – согласно выбранному пользователем рисунку заполнения и плотности, где плотность 0% означает наличие полости, а 100% - полное её заполнение пластиком [2, 3].

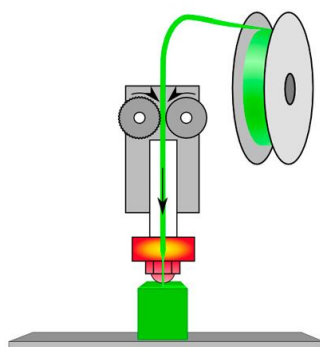


Рис. 1. Схема работы блока подачи пластика 3D-принтера технологии *FDM*

Целями работы поставлено исследование зависимости прочностных характеристик от различных факторов (тип материала, плотность внутреннего заполнения, направление укладки слоёв), а также представление графиков зависимости прочности от изменяющегося параметра. С целью сделать результат исследования более точным, предполагаем, что необходимые для корректной печати параметры, а именно температура сопла и нагревающего стола, поток, скорость работы вентилятора обдува были откалиброваны, а также «шаблон» заполнения и количество стенок не менялись («сетка» и 3 соответственно).

Задачами работы ставятся:

- Выбор оптимального для исследования тела, которое в полной мере сможет показать зависимость прочности объекта, на который влияет один определённый вид деформации – изгиб;
- Моделирование полученного тела с использованием САПР и последующее изготовление моделей на 3D-принтере, использующем технологию *FDM*;
- Проведение эксперимента над полученным телом с использованием специального оборудования;
- Построение графиков зависимости и анализ результатов.

Для исследования был выбран один из наиболее доступных на рынке пластиков для *FDM*-печати материал – *PET-G*-пластик компании *Bestfilament* (Производство: Россия) – модифицированный PET-пластик, экологически чист, имеет средние температуры плавления и частично упругую деформацию, подогрев стола при печати обязателен (40 – 80 °С), имеет отличную спекаемость по слоям).

Моделирование тела для экспериментов проводилось в отечественной САПР Компас-3D ввиду её простоты и наличия бесплатной версии для студентов технических вузов. Результат проектирования можно увидеть на рис. 2 и рис. 3.

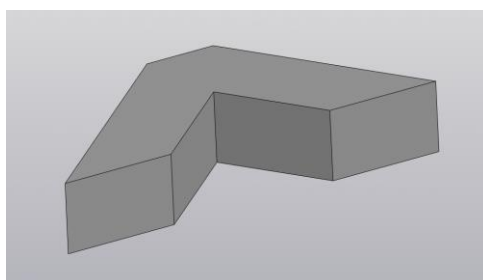


Рис. 2. Тестовая модель

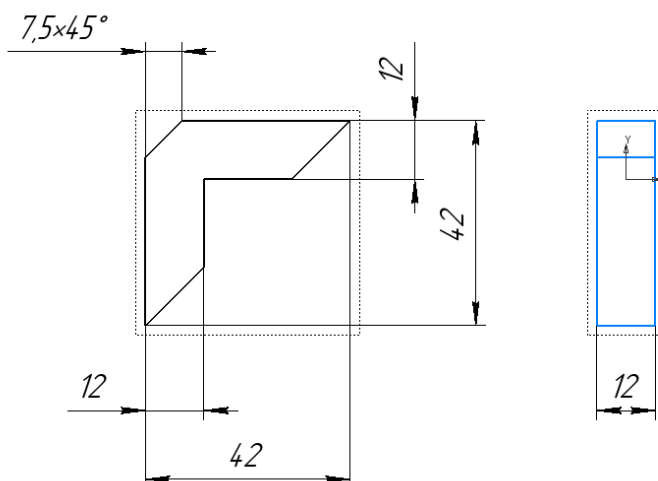


Рис. 3. Чертёж тестовой модели

Импорт файла из программы необходимо делать в электронном формате, который способен прочесть слайсер (специальная программа, выполняющая «нарезку» 3D-модели на слои в формат *G-Code*, понятный 3D-принтеру). В этом исследовании в качестве слайсера применяется *Ultimaker Cura* версии 5.1 ввиду наличия бесплатной версии без ограничения возможностей, хорошему пользовательскому интерфейсу и простоте освоения новичкам 3D-печати. Произведена печать 27 тестовых моделей, отличающихся направлением слоёв (параллельно основанию, перпендикулярно и под наклоном 45°) и плотностью заполнения (20...100% с шагом 10%). Деталь после нарезки в слайсере изображена на рис. 4.

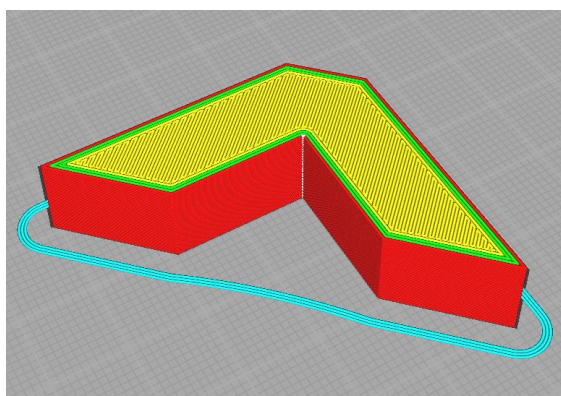


Рис. 4. Тестовая модель после нарезки на слои

При проведении экспериментов использовалась Испытательная машина фирмы "Метротест" РЭМ-50-1-1, измеряющая нагрузку (в кН), время (в с) и деформацию (в мм). Каждая деталь прошла тест, изображённый на рис. 5, результатом которого является массив данных, требующих обработки. После её проведения, по каждому измерению можно построить график, подобный изображённому на рис. 6.



Рис. 5. Проведение эксперимента

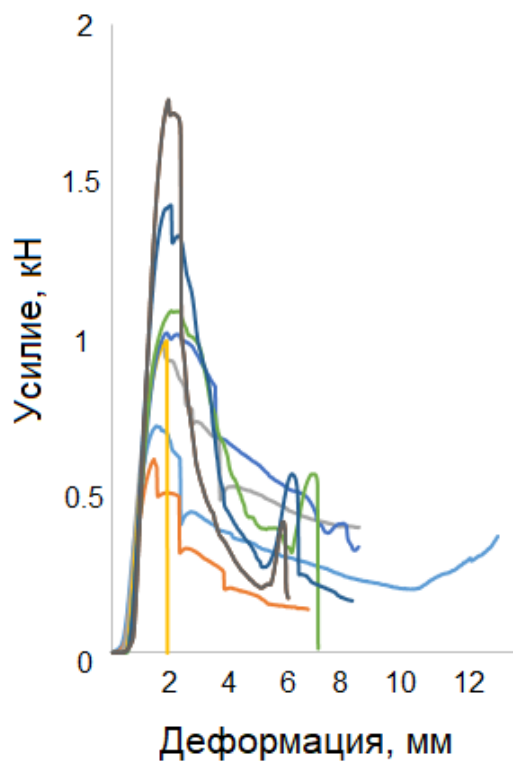


Рис. 6. Графики зависимости деформации (мм) от прикладываемого усилия (%) при горизонтальном направлении слоёв

Графики зависимости прочности детали в зависимости от плотности заполнения и направления слоёв представлены на рис. 7.

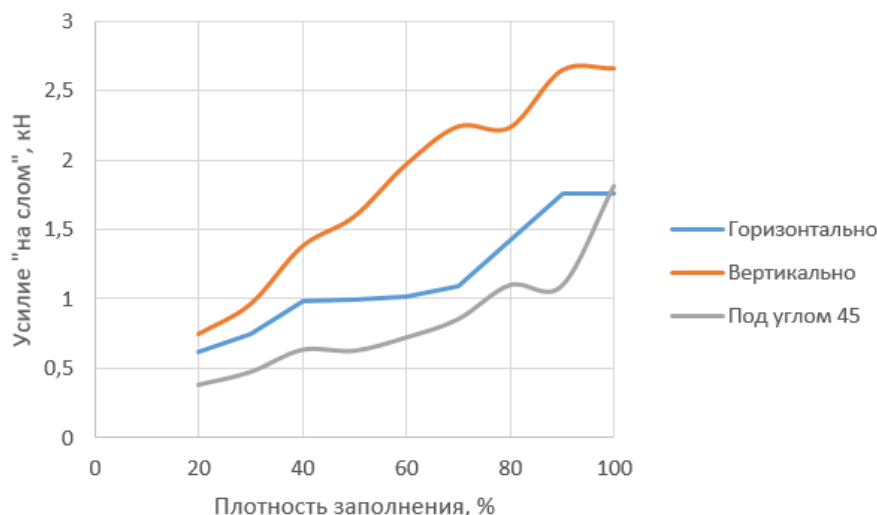


Рис. 7. Зависимость усилия «на слом» (кН) от плотности заполнения (%) при различных направлениях слоёв

Исходя из графиков, можно сделать вывод, что зависимость прочности от плотности заполнения близка к линейной. Также, направление укладки слоёв заметно влияет на необходимое для повреждения усилие; деталь, слои которой направлены параллельно вектору прикладываемого усилия, прочнее остальных в 1.6 раза.

Работа выполнена при финансовой поддержке гранта РФФИ (проект № 20-73-10171).

Список используемых источников:

1. Шкуро А. Е., Кривоногов П.С. Технологии и материалы 3D-печати: учеб. пособие. Екатеринбург: Уральский гос. лесотехн. ун-т, 2017.
2. ГОСТ ISO 7743-2013 Резина или термоэластопласты. Определение упругопрочностных свойств при сжатии. Введ. 2015-01-01 М. 2016. 27 с.
3. Гибсон Я., Розен Д., Стакер Б. Технологии аддитивного производства. М.: ТЕХНОСФЕРА, 2016. 656 с.

Litvinov A., Balabanov S.

*The Bonch-Bruевич Saint-Petersburg State University of Telecommunication
Institute of Silicate Chemistry, Russian Academy of Sciences (ISC RAS)*

Investigation of the dependence of the strength characteristics of the product on the parameters of 3D-printing and the material type.

Various technologies can be used for the production of parts for various purposes, including 3D printing by layer-by-layer deposition of plastic. The parts produced in this way have their advantages and disadvantages; the question of the strength of the finished product remains open. It depends on a lot of settings that can be changed before being sent to print.

Key words: 3D printing, durability of plastic products, PET-G plastic, manufacturing.

УДК 621.382.232
ГРНТИ 29.19.31

СОВРЕМЕННОЕ СОСТОЯНИЕ ФУНКЦИОНИРОВАНИЯ И РАЗВИТИЯ СВЕТОДИОДНОЙ ТЕХНИКИ, КОНСТРУКТОРСКО- ТЕХНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ПОВЫШЕНИЯ КАЧЕСТВА

Е. А. Махалов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Тенденция роста использования и развития искусственных источников света увеличивается. Лидерами на рынке в настоящее время считаются светодиодные светильники. Несмотря на их популярность, эффективность и удобство, проявляются проблемы, уменьшающие срок использования светодиодных источников света. Для решения этой задачи можно предложить ряд решений, связанных с регулировкой электрической цепи, а также конструкцией и материалами самого светодиода.

LED, светоизлучающие диоды, полупроводники, светотехника

Использование светодиодного освещения в мире неуклонно растет. Согласно отчету организации «Лайтинг Бизнес Консалтинг», рынок профессиональных светильников в 2019 году показал прирост в +11,9% в количественном выражении, достигнув уровня более 71,3 млн. шт., и +12,3% в стоимостном, составив 63,9 млрд. руб. [1]. На рис. 1 показано изменение оценки рынка с 2017 по 2019 год.

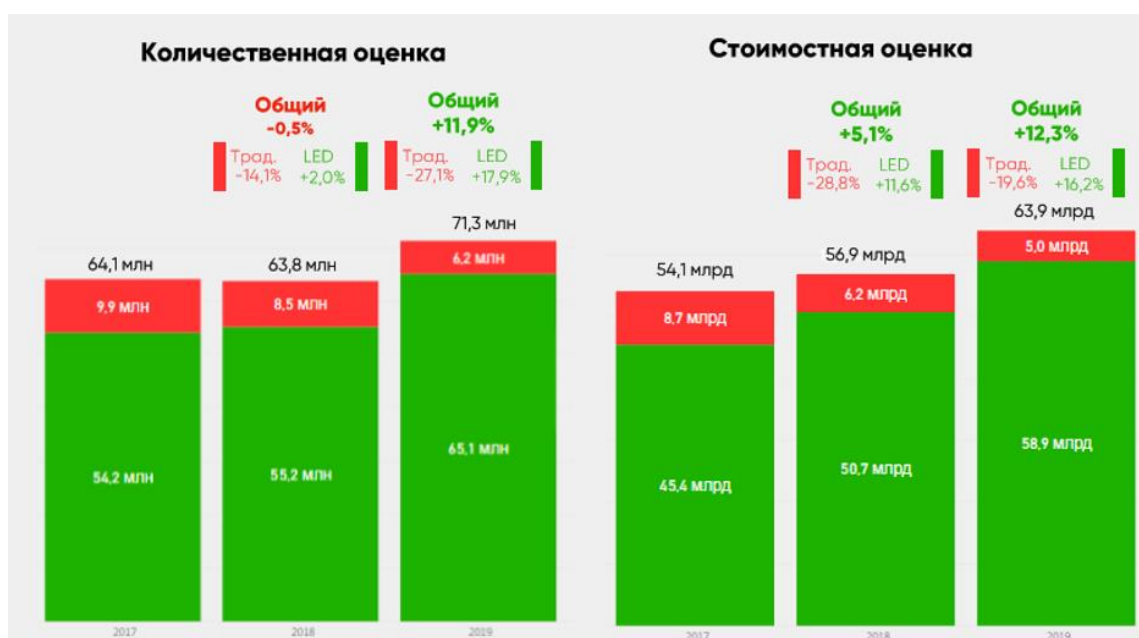


Рис. 1. Изменение оценки рынка с 2017 по 2019 год

Динамика средней цены светильника светодиодного или традиционного отображена на рис. 2 [1]. Исходя из этого, можно заметить, что в 2016 году разница цен составляла 555 руб., что составляет 86% цены традиционного

светильника, когда в 2017 цена светодиодного стала меньше традиционного. В 2018 цена светодиодного светильника хоть и осталась больше традиционного, но разница цен составила 27%.



Рис. 2. Динамика средней цены светодиодного и традиционного светильника

При этом, согласно отчету за 2020 год от ассоциации «Честная позиция» под проектом «Соответствие в светотехнике», из 42 протестированных моделей светильников только 10 (~25%) соответствуют всем требованиям и стандартам [2]. На рынке наблюдается тенденция одновременного снижения цены и снижение качества светодиодных светильников.

Светодиодные светильники представляют собой последовательно соединенные светоизлучающие диоды (светодиоды) на печатной плате, размещенной в едином корпусе. Корпус является несущей конструкцией для платы со светодиодами, который, как правило, является радиатором для изделия. Для питания прибора используются блоки питания (драйверы). Они могут идти отдельно от светильника, а могут быть интегрированы в конструкцию лампы.

Так как светодиоды подключаются последовательно, выход из строя хотя бы одного светодиода будет означать выход из строя всего светодиодного светильника.

Неисправности светодиодов принято делить на три основных группы:

1. Неисправности, связанные с повреждением кристалла. В ходе нормальной эксплуатации световой выход светодиодов постепенно снижается на протяжении всего срока их службы. КПД снижается за счёт роста числа дефектов. При этом кристалл продолжает потреблять электроэнергию, выделение тепла увеличивается, а светоотдача снижается. Это приводит к ограничению срока службы светодиодов и к необходимости учёта времени наработки;

2. Неисправности, вызванные повреждением токоподводящих цепей. Изменения в токовой цепи могут приводить к увеличению электрического сопротивления. Наиболее частая причина разрушений, которая вызывает снижение интенсивности светового излучения, приводит к временной нестабильности свечения или полному отказу;

3. Неисправности, вызванные повреждением корпуса. Существуют две основные причины неисправностей корпуса, это заводской брак и нарушение техпроцесса монтажа светодиодов в конечное изделие [3].

Все перечисленные неисправности приводят к основной проблеме и причине выхода из строя светодиодов. Основная причина снижения ресурса светодиодов – превышение рабочей температуры кристалла [3].

Ведутся разработки в области синтеза светоизлучающих слоев на светоизлучающем диоде. Например, при изготовлении коаксиального полуполярного светоизлучающего диода с матрицей InGaN / GaN на канавках добились существенных результатов уменьшения снижения эффективности. Результаты показывают, что синтезированная матрица имеет две полуполярные плоскости с увеличенным качеством кристаллов. Коэффициент снижения эффективности составил около 9,7% при увеличении вводимого тока с 3 до 100 А / см², что в значительной степени снижает на 47% по сравнению с обычными светодиодами [4]. На рис. 3 изображена схема синтеза.

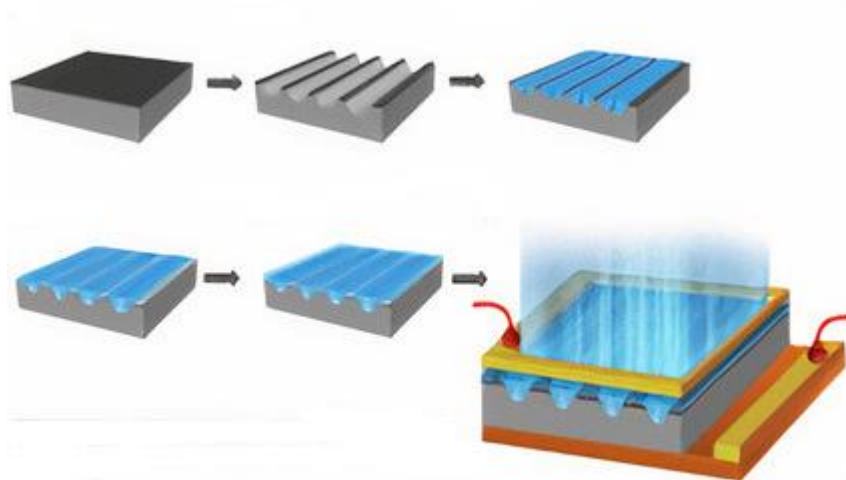


Рис. 3. Схема синтеза матрицы на InGaN / GaN на канавках

Для увеличения срока службы светодиода и, соответственно, светодиодного светильника, можно использовать ряд технических решений:

1. Увеличение теплоотдачи с лампы во внешнюю среду посредством внедрения новейших форм и материалов радиаторов. Постоянно поддерживаемая оптимальная температура светоизлучающих полупроводниковых слоев является основополагающим в ресурсе работы лампы;

2. Внедрение новых схем, компонентов элементной базы и фильтров питания. Также существует возможность внедрения робастных систем, связывающей условия работы светильника с его световыми характеристиками. Предлагаемые учеными решения для проектирования робастных систем управления представлены такими основными направлениями – применение регуляторов, которые обеспечивают требуемый запас устойчивости системы, использование различных алгоритмов систем слежения [5];

3. Смена материалов в конструкции светодиода (подложка, корпус, люминофор, отражатель, линза и т.д.).

В заключение можно сделать вывод о том, что развитие светодиодного освещения в настоящее время имеет экономическое обоснование. Развитие можно проводить в направлениях целой конструкции светодиодных светильников, их частей, электрических схем и непосредственно модернизировать конструкцию светодиода, схему наращивания и состав светоизлучающих слоев.

Список используемых источников:

1. Рост рынка профессиональных светильников в 2019 г. [Электронный ресурс] // URL: <https://www.lbconsulting.ru/lighting-market/lighting/2020/rost-rynka-professionalnykh-svetilnikov-v-2019-g/> (дата обращения 14.11.2022).
2. Отчет по мониторингу 2020 [Электронный ресурс] // URL: https://www.fairp.ru/_files/ugd/825a4d_4e9feab43abf436393c0c60c26405a93.pdf (дата обращения 14.11.2022).
3. Косарев В.А. Анализ неисправностей и методов контроля светодиодов // Электротехника : Вестник УлГТУ 1/2020, Ульяновск, 16 нояб., 2020 С. 30–35.
4. Xingjun Luo, Weidong Song, Hu Wanga, Yiming Sun, Bolin Zhang, Linyuan Wang, Jiaqi Guo, Longfei He, Kang Zhang, Shuti Li Coaxial semipolar InGaN/GaN microwire array LED with substantially suppressed efficiency droop [Электронный ресурс] // URL: <https://www.sciencedirect.com/science/article/abs/pii/S0022231319306258> (дата обращения 15.11.2022).
5. Григорьева С. В. Оптимизация светодиодных систем освещения с элементами робастного управления : доктор философии (PhD) : Усть-Камнегорск, 2017. 136 с.

Mahalov E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Current state of functioning and development of LED technology, design and technological problems of quality improvement.

The growth trend in the use and development of artificial light sources is increasing. LED lamps are currently considered the market leaders. Despite their popularity, efficiency and convenience, there are problems that reduce the lifespan of LED light sources. To solve this problem, a number of solutions can be proposed related to the regulation of the electrical circuit, as well as the design and materials of the LED itself.

Key words: LED, light emitting diodes, semiconductors, lighting engineering.

УДК 62–791.2
ГРНТИ 47.14.17

ПРОЕКТИРОВАНИЕ ПЛАТЫ УПРАВЛЕНИЯ УСТРОЙСТВА КЛИМАТИЧЕСКОГО КОНТРОЛЯ С ПЕРЕДАЧЕЙ ДАННЫХ

Д. А. Поленова, В. Н. Мордовин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Каждый человек имеет право на благоприятную окружающую среду и достоверную информацию о ее состоянии. Настоящая статья посвящена вопросам разработки платы управления устройства климатического контроля с передачей данных. На основе проанализированных существующих климатических систем были разработаны технические требования и электрические схемы. В статье представлена 3D модель платы управления устройства климатического контроля с GSM-модулем, спроектированная в САПР Altium Designer.

климатическая система, проектирование, трассировка, GSM-модуль, передача данных, двусторонняя печатная плата.

Климатическая система – это система, которая обеспечивает поддержание необходимого климата или его контроль.

Для успешного проектирования печатной платы управления устройства климатического контроля с передачей данных необходимо выполнить следующие задачи:

- провести анализ существующих видов устройств климатического контроля и их функционирования;
- осуществить проектирование и моделирование платы управления;

Существующие виды климатических систем (КС) имеют схожую структуру и включают в свой состав различные датчики, микроконтроллер, жидкокристаллический дисплей. Типовая структурная схема представлена на рис. 1.



Рис. 1. Типовая структурная схема КС

Для анализа были выбраны КС китайского и отечественного производства с различным функционалом. Сравнительные характеристики рассмотренных климатических систем представлены в таблице 1.

ТАБЛИЦА 1. Сравнительная характеристика климатических систем

Критерий	Xiaomi MiJia	MagicAir	Alonio T2
Питание	автономное, CR2032	5 В, 1 А кабель питания USB-A, блок питания для подключения к сети 230 В	от сети 220
Датчики	температуры, влажности	температуры, влажности, углекислого газа,	температуры
Диапазон измеряемых параметров	от 0 до 60 °С от 0 до 100 %	от –10 до 85 °С от 0 до 95 % от 0 до 5000 ppm	от –10 до 50°С
Точность	±0,3°С, ±3%	±1,5°С, ±4%, ±50 ppm + 5%	±1,5°С
Оповещение	—	облачный сервер, приложение	SMS/MMS
Связь	—	по РК RF на частоте 868 МГц или по технологии, совместимой с Bluetooth 4.2; с роутером по Wi-Fi IEEE 802.11b/g/n (2,4 ГГц) для доступа к облачному серверу через интернет	сотовая GSM
Доп. функции	—	облачный сервер, приложение, управление ИУ	оповещение пользователя
Страна	Китай	Россия	Россия
Стоимость, руб	1490-2170	18490	6799

Главным преимуществом системы MagicAir является мониторинг параметров через приложение и дистанционное управление исполнительными устройствами, но без приобретения специальных приборов эта функция бесполезна, предпочтительнее в этом случае приобрести Alonio T2. Однако данная система не позволяет отслеживать параметры пользователю на постоянной основе, как на дисплее (по причине его отсутствия), так и дистанционно (только по запросу), при этом Alonio T2 имеет только датчик температуры.

Анализ существующих систем выявил, что необходима разработка устройства климатического контроля с GSM-модулем, и позволил составить основные технические требования для разработки КС [1]:

- устройство должно быть выполнено на базе микроконтроллера;
- устройство должно иметь минимум 3 датчика: атмосферного давления, влажности и температуры;
- устройство должно иметь GSM-модуль, позволяющий отправлять пользователю данные об измеряемых климатических параметрах через СМС;
- для удобства эксплуатации все электрорадиоэлементы (ЭРЭ) и компоненты должны устанавливаться непосредственно на плату.

По техническим требованиям была разработана структурная схема (рис. 2). Микроконтроллер является центром системы, который связывает между собой все основные функциональные блоки.

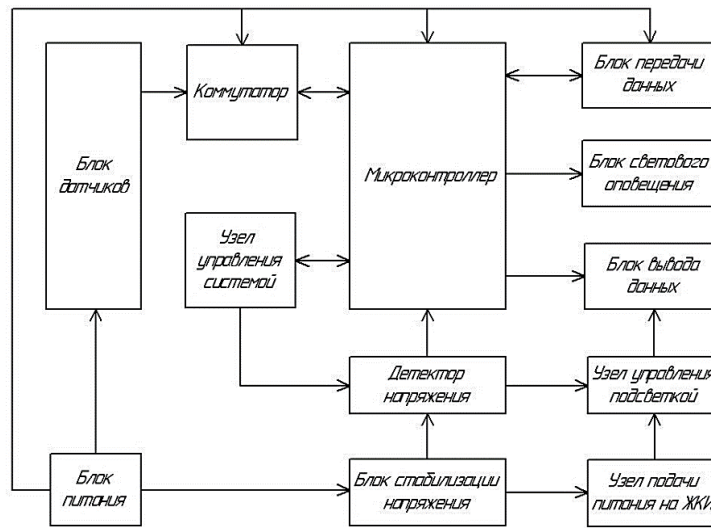


Рис. 2. Схема структурная КС

Затем была разработана функциональная и принципиальная схема [2]. Принципиальная схема представлена на рис. 3.

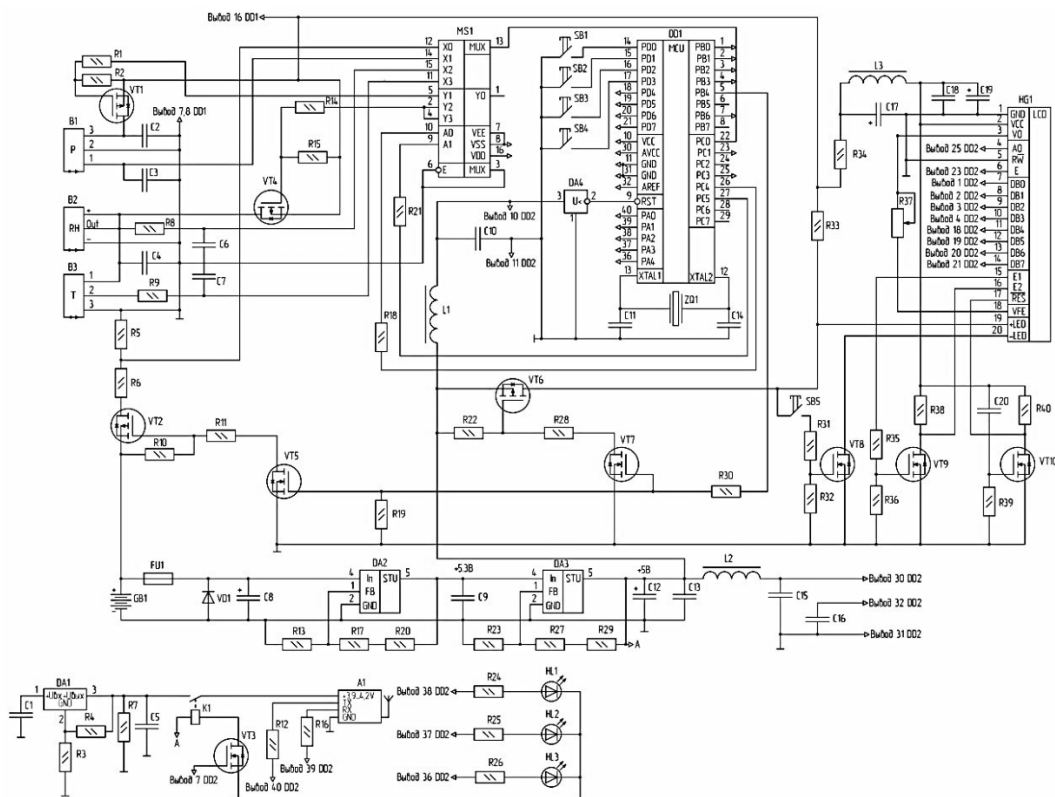


Рис. 3. Схема принципиальная КС

По принципиальной схеме была произведена трассировка печатной платы (ПП) и проектирование в САПР Altium Designer (рис. 4, 5). Для того, чтобы

увеличить трассировочную способность ПП, уменьшить габариты ПП и избежать присутствия массивных проводов, было принято решение спроектировать двустороннюю печатную плату.

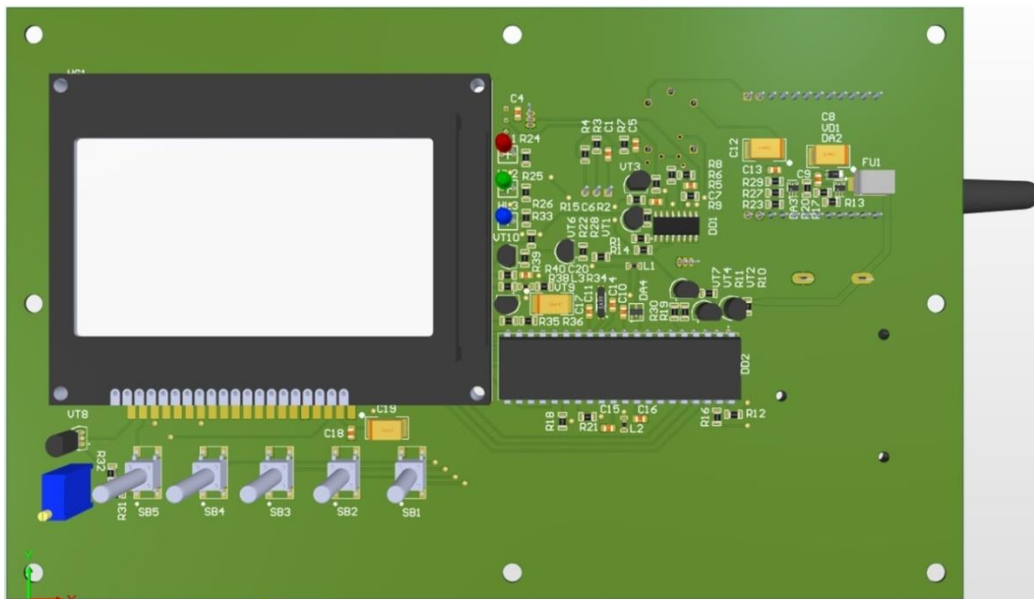


Рис. 4. 3D модель ПП климатической системы (вид сверху)

Трассировка проводилась с шириной проводника 0,25 мм, при размере фольги 35 мкм. Так как устройство работает от питания + 9 В со слабыми токами, цепи питания были выполнены дорожкой шириной 1,5 мм.

Так как к микроконтроллеру осуществляется множество подключений, было решено расположить его относительно ближе к центру рядом с дисплеем.

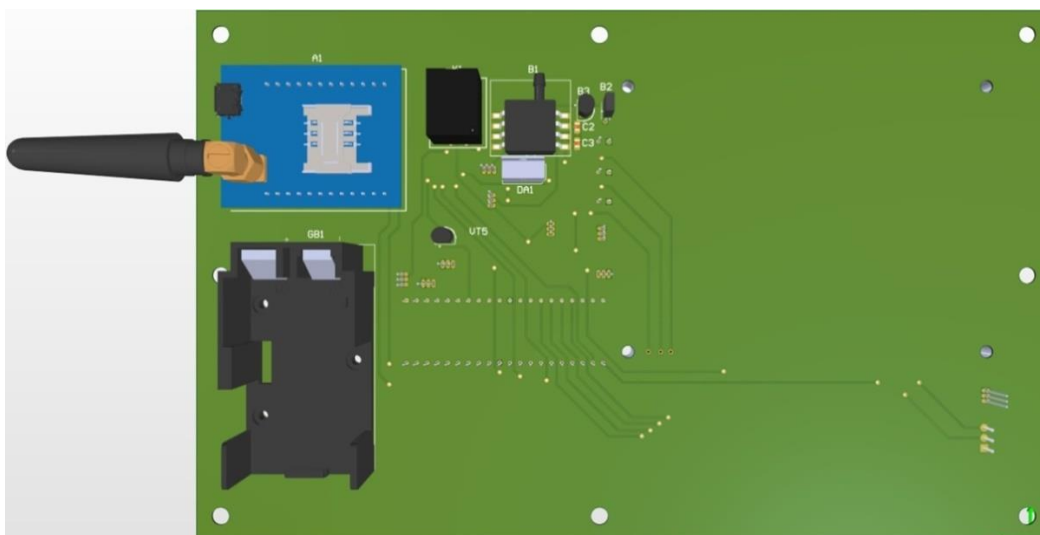


Рис. 5 — 3D модель ПП климатической системы (вид снизу)

На другой стороне расположены датчики, GSM-модуль и батарейный отсек. Для того, чтобы избежать нагрева датчиков, было принято решение расположить их на другой стороне и ближе к краю платы для точного измерения климатических параметров. GSM-модуль и батарейный отсек были также

расположены с этой стороны для удобства установки SIM-карты и замены батареи.

Таким образом, была спроектирована плата управления устройства климатического контроля с передачей данных, удовлетворяющая основным техническим требованиям.

Список используемых источников:

1. ГОСТ Р 58712-2019. Автоматизированная метеорологическая измерительная система. Общие технические требования. М.: Стандартинформ, 2019. – 1313 с.
2. ГОСТ 2.702-2011 Единая система конструкторской документации (ЕСКД). Правила выполнения электрических схем. М.: Стандартинформ, 2011 год. – 39 с.

Polenova D., Mordovin V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Designing a control board for a climate control system with data communication.

Everyone has the right to a favorable environment and reliable information about its condition. This article is devoted to the development of a control board for a climate control device with data transmission. Based on the analyzed existing climate systems, technical requirements and wiring diagrams were developed. The article describes a 3D model of the control board for a climate control device with a GSM module, designed in Altium Designer CAD.

Key words: climate system, design, tracing, GSM module, data transmission, two-sided printed circuit board.

Секция 2.4
Радиотехнические системы и антенны

УДК 621.396.96
ГРНТИ 49.33.29

УВЕЛИЧЕНИЕ ТОЧНОСТИ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ ИСТОЧНИКА РАДИОИЗЛУЧЕНИЯ ПУТЕМ ИСПОЛЬЗОВАНИЯ ИЗВЕСТНЫХ ИСТОЧНИКОВ СИГНАЛА

Н. А. Афанасьев, А. Н. Ликонцев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире существует множества методов геолокации источников радиоизлучения, такие как разностно-дальномерный метод и разностно-частотный. В данной статье предлагается рассмотреть метод повышения точности геолокации, путем использования известного источника сигнала.

определение места положения, TDOA, FDOA, улучшение точности геолокации.

В современном мире существуют 2 основных метода определения места положение (ОМП) источника радиоизлучения (ИРИ), такие как TDOA и FDOA методы. Метод TDOA (Time Difference of Arrival) использует разницу расстояний прохождения сигнала для каждой пары космических аппаратов (КА) для построения линий положения [1]. Метод FDOA (Frequency difference of arrival) использует разницу частотных отстроек при приеме сигнала вызванную доплеровским смещением частоты при движении КА от ИРИ до поста приема (ПОСТ) [2].

Входными параметрами, для ОМП являются частотные и временные отстройки после корреляционной обработки сигнала, а также TLE (two-line element) файлы для задания координат КА и их скоростей.

На рис. 1 представлена система передачи сигнала, состоящая из: 2-х спутниковых ретрансляторов, приёмной и передающей станций, а также контрольной станции с известными координатами.



Рис. 1. Схема передачи сигнала

Для улучшения точностей ОМП предлагается использовать контрольную станцию, для нивелирования ошибок, внесенных неточностями определения

координат КА и его скоростей, при использовании ТЛЕ файлов. Рассчитав временную и частотную отстройку для искомого ИРИ, т.е. dt_{meas} и df_{meas} , рассчитывается временную и частотную отстройку для контрольной станции, dt_{KC} и df_{KC} соответственно.

Далее выполняется поиск корректирующего значения для выбранного ТЛЕ файла путем нахождения разницы между расчётными отстройками, $dt_{ТЛЕ}$ и $df_{ТЛЕ}$, и отстройками для ИРИ с известными координатами (1,2):

$$dt_k = dt_{ТЛЕ} - dt_{KC} \quad (1)$$

$$df_k = df_{ТЛЕ} - df_{KC} \quad (2)$$

После чего выполняется корректировка полученных измерений для искомого ИРИ с помощью рассчитанных корректирующих значений (3,4):

$$dt = dt_{meas} + dt_k \quad (3)$$

$$df = df_{meas} + df_k \quad (4)$$

Так как для успешного ОМП необходимо построить две линии положения, использовалась модель, основанная сразу на двух методах геолокации, TDOA и FDOA, обозначенные на рис. 2 и 3. Так же отображены координаты ИРИ (iri), контрольной станции (ref) и приемной станции (post).

На рис. 2 рассчитаны линии положения для системы без использования ИРИ с известными координатами. Результаты ОМП и координаты приемных и передающих станций представлены в таблице 1.

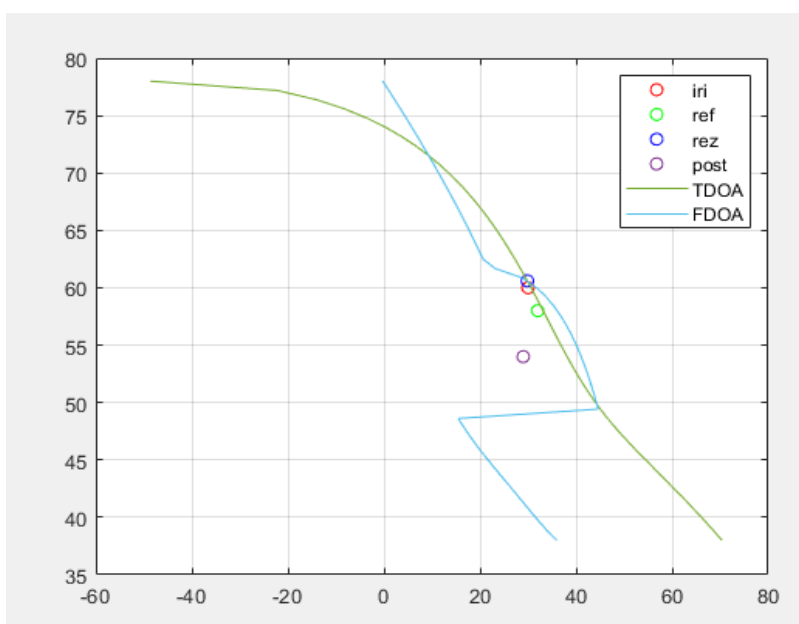


Рис. 2. Без корректировки.

ТАБЛИЦА 1

	Широта	Долгота
Пост	54	29
Источник	60	30
Выходные координаты	63.5325	24.5516
Ошибка ОМП	487097 м	

На рис. 3 рассчитаны линии положения с использованием данных после корректировки по известному ИРИ. Результаты ОМП и координаты приемных и передающих станций представлены в таблице 2.

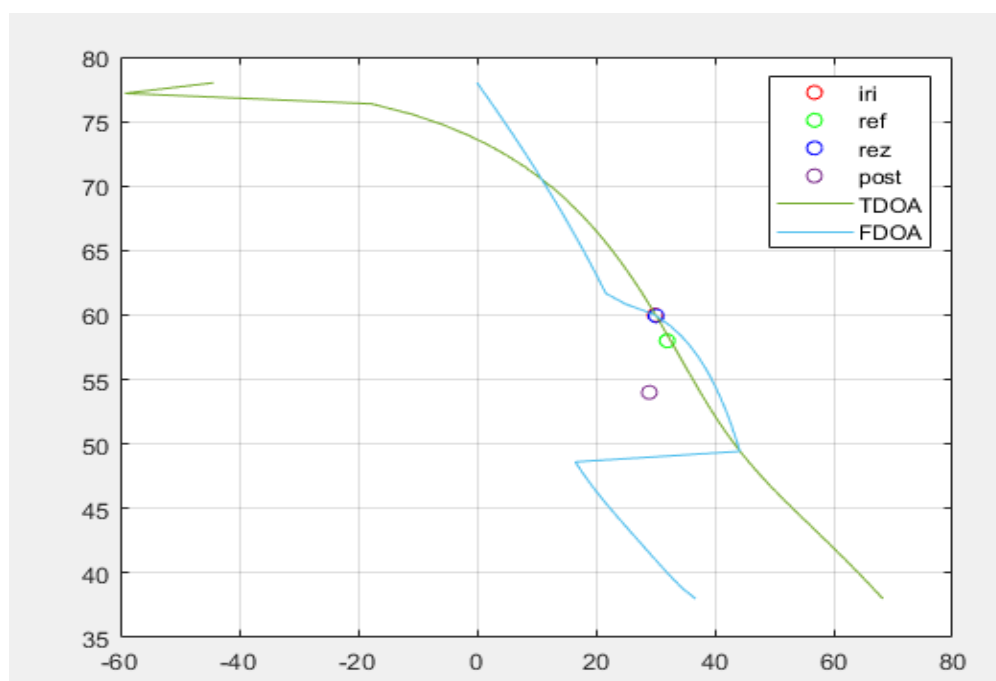


Рис. 3. С корректировкой по известному излучателю.

ТАБЛИЦА 2

	Широта	Долгота
Пост	54	29
Источник	60	30
Координаты контрольной станции	58	32
Выходные координаты	59.9397	30.1382
Ошибка ОМП	10231 м	

Из результатов видно, что использование источника радиоизлучения с известными координатами на порядок увеличивает точность определения местоположения искомого источника и обладает точностью на порядок выше, системы без корректировки и может быть рекомендована для применения в спутниковой геолокации.

Список используемых источников:

1. Севидов В.В. «Варианты реализации разностно-дальномерного метода определения координат земных станций по сигналам спутников-ретрансляторов» - Радиотехника, электроника и связь (РЭИС-2015)
2. Ануфриев А. А., Севидов В.В., Чиркин П.М., Шипунов В.А. «Оценка вектора скорости спутника-ретранслятора разностно-доплеровским способом по радиосигналам четырех опорных реперных станций» - технические и естественные НАУКИ Сборник избранных статей по материалам Международной научной конференции. 2020.

Afanasev N., Likontsev A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Increasing the accuracy of radio emission location by using known signal sources.

In the modern world, there are many methods for geolocation of radio emission sources, such as the time-difference method and the frequency-difference method. This article proposes to consider a method for improving the accuracy of geolocation by using a known signal source.

Key words: positioning, TDOA, FDOA, improving geolocation accuracy.

УДК 621.396.67
ГРНТИ 47.45.29

АДАПТИВНАЯ ОБРАБОТКА СИГНАЛОВ С ИСПОЛЬЗОВАНИЕ МЕТОДА ПАРАЛЛЕЛЬНОЙ РЕГУЛЯРИЗАЦИИ RLS АЛГОРИТМА

Е. И. Глушанков, Д. М. Кирсанов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе рассматривается обработка сигналов при невозможности получить корректное решение из-за ограниченного объема обучающей выборки размерности меньшей, чем размерность импульсной характеристики. Для решения этой задачи рассматривается параллельный RLS-алгоритм с использованием регуляризации для обеспечения устойчивости при обработке нестационарных сигналов и моделирование его в среде MATLAB.

MATLAB, регуляризация, радиотехнические системы, некорректные задачи

В настоящее время при разработке устройств обработки сигналов в радиотехнических системах необходимо обеспечивать требуемое быстродействие при обеспечении необходимых параметров по помехоустойчивости. При этом выбирается минимально необходимый объем обучающей выборки, зачастую меньшей размерности импульсной характеристики фильтра. Однако в данном случае оцениваемые корреляционные матрицы могут стать вырожденными или плохо обусловленными, а задача Винеровской фильтрации становится некорректно поставленной [1]. Для решения таких задач возможно использование методов регуляризации.

Благодаря использованию регуляризации в RLS алгоритме, мы получаем независимые вычисления, обусловленные входным сигналом и регуляризацией, за счет чего можем обрабатывать их параллельно. Параллельные вычисления дает хороший выигрыш в скорости при этом не увеличивая сложность вычислений. Целью многоканальной адаптивной фильтрации по LS- критерию является минимизация на интервале наблюдения энергии сигнала ошибки между сигналом основного входа $d(k)$ и выходным сигналом адаптивного фильтра, т. е. минимизация функционала [2]:

$$E_N(k) = \sum_{i=1}^k \lambda^{k-i} [d(i) - h_N^H(k) X_N(i)]^2,$$

где h_N^H – вектор весовых коэффициентов M -канального адаптивного фильтра, $X_N(k)$ – вектор сигналов M -канального адаптивного фильтра, N_m – число весовых коэффициентов в m -м канале адаптивного фильтра.

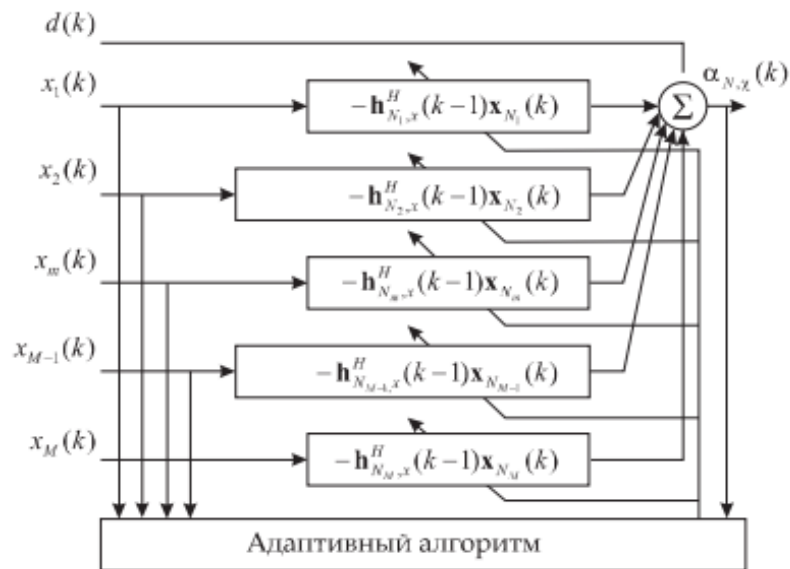


Рис. 1. Многоканальный адаптивный фильтр

Из условия минимума функционала следует решение задачи многоканальной оптимальной винеровской фильтрации[3]:

$$h_N(k) = R_N^{-1}(k)r_N(k)$$

Для сравнения с другими адаптивными алгоритмами была создана модель в среде MATLAB, в которой перед алгоритмами LMS, NMLS и параллельно регуляризованный RLS стояла задача отфильтровать входной сигнал, смешанный с белым шумом. На рис. 2 показан результат сравнения, где $x(n)$ входной сигнал, а $d(n)$ – опорный сигнал, $e(n)$ – сигнал ошибки.

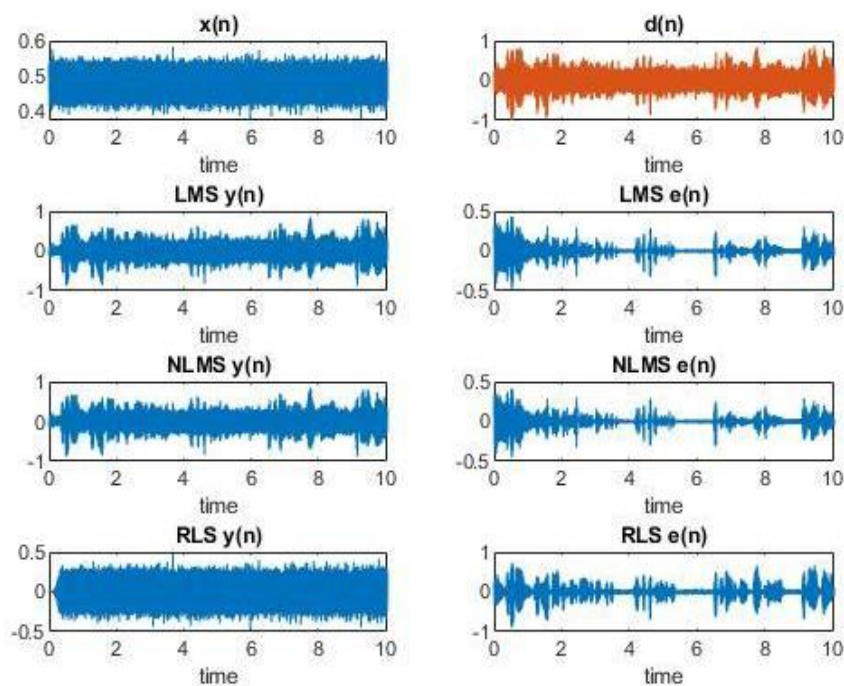


Рис. 2. Сравнение алгоритмов при шумоподавлении.

Как видно из сравнения, параллельный регуляризованный алгоритм RLS справился с задачей лучше остальных и максимально приближен к входному сигналу. Такой результат получается благодаря высокой скорости RLS алгоритма, которая в свою очередь достигается параллельными вычислениями, а также благодаря регуляризации, которая дает большую устойчивость. В отличие от последовательных вычислений, в основе параллельных лежит лемма об обращении матриц следующего вида:

$$R^{-1} = B^{-1} - B^{-1}CA^{-1}DB^{-1},$$

где $A = DB^{-1}C + S$, а C и D – матрицы

Алгоритмы LMS и NMLS так же могли достигнуть лучшего результата при увеличении, например, шага сходимости, но при минимальных затратах параллельный регуляризованный алгоритм всегда будет эффективнее.

Так же был проведен анализ зависимости среднеквадратичной ошибки от числа итераций.

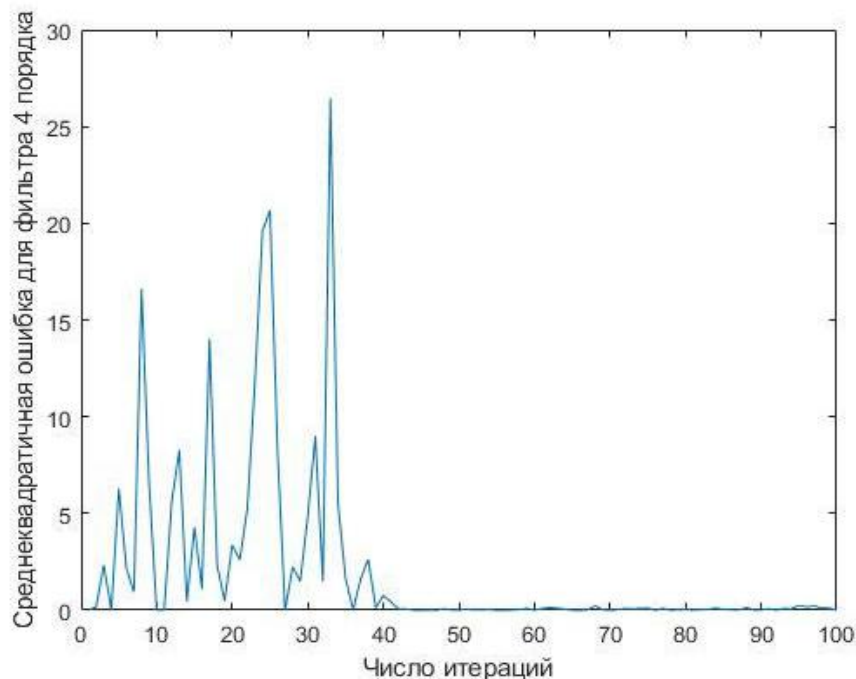


Рис. 3. Зависимость средней квадратичной ошибки от числа итераций.

Минимизация среднего квадратичного сигнала ошибки между выходом адаптивного фильтра и желаемым сигналом является наиболее распространенным критерием оптимизации адаптивных фильтров. Как видно на рис. 2, алгоритм сходится уже на 40 итерации, что является хорошим результатом, так как для многих других алгоритмов минимальное число итераций около 100.

Для реализации алгоритма можно использовать как КИХ-фильтр, так и БИХ-фильтр, поэтому было приятно решение сравнить эффективность шумоподавления между ними.

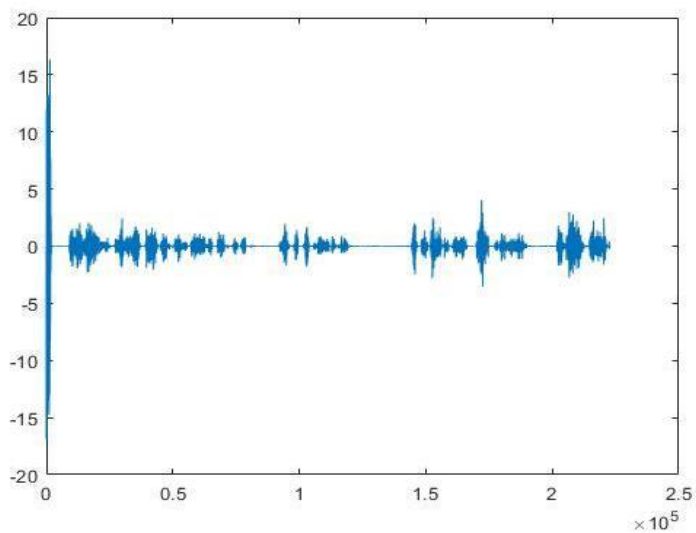


Рис. 4. Шумоподавление КИХ-фильтром 10 порядка при дисперсии шума 10

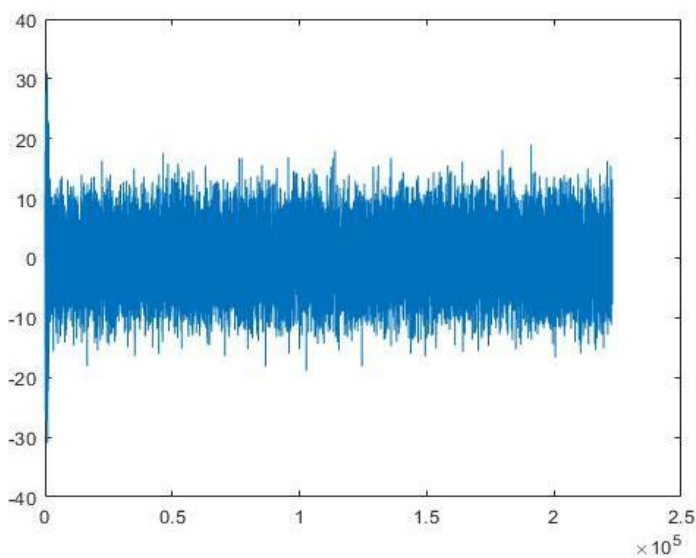


Рис. 5. Шумоподавление БИХ-фильтром 10 порядка при дисперсии шума 10

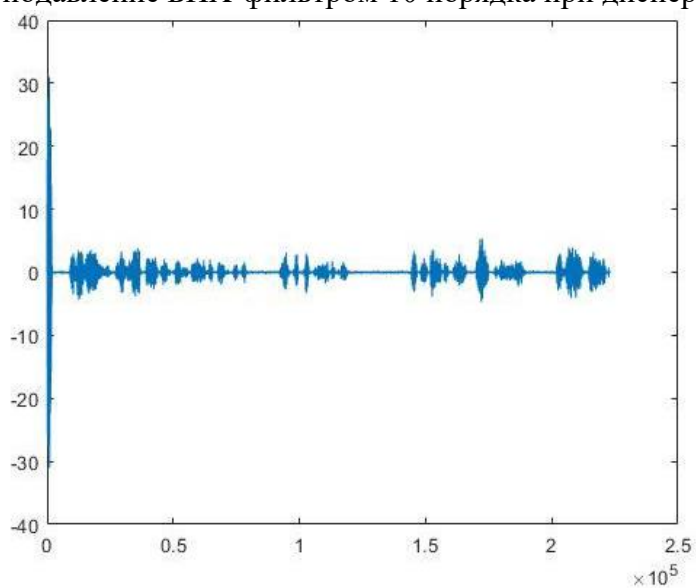


Рис. 6. Шумоподавление БИХ-фильтром 10 порядка при дисперсии шума 50

Как видно из рисунков 4,5,6 БИХ-фильтр требует для шумоподавления не меньше 50-го порядка, что значительно больше при сравнении с КИХ-фильтром. А порядок фильтра влияет на количество требуемых ресурсов, так как это количество коэффициентов фильтра, и оно связано с количеством умножителей, необходимых для реализации. К тому же БИХ-фильтры крайне неустойчивы.

Таким образом, использование параллельного регуляризованного RLS алгоритма является более эффективным методом шумоподавления, за счет скорости и решением некорректных задач с помощью регуляризации. Наиболее подходящее число итераций для минимизации ошибки – 50. При выборе фильтра для реализации лучше использовать КИХ-фильтр, так как ему необходимо меньше ресурсов для решения задачи, а также он более устойчив, чем БИХ-фильтр.

Список используемых источников:

1. Glushankov E.I., Kirik, D.I., Kirsanov, D.M., Rylov, E.A. Adaptation of antenna arrays with using correlation matrices of a special types // Systems of Signal Synchronization, Generating and Processing in Telecommunications // материал науч. конф., Светлогорск, 30 июня -2 июля 2021г. // SYNCHROINFO 2021 - Conference Proceedings, 9488331
2. Тихонов А.Н., Арсенин В.Я. Методы решения некорректных задач. – М.: Наука, 1979. – 286 с.
3. Джиган В.И. Параллельный регуляризованный быстрый RLS алгоритм многоканальной адаптивной фильтрации со скользящим окном и линейными ограничениями // Труды X-й Международной конференции «Радиолокация, навигация, связь (RLNC-2004)» (Воронеж, 13 - 15 апреля 2004 г.). Воронеж, 2004. Т. 1. С. 132-142.

Glushankov E., Kirsanov, D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Adaptive signal processing using the parallel regularization method of the RLS algorithm.

In this paper we consider the processing of signals when it is impossible to obtain a correct solution due to the limited volume of the training sample of a dimension less than the dimensionality of the impulse response. To solve this problem, we consider the parallel RLS-algorithm with the use of regularization to ensure stability in the processing of nonstationary signals and modeling it in MATLAB environment.

Key words: *MATLAB, regularization, radio systems, incorrect problems.*

УДК 621.396
ГРНТИ 49.37.29

АЛГОРИТМ ДЕКОДИРОВАНИЯ БЛОКОВЫХ КОДОВ С ИСПОЛЬЗОВАНИЕМ ПСЕВДООБРАЩЕНИЯ ПОРОЖДАЮЩЕЙ МАТРИЦЫ

Е. И. Глушанков, М. А. Мебония

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрен алгоритм декодирования блочных кодов с использованием псевдообращения порождающей матрицы. Предложен модифицированный алгоритм псевдообращения, основанный на скелетном разложении матрицы, и показана возможность его применения для декодирования.

блочные коды, порождающая матрица, псевдообращение матрицы, декодирование

Кодирование и декодирование несистематических блочных кодов (как обыкновенных линейных, так и циклических) возможно с использованием порождающей матрицы кода, способы нахождения которой достаточно подробно изложены в литературе [1 – 3]. Так, блочный (n,k) -код полностью определяется порождающей матрицей G размером $(n,n-k)$ с двоичными матричными элементами. При этом каждое кодовое слово является линейной комбинацией строк матрицы G , а каждая линейная комбинация строк G – кодовым словом.

Простейший способ декодирования блочных кодов после исправления ошибок в кодовой комбинации синдромным или итерационным методом состоит в умножении принятого кодового вектора на обратную порождающую матрицу. Методы построения обратной матрицы были рассмотрены в [4 – 5], однако в связи со сложностью и низкой точностью подобные процедуры не получили широкого распространения на практике. В связи с тем, что порождающая матрица является прямоугольной, необходимо осуществлять не обыкновенное обращение, а псевдообращение порождающей матрицы. В настоящее время появились различные достаточно эффективные методы псевдообращения [6], что позволяет вернуться к использованию данной процедуры при декодировании несистематических блочных кодов.

В данном случае псевдообращение можно понимать, как наилучшую аппроксимацию (по методу наименьших квадратов) решения соответствующей системы линейных уравнений, первым этапом которой является скелетное разложение матрицы, а вторым – непосредственно поиск решения системы через псевдообращение. Запишем модифицированный алгоритм псевдообращения следующим образом:

```
clc
clear all
%берем порождающую матрицу

n = input('Введите количество столбцов матрицы:')
m = input('Введите количество строк матрицы ')

por = randi([0 1], m , n)
```

```
%произвольный двоичный вектор
```

```
vek = randi([0 1], 1, m)
```

```
%получаем вектор путем умножения:
```

```
semel = vek*por
```

```
%псевдообразная от порождающей:
```

```
psev = pinv(por)
```

```
%получаем исходный вектор:
```

```
ishvek = semel*psev
```

Результаты моделирования для различных информационных векторов:

Введите количество столбцов матрицы:7

```
n =
```

```
7
```

Введите количество строк матрицы 4

```
m =
```

```
4
```

```
por =
```

```
1 1 1 1 0 1 1
```

```
1 0 1 0 1 0 1
```

```
0 0 0 1 1 1 1
```

```
1 1 1 0 1 1 0
```

```
vek =
```

```
1 0 1 0
```

```
semel =
```

```
1 1 1 2 1 2 2
```

```
psev =
```

```
0.1449 0.2319 -0.2464 0.0435
```

```
0.2029 -0.2754 -0.1449 0.2609
```

```
0.1449 0.2319 -0.2464 0.0435
```

```
0.2754 -0.1594 0.2319 -0.2174
```

```
-0.5072 0.1884 0.3623 0.3478
```

```
0.0145 -0.3768 0.2754 0.3043
```

```
0.2174 0.3478 0.1304 -0.4348
```

```
ishvek =
```

```
1.0000 -0.0000 1.0000 -0.0000
```

Рассмотрим данный алгоритм на примере моделированной в Симулинк схемы.

В данной схеме блок Bernoulli Binary Generator задает случайную последовательность двоичных чисел, которая в дальнейшем приходит на кодер Хэмминга (Hamming Encoder). В кодере Хэмминга последовательность из 4 элементов преобразуется в последовательность из 7 элементов, путем добавления избыточных проверочных символов. Закодированная последовательность суммируется с белым шумом (мощность шума 90 дБ) (Band-Limited White Noise). После чего закодированная последовательность с

ошибками поступает на декодер Хэмминга (Hamming Decoder), где с помощью избыточных символов могут быть обнаружены и исправлены ошибки. Затем сравнивается изначально закодированная последовательность с декодированной для подсчета ошибок на блок Error Rate Calculation, с которого на дисплей (Display) выводится частота ошибок, число обнаруженных ошибок, общее количество символов по сравнению.

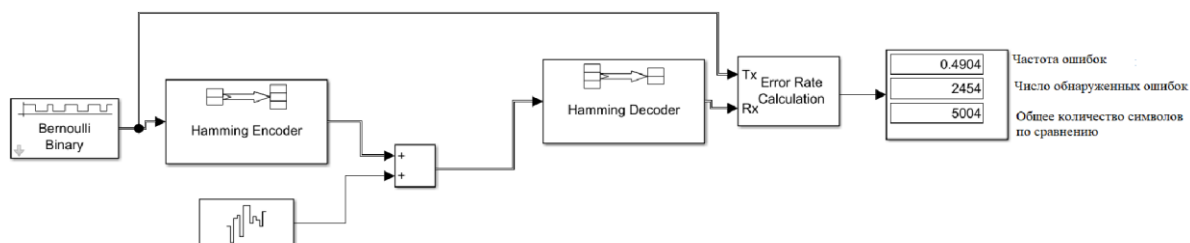


Рис. 1. Схема имитированной передачи сигнала

Таким образом, использование метода псевдообращения порождающей матрицы позволяет осуществить простую процедуру декодирования блочных несистематических кодов. Как видно из схемы, при мощности шума 90 дБ вероятность ошибок становится 0.5, что делает невозможным передачу сигнала.

Список используемых источников:

1. Коржик В.И., Финк Л.М. Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой. – М.: Связь, 1975. – 271 с.
2. Варгаузин В.А., Цикин И.А. Методы повышения энергетической и спектральной эффективности цифровой радиосвязи. – СПб: БХВ-Петербург, 2013. – 352 с.
3. Волков Л.Н., Немировский М.С., Шинаков Ю.С. Системы цифровой радиосвязи: базовые методы и характеристики. – М.: Эко-Трендз, 2005. – 392 с.
4. Берликэмп Э. Алгебраическая теория кодирования. – М.: Мир, 1971. – 478 с.
5. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2005. – 320 с.
6. Цехан О.Б. Матричный анализ. – Гродно: ГГУ, 2010. – 372 с.

Glushankov E., Meboniya M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Block Code Decoding Algorithm Using Generator Matrix Pseudo-Inversion.

An algorithm for decoding block codes using pseudo-circulation of the generating matrix is considered. A modified pseudo-circulation algorithm based on the skeletal representation of a square matrix is proposed and the possibility of its application for decoding is shown.

Key words: *block codes, generating matrix, pseudo-circulation of the matrix, decoding.*

УДК 621.391
ГРНТИ 47.05.09

ПСЕВДОСЛУЧАЙНОЕ ВКЛЮЧЕНИЕ АНТЕНН КАК МЕТОД ПОВЫШЕНИЯ ЭНЕРГЕТИЧЕСКОЙ ЭФФЕКТИВНОСТИ СИСТЕМ ЦИФРОВОЙ РАДИОСВЯЗИ

Е. И. Глушанков, В. В. Пуршель

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье предлагается новый метод повышения энергетической эффективности за счёт псевдослучайного включения антенн каждый такт времени. Данный метод является модификацией пространственно-временного кодирования. Для анализа эффективности нового метода проведено сравнительное моделирование.

помехоустойчивость, энергетическая эффективность, MIMO

В зависимости от целей и условий функционирования системы радиосвязи оценка энергетической эффективности основывается на определённых показателях. В качестве универсального показателя энергетической эффективности системы цифровой радиосвязи принято рассматривать следующую величину:

$$h^2 = \frac{E_b}{N_0}$$

характеризующую энергетические затраты на передачу одного бита информации для обеспечения величины средней вероятности ошибочного приема одного символа (или бита) передаваемого сообщения не выше заданного значения в условиях воздействия аддитивного белого гауссового шума со спектральной плотностью средней мощности $\frac{N_0}{2}$. [1]

В 80-90-е годы прошлого века получил развитие метод пространственного кодирования, который сейчас известен как MIMO (Multiple Input Multiple Output). Такой метод позволяет увеличить энергетическую эффективность за счёт использования системы из $N \times M$ антенн и пространственно-временное кодирование (например, блочные методы пространственно-временного кодирования на основе схемы Аламоути). [2]

Предлагаемый метод псевдослучайного включения антенн является модификацией пространственно-временного кодирования. Метод основан на передачи информационного потока каждый временной такт при включении псевдослучайным образом N из M антенн. Псевдослучайный закон, по которому включаются антенны, одинаков и известен для передающей и приёмной сторон.

На рис. 1 представлена схема рассматриваемого метода для системы 4×4 антенн. Кодированный и модулированный информационный поток поступает на вход системы из 4 антенн (1). Блок переключения (2) регулирует включение

антенн: сначала псевдослучайным образом выбирается антенна №1 для передачи, а потом антенна №2 так, чтобы номера выбранных антенн не были одинаковыми. Далее (3) двумя wybranными антеннами сигнал транслируется через канал передачи на приёмную сторону (4). На приёмной стороне блок переключения (5) регулирует включение приёмных антенн по такому же псевдослучайному закону, что и блок переключения на передающей стороне. После приёма (6) информационный поток демодулируется и декодируется.



Рис. 1. Схема работы метода псевдослучайного включения антенн для системы 4x4 антенн

Достоинством такого метода является возможность не только программной, но и аппаратной, и программно-аппаратной реализации. Метод псевдослучайного включения антенн можно применять в системах, где требуется высокая защищённость.

Для анализа энергетической эффективности было проведено сравнительное моделирование трёх систем радиосвязи с BPSK: детерминированная система 1x1, детерминированная система 2x2 и система с псевдослучайным включением антенн. На рис. 2 представлены результаты моделирования. Использование такого метода позволяет добиться энергетического выигрыша около 4 дБ при величине ошибки 10^{-3} и около 10 дБ при величине ошибки 10^{-4} .

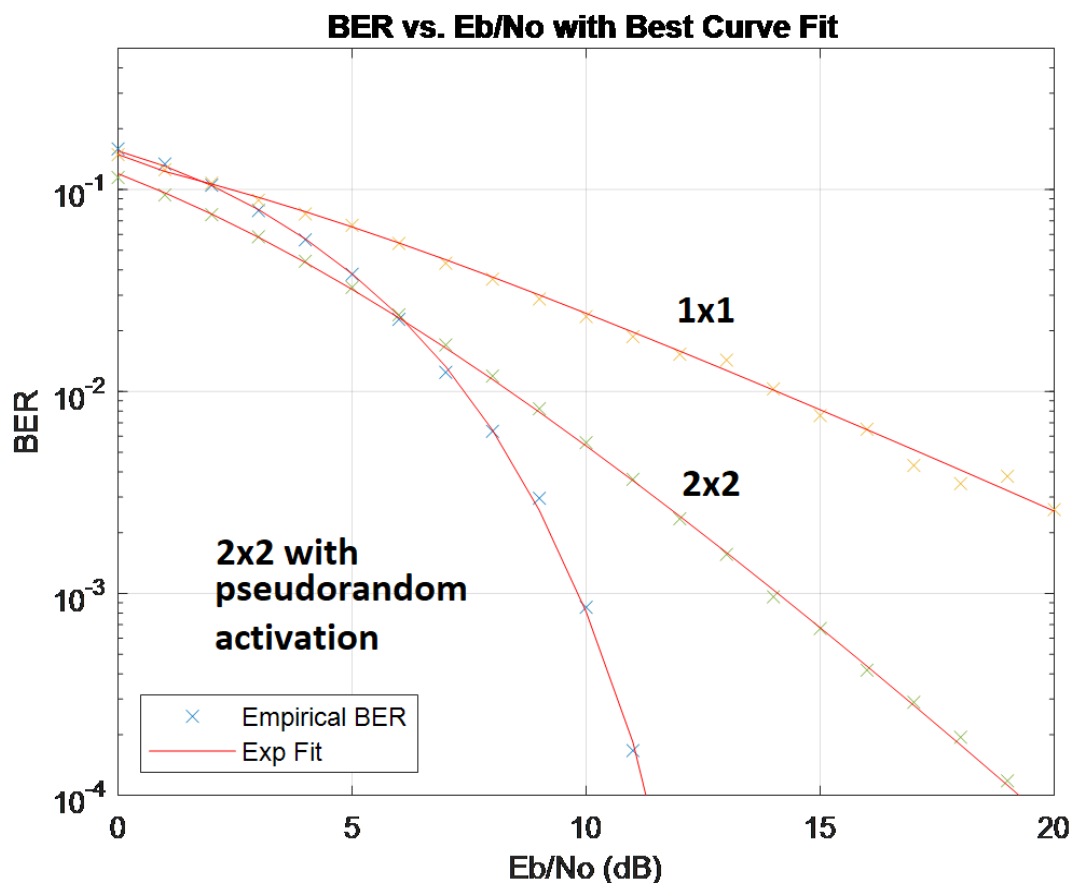


Рис. 2. Результаты моделирования

Список используемых источников:

1. В. А. Варгаузин, И. А. Цикин. Методы повышения энергетической и спектральной эффективности цифровой радиосвязи: учеб. пособие. СПб. : БХВ-Петербург, 2013. 352 с.
2. И. Степанец, Г. Фокин. Особенности реализации Massive MIMO в сетях 5G // Первая мила. 2018. N 1. С. 46–52.

Glushankov E., Purshel V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Pseudorandom activation of antennas as a method of increasing the energy efficiency of digital radio communication systems.

The article proposes a new method of increasing energy efficiency by pseudorandom activation of antennas every clock cycle. This method is a modification of space-time coding. Comparative modeling was carried out to analyze the effectiveness of the new method.

Key words: noise immunity, energy efficiency, MIMO.

УДК 621.317.343.3
ГРНТИ 47.14.13

СОЗДАНИЕ ПРИЛОЖЕНИЕ ДЛЯ РАСЧЕТА ЭЛЕМЕНТОВ СОГЛАСОВАНИЯ СВЧ-УСТРОЙСТВ

К. О. Коровин, М. А. Никитин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Согласование СВЧ-устройств – важная задача в проектировании линий связи. Для согласования СВЧ-устройств используют такой инструмент, как диаграмма Смита. Долгое время, чтобы использовать данную диаграмму, требовалось выполнять сложные графические построения. Сейчас с помощью навыков программирования можно самостоятельно построить диаграмму Смита для решения различных видов задач.

MATLAB, GUI, диаграмма Смита, СВЧ

Параметры электрических компонентов и схем изменяют входные сигналы по величине и фазе. Любой синусоидальный сигнал, поступающий на вход, появится и на выходе устройства на той же самой частоте. Как активные, так и пассивные нелинейные элементы схемы могут сместить входной сигнал по частоте или внести дополнительные частотные компоненты, например, гармоники или нежелательные комбинационные составляющие. Мощные входные сигналы могут изменить характер работы линейных устройств, приводя к компрессии или насыщению и вызывая нелинейный эффект.

Для того чтобы успешно передавать или принимать сигналы, особенно в СВЧ-диапазоне, передающие устройства, такие как линии передачи, антенны или усилители, должны отличаться хорошим согласованием сопротивления с источником сигнала. Рассогласование сопротивления происходит, когда реальные и мнимые части входного и выходного импеданса плохо согласованы между двумя связанными устройствами [1].

Для понимания того, как должны быть согласованы СВЧ-устройства, используются диаграмма Смита. Диаграмма Смита представляет собой круговой график с множеством переплетенных окружностей (рис. 1). При правильном использовании согласование импедансов быть выполнено без каких-либо вычислений. Единственное, что требуется, – это считывать значения и следовать им по окружностям.

Диаграмма Смита представляет собой полярный график комплексного коэффициента отражения. Математически он определяется как параметр рассеяния от порта 1, или s_{11} . Диаграмма разрабатывается путем исследования нагрузки, импеданс которой должен быть согласован. Вместо того, чтобы напрямую рассматривать импеданс, можно выражать коэффициент отражения, который используется, чтобы охарактеризовать нагрузку [2].

Точки, расположенные на окружности, представляют собой все импедансы, характеризующиеся одним и тем же значением действительной части импеданса. Например, окружность $r = 1$ имеет центр в координатах $(0,5, 0)$ и радиус $0,5$. Она включает в себя точку $(0, 0)$, которая является нулевой точкой отражения (нагрузка согласована с характеристическим сопротивлением). Короткое замыкание в качестве нагрузки представляет собой круг с центром в координате $(0, 0)$ и радиусом 1 . Для разомкнутой цепи в качестве нагрузки окружность вырождается в одну точку (с центром в $(1, 0)$ и радиусом 0). Это соответствует

максимальному коэффициенту отражения, равному 1, при котором вся падающая волна отражается полностью [3].

При разработке диаграммы Смита следует помнить о следующем:

- все окружности имеют одну и ту же единственную точку пересечения в координате (1, 0);
- окружность с нулевым сопротивлением, на которой нет сопротивления ($r = 0$), является наибольшей;
- окружность бесконечного активного сопротивления сокращается до одной точки в точке (1, 0);
- не должно быть отрицательных активных сопротивлений. Если одно (или несколько) появится, мы столкнемся с возможностью возникновения колебаний;
- выбрать другое значение активного сопротивления можно, просто выбрав другую окружность, соответствующую новому значению.

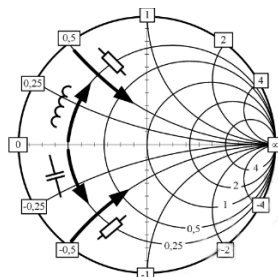


Рис. 1. Диаграмма Смита

Диаграмма Смита позволяет также решить такие задачи, как:

- расчёт коэффициента отражения по известному комплексному сопротивлению;
- расчёт коэффициента отражения и сопротивления линии в произвольном сечении;
- расчёт расстояния от нагрузки до произвольного сечения с заданным значением коэффициента отражения;
- расчёт коэффициента стоячей волны и коэффициента бегущей волны;
- определение проводимости по заданному сопротивлению;
- согласование импедансов.

Но для решения проблем согласования СВЧ-устройств требуется видеть, как изменяется входной импеданс при добавлении элемента в схему [3]. Поэтому предлагается создание приложения, которое позволит анализировать изменения входного импеданса. Интерфейс приложения представлен на рис. 2.

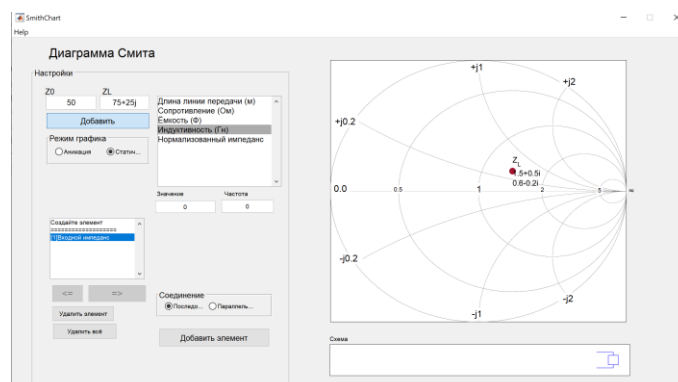


Рис. 2. Интерфейс приложения

Диаграмма Смита в таком виде позволяет выполнять автоматизированным методом операцию, которую ранее можно было выполнить только с помощью графических построений и сложных расчётов. На рис. 3 показан пример изменения импеданса для подключения к входной нагрузке две последовательно соединённых резистора.

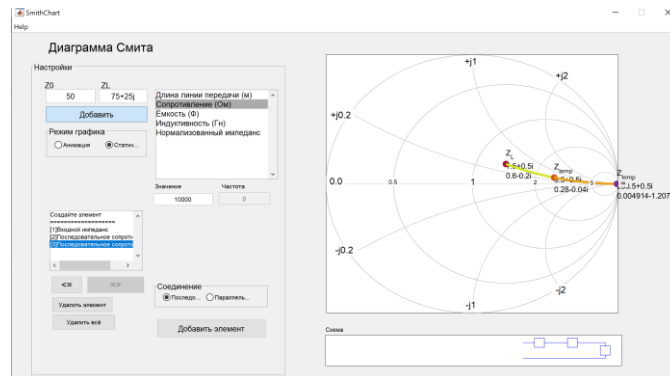


Рис. 3. Пример изменения импеданса при $R_1 = 100 \text{ Ом}$, $R_2 = 10000 \text{ Ом}$

В будущем планируется улучшение работы алгоритма, который рассчитывает изменение импеданса, увеличение количество параметров, которые можно рассчитать с помощью диаграммы Смита, и модернизация интерфейса.

Список используемых источников:

1. Применение диаграммы Смита при согласовании устройств [Электронный ресурс]. URL: <http://rabfoo.qrz.ru/smith.html> (дата обращения 06.11.2022).
2. Согласование импедансов и диаграмма Смита [Электронный ресурс]. URL: <https://radioprogram.ru/post/1387> (дата обращения 01.11.2022).
3. Курушин А.А. Проектирование СВЧ устройств с использованием электронной диаграммы Смита/ под ред. д.т.н., проф. Когана Б.Л. Москва: изд. МЭИ, 2008. 120 с.

Korovin K., Nikitin M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Application for matching microwave devices.

The matching of microwave devices is an important task in the design of communication lines. A tool such as the Smith diagram is used to match microwave devices. For a long time, to use this diagram, it was necessary to perform difficult graphical constructions. Now, with the help of programming skills, you can independently create a Smith diagram to solve various types of problems.

Key words: MATLAB, GUI, Smith Chart, microwave.

УДК 621.396
ГРНТИ 49.43.29

АЛГОРИТМ УПРАВЛЕНИЯ АМПЛИТУДНО-ФАЗОВЫМ РАСПРЕДЕЛЕНИЕМ ТОКА В АНТЕННЫХ ЭЛЕМЕНТАХ ПЕРЕДАЮЩЕЙ ФАЗИРОВАННОЙ АНТЕННОЙ РЕШЕТКИ

М. Н. Лавров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрена задача разработки алгоритма адаптивного управления амплитудно-фазовым распределением тока в антенных элементах передающей фазированной антенной решетки для формирования нескольких максимумов диаграммы направленности с целью получения оптимальных энергетических параметров радиоканалов в заданных направлениях. Проведено моделирование и решена оптимизационная задача на языке программирования python.

антенная решетка, диаграмма направленности, параметры радиоканалов, python

Задача разработки алгоритма адаптивного управления амплитудно-фазовым распределением тока в антенных элементах передающей фазированной антенной решетки (АФАР) для формирования нескольких максимумов диаграммы направленности с целью получения оптимальных энергетических параметров радиоканалов в заданных направлениях может быть разделена на несколько подзадач.

На начальном этапе исследования формулируется задача формирования неадаптивной ДН в виде оптимизационной задачи для поиска вектора весовых коэффициентов АР. Целевая функция такой задачи задается в следующем виде [1]:

$$A(\theta) = \sum_{i=1}^N w_i e^{j(i-1)\varphi}$$

где

$$\varphi = 2\pi(d / \lambda_0) \sin \theta$$

$A(\theta)$ – ДН АР, w – вектор весовых коэффициентов, N – количество элементов АР, d – расстояние между элементами, λ_0 – длина волны $x(t)$, θ – угол прихода луча. Схема представлена на рис 1.

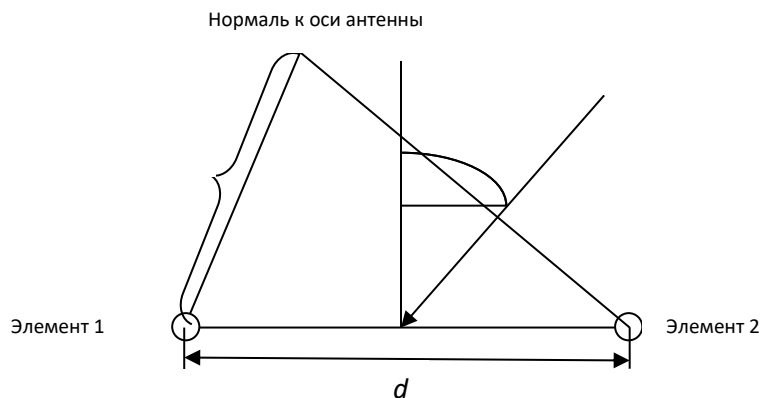


Рис. 1. Антенная решетка, состоящая из ненаправленных элементов.

Целевая функция максимизируется в направлении прихода луча, при ограничениях на значение функции в двух других направлениях:

$$\begin{cases} \sum_{i=1}^N w_i e^{j(i-1)\varphi} \text{ max, при } \theta = 0 \\ \sum_{i=1}^N w_i e^{j(i-1)\varphi} = 0, \text{ при } \theta = 60^\circ \\ \sum_{i=1}^N w_i e^{j(i-1)\varphi} = 0, \text{ при } \theta = 270^\circ \end{cases}$$

В ходе решения необходимо использование нескольких алгоритмов оптимизации, на основе результата работы которых следует провести сравнительный анализ использованных методов.

Первые результаты моделирования представлены на рис. 2. На графике показана оптимизированная ДН при ограничении по углу прихода помехового сигнала 60 и 45 градусов.

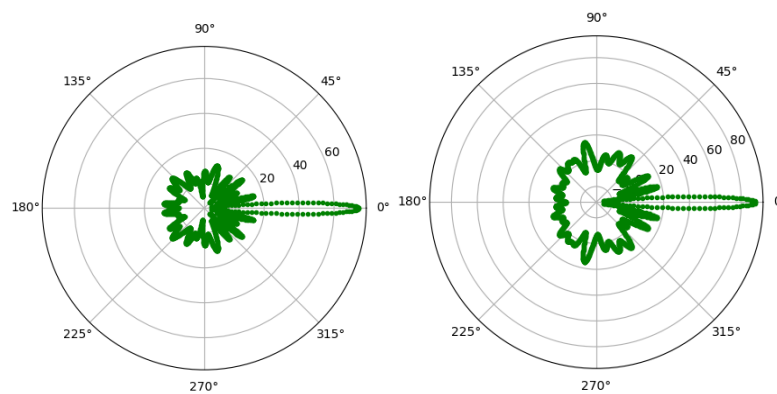


Рис. 2 Оптимизированная ДН с минимизацией по направлениям 60 (слева) и 45 (справа) градусов.

В качестве обзорного материала были рассмотрены адаптивные алгоритмы [3].

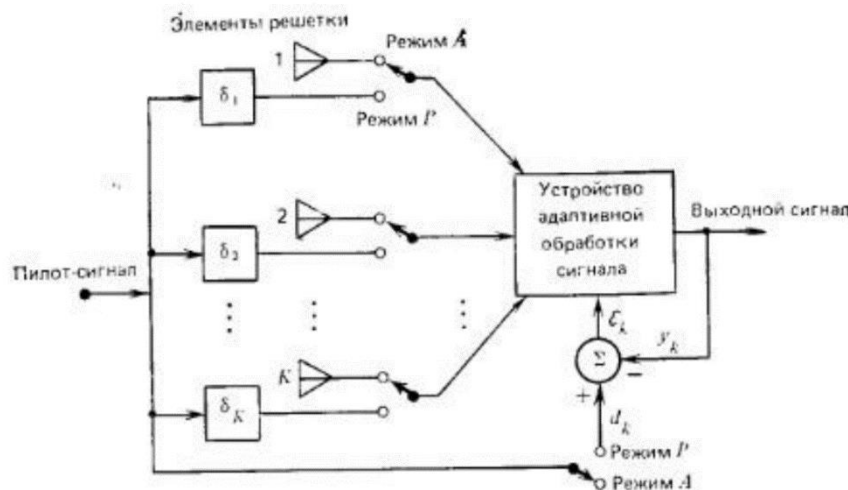


Рис. 3. Схема получения местного пилот-сигнала [3]

На рис. 3 приведена схема получения местного пилот-сигнала, который передается с антенны, расположенной на некотором расстоянии от решетки, в необходимом направлении приема.

На входные устройства обработки подаются либо действительные входные сигналы элементов антенны (в режиме А), либо множество задержанных сигналов, полученных от генератора пилот-сигнала (в режиме Р).

Идеальные задержки выбраны так, что множество входных сигналов идентично сигналам, которые принимались бы решеткой от расположенного на расстоянии источника пилот-сигнала с плоской волной в требуемом направлении приема, которое соответствует основному лепестку ДН на приеме

Во время адаптации в режиме Р входные сигналы адаптивного устройства обработки получают из пилот-сигнала, а его полезным откликом является собственно пилот-сигнал. Например, при синусоидальном пилот-сигнале адаптация весовых коэффициентов с целью минимизации СКО приводит к тому, что коэффициент передачи антенной решетки в направлении приема имеет заданные амплитуду и фазовый сдвиг.

Во время адаптации в режиме А все сигналы, подаваемые на адаптивное устройство обработки, принимаются элементами антенны из реального поля с шумом. В этом режиме процесс адаптации приводит к подавлению всех принятых сигналов, так как полезный отклик равен нулю. Однако непрерывное функционирование в режиме А приводит к тому, что значения всех весовых коэффициентов стремятся к нулю, и система отключается. Тем не менее при частом чередовании режимов Р и А в течение адаптации в каждом из них происходят лишь небольшие изменения вектора весовых коэффициентов, и можно приближенно поддерживать луч с единичным коэффициентом передачи в заданном направлении приема и, помимо этого, приблизительно минимизировать мощность принимаемой помехи.

В качестве пилот-сигнала можно взять сумму нескольких синусоидальных сигналов с различными частотами, так что при адаптации в режиме Р коэффициент передачи и фаза антенны имеют заданные для каждой из этих частот значения в направлении приёма.

Список используемых источников:

1. Монзинго Н.А., Миллер Т.У. Адаптивные антенные решетки введение в теорию. М. Радио и связь, 1986.
2. Гончаров В.А. Методы оптимизации учебное пособие. М. Высшее образование, 2009
3. Уидроу Б., Стирнз С. Адаптивная обработка сигналов

Lavrov M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Management algorithm of amplitude-phase current distribution in antenna elements of transmitting phased antenna array.

This article focuses on development of an adaptive algorithm to manage amplitude-phase current distribution in antenna elements of transmitting phased antenna array for forming several diagram maximums in purpose of radio channel energy parameters optimization in stated directions. Optimization and modeling results has been obtained by the use of python programming language.

Key words: *antenna array, directional pattern, radio channel parameters, python.*

УДК 629.783
ГРНТИ 89.29.55

ОЦЕНКА ДАЛЬНЕЙШЕГО РАЗВИТИЯ СТАНДАРТОВ СПУТНИКОВОЙ ПЕРЕДАЧИ ДАННЫХ

А. Н. Ликонцев, Д. А. Нев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассмотрены методы повышения качества передачи данных в спутниковых системах. Проведена оценка тенденции развития технологий повышения качества в системах спутникового вещания. Также проведен анализ стандартов передачи данных в спутниковой системе и создана сравнительная модель в среде Simulink.

DVB-S2, DVB-S2X, VSAT, FEC, ACM

Современная спутниковая связь является одним из направлений развития радиорелейных коммуникаций. В данном случае это применение орбитальных спутников в качестве ретрансляторов. Технологии спутниковой связи позволяют использовать один или несколько ретрансляторов для обеспечения качественной передачи радиосигнала на большие расстояния.

HTS

В последнее время скорость передачи данных спутниковых систем значительно выросла благодаря применению High Throughput Satellite (HTS). HTS – это спутники с высокой пропускной способностью, которая достигается за счет одновременного использования множества лучей. Данное преимущество и отличает HTS от классических спутниковых систем, где применяется только один луч.

Использование множества лучей делает возможным переиспользование частотного ресурса, доступного конкретному спутнику. Что в условиях ограниченности позволяет оптимизировать использование частотных диапазонов. В следствие чего, покрытие одного спутника становится ограничено только видимой частью Земли.

Переиспользование частот позволяет увеличить ширину полосы и, соответственно, максимально возможную скорость передачи данных. Улучшение этих характеристик позволяет передавать телевизионный и интернет трафик с большим разрешением на пользовательские терминалы, например, такие как Very Small Aperture Terminal (VSAT) [1].

VSAT

Лидером в области спутниковой связи на сегодняшний день является VSAT — технология, в основе которой лежит применение абонентского терминала с антенной малого диаметра, находящегося под управлением центральной земной станции спутниковой связи.

Информация передается следующим образом:

Запрос от наземного оборудования через терминал VSAT передается на геостационарный спутник, а затем поступает в центр управления сетью спутникового оператора, отправляющего данные в глобальную сеть. Получив ответ, оператор через спутник передает данные на VSAT-терминал абонента. Подавляющее большинство существующих VSAT-сетей работает в Ku- и Ka-диапазонах. Преимущество Ka-диапазона заключается в ширине полосы – она наибольшая из всех существующих на данный момент диапазонов. Диапазоны, используемые в спутниковых системах, представлены на рис. 1.

Диапазоны используемые в спутниковых системах



Рис. 1. Диапазоны спутниковых систем

Станции VSAT относятся к классу станций фиксированной спутниковой связи (ФСС). Для ФСС регламентом МСЭ приняты диапазоны частот C (6/4 ГГц), Ku (14/11 ГГц) и Ka (20/30 ГГц). Но сегодня, помимо традиционных VSAT, существуют станции, которые относят к перемещаемым или мобильным.

В спутниковых системах поддерживается динамическое изменение скорости кодирования в обратных каналах (от VSAT к хабу) без перехода VSAT на другой обратный канал. Переключение происходит автоматически в зависимости от изменения погодных условий в месте расположения станции или хаба. Если изменения скорости кодирования оказывается недостаточно для компенсации повышенного затухания, то VSAT автоматически переходит на более низкую символьную скорость. Кроме того, VSAT поддерживает регулировку мощности излучения в обратном канале.

Все изменения и переключения происходят под управлением хаба, который постоянно контролирует уровень и качество сигнала от всех VSAT по замкнутой петле [2].

ФЕС

Поскольку требования к полосе пропускания увеличиваются, а допуск на ошибки и задержку уменьшаются, разработчики систем передачи данных искали новые способы расширения доступной полосы пропускания и повышения качества передачи. Одно из решений — это прямое исправление ошибок (ФЕС), в течение многих лет этот метод используется для обеспечения эффективной высококачественной передачи данных по шумным каналам.

ФЕС — это метод цифровой обработки сигналов, используемый для повышения надежности данных. Это делается путем введения избыточных данных, называемых кодом с исправлением ошибок, перед передачей или хранением данных. Передача сигналов с ФЕС и без представлена на рис. 2. ФЕС позволяет приемнику исправлять ошибки без обратного канала для запроса повторной передачи данных.



Рис. 2. Работа FEC

Кодирование с упреждающей коррекцией ошибок (FEC) осуществляет связывание внешнего кода BCH (код Боуза-Чоудхури-Хоквингема) и внутренних кодов LDPC.

DVB-S2/DVB-S2X

В зависимости от области применения блоки кодов FEC могут иметь длину 64 800 либо 16 200 битов. Когда используются переменные кодирование и модуляция (VCM) либо ACM, FEC и режим модуляции являются постоянными в пределах кадра, однако могут быть изменены в других кадрах; более того, переданный сигнал может содержать смесь нормальных и коротких кодовых блоков.

При выборе группы модуляции и кодовых скоростей можно выбрать эффективность использования спектра в пределах от 0,5 до 4,5 битов на символ в зависимости от возможностей и ограничений используемого спутникового ретранслятора. Модуляции, применяемые в стандарте DVB-S2, приведены на рис. 3.

Стандарт DVB-S2X основан на стандарте DVB-S2, но благодаря применению более совершенных технологий диапазон выбора расширен до 0,1-6 бит на символ.

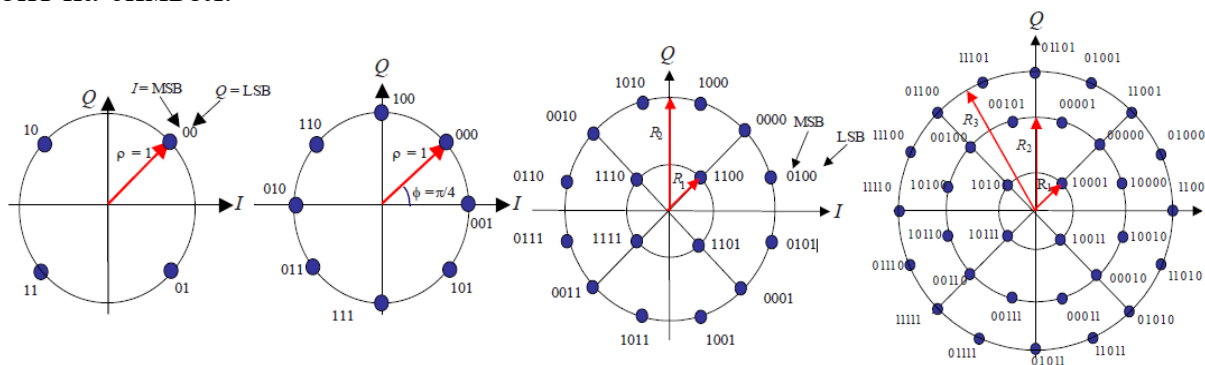


Рис. 3. Модуляционные созвездия

Модель

В программе Simulink на базе MATLAB была создана модель для оценочного сравнения DVB-S2 и его расширения DVB-S2X. Полученные данные были собраны и проанализированы в программе Excel. Эта модель создана для оценки тенденции развития данного стандарта и технологий применяемых в DVB. Результат анализа модели представлен на рис. 4 [3].

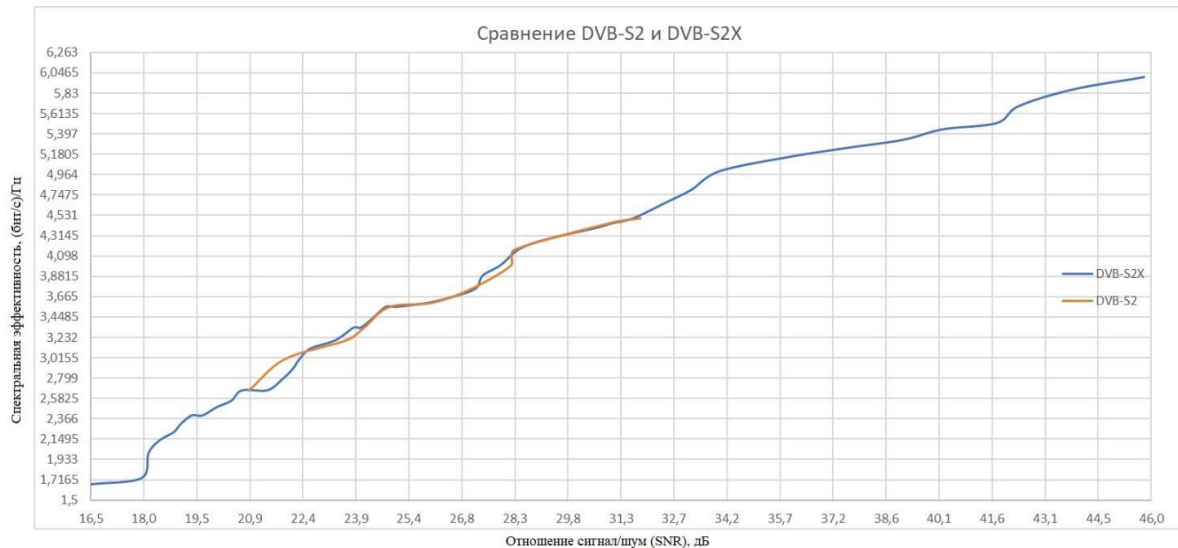


Рис. 4. Сравнение стандартов DVB-S2 и DVB-S2X.

В модели созданы два спутниковых канала передачи данных в одном, из которых используется DVB-S2, в другом DVB-S2X. В ходе сравнения были оценены диапазоны отношения сигнал/шум, при котором система поддерживает безошибочную передачу данных. Были рассчитаны спектральные эффективности, без учета ширины полосы пропускания. И по ним построен график представленный на рис. 4.

В ходе анализа созданной модели и существующих технологий можно сделать следующие выводы о тенденции развития стандартов систем спутниковой передачи данных:

- Освоение нового Ka- диапазона. Благодаря широкой полосе частот в данном диапазоне можно использовать более широкие каналы, что прямо пропорционально повлияет на скорость передачи данных.
- Развитие терминалов VSAT, повсеместное их использование, а также полная интеграция терминалов в сферу подвижной связи
- Использование более точных алгоритмов адаптивного выбора кодирования и модуляции с целью повышения эффективности использования спектра.
- Из графика (рис. 3) видно, что DVB-S2X имеет расширенный диапазон спектральной эффективности, поэтому расширяется диапазон отношения сигнал/шум, следовательно в следующих стандартах также будет расширение вышеперечисленных диапазонов для получения максимальной выгоды в зависимости от качества тракта.

Список используемых источников:

1. R. Swinford, B. Grau, High Throughput Satellites //ADL – 2015
2. <https://forumtech.ru/novosti-v-sfere-telekommunikaczij/antenny-vsats> (дата обращения 11.11.2022)
3. Цифровая спутниковая система радиовещания с гибкой конфигурацией (телевидение, звук и данные) Серия ВО Спутниковое Рекомендация МСЭ-R ВО.1784-1 (12/2016)

Nev D., Likontsev A.

The Bonch-Bruевич St. Petersburg State University of Telecommunication

Evaluation of the further development of satellite data transmission standards.

The article discusses methods for improving the quality of data transmission in satellite systems. An assessment of the trend in the development of quality improvement technologies in satellite broadcasting systems has been carried out. The analysis of data transmission standards in the satellite system was also carried out and a comparative model was created in the Simulink environment.

Key words: DVB-S2, DVB-S2, VSAT, FEC, ACM.

УДК 621.396.13
ГРНТИ 49.33.01

АНАЛИЗ ТЕХНИЧЕСКИХ РЕШЕНИЙ, ПРИМЕНЯЕМЫХ В СЕТИ СПУТНИКОВОЙ СВЯЗИ STARLINK

А. Н. Ликонцев, В. А. Осипова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Сеть Starlink интересна тем, что всего за 15 лет, прошедших с момента основания проекта в 2007 году, она стала крупнейшим проектом в области спутниковой связи. Спутниковый сегмент сети Starlink в настоящий момент состоит из более чем 2500 активных спутников, то есть по количеству космических аппаратов уже превосходит все остальные существующие группировки в несколько раз, и это при том, что проект прошел только половину первой фазы развертывания. В докладе рассмотрены некоторые технические решения, использованные Starlink в своем проекте, и которые позволили приступить к его реализации в такие короткие сроки.

спутниковые системы связи, группировка Starlink, технические решения Starlink, серийное производство спутников

Архитектура системы Starlink, так же как и других спутниковых систем связи, состоит из трех основных компонентов: группировки спутников, сети наземных станций и пользовательских терминалов.

В рамках первой фазы компания SpaceX планировала развернуть группировку из 4408 аппаратов, размещенных на орбитах высотой 1100 - 1300 км для работы в Ku/Ka-диапазонах. Второй этап развития системы предполагал создание еще одного созвездия из 7518 аппаратов, которые будут размещены на орбитах высотой 330 – 350 км, работающих в V-диапазоне [1].

Спутники Starlink начали запускать только в 2019 году, и за три года смогли создать группировку из более чем 3000 космических аппаратов [2]. По данным SpaceX, ее производственные мощности позволяют производить до 120 спутников Starlink в месяц, в то время как средний срок производства спутника связи для геостационарной орбиты составляет сейчас 2-3 года. Достичь таких высоких показателей позволило освоение серийного производства спутников, которые впервые начали выпускаться на заводах в промышленных масштабах. До этого изготовление космических аппаратов оставалось фактически ручным трудом, который осуществлялся по индивидуальным проектам, что и обуславливало их высокую стоимость и длительный производственный цикл [1]. Разработка космических аппаратов Starlink изначально велась с учетом группового запуска ракетой Falcon 9, которая за один старт выводила сразу 60 спутников. [3]. Несмотря на то, что изначально планировалось размещение космических аппаратов на высоте 1100 - 1300 км, сейчас большинство из них находится на орбитах высотой 540 – 550 км и наклоном в 53 градуса. Именно такие характеристики орбиты дают возможность решить сразу несколько задач: наклонение в 53 градуса способно обеспечить покрытие территорий, на которых

проживает большая часть населения Земли, а низкие орбиты значительно уменьшают задержку сигнала до конечного потребителя. Для геостационарной орбиты задержка в одном направлении составляет 600-800 мс, в то время как для низкоорбитальных сетей она составляет менее 100 мс. Это позволяет абонентам Starlink работать с такими интернет-приложениями как VPN-туннели, удаленный рабочий стол, компьютерные игры-шутеры, а также совершать телефонные разговоры. Запас топлива на спутнике способен удерживать его на рабочей орбите течение пяти лет. После выработки ресурса спутник изменяет орбиту с круговой на эллиптическую и снижается до 250 км, где, за счет торможения об остатки атмосферы достаточно быстро затормозится и сгорит. Любопытно то, что в случае поломки спутник Starlink так же сможет самостоятельно в течение нескольких лет сойти с рабочей орбиты и сгореть в земной атмосфере, что уменьшит вероятность его столкновения с другими космическими аппаратами. Таким образом, низкая орбита служит своеобразным естественным защитным механизмом.

В процессе реализации в проект вносились изменения, касающиеся как высоты орбиты спутников, так и размещаемого на спутниках оборудования. Так спутники первого поколения v 1.0 имели массу 260 кг и были оснащены только четырьмя антеннами с фазированной решеткой, работающими в Ku и Ka диапазонах для передачи данных на Землю, поскольку работали только как ретранслятор, и автономной системой навигации, позволяющей им самостоятельно выполнять маневры уклонения от потенциально опасных объектов [4].

Первая цепочка из 60 спутников была очень хорошо видна на фоне звездного неба из-за отражающегося от плоских поверхностей солнечного света, и вызвала недовольство со стороны астрономов [3]. Для решения такой проблемы на поверхность спутников стали наносить специальное покрытие, а затем разработали специальный козырек, защищающий антенны от солнечных лучей. Поэтому более поздние спутники v 1.0 получили специальные защитные козырьки, снижающие их блеск на ночном небе. Однако появилась другая проблема, вызывающая беспокойство теперь уже радиоастрономов. Было обнаружено, что спутники будут мешать работе одного из каналов радиотелескопа, затрудняя поиск органических молекул в космосе. В целом проблема светового загрязнения неба очень серьезная и решить её полностью в настоящий момент невозможно [5].

На первом этапе система Starlink работает следующим образом: антенна пользователя посылает сигнал на пролетающий рядом спутник, а тот пересылает его на наземную станцию, которая имеет доступ к интернету или процесс происходит в обратном направлении. Такая схема работает лишь там, где на расстоянии до тысячи километров от абонентского терминала есть наземная станция. Таким образом, площадь океанов выпадает из зоны покрытия. Но это ограничение снимает дооснащение спутников лазерной системой связи. И следующая модификация спутников v 1.5, уже оснащённая лазерной системой связи, позволяет спутникам обмениваться данными между собой, исключая при

этом промежуточные наземные станции из цепочки, снимая таким образом ограничения на расстояние. Управление направлением луча реализуется системой линз, а такая оптическая часть требует достаточно больших габаритов. Из-за дополнительного оборудования масса спутников увеличилась на 35 кг по сравнению с v 1.0. Появились сведения, что на последнем поколении спутников специальные козырьки заменили плохо отражающим свет покрытием нижней направленной на Землю части спутников. Скорее всего, это связано с попыткой снизить стартовую массу космических аппаратов, увеличившуюся после установки на них лазерных приемопередатчиков. Уже ведутся работы над созданием спутников модификации v 2.0, которые должны будут иметь еще большие технические возможности, и будут выводиться на орбиту при помощи нового космического корабля Starship [5].

В наземном сегменте для создания связи между центрами управления, шлюзовыми станциями и абонентскими терминалами проект Starlink в основном использует уже построенные волоконно-оптические сети Google, а шлюзовые станции планирует размещать прямо на зданиях, где находятся центры управления сетью [1]. Место расположения единого общего центра управления, координирующего работу всех шлюзовых станций и всех терминалов, задающего единое время, является самой засекреченной частью спутниковой системы Starlink.

Шлюзовые станции представляет собой комплекс из восьми стоящих рядом поворотных антенн, закрытых специальными радиопрозрачными колпаками. Антенны позволяют совершать обмен данными между спутником и терминалом в обоих направлениях. Сами антенны работают по очереди: четыре из них поворачиваются к пролетающим над ними четырём разным спутникам, остальные четыре в это время возвращаются в исходное положение, чтобы начать ловить сигнал следующего пролетающего спутника.

Спутник своим сигналом покрывает на Земле территорию радиусом около 950 километров. На высоте 550 км он движется с такой скоростью, что время пролета в зоне видимости абонентского терминала составляет всего 4,1 минуту. При выходе спутника из зоны видимости, терминал тут же находит ему замену и переключается на следующий спутник. Сам спутник способен одновременно обслужить множество терминалов [6]. Точной информации о количестве лучей на спутнике StarLink нет, однако специалисты предполагают, что их не более 16 [1], и каждый луч могут ловить несколько абонентов сразу. Почти все технические решения Starlink держатся в секрете, но известно, что первые пользовательский абонентский терминалы имели в своём составе антенну, оборудованную электроприводом, позволяющем антенне вращаться в горизонтальной плоскости на 360 градусов и отклоняться на 60-70 градусов в вертикальной плоскости. Вероятно, поворотом антенны за спутником должна была решаться задача увеличения времени сеанса связи с каждым спутником.

Среди методов доступа абонентского терминала к радиочастотному спектру на спутнике выделяют следующие: с постоянным закреплением полосы частот за терминалом, и доступ по требованию.

Первый метод значительно проще в аппаратной реализации, при этом за каждым терминалом закрепляется определенная часть частотного спектра на спутнике. Преимуществом этого метода является быстрота установления связи – как только антенна терминала наводится на спутник, может начаться передача информации на шлюзовые станции. Недостаток такого метода заключается в том, что спутниковый сегмент используется нерационально, так как большую часть времени абонентский терминал не передает информацию.

Второй метод заключается в доступе нескольких абонентов к одному частотному каналу с временным или частотным разделением. Методы с групповым доступом, несмотря на сложность их реализации и требования синхронизации в отправке пакетов от абонентских терминалов, позволяют в несколько десятков раз эффективнее использовать частотный диапазон сети и передать в десятки раз больше информации (абонентского трафика).

Какой именно метод доступа используется в системе Starlink не известно, но специалисты, внимательно изучающие все находящиеся в свободном доступе материалы, полагают, что в канале используется метод, называемый мультиплексированием с временным разделением каналов (TDMA – Time Division Multiple Access) [1].

Уже достигнутые цифры и масштабы проекта очень сильно выпадают за границы привычного мира спутниковых коммуникаций. В ближайшей перспективе StarLink предстоит решить вопросы с обеспечением стабильной надежной связи с движущимися объектами, например между спутниками или между спутником и самолетом, так как такие системы должны иметь очень точную и быструю систему прицеливания. И, несмотря на то, что задача решается на практике, в проектах подобного масштаба до сих пор никто реализована не была.

Список используемых источников:

1. Энциклопедия Starlink. Глобальная сеть широкополосного спутникового интернета Starlink. [Электронный ресурс]. URL: <https://www.comnews.ru/content/209438/2020-10-07/2020-w41/enciklopediya-starlink#toc19> (дата обращения: 15.11.2022).

2. Список спутников Starlink. [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Список_спутников_Starlink (дата обращения: 15.11.2022).

3. Starlink. Как устроена система глобального спутникового интернета. [Электронный ресурс]. URL: <https://universemagazine.com/ru/starlink-kak-ustroena-sistema-globalnogo-sputnikovogo-interneta/> (дата обращения: 15.11.2022).

4. Starlink: что это за технология и как она влияет на интернет будущего. [Электронный ресурс]. URL: <https://lindeal.com/trends/starlink-chto-eh-to-za-tekhnologiya-i-kak-ona-vliyaet-na-internet-budushchego> (дата обращения: 15.11.2022).

5. Копиев Г. Нужно больше маневров: как спутники Starlink меняют жизнь баллистиков и астрономов [Электронный ресурс]. URL: <https://nplus1.ru/blog/2022/07/12/starlink> (дата обращения: 15.11.2022).

6. Что такое сеть Starlink. [Электронный ресурс]. URL: <https://life.ru/p/1536227> (дата обращения: 15.11.2022).

Likoncev A., Osipova V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of technical solutions used in the Starlink satellite communication network.

The Starlink network is interesting because in just 15 years since the project was founded in 2007, it has become the largest project in the field of satellite communications. The satellite segment of the Starlink network currently consists of more than 2500 active satellites, that is, the number of spacecraft already exceeds all other existing constellations by several times, and this despite the fact that the project has passed only half of the first phase of deployment. The report discusses some of the technical solutions used by Starlink in its project, and which made it possible to start its implementation in such a short time.

Key words: satellite communication systems, Starlink constellation, Starlink technical solutions, mass production of satellites.

УДК 621.396.962
ГРНТИ 47.49.43

ИССЛЕДОВАНИЕ СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИК ОПТИЧЕСКОГО TOF-ДАТЧИКА РАССТОЯНИЯ VL53L0X

Е. И. Червинко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье приведен анализ статистических характеристик датчика расстояния VL53L0X, используемого в разработанном автором в макете оптического лоатора для проведения лабораторных работ

оптические лоаторы, ToF-датчики, Arduino, Embedded

На данный момент продолжается разработка макета оптического лоатора для постановки лабораторных работ на кафедре РОС. В данной системе в качестве излучателя и приемника отраженной ЭМВ инфракрасного спектра был применен ToF-датчик расстояния VL53L1X от STMicroelectronics. В ходе разработки проекта возникла потребность в исследовании статистических характеристик датчика в зависимости от расстояния перед объектом, освещенности среды и степени поглощения ЭМВ материалом объекта. В данной работе приведены исследования статистических характеристик данного датчика и определена зависимость этих характеристик от расстояния. VL53L1X входит в новое поколение высокопроизводительных времяпролетных TOF-датчиков расстояния, основанных на технологии FlightSense. Принцип работы ToF (Time of Flight)-датчиков заключается в следующем: Лазерный диод излучает фотоны, а фотодетектор регистрирует отраженный луч. По времени, за которое фотоны отражаются от объекта и попадают на фотодетектор, датчик определяет расстояние (рис. 1).

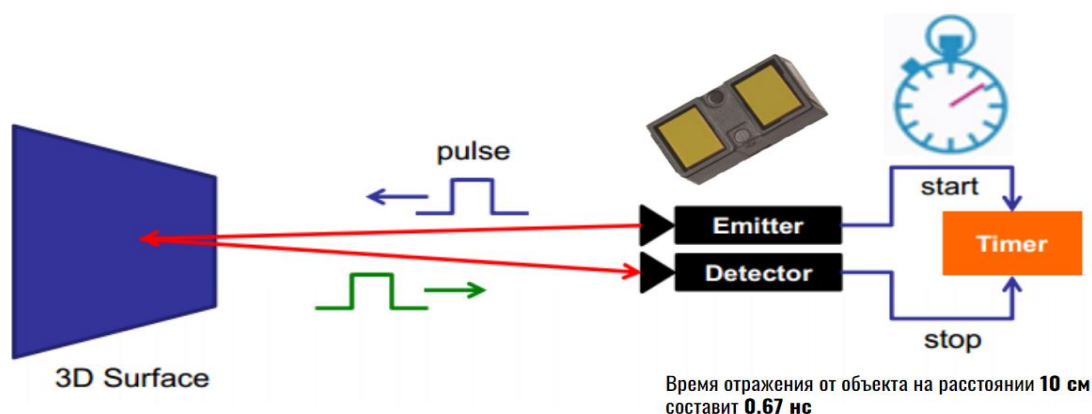


Рис. 1. Принцип работы технологии Time of Flight

VL53L1X способен работать через последовательную дуплексную шину I2C, что позволяет легко настраивать датчик и получать с него готовые значения расстояния управляемым контроллером Arduino. Очевидно, что у датчика

существует погрешность измерений, которая становится больше с увеличением расстояния до объекта. Наличие помех (освещения со спектром излучения, к которому чувствителен датчик. Для исследования статистических характеристик измерений расстояния датчиком VL53L1X требуется знать реальное расстояние до объекта. Чем больше объем выборки однократных измерений этого расстояния, тем точнее можно будет провести изучение характеристик. Для реализации этих измерений был написан код для 1000 замеров и отправки их на компьютер через шину UART. Далее эти данные были перенесены в Excel (рис. 2) с последующим переносом их в среду MathCad(рис. 3). Теперь можно было проводить исследования статистических характеристик датчика VL53L1X.

Дата	10.03.2022		Дата	10.03.2022		Дата	10.03.2022	
Параметры	R до объекта	Освещение	Параметры	R до объекта	Освещение	Параметры	R до объекта	Освещение
	1000	Еств + Иск		500	Еств + Иск		200	Еств + Иск
Величины	n	R	Величины	n	R	Величины	n	R
Объект - Белая пластина	0	1013	Объект - Белая пластина	0	536	Объект - Белая пластина	0	224
	1	1027		1	531		1	228
	2	1006		2	535		2	225
	3	1027		3	533		3	225
	4	1047		4	534		4	227

Рис. 2. Окно Excel с извлеченными из терминала значениями расстояний

```

R11 := (1013 1027 1006 1027 1047 1038 1051 1036 1040 1037 1071 1023 1040 1041 1029 1042 1035 1006 1037 1007
R21 := (536 531 535 533 534 538 531 535 531 537 541 533 541 529 529 536 532 537 536 535 535 534 534 533 5
R31 := (224 228 225 225 227 226 227 225 224 226 225 225 224 224 225 226 226 227 225 228 224 225 228 225 2
R12 := (1032 1038 1033 1044 1048 1047 1031 1037 1034 1033 1023 1027 1031 1020 1028 1047 1049 1010 1023 1025
R22 := (531 540 534 536 534 536 532 541 533 533 528 534 535 530 530 531 539 529 538 536 532 531 531 536 5
R32 := (226 229 229 224 230 226 227 227 227 228 226 225 226 226 226 225 227 226 225 228 228 226 227 225 2
    
```

Рис. 3. Перенесенные в MathCad значения расстояний

Измерения были проведены по следующим 2м критериям:

- 1) Расстояние до объекта перед датчиком - 1000мм, 500мм и 200мм.
- 2) Наличие искусственного освещения в помещении, где производятся измерения.

Так были сформированы 6 векторов R_{nm} , где $n=1,2,3$ – номер расстояния (1 -1000мм, 2 - 500мм, 3 - 200мм), а m - номер наличия искусственного освещения(1 - искусственное освещение присутствует, 2 - отсутствует). После извлечения значений измеренных расстояний была реализована функция гистограммы плотности распределения значений в зависимости от принятого на входе 1000-мерного вектора R_{nm} (рис. 4). На рис. 5 представлена гистограмма ПРЗ при $R = 1000$ мм и количестве столбиков $L = 500$.

$$M := \frac{\sum_{i=0}^{L-1} R_i}{L} = 1.034 \times 10^3$$

$$D := \frac{\sum_{i=0}^{L-1} (R_i - M)^2}{L} = 347.76$$

$$\text{sigma} := \sqrt{D} = 18.648$$

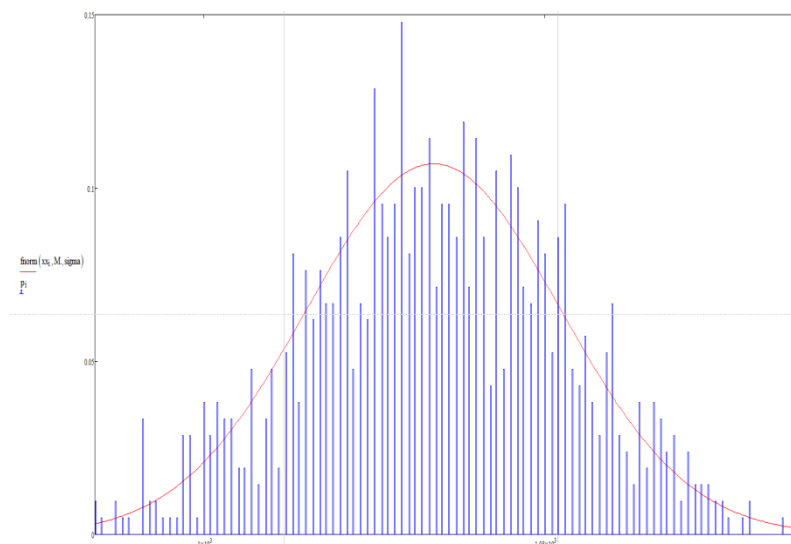


Рис. 6. Формулы нахождения стат. величин и гистограмма PЗ при R =1000мм и L = 500

Для доказательства гауссова закона распределения измеренных расстояний с датчика был использован критерий согласия Пирсона χ^2 . Окно программы MathCAD с вычислением критерия Пирсона представлен на рис. 7 с введенными гипотезами:

- H0 - случайный процесс имеет гауссов закон распределения
- H1 - случайный процесс имеет иной закон распределения

$$\chi_i := \sum_{i=0}^{L-1} \left(\frac{p_i - \text{fnorm}(xx_i, M, \text{sigma})}{\text{fnorm}(xx_i, M, \text{sigma})} \right) = 21.846 \quad \chi_{i_crit} := 27.41585 \quad \text{Из таблицы коэффициентов Пирсона}$$

$\underline{m} := L = 50$
 $r := 2$ потому что есть только 2 параметра у норм. распр
 $k := m - r - 1 = 47$

$\chi_i < \chi_{i_crit}$, значит нулевую гипотезу о нормальном законе распределения принимает при $\alpha=0.99$

Рис. 7. Нахождение критерия Пирсона в среде MathCAD

На рис. 8 приведен график с функциями, где красным отмечены функции плотности распределения без искусственного освещения в помещении во время измерений, синим - с освещением.

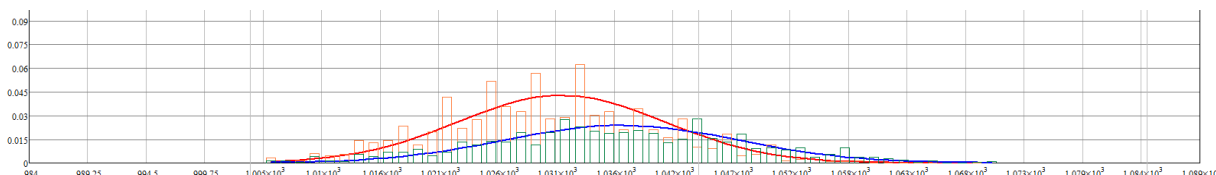


Рис. 8. ЗРСВ при R = 1000 мм (красный - без иск. освещения, синий - с иск. освещением)

По рисунку 8 видно, что наличие освещенности дает некоторое смещение математического ожидания относительно реального значения расстояния. Разумеется, наличие освещения создает помехи для датчика, из-за этого разброс значений расстояния больше, если на момент измерений включены источники освещения. То есть точнее всего датчик работает в темноте. В последствии были

проведены вычисления для реализаций графиков функций распределения для разных расстояний (200, 500, 1000 мм) до датчика (рис. 9).

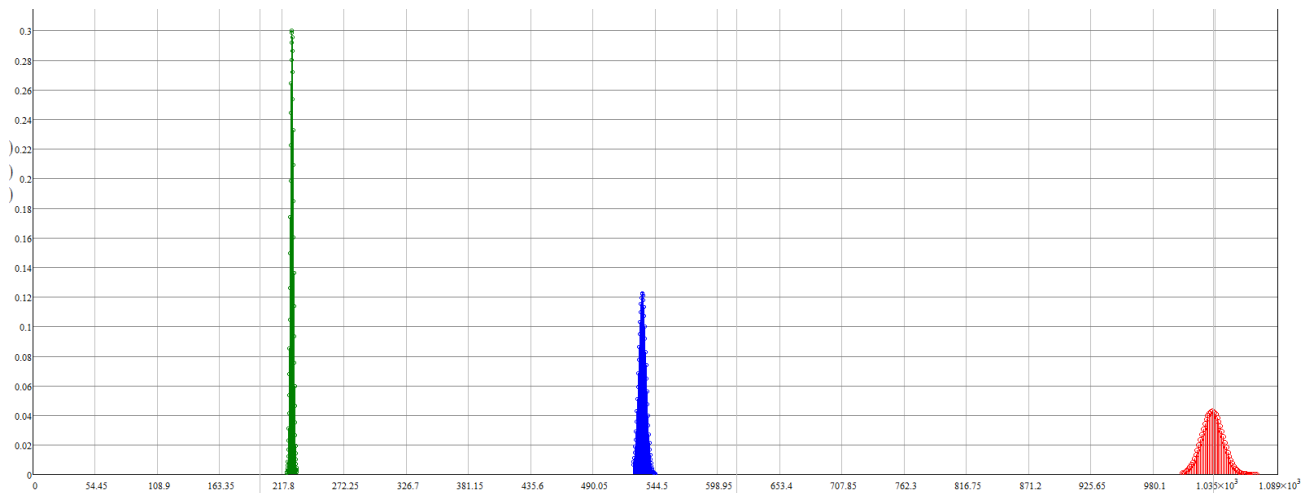


Рис. 9. ЗРСВ при $R = 200, 500$ и 1000 мм

В работе были исследованы статистические характеристики датчика VL53L1X, определена высокая степень зависимости погрешностей датчика от наличия освещения в помещении с датчиком на момент измерений, выявлена зависимость разброса значений измеренных расстояний от самого расстояния.

Список используемых источников:

1. Лазерные датчики ST: измерение расстояния до объекта стало более надежным и быстрым [сайт]. URL: <https://www.compel.ru/lib/142189/> (дата обращения: 13.11.2022 г.).
2. Для 3D-систем: датчик света и приближения VL6180 [сайт]. URL: <https://www.compel.ru/lib/73675/> (дата обращения: 13.11.2022 г.).
3. Arduino Uno [сайт]. URL: <http://arduino.ru/Hardware/ArduinoBoardUno> (дата обращения: 13.11.2022 г.).
4. Основные сведения о протоколе UART [сайт]. URL: https://www.rohde-schwarz.com/ru/products/test-and-measurement/oscilloscopes/educational-content/understanding-uart_254524.html (дата обращения: 13.11.2022 г.).

Chervinko E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Investigation of statistical characteristics of the optical ToF distance sensor VL53L0X.

The article presents an analysis of the statistical characteristics of the VL53L0X distance sensor used in the optical locator layout developed by the author for laboratory work.

Key words: *optical locators, ToF sensors, Arduino, embedded-development.*

Секция 2.5.
Цифровая обработка сигналов

УДК 621.397.132.59
ГРНТИ 47.14.03

РАЗРАБОТКА МОДУЛЯ ПРИЁМА ЦИФРОВОГО ВИДЕОПОТОКА НА ПРОГРАММИРУЕМОЙ ЛОГИЧЕСКОЙ ИНТЕГРАЛЬНОЙ СХЕМЕ

А. К. Лебедев, И. Н. Чернов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В системах передачи видеоданных используются различные протоколы. Для удобства обработки видеоданных используют системы преобразования протоколов. В настоящем докладе приведена работа по созданию модуля преобразования стандартов BT601, BT656 в стандарт Avalon-ST с использованием языка проектирования System Verilog для программируемой логической интегральной схемы.

ПЛИС, видеосигнал, System Verilog, BT601, BT656, Avalon-ST

В системах обработки видео стремятся к единому виду передачи потока данных, но это не всегда возможно. Потому что различные устройства используют различные стандарты. Для удобства соединения этих устройств в одну систему потоки данных приводят к единому виду.

В данной работе рассматривается преобразование стандартов BT601 и BT656 в стандарт фирмы Intel Avalon-ST.

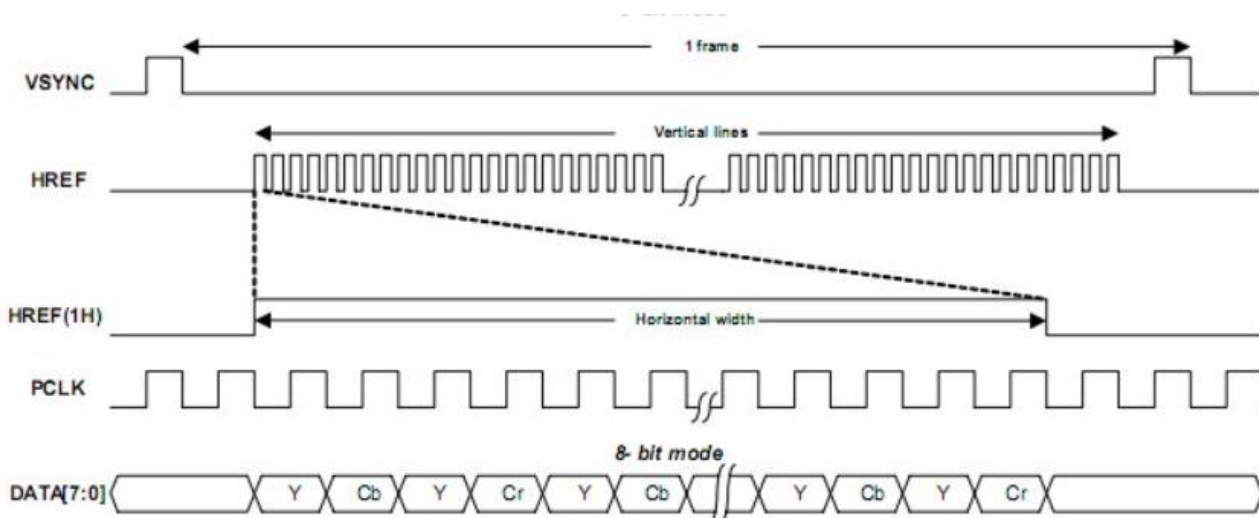


Рис. 1. Диаграмма передачи данных кадра по стандарту BT601.

Стандарт BT601 предлагает передавать данные с отдельным выводом для строчной и полевой синхронизации [1]. Пример диаграммы передачи данных по стандарту BT601 приведен на рис. 1.



Рис. 2. Диаграмма передачи данных кадра по стандарту BT656.

Стандарт BT656 имеет встроенные в поток данных опорные сигналы синхронизации. По ключевым словам, определяется информация о строке или поле [2]. Пример диаграммы передачи данных по стандарту BT656 приведен на рис. 2.

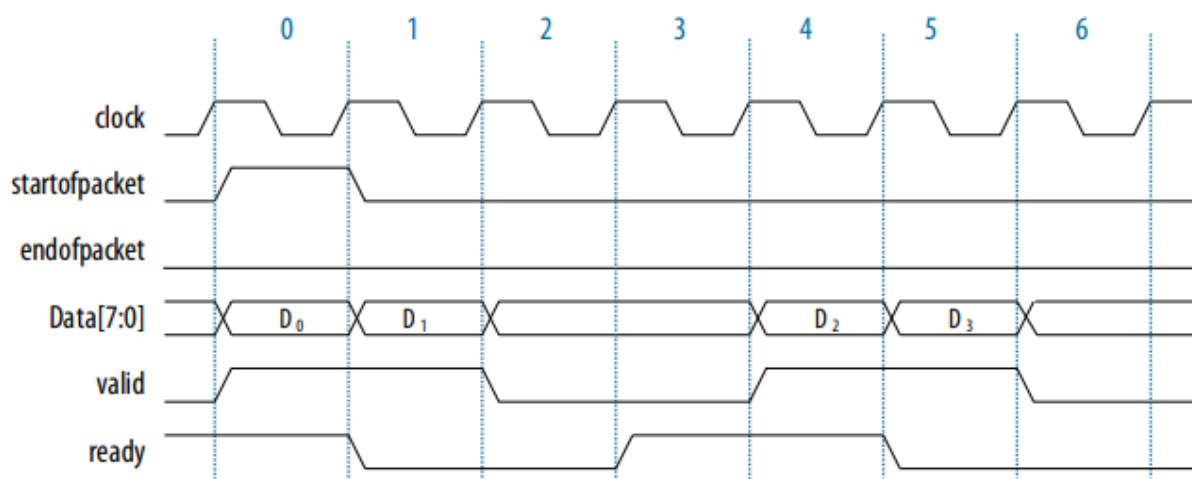


Рис. 3. Диаграмма передачи данных кадра по стандарту Avalon-ST.

Стандарт Avalon-ST использует контрольные пакеты для определения параметров кадра, а также самих данных кадра. Пример диаграммы передачи данных по стандарту Avalon-ST приведен на рис. 3. К контрольным пакетам можно добавлять пользовательские пакеты, что даёт больше возможностей для управления данными кадра [3]. Пример расположения пользовательских пакетов приведен на рис. 4.

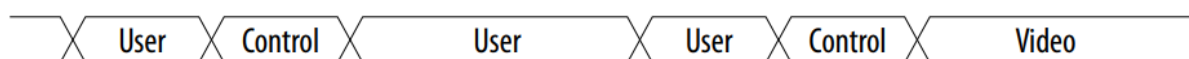


Рис. 4. Рекомендуемое стандартом расположение пакетов в потоке.

Приведение потоков данных к одному виду позволяет эффективнее использовать ресурсы интегральной схемы и обеспечивает удобство работы с

внутренними интерфейсами системы, которые играют важную роль в обработке информации.

Разрабатываемый модуль, приведённый на рис. 5, предназначен для приёма видео в стандартах BT601 или BT656, и преобразования в Avalon-ST на ПЛИС с использованием языка проектирования System Verilog. Использование этого модуля позволяет отказаться от платных аналогов, требующих лицензию Intel.

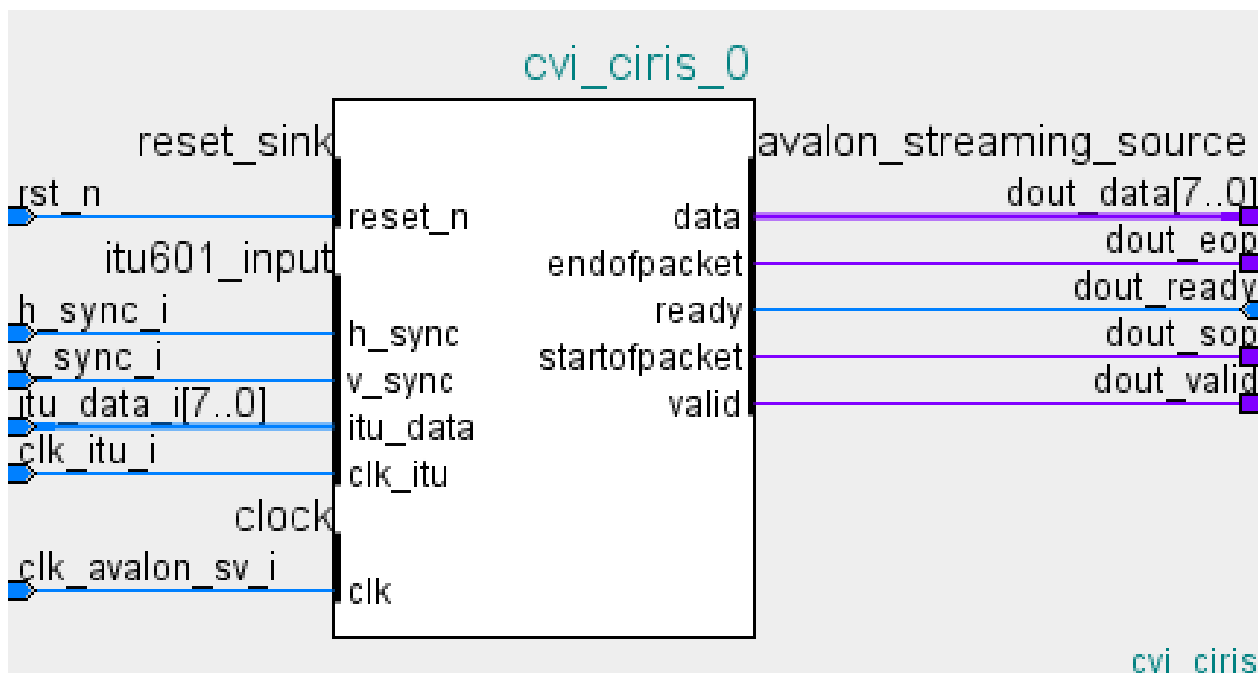


Рис. 5. Рекомендуемое стандартом расположение пакетов в потоке.

Разработка модуля включает следующие этапы:

- Изучение особенностей стандартов BT601, BT656, Avalon-ST;
- Рассмотрение существующих алгоритмов преобразования потоков;
- Разработка модуля на языке System Verilog для ПЛИС;
- Написание testbench для проверки корректности работы модуля, отладка, как общих, так и отдельных ситуаций;
- Проверка модуля с использованием камеры и отладочной платы и конечная отладка.

Использование современного языка проектирования цифровых устройств System Verilog позволяет использовать различные тестовые конструкции, которые облегчают моделирование и отладку работы модуля. Моделирование производится с использованием среды Questa Sim. Пример моделирования приведен на рис. 6.

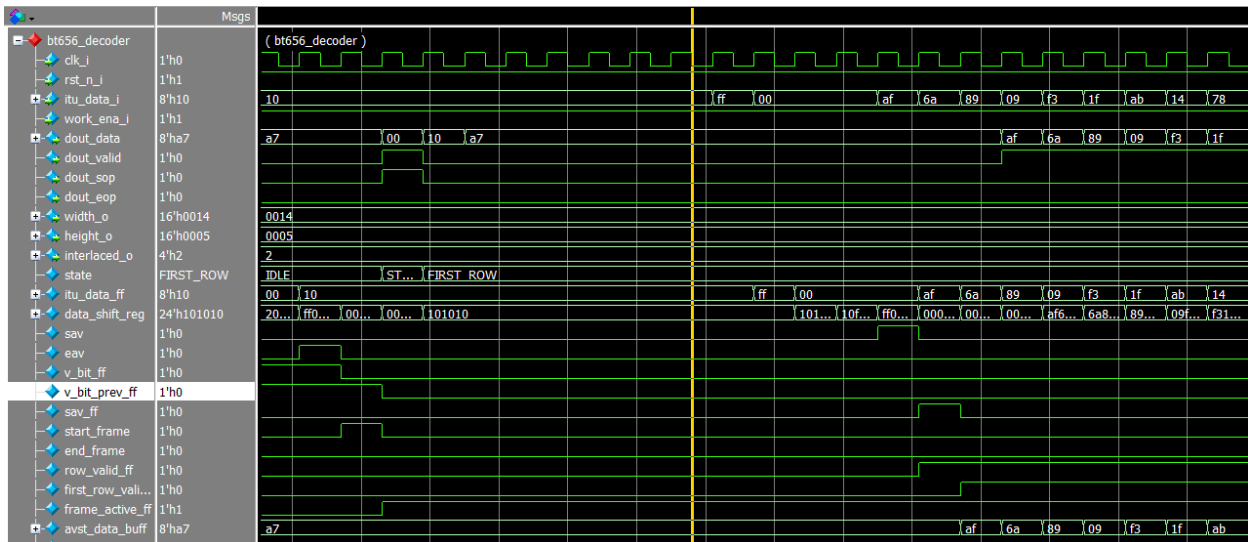


Рис. 6. Результаты моделирования модуля в процессе отладки в среде Questa Sim

Разработанный модуль является универсальным за счет своей архитектуры, которая исключает использование модулей различных производителей ПЛИС, что даёт возможность применять его в устройствах различных фирм. Не менее важным фактом является и наличие параметризации модуля, которая позволяет выбирать ширину входных данных, формат кадра и стандарт, по которому будет передаваться видеопоток не меняя код, а лишь выбирая параметры в графическом интерфейсе САПР, через которую производится сборка проекта на ПЛИС.

Таким образом, при дальнейшем развитии модуля можно сделать выбор выходного протокола с возможностью замены интерфейса Avalon-ST на интерфейс AXI, который в последнее время набирает популярность среди разработчиков.

Список используемых источников:

1. Recommendation ITU-R BT.601-7. - The ITU Radiocommunication Assembly. - 2017.
2. Recommendation ITU-R BT.656-5. - The ITU Radiocommunication Assembly - 2017
3. Video and Image Processing Suite User Guide. Intel, Ink. 2021.02.12

Lebedev A., Chernov I.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Development of a digital video stream reception module on a programmable logic integrated circuit.

Various protocols are used in video transmission systems. For the convenience of video data processing, protocol conversion systems are used. This report presents work on the creation of a module to convert the standards BT601, BT656 to Avalon-ST standard using the System Verilog design language for programmable logic integrated circuit.

Key words: *FPGA, video signal, System Verilog, BT601, BT656, Avalon-ST.*

УДК 62.519
ГРНТИ 47.63.29

РАЗРАБОТКА СИСТЕМЫ УДАЛЕННОГО УПРАВЛЕНИЯ СТЕНДОВЫМ ОБОРУДОВАНИЕМ

Г. А. Михаль, И. В. Муравьёва, И. Н. Чернов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время всё чаще появляется необходимость в удалённой работе. Реализация системы удалённого контроля стендовым оборудованием позволит оптимизировать процесс работы с устройствами различных предприятий, связанным с разработкой программно-аппаратных средств или проводящим учебно-просветительскую деятельность. В докладе описан первый этап разработки данной системы - модуль взаимодействия сервера с платой esp32 по https протоколу.

микроконтроллер Esp-32, стендовое оборудование, REST API, автоматизация, React

В настоящее время учебные заведения осуществляют образовательный процесс с использованием новейших достижений техники. Благодаря этому развиваются более эффективные подходы к обучению и совершенствованию методики преподавания. В силу появления современного программного обеспечения, микроконтроллеров и печатных плат появилась возможность объединить их в одно устройство, которое бы обеспечивало управление стендовым оборудованием.

Схема работы удаленного управления стендовым оборудованием подразумевает передачу данных со стендового оборудования по беспроводной сети на сервер с последующей обработкой и визуализацией в клиентских приложениях – пользователи получают картину работы стенда в реальном времени, а также могут формировать отчеты о состоянии оборудования за определенный временной интервал.

Дистанционное управление оборудованием позволяет выполнять следующие задачи:

1. Автоматизация учебного процесса;
2. Контроль работы стенда в реальном времени - вся информация, поступающая от объектов, сохраняется в базе данных и может быть использована для анализа и отчетов;
3. Возможность управления стендом на любой удаленности.

В качестве одного из основополагающих элементов стенда используется микроконтроллер esp-32. Микросхема представляет собой систему на кристалле с интегрированным Wi-Fi и Bluetooth контроллерами. Отличительными особенностями esp-32 является развитая периферия, хорошие вычислительные способности и низкая цена [1]. На рис. 1 представлена распиновка модуля esp-32.

В качестве языка программирования используется JavaScript. Это обеспечивает гибкость работы клиентского ПО: для работы удаленного пользователя необходим только стандартный Интернет-обозреватель, осуществляющий загрузку (с сервера системы) и исполнение JavaScript кода, реализующего пользовательский интерфейс для дистанционного управления лабораторным стендом.

Внешние пользовательские интерфейсы создаются с помощью библиотеки JavaScript – React. Сильнейшей стороной React [5] является то, что все компоненты пользовательского интерфейса могут быть выражены в виде наборов чистых функций. Для перерисовок React использует Virtual DOM. Это позволяет обновлять только изменившиеся узлы DOM-дерева, вместо перерисовки всей страницы. Благодаря этому разработка не расходует лишние ресурсы.

Первый этап разработки удаленного управления стендовым оборудованием заключается в разработке модуля взаимодействия сервера с платой esp32 по https протоколу. Главным преимуществом https является то, что этот протокол делает ваш сайт более безопасным для пользователей. Он защищает передачу информации от пользователя сайту. Это особенно важно для тех ресурсов, где требуется вводить данные кредитной карты или другие персональные сведения.

Таким образом, современный уровень развития телекоммуникационных технологий и средств предоставляет широкие возможности, связанные с передачей данных на большие расстояния, создание распределенных приложений, работающих через сеть, обмен аудио и видео информацией и многое другое. Подобные достижения в последнее десятилетие стали возможными благодаря интеграции компьютерных систем с сетевыми технологиями. Результатом выполнения данной работы является система удаленного управления стендовым оборудованием. Данная разработка позволит автоматизировать учебный процесс. Студент получит возможность авторизоваться в приложении и получить доступ к лабораторному стенду для учебных целей. На рис. 3 показано взаимодействие клиента, платы и сервера.

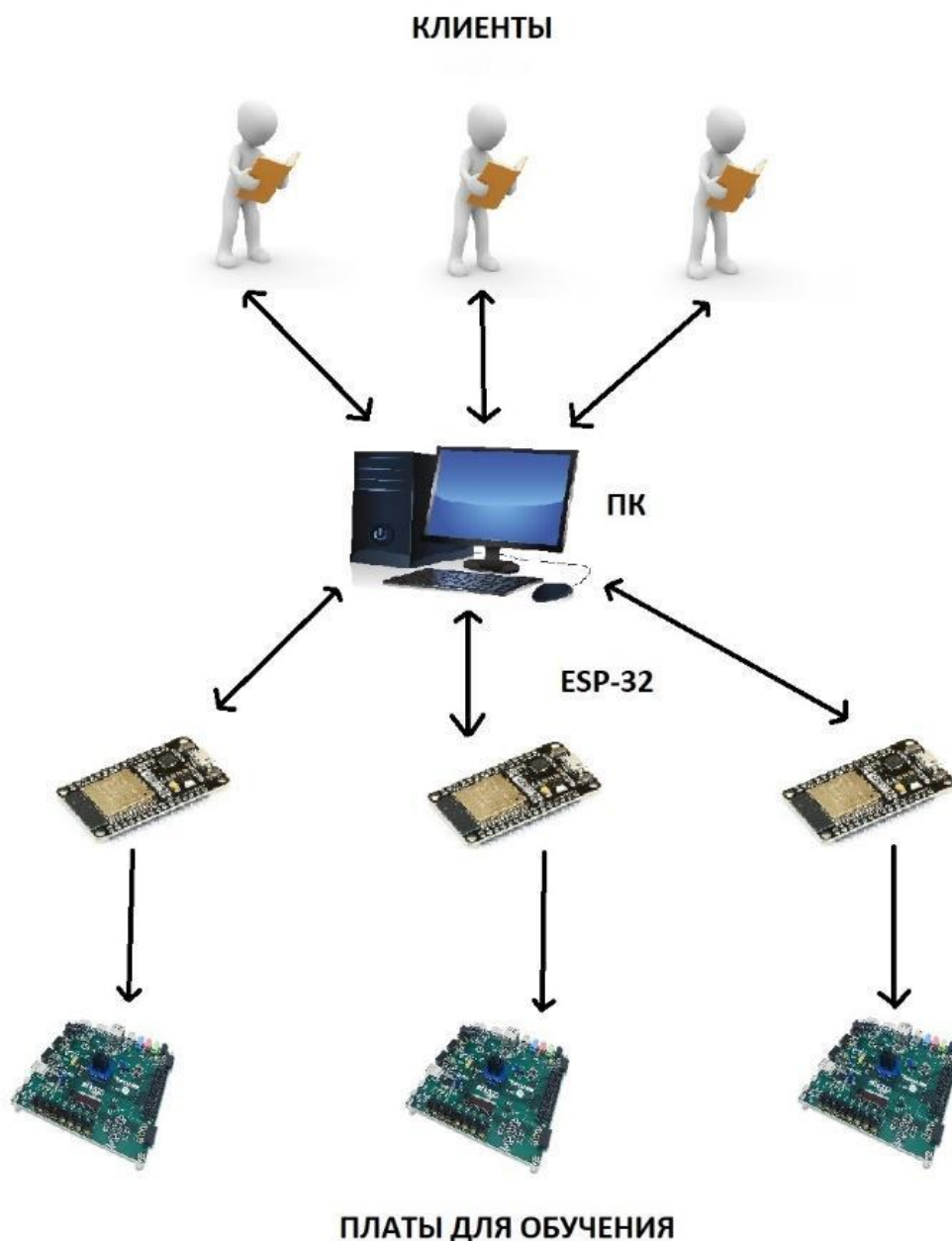


Рис. 3 Взаимодействие клиента, платы и сервера

Список используемых источников:

1. Документация микроконтроллера Esp-32 [Электронный ресурс]. URL: https://www.espressif.com/sites/default/files/documentation/esp32_technical_reference_manual_en.pdf (дата обращения 19.11.2022).
2. Арно Л. Проектирование веб-API. 2020 г., страницы 92-94
3. Документация REST API [Электронный ресурс]. URL: https://www.cs-cart.ru/docs/4.6.x/developer_guide/api/ (дата обращения 19.11.2022).
4. Арно Л. Проектирование веб-API. 2020 г., страницы 79-81
5. Документация React [Электронный ресурс]. URL: <https://ru.react.js.org/docs/getting-started.html> (дата обращения 19.11.2022).

Michal G., Muravyova I., Chernov I.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Remote control system development for stand equipment.

Nowadays, there is an increasing need for remote work. The implementation of a remote control system for bench equipment will optimize the process of working with devices for various enterprises associated with the development of software and hardware or conducting educational activities. The paper describes the first stage of development of this system - the server interaction module with the esp32 board via the https protocol.

Key words: microcontroller Esp-32, stand equipment, REST API, automation, React.

**Секция 2.6.
Экология формирования информационного пространства**

УДК 330.5.051
ГРНТИ 87.35.29

ПРИРОДНО-РЕСУРСНЫЙ ПОТЕНЦИАЛ СМОЛЕНСКОЙ ОБЛАСТИ И ЕГО ИНТЕГРАЛЬНАЯ ОЦЕНКА

М. В. Белоцерковский

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Природные ресурсы являются важной частью экономического потенциала региона, правильная оценка предопределяет рациональность использования и добычи этих ресурсов. Также, определение ресурсного потенциала региона предоставляет возможность разработки стратегии устойчивого развития региона. В публикации проводится оценка ресурсообеспеченности Смоленской области на душу населения и выявление перспектив развития экономики, промышленности и освоения ресурсной базы в соответствии с территориальным положением.

природные ресурсы, общераспространенные полезные ископаемые, ресурсообеспеченность

Смоленская область расположена в центральной части Восточно-Европейской равнины на западе Европейской части России. Имеет границы: на севере и северо-западе Тверской с и Псковской областями, на востоке - с Калужской и Московской областями, на юго-востоке - с Брянской областью, на юге и на западе область имеет государственную границу с Республикой Беларусь, Витебской и Могилевской областями. Общая площадь территории - 49,8 тыс. км² (7,6% площади Центрального округа). Численность постоянного населения Смоленской области на 1 января 2022 года составила 909,9 тыс. человек [1].

Забор воды из водных объектов за 2021 год составил 147,67 млн.м³. Из общего объема использованной воды 33,3% (44,87 м³) используется на хозяйственно-питьевые нужды, 63,4% (85,3 млн. м³) на производственные нужды, 3,3 % (4,4 млн.м³) на нужды сельскохозяйственного водоснабжения, прочие нужды и рыбного хозяйства. 51,08% (68,74 млн. м³) от общего объема использованной воды приходится на предприятия по производству и распределению электроэнергии [2].

Земли с/х назначения имеют площадь: 2219,9 тыс. га. Это 44,6 % от общей площади Смоленской области. Общая площадь лесов Смоленской области по состоянию на 01.01.2022 года составляет 2186,5 тыс. га, лесистость области – 41,8%. Это средний показатель для Центрального федерального округа. Общий запас древесины в тысячах метрах кубических: 300201,7 [3].

Главенствующее место в структуре минерально-сырьевой базы Смоленской области занимают бурый уголь, песчано-гравийный материал, огнеупорная глина, цементное сырье, сапропели, торф и строительные камни. В структуре добычи (кроме подземных вод) основная доля приходится на песчано-гравийный материал (89,9 %) и песок строительный (6,2 %). По объему добычи песчано-

гравийного материала Смоленская область занимает одно из первых мест в Центральном федеральном округе (25% от суммарного объема добычи на территории ЦФО).

Общераспространенные полезные ископаемые четвертичных отложений являются большей частью разведанных запасов.

Подземные воды полностью обеспечивают питьевые и хозяйственно-бытовые потребности населения. Текущая и перспективная потребности Смоленской области полностью обеспечены как прогнозными ресурсами, так и эксплуатационными запасами.

Всего на территории области выявлено, оценено и разведано 9 месторождений минеральных подземных вод и рассолов с запасами 1042 м³/сутки, из них прошли государственную экспертизу запасы в количестве 462 м³/сутки по категориям А+В. В пределах Смоленской области минеральные подземные воды используются ограниченно, хотя их ресурсы значительны, а возможная сфера применения очень широка.

На территории Смоленской области сформировано 53 рыбоводных участков (РВУ) из них переданы рыбоводным хозяйствам в пользование 38. Рыбоводными хозяйствами в 2021 г. выпущено 41737 шт. посадочного материала и осуществлён вылов 39,34 тонн товарной рыбы. Передовиками в рыбохозяйственной деятельности являются две компании:

1. АО «Смоленскрыбхоз» - была произведена в 2021 г. 191 тонна товарной рыбы;

2. ООО «Садки» - в 2021 г. было произведено 328 тонн рыбы осетровых пород.

Также, на территории области имеется национальный парк «Смоленское Поозерье». Был основан в 1992 году, площадь парка: 146,3 тыс. га. Ландшафты представлены моренно-холмистыми, зандровыми и озёрными равнинами с различными формами ледникового и водно-ледникового рельефа на границе расположения Валдайского оледенения. Охватывает бассейн р. Ельша, притока р. Межа (басс. Зап. Двины). Имеется на территории парка 30 больших и малых озёр, соединённых протоками. В озёрах и реках водится до 28 видов рыб. Сохранились археологические памятники каменного, бронзового и железного веков [4].

ТАБЛИЦА 1. Обеспеченность Смоленской области ресурсами на душу населения (2021)

Субъект федерации	Территория, км. кв./чел	С/х угодья, га/чел	Площадь лесничества, га/чел	Запас древесины, м ³ /чел	Рыбные ресурсы, т/чел
Смоленская область	0,055	0,242	2,189	329,928	0,00057039

ТАБЛИЦА 2. Обеспеченность Смоленской области полезными ископаемыми на душу населения

Уголь бурый, тыс. т./ чел.	Торф, т./ чел.	Запасы питьевых подземных вод м3/сутки./ чел.	Минеральные воды м3/сутки./ чел.	Керамическое сырье м3/чел	Песчано-гравийный материал м3/чел	Песок строительный м3/чел
1,64	513,7	0,73	0,00114518	82,5277503	465,107155	71,9518628

В таблице 1 и таблице 2 представлены результаты расчета ресурсообеспеченности на душу населения. По этим данным была произведена оценка относительной обеспеченности по отдельным ресурсам, результаты представлены в таблице 3.

ТАБЛИЦА 3. Относительная обеспеченность Смоленской области по отдельным видам ресурсов, балл

С/х угодья	Запас древесины	Рыбные ресурсы	Буры й уголь	Нефть	Природный газ	Медная руда	Марганцевая руда	Железная руда	Итого
2	1	1	2	0	0	0	0	0	6

Хоть на территории области не имеются важные ресурсы федерального значения (нефть, природный газ, металлы), это компенсируется обилием ресурсов регионального назначения.

Исходя из приведенных выше фактов можно сделать вывод, что Смоленская область занимает важное место в Центральном Федеральном Округе по объему ресурсов строительных материалов. И также имеет большой потенциал по строительным ресурсам, потому что освоена малая часть месторождений, имеется большая часть потенциальных месторождений с огромными запасами ресурсов. По количеству разведанных запасов торфа область занимает четвертое место в Центральном федеральном округе, это хороший показатель, так как торф благодаря своим свойствам имеет много сфер применения и относительно дешевую стоимость добычи. Также область не использует весь свой потенциал минеральных вод, есть возможность включения в более активное хозяйственное использование в будущем.

Таким образом, благодаря своему географическому положению и располагая необходимыми территориальными и сырьевыми ресурсами, Смоленская область является одним из самых перспективных и ценных регионов для развития обрабатывающей и строительной промышленности.

Список используемых источников:

1. Государственный доклад «О состоянии и об охране окружающей среды Российской Федерации в 2020 году» [Электронный ресурс]. URL: https://www.mnr.gov.ru/docs/gosudarstvennye_doklady/ (дата обращения 25.10.2022).
2. Доклад «О состоянии и об охране окружающей среды Смоленской области в 2021 году» [Электронный ресурс]. URL: <https://prirod.admin-smolensk.ru/doklad-o-sostoyanii-i-ohrane-okruzhayuschej-sredy-v-smolenskoj-oblasti/> (дата обращения 25.10.2022).
3. Природа России. Национальный портал / создан Национальным информационным агентством «Природные ресурсы» (НИА-Природа) [Электронный ресурс]. URL: <http://www.priroda.ru> (дата обращения 25.10.2022).
4. Национальный парк Смоленское поозерье [Электронный ресурс]. URL: <http://www.poozerie.ru/about/ustav-parka/kadastruvaya-informaciya/> (дата обращения 25.10.2022).

Belotserkovsky M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Natural Resource Potential of Smolensk areas and it is integral Assessment.

Natural resources are an important part of the economic potential of the region a correct assessment determines the rationality of the use and extraction of these resources. The determination of the resource potential of the region provides an opportunity to develop a strategy for the sustainable development of the region. The publication assesses the resource availability of the Smolensk region per capita and identifies prospects for the development of the economy, industry and the development of the resource base in accordance with the territorial situation.

Key words: natural resources, common minerals, resource availability.

УДК 691.619.8
ГРНТИ 87.15.15

ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ МИНЕРАЛОВАТНОГО ПРОИЗВОДСТВА

Н. М. Загребаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрены основные разновидности минеральной ваты и показаны преимущества каменной ваты по ряду технических характеристик. Проведен детальный анализ технологических особенностей производства каменной ваты. Выявлен ряд экологических преимуществ, присущих данной технологии. Показано, что реализация такого процесса позволяет сократить расходы предприятий на закупаемое исходное сырье, количество образуемых отходов и обеспечить практически полный рециклинг и использование низкоконцентрированных фенолформальдегидных смол в составе связующего.

минераловатное производство, каменная вата, экологическая безопасность, фенолформальдегидные смолы, рециклинг

Минеральная вата – это волокнистый материал, применяемый для тепловой изоляции, для изоляции высокотемпературных поверхностей, огнезащиты конструкций, а также звукоизоляции. В зависимости от исходного сырья существуют следующие разновидности минеральной ваты [1]:

- Стекланная вата (стекловата) – минеральная вата, полученная в основном из расплава природного песка или стекла;
- Каменная вата - минеральная вата, полученная преимущественно из расплава изверженных горных пород;
- Шлаковая вата (шлаковата) - минеральная вата, полученная из расплава доменного шлака.

Стоит отметить, что как правило, когда говорят о минеральной вате, подразумевается именно каменная вата.

Суть технологии производства данных видов материалов одинакова – исходное сырье плавится в плавильном аппарате (как правило это печь-вагранка), затем полученный расплав вытягивается в волокна, из которых формируется будущая продукция.

Однако, в деталях кроются отличия, которые влияют непосредственно на основные характеристики производимой продукции. Сравнение видов минеральной ваты по техническим характеристикам [2] представлено в таблице 1.

ТАБЛИЦА 1. Сравнительный анализ основных технических характеристик видов минеральной ваты

Наименование параметра	Стекловолоконная вата	Каменная вата	Шлаковая вата
Толщина волокон, мкм	от 5 до 15	От 3 до 5	От 4 до 12
Длина волокон, мм	от 15 до 50	До 16	До 16
Плотность материала, кг/м ³	Не более 130	От 25 до 220	От 75 до 400
Коэффициент теплопроводности, Вт/(м ² *К)	0,038-0,046	0,035-0,042	0,46-0,048
Температурный диапазон использования, °С	От -60 до +450	От -180 до +700	От -60 до 250
Класс огнестойкости (НГ/Г)	негорючие	негорючие	негорючие
Коэффициент звукопоглощения	0,8-0,92	0,75-0,95	0,75-0,82
Влагопоглощение, (% от массы за 24 ч)	<1.7	<0.095	<1.9
Колкость	да	нет	да

Исходя из представленных характеристик, можно сделать вывод о явном преимуществе каменной ваты над остальными видами, в связи с чем данная продукция является наиболее востребованной на рынке сбыта.

Технология производства каменной ваты заключается в следующем. Сырьё – каменный материал (щебень, доломит, габбро-диабаз, известняк) – и энергоноситель (кокс) в соответствии с рецептурой непрерывно дозируются в плавильный аппарат (вагранку), где разогреваются до температуры плавления 1400-1600 °С. Температура плавления регулируется системой охлаждения, где в качестве охладителя выступает вода.

Поскольку технология производства аналогична металлургическому, но с обратными процессами, каждые несколько часов из вагранки осуществляется слив сплава металлов, содержащихся в каменном сырье, в изложницу, где застывает и получают слитки.

Далее, полученный расплав по системе натекания подается на установку волокнообразования – центрифугу, которая предназначена для преобразования струи расплава в минеральные волокна с нанесением на их поверхность путем распыления раствора связующего, обеспечивающего в последствии скрепление волокон между собой. В качестве связующего используются фенолформальдегидные смолы, которые обеспечивают надежное скрепление волокон между собой и их стойкость к повышенным температурам, а также обеспыливающие и гидрофобизирующие эмульсии.

После центрифуги сильный поток воздуха вытягивает волокна и перемещает их в камеру волокносаждения, где происходит формирование первичного слоя. После чего ковёр каменной ваты раскладывается и сжимается до необходимых параметров путем прессования. Затем, влажная каменная вата поступает в камеру полимеризации, где происходит полимеризация раствора связующего под воздействием горячих циркулирующих газов.

После камеры полимеризации ковёр каменной ваты охлаждается и поступает на распиловку по заданным параметрам готовой продукции. Сформированные плиты каменной ваты укладываются стопками и упаковываются в несколько слоёв упаковочной пленки с нанесением маркировки. После чего, готовая продукция отгружается потребителю.

Графически схема производства каменной ваты представлена на рис. 1.

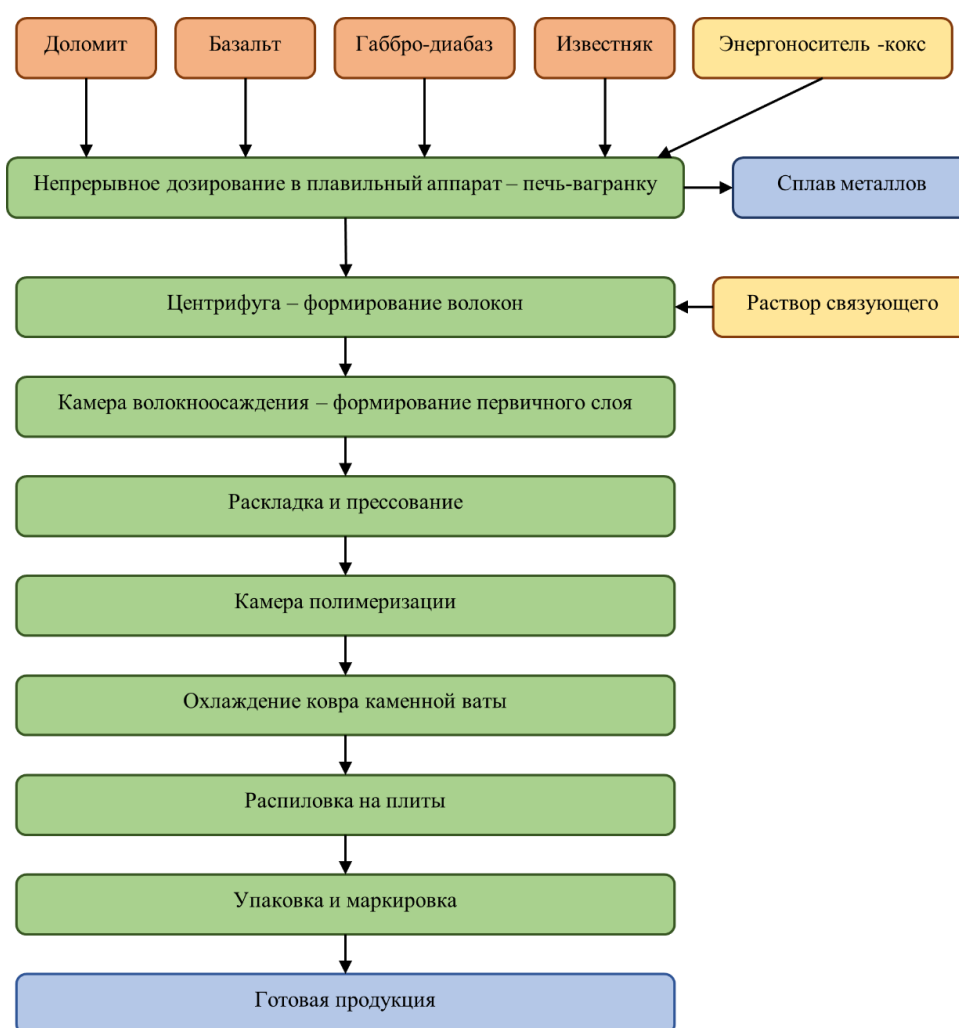


Рис. 1. Схема производства каменной ваты

Одним из достоинств, обеспечивающего экологическую безопасность данного производства, является его безотходность. Как правило, производители каменной ваты, стремясь получить наибольшую экономическую выгоду от своего производства, задействуют механизмы, приводящие также и к экологической безопасности. Речь идёт об использовании отходов в производственном процессе.

Ошметки влажной ваты, обрезки, возвратные края, брак продукции, фильтры и пыль от газоочистки – повторно используются в производстве. Отходы измельчаются, смешиваются с цементом и водой, а из полученной смеси на специальных установках изготавливаются брикеты, которые в дальнейшем дозируются в плавильный аппарат совместно с каменным материалом.

Данная технология позволяет не только сократить расходы предприятий на закупаемое исходное сырье, но также сократить количество образуемых отходов, вплоть до 100% рециклинга собственной продукции.

В части загрязнения атмосферного воздуха технология производства также претерпела ряд изменений, приведших к повышению экологической безопасности. В минераловатном производстве в качестве связующего применяется фенолформальдегидная смола, обладающая низкой теплопроводностью, высокими сцепляющими свойствами к различным материалам. Также, смола обеспечивает каменной вате негорючие свойства, что позволяет производителям успешно конкурировать на рынке с дешевым, но весьма пожароопасным пенополистиролом [3].

Фенолформальдегидные смолы составляют порядка 2% от общего объема используемого сырья. Технология производства такова, что последние 10 лет используются смолы с наименьшим содержанием свободных фенола и формальдегида, что существенно снижает их значения в составе выбросов в атмосферу – при переходе с концентрированных смол на более экологичные, выброс фенола снизился на 50%, формальдегида – на 85%. Применение таких смол осуществляется также и для того, чтобы избежать возникновения в готовой продукции участков уплотнения ваты с высоким содержанием связующего, поскольку в дальнейшем это приводит к окислению свободного фенола (как правило данный процесс происходит за сутки) и возникновению хинона, что в дальнейшем обуславливает появление «фенольных пятен» на плитах и потере потребительских свойств.

Таким образом, экологическая безопасность производства каменной ваты достигается путем модификации технологии производства, включающей в себя практически стопроцентный рециклинг и использование низкоконцентрированных фенолформальдегидных смол в составе связующего.

Каменная вата отличается от остальных видов продукции минераловатного производства не только техническими преимуществами, но и более экологичной технологией изготовления.

Список используемых источников:

1. ГОСТ 31913-2011 (EN ISO 9229:2007). Материалы и изделия теплоизоляционные. Термины и определения. – Введ. 2013-07-01. – Москва: Стандартинформ: Изд-во стандартов, 2013. 24 с.
2. Виды минеральной ваты и их характеристики [Электронный ресурс]. URL: <https://www.econel.ru/mineralnaya-vata/> (дата обращения 15.10.2022).
3. Кузнецова О. Н. Пропиточная композиция для теплоизоляционного материала на основе базальтового волокна // Вестник Казанского технологического университета. 2012. С. 129-131.

Zagrebaeva N.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Environmental safety of mineral wool production.

This article discusses the main varieties of mineral wool and shows the advantages of stone wool in a number of technical characteristics. A detailed analysis of the technological features of stone wool production was carried out. A number of environmental advantages inherent in this technology have been identified. It has been shown that the implementation of such a process reduces the costs of enterprises for the purchased raw materials, the amount of waste generated and ensures almost complete recycling and the use of low-concentration phenol-formaldehyde resins in the binder.

Key words: *mineral wool production, stone wool, environmental safety, phenol-formaldehyde resins, recycling.*

УДК 614.7
ГРНТИ 87

БЛОЧНО МОДУЛЬНАЯ ВОДООЧИСТНАЯ СТАНЦИЯ

А. А. Карпекин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Проблема загрязнения воды является актуальной на протяжении последних нескольких лет. Загрязнение поверхностных водоемов промышленными стоками не позволяет использовать ее в качестве питьевой без специальной обработки. Наиболее эффективными на сегодняшний день способами получения чистой воды являются методы баромембранных технологии, в частности метод обратного осмоса. Практическое применение этого метода требует тщательной предварительной обработки воды, в том числе с использованием микрофльтрации.

загрязнение воды, питьевая вода, баромембранная технология, обратный осмос.

Станция предназначена для очистки природных вод с целью получения воды питьевого качества в соответствии с требованиями действующих нормативных документов [1,2].

Станция может использоваться для очистки сильно загрязненной артезианской воды. Очистке подлежит вода из скважины (подземного водоносного горизонта), в корректировке нуждаются следующие показатели:

- Жесткость общая (19,4 мг/л при норме 7,0 мг/л);
- Нитрат-ион (102,84 мг/л при норме 45,0 мг/л);
- Сухой остаток (солесодержание) (1014,5 мг/л при норме 1000,0 мг/л);

Паспортная производительность станции по очищенной воде питьевого качества составляет 4,2 м³/ч, 90 м³/сут.

Исходя из анализа исходной воды, очистка предусматривается по следующей схеме:

- очистка воды на механических фильтрах с автоматической промывкой;
- осаждение примесей на фильтрах с каталитической загрузкой;
- обработка воды 10% раствором соляной кислоты пропорционально датчику рН;
- дозирование антискаланта, препятствующего отложению солей жесткости на поверхности мембранных элементов;
- удаление из воды растворенных ионов на обратноосмотической установке;
- хлорирование очищенной воды гипохлоритом натрия для пролонгированного эффекта обеззараживания.

Дозирование реагентов предусматривается автоматическими мембранными насосами-дозаторами пропорционально внешнему mA сигналу от водомера на трубопроводах исходной и очищенной воды. Для подачи исходной воды на очистку установлены насосы Jetex 4-2, для промывки фильтров с каталитической загрузкой используются насосы Jetex 4-4. В качестве регулирующей и запорной

арматуры используются двух и трехходовые ручные клапана и клапана с электроприводом.

Дисковые фильтры Raifil RL-Q02 с автоматической промывкой для удаления из очищаемой воды твердых загрязнений, таких как песок, окалина и других нерастворенных примесей. В предлагаемой схеме степень фильтрации 50 мкм. Фильтрующим элементом являются диски из полипропилена. Вода, проходя через сжатые диски, очищается от механических взвесей. Очистка фильтров производится током воды по автономному сигналу управляющего клапана фильтра в заданное время. Промывные воды сбрасываются в канализацию.

Блок осветления, включающий в себя четыре параллельно подключенных напорных фильтра с алюмосиликатной фильтрующей загрузкой (сорбент АС). Фильтры предназначены для осаждения примесей в слое загрузки с каталитическими свойствами. Промывка фильтров осуществляется поочередно в автоматическом режиме через заданный интервал времени, при этом промывные воды направляются в канализацию. Промывка одного фильтра осуществляется очищенной водой насосами за счет переключения потоков автоматическими трехходовыми клапанами с электроприводами. Сигналом к началу промывки служит заданное время.

Исходная вода с расходом 5,4 м³/ч поступает в узел фильтров грубой очистки ФМ.1...3(см. рис. 1.) с автоматической промывкой, который необходим для задержания грубодисперсных частиц. Промывка фильтра производится в автоматическом режиме по таймеру. Промывная вода отводится в канализацию. После фильтров грубой очистки вода разделяется на два потока, один поток смешивается с пермеатом (обессоленной водой), а второй поток подается на засыпные фильтры обезжелезивания воды с целью задержания мелкодисперсных взвешенных веществ и железа, тем самым защищая мембраны обратного осмос от отложений нерастворимых веществ и продлевая срок службы мембранных элементов.

Узел фильтров обезжелезивания ФН.1...4(см. рис. 1.), выполняет функцию защитных фильтров. Узел включает в себя 4 фильтра, загруженных фильтрующей загрузкой «Сорбент АС», в качестве подложки используется кварцевый песок. Гранулы «Сорбент АС» имеют ломаные края и неравномерную поверхность, а также пористость что обеспечивает высокую поверхность фильтрации и позволяют добиться хорошей эффективности при удалении взвешенных частиц и железа. Промывка фильтров производится очищенной водой в автоматическом режиме по таймеру, перенаправление потоков производится при помощи автоматических.

После последовательной фильтрации вода обрабатывается 10% раствором соляной кислоты пропорционально датчику рН, с целью предотвращения отложений солей жесткости на поверхности мембранных элементов и направляется в промежуточную ёмкость общим объемом 5 м³.

При помощи промывного насоса Н2.1...2(см. рис. 1.) вода из резервуара поступает на обратную промывку фильтров обезжелезивания.

При помощи насосов Н1.1...2(см. рис. 1.) вода поступает на установки обратного осмоса. Перед подачей воды на установки обессоливания в очищенную воду дозируется антискалант (НД2.1...2) (см. рис. 1.), препятствующий отложению солей жесткости на поверхности мембранных элементов. Вода поступает на узлы обратноосмотического обессоливания воды УОО1...2(см. рис. 1.), в котором осуществляется удаление из воды растворенных ионов. Исходная вода направляется повышающим давлением насосом через коллектор внутрь напорных корпусов, внутри которых установлены обратноосмотические мембраны. Давление и расход воды в мембранном блоке поддерживается регулируемыми дросселями. Управление установками возможно в ручном или автоматическом режимах. Для регенерации мембран предусматривается установка химической промывки обратного осмоса, состоящая из емкости для приготовления моющего раствора, насоса подачи раствора на мембранную установку и фильтра.

Перед подачей воды на установки обессоливания в очищенную воду дозируется антискалант (НД2.1...2) (см. рис. 1.), препятствующий отложению солей жесткости на поверхности мембранных элементов.

После обратно осмотических мембран в очищенную воду дозируется гипохлорит натрия насосами дозирования НД3.1...2(см.рис. 1.), который необходим для обеззараживания воды.

Для удаления воздуха при заполнении водой насосов Н1.1...2(Н2.1...2) (см. рис. 1.) необходимо при закрытом кране с напорной стороны открутить выпускной штуцер для удаления воздуха. Медленно открыть кран с всасывающей стороны и подождать, пока из отверстия не польется вода и из насоса полностью не выйдет воздух. Завернуть штуцер. Плавно открыть кран на напорной линии и продолжить запуск, следя за давлением.

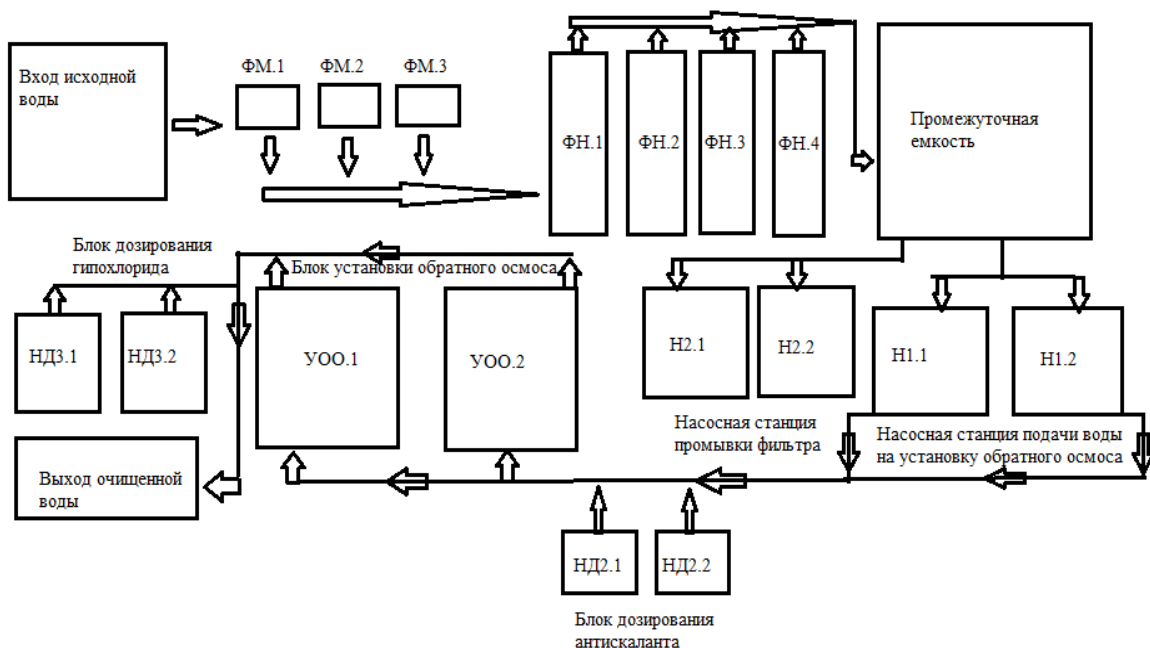


Рис. 1. Схема очистки воды

Исходя из изложенного можно сделать вывод, что станция может быть использована для очистки сильно загрязненной артезианской воды, а предложенная технологическая схема очистки обеспечивает получение чистой питьевой водой в соответствии с требованиями действующей нормативной документации.

Список используемых источников:

1. СанПиН 2.1.4.1074-01 «Питьевая вода. Гигиенические требования к качеству воды централизованных систем питьевого водоснабжения. Контроль качества» от 26 сентября 2001 года N 24, с изменениями на 2 апреля 2018 года.
2. ГОСТ 2874-82 «Вода питьевая. Гигиенические требования и контроль за качеством. Номер документа 2874-82. От 2021 года.

Karpekin A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Block-modular treatment plant.

The problem of water pollution has been relevant for the past few years. Pollution of surface water bodies with industrial waste does not allow it to be used as drinking water without special treatment. To date, the most effective methods for obtaining clean water are the methods of baromembrane technology, in particular the reverse osmosis method. The practical application of this method requires careful pre-treatment of water, including the use of microfiltration..

Key words: water pollution, drinking water, baromembrane technology, reverse osmosis.

УДК 676.038.2
ГРНТИ 87.53.15

ЭКОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ПЕРЕРАБОТКИ МАКУЛАТУРЫ И ПУТИ ИХ РЕШЕНИЯ

О. П. Ковалева¹, Н. Е. Манвелова², А. И. Огай²

¹Санкт-Петербургский государственный лесотехнический университет им. С. М. Кирова

²Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время возрастает потребление природных ресурсов, однако материальная выгода интересует человека больше, чем забота о последствиях его деятельности. Ограниченность сырьевых ресурсов древесины обуславливает необходимость полномасштабной утилизации многотоннажного отхода производства и потребления – макулатуры для производства различных видов картонно-бумажной продукции. В данной статье проанализированы экологические проблемы переработки макулатуры и рассмотрены пути их решения.

переработка макулатуры, сточные воды, твердые отходы, эколого-технологические преимущества

Одним из способов снижения негативного воздействия от ЦБП на окружающую среду и экономии ценнейшего ресурса – древесины, является утилизация макулатуры. Макулатура представляет собой отслужившие свой срок или испорченные влиянием посторонних веществ изделия из бумаги и картона, а также отходы их производства и переработки. Уже многие годы макулатура является не просто отходами жизнедеятельности человека, а ценным сырьем, переработка которого экологически целесообразна и экономически выгодна. Макулатура имеет важное свойство, которое заключается в возможности многократной переработки с получением вторичного волокна, пригодного для производства бумаги и картона.

Несмотря на то, что в настоящее время бумага стала меньше использоваться в документообороте и началось повсеместное использование цифровых носителей и виртуальной коммуникации, вырос спрос на бумажную упаковочную продукцию [1].

В России ежегодно образуется около 15 млн. тонн макулатуры, из которых пригодно для переработки 12 млн. тонн, но фактически собирается только 4 млн. тонн, т.е. коэффициент собираемости макулатуры – менее 30%, что в два раза уступает среднеевропейскому уровню [2]. Главной причиной является неразвитость системы сбора вторичного бумажного сырья, особенно у населения. Наибольший объем макулатуры собирается в Московской и Ленинградской областях. В промышленности образуется около 7,1 млн тонн перерабатываемых бумажных отходов. МС-5Б и МС-6Б – наиболее распространенные марки макулатуры в России, поскольку именно они в большем количестве образуются, собираются и перерабатываются [3]. Наиболее ценные марки макулатуры – МС-1А и МС-2А, содержащие беленую

целлюлозу.

Переработчики макулатуры располагаются в промышленно развитых районах России — местах образования основной массы макулатуры. К ним можно отнести такие предприятия, как: ООО «Картонтара» г. Майкоп; АО «Бумажная Фабрика «Коммунар»; АО «Техническая бумага»; ОАО «Набережно-Челнинский картонно-бумажный комбинат», «Сухонский картонно-бумажный комбинат», «Окуловская бумажная фабрика» и др. В настоящее время на вторичном волокнистом сырье работает более 200 предприятий Российской Федерации. Основная масса макулатуры, переработанной в 2021 году, была использована для изготовления картонных коробок и гофротары. При этом переработка вторичного сырья имеет как положительные, так и отрицательные аспекты, характеристика которых приведена в таблице 1.

ТАБЛИЦА 1. Эколого-технологические аспекты переработки макулатуры

Положительные	Отрицательные	Пути решения
Снижает уровень загрязнения атмосферы на 74%, воды – на 35%	Качественные характеристики продукции, изготовленной из макулатуры, ниже, чем из первичного волокна	Грамотно утилизировать бумажный мусор
Сокращает вырубку деревьев	Улучшение качественных характеристик приводит к повышению стоимости продукции	Осознанно подходить к потреблению
Сокращает количества потребляемой электроэнергии на 40–65%	При многократном использовании снижается качество вторичного волокнистого полуфабриката	Использовать переработанную бумагу
Уменьшает площади мусорных полигонов	Процедура переработки пока не имеет широкого распространения в нашей стране	Использовать электронные носители информации
Средняя стоимость 1 тонны макулатуры в 2-4 раза меньше 1 тонны целлюлозы	Значительные финансовые затраты на начальных этапах	Сохранять бумагу, использованную только с одной стороны

Согласно справочным документам по наилучшим доступным технологиям (НДТ) в ЦБП (Reference Documents on Best Available Techniques in the Pulp and Paper Industry, December 2001 (BREF)), при переработке макулатуры основное воздействие на окружающую среду оказывают сбросы в водоёмы и твердые отходы (таблица 2) [4].

ТАБЛИЦА 2. Технологические нормативы сбросов сточных вод и газовых выбросов при переработке макулатуры

Компонент сбросов на 1 т а.с. волокна	Ед. измерения	Механически очищенная макулатурная масса	Макулатурная масса с удалением печатной краски
Количество сточных вод	м ³ /т	6,0	15,0
ХПК	кг/т	1,1	3,1
БПК ₅	кг/т	0,1	0,15
ВВ	кг/т	0,15	0,3
АОХ	кг/т	0,004	0,008
N _{общ}	кг/т	0,05	0,1
P _{общ}	кг/т	0,002	0,03
Твердые отходы	кг/т	100	150

Производственная вода линии переработки макулатуры содержит растворенные и нерастворимые вещества органического и неорганического характера. Удаление нерастворимых веществ из производственной воды, таких как мелкое волокно и минеральные частицы наполнителей и меловальных покрытий, осуществляется на различных очистных аппаратах. Растворенные вещества, присутствующие в производственной воде, имеют различное происхождение: некоторые поступают со свежей водой, другие – с первичными полуфабрикатами (лигнин, неорганические соли и экстрактивные вещества). Значительное влияние на состав и свойства производственной воды оказывают вещества, содержащиеся в макулатурном сырье, в том числе различные химические добавки, использованные при производстве и обработке бумаги или картона [5].

Содержание соединений тяжелых металлов в бумажно-картонной продукции зависит от вида используемого сырья: газетная, журнальная или смешанная офисная макулатура, отходы супермаркетов или гофротара. Содержание соединений тяжелых металлов таких, как ртуть и кадмий, соответствует содержанию их в исходном древесном сырье или первичных полуфабрикатах. Повышенное содержание АОХ имеет место в газетной, журнальной макулатуре вследствие наличия хлорсодержащих желтых пигментов, используемых при офсетной и глубокой печати. Источниками АОХ являются некоторые химические добавки (например, полиамидные смолы, модифицированные эпихлоргидрином), макулатура из целлюлозы, беленой с использованием соединений хлора, печатные краски. Благодаря широкому распространению бесхлорной отбеливания концентрация АОХ ощутимо снижается. Сточные воды предприятий, использующих макулатуру, содержат низкие концентрации биогенных веществ - соединений азота и фосфора. Органически связанные соединения азота поступают в составе некоторых химических добавок (катионный крахмал, катионный полиакриламид и пр.).

Количество твердых отходов в значительной степени определяется технологией сбора и предварительного сортирования макулатуры. Жесткое

следование требованиям стандарта для сортовой макулатуры, использование сортов макулатуры в соответствии с регламентируемыми положениями значительно снижают количество твердых отходов от подготовки макулатурной массы. Различия в уровнях твердых отходов для макулатуры, очищенной от печатной краски, определяются дополнительным наличием шлама, содержащего короткие волокна, наполнители, краски, экстрагируемые вещества, которые образуются на стадиях флотации и промывки.

При этом отходы переработки макулатуры могут представлять собой вторичные «природные» ресурсы: неорганические компоненты золы могут использоваться в производстве стройматериалов; флотошлам может направляться на изготовление волокнистого пеносорбента, предназначенного для очистки водоемов от масляных и нефтяных пятен и т.д. Разработана схема переработки твердых волокнодержащих отходов в волокнистый измельченный продукт (ВИП), который предлагается использовать в качестве термоизоляционной засыпки в домостроении, а также для очистки производственных площадей, связанных с разливом масла, нефти и нефтепродуктов. Способность ВИП поглощать масляные жидкости в 4...6 раз превосходит способности активированного угля [5].

Макулатура, таким образом, уже не просто бумажный отход, это перерабатываемый материал, который должен продолжать служить экономическим целям. Широкое использование макулатуры как вторичного сырья для производства бумаги и картона позволяет существенно сокращать объем вырубki лесов, исключает затраты на заготовку, транспортировку и восстановление. К тому же это способствует снижению затрат на сырье, т.к. 1 т макулатуры стоит в 2-4 раза дешевле, чем 1 т целлюлозы, уменьшает расходы на транспортировку сырья и продукции [6].

Макулатурный рынок является не только самым емким, но и стабильно растущим сегментом вторичного сырья, поскольку для мировой целлюлозно-бумажной промышленности характерно увеличение доли макулатурного сырья как основы производства [7]. Российский показатель доли перерабатываемой макулатуры близок к мировому, который составляет около 65% [8].

Таким образом, макулатура является одним из наиболее часто перерабатываемых материалов, на ее долю приходится половина материалов, собираемых для вторичной переработки по весу. При этом переработка макулатуры имеет ряд эколого-технологических преимуществ в сравнении с традиционными технологиями химической переработки древесины, так как является менее экологически агрессивной, и кроме того, позволяет сокращать расход древесины и сохранять лес, ибо лес – это одно из наиболее ценных природных богатств, которое обеспечивает жизнедеятельность природы и человека.

Список используемых источников:

1. Переработка макулатуры: положительное влияние на экологию: [Электронный ресурс] // Компания МАК Group. М., 2022. URL: <https://makulatura24.ru/staty/pererabotka-makulatury-polozhitelnoe-vliyanie-na-ekologiyu> (Дата обращения 15.10.22)
2. Волкова А. В. Рынок утилизации отходов. Макулатура. М. : НИУВШЭ, 2018. 36 с.
3. Вильде О. Макулатурный потенциал. Что сдерживает переработку вторсырья: [Электронный ресурс] // Цикличная отрасль. URL: <https://sber.pro/publication/makulaturnyi-potentsial-cto-sderzhivaet-pererabotku-vtorsyrgia> (Дата обращения 17.10.2022)
4. Информационно-технический справочник по наилучшим доступным технологиям ИТС-1 2015. Производство целлюлозы, древесной массы, бумаги, картона. М. : Бюро НДТ, 2015. 479 с.
5. Ковалева О. П. Вопросы экологии в переработке макулатуры // «Современные тенденции в развитии производства бумаги, картона, гофрокартона из макулатурного сырья»: материалы 11-ой междунар. науч-техн. конф., 20-21 мая 2010 г. М. : ГОУ ВПО МГУЛ, 2010. С.53-56.
6. Waste Paper in Russia = OCC Only. Rescue in EPR: [Электронный ресурс] // Gofro expert, 2020. URL: <https://gofro.expert/novosti/b-waste-paper-in-russia-occ-only-rescue-in-epr-b/>. (Дата обращения 17.10.2022)
7. Подтероб А. К., Симанько Н. А., Шевцова М. В. Характеристика рынков отдельных видов отходов. Витебск : УО «ВГТУ», 2020. С. 205-207.
8. День без бумаги: переработка макулатуры в России: [Электронный ресурс] // ИА «Тулская пресса», Тула, 2022 // URL: <https://www.tulapressa.ru/2022/10/den-bez-bumagi-pererabotka-makulatury-v-rossii-vyroslo-v-6-raz-za-20-let-rosselxozbank/> (Дата обращения 01.11.2022)

Kovaleva O.¹, Manvelova N.², Ogai A.²

¹*Saint Petersburg State Forest Technical University*

²*The Bonch-Bruевич Saint-Petersburg State University of Telecommunication*

Environmental problems of waste paper recycling and ways to solve them.

Currently, the consumption of natural resources is increasing, but the material benefit interests a person more than caring about the consequences of his activities. The limited raw material resources of wood necessitate the full-scale utilization of multi-tonnage waste of production and consumption - waste paper for the production of various cardboard and paper goods. This article analyzes the environmental problems of waste paper recycling and considers ways to solve them.

Key words: *waste paper recycling, waste water, solid waste, ecological and technological advantages.*

УДК 504.064.38
ГРНТИ 87.17.81

ОПРЕДЕЛЕНИЕ БЕНЗАПИРЕНА В АТМОСФЕРНОМ ВОЗДУХЕ МЕТОДОМ ВЫСОКОЭФФЕКТИВНОЙ ЖИДКОСТНОЙ ХРОМАТОГРАФИИ

Н. Е. Манвелова, Е. А. Чабаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Для контроля содержания бензапирена в атмосферном воздухе применяется метод высокоэффективной жидкостной хроматографии. Имеющиеся современные приборы-хроматографы очень чувствительны и способны решать большое количество сложных аналитических задач, в том числе обнаружение минимального присутствия бензапирена в исследуемых объектах.

нормирование бензапирена, лабораторные исследования, жидкостная хроматография

Бензапирен открыт в 1933 году как канцерогенный компонент сажи и смолы. Относится к ПАУ и является веществом первого класса опасности. Образуется при сгорании углеводородного жидкого, твердого и газообразного топлива (в меньшей степени).

Полициклические ароматические углеводороды (ПАУ) устойчивы в любой среде и трудно поддаются разрушению. В России имеет ПДК только одно соединение этого класса – бензапирен, наиболее стойкий и сильный канцероген среди ПАУ, который является индикатором наличия канцерогенных ПАУ в окружающей среде [1]. В настоящее время нормы предельно допустимой концентрации (ПДК) воздействия бензапирена закреплены в СанПиН 1.2.3685-21 [2]. На текущий момент № 7-ФЗ ст. 65 и ГОСТ Р 56062-2014 установлено, что в целях обеспечения соблюдения требований, установленных законодательством в области охраны окружающей среды необходимо проводить экологический контроль [3, 4].

Определение полициклических и летучих ароматических углеводородов в атмосферном воздухе относится к числу сложных аналитических задач. Для их решения применяется современный метод анализа – высокоэффективная жидкостная хроматография (ВЭЖХ).

Высокоэффективная жидкостная хроматография (ВЭЖХ) — один из наиболее востребованных методов инструментального анализа, который используется в различных областях промышленности. К жидкостным хроматографам предъявляются такие требования, как высокая чувствительность, воспроизводимость, эффективность [5].

В качестве объекта исследования выступает атмосферный воздух в городе Череповец Вологодской области. Способом наличия или отсутствия бензапирена в атмосферном воздухе использовали метод ВЭЖХ.

Определение массовой концентрации бензапирена выполнялись путем отбора проб атмосферного воздуха аспиратором ПУ-4Э на фильтры АХА на границе санитарно-защитной зоны металлургического предприятия г. Череповца в течение 30 минут на высоте 1,5 метра и последующего анализа проб в испытательной аналитической лаборатории в соответствии с методикой М-02-902-150-07 [6].

Методика обеспечивает выполнение измерений в диапазоне концентраций 0,0005 — 0,05 мкг/м³ с погрешностью, не превышающей $\pm 25\%$ при доверительной вероятности 0,95 [6].

Измерения концентрации анализируемых соединений выполняют на жидкостном хроматографе LC-20 Prominence (Schimadzu), который представлен на рис. 1.



Рис. 1. Жидкостной хроматограф LC-20 Prominence (Schimadzu)

Общая принципиальная схема устройства высокоэффективного жидкостного хроматографа (ВЭЖХ) LC-20 Prominence (Schimadzu) показана на рис. 2.

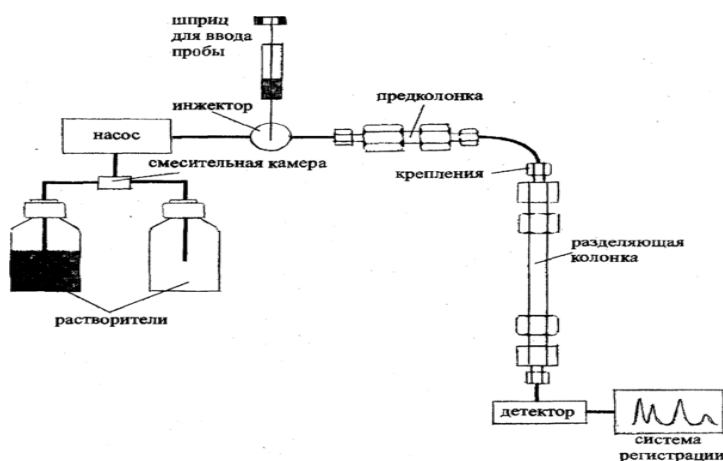


Рис. 2. Схема устройства ВЭЖХ LC-20 Prominence (Schimadzu) [7]

Для анализа бензапирена выполнялись требования методики М-02-902-150-07, а именно: отбор проб выполнялся по ГОСТ 17.2.3.01-86 «Охрана природы. Атмосфера. Правила контроля качества воздуха населенных пунктов» [8] и РД 52.04.186-89 «Руководство по контролю загрязнения атмосферы», ч.1, п.4.4.1 [9].

После отбора проб и пробоподготовки пробы вводятся в хроматограф и проводится анализ методом высокоэффективной жидкостной хроматографии. Хроматограмма бензапирена в пробе воздуха от 14.10.2022 представлена на рис. 3.

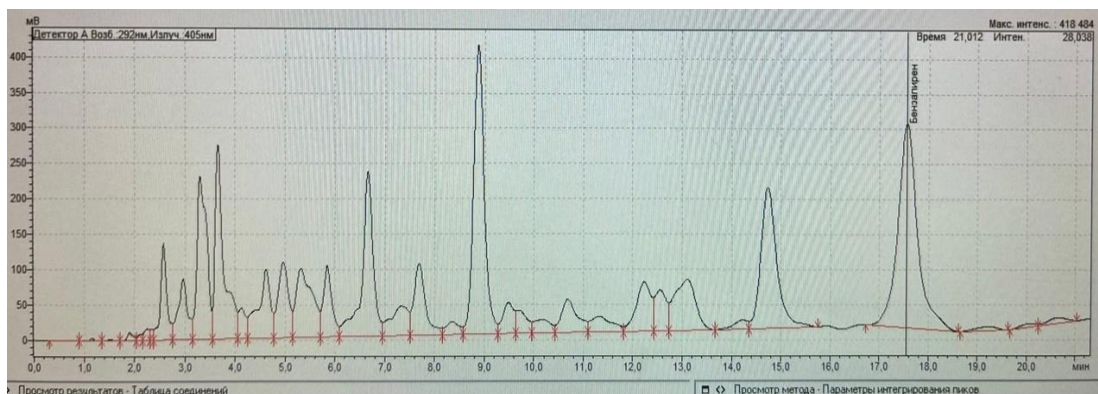


Рис. 3. Хроматограмма бензапирена в пробе воздуха

Время определения бензапирена хроматографом составило – 17,5 минут. Массовая концентрация бензапирена в пробе воздуха составила 0,02501 мкг/мл.

Массовую концентрацию бензапирена в каждой пробе воздуха вычисляют по формуле 1:

$$X_{1(2)} = \frac{C \cdot n \cdot 1000}{\alpha \cdot V_0}, \quad (1)$$

где C – показания хроматографа, мкг/см³, n – степень разбавления хроматографической пробы ацетонитрилом, см³, α – коэффициент извлечения бензапирена (значение, установленное разработчиком), V_0 – объем отобранного газа, приведенного к н.у., дм³

Вычисление результатов измерений представлены в таблице 1.

ТАБЛИЦА 1. Расчёт массовой концентрации бензапирена в пробах воздуха

Показатели	Проба №1	Проба №2
Показания хроматографа, мкг/см ³	0,02501	0,02217
Степень разбавления, см ³	1	1
Коэффициент извлечения бензапирена	0,87	0,87

Холостая проба, мкг/см ³	0,00009	0,00009
Объем отобранного газа, приведенный к н.у., дм ³	462,95	462,95
X, мкг/м ³	0,05999	0,05487
X _{ср} , мкг/м ³	0,05743	

Как следует из таблицы 1 средняя величина концентрации бензапирена из двух параллельно отобранных проб на границе санитарно-защитной зоны металлургического предприятия составила 0,05743 мкг/м³, когда ПДКс.с. 0,001 мкг/м³. Из этого следует, что превышение ПДКс.с. бензапирена на границе санитарно-защитной зоны составляет 57 раз.

Возможным источником выброса бензапирена в атмосферный воздух может быть цех по переработке смолы, в котором производят электродный каменноугольный пек и побочный продукт производства кокса – каменноугольную смолу. При нормальном функционировании смолоперерабатывающего цеха выбросы бензапирена не превышают ПДКс.с..

Бензапирен — канцероген, отнесен к веществам первого класса опасности, является результатом технического прогресса вследствие деятельности человека. Будучи химически устойчивым, обладая свойствами биоаккумуляции, он, попав и накапливаясь в организме, действует постоянно. В настоящее время бензапирен требует постоянного аналитического контроля. Метод ВЭЖХ позволяет с высокой точностью и минимальными затратами по времени определять самые низкие концентрации бензапирена в пробах атмосферного воздуха.

Список используемых источников:

1. Определение ароматических углеводородов в воде [Электронный ресурс]. URL: <https://nortest.pro/stati/voda/opredelenie-aromaticheskikh-uglevodorodov-v-vode.html> (дата обращения 28.10.2022).
2. СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания» (утв. главным государственным санитарным врачом РФ 28.01.2021 г.) [Электронный ресурс]. URL: <https://docs.cntd.ru/document/573500115> (дата обращения 20.10.2022).
3. Закон РФ «Об охране окружающей среды», № 7-ФЗ от 10.01.2002 (с изм. от 01.09.2022) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_34823/ (дата обращения 20.10.2022).
4. ГОСТ Р 56061–2014. Производственный экологический контроль. Общие положения [Электронный ресурс]. URL: <https://docs.cntd.ru/document/1200111620> (дата обращения 20.10.2022).
5. Серия LC-20 Prominence [Электронный ресурс]. URL: <https://www.shimadzu.ru/zhidkostnyj-hromatograf-lc-20-prominence> (дата обращения 20.10.2022).

6. ООО "Аналит" Методика выполнений измерений массовой концентрации полициклических ароматических углеводородов в атмосферном воздухе и промышленных выбросов методом высокоэффективной жидкостной хроматографии. - СПб.: 2008. С.20.

7. Жидкостная хроматография [Электронный ресурс]. URL: https://studref.com/462626/matematika_himiya_fizik/zhidkostnaya_hromatografiya (дата обращения 20.10.2022).

8. ГОСТ 17.2.3.01-86 Охрана природы. Атмосфера. Правила контроля качества воздуха населенных пунктов [Электронный ресурс]. URL: <https://files.stroyinf.ru/Data2/1/4294851/4294851978.htm> (дата обращения 20.10.2022).

9. РД 52.04.186-89 Руководство по контролю загрязнения атмосферы [Электронный ресурс]. URL: <https://files.stroyinf.ru/Data2/1/4294851/4294851978.htm> (дата обращения 20.10.2022).

Manvelova N., Chabaeva E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

Determination of Benzapyrene in atmospheric air by high performance liquid chromatography. To control the content of Benzapyrene in the atmospheric air, the method of high performance liquid chromatography is used. Available modern chromatographic instruments are very sensitive and capable of solving a large number of complex analytical problems, including the detection of the minimum presence of benzapyrene in the objects under study.

Key words: *rationing of benzapyrene, laboratory research, liquid chromatography.*

УДК 504.05
ГРНТИ 87.19.15

ДИНАМИКА ПОКАЗАТЕЛЕЙ КАЧЕСТВА ВОДЫ В РЕКЕ САМАРА И АНАЛИЗ ВЛИЯЮЩИХ НА НЕГО АНТРОПОГЕННЫХ И ТЕХНОГЕННЫХ ФАКТОРОВ

Е. Е. Мороз

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Во многих странах уже достаточно давно обозначена проблема обеспечения водой растущего с каждым годом количества людей и хозяйства. Такая проблема возникла в результате хозяйственной и промышленной деятельности человека, что непосредственно влияет на состояние воды. Для определения доли влияния человека на качество воды в реке Самара был использован химико-аналитический метод.

состояние вод, окружающая среда, экология, загрязнение, промышленность

Введение

Самара – это река, расположенная в Самарской и Оренбургской областях России, являющая левым притоком реки Волга и впадающая в Саратовское водохранилище. В данной статье была проведена оценка качества воды в реке Самара.

Формирование состава поверхностных вод, происходит под влиянием естественных и антропогенных факторов. Примерами естественных являются химические характеристики подземных и атмосферных вод, которые питают водотоки и водоёмы. В случае относительно чистых территорий, химический состав определяется естественными факторами [1]. В городской черте формирование поверхностного стока происходит по большей части за счёт сброса промышленных и сточных вод и дополнительно из-за утечек в местах скопления или транспортировки. Данные факторы отражаются на химических характеристиках вод, и являются причинами их загрязнения. Факторы же антропогенные значительно влияют на гидрохимический фон территории изменяя его.

Кроме природных источников загрязнения вод, существенное влияние на качественные характеристики воды оказывают антропогенные факторы, рассмотрим те, которые оказывают наибольшее влияние:

- Промышленные предприятия сбрасывающие сточные воды, в результате чего, коренным образом меняется состав воды и происходит появление специфических веществ, оказывающих заметное влияние на природный фон;
- Загрязнения, вызванные удобрениями, которые поступают с сельскохозяйственных полей.

Оценка вод в реке Самара

Выполним оценку вод в реке Самара для этого составим таблицу показателей содержания веществ в воде (таблица 1) [3].

ТАБЛИЦА 1. Показатели загрязняющих веществ в реке Самара за последние 12 лет.

№	Показатели	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
1	Марганец, мг/л	0,3-0,4	0,5-0,7	0,4-0,5	0,4-0,5	0,4-0,8	0,4-0,8	0,3-0,4	0,4-0,6	0,2-0,6	0,2-0,6	0,2-0,3	0,2-0,3
2	Медь, мг/л	2-4	3-5	3-5	4	1-4	2-3	2-3	3-6	3-4	2-3	2-3	2-3
3	Трудноокисляемые органические вещества, мг/л	21,9-28,5	22,0-30,6	22,8-29,4	21,9-33,0	21,0-29,9	21,0-29,9	21,0-29,9	22,0-30,4	22,0-30,4	20,8-25,1	17,5-26,1	17,5-26,1
4	Легкоокисляемые органические вещества, мг/л	2,38-3,00	2,00-3,20	1,80-3,30	1,60-3,06	1,38-2,56	1,66-2,16	1,66-2,16	1,70-2,30	1,70-2,30	1,56-2,43	1,91-2,28	1,91-2,28
5	Сульфаты, мг/л	71,5-201	73,1-148	77,6-153	41,1-166	82,2-178	119-212	119-212	109-167	109-167	100-171	141-227	141-227
6	Магний, мг/л	-	-	-	-	-	-	-	36,7-45,3	36,7-45,3	41,9-62,8	37,4-46,4	37,4-46,4

Для проведения анализа рассмотрим нормы предельно допустимой концентрации данных веществ в воде [4] (таблица 2).

ТАБЛИЦА 2. Нормы ПДК.

№	Показатели	Нормы ПДК, мг/л
1	Марганец	0,1
2	Медь	1
3	Трудноокисляемые органические вещества	15
4	Легкоокисляемые органические вещества	3
5	Сульфаты	100
6	Магний	50

Сопоставляя значения из таблиц 1 и 2, делаем вывод о том, что по некоторым из показателей имеется превышение норм ПДК, также прослеживается положительная динамика роста веществ, загрязняющих воды, что негативным образом влияет на водную систему, нарушая её экологическое равновесие. Результаты анализа занесем в таблицу 3.

ТАБЛИЦА 3. Процент превышения ПДК в реке Самара за 2021 год.

№	Показатели	Превышение, ПДК
1	Марганец	2,5
2	Медь	2,5
3	Трудноокисляемые органические вещества	1,45
4	Легкоокисляемые органические вещества	0,7
5	Сульфаты	1,84
6	Магний	0,84

Причины загрязнения

Основное влияние, на качество вод в реке Самара, оказывается смывом удобрений с полей сельского хозяйства. Существенный вклад в загрязнение участка реки, вносятся пунктами контроля у населенного пункта Алексеевка и города Самара, в данных местах обнаружены самые высокие концентрации БПК₅, что является следствием сброса сточных вод от сельского и коммунального хозяйства.

Более семидесяти промышленных предприятий располагаются в Самарской области, в большинстве случаев данные предприятия имеют примитивные очистные сооружения, или неправильно эксплуатируются, что соответственно снижает их эффективность. На многих предприятиях и вовсе не имеется никаких очистных сооружений, в том числе и на машиностроительных, стоки которых могут оказывать существенное влияние на гидрохимический и биологический состав реки Самара. Примерами основных загрязнителей являются: нефтепродукты, хром, циан, щелочи, кислоты, смолы и соли металлов.

К тому же одной из основных проблем реки Самара являются сточные воды и грязная вода из притоков реки, например, реки Падовка [5].

Рост промышленности и сельскохозяйственного производства, урбанизация и рост численности людей приводит к существенному увеличению объёма потребляемой воды, что также ведет к загрязнению и истощению вод. Поэтому в наше время все больше внимания отводится проблеме рационального использования и охране вод. Для этого руководство области ведет работу с расположенными на прибрежной территории предприятиями, в том числе при помощи «Роспотребнадзора» проводит контроль очистных сооружений. Также правительство области делает ежегодный доклад о состоянии окружающей

среды за прошедший год. В данном докладе внимание уделяется всем процессам, которые происходили с природными ресурсами за прошедший год, затем происходит сравнение полученных результатов с предыдущим годом, а также рассматриваются возможные меры воздействия. Также стоит отметить природоохранные мероприятия в рамках программы «Возрождение Волги», которые оказали определенное воздействие на улучшение в бассейне реки Волги экологической обстановки. Однако, несмотря на все предпринятые меры, экологическая обстановка в бассейне реки Волги, а как следствие и реки Самары, остаётся напряженной, особенно в крупнейших городах Поволжья и в районах крупного сельскохозяйственного производства.

Меры по снижению загрязнения вод

Проводя анализ и сравнение качества исследуемой реки, можно сделать вывод о необходимости принятия мер по снижению уровня загрязнения поверхностных вод. Необходимы такие меры как: модернизация очистных сооружений прибрежных предприятий, постоянный мониторинг состояния окружающей среды, а в частности вод, также необходимо непосредственное участие города в решении проблемы, а именно участие в федеральных и государственных программах по охране рек и активное участие населения в процессе уборки водных объектов.

Приведенные выше меры уже частично применяются в Самаре и Самарской области, однако этого недостаточно для восстановления чистоты рек на территории Самары и области. Для наилучшего результата необходимо вводить инновационные методы и меры по борьбе с загрязнением, также заняться постепенным закрытием или переносом предприятий, находящихся непосредственно в водоохранной зоне.

Заключение

Рациональное использование вод в наше время является насущной проблемой. Прежде всего необходимо охранять водные пространства от загрязнения и решать проблему сброса сточных вод промышленности. В частности, необходимо ограничить сброс в водоёмы и применять усовершенствованные технологии производства, очистки и утилизации.

Местные власти при помощи государственных тратят много сил на препятствование загрязнению малых рек, используя различные государственные программы, а также проводя проверки на предприятиях, в то же время сами жители объединяются в экологические союзы и бригады, для самостоятельной очистки рек и русел от мусора.

Несмотря на это, на основе анализа полученных материалов, можно сделать вывод о достаточной загрязненности поверхностных вод рек Самара и её притоков, что негативно сказывается на ихтиофауне, а также несет опасные заболевания для жителей данного региона [6]. Основой загрязнения преимущественно выступает антропогенный фактор. Как уже говорилось ранее для решения данной проблемы необходимо продолжить и существенно усилить не только контроль, но и модернизации очистных сооружений, необходимо провести восстановление городской канализации и «ливнёвок», кроме этого налаживать работу организаций, осуществляющих контроль данных сооружений, а также проводить беседы с активным населением в виде экологических кружков, семинаров и бесед, что позволит разъяснить гражданам важность защиты и заботы о водах.

Выводы

Таким образом, анализ гидрохимических показателей реки Самара за последние 12 лет позволил сделать следующие выводы:

– Приоритетными загрязняющими веществами реки Самара являются органические вещества (БПК₅ и ХПК), соединения меди и марганца и сульфат-ионы.

– Прослеживается тенденция снижения содержания трудноокисляемых органических веществ в составе вод.

– Качество воды в реке Самара, в большей степени формируется под влиянием антропогенной нагрузки.

Список используемых источников:

1. Данилов-Данильян В. И. и др. Оценка допустимых изъятий стока в бассейнах малых рек: основные методические положения //Водные ресурсы. – 2006. – Т. 33. – №. 2. – С. 224-238.

2. Максимова А. М., Нестеров Д. А. Экологические проблемы малых водотоков //Известия Российского государственного педагогического университета им. АИ Герцена. – 2014. – №. 165. – С. 132-138.

3. Гидрохимический институт федеральной службы по гидрометеорологии и мониторингу окружающей среды/ ежегодники за 2010-2021 года «Качество поверхностных вод РФ».

4. Онищенко Г. Г. ПРЕДЕЛЬНО ДОПУСТИМЫЕ КОНЦЕНТРАЦИИ (ПДК) ХИМИЧЕСКИХ ВЕЩЕСТВ В ВОДЕ ВОДНЫХ ОБЪЕКТОВ ХОЗЯЙСТВЕННО-ПИТЬЕВОГО И КУЛЬТУРНО-БЫТОВОГО ВОДОПОЛЬЗОВАНИЯ //Дополнения и изменения к ГН. – 2008. – Т. 2. – №. 5. – С. 1315-03.

5. Сергеев Е. М., Кофф Г. Л. (ред.). Рациональное использование и охрана окружающей среды городов. – Наука, 1989.

6. Сухачева И. Ф. и др. Экопатологические аспекты санитарно-гигиенического состояния малых рек Самарской области в условиях антропогенного воздействия //Известия Самарского научного центра Российской академии наук. – 2010. – Т. 12. – №. 1-6. – С. 1511-1515.

Moroz E.

The Bonch-Bruевич Saint Petersburg state university of telecommunication

Dynamics of water quality indicators in the Samara river and analysis of anthropogenic and technogenic factors affecting it.

In many countries, the problem of providing water to the growing number of people and households has been identified for a long time. This problem arose as a result of human economic and industrial activities, which directly affects the state of water. To determine the proportion of human influence on water quality in the Samara River, a chemical-analytical method was used.

Key words: *state of waters, environment, ecology, pollution, industry.*

УДК 621.396.99
ГРНТИ 49.33.29

ПРИРОДНО-РЕСУРСНЫЙ ПОТЕНЦИАЛ ПРИМОРСКОГО КРАЯ И ЕГО ИНТЕГРАЛЬНАЯ ОЦЕНКА

И. В. Назаров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассмотрены природные ресурсы и условия Приморского края. Представлены виды хозяйственной деятельности на территории края. В статье дано определение природно-ресурсного потенциала. Проведена интегральная оценка природно-ресурсного потенциала региона, показателями которой стали различные виды природных ресурсов с их степенью обеспеченности на душу населения.

природно-ресурсный потенциал, природные ресурсы, интегральная балльная оценка, Приморский край, ресурсообеспеченность

Природно-ресурсный потенциал - совокупность естественных ресурсов, являющихся основой экономического развития территории. Величина природно-ресурсного потенциала представляет собой сумму потенциалов отдельных видов природных ресурсов. Интегральная оценка природно-ресурсного потенциала региона с помощью балльной системы позволяет оценить значимость каждого вида ресурсов в баллах, а затем суммировать величины их запасов.

Приморский край расположен на юге Дальнего Востока, в юго-восточной части РФ. На севере граничит с Хабаровским краем, на западе с Китаем, на юго-западе с Северной Кореей, с юга и востока омывается Японским морем. Территория Приморья на три четверти занята горами Сихотэ-Алинской и Восточно-Маньчжурской горных областей. Остальная часть территории имеет равнинный характер [1].

Регион обладает значительными природными ресурсами: мягкий климат, теплое море, особая эстетическая ценность разнообразных приморских и таежных ландшафтов, наличие многих реликтовых видов животных и растений [4], флора и фауна отличаются сочетанием южных и северных видов. Климат умеренно-муссонный. Зона широколиственных лесов, леса составляют до 90% всей площади. Почвы бурые лесные. По территории края протекает около 600 рек длиной более 10 км. Крупнейшей рекой края является Уссури. Приморский край имеет в прибрежных водах значительные морские биологические ресурсы. Они состоят из различных пород рыб (сельдь, камбала, навага, минтай, лосось, терпуг, корюшка), беспозвоночных (крабы, креветки, моллюски), водорослей (ламинария (морская капуста), анфельция, грацилярия и др.) [5].

В Приморье открыт целый ряд крупных и уникальных месторождений разнообразных полезных ископаемых (уголь бурый и каменный, олово, вольфрам, свинец, цинк и т.д.), на базе которых создана и функционирует одна из самых мощных на Дальнем Востоке горнодобывающая промышленность. В Приморском крае, на территориальном балансе, числятся 322 месторождения общераспространенных полезных ископаемых, с суммарными запасами 1 459

млн м³. Значительны запасы и объемы добычи флюорита, бора, серебра, золота, германия, сурьмы, кадмия, таллия и т.д. Размещение основных рудоносных площадей в Приморском крае представлено на рис. 1.

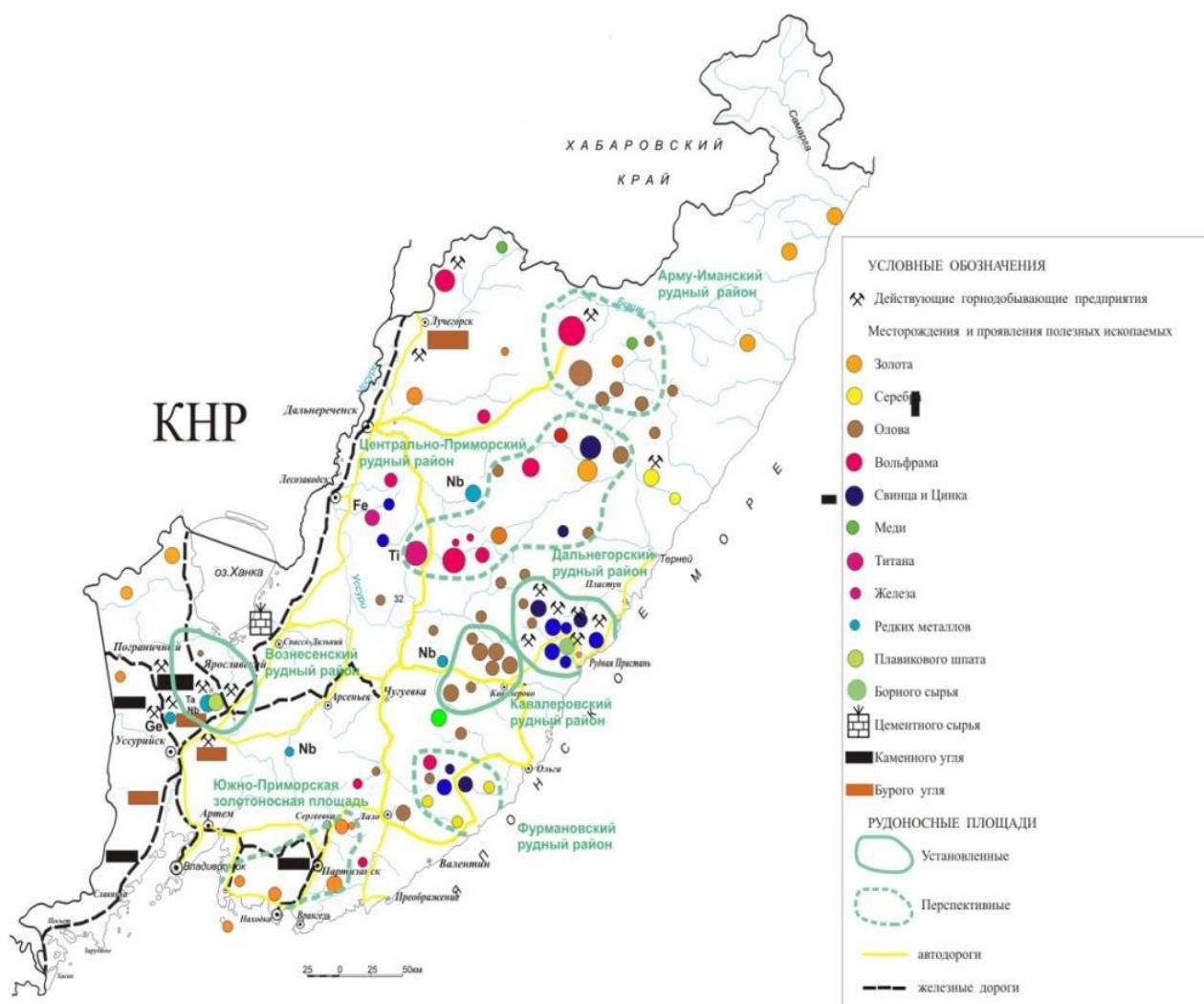


Рис. 1. Размещение основных рудоносных площадей в Приморском крае [6]

Приморский край занимает выгодное географическое положение. Приграничное положение и незамерзающие морские порты создают благоприятные условия для сотрудничества со странами Азиатско-Тихоокеанского региона, Северо-Восточной и Юго-Восточной Азии [1]. Данный субъект является единственным и важнейшим интеграционным регионом во внутренней структуре Дальнего Востока для Магаданской области, Чукотки, Камчатки и Сахалина [3].

Основные экологические проблемы Приморского края:

- загрязнение атмосферного воздуха (загазованность, запыленность воздуха);
- загрязнение и изменение свойств поверхностных и подземных вод;
- загрязнение растительного и почвенного покрова;
- нарушение местообитаний животных, их гибель, миграция;
- изменение рельефа местности и другие.

Развитие экономики края осуществлялось без должного учета устойчивости природы к антропогенной нагрузке, экологических последствий, единой природоохранной политики.

Приморский край занимает второе место после Якутии по выбросам и сбросам загрязняющих веществ во всем Дальневосточном регионе в 2020 г. Наибольший «вклад» в загрязнение компонентов окружающей среды (до 51%) вносит топливно-энергетический и минерально-сырьевой комплекс.

Экологические нарушения неминуемо отразились не только на природе края, но и на его населении. В связи с загрязнением среды в последние годы ухудшилось состояние здоровья людей, во многом рост смертности также обусловлен качеством окружающей среды. Наибольшая острота этой проблемы характерна для крупных промышленных городов: Владивосток, Спасск-Дальний, Арсеньев, Уссурийск [2].

По итогу была проведена интегральная оценка природно-ресурсного потенциала Приморского края (табл. 1).

ТАБЛИЦА 1. Относительная обеспеченность Приморского края по отдельным видам ресурсов, балл

С/х угодия	Запас древесины	Рыб. ресурсы	Нефть	Природ. газ	Уголь	Желез. руда	Мед. руда	Марганц. руда	Итого
3	1	4	-	-	2	-	1	-	11

В результате обеспеченность природными ресурсами в Приморском крае оценивается в 11 баллов.

Список используемых источников:

1. Бакланов, П.Я. Экономико-географическое и геополитическое положение Тихоокеанской России / П.Я. Бакланов, М. Т. Романов. - Владивосток: Дальнаука, 2009. – 172;
2. Берсенев Ю.И., Сотникова О.В., Цой Б.В. Состояние окружающей среды в Приморском крае (учебно-методическое пособие)// URL: <http://www.wwf.ru/resources/publ/book/175> (дата обращения: 12.11.2022);
3. Бурилова В.С, Филичева Т.П. Геополитическое положение как фактор развития Приморского края: история и современность в оценке отечественных и зарубежных ученых // Территория новых возможностей. 2015. №1 (28). URL: <https://cyberleninka.ru/article/n/geopoliticheskoe-polozhenie-kak-faktor-razvitiya-primorskogo-kraja-istoriya-i-sovremennost-v-otsenke-otechestvennyh-i-zarubezhnyh> (дата обращения: 12.11.2022);
4. Жеурова С.В. Природно-ресурсный потенциал Приморского края и некоторые современные методы оценки природно-ресурсного потенциала // Территория новых возможностей. 2010. №2 (6). URL: <https://cyberleninka.ru/article/n/prirodno-resursnyy-potentsial-primorskogo-kraja-i-nekotorye-sovremennye-metody-otsenki-prirodno-resursnogo-potentsiala> (дата обращения: 12.11.2022);
5. Растительность Приморского края// URL: <http://www.fegi.ru/primorye/biology/flora.htm> (дата обращения: 12.11.2022);

6. Состояние и использование МСБ Приморского края ДВО// URL: http://www.vsegei.ru/ru/info/gisatlas/dvfo/primorsky_kray/MSB_09.doc (дата обращения: 12.11.2022).

Nazarov I.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Natural Resource Potential of Primorsky Krai and its integral Assessment.

This article describes the natural resources and conditions of Primorsky Krai. The types of economic activity on the territory of the region are presented. The article defines the natural resource potential. An integrated assessment of the natural resource potential of the region was carried out, indicators of which were various types of natural resources with their degree of availability per capita.

Key words: natural resource potential, natural resources, integral point assessment, Primorsky Krai, availability of resources.

УДК 504.054
ГРНТИ 87.27.33

СОЦИАЛЬНО-ЭКОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ОБЪЕКТОВ РАЗМЕЩЕНИЯ ОТХОДОВ

О. А. Николаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время существует проблема размещения отходов. Для этого используются полигоны, расположение и дальнейшая рекультивация которых имеют влияние на мнение населения. Одним из таких полигонов является полигон твердых бытовых отходов «Новоселки». Объект может оказывать влияние на район, в котором находится, а также на два близлежащих района. На данный момент воздействие на социальную сферу минимально.

отходы, рекультивация, полигон твердых бытовых отходов, захоронения, социально-экономическая сфера

В настоящее время наблюдается рост недовольства граждан, вызванный проблемами размещения полигонов твердых бытовых отходов. Выбор местоположения полигона и его дальнейшее функционирование оказывает непосредственное влияние на жилые, рабочие и рекреационные зоны.

Появление отходов является неотъемлемым сопутствующим процессом жизни современного человека. На полигонах размещаются отходы производства и потребления- предметы и вещества, появившиеся в результате производства, выполнения работ, оказания услуг или в процессе потребления, подлежащие дальнейшему захоронению. Объемы отходов зависят от численности населения, находящихся в городе производств и масштабов самого города. Каждый год наблюдается увеличение количества отходов, а появление несанкционированных, нерегулируемых свалок лишь усугубляет проблему.

Преимущества использования полигонов заключаются в том, что отходы концентрируются на специальной, оборудованной и защищенной территории, конструкция полигонов минимизирует негативное воздействие на окружающую среду. Проблемы, относящиеся к деятельности полигонов, связаны с нарушением требований технологий захоронения, которые могут нанести существенный ущерб окружающей среде. Выбросы свалочного газа порой приводят к взрывам и возгораниям, проникновение фильтрата в почвы и грунтовые воды может привести к уничтожению окружающей флоры и фауны, а неприятные запахи и выбросы наносят ущерб близлежащим районам, вызывают недовольство населения, а также наносит экономический ущерб.

Размещение полигонов имеет ряд проблем, волнующих местное население. Одной из них является расстояние от объекта размещения до жилой зоны. При наличии органических отходов существует риск взрывов и повышение пожароопасности объекта, в связи. Свалочный фильтрат оказывает негативное влияние на грунтовые воды и производит общетоксическое действие на все

живые организмы. К таким последствиям приводят нормы, применяемые для всех объектов. Каждый полигон имеет свою специфику и уникальность, а усредненные значения в нормативной документации не всегда и не для всех актуальны.

Мусор накапливается на полигоне, пока он не достигнет максимальной заполняемости или не закончится срок эксплуатации. После закрытия полигона появляется потребность в рекультивации- комплексе работ, задачи которых направлены на снижение негативных процессов, происходящих в толще мусора, а также возвращение земель в пригодное для эксплуатации состояние.

Рекультивация полигонов ТБО происходит в два этапа- технический и биологический. Первый включает в себя составление проектной документации, подготовку площадки, транспортирование материалов, остановку вредного воздействия на окружающую среду и строительно-монтажные работы на участке. Второй этап направлен на восстановление экологической системы. На подготовленной территории проводится обработка земли, посев и посадка растений [1].

Восстановленная территория в дальнейшем используется в сельском, водном, лесном хозяйствах, а также в рекреационных целях.

С 1972 года функционирует самый крупный в г. Санкт-Петербурге полигон твердых бытовых отходов «Новоселки». Он обслуживает Петроградский, Выборгский, Калининский, Приморский и Курортный районы. На нем размещаются преимущественно бытовые отходы, а также крупногабаритный промышленный мусор. Базовая гидроизоляция отсутствовала, а системы по сбору и переработке газа не строились.

В 2018 году в рамках заключенного государственного контракта началась рекультивация полигона. Работы выполняются в соответствии с проектной документацией по рекультивации. Проект прошел общественное обсуждение и был одобрен жителями и общественными природоохранными организациями.

Проект предусматривает 2 этапа, рассчитанные на 7 лет: 3 года для технического и 4 для биологического. Планируется установка станции дегазации и переработки газа в электроэнергию. Предполагается обеспечить сбор дренажного стока (фильтрата) от подошвы полигона с устройством сети пробуренных скважин и отведение в накопительные резервуары с последующей передачей фильтрата на очистные сооружения.

На сегодняшний день выполнен технический этап рекультивации первой захватки, весной 2022г. были проведены инженерные изыскания, на основе которых составляется документация для второй захватки, всего их три.

В рамках составления проектной документации был выполнен анализ социально-экономической сферы, рассмотрены три административных района г. Санкт-Петербург, оценено влияние работ по рекультивации полигона на население и экономическую деятельность вокруг объекта.

Полигон расположен в Выборгском районе г. Санкт-Петербург, вблизи границ с Курортным и Приморским районами, что представлено на рис. 1.



Следовательно, для оценки влияния на социально-экономическую сферу стоит рассмотреть все три района.



Рис. 1. Местоположение полигона ТБО «Новоселки» на карте Генплана Санкт-Петербурга

ТАБЛИЦА 1. Функциональные зоны, окружающие полигон ТБО «Новоселки» [4]

Вид функциональной зоны	Описание функциональной зоны
ПД	Зона объектов производственного, транспортно-логистического, складского назначения, инженерной инфраструктуры с включением объектов общественно-деловой застройки, связанных с обслуживанием данной зоны
И1	Зона инженерной и транспортной инфраструктур, коммунальных объектов, объектов санитарной очистки с включением складских и производственных объектов
И2	Зона объектов воздушного транспорта с включением объектов общественно-деловой застройки, связанных с обслуживанием данной зоны
И3	Зона объектов железнодорожного транспорта с включением объектов общественно-деловой и инженерной инфраструктур, связанных с обслуживанием данной зоны
Р1	Зона городских лесов
Р5	Зона зеленых насаждений, выполняющих специальные функции, с включением объектов, допустимых в соответствии с действующим законодательством
К1	Зона кладбищ и крематориев
У	Зона городских скоростных дорог, магистралей непрерывного движения и магистралей городского назначения с включением объектов инженерной инфраструктуры
А	Земли водного фонда

Вид функциональной зоны	Описание функциональной зоны
	Территории, планируемые для развития зон многоквартирной жилой застройки с включением общественно-деловой застройки и инженерной инфраструктуры, связанных с обслуживанием данной зоны
	Территории, планируемые для развития зон объектов рекреационного назначения с включением объектов инженерной инфраструктуры

Выборгский район – один из крупнейших в городе. Его площадь составляет 11550 га. Общая численность населения Выборгского района составляет 528 147 жителей (на 05.04.2022г.) [2]. В границах района расположены 8 внутригородских муниципальных образований: Сампсониевское, Светлановское. С северо-восточной стороны находится Левашово. Ближайшая жилая зона к объекту рекультивации расположена:

- на расстоянии 1950 м и более в северном направлении (частные жилые дома по адресу: пос. Левашово, Новоселки, Горское шоссе, д. 128 лит. А, 130 лит. А и др.);

- на расстоянии 2350 м и более в восточном направлении от границы площадки (частные жилые дома, расположенные в пос. Парголово по адресу: 1-ая Успенская, д.40а, 39а,38а, 36 и др.);

- на расстоянии 2500 м и более в южном направлении от границы площадки (частные жилые дома, расположенные в пос. Большая Каменка, д.2а, д. 81, 77, 75 и др.).

Рядом с объектом расположен аэродром Левашово, после рекультивации полигон не будет оказывать на него влияния.

В непосредственной близости к полигону отсутствуют общеобразовательные и здравоохранительные объекты, а также объекты культурного наследия. Таким образом, влияния на них оказано не будет.

Объект находится в зоне инженерной и транспортной инфраструктур и объектов внешнего транспорта, для данной зоны свойственно расположение объектов санитарной очистки с включением складских и производственных, коммунальных объектов [3].

Среднее число дней с сильным ветром (более 15 м/с) в год составляет 32,9, наибольшее – 72 [5]. Преобладающими ветрами, как видно на рис. 2, являются юго-западные. Из этого следует, что большая часть воздушных масс будет двигаться в сторону Приморского и Курортного районов, в сторону местности, где жилая застройка отсутствует.

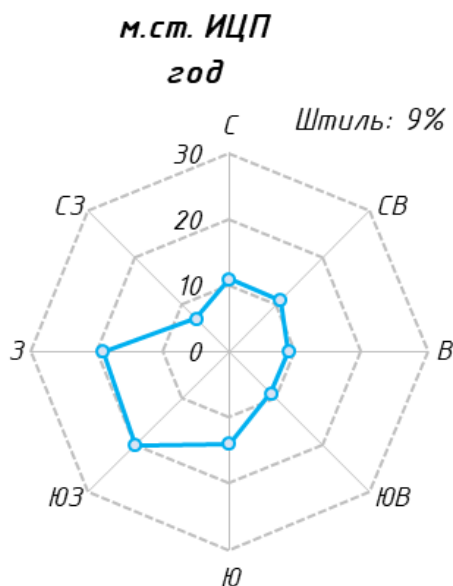


Рис. 2. Среднегодовая повторяемость (%) направлений ветра (Роза ветров) [5]

Обработка отходов несет потенциальную опасность, связанную с химическим, бактериологическим и микробиологическим загрязнениями, которые могут привести к увеличению процента заболеваемости и смертности.

Во время строительно-монтажных работ возникает шумовое загрязнение, а также выбросы пыли и веществ, вследствие которых возникает риск для здоровья человека.

Перечисленные выше факторы могут привести к повышенному уровню стресса населения. Исходя из того, что вокруг полигона отсутствует жилая застройка, а направление ветров в сторону без нее, можно полагать, что негативное влияние будет минимальным.

Объект находится в зоне инженерной и транспортной инфраструктур и объектов внешнего транспорта, вблизи жилые зоны отсутствуют, что видно на рис. 1, функциональные зоны описаны в таблице 1. Из этого следует, что на данный момент воздействие на социальную сферу минимально. Но стоит учитывать, что земли со стороны Приморского района отмечены как «Территории, планируемые для размещения зон многоквартирной жилой застройки с изменением функции на перспективу (2025 год)», следовательно, на этих землях планируется жилая застройка. Размещенный рядом полигон может повлиять на общественное мнение и привести к снижению изначальной стоимости квартир в связи с уменьшением спроса.

Список используемых источников:

1. Васильченко А.В. Рекультивация нарушенных земель: учеб. пособие. М. : ОГУ, 2017. 230 с.
2. Численность населения Санкт-Петербурга: [Электронный ресурс] URL: <https://petrostat.gks.ru/storage/mediabank/Числ.СПб%20на%2001.01.2022%20.pdf> (Дата обращения 01.11.2022)

3. Стурман В. И. Проблемы инженерных изысканий на объектах размещения твердых коммунальных и промышленных отходов при прохождении государственной экологической экспертизы // Инженерные изыскания. 2021. № 15. С. 42-53.

4. Генеральный план Санкт-Петербурга: [Электронный ресурс] URL: <https://portal.kgainfo.spb.ru/Genplan/> (Дата обращения 01.11.2022)

5. Метеорологический архив: [Электронный ресурс] // [Meteoblue.com](https://www.meteoblue.com/ru/погода/historyclimate/weatherarchive).2006-2022. URL: <https://www.meteoblue.com/ru/погода/historyclimate/weatherarchive> (Дата обращения 01.11.2022)

Nikolaeva O.A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Socio-environmental problems of waste disposal facilities.

Currently, there is a problem of waste disposal. For this purpose, polygons are used, the location and further reclamation of which have an impact on the opinion of the population. One of these landfills is the Novoselki solid waste landfill. An object can have an impact on the area in which it is located, as well as on two nearby areas. At the moment, the impact on the social sphere is minimal.

Key words: waste, recultivation, landfill of solid household waste, burial, socio-economic sphere.

УДК 504.055:504.064

ГРНТИ 87.55.81

ПРИБОРНОЕ ОБЕСПЕЧЕНИЕ И НОВЫЕ ВОЗМОЖНОСТИ ИССЛЕДОВАНИЯ ПРОБЛЕМ ЭЛЕКТРОМАГНИТНОГО ЗАГРЯЗНЕНИЯ

В. И. Стурман

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Изложены основные закономерности пространственного распределения и изменчивости электрических и магнитных полей промышленной частоты в Санкт-Петербурге и ряде других городов. Представлены первые результаты измерения характеристик высокочастотных электромагнитных полей в Санкт-Петербурге и окрестностях. Определены задачи дальнейших исследований электромагнитного загрязнения.

картографирование электромагнитных полей, мониторинг электромагнитных полей, электромагнитное загрязнение

Возможности исследования электромагнитного загрязнения в решающей степени определяются характеристиками применяемых для этой цели приборов, а также рациональной организацией их использования. В предшествующий период 2016-22 гг. при помощи единственного прибора Gigahertz Solutions ME 3830 В М/Е Analyser удалось выявить основные закономерности пространственной изменчивости и временной динамики электрических и магнитных полей промышленной частоты [1, 2], включая:

- приуроченность электрических полей напряженностью более нескольких в/м только к высоковольтным линиям (ВЛ) электропередач, в пределах расстояний до десятков и первых сотен метров от них;

- повсеместную распространенность и сильную изменчивость магнитных полей (характеризуемых значениями магнитной индукции), от всей совокупности электрических приборов и устройств производственного и бытового назначения в пределах урбанизированных территорий («электромагнитный смог»);

- зависимость напряженности магнитных полей от характера использования и застройки территорий, с максимумами в исторических центрах городов и минимумами в зеленых зонах, повышенными значениями в застройке прошедших десятилетий (вследствие несоответствия электропроводки нагрузкам от современной бытовой техники) и более низкими значениями в современной застройке;

- необходимость учета при мониторинге электрических и магнитных полей времени максимального электропотребления (максимумы в дневные и отчасти утренние часы в теплый период года и вечерние максимумы в холодный);

- масштабы сезонной динамики (в 1,4-1,6 раза) и межгодовой изменчивости (порядка 10% за 5 лет) нагрузок раскрывают показатели отпуска электроэнергии

по месяцам;

- колебания электрических и магнитных полей в зависимости от времени суток и метеоусловий (ослабление диэлектрических свойств воздуха с увеличением его влажности, что существенно для электрических полей) и нагрузки на системы электроснабжения (что значимо для магнитных полей);

- наличие в пределах урбанизированных территорий аномально повышенных значений напряженности электрического поля и магнитной индукции, обусловленных недостаточно экранированными кабелями подземной прокладки, причем распространенность таких аномалий увеличивается с ростом влажности климата и близости грунтовых вод;

- наличие в каждом из изученных городов (Санкт-Петербург, Москва, Казань, Ижевск, Калининград, Петрозаводск, Белгород) наряду с общими закономерностями местных особенностей, отражающих исторически сложившиеся особенности планировки и застройки.

Выполнены работы по составлению изолинейных карт магнитных полей в перечисленных городах.

Получение кафедрой экологической безопасности телекоммуникаций СПбГУТ новых приборов расширяет возможности картографирования и мониторинга техногенных электромагнитных полей и электромагнитного загрязнения.

Измеритель электромагнитного поля промышленной частоты ВЕ-50и предназначен для проведения мероприятий по охране труда, производственного контроля и контроля требований коммунальной гигиены. Прибор совмещает свойства высокоточных профессиональных измерителей с компактностью и простотой обслуживания бытовых приборов. Особенно важными являются достаточно высокие верхние границы диапазонов измерения – напряженности до 50 кВ/м и магнитной индукции до 5000 мкТл. Это позволяет не только фиксировать ширину зон превышения значений 2 кВ/м и 2 мТл, как это имело место ранее, но и фиксировать максимальные значения, в т.ч. непосредственно под проводами высоковольтных линий. Максимальные измеренные значения напряженности в местах наибольшего провисания проводов составили:

- 23,2 кВ/м под ВЛ-220 кВ в Мурино;
- 6,3 кВ/м под ВЛ-110 кВ там же;
- 14,4 кВ/м под ВЛ-330 кВ там же;
- 5,9 кВ/м под ВЛ-330 кВ у пересечения пр. Маршала Блюхера и Кондратьевского;
- 2,4 кВ/м под ВЛ-110 кВ там же.

Максимальные значения магнитной индукции в тех же местах составили:

- 4,5 мкТл под ВЛ-220 кВ в Мурино;
- 2,9 мкТл под ВЛ-110 кВ там же;
- 5,8 мкТл под ВЛ-330 кВ там же;
- 0,46 мкТл под ВЛ-330 кВ у пересечения пр. Блюхера и Кондратьевского;
- 0,45 мкТл под ВЛ-110 кВ там же.

Все указанные значения напряженности выходит за пределы допустимого

для населенной местности; показатели магнитной индукции находятся в допустимых пределах, согласно СанПиН 1.2.3685-21 [3].

Ближайшие задачи исследований при помощи нового прибора ВЕ-50и включают продолжение мониторинга электрических и магнитных полей высоковольтных линий в условиях меняющейся социально-экономической ситуации, а также расширение территорий, для которых будет выполнено картографирование магнитных полей, в чём могут принять участие студенты.

Измеритель уровня электромагнитного излучения МЕГЕОН 07300 позволяет приступить к изучению распределения высокочастотных электромагнитных полей, что пока остается крайне слабо изученной областью электромагнитной экологии. Публикации о пространственном распределении характеристик высокочастотных электромагнитных полей пока единичны.

Диапазон считываемых частот от 50 МГц до 3,5 ГГц охватывает почти все источники радиоизлучения. Наряду с напряженностью электрического поля и магнитной индукцией, прибор позволяет измерять плотности мощности электромагнитного излучения, в mW/m^2 и W/cm^2 .

Первые результаты исследований при помощи нового прибора МЕГЕОН 07300 показали, что распределение характеристик высокочастотных электромагнитных полей в пределах Санкт-Петербурга и пригородной зоны практически не зависит (либо зависит, но очень сложным и труднопредсказуемым образом) от характера использования и застройки территорий, но контролируется размещением, мощностями и режимами работы передающих радиотехнических устройств (ПРТО). Типичные для городской территории значения в диапазоне от 50 МГц до 3,5 ГГц составляют: напряженность 1-3 v/m , магнитная индукция 3-6 mA/m , плотность потока 10-15 mW/m^2 . Максимальное значение до 60 mW/m^2 было отмечено однократно вблизи базовой станции сотовой связи у станции метро Улица Дыбенко, но не нашло подтверждения при последующих повторных измерениях. Неожиданно низкими (на уровне и ниже указанных обычных значений для городской территории) оказались результаты измерений в историческом центре города (Невский проспект) и телевышки. Сопоставление с гигиеническими нормативами проблематично вследствие неполного совпадения диапазонов измерений и нормирования, а также крайне неоднозначной ситуации в области нормирования высокочастотных полей [4].

Ближайшие задачи исследований при помощи нового прибора МЕГЕОН 07300 включают, прежде всего, организацию и ведение мониторинга вблизи базовых станций сотовой связи в целях формирования статистически значимых баз данных и оценки изменчивости характеристик по секторам и направлениям работы ПРТО. Для этого потребуются измерения на разных высотных уровнях, в разное время суток, в рабочие и нерабочие дни, в чём также могут принять участие студенты.

Список используемых источников:

1. Стурман В.И. Электромагнитные поля промышленного диапазона частот в условиях городской среды как объект эколого-географического исследования // География и природные

ресурсы. 2019. №1. С. 21-28.

2. Стурман В.И., Логиновская А.Н. Техногенные электромагнитные поля на городских территориях и подходы к их картографированию // Известия РАН. Серия географическая. 2022. Т. 86. № 2. С. 255–267.

3. СанПиН 1.2.3685-21 "Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания». М. : 2021. 469 с.

4. Григорьев О.А. Актуальные вопросы радиобиологии и гигиены неионизирующих излучений в связи с развитием новых технологий // Актуальные проблемы радиобиологии и гигиены неионизирующих излучений : материалы всерос. конф., Москва, 12-13 нояб. 2019 г. М. : 2019. С. 63-65.

Sturman V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Instrumentation and new research opportunities for electromagnetic pollution problems.

The main patterns of spatial distribution and variability of electric and magnetic fields of industrial frequency in St. Petersburg and a number of other cities are described. The first results of measuring the characteristics of high-frequency electromagnetic fields in St. Petersburg and the surrounding area are presented. The tasks of further studies of electromagnetic pollution are determined.

Key words: *mapping of electromagnetic fields, monitoring of electromagnetic fields, electromagnetic pollution.*

УДК 504.3.054 (470.23-25)

ГРНТИ 87.03.17

ОЦЕНКА ВЛИЯНИЯ МЕТЕОРОЛОГИЧЕСКИХ ПАРАМЕТРОВ НА КОНЦЕНТРАЦИИ ЗАГРЯЗНЯЮЩИХ ВЕЩЕСТВ В АТМОСФЕРЕ КИРОВСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА

Е. В. Судьина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье изучено влияние метеоусловий на динамику концентраций загрязняющих веществ в атмосферном воздухе Кировского района Санкт-Петербурга. Установлены корреляционные связи между концентрациями загрязняющих веществ и пятью метеорологическими параметрами (температура воздуха, давление, относительная влажность, осадки и параметры ветра).

атмосферный воздух, наземные и дистанционные средства мониторинга, динамика загрязнения, метеорологические характеристики, корреляционный анализ

Атмосферный воздух – жизненно важный компонент окружающей среды, представляющий собой естественную смесь газов атмосферы, находящуюся за пределами жилых, производственных и иных помещений [1].

В соответствии с этим, любое нежелательное изменение его состава, вызванное как антропогенными, так и естественными факторами, приводит к загрязнению и, следовательно, оказывает негативное влияние на здоровье населения и окружающую среду в целом. Главную роль среди этих факторов играют метеорологические параметры, обуславливая, по современным оценкам, более 70% изменчивости примесей, находящихся в воздухе промышленных мегаполисов [2].

Для оценки состояния атмосферного воздуха описанного выше района применялись данные наземных (автоматические станции Санкт-Петербурга (АСМ-АВ-5; АСМ-АВ-13)) и дистанционных средств мониторинга (breezometer [3], ventusky [4]).

На первом этапе работы в течение 40 дней (с 1 октября по 11 ноября 2022 г.) проводился сбор данных о концентрациях загрязняющих веществ (диоксид азота NO_2 , взвешенные частицы $\text{PM}_{2,5}$ и PM_{10} , диоксид серы SO_2 , углерод оксид CO и озон O_3) в 22 точках, которые были равномерно распределены по территории Кировского района (рис. 1), а также фиксировалась информация о метеорологических характеристиках (температура, давление, влажность, осадки, скорость и направление ветра).

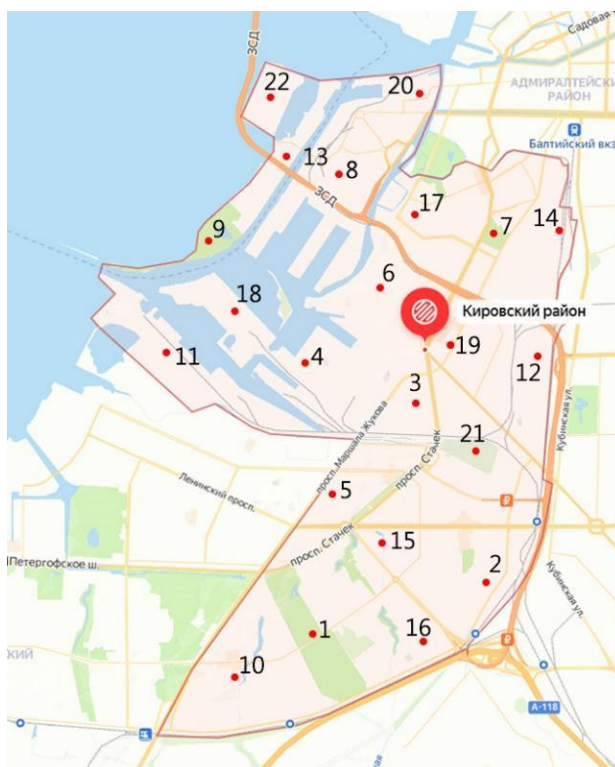


Рис. 1. Расположение точек наблюдения в Кировском районе

Средняя концентрация диоксида азота составила $0,03 \text{ мг/м}^3$ ($0,1 \text{ ПДК}_{\text{cc}}$), окиси углерода – $0,28 \text{ мг/м}^3$ ($3,0 \text{ ПДК}_{\text{cc}}$), диоксида серы – $0,01 \text{ мг/м}^3$ ($0,05 \text{ ПДК}_{\text{cc}}$), озона – $0,03 \text{ мг/м}^3$ ($0,1 \text{ ПДК}_{\text{cc}}$), взвешенных частиц $\text{PM}_{2,5}$ и PM_{10} – $0,008 \text{ мг/м}^3$, $0,012 \text{ мг/м}^3$ ($0,035 \text{ ПДК}_{\text{cc}}$ и $0,06 \text{ ПДК}_{\text{cc}}$ соответственно).

Максимальная концентрация за период исследования по диоксиду азота составила $0,14 \text{ мг/м}^3$ в точке наблюдения 3; по углерод оксиду – $1,07 \text{ мг/м}^3$ в точке 5; по диоксиду серы – $0,041 \text{ мг/м}^3$ в точке наблюдения 10; по озону – $0,072 \text{ мг/м}^3$ в нескольких точках; по взвешенным частицам $\text{PM}_{2,5}$ и PM_{10} – $0,041 \text{ мг/м}^3$ и $0,075 \text{ мг/м}^3$ в точке 3. Все максимальные концентрации в момент исследования отмечались в рабочие дни в вечернее время.

Случаи небольшого превышения предельно допустимых концентраций наблюдаются только по диоксиду азота, остальные же значения концентраций являются полностью безопасными для состояния здоровья населения и соответствуют низкому уровню загрязнения атмосферного воздуха.

Также была произведена обработка данных о метеорологических характеристиках в период мониторинга, средние значения по каждому из показателей составили: атмосферное давление – 779 мм.рт.ст. , температура – $7,5^\circ\text{C}$, скорость ветра – 2 м/с , влажность – 82% , осадки – $0,92 \text{ мм}$. Преобладающие ветра имели юго-западное направление [5].

На втором этапе работы путем корреляционного анализа были выявлены силы связи между средними значениями концентраций загрязняющих веществ (ЗВ) и метеорологическими параметрами (табл. 1).

ТАБЛИЦА 1. Корреляционная матрица за исследуемый период

ЗВ Метео- параметры	Средние значения концентраций ЗВ за исследуемый период					
	СО	NO ₂	SO ₂	PM _{2,5}	PM ₁₀	O ₃
Температура	-0,329	-0,627	-0,250	-0,342	-0,367	0,349
Давление	0,369	0,385	0,429	0,158	0,182	-0,538
Влажность	0,222	0,232	0,014	0,352	0,332	-0,357
Осадки	-0,193	-0,054	-0,043	-0,069	-0,082	0,196
Скорость ветра	-0,603	-0,668	-0,411	-0,370	-0,378	0,738

Таблица 1 дает представление о роли сил связи:

- прямая зависимость от давления и влажности, что отражает накопление ЗВ при антициклональных условиях;
- обратная зависимость от скорости ветра (отражает интенсивность перемешивания воздуха), температуры (отражает накопление ЗВ при антициклональных условиях в переходный период) и осадков (отражает роль осадков в процессах самоочистения).

У озона отмечаются противоположные от других исследуемых элементов силы связи.

Наибольшее влияние на уровень примесей оказывает скорость ветра, а на диоксид серы – давление. Концентрации ЗВ уменьшаются с увеличением скорости ветра, а у озона увеличиваются.

Влияние скорости ветра на уровень загрязнения отражает рис. 2, где представлены гистограммы средних значений концентраций ЗВ, рассчитанных в пределах двух диапазонов скоростей ветра.

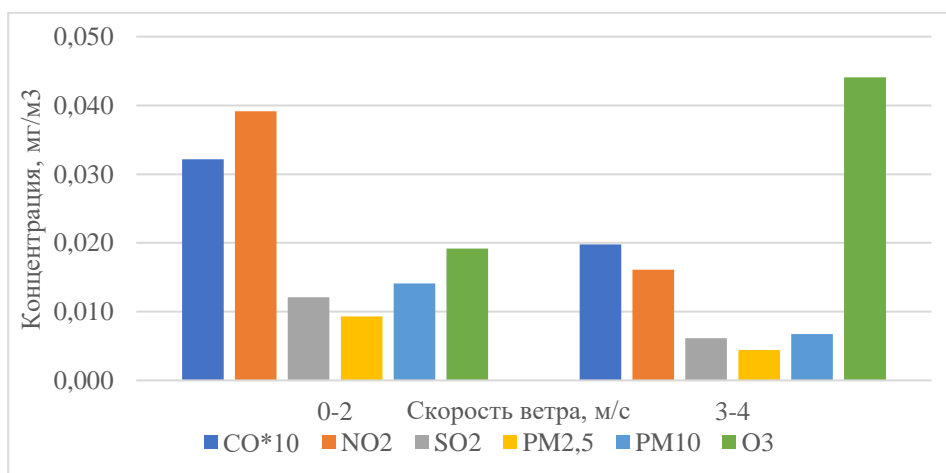


Рис. 2. Концентрация ЗВ в диапазонах разных скоростей ветра

Хорошо видно, что концентрации уменьшаются (кроме O₃) с увеличением скорости ветра. Объясняет тем, что ветер усиливает турбулентный обмен в приземном слое атмосферы, что способствует перемешиванию примесей с окружающим воздухом, и тем самым приводит к уменьшению их приземных концентраций. В свою очередь, при скорости ветра 0-2 м/с, создаются наиболее

неблагоприятные метеоусловия для рассеивания примесей, приводящие к повышению их концентраций в приземном слое воздуха [6].

Результаты оценки влияния давления воздуха на концентрации ЗВ, представлены в таблице 2 и на рис. 3, в которых приводятся средние концентрации ЗВ, соответствующие различным диапазонам атмосферного давления с октября по ноябрь.

ТАБЛИЦА 2. Средние значения концентраций ЗВ в пределах разных диапазонов давления в исследуемый период

Диапазон, мм.рт.ст.	Загрязняющее вещество, мг/м ³					
	СО	NO ₂	SO ₂	PM _{2,5}	PM ₁₀	O ₃
<760	0,23484	0,025008	0,006556	0,006807	0,010186	0,03377
>760	0,3141	0,03707	0,012935	0,008438	0,01304	0,022806

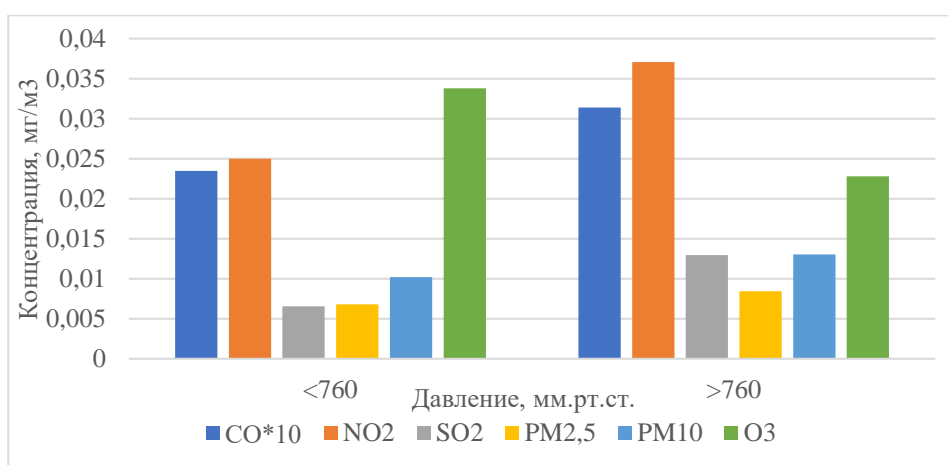


Рис. 3. Средние значения концентраций ЗВ в пределах разных диапазонов давления

Согласно гистограммам у всех ЗВ (кроме O₃) замечен рост концентраций с увеличением атмосферного давления, т.к. ухудшаются условия рассеивания. Концентрации диоксида серы возрастают почти в 2 раза, диоксида азота – приблизительно в 1,5 раза.

На третьем этапе работы было установлено, к какому уровню загрязнения атмосферы относится исследуемая территория, т.е. во сколько раз суммарный уровень загрязнения воздуха превышает допустимое значение по рассматриваемой совокупности примесей в целом.

Расчет проводился по 5 веществам, которые определяли основной вклад в создание высокого уровня загрязнения в исследуемый период. И в соответствии с существующими методами оценки уровня загрязнения считается низким (ИЗА=0,8), что относится к удовлетворительной медико-экологической ситуации.

Таким образом, рассмотренные метеорологические параметры в разной степени поддерживают высокий уровень ЗВ в воздушном бассейне Кировского района Санкт-Петербурга. Учет метеорологической обусловленности колебаний уровня примесей позволяет объяснить и предсказать появление экстремально высоких загрязнений.

Список используемых источников:

1. Федеральный закон от 04.05.1999 N 96-ФЗ (ред. от 11.06.2021) "Об охране атмосферного воздуха" // СПС КонсультантПлюс
2. Безуглая Э.Ю. Мониторинг состояния загрязнения атмосферы в городах. – Л.: Гидрометиздат, 1986. - 200с.
3. Точное качество воздуха – BreezoMeter: [сайт]. – 2022. – Текст: электронный. – URL: <https://www.breezometer.com/> (дата обращения 11.11.2022)
4. Ventusky – прогноз погоды на карте: [сайт]. – 2022. – Текст: электронный. – URL: <https://www.ventusky.com/> (дата обращения 11.11.2022)
5. Расписание погоды: [сайт]. – Санкт Петербург, 2022. – Текст: электронный. – URL: <https://rp5.ru/> (дата обращения 11.11.2022)
6. Экологический портал Санкт-Петербурга: [сайт]. – Санкт Петербург, 2022. – Текст: электронный. – URL: <https://www.infoeco.ru/> (дата обращения 12.11.2022)

Sudina E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Assessment of the influence of meteorological parameters on the concentrations of pollutants in the atmosphere of the Kirovsky district of St. Petersburg.

The article studies the influence of weather conditions on the dynamics of concentrations of pollutants in the atmospheric air of the Kirovsky district of St. Petersburg from October 1 to November 11, 2022. Correlations between concentrations of pollutants and five meteorological parameters (air temperature, pressure, relative humidity, precipitation and wind parameters) have been established.

Key words: atmospheric air, ground and remote monitoring tools, pollution dynamics, metrological characteristics, correlation analysis.

УДК 504.75.05
ГРНТИ 39.01.05

АНАЛИЗ ШУМОВОГО ЗАГРЯЗНЕНИЯ ТЕРРИТОРИЙ МУНИЦИПАЛЬНЫХ ОКРУГОВ №65 И №68 ПРИМОРСКОГО РАЙОНА Г. САНКТ-ПЕТЕРБУРГА (С ПРИМЕНЕНИЕМ ГИС-ТЕХНОЛОГИЙ)

Е. С. Сычёва

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе проведен анализ шумового загрязнения территорий муниципальных округов №65 и №68 Приморского района г. Санкт-Петербурга. Выполнены замеры фактического уровня шума в 78 точках Приморского района с дальнейшим нанесением результатов на карты с использованием геоинформационных технологий.

шумовое загрязнение, геоинформационные системы, построение карт, интерполяция, изолинии

Одна из болезненных экологических проблем для Петербурга – шумовое загрязнение. Исследования 2018 года показали, что вблизи фасадов жилых домов, прилегающих к крупным городским магистралям (КАД, ЗСД), наблюдаются превышения нормативных значений уровня шума (55 дБА в дневное время и 45 дБА в ночное время) [1].

Было проведено подробное исследование территорий №65 и №68 муниципальных округов Приморского района с целью получения наиболее точных и подробных фактических значений уровня шума, измеряемого в акустических децибелах.

Для проведения замеров был использован шумомер DT-8851. Обработка полученных результатов проводилась в геоинформационной системе ArcGIS, а также сопутствующим ей программном обеспечении ArcMap в котором на карту исследуемого района наносились точки проведения замеров с координатной привязкой и фактическими значениями в дБА. Всего было взято 78 точек в Приморском районе Санкт-Петербурга, в каждой из которых были проведены замеры уровня шума (рис. 1).

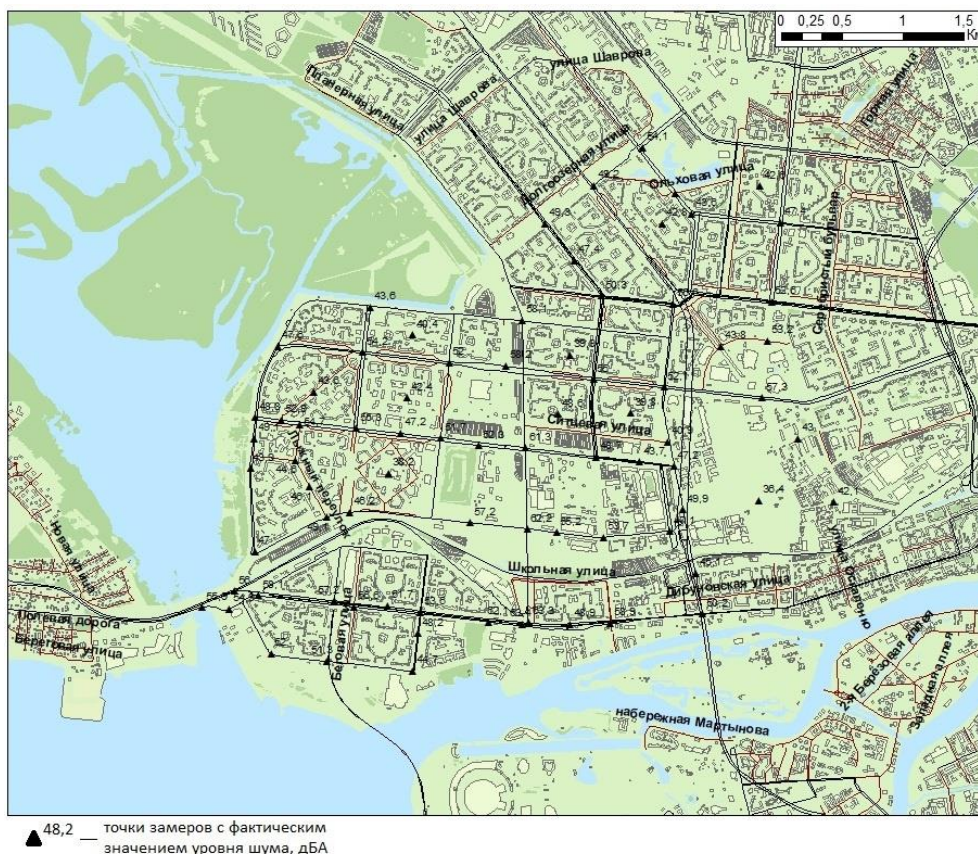


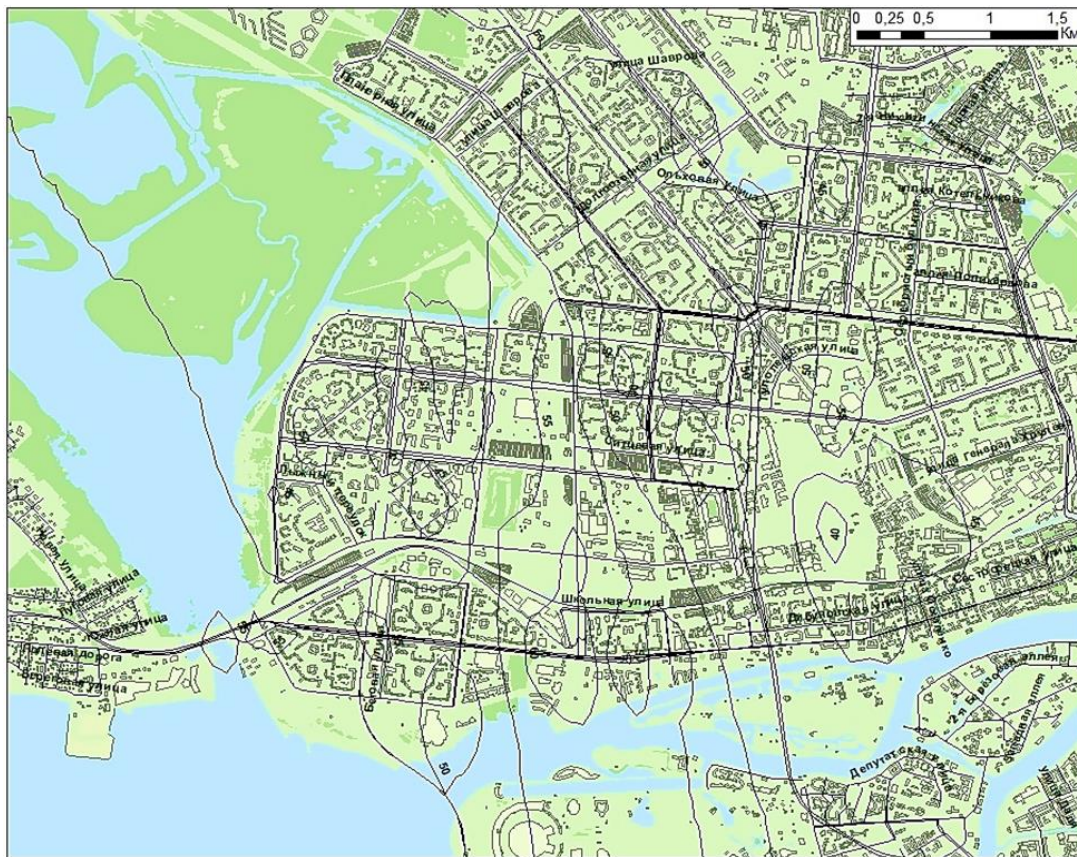
Рис. 1. Карта расположения точек замеров с фактическими значениями уровня шума

Далее для наиболее удобной визуализации создана карта с интерполяцией растра, позволяющая организовать акустический мониторинг на общей научной и методической основе (рис 2).



Рис. 2. Карта с наложением интерполяции растра методом ОВР, дБА

Далее на базе созданной карты интерполяции, используя слой интерполяций, создана карта с изолиниями, представленная на рис 3.



55 Изолинии значений
уровня шума, дБА

Рис. 3. Карта с наложением изолиний

Из проведенных замеров и полученных карт отчетливо видно, что наивысший показатель уровня шума находится вблизи с ЗСД на пересечении Приморского шоссе, Планерной улицы и улицы Савушкина. На данном участке находится дорожная развилка, проходит ЗСД и располагаются несколько парковок рядом с торговыми центрами (ТРЦ «Вилла» и гипермаркет «Лента»). Показатели на данном участке колеблются от 59 до 64 дБА. Помимо прочего, на карте с наложением интерполяции (рис. 2) видно, что на территории между Лахта Центром и Тинькофф Ареной показатели выше, чем ожидалось – от 56 дБА и выше. Это связано с проведением строительства эстакадных съездов во время проведения замеров на данной территории.

Исходя из данных СанПиН 1.2.3685-21 [2], можно сделать вывод о том, что средний уровень шумового загрязнения на исследуемой территории является приемлемым и не несет опасности здоровью населения.

Список используемых источников:

1. Баклакова, В.В. Исследование шумового загрязнения селитебной зоны / В.В. Баклакова // Форум молодых ученых, 2018. – №6(22) – 8 с.

2. СанПиН 1.2.3685-21. Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания. – Введ. 28.01.2021. – Москва. – №2 [Электронный ресурс]. URL: <https://fsvps.gov.ru/sites/default/files/nra-files/2021/01/28/sanpin1.2.3685-21.pdf> (дата обращения 02.11.2022).

Sycheva E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of noise pollution of the territories of municipal districts 65 and 68 of the primorsky district of st. Petersburg using gis technologies

This article contains noise pollution analysis in municipal districts №65 and №68, territories of the Primorsky district, St. Petersburg. Actual noise level measurements were taken in 78 points of the Primorsky district with further mapping results using geoinformation technologies.

Key words: *noise pollution analysis, geoinformation systems, mapping, interpolation, isolines.*

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

Секция 3.1.

Безопасность компьютерных систем и сетей связи

УДК 004.56
ГРНТИ 81.93.29

РАЗРАБОТКА МОДЕЛИ СИГНАТУР АТАК ОБЕСПЕЧИВАЮЩИХ ОБНАРУЖЕНИЕ АТАК И АНОМАЛИЙ

Г. Т. Абраменко, А. Л. Зрелова, М. В. Мельник

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В последние годы кибератаки, направленные на информационные системы компаний и государственных учреждений, становятся все более изощренными. Возрастает риск утечки информации из-за целенаправленных атак и атак, использующих нераскрытые уязвимости, как программного обеспечения сервисов, так и информационной инфраструктуры в целом. В связи с этим предлагается разработка модели сигнатур для обнаружений атак и аномалий.

облачная безопасность, обнаружение атак и аномалий, белый список, черный список.

Контейнеры — по-настоящему перспективная технология, которая позволяет развертывать приложения, с помощью которой ядро или ядро ОС может разрешить выполнение нескольких изолированных процессов в одном устройстве. Контейнеры совместно используют ядро базового дистрибутива и работают поверх этой общей среды. Это означает, что каждый контейнер состоит из приложения, а также всех его зависимостей, библиотек и файлов конфигурации, но, в отличие от виртуальных машин или ПК, устраняются любые потенциально проблемные различия в базовой инфраструктуре. Базовая модель развертывания контейнеров на одном хосте представлена на рис. 1.

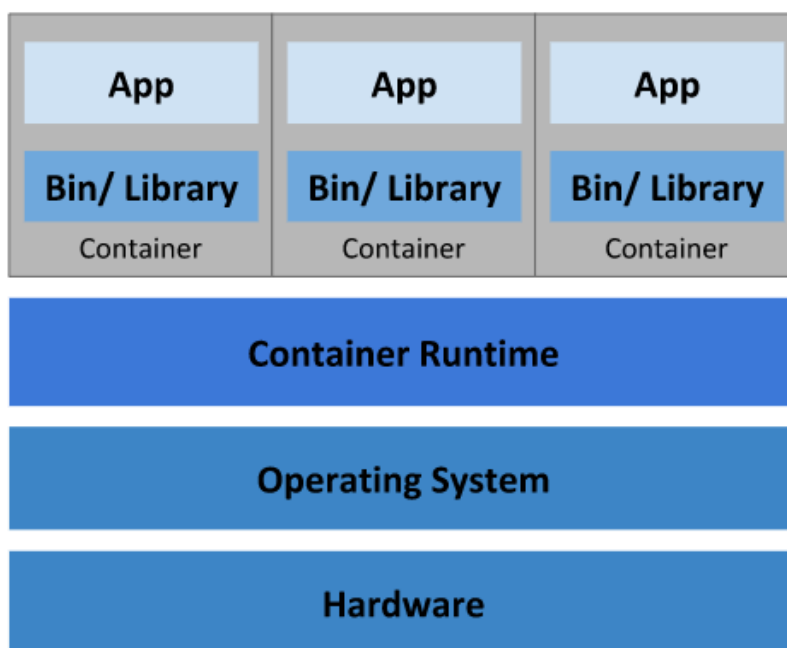


Рис. 1. Базовый вид инфраструктуры состоящей из контейнеров

Ряд преимуществ контейнеров, по сравнению с другими типами виртуализации:

- Легкость: Контейнеры легче запускать, выполнять и масштабировать.
- Низкий уровень ресурсов: контейнеры потребляют меньше ресурсов, что позволяет повысить плотность приложений.
- Обратная совместимость: контейнеры можно использовать с существующими приложениями практически без изменений.
- Модернизированный: контейнеры хорошо сочетаются с современными архитектурами приложений, такими как микросервисы.

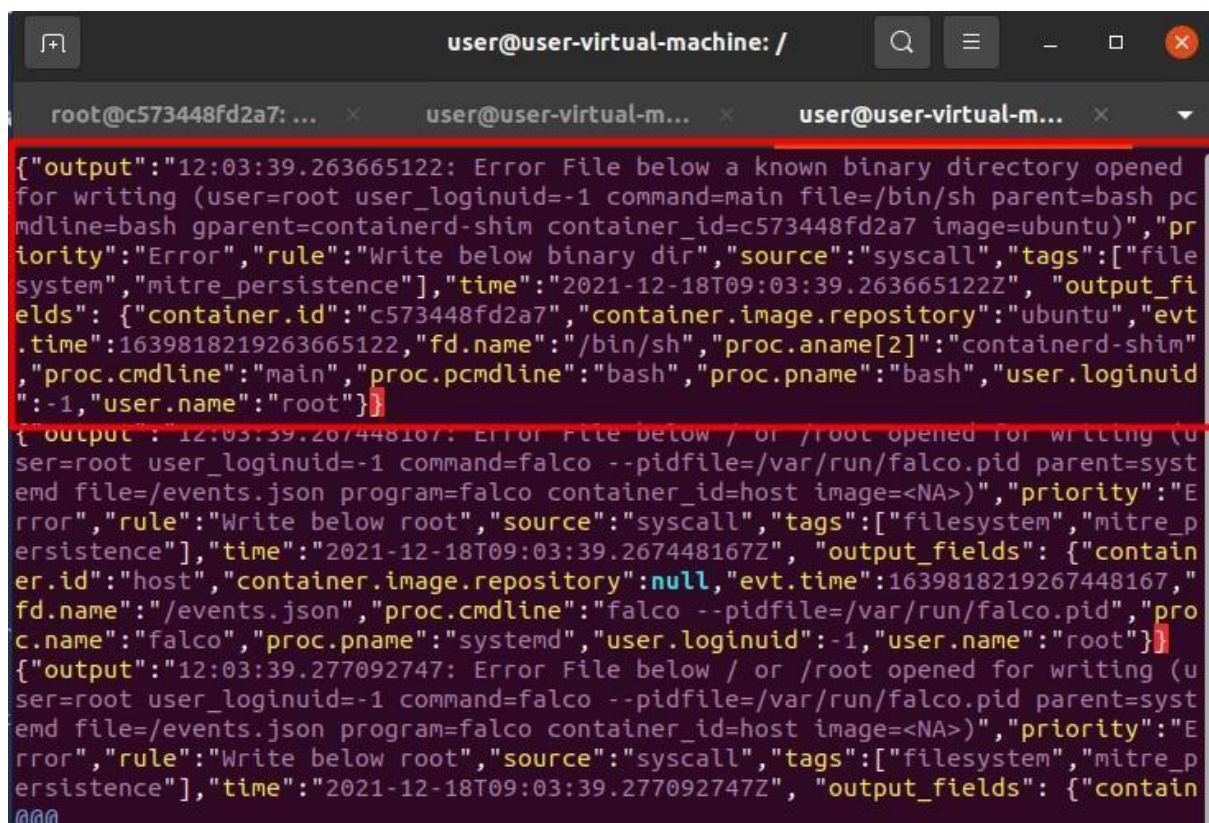
Быстро развивающиеся технологии, микросервисных архитектур и их масштабирование способствовали развитию систем облачных вычислений и контейнеризации.

По оценкам Gartner, к 2022 году более 75 % организаций по всему миру будут использовать контейнерные приложения в производственной среде по сравнению с менее чем 30 % в 2021 году [1]. Контейнерные технологии имеют ряд преимуществ. Они экономичны в использовании ресурсов, что жизненно важно для поставщика облачных услуг. Развертывание, управление и масштабирование контейнерными системами упрощается использованием дополнительных инструментов, такие как Kubernetes, Service Discovery и другие.

Вместе со стремительным развитием технологий контейнеризации появились и новые угрозы [2], такие как побег из контейнера, повышение привилегий, компрометация образа и другие. Уязвимость одного сервиса, находящегося в контейнере, ставит под удар и другие сервисы работающие в соседних контейнерах в системе контейнеризации или на хосте.

Исходя из того, что злоумышленники постоянно находят всё новые и новые методы эксплуатации уязвимостей [3], важным шагом для защиты сервисов [4] в системе контейнеризации будет создание сигнатур атак. Сигнатура атаки может включать в себя такие аргументы, как системный вызов, имя процесса, идентификатор события, адрес стэка, аргументы стэка, идентификатор пользователя, идентификатор контейнера, время события и так далее.

На рис. 2 представлен пример сигнатуры атаки, который был получен в результате использования SIEM-системы «Faslo».



```
user@user-virtual-machine: /
root@c573448fd2a7: ... x user@user-virtual-m... x user@user-virtual-m... x
{"output": "12:03:39.263665122: Error File below a known binary directory opened for writing (user=root user_loginuid=-1 command=main file=/bin/sh parent=pc mdline=bash gparent=containerd-shim container_id=c573448fd2a7 image=ubuntu)", "priority": "Error", "rule": "Write below binary dir", "source": "syscall", "tags": ["filesystem", "mitre_persistence"], "time": "2021-12-18T09:03:39.263665122Z", "output_fields": {"container.id": "c573448fd2a7", "container.image.repository": "ubuntu", "evt.time": "1639818219263665122", "fd.name": "/bin/sh", "proc.aname[2]": "containerd-shim", "proc.cmdline": "main", "proc.pcmdline": "bash", "proc.pname": "bash", "user.loginuid": "-1", "user.name": "root"}}
{ output : 12:03:39.267448167: Error File below / or /root opened for writing (user=root user_loginuid=-1 command=falco --pidfile=/var/run/falco.pid parent=sysem d file=/events.json program=falco container_id=host image=<NA>)", "priority": "Error", "rule": "Write below root", "source": "syscall", "tags": ["filesystem", "mitre_persistence"], "time": "2021-12-18T09:03:39.267448167Z", "output_fields": {"container.id": "host", "container.image.repository": "null", "evt.time": "1639818219267448167", "fd.name": "/events.json", "proc.cmdline": "falco --pidfile=/var/run/falco.pid", "proc.name": "falco", "proc.pname": "systemd", "user.loginuid": "-1", "user.name": "root"}}
{"output": "12:03:39.277092747: Error File below / or /root opened for writing (user=root user_loginuid=-1 command=falco --pidfile=/var/run/falco.pid parent=sysem d file=/events.json program=falco container_id=host image=<NA>)", "priority": "Error", "rule": "Write below root", "source": "syscall", "tags": ["filesystem", "mitre_persistence"], "time": "2021-12-18T09:03:39.277092747Z", "output_fields": {"contain
@@@
```

Рис. 2. Пример сигнатуры атаки

Уведомления были настроены следующим образом, что при открытии документа в конкретно заданной директории и попытке записи в файл «Falco» распознавал действия как атаку и выводило уведомления такого вида.

Целью исследования является разработка модели сигнатур атак, алгоритмов генерации маски атаки и профиля нормального поведения, обеспечивающих обнаружение атак и аномалий. Предполагается, что такой подход позволит адаптировать систему защиты сервисов и приложений, развернутых в контейнерах или в облачных инстансах.

В результате экспериментального исследования разрабатывается стенд для создания масок атак представляющий из себя серверную инфраструктуру состоящую из ряда контейнеров, которые содержат полноценное веб-приложение. Веб-приложение будет являться открытой площадкой для ведения переписки, позволяющее обмениваться файлами и имеет ряд уязвимостей, необходимых для проведения ряда исследований.

В ходе исследований также планируется разработать сценарии атак, такие как мисконфигурации, майнинг, отказ в обслуживании, шифрование данных, внедрение команд и другие. Планируется создать наборы данных имитации активности 100 пользователей, где каждый пользователь представляет свою уникальную активность.

Список используемых источников:

1. Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024: [Электронный ресурс]. URL: <https://www.gartner.com/en/newsroom/press-releases/2020-06-25-gartner-forecasts-strong->

revenue-growth-for-global-co?utm_source=partner&utm_medium=partner&utm_campaign=7014K000000mVAK (Дата обращения 06.11.2022).

2. Котенко И. В., Кулешов А. А., Ушаков И. А. Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack // Информатика и автоматизация. 2017. Т. 5. №. 54. С. 5-34.

3. Гурбатов Г. О., Паничев А. Д., Ушаков И. А. Обеспечение безопасности kubernetes // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы X Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 24-25 февр. 2021 г. СПб. : СПбГУТ, 2021. С. 282-286.

4. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Информационные технологии и телекоммуникации. 2021. Т. 9. №. 1. С. 47-58.

Abramenko G., Zrelova A., Melnik M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Development of a model of attack signatures that provide detection of attacks and anomalies. In recent years, cyberattacks aimed at the information systems of companies and government agencies have become increasingly sophisticated. The risk of information leakage is increasing due to targeted attacks and attacks that use undisclosed vulnerabilities, such as service software, and information infrastructure in general. In this regard, it is proposed to develop a signature model for detecting attacks and anomalies.

Key words: cloud security, attack and anomaly detection, whitelist, blacklist.

УДК 004.725.4
ГРНТИ 49.33.33

ОПРОС ПО ОБНАРУЖЕНИЮ СЕТЕВЫХ АНОМАЛИЙ НА ОСНОВЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЧЕСКИХ ТЕНДЕНЦИЙ

Д. Аконя, И. А. Ушаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время, несмотря на достижения, достигнутые за последние 30 лет, обнаружение аномалий в сетевом поведении все еще является незрелой технологией в сочетании с нехваткой коммерческих инструментов, позволяющих сделать его эффективным процессом мониторинга корпоративных сетей для обнаружения аномального поведения в сетевом трафике, что делает его важным и динамичная область исследований.

обнаружение аномалий, сетевые вторжения и система обнаружения, обнаружение вторжений, сетевой трафик, аномалии сетевого трафика, межсетевые экраны

Автоматизация сетевой инфраструктуры для выявления аномалий в сетевом трафике является важной задачей из-за сложности и скорости работы современных технологий. В настоящее время сети представляют собой сложные системы, в которых такие задачи, как правильная конфигурация компонентов, контроль изменений во времени или сама проверка правильности работы, являются чрезвычайно трудоемкой работой, требующей высокой квалификации персонала, а также большого количества времени и усилий.

В области системного управления сетевые сбои обычно подразделяются на две категории: жесткие и программные сбои [1]. Строго говоря, разница между ними дается не характером явления, вызвавшего неисправность (существуют и другие классификации по этому критерию), а степенью тяжести достигнутого состояния. Таким образом, мягкие отказы соответствуют снижению производительности любого параметра сетевого элемента, например увеличению задержки ответа службы или уменьшению доступной полосы пропускания.

ТАБЛИЦА 1. Сравнение часто используемых источников данных для обнаружения сетевых аномалий [2]

Источник	Преимущества	Недостатки
TCP dump	Предоставляет исчерпывающую информацию о работе стека протоколов TCP/IP.	Ограниченная информация
SNMP	Широко распространенный протокол	Только счетчики пакетов и битовых интерфейсов
	Доступные детализированные данные	Нет информации об IP-портах и портах TCP/UDP

IP Flow	Более низкая стоимость обработки	Ненадежное состояние протокола UDP
	Основано только на заголовках пакетов	Недостатки SCTP в сценариях, когда несколько сетевых интерфейсов должны взаимодействовать с несколькими сборщиками данных о потоках.
	Уменьшение проблем с конфиденциальностью	Трудно понять сквозной трафик
	Подробные данные о трафике	Методы выборки предлагают ненадежное представление о всей сети.

Классификация аномалий на основе ее причинного аспекта.

Причинный аспект различает аномалии в зависимости от их причины, относительно их злонамеренного или незлонамеренного аспекта. Аномалии не всегда связаны с атаками, направленными на повреждение компьютерных систем или кражу информации.

Система обнаружения сетевых аномалий.

Сетевые аномалии возникают из-за изменения «нормального» поведения сети (аномальное поведение). Как только аномалия обнаружена, обнаружение аномалии поведения сети либо инициирует автоматический ответ, либо уведомляет группы безопасности.

Архитектура системы обнаружения сетевых аномалий.

Обнаружение аномалий поведения в сети предназначено для противодействия таким угрозам. Обнаружение аномалий поведения в сети использует искусственный интеллект (ИИ) и машинное обучение (МО) для обнаружения скрытых угроз в тех частях сетевой инфраструктуры, которые не могут быть обнаружены другими инструментами безопасности, а затем уведомляет сетевые группы (рис. 1).

Непрерывный мониторинг является важной функцией обнаружения аномалий поведения сети, дополняя приложения для защиты от угроз, такие как решения для обнаружения вирусов и шпионского программного обеспечения, дополнительным уровнем безопасности.

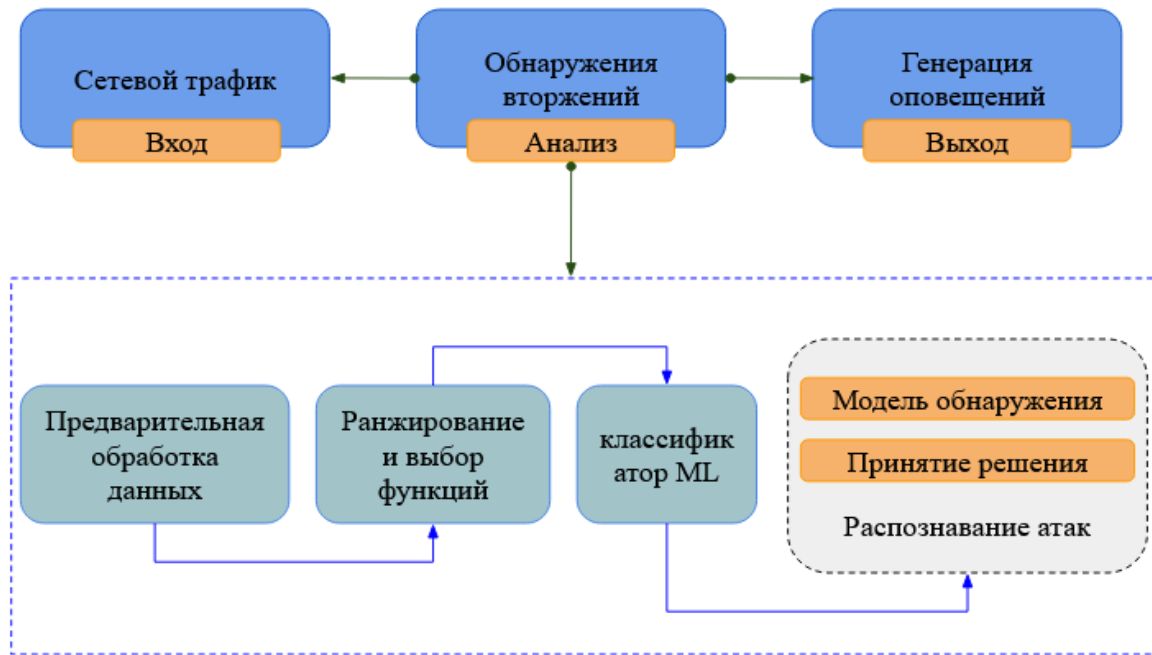


Рис. 1. Архитектура системы обнаружения сетевых аномалий

Характеристики сети, отслеживаемые программами обнаружения аномалий поведения сети в масштабе, включают пакеты, полосу пропускания, байты, объем трафика и используемый протокол. Любое подозрительное событие регистрируется в отчете и состоит из исходного и конечного IP-адресов, соответствующих портов, протоколов, временных меток и т. д. [3]

Firewall.

Firewall - это система безопасности компьютерной сети, которая ограничивает входящий, исходящий или внутренний интернет-трафик в частной сети. Как правило, он предназначен для предотвращения злонамеренной активности и предотвращения несанкционированных действий в интернете со стороны кого-либо — внутри или за пределами частной сети.

Firewall может быть аппаратным, программным, программным обеспечением как услугой (SaaS), общедоступным облаком или частным облаком (виртуальным).

Типы Firewall.

Межсетевые экраны можно разделить на два типа: межсетевые экраны на основе хоста и межсетевые экраны на основе сети (рис. 2).

Host-based firewalls.

На каждом сетевом узле установлен межсетевой экран на основе хоста, который контролирует каждый входящий и исходящий пакет. Это программное приложение или набор приложений, которые входят в состав операционной системы. Межсетевой экран хоста защищает каждый хост от атак и несанкционированного доступа.

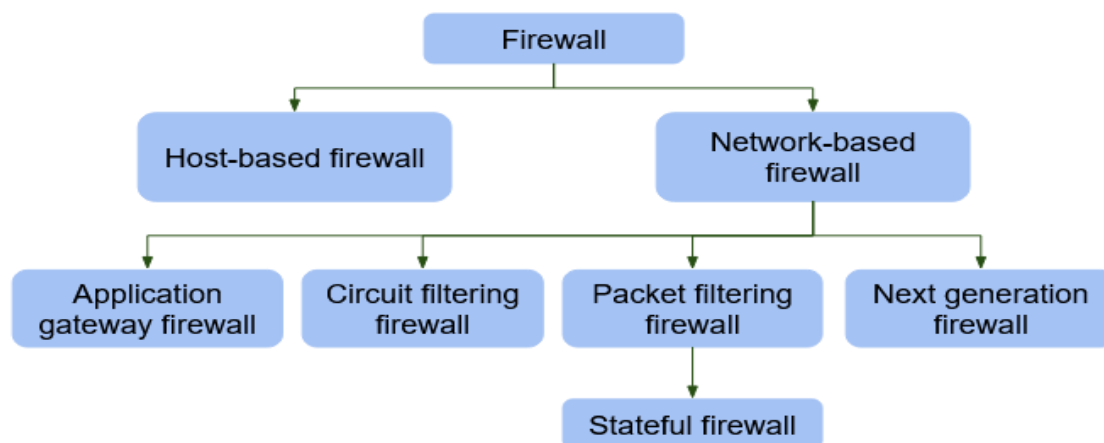


Рис. 2. Типы межсетевые экраны

Network-based firewalls.

Эти межсетевые экраны фильтруют весь входящий и исходящий трафик по сети, используя правила брандмауэра. Сетевой брандмауэр обычно представляет собой выделенную систему с установленным проприетарным программным обеспечением [3].

Заключение.

В этой статье мы рассмотрели краткий обзор обнаружения сетевых аномалий, основанный на текущих технологических тенденциях, чтобы обеспечить теоретическое понимание проблемы обнаружения аномалий в отношении различных аспектов, связанных с ней.

Список используемых источников:

1. Z. Zhang, C. Manikopoulos, J. Jorgenson, Architecture of generalized network service anomaly and fault thresholds, Proceedings of MMNS, Lecture Notes in Computer Science 2216 2001; 241–255. [Электронный ресурс]. - Режим доступа: https://link.springer.com/chapter/10.1007/3-540-45508-6_21.
2. Fernandes, G., Rodrigues, J.J.P.C., Carvalho, L.F. *et al.* A comprehensive survey on network anomaly detection. *Telecommun Syst* **70**, 447–489 (2019). [Электронный ресурс]. - Режим доступа: <https://doi.org/10.1007/s11235-018-0475-8>.
3. Spiceworks : Network anomaly detections. [Электронный ресурс]. - Режим доступа: <https://www.spiceworks.com/tech/networking/articles/network-behavior-anomaly-detection/>.

Akonya J., Ushakov I.

The Bonch-Bruевич Saint-Peterburg State University of Telecommunications

Network anomaly detection survey based on current technology trends.

At present, despite advances made over the past 30 years, network behavior anomaly detection is still an immature technology coupled with a lack of commercial tools to make it an effective enterprise network monitoring process to detect anomalous behavior in network traffic, making it an important and dynamic area of research.

Key words: *anomaly detection, network intrusion and detection system, intrusion detection, network traffic, network traffic anomalies, firewalls.*

УДК 004.056
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ТИПОВОГО ОБЪЕКТА КИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО ЗАЩИТЕ ИНФОРМАЦИИ

А. Г. Александрова, Д. О. Потомако

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире и, в частности, в сложившейся геополитической ситуации тема защиты информации, обрабатываемой в системах, относящихся к критической информационной инфраструктуре (КИИ), становится всё более актуальной. В связи с этим было проведено исследование системы защиты информации типового объекта критической информационной инфраструктуры на предмет соответствия требованиям, установленным законодательством.

критическая информационная инфраструктура, система защиты информации, локальная вычислительная сеть

В настоящее время объекты критической информационной инфраструктуры подвергаются большому количеству целевых компьютерных атак. Согласно статистике, количество кибератак на ОКИИ увеличилось в несколько раз за период с 2019 по 2021 год [1]. Так же за март 2022 года всего за несколько недель был зафиксирован рост атак на ОКИИ в 4-5 раз по сравнению с предыдущим месяцем [2].

Исходя из статистики можно сделать вывод о необходимости качественного и достаточного обеспечения защиты информации объектов КИИ в соответствии с законодательством в области информационной безопасности, а именно соблюдения мер указанных в приказе ФСТЭК России № 239 от 25 декабря 2017 г. «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»[3].

Объектом исследования является автоматизированная система в защищённом исполнении одного из предприятий атомной промышленности, которая представляет собой локальную вычислительную сеть, защищённую на разных уровнях взаимодействия (рис. 1).

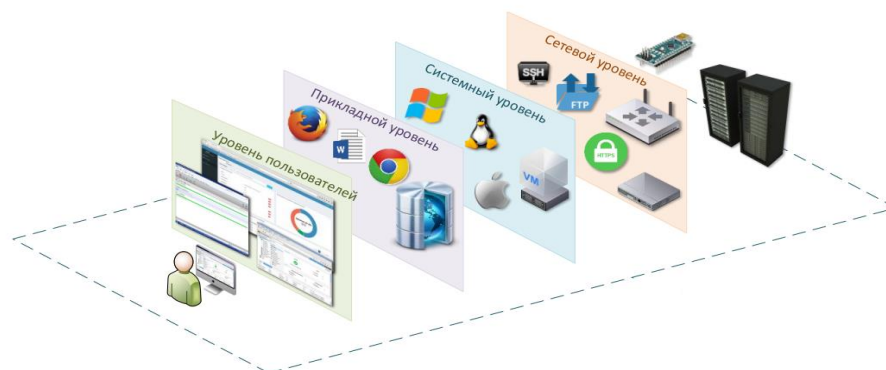


Рис. 1. Уровни взаимодействия в АСЗИ

Согласно Федеральному закону № 187 «О безопасности критической информационной инфраструктуры» необходимо обеспечивать безопасность критической информационной инфраструктуры в целях её функционирования при проведении компьютерных атак. Критической информационной инфраструктурой являются объекты КИИ и сети их взаимодействия. К объектам КИИ относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления технологическими процессами, а также сети взаимодействия между такими объектами. Все объекты критической информационной инфраструктуры подлежат категорированию, в процессе категорирования исходя из критериев значимости, а именно социальной, политической, экономической, экологической, оборонно-промышленной значимости, присваивается одна из трёх категорий [4]. Если в ходе категорирования, объекту КИИ была присвоена категория значимости он становится значимым объектом КИИ и заноситься в реестр таких объектов.

Стоит отметить, что исследованный объект критической информационной инфраструктуры не имеет категории значимости, и следовательно, не относится к значимым объектам критической информационной инфраструктуры, но по решению субъекта защита информации осуществляется согласно требованиям, предъявленным к объектам, которым присвоена третья категория значимости. Для обеспечения защиты информации значимых объектов КИИ должны применяться сертифицированные средства защиты, перечень таких средств защиты представлен в реестре ФСТЭК России.

Анализ исходных данных и оценка соответствия.

В ходе исследования был проведён анализ системы защиты информации объекта критической информационной инфраструктуры, которая включает в себя следующие средства защиты информации:

- 1) средство защиты от несанкционированного доступа;
- 2) средство антивирусной защиты;
- 3) система межсетевое экранирования;
- 4) система мониторинга и сбора информации о событиях безопасности

Помимо перечисленных средств защиты информации используются технология dot1x, разделение сети на Vlan-ы, терминальный доступ в сеть Интернет.

Средство защиты информации от несанкционированного доступа представляет собой систему, включающую в себя средства централизованного управления, защитный функционал, а также средства оперативного реагирования и мониторинга безопасности информационной системы, и имеет следующий набор функций: разграничение прав доступа, организация безопасного входа в систему, контроль подключаемых устройств, создание доверенной среды, контроль действий приложений, регистрация, учёт и мониторинг событий ИБ.

Используемое в АСЗИ средство антивирусной защиты (далее - САВЗ) обеспечивает многоуровневую (эшелонированную) защиту, контроль программ и устройств, веб-контроль, шифрование данных, что называется «проактивными» технологиями. САВЗ имеет панель управления,

предназначенную для централизованного решения задач по обслуживанию и управлению системы защиты. САВЗ включает в себя компоненты защиты и контроля. К компонентам защиты относятся:

- анализ поведения (получение данных о действиях программ и их передача другим компонентам);
- защита от эксплойтов (отслеживание исполняемых файлов, запускаемых уязвимыми программами, блокировка запуска файла если запуск не инициирован пользователем);
- предотвращение вторжений (регистрация действий, совершаемых программами в ОС и регулирование действий программ согласно правилам доступа к информации);
- откат вредоносных действий (отмена действий, произведённых вредоносными программами);
- защита от файловых угроз (перехват обращений к файлу и проверка этого файла на присутствие вирусов и программ, представляющих угрозу);
- защита от веб-угроз;
- защита от почтовых угроз.
- К компонентам контроля относятся:
 - контроль программ (отслеживание попыток запуска программ пользователями и регулирование запуска программ);
 - контроль устройств (ограничение доступа к устройствам, являющихся источниками информации);
 - веб-контроль (ограничение доступа к веб-ресурсам для разных групп пользователей);
 - адаптивный контроль аномалий (отслеживание и регулирование потенциально опасных действий, не характерных для защищаемого АРМ).

Система межсетевого экранирования, используемая для защиты сети, обладает следующим набором функций: построение частных виртуальных сетей, удалённый доступ с мобильных устройств, система предотвращения вторжений (IPS), защита от ботнет сетей, потоковый антивирус, защита корпоративной почты, интеграция со службой Active Directory, мониторинг параметров, межсетевой экран уровня приложений, безопасность Web + функционал Proxu, защита от утечек информации (DLP), технология песочницы, технология отчистки файлов и приоритезация трафика (QoS).

Для мониторинга событий ИБ и выявления инцидентов в реальном времени в АСЗИ используется система класса SIEM, обеспечивающая возможность проведения 3-х видов мероприятий: превентивные, детективные и коррективные. Функциональные возможности рассматриваемой системы мониторинга событий ИБ и выявления инцидентов в реальном времени:

- сбор событий от разных источников, с поддержкой таких протоколов как syslog, windows Event Log, NetFlow, SNMP и т.д.;
- нормализация событий и приведение их к общему стандарту, а также подготовка к дальнейшей обработке (событие безопасности преобразовывается в структурированный объект с обязательными параметрами: дата/время, идентификатор, актив, к которому относятся события, тип действия и статус);

- фильтрация событий, не относящихся к безопасности;
- удаление или объединение повторяющихся событий для сокращения объема хранения (агрегация);
- поиск взаимосвязанных инцидентов по заданным правилам и их анализ (корреляция);
- журналирование событий и состояний систем для проведения глубокого анализа.

Перейдём к рассмотрению технологии IEEE 802.1X (dot1x). Технология dot1x предназначена для аутентификации и авторизации на канальном уровне. При подключении к сетевому интерфейсу пользователь может отправлять только служебную информацию для прохождения процедуры аутентификации. Аутентификация dot1x используется в качестве механизма управления доступом для интерфейсов LAN (Local Area Network). Таким образом, с помощью технологии dot1x реализована защита от несанкционированного подключения к ЛВС.

Также в АСЗИ применяется технология сегментирования сети VLAN, которая позволяет объединять устройства в сети в отдельные группы в зависимости от выполняемых функций отделами или подразделениями предприятия. VLAN позволяет логически объединять устройства, независимо от их физического расположения. С точки зрения информационной безопасности технология VLAN используется для изолирования трафика в рамках одного VLAN, то есть получение несанкционированного доступа к трафику из другого VLAN невозможно.

Заключение.

Проанализировав возможности перечисленных выше средств защиты информации, применяемых в исследованной локальной вычислительной сети, был сделан вывод о возможности «перекрытия» данными средствами защиты информации мер, предъявленных к информационной системе [3], результаты представлены в таблице 1.

ТАБЛИЦА 1. Меры защиты информации, выполняемые средствами защиты информации

Средство защиты информации	Меры
Средство защиты от НСД	УПД.2; УПД.6; УПД.10; УПД.11; ЗНИ.5; ЗНИ.7; ЗИС.21; ОПО.1.
Средство антивирусной защиты	ИАФ.2; АВЗ.1; АВЗ.2; АВЗ.4; ОЦЛ.1; ЗИС.3; ОПО.1.
Система межсетевое экранирования	ИАФ.5; ИАФ.7; УПД.13; УПД.14; ЗИС.6; ЗИС.19; ЗИС.20; ЗИС.21; ЗИС.32; ЗИС.34; ЗИС.35; ЗИС.38; ОПО.1.
Система мониторинга и сбора информации о событиях безопасности	АУД.4; АУД.6; АУД.7; АУД.8; ИНЦ.1; ИНЦ.2; ИНЦ.3; ИНЦ.6; ОПО.1.
Системное ПО	ИАФ.1; ИАФ.2; ИАФ.3; ИАФ.4; УПД.1; УПД.2; УПД.4; УПД.5; АУД.3; ОДТ.4; ОДТ.5; ОДТ.6; ОДТ.8; ЗИС.1.

Все проанализированные меры обеспечивают выполнение базового набора мер, следовательно, организация защиты информации типового объекта КИИ

удовлетворяет требованиям по обеспечению защиты информации в соответствии с 3-ей категорией значимости.

Список используемых источников:

1. ЦИПР 2021 [Электронный ресурс]. URL: <https://www.group-ib.ru/media-center/press-releases/critical-infrastructure-2021/> (дата обращения 13.10.2022).
2. Новостной портал cisoclub [Электронный ресурс]. URL: <https://cisoclub.ru/v-rossii-rastyot-kolichestvo-kiberatak-na-sistemy-gosudarstvennogo-upravleniya-i-obekty-kii/> (дата обращения 13.10.2022).
3. Приказ ФСТЭК России № 239 от 25 декабря 2017 г. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (дата обращения 13.10.2022)
4. Федеральный Закон Российской Федерации № 187 «О безопасности критической информационной инфраструктуры» (дата обращения 13.10.2022)

Aleksandrova A., Potomako D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Study of the information security system of a typical cue object for compliance with information security requirements.

In the modern world and, in particular, in the current geopolitical situation, the topic of protecting information processed in systems related to critical information infrastructure (CII) is becoming more and more relevant. In this regard, a study of the information protection system of a typical object of critical information infrastructure was carried out for compliance with the requirements established by law.

Key words: critical information infrastructure, information security system, local area network.

УДК 004.056
ГРНТИ 81.93.29

МОДЕЛЬ УГРОЗ ДЛЯ ТИПОВОГО ОБЪЕКТА КИИ, ФУНКЦИОНИРУЮЩЕГО В СФЕРЕ АТОМНОЙ ЭНЕРГЕТИКИ

А. Г. Александрова, Д. О. Потомако

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Объекты критической информационной инфраструктуры являются важной составляющей экономики государства. Все сферы функционирования критических объектов играют основополагающую роль в жизни населения страны. Обеспечение безопасности объектов критической информационной инфраструктуры – одно из основных направлений политики государства. Достаточный уровень информационной безопасности для любой информационной системы подразумевает перекрытие возможных угроз безопасности организационными и техническими мерами по защите информации. Для определения необходимого набора мер предлагается использовать разработанную модель угроз.

критическая информационная инфраструктура, модель угроз, нарушитель, информационная безопасность

В настоящее время особое значение приобретает обеспечение информационной безопасности объектов критической информационной инфраструктуры, так как по мнению ведущих экспертов в данной области, сейчас против России ведется организованная кибервойна, целью которой является вывод из строя всей критической инфраструктуры страны [1]. В связи с этим была создана программа импортозамещения, был опубликован указ №166 от 30 марта 2022 г. «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации», который предписывает согласовывать закупки иностранного ПО для использования на значимых объектах КИИ для субъектов КИИ, выступающих заказчиками закупок в соответствии с Федеральным законом №223, а также вводит полный запрет на использование таких продуктов с 2025 года [2].

Для выбора необходимого программного обеспечения, программно-аппаратных комплексов, в том числе средств защиты информации, которые позволяли бы качественно и достаточно обеспечивать информационную безопасность информационных систем объектов критической информационной инфраструктуры (КИИ), необходимо определить актуальные источники угроз безопасности, и следовательно, актуальные угрозы информационной безопасности.

Под источниками угроз безопасности информации подразумеваются нарушители. Все нарушители делятся на внешних и внутренних. Внешние нарушители – нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации [3]. К внешним нарушителям можно отнести: преступные организации, конкурентов, физических лиц (хакеров) и бывших работников или пользователей информационной системы. Внутренние нарушители – нарушители, имеющие права доступа в контролируемую (охраняемую) зону

(территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей [3]. К внутренним нарушителям можно отнести: администраторов системы, операторов системы, обслуживающий персонал и т.д.

Для определения актуальных угроз безопасности разрабатывается модель угроз безопасности для конкретной информационной системы. Структура модели угроз безопасности информации согласно методическому документу ФСТЭК по определению актуальных угроз от 5 февраля 2021 г. [3] представлена на рис. 1.



Рис. 1. Структура модели угроз безопасности информации

В процессе разработки модели угроз в первую очередь определяются негативные последствия, наступающие вследствие возникновения угроз безопасности информации. Примеры выявленных негативных последствий для объекта критической информационной инфраструктуры, функционирующего в сфере атомной энергетики представлены в таблице 1.

ТАБЛИЦА 1. Виды рисков и негативные последствия.

№	Виды риска (ущерба)	Возможные негативные последствия
1	(У1) Ущерб физическому лицу	- нарушение конфиденциальности (утечка) ПДн; - разглашение ПДн граждан; - и т. д.
2	(У2) Ущерб юридическому лицу	- недополучение ожидаемой прибыли; - необходимость дополнительных затрат на закупку товаров, работ или услуг (в том числе закупка ПО и ТС, вышедших из строя, замена, настройка, ремонт указанных средств); - нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и (или) процесса; - и т. д.
3	(У3) Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	- снижение уровня дохода государственной корпорации, государственной организации или организации с государственным участием; - возникновение ущерба бюджетам Российской Федерации; - утечка информации ограниченного доступа; - и т. д.

В ходе оценки угроз безопасности информации должны быть определены информационные ресурсы и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям – объекты воздействия. К объектам воздействия можно отнести:

- информация (данные), содержащаяся в системах и сетях (в том числе защищаемая информация, персональные данные, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.);
- программно-аппаратные средства обработки и хранения информации (в том числе автоматизированные рабочие места, серверы, включая промышленные, средства отображения информации, программируемые логические контроллеры, и т.д.);
- программные средства (в том числе системное и прикладное программное обеспечение, включая серверы приложений, веб-приложений, системы управления базами данных, системы виртуализации);
- машинные носители информации, содержащие как защищаемую информацию, так и аутентификационную информацию;
- и т.д.

Угроза безопасности информации возможна, если имеются нарушитель или иной источник угрозы, объект, на который осуществляются воздействия, способы реализации угрозы безопасности информации, а реализация угрозы может привести к негативным последствиям [3]. Примеры внутренних и внешних нарушителей, то есть источников угроз безопасности информации, а также возможных целей реализации угроз безопасности приведены в таблице 2.

ТАБЛИЦА 2. Нарушители и цели реализации угроз безопасности информации.

№	Виды нарушителя	Возможные цели реализации угроз безопасности информации
1	Специальные службы иностранных государств	Нанесение ущерба государству в области обеспечения обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики, в том числе дискредитация или дестабилизация деятельности отдельных органов государственной власти, организаций, получение конкурентных преимуществ на уровне государства, срыв заключения международных договоров, создание внутривластного кризиса
2	Конкурирующие организации	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды
3	Системные администраторы и администраторы безопасности	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Мечь за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия.

Для построения сценариев реализации угроз безопасности информации для КИИ необходимо определить основные тактики и типовые техники, которые им соответствуют. После определения тактик, разрабатываются сценарии реализации угроз безопасности, при этом необходимо учитывать особенности объектов критической информационной инфраструктуры. Сценарий угрозы – последовательность действий нарушителя, способная привести к реализации угрозы [3]. В сценариях угроз прописаны возможные применяемые техники для реализации той или иной угрозы безопасности информации в системе через прописанные тактики. Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации [3]. Пример сценария для способа реализации «Угроза несанкционированного доступа к базе данных, содержащей защищаемую информацию» представлен на рис. 2.

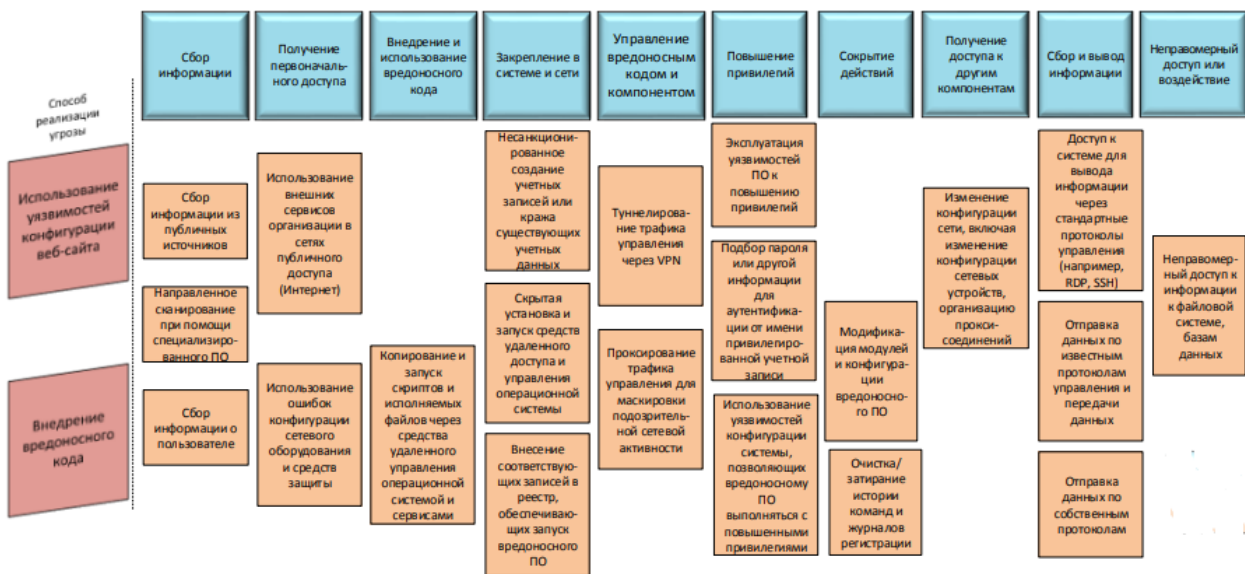


Рис. 2. Пример сценария угроз с указанием тактик и техник

Последним этапом разработки модели угроз безопасности информации является определение актуальных угроз безопасности исходя из данных, полученных на предыдущих этапах.

Таким образом, внедрение разработанной модели угроз для типового объекта КИИ, функционирующего в сфере атомной энергетики позволит решить следующие задачи:

- определить базовый набор мер для обеспечения информационной безопасности;
- разработать систему защиты информации, которая обеспечит предотвращение реализации актуальных угроз безопасности информации;
- определить мероприятия, направленные на предотвращение несанкционированного доступа;
- контролировать уровень защищенности объекта КИИ.

Модель угроз безопасности информации поможет оценить все возможные угрозы и уязвимости для типового объекта критической информационной инфраструктуры, а также выбрать необходимые средства защиты информации для обеспечения достаточного уровня защищенности.

Список используемых источников:

1. Новостной портал TAdviser: [Электронный ресурс]. URL: <https://inlnk.ru/poXPmR> (Дата обращения 03.11.2022).
2. CNews Analytics: [Электронный ресурс]. URL: https://www.cnews.ru/reviews/importozameshchenie_2022/cases/perehod_na_otchestvennye_analogi (Дата обращения 03.11.2022).
3. Методический документ методика оценки угроз безопасности информации, Утвержден ФСТЭК России 5 февраля 2021 г.

Aleksandrova A., Potomako D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Threat model for a typical cue object operating in the field of nuclear energy.

Critical information infrastructure facilities are an important component of the state's economy. All areas of functioning of critical facilities play a fundamental role in the life of the country's population. Ensuring the security of critical information infrastructure facilities is one of the main directions of state policy. A sufficient level of information security for any information system implies the overlap of possible security threats with organizational and technical measures to protect information. To determine the required set of measures, it is proposed to use the developed threat model.

Key words: critical information infrastructure, threat model, intruder, information security

УДК 004.056.5
ГРНТИ 81.93.29

СРАВНЕНИЕ СПОСОБОВ КОНТРОЛЯ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

И. Н. Бабков, З. А. Федорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются вопросы контроля состояния информационной безопасности на предприятии. Приведены способы проведения контроля, выполняемые как вручную, так и автоматизировано; дана их характеристика и сравнение. Статья может быть полезна при выборе конкретных способов контроля состояния информационной безопасности на различных предприятиях.

информационная безопасность, комплексная система защиты информации, SIEM-системы, DLP-системы, SOC, политика информационной безопасности, информационные системы, защита информации

В настоящее время резко возрастает количество разнообразных кибератак на информационные ресурсы предприятий. В связи с этим необходимо сокращать время реагирования на события и инциденты информационной безопасности.

Процесс обеспечения информационной безопасности (ИБ) осуществляется в течение всего времени работы предприятия [1, с. 135]. Контроль состояния ИБ можно проводить разными способами, как вручную, так и автоматизировано, осуществляя:

- анализ журналов аудита;
- получение данных из подсистем комплексной системы защиты информации (КСЗИ);
- DLP-системы;
- SIEM-системы и др.

Выбор наиболее приемлемого способа контроля определяется видом деятельности, возможностями и размером предприятия.

Рассмотрим вышеперечисленные способы контроля состояния информационной безопасности подробнее.

1. Контроль состояния информационной безопасности с помощью журналов.

Организация неавтоматизированной работы с событиями – трудоемкая задача. Большое количество данных в различных форматах необходимо собирать и обрабатывать, вести их архив. Чтобы организовать эффективную ручную обработку событий безопасности, необходимо большое количество квалифицированных специалистов-аналитиков.

Даже на небольшом предприятии в журналах аудита может регистрироваться до нескольких десятков событий в секунду, что делает их анализ данным способом длительным и неэффективным. Из-за большого объема работы вручную этот способ часто не отражает всей текущей ситуации.

Информация о событиях должна постоянно накапливаться и анализироваться для получения реального представления об уровне информационной безопасности на предприятии. Проанализировать собранные вручную данные без использования автоматизированных систем практически невозможно. Сейчас такой способ редко встречается – обычно на малых предприятиях. В этом случае, чтобы минимизировать возможные последствия для корпоративной информации, необходимо создать «сильную» и всеобъемлющую политику информационной безопасности (ПИБ), предусматривающую все возможные угрозы для предприятия.

2. Контроль состояния информационной безопасности – получение данных из подсистем КСЗИ.

Для этого подхода также характерен ручной анализ. Информация о событиях ИБ собирается средствами аудита, встроенными в системное и прикладное программное обеспечение, и анализируется администраторами безопасности с помощью стандартных средств просмотра журналов.

Несмотря на большое количество антивирусных приложений, межсетевых экранов и других средств защиты информации, не видно общей картины происходящего в инфраструктуре предприятия, так как механизмы защиты работают изолированно друг от друга; между ними нет связи, позволяющей централизованно следить за событиями ИБ, как можно быстрее обнаруживать и реагировать на инциденты.

В таком случае, специалисты тратят значительные усилия на реализацию основной функции анализа – например, объединение данных журналов с нескольких машин в сети. Как правило, этот подход имеет низкую эффективность и оперативность анализа, а также реагирования. Такой способ чаще всего встречается в небольших компьютерных сетях с ограниченным количеством пользователей.

Для оптимального контроля событий нарушения ИБ необходимо автоматизировать процессы обработки событий информационной безопасности, ведения журналов, которые при ручном анализе займут очень большое время.

Автоматизированные системы обработки событий должны:

- позволять собирать события от всех программно-технических средств обеспечения защищенности, используемых на предприятии;
- приводить события к единому, удобному для понимания формату;
- хранить необходимые объемы данных;
- предоставлять возможность поиска в архиве;
- предоставлять механизмы формирования отчетов;
- осуществлять корреляцию собранных событий [2, с. 20].

Процесс обработки событий в таком случае включает основные шаги: нормализация (приведение к единому формату) и агрегирование (накопление) данных, корреляция и визуализация.

Ошибочные или преднамеренные действия персонала наносят ощутимый вред безопасности предприятия. Для преодоления этой проблемы внедряются системы предотвращения утечки данных (DLP-системы), а также системы анализа и сбора информации (SIEM-системы).

3. Контроль состояния информационной безопасности с помощью DLP-

систем.

DLP-системы являются программно-аппаратными комплексами средств, которые обеспечивают защиту корпоративной информации от угроз неправомерной передачи данных из защищенного сегмента автоматизированной системы путем осуществления анализа трафика и выполнения определенных действий (мониторинг, блокирование, перемещение в карантин), в зависимости от обнаруженного содержания [3, с. 75].

DLP-системы могут отслеживать и регистрировать данные, которые покинули информационную систему предприятия через электронную почту или интернет, а также блокировать передачу данных, соответствующих определенным критериям (например, номера социального страхования, номера банковских счетов и медицинские данные).

Основные функции DLP-системы:

- предотвращение убытков, связанных с утечкой корпоративной информации;
- выявление случаев мошенничества и саботажа;
- контроль соблюдения трудовой дисциплины и регламента работы;
- повышение производительности труда сотрудников;
- предотвращение использования работниками корпоративных ресурсов в личных целях;
- выполнение требований регуляторов;
- упрощение процесса мониторинга.

4. Контроль состояния информационной безопасности с помощью SIEM-систем.

Система управления информацией и событиями безопасности (SIEM-система) обеспечивает обнаружение угроз и реагирование на инциденты путем сбора данных о событиях безопасности с основных систем информационной безопасности в режиме реального времени и представления этих данных в виде оперативной информации через единый интерфейс. SIEM-система позволяет уменьшить возможный ущерб путем выявления угрозы и принятия мер до того, как системам предприятия будет нанесен ущерб [4, с. 73].

Статистические данные, собранные и обработанные с помощью SIEM-системы позволяют сделать вывод об эффективности работы как системы безопасности всего предприятия, так отдельных средств защиты информации. Она обеспечивает аналитику безопасности и дает возможность анализировать данные журналов, чтобы составить картину произошедших инцидентов безопасности.

С помощью SIEM-системы можно добиться почти полной автоматизации процесса выявления угроз, что существенно упрощает управление безопасностью и администрирование на предприятии.

Внедрение SIEM – первый шаг на пути создания механизма Security Operations Center (SOC).

5. Контроль состояния информационной безопасности с помощью системы оперативного управления информационной безопасностью.

Уникальность SOC состоит в комплексном подходе к обеспечению

информационной безопасности, основанном на трех направлениях – люди, процессы и технологии. Каждый участник SOC знает свои роли и обязанности, правила реагирования и процессы взаимодействия с другими.

На крупных предприятиях с развитой ИТ-инфраструктурой и большим количеством средств защиты проблематично получить полную картину без специализированных технических средств.

SOC предоставляет полную картину текущего состояния информационной безопасности предприятия. Данные поступают из различных источников – с операционных систем, сетевых устройств, баз данных, приложений. С его помощью можно отслеживать события, происходящие в информационной системе, анализировать их и сопоставлять с другими данными, отслеживать степень выполнения требований законодательства, нормативных актов и ПИБ, существующие уязвимости, оперативно реагировать на обнаруженные инциденты ИБ [5, с. 35].

SOC – это совокупность взаимосвязанных и хорошо отлаженных процессов управления информационной безопасностью:

- контроль состояния ИБ (мониторинг событий, аудит действий сотрудников);
- управление инцидентами ИБ;
- обеспечение выполнения требований законодательства, международных и отраслевых стандартов, политики информационной безопасности;
- четкое разделение должностных обязанностей внутри предприятия.

Таким образом, при организации обеспечения безопасности с помощью SOC возможно наладить непрерывный процесс повышения эффективности существующих мер защиты. Проведение постоянного анализа текущих событий и инцидентов ИБ, установление причин их возникновения с привлечением различных подразделений дает возможность оценить результативность применяемых на предприятии защитных мер, выявить недостатки и выработать предложения по их замене или корректировке. С помощью SOC можно организовать эффективную работу сотрудников путем сведения данных на одну консоль и автоматизации анализа событий ИБ.

Автоматизация процесса управления инцидентами информационной безопасности позволяет:

- незамедлительно принимать решение по устранению инцидента, на основе анализа сведений о ранее произошедших инцидентах;
- хранить и обрабатывать информацию о событиях и инцидентах ИБ, а также о действиях, предпринятых для их устранения;
- анализировать собранные данные.

Можно сделать вывод, что аналитика безопасности развивается, используя новые технологии. Благодаря этому, происходит оптимизация контроля информационной безопасности.

В данной статье проведено сравнение способов контроля состояния ИБ на различных предприятиях по критерию эффективности. Также проведены оценки возможностей автоматизированных систем различных классов и назначения (DLP, SIEM, SOC) в части контроля состояния ИБ. С учетом полученных результатов, при выборе способов контроля на конкретном предприятии

целесообразно максимально использовать получение данных из автоматизированных систем. При этом, для учета специфики предприятия, необходимо разработать соответствующий регламент проведения контроля состояния ИБ.

Список используемых источников:

1. Шаньгин В.Ф. Информационная безопасность и защита информации. М.: ДМК, 2014. – 702 с.
2. Мелехин И. Управление инцидентами // JetInfo: Информационный бюллетень – 2006. – № 7 (158). – с. 14–20.
3. Андрианов В.И., Бахтин Д.В., Штеренберг С.И. DLP-система для защиты корпоративных или персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. – СПб.: СПбГУТ – 2020. – Т.1., с. 75–80. URL: <https://www.sut.ru/doci/nauka/1AEA/APINO/9-APINO-2020,%20T.1.pdf> (дата обращения: 17.10.2022).
4. Бабков И.Н. Анализ эффективности SIEM-системы в организации // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. – СПб.: СПбГУТ – 2021. – Т.1., с. 72–77. URL: <https://www.sut.ru/doci/nauka/1AEA/APINO/10-APINO-2021.%20T.1.pdf> (дата обращения: 20.10.2022).
5. Медведев А. Самый безопасный SOC // JetInfo: Информационный бюллетень – 2011. – № 3 (212). – с. 9–37.

Babkov I., Fedorova Z.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

The ways of information security monitoring at the enterprise.

The article discusses the issues of monitoring the information security at the enterprise. It describes the ways of control that are carried out manually and automatically. Characteristics of each of these methods are presented.

Key words: information security, integrated information security system, SIEM-systems, DLP-systems, SOC, information security policy, information systems, information protection.

УДК 004.056.53
ГРНТИ 81.93.29

ИЗУЧЕНИЕ ЗАЩИТНЫХ МЕХАНИЗМОВ DNS-ФАРМИНГА

Абдельрахман Баракат

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В этой статье мы поговорим об атаке DNS pharming, а также о самых популярных методах применения этой атаки, а также об основных методах защиты ваших систем от этой атаки.

DNS, Фарминг, Веб-сайты, IP-адреса, HTTP, HTTPS, SMS

Представьте себе, что в качестве шутки над младшими ученики старшей школы меняют все номера комнат в своем кампусе средней школы, чтобы новые ученики, которые еще не знают планировку кампуса, на следующий день заблудились и оказались не в тех классах. Теперь представьте, что несопадающие номера комнат записаны в каталоге кампуса, и студенты продолжают ходить не в те комнаты, пока кто-нибудь, наконец, не заметит и не исправит каталог.

Так что, если пользователь хотел перейти на веб-сайт, но запись DNS была неверной, и вся информация, введенная пользователем, регистрируется во вредоносной базе данных, это называется фармингом DNS.

DNS-фарминг [1] – это мошенническая практика, при которой вредоносный код устанавливается на персональный компьютер (ПК) или сервер, направляя пользователей по ложному пути на мошеннические веб-сайты без их ведома или согласия. Цель состоит в том, чтобы пользователи вводили свою личную информацию. Как только информация, такая как номер кредитной карты, номер банковского счета или пароль, была введена на мошенническом веб-сайте, преступники получают ее, и конечным результатом может стать кража личных данных.

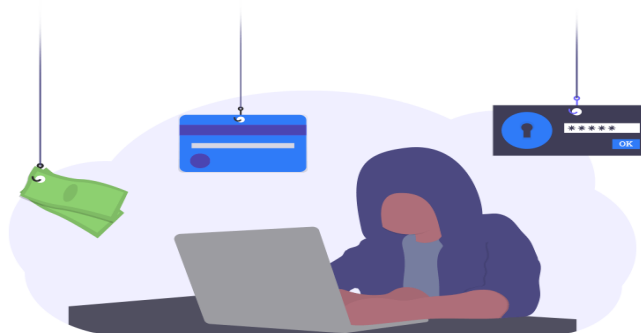


Рис. 1. Цели DNS-фарминга

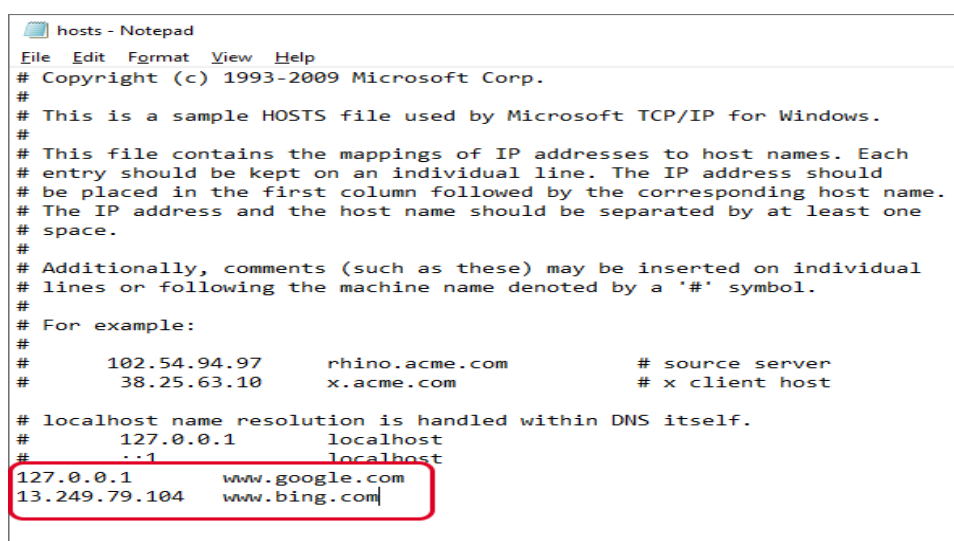
Кого затрагивает DNS-фарминг [2]?

DNS-фарминг в первую очередь влияет на конечных пользователей, но также может повлиять на владельцев веб-сайтов.

Популярные фарминговые атаки на DNS [3]:

1. Изменение файла HOSTS, когда злоумышленники уже скомпрометировали компьютер жертвы:

Используются пары имени хоста и IP-адреса в файле HOSTS (/etc/hosts). для локального поиска; они имеют преимущество перед удаленным поиском DNS. Например, если имеется следующее запись в файле HOSTS на компьютере пользователя, www.google.com будет разрешен как 127.0.0.1 в компьютер пользователя без запроса DNS-сервера



```

hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com               # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
127.0.0.1       www.google.com
13.249.79.104  www.bing.com
    
```

Рис. 2. Записи файла хоста

2. Прямая подделка ответа пользователю:

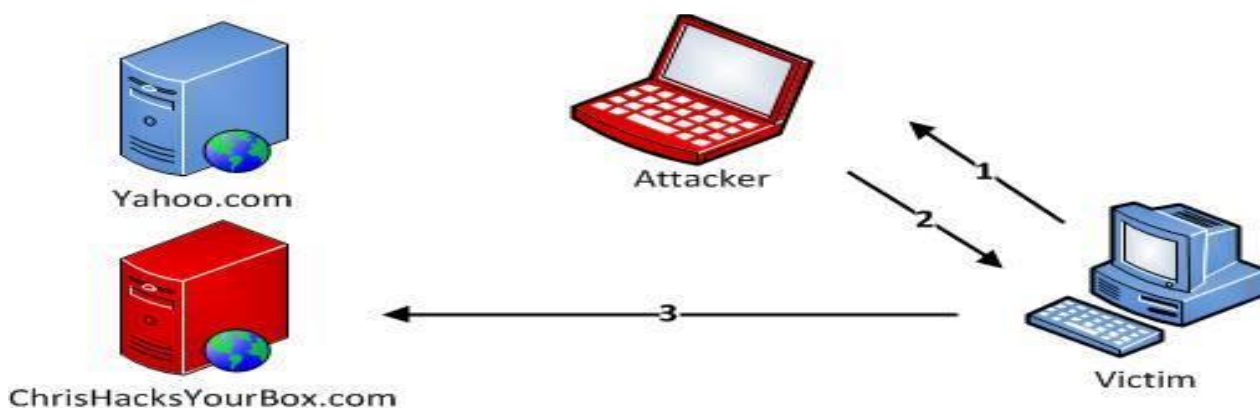
В этой атаке машина жертвы не была скомпрометирована, поэтому злоумышленники не могут напрямую изменить DNS процесс запроса на машине жертвы. Однако, если злоумышленники находятся в той же локальной сети, что и жертвы, они все еще могут нанести большой ущерб.

Когда пользователь вводит имя веб-сайта (имя узла, например www.example.com) в веб-браузере, компьютер пользователя отправит DNS-запрос на DNS-сервер для разрешения IP-адреса имени хоста.

Услышав этот запрос DNS, злоумышленники могут подделать поддельный ответ DNS. Поддельный ответ DNS будет принят компьютером пользователя, если он соответствует следующим критериям:

- Исходный IP-адрес должен совпадать с IP-адресом DNS-сервера.
- IP-адрес назначения должен совпадать с IP-адресом машины пользователя.
- Номер исходного порта (UDP-порт) должен совпадать с номером порта, на который был отправлен DNS-запрос. (обычно порт 53).
- Номер порта назначения должен совпадать с номером порта, с которого был отправлен DNS-запрос.

- Контрольная сумма UDP должна быть правильно рассчитана.
- Идентификатор транзакции должен совпадать с идентификатором транзакции в DNS-запросе.
- Имя домена в разделе вопроса ответа должно совпадать с именем домена в вопросе.
- Имя домена в разделе ответов должно совпадать с именем домена в разделе вопросов
- Компьютер пользователя должен получить DNS-ответ злоумышленника, прежде чем он получит легитимный DNS-ответ.



1. Legitimate DNS Request Destined for DNS Server
2. Fake DNS Reply from Listening Attacker
3. Victim begins communicating with malicious site as a result

Рис. 3. Атаковать пользователя напрямую, отвечая на DNS-запрос

3. Отравление кеша DNS-сервера:

Вышеупомянутая атака нацелена на машину пользователя. Для достижения длительного эффекта каждый раз, когда пользователь машина отправляет DNS-запрос для `www.example.com`, машина злоумышленника должна отправить поддельный DNS-ответ. Это может быть не так эффективно; есть гораздо лучший способ проводить атаки, нацеливаясь на DNS-сервер вместо машины пользователя.

Когда DNS-сервер Z получает запрос, если имя хоста не находится в домене Z, он запрашивает другие DNS-серверы для разрешения имени хоста. Обратите внимание, что домен нашего DNS-сервера это `example.com`; поэтому для DNS-запросов других доменов (например, `www.google.com`) DNS-запросы сервер Z будет запрашивать другие DNS-серверы. Однако, прежде чем Z запрашивает другие DNS-серверы, он сначала ищет ответ из собственного кэша; если ответ есть, DNS-сервер Z просто ответит информацией от своего кеша. Если ответа нет в кеше, DNS-сервер попытается получить ответ от других DNS-серверов.

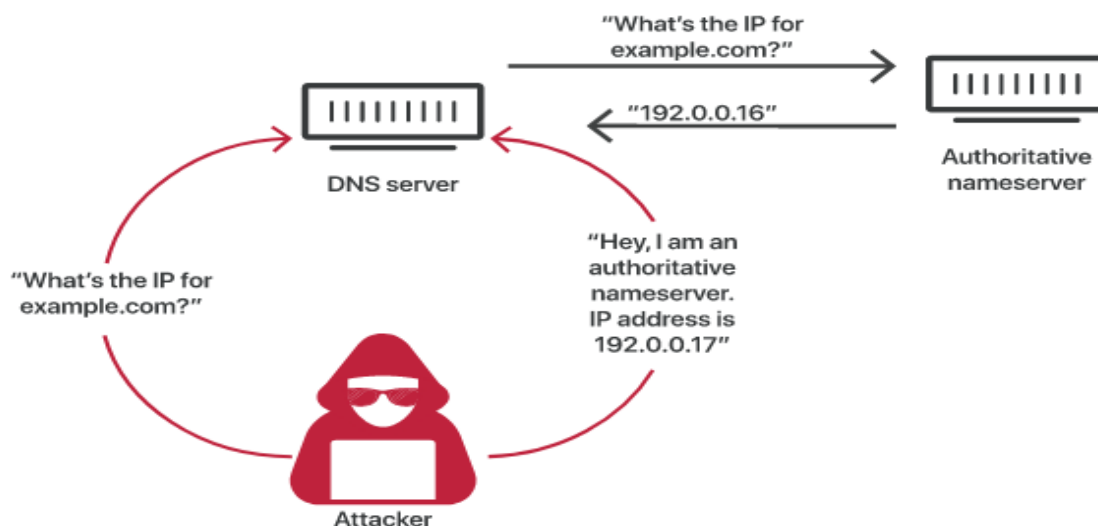


Рис. 4. Атака DNS-сервера в той же локальной сети

Методы профилактики против фарминга[4]:

- Будьте осторожны, если вы иногда используете менеджер паролей; Менеджер паролей запомнит данные для входа и автоматически заполнит для вас имя пользователя и пароль, если сайт является законным. Менеджер паролей не так легко обмануть, и если автозаполнение не происходит, это означает, что веб-сайт был подделан.

- Установите хорошее антивирусное программное обеспечение, которое может блокировать активное вредоносное ПО, пытающееся взломать ваше устройство, и блокировать доступ к подозрительным веб-сайтам, что может привести к отравлению DNS при доступе.

- Используйте хорошего, уважаемого интернет-провайдера, который по умолчанию предотвратит подозрительные перенаправления.

- Используйте известный DNS-сервер. Обычно это сервер интернет-провайдера, однако пользователи могут переключиться на определенный DNS-сервер для дополнительной защиты.

- Убедитесь, что ссылки начинаются с HTTPS, а не только с HTTP.

- Не нажимайте на ссылки или вложения из неизвестных источников электронной почты или SMS.

- Убедитесь, что URL-адрес является законным без каких-либо опечаток, поскольку фармеры иногда используют орфографические приемы, чтобы обмануть посетителей.

- Не нажимайте ничего на подозрительном веб-сайте. Подозрительные веб-сайты могут быть обнаружены по количеству присутствующих грамматических ошибок, странным шрифтам и цветовым кодам, а также отсутствующему содержанию, например, отсутствующим разделам условий и положений.

- Включите двухфакторную аутентификацию, чтобы хакерам было сложнее обойти ваши данные для входа. В этом случае, даже если преступники

получили ваши данные для входа, они не могут получить доступ к вашей учетной записи.

Список используемых источников:

1. pharming [Электронный ресурс]. URL: <https://www.techtarget.com/searchsecurity/definition/pharming> (дата обращения 14.11.2022).
2. DNS Pharming [Электронный ресурс]. URL: <https://www.whatsmydns.net/dns-security/dns-attacks/dns-pharming> (дата обращения 14.11.2022).
3. DNS Pharming Attack Lab [Электронный ресурс]. URL: <https://www.utc.edu/sites/default/files/2021-04/dns.pdf> (дата обращения 14.11.2022).
4. The Dangers Associated With Pharming [Электронный ресурс]. URL: <https://www.securiwiiser.com/blog/the-dangers-associated-with-pharming/> (дата обращения 14.11.2022).

Abdelrahman Barakat

The Bonch-Bruevich St. Petersburg State University of Telecommunications

Studying protective mechanisms of DNS-pharming.

In this article, we cover the use of DNS pharming, as well as the most popular methods of this attack, as well as the main methods for protecting your systems from this attack.

Key words: DNS, Pharming, Websites, IP addresses, HTTP, HTTPS, SMS.

УДК 004.658:65.011.56
ГРНТИ 50.41.21:71.01.85

РАЗРАБОТКА АВТОМАТИЗИРОВАННОГО ПРОЦЕССА ПО КОРРЕЛЯЦИИ ИНФОРМАЦИИ МЕЖДУ ТАБЛИЦЕЙ БАЗЫ ДАННЫХ POSTGRESQL И ACTIVE DIRECTORY

Э. В. Бирих, К. П. Волокушина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В представленном докладе представлен результат разработки автоматизированного решения для регулирования информации между сторонней таблицей и Active Directory. Программа позволяет пользователю коррелировать добавляемые, обновляемые или удаляемые данные, определяя, как именно изменится информация в службу каталогов. Данное решение позволяет сократить количество возникаемых ошибок при переносе данных, сокращает время исполнения поставленной задачи и повышает производительность за счет экономии ресурсов, затрачиваемых человеком на выполнение представленной работы.

Active Directory, Camunda, Python, автоматизация, базы данных, код

Автоматизация рутинных процессов при использовании сетевых технологий является одной из самых приоритетных задач сегодняшнего времени. В особенности, когда задача состоит в корреляции большого количества данных между разными системами, поскольку перенос данных вручную может сопровождаться как ошибками, так и затратой большого количества времени. Целью данной статьи является реализация интеграции информации из сторонней таблицы в Active Directory с использованием языка программирования Python, а также сервиса Camunda для создания саморегулирующихся процессов.

Язык программирования Python и используемые библиотеки.

Высокоуровневый язык программирования Python является одним из самых распространенных в своей категории благодаря не только простоте использования и скорости разработки проектов, но и широкому спектру доступных библиотек. Среди последних, применяемых для работы с базами данных и Active Directory, наиболее активно используются `psycopg2` и `ruad`.

– `psycopg` – адаптер базы данных PostgreSQL для языка программирования Python. В основном реализован на C как обертка `libpq`, что приводит к большей эффективности и безопасности. Многие типы Python поддерживаются стандартными и адаптированы к соответствующим типам данных PostgreSQL; адаптация может быть расширена благодаря гибкой системе оптимизированию объектов [1].

– `ruad` - библиотека Python, предназначенная для обеспечения простого интерфейса с Active Directory через ADSI на платформе Windows [2].

Выбор был сделан в пользу этих библиотек, поскольку первая позволяет работать с базами данных по типу PostgreSQL, вторая имеет самую большую

функционал для работы со службой каталогов. При помощи представленных модулей был реализован основной рабочий принцип конечной программы, а также вспомогательный скрипт, используемый на начальном этапе разработки с целью предварительной корреляции данных. Модуль позволяет собрать данные из таблицы и Active Directory, а затем проверяет наличие или отсутствие тех или иных составляющих. По полученным данным проводится регулирование данных вручную с целью контроля информации во избежание дальнейших возможных ошибок.

Триггерные процедуры PostgreSQL.

PostgreSQL позволяет создавать триггерные процедуры, которые будут вызываться при изменениях данных или событиях в базе данных. Триггерная процедура создаётся командой `create function`, при этом у функции не должно быть аргументов, а типом возвращаемого значения должен быть `trigger` (для триггеров, срабатывающих при изменениях данных). Для триггеров автоматически определяются специальные локальные переменные с именами вида `tg_имя`, описывающие условие, повлёкшее вызов триггера.

Когда функция на PostgreSQL срабатывает как триггер, в блоке верхнего уровня автоматически создаются несколько специальных переменных:

- `new` - тип данных `record`. переменная содержит новую строку базы данных для команд `insert/update` в триггерах уровня строки. в триггерах уровня оператора и для команды `delete` этой переменной значение не присваивается.

- `old` - тип данных `record`. переменная содержит старую строку базы данных для команд `update/delete` в триггерах уровня строки. в триггерах уровня оператора и для команды `insert` этой переменной значение не присваивается.

- `tg_name` - тип данных `name`. переменная содержит имя сработавшего триггера.

- `tg_relname` - тип данных `name`. имя таблицы, для которой сработал триггер. эта переменная устарела и может стать недоступной в будущих релизах. вместо неё нужно использовать `tg_table_name`.

- `tg_table_name` - тип данных `name`. имя таблицы, для которой сработал триггер.

- `tg_nargs` - тип данных `integer`. число аргументов в команде `create trigger`, которые передаются в триггерную процедуру [3].

В программе, тематике которой посвящен данный доклад, обрабатываются триггеры типов `update`, `insert` и `delete` при помощи созданных скриптом, написанном на ранее указанном языке программирования Python, функций (рис. 1).


```

owner = 'OWNER'
table_name = 'SOME_TABLE'

for_insert = ""
CREATE OR REPLACE FUNCTION new_record_notify()
RETURNS trigger AS
$BODY$
BEGIN
PERFORM pg_notify('new_record', row_to_json(NEW)::text);
RETURN NEW;
END;
$BODY$
LANGUAGE plpgsql VOLATILE
COST 100;
ALTER FUNCTION new_record_notify()
OWNER TO {owner};

CREATE TRIGGER add_new_data_event_trigger
AFTER INSERT
ON {table_name}
FOR EACH ROW
EXECUTE PROCEDURE new_record_notify();

"".format(owner=owner, table_name=table_name)
    
```

Рис. 1. Пример триггерной функции и обработка триггера типа insert, реализованные при помощи Python

Проектирование схемы автоматизированного процесса при помощи сервиса Camunda.

Camunda - это платформа для автоматизации и моделирования рабочих процессов. Она представляет собой набор библиотек, которые и позволяют выполнять описанные процессы [4]. Для интеграции Camunda в проект достаточно добавить несколько зависимостей, а также использовать специальный api для используемого языка программирования. В данном случае использовалась библиотека русcamunda – клиент api Python REST для механизма автоматизации рабочего процесса и принятия решений Camunda [5]. С помощью данного метода были реализованы workers – саморегулирующиеся объекты, реагирующие на привязанные к ним функции/события и посылающие сигналы на сервис Camunda, где идет обработка поступившей информации в соответствии с составленной схемой событий (рис. 2).

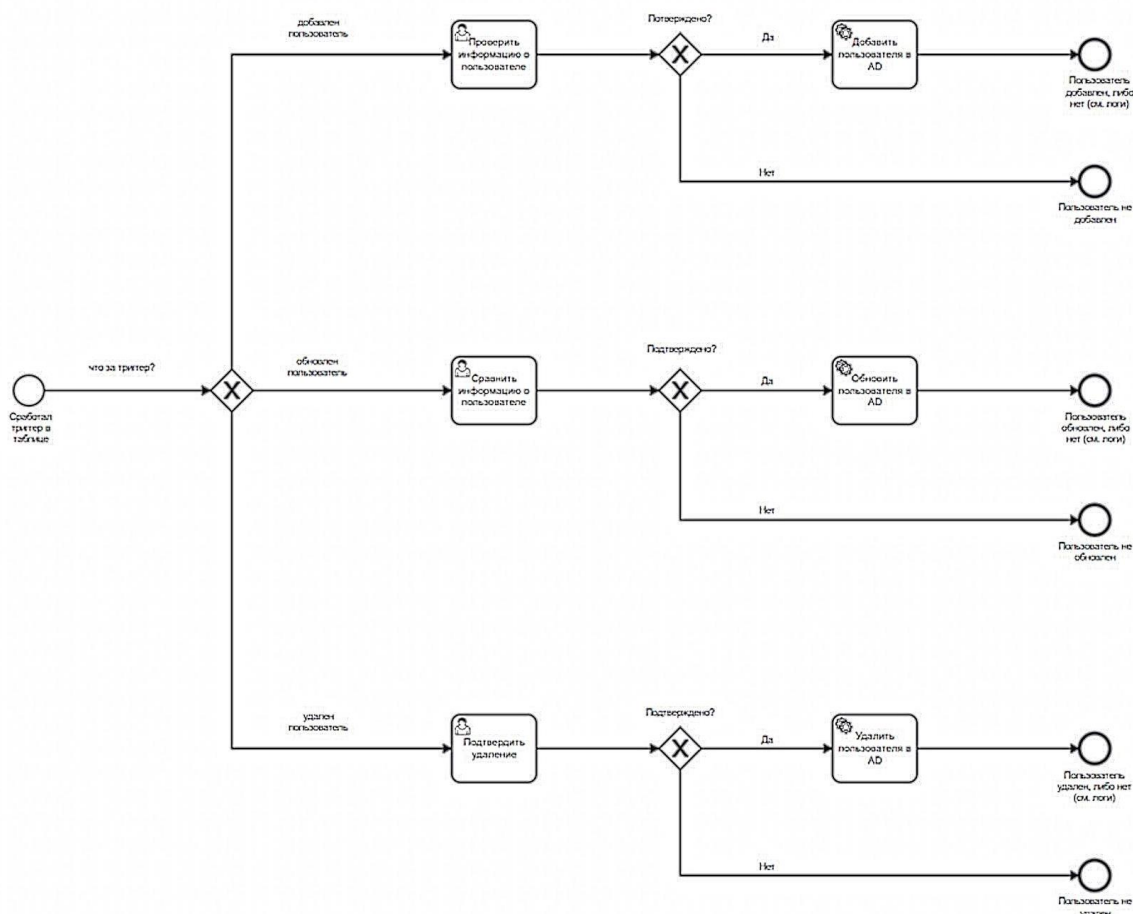


Рис. 2. Схема процессов программы от изменений в таблице базы данных до поступления обработанной информации в Active Directory

Общий функционал программы.

Итоговая программа представляет из себя сервис, состоящий из двух потоков: первый отслеживает и обрабатывает изменения в указанной таблице, и, если действие происходит – отправляет сигнал, на который реагирует второй основной модуль проекта. Последний создает рабочий процесс для Samunda в соответствии с составленной заранее схемой-обработчиком событий. В зависимости от полученного сигнала, появляется то или иное информационное сообщение, содержащее об изменениях таблицы из базы данных, после чего ожидается подтверждение человеком действий или же их отмену. В случае положительной проверки, данные будут либо добавлены в Active Directory, либо изменены в службе каталогов, либо же удалены из нее, в зависимости от контекста изначального сигнала. Конечный этап работы программы – логгирование произведенных действий.

В соответствии с описанными ранее инструментами и модулями, итоговым результатом проделанной работы стал сервис, служащий в качестве вспомогательной утилиты для администрирования взаимодействия таблиц и службы каталогов Active Directory.

Данный проект позволяет сократить количество создаваемых ошибок по сравнению с переносом данных вручную, обеспечивает гибкую систему

отслеживания действий, а также экономит затрачиваемые человеком ресурсы на рутинные задачи, что приводит к большей производительности труда.

Помимо вышеперечисленного, развитие функционала программы в будущем может быть направлено не только на обеспечения контроля процессов, но и на защиту информации, передаваемой из таблицы баз данных [6].

Список используемых источников:

1. Psycorg2. Описание проекта [Электронный ресурс]. URL: <https://pypi.org/project/psycorg2> (дата последнего обращения: 11.11.2022)
2. Pyad. Описание проекта [Электронный ресурс]. URL: <https://pypi.org/project/pyad> (дата последнего обращения: 11.11.2022)
3. Триггерные процедуры. Триггеры при изменении данных [Электронный ресурс]. URL: <https://postgrespro.ru/docs/postgresql/9.6/plpgsql-trigger> (дата последнего обращения: 11.11.2022)
4. Camunda. The Universal Process Orchestrator [Электронный ресурс]. URL: <https://camunda.com/platform> (дата последнего обращения: 11.11.2022)
5. Pysamunda. Описание проекта [Электронный ресурс]. URL: <https://pypi.org/project/pysamunda> (дата последнего обращения: 11.11.2022)
6. Бирих Э.В., Виткова Л.А., Гореленко В.В., Казаков Д.Б. Защита информации в базах данных [Электронный ресурс] // Актуальные проблемы инфотелекоммуникаций в науке и образовании: материалы конференции АПИНО 2017, 01–02 марта 2017 г. СПб: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2017. С. 89–92. URL: <https://www.sut.ru/doci/nauka/bapino/apino2017-2.pdf> (дата последнего обращения: 14.11.2022)

Birikh E., Volokushina K.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

Development of automated process for correlation of information between PostgreSQL database table and Active Directory.

The presented report presents the result of the development of an automated solution for correlating information between a third-party table and Active Directory. The program allows the user to adjust the data to be added, updated or deleted, determining exactly how the information changes to the directory service. This solution allows you to reduce the number of errors encountered during data transfer, reduce the execution time of the task and increase performance by saving the resources spent by a person on the work presented.

Key words: Active Directory, Camunda, Python, automation, databases, code.

УДК 004.056
ГРНТИ 81.93.29

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ДЕЦЕНТРАЛИЗОВАННОЙ БЛОКЧЕЙН ПЛАТФОРМЫ TON

М. Э. Богомаз, А. А. Нечаев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Значительный прогресс в области построения децентрализованных платформ, основанных на технологии блокчейн, приводит к необходимости повышенного внимания исследователей к анализу возможностей соответствующих систем и их стойкости. Существующие решения используются в качестве инструмента для проведения быстрых и безопасных транзакций между пользователями из любых точек мира, а также для создания децентрализованных приложений. В работе проводится анализ Telegram Open Network – проект, предлагающий новые возможности как в производительности и масштабируемости, так и в скорости выполнения транзакций и смарт контрактов. Кроме того, предоставляется возможность создания сайтов на базе блокчейна.

TON, блокчейн, децентрализованная сеть, криптовалюта, Gram, смарт-контракты

Блокчейн – это особая технология хранения данных, основанная на выстроенной непрерывной последовательности блоков. История блокчейна начинается в 2008 году, когда некий разработчик (или группа разработчиков) под псевдонимом Сатоши Накамото предложил реализацию системы блокчейн в качестве реестра для первой криптовалюты – биткоин [1]. Первая версия криптовалюты была представлена в 2009 году с реализацией децентрализованного блокчейна, который обеспечивает хранение всех транзакций в системе.

На сегодняшний день применение технологии блокчейн не ограничивается криптовалютами. Так, в 2015 году канадско-российский программист Виталик Бутерин представил Ethereum – одноименную криптовалюту и платформу для создания децентрализованных приложений, работающих на базе умных контрактов. Помимо финансовой сферы, технологию блокчейн используют для установления авторства и права владения, проверки подлинности, в средствах электронного голосования, видеоиграх и в других отраслях.

Однако, несмотря на применяемость технологии блокчейн, за 13 лет она так и не смогла решить свою ключевую задачу — стать удобным и доступным инструментом для рядового пользователя. Технологией интересуются малое количество предприятий, несмотря на огромную возможность применения, а товары и услуги по-прежнему легче покупать за привычную валюту, а не за цифровую. В данной статье рассматривается сеть TON – Telegram Open Network, которая создавалась с целью решить проблему доступности и принятия технологии блокчейн и криптовалюты, в частности.

Что такое TON и как он работает?

TON (Telegram Open Network) – децентрализованная оверлейная P2P сеть. Защиту и анонимность в данной сети обеспечивают встроенные прокси и анонимайзеры. На этой платформе сосредоточены сервисы обмена сообщениями, платежные операции в криптовалюте Gram, сервис для хранения

различных данных и система для создания децентрализованных приложений на основе умных контрактов. Изначально концепция TON разрабатывалась Telegram, после проект разрабатывался сообществом.

С момента создания идеи TON собралось множество противоречивых мнений. С одной стороны, блокчейн позволит пользоваться свободным Интернетом даже в странах с повышенной Интернет-цензурой, ведь ни один государственный регулятор не сможет ограничить пользователя от попадания в сеть. С другой стороны, подобная свобода действий открывает простор для распространения нелегальных материалов.

Главной задачей было создать протокол с быстрыми, недорогими и масштабируемыми транзакциями, как финансовыми, так и нет. Поскольку у Telegram есть огромная аудитория, насчитывающая более 700 миллионов пользователей, немаловажным аспектом было создание доступного интерфейса и прозрачной работы блокчейна для рядового пользователя. С таким ресурсом TON мог бы стать самой популярной криптовалютой в мире.

Другая задача TON – объединить другие блокчейны. Отличительная особенность TON заключается в том, что он спроектирован как блокчейн из блокчейнов, то есть любой блок из блокчейна TON в будущем может стать самостоятельным блокчейном [2]. Нужно это для того, чтобы масштабироваться в зависимости от нагрузки пользователями сети, а также иметь связь с другими блокчейнами. Для этого существуют специальные мосты, которые с помощью смарт-контракта блокируют криптовалюту в одной сети и создают такое же количество криптовалюты в другом кошельке. Уникальным фактором блокчейна TON является его самовосстанавливающийся механизм вертикальной цепочки блоков и мгновенная маршрутизация гиперкубов, которые делают его быстрым, надежным, масштабируемым и самосогласованным одновременно.

Структура TON.

Как и любая другая экосистема, TON собирает в себя несколько инструментов для обеспечения безопасности, возможности проведения платежей, хранения данных, возможности создания распределенных по сети приложений, а также анонимности.

Рассмотрим более подробно структуру TON:

– TON Blockchain – ядро платежной системы с криптовалютой Gram, поддерживающее несколько миллионов платежей в секунду.

– TON P2P Network – сеть класса peer to peer для общения клиентов сети TON.

– TON Storage – распределенное хранилище данных для сервисов и пользователей. Идея заключается в хранении данных не на серверах, а на клиентских устройствах, которые обмениваются данными. Таким образом, TON избегает возможное действие регулятора, ведь в сети нет сервера, который можно заблокировать, вся информация распределена между пользователями, а его каналы защищены криптографическими протоколами.

– TON Proxy – сервис, отвечающий за анонимность, по архитектуре подобный Tor. При таком подходе, любые блокировки по IP становятся бессмысленными, ведь клиенты общаются непосредственно друг с другом, без участия сервера. В логах провайдеров не будет отображаться целевой узел, ведь

он скрыт цепочкой из нескольких проху посредников через криптографический тоннель.

– TON DHT – хэш-таблица для хранения произвольных значений. Создана для того, чтобы помогать TON Storage в нахождении раздающих узлов сети, а TON Proху для поиска посредников в передаче информации [3].

– TON Services – площадка для создания децентрализованных приложений, поддерживающая создание двух типов приложений: TON Sites и Fog Services. TON Sites – аналог сайтов Интернета с поддержкой ввода вывода данных и гиперссылок. Главное отличие от обычного сайта, как и главная идея самого блокчейна – невозможность блокировки внешнего государственного цензора, поскольку приложение распределено между клиентами сети. Fog Services – сервисные TON Services, необходимые для поддержания технологии. Они также не могут быть заблокированы цензором, ведь не находятся на серверах.

– TON DNS – децентрализованная система имен, использующая привычные доменные имена, подобные Интернету, однако отождествлять, например, домены .com и .top нельзя.

– TON Payments сервис для возможности проведения платежей в криптовалюте Gram.

– TON Virtual Machine – виртуальная машина TON, выполняющая смарт-контракты. Помимо платежей, с помощью смарт контрактов пользователи могут оформлять договоры по любым сделкам внутри сети TON. Ключевое преимущество перед электронной цифровой подписью является то, что само содержание договора становится форматизированным на основе автоматически обрабатываемых алгоритмов. Для написания смарт контрактов TON предлагает язык программирования FunC, а за обработку контрактов отвечает низкоуровневой fift.

– TON Messages – протокол обмена сообщениями как между узлами сети, так и между сервисами.

– TON Hypercube Routing – система, позволяющая доставлять и обрабатывать сообщение, созданное в блоке одного шардчейна, в следующий блок целевой шардчейны [4], в независимости от общего количества шардчейн в системе

– TON Validators – участники сети, проверяющие блоки и способствующие безопасности сети.

Сравнение TON с Ethereum и Solana.

Архитектура, описанная выше, позволяет блокчейн-экосистеме TON оставаться конкурентоспособной. Однако существуют и другие проекты, с похожими механизмами, но разными предназначениями. В таблице 1 проведен сравнительный анализ TON с Ethereum [5] – первой платформой, использовавшей технологию блокчейн не только для криптовалюты, и показавшей технологию смарт-контрактов, и с Solana – еще одной общедоступной блокчейн-платформой с возможностью стабильного масштабирования.

ТАБЛИЦА 1. Сравнение блокчейн-систем TON, Ethereum и Solana

Параметр	TON	Ethereum 2.0	Solana
Время создания блока	5 секунд	12 секунд	1 секунда
Время завершения блока	6 секунд	10-15 минут	6,4 секунды
Скорость выполнения простых транзакций	Высокая	Высокая	Высокая
Скорость выполнения сложных транзакций	Высокая	Низкая	Очень низкая
Шардинг	До 2^{60} шардов	До 2^6 шардов	Отсутствует
Взаимодействие шардчейнами	Практически мгновенное	Медленное	Отсутствует

На основе данных из таблицы, можно сравнить системы по ряду ключевых качеств:

– Скорость. Ethereum значительно проигрывает в скорости. Несмотря на то, что Solana создает блок за 1 секунду, на завершение блока тратится 5,4 секунды, что немного больше, чем в блокчейне TON.

– Производительность. Стоит отметить, что все 3 блокчейна полны по Тьюрингу, что позволяет реализовать вычислимую функцию любой сложности. Однако Ethereum полный только в сети Beacon Chain, это означает что дополнительные транзакции могут проходить вне децентрализованной сети, из-за отсутствия взаимодействия с другими сегментами. Solana хорошо работает с большим количеством простых операций, при условии, что вся информация хранится в оперативной памяти, иначе у блокчейна возникают проблемы отказа в обслуживании из-за перегрузки. Таким образом, Solana не подходит для больших серьезных проектов, в отличие от TON.

– Масштабируемость. TON поддерживает до 2^{32} рабочих цепей, каждая из которых поддерживает до 2^{60} шардчейн с мгновенной связью [6], что позволяет TON десятки миллионов транзакций в секунду. У Solana нет поддержки шардинга, а вот у Ethereum'а есть, но всего до 64 шардчейн, с условием что время до завершения блока около 10-15 минут.

В настоящей работе был описан принцип работы блокчейн платформы TON, ее архитектура и возможности. Также был проведен сравнительный анализ с блокчейн системами Ethereum и Solana, который показал, что по ключевым параметрам блокчейн TON является предпочтительнее, как для разработчика, так и для рядового пользователя.

Таким образом, несмотря на многообразие различных платформ, использующих технологию блокчейн, TON обладает множеством преимуществ. На данный момент реализованы практически все модули, описанные в архитектуре TON, за исключением TON Storage. Также у блокчейна есть свой кошелек и мост в Ethereum и Bitcoin, и обратно. На сегодняшний день, TON работает и доступен любому, кто хочет использовать преимущества технологии блокчейн.

Список используемых источников:

1. Башир И. Блокчейн: архитектура, криптовалюты, инструменты разработки, смарт-контракты. Москва: ДМК Пресс, 2019. 538 с.

2. Николай Дуров. The Open Network [Электронный ресурс]. URL: <https://ton-blockchain.github.io/docs/ton.pdf> (дата обращения 02.11.2022).

3. Новицкий И.О., Шилин Л.Ю. Ton: Telegram Open Network // Информационные технологии и системы 2019 (ИТС 2019) = Information Technologies and Systems 2019 (ITS 2019): материалы международной научной конференции, Минск, 30 октября 2019 г. БГУИР, Минск, 2019. С. 250 – 251.

4. Николай Дуров. Telegram Open Network Blockchain [Электронный ресурс]. URL: <https://ton-blockchain.github.io/docs/tblkch.pdf> (дата обращения 02.11.2022).

5. Сравнение TON и Ethereum 2.0 [Электронный ресурс]. URL: <https://tonblockchain.ru/comparison-ethereum/> (дата обращения 06.11.2022).

6. Хабр: Telegram Open Network: теория и практика от валидатора сети [Электронный ресурс]. URL: <https://habr.com/ru/company/mercuryo/blog/479354/> (дата обращения 04.11.2022).

Bogomaz M., Nechaev A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Comparative analysis of the decentralized blockchain platform TON.

Significant progress in the field of building decentralized platforms based on delivery technologies leads to the need for increased attention to the analysis of the possibility of using systems and their durability. Essential solutions are used as a tool for making fast and secure transactions between users from anywhere in the world, as well as for creating decentralized applications. The paper analyzes the Telegram Open Network, a project that offers new opportunities both in performance and scalability, as well as in the speed of transactions and smart contracts. In addition, it is possible to create sites based on traffic.

Key words: TON, blockchain, decentralized network, cryptocurrency, Gram, smart contract.

УДК 343.9
ГРНТИ 10.85

ИССЛЕДОВАНИЕ ОБНОВЛЁННЫХ ПРИНЦИПОВ СБОРА ЦИФРОВЫХ УЛИК

В. И. Борисов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На протяжении более десяти лет принципы сбора цифровых улик оставались неизменными, и помогали работе экспертов в цифровой криминалистике по всему миру. Однако темпы развития цифровых устройств и непосредственно области цифровой криминалистики привели к пересмотру и обновлению принципов сбора цифровых улик. В данной работе предлагается рассмотреть и обсудить обновленный набор принципов.

цифровая криминалистика, форензика, сбор цифровых улик, фундаментальные принципы

Несмотря на то, что на протяжении уже более десяти лет, принципы сбора цифровых улик остаются неизменными, их влияние на область цифровой криминалистики сложно недооценить: эти принципы интегрированы в руководства по сбору улик международных и национальных организаций, связанных с расследованиями преступлений, в которых участвуют цифровые улики; одним из главных требований большинства вакансий в области цифровой криминалистики является умение объяснить применимость этих принципов на практике в процессе расследования; кроме того все практические указания по сбору улик формируются на основе этих самых принципов, так как их соблюдение в последующем при даче экспертных показаний в суде является показателем качества, проведённой экспертизы.

Данные принципы были разработаны Ассоциацией Шефов Полиции (АСРО), некоммерческой организацией действующей на территории Соединённого Королевства Великобритании, поэтому далее по тексту исходные принципы по сбору цифровых улик будут именоваться принципами АСРО (реже – существующими принципами), а принципы предложенные им на смену – обновлёнными принципами.

Хорсман в своей работе [1], выдвигает несколько причин, по которым следует произвести пересмотр и дополнение принципов сбора цифровых улик. Основная мысль, которую можно обобщить из существующих четырёх принципов сбора цифровых улик следующая: "необходимо сохранить цифровые данные в их изначальной форме и если всё-таки придётся их изменить, то убедитесь, что вы понимаете, что вы делаете; Все произошедшие изменения должны быть задокументированы; Человек, который несёт ответственность за ход расследования, также отвечает и за соблюдение действующего законодательства совместно с вышеизложенными принципами".

Такая формулировка, по мнению автора, определённо не может выступать гарантией качества проведённой экспертизы, так как не накладывает никаких обязательств на практикующего эксперта по подтверждению точности проведённой экспертизы; как и не накладывают обязательств на качество и надёжность выбранных методов. Другими словами, принципы АСРО не формулируют критериев для обоснования выбора тех или иных методов, и более того, существующие принципы даже не требуют обосновывать этот выбор.

Помимо этого, с точки зрения автора, существующие принципы, не отвечают возникающим глобальным изменениям, с которыми приходится считаться экспертам, при проведении исследований, таким как растущая тенденция на обеспечение конфиденциальности, при проведении цифровой криминалистической экспертизы, а также необходимость снизить время прерывания тех или иных процессов, которые неизбежно возникают в ходе следственных мероприятий.

Также поводом для беспокойства можно считать и то, что за последние уже более десяти лет, принципы оставались неизменными, игнорируя происходящие изменения в области цифровой криминалистики и технологиях, что может являться индикатором стагнации.

В связи со всеми вышеперечисленными причинами, автор работы [1] считает необходимым начать различные процессы связанные с обсуждением, пересмотром и обновлением текущих принципов сбора цифровых улик, и в качестве первого шага предлагает восемь новых принципов, которые были обновлены в соответствии с текущим уровнем развития области цифровой криминалистики.

ТАБЛИЦА 1. Соответствие исходных принципов обновлённым

Номер исходного принципа	Номер обновлённого принципа	Действие	Комментарий
№4	№1	Переопределен	Оригинальный принцип возлагал всю ответственность на вышестоящую правоохранительных орган ответственных за ход расследования; Обновленный принцип разделяет ответственность между экспертом и правоохранительным органом на основании областей экспертизы.
–	№2	Введён впервые	Данный принцип требует от стороны проводящей расследование, действовать исключительно в рамках правового поля, что способствует взаимодействию между экспертом и правоохранительным органом.
–	№3	Введён впервые	Данный принцип требует эксперта учитывать вопросы конфиденциальности и адекватности сроков изъятия при соблюдении полноты сбора улик.
–	№4	Введён впервые	Данный принцип, формулирует критерии по выбору метода сбора цифровых улик, а

			также требует от него использования методов отвечающих этим критериям явным образом.
№1	№5	Уточнён	Оригинальный принцип требовал неукоснительного соблюдения целостности данных, обновленный принцип утверждает, что эксперт должен предпринять все разумные шаги по сохранению целостности данных, принимая во внимание ряд инвазивных техник используемых для извлечения улик, и технологий, применительно которым целостность без изменений не может быть обеспечена.
№2	№6	Уточнён	Данный принцип предотвращает «слепое» использование процедур, работу которых эксперт не понимает. Помимо этого, данный принцип в новой формулировке также устанавливает приоритет применения инвазивных методов.
–	№7	Введён впервые	Данный принцип покрывает область, ранее не рассмотренную в контексте принципов АСРО, а именно необходимость подвергать проверке результаты проведённой экспертизы
№3	№8	Уточнён	Данный принцип в новой формулировке требует вести журнал аудита, в котором будут задокументированы все процедуры, которые были проведены в ходе расследования, для возможности получения сравнимых результатов третьей стороной в ходе изучения этого журнала. Здесь важно отметить использование слова «сравнимые», что указывает на то, что некоторые процессы не могут быть повторно воспроизведены, а также некоторые процессы могут быть воспроизведены, но их результаты не окажутся идентичными.

Преимуществом обновлённых принципов является то, что они покрывают области, ранее не затронутые принципами АСРО. Однако у обновлённых принципов есть ряд аспектов, к которым возникают вопросы.

Обновлённые принципы сформулированы достаточно абстрактно, что с одной стороны позволяет адаптировать и применять их в абсолютном большинстве ситуаций, возникающих в ходе расследования, но с другой стороны оставляет пространство для разночтений, которые в последствие необходимо будет устранять в руководствах более низкого уровня.

Примером такого принципа является обновленный принцип №3, который направлен на снижение числа задержек и прерываний, связанных с изъятием

временем изъятия носителей цифровых улик, объёмом изымаемых носителей и вторжением в процессы, в ходе расследования. Формулируется он следующим образом: «Эксперт должен приложить все обоснованные усилия, чтобы найти все возможные источники потенциальных улик, относящиеся к расследованию с учётом необходимости и адекватности по отношению к любым устройствам и данным, которые изымаются/собираются. Должны быть приняты все обоснованные меры по ограничению побочных вторжений в процессы в ходе расследования».

Как можно заметить, данный принцип, хотя и говорит о необходимости прилагать все усилия по минимизации неудобств, связанных с расследованием, при этом не стремится установить конкретные сроки, для различных категорий изымаемых устройств и прерываемых процессов. А также не требует уточнения данных сроков в целом. Это в свою очередь оставляет возможность сохранять сроки изъятия/вторжения неопределёнными, по усмотрению практикующего эксперта или правоохранительного органа, что может приводить к задержкам или изъятию носителей в нерациональных объёмах, что в конечном итоге приведёт к противоречию данного принципа самому себе, а также нарушит обновленный принцип №2, который обязует сторону проведения расследования соблюдать вышеописанные принципы.

Аналогичным образом обновленный принцип №6, оставляет пространство для различных трактовок и не требует уточнять их в нижестоящих руководствах по изъятию цифровых улик. А именно, согласно [1] «требование быть компетентным должно предотвращать от "слепой" реализации процедур, принцип работы которых эксперту не ясен». Не ясно в таком случае, как должен поступать эксперт в случае применения автоматизированных инструментов, как с открытым, так и закрытым исходным кодом. Не уточняется: должен ли он понимать только принцип реализуемой в ходе расследования процедуры или ему следует досконально изучить конкретную реализацию процедуры в составе автоматизированного инструмента.

В случае инструментов с закрытым исходным кодом понимание их работы, затруднено и возможно только с помощью применения различных техник обратного инжиниринга, это в свою очередь может нарушать действующее законодательство в области авторского права, и более такого такой анализ вряд ли возможен в адекватное время в контексте проводимого расследования и в частности обновлённого принципа №3, описанного выше.

Таким образом, можно сказать, что предложенный набор обновлённых принципов несомненно делает шаг вперёд относительно принципов АСРО, а также способствует такому важному явлению, как начало дискуссии относительно фундаментальных принципов по изъятию цифровых улик, что по мнению автора, в будущем, приведёт к пересмотру принципов АСРО применяемых практически повсеместно. Однако есть все основания утверждать, что и обновлённые принципы должны стать предметом пристального изучения в сообществе практикующих экспертов в области цифровой криминалистики и смежных с ней областях.

Список используемых источников:

1. Graem Horsman. ACPO principles for digital evidence: Time for an update? // Forensics Science International: Reports. 2020. N 100076. С. 1-6.

Borisov V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Review of updated ACPO's Principles.

Remaining unchanged for over 10 years and supports operation of digital forensics' experts all over the world. But high rate of changes in technology landscape and digital forensics field leads to start of reviewing and updating existing principles. In current paper I offer to consider and discuss updated principles.

Key words: digital criminalistics, forensics, digital evidence collection, fundamental principles.

УДК 004.421.5
ГРНТИ 28.29.51

ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНЫХ БУЛЕВЫХ ФУНКЦИЙ В КЛАССЕ МАЛОЙ РАЗМЕРНОСТИ

А. А. Воронцов, С. Н. Шемякин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича.

В статье рассматривается вопрос поиска булевых функций от малого числа переменных с некоторыми необходимыми свойствами и определяется набор этих свойств. Такие булевы функции используются, например, для построения различных датчиков псевдослучайных двоичных последовательностей.

Булевы функции, алгебра логики, нелинейность, уравновешенность, шифры гаммирования, преобразование Уолша-Адамара, нелинейные узлы усложнения

Булевы функции являются одним из важнейших понятий алгебры логики. Теория булевых функций была введена английским математиком Дж. Булем в XIX веке. Они применяются для построения различных криптографических примитивов [1].

Булевой функцией (БФ) от n переменных называется отображение $f: Z_2^n \rightarrow Z_2$. Булева функция от n переменных именуется n -местной булевой функцией. Для n -местной булевой функции используется обозначение $f(x) = (x_1, x_2, \dots, x_n)$ [3]. Z_2 представляет конечное поле из двух элементов: 0 и 1.

Булевы функции могут быть заданы различными способами, например, с помощью таблицы истинности или полинома Жегалкина. Таблица истинности БФ представляет собой последовательность значений этой функции, которая состоит из элементов 0 и 1 и имеет вид: $f(b_0) f(b_1) \dots f(b_{2^n-1})$ где b_i поочередно принимает все значения из $GF(2)^n$ [2]. Строки таблицы истинности соответствуют набору элементов поля, а в столбцах находятся значения этих элементов и значения функции. Строка истинности – строка, состоящая из поочередно записанных значений функции при каждом значении ее аргументов, записанная в лексикографическом порядке.

Полином Жегалкина имеет вид:

$$f(x_1, x_2, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus \dots \oplus a_{123} x_1 x_2 x_3 \oplus \dots \oplus a_{123\dots n} x_1 x_2 x_3 \dots x_n,$$

где $a_0, a_1, a_2, \dots, a_n, a_{12}, a_{123\dots n}$ – коэффициенты полинома Жегалкина, являющиеся константами 0 или 1. Операция произведения здесь эквивалентна операции AND(&), а операция суммирования – операции сложения по модулю 2, XOR(\oplus) в поле $GF(2)$ [1].

Также существует эквивалентное полиному Жегалкина представление БФ, которое называют алгебраической нормальной формой (АНФ):

$$f(x_1 \dots x_n) = a_0 \oplus \sum_{1 \leq i_1 < \dots < i_k \leq n} a_{i_1 \dots i_k} \prod_{j=1}^k x_{i_j}$$

Вес булевой функции $f(x) = (x_1, x_2, \dots, x_n)$ – это количество единичных компонент x_i :

$$wt(f) = \sum_{x \in Z_2^n} f(x) = |\{x \in Z_2^n : f(x) = 1\}|$$

Алгебраическая степень функции f ($\deg(f)$) – количество переменных в слагаемом полинома Жегалкина функции f наибольшей длины [1].

БФ называется уравновешенной, или сбалансированной, если $wt(f) = 2^{n-1}$. Т.е. булева функция является уравновешенной, если она принимает значения 0 и 1 с равной вероятностью при равновероятностных значениях аргументов [2].

Первый показатель качества криптографической БФ – алгебраическая степень АНФ. БФ, значения алгебраической степени которых ≤ 1 , носят название аффинных. Если аффинная функция представляется суммой некоторых переменных, то она называется линейной БФ. Функции, имеющие слагаемые с алгебраической степенью > 1 – нелинейные БФ [3].

Второй показатель качества – нелинейность булевой функции $N(f)$ — это расстояние Хэмминга от строки истинности функции f до множества всех аффинных функций [3]:

$$N_f = d(f, A(n)) = d(f, g)$$

Значение показателя нелинейности БФ может быть определено при рассмотрении представления Уолша-Адамара (ПУА) функции. Данное преобразование имеет вид [3]:

$$\hat{f}(a) = \sum_{x \in Z_2^n} (-1)^{f(x) \oplus (a,x)}$$

Значения $\hat{f}(a)$ называются коэффициентами ПУА. Коэффициент ПУА $\hat{f}(a)$ является разностью между расстоянием Хэмминга от функции $f(x)$ до аффинных и линейных функций [3]:

$$\hat{f}(a) = \sigma_i - \delta_i,$$

где σ_i – расстояние Хэмминга от функции f до i -й аффинной функции ($d(f, g_i)$);

δ_i – расстояние Хэмминга от функции f до i -й линейной функции ($d(f, h_i)$).

Третий показатель качества БФ – существенность всех переменных. Переменная x_i является существенной переменной булевой функции $f(x)$ если выполняется следующее условие [1]:

$$f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n) \neq f(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n)$$

В ином случае переменная x_i именуется фиктивной переменной булевой функции $f(x)$.

Четвёртый показатель качества – корреляционная иммунность. Это свойство показывает, что выходное значение булевой функции не зависит от любой входной комбинации из m элементов своих аргументов. Функция $f \in P_2(n)$ называется корреляционно-иммунной $cor(f)$ порядка m , $0 < m \leq n$, если для любой её подфункции f' от $n - m$ переменных выполняется равенство $w(f') = w(f)/2^m$ [3].

Подфункция БФ f' от переменных x_1, \dots, x_n — это булева функция, полученная из функции f , в которой вместо переменных x_{i1}, \dots, x_{ik} подставляются конкретные константы a_1, \dots, a_k , принимающие значения 0 или 1. Чтобы оценить корреляционную иммунность заданной функции, необходимо знать связь между алгебраической степенью БФ от n переменных и ее корреляционной иммунностью. Для проведения этой оценки вводится неравенство Зигенталера, формулируемое следующим образом [3]:

1. Для любой БФ f справедливо неравенство:

$$\deg(f) + cor(f) \leq n$$

2. Если f – уравновешена и $cor(f) \leq n - 2$, то:

$$\deg(f) + cor(f) \leq n - 1$$

Пятый показатель качества – выполнение строгого лавинного критерия (СЛК) [3]. Булева функция f удовлетворяет строгому лавинному критерию, если значение автокорреляционной функции $\Delta f(a) = 0$ для всех a , таких, что $w(a) = 1$.

Функцией автокорреляции $\Delta f(a)$ для $f \in P_2(n)$ называется функция, определяемая как:

$$\Delta f(a) = \sum_{x \in Z_2^n} (-1)^{f(x) \oplus f(x \oplus a)}$$

Необходимо, чтобы значения АКФ равнялись 0 для входных наборов значений, вес которых равен 1 [3].

Перебор всех возможных БФ от одной или двух переменных показал, что они не могут быть использованы в качестве криптографических функций. Поиск среди БФ от трех переменных в работе [5] дал 32 БФ. Однако у них отсутствует корреляционная иммунность. Следовательно, для поиска криптографических функций необходимо проводить проверку среди функций, зависящих не менее чем от 4-х переменных.

Таким образом, формулируется следующий список требований к криптографическим БФ:

1. Уравновешенность (сбалансированность, равновероятность).
2. Нелинейность полинома Жегалкина.
3. Корреляционная иммунность.
4. Отсутствие фиктивных переменных.
5. Выполнение СЛК.

Общее количество булевых функций от четырех переменных составляет 65536. Из этого числа должны быть исключены линейные, аффинные и неуравновешенные функции. Для дальнейшего рассмотрения остаются уравновешенные нелинейные функции из класса $P_2(4)$, количество которых составляет 693 [4].

В работе [4] производится полный перебор оставшихся 693 БФ и отфильтровываются функции, несоответствующие указанным критериям. В итоге остается 13 булевых функций, удовлетворяющих всем необходимыми требованиям, которые могут быть использованы для различных практических задач, например для построения нелинейных узлов усложнения. Пример криптографической БФ от четырех переменных: $f^{1_2}(x) = 1000101111010001$.

В статье был рассмотрен вопрос существования оптимальных булевых функций в классе малой размерности. Перечисленный в статье набор требований к криптографическим булевым функциям не является исчерпывающим. Поиск БФ, для которых выполняются дополнительные критерии, например, отсутствие линейных и псевдолинейных переменных, тривиальность группы инерции или алгебраическая иммунность, может служить темой для дополнительных исследований.

Список используемых источников:

1. Логачёв, О. А. Булевы функции в теории кодирования и криптологии : [Текст] : учебное пособие / О. А. Логачёв, А. А. Сальников, В.В. Яценко. – Москва: МЦНМО, 2004. – 470 с. – 500 экз. – ISBN: 5-94057-117-4. - Текст : электронный.
2. Коржик, В. И. Основы криптографии : [Текст] : учебное пособие / В. И. Коржик, В. П. Просихин, В. А. Яковлев ; рец.: Р. Р. Биккенин, Б. В. Изотов. — СПб. : СПбГУТ, 2014. - 277 с. : ил. - ISBN 978-5-89160-097-3 : Б. ц. - Текст : электронный.
3. Панкратова И.А. Булевы функции в криптографии: учеб. пособие. СПб.: Издательство "Лань", 2019. 92 с.
4. Скоробогатова Е.А. Использование лавинного критерия при выборе нелинейного узла усложнения в шифраторах гаммирования: выпускная квалификационная работа / Е.А. Скоробогатова. — СПб. : СПбГУТ, 2022. - 103 с. : ил. - Текст : электронный.
5. Ахметшина М.Э. Определение криптографических свойств булевых функций у блочного шифратора [Текст] : выпускная квалификационная работа / М.Э. Ахметшина. — СПб. : СПбГУТ, 2020. - 93 с. : ил. - Текст : электронный.

Vorontsov.A., Shemyakin S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Determination of optimal boolean functions in a class of small dimension.

The question of searching for Boolean functions of a small number of variables with some necessary properties is considered. Such functions are used in various sensors of pseudo-random binary sequences.

Key words: Boolean functions, logical algebra, non-linearity, poise, gamma ciphers, Walsh-Hadamard transform, non-linear complexity nodes.

УДК 004.056.53
ГРНТИ 49.33.35

АРХИТЕКТУРА УСТРОЙСТВА АВТОМАТИЗИРОВАННОГО АУДИТА БЕЗОПАСНОСТИ СЕТЕЙ СЕМЕЙСТВА IEEE 802.11

Г. Е. Ворошнин, Е. А. Забзеев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Сегодня беспроводные Wi-Fi сети используются практически повсеместно: их можно встретить как в жилых помещениях, магазинах, кафе, метро, так и в офисах большинства организаций. Современному человеку трудно представить жизнь без беспроводного доступа в Интернет. Обычный пользователь редко задумывается о безопасности используемого способа доступа к мировой паутине. Насколько надежно защищены данные, которые он передает и получает? Ежегодно происходит множество случаев нарушения информационной безопасности сетей семейства IEEE 802.11. Одной из основных уязвимостей беспроводных сетей является общедоступная среда передачи данных, позволяющая перехватывать и передавать любые данные злоумышленникам. Учитывая постоянное совершенствование методов атак, можно утверждать о необходимости регулярного контроля средств обеспечения информационной безопасности. Даже самые современные средства обеспечения безопасности беспроводных сетей не могут защитить ее от элементарных атак, ухудшающих или нарушающих работу сетевого и клиентского оборудования. Принимая во внимание данный фактор, существует необходимость в разработке устройства, осуществляющего регулярные проверки средств обеспечения информационной безопасности. Такой прибор позволит проверять устойчивость беспроводной сети к атакам, готовность специалистов по информационной безопасности к нештатным ситуациям, а также выявлять уязвимости сети.

информационная безопасность, безопасность беспроводных сетей, IEEE 802.11, penetration testing, устройство тестирования беспроводных сетей

Популярная и очень распространенная технология Wi-Fi стала повседневным элементом в жизни почти каждого современного пользователя сети Интернет. Общедоступная среда передачи данных, используемая в данной технологии, подвергает опасности как личную информацию пользователей, так и секретные данные организаций. Этот недостаток позволяет как перехватывать все данные, передаваемые в сети, так и выводить в беспроводную среду любую информацию или шум [1].

Несмотря на угрозы безопасности, трудно отказаться от использования беспроводных сетей семейства IEEE 802.11, так как они являются очень удобными и распространенными. Для обеспечения необходимого уровня защиты передаваемой информации используется множество средств: шифрование трафика, межсетевые экраны, системы wIPS [2], wIDS и многое другое. Для проведения аудита защищенности сети в настоящее время часто приходится обращаться к профильным организациям. Такие организации, в свою очередь, используют различные утилиты для проведения тестирования и мониторинга сети.

Исходя из данной ситуации, можно прийти к выводу, что необходимо создание устройства, которое могло бы многосторонне и качественно провести анализ устойчивости сети к различным видам атак. Также такое решение будет целесообразно с точки зрения закона, а именно в соответствии с приказами ФСТЭК №17 и №21 [3-4]. В данных документах говорится, что необходимо:

– обеспечивать меры по обнаружению (предотвращению) вторжений, которые должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия;

– осуществлять регулярный контроль эффективности применения систем защиты при эксплуатации средств защиты информации, в том числе и IPS модулей [5], на объектах информатизации.

На первом этапе проектирования такого устройства необходимо создать требования [6], которым оно должно соответствовать:

1. Требование к комплексности изделия. Инструмент должен реализовывать тестирование сетей в различных направлениях – пассивное (мониторинг), активное (DoS-атаки, атаки на сетевые протоколы и пр);

2. Требование к автоматизации и гибкости изделия. Инструмент должен производить различные виды атак с минимальным участием человека, при этом не исключая возможность тонкой настройки;

3. Требование к простоте изделия. При использовании утилиты не должны требоваться глубокие знания в сфере сетей, методик проведения атак и прочего;

4. Необходима интеграция программного обеспечения с внешними системами, такими как wIPS, wIDS, SIEM и некоторыми другими.

В соответствии с первым пунктом требований и классификацией [6] инструментов атаки на беспроводные сети можно прийти к выводу, что в архитектуру устройства должны быть включены следующие структурные элементы:

1. Модуль пассивного тестирования;
2. Модуль взаимодействия с внешними системами;
3. Модуль активного тестирования.

В простейшем представлении архитектура программного обеспечения, выполняющего аудит безопасности беспроводной сети, представлена на рис. 1.

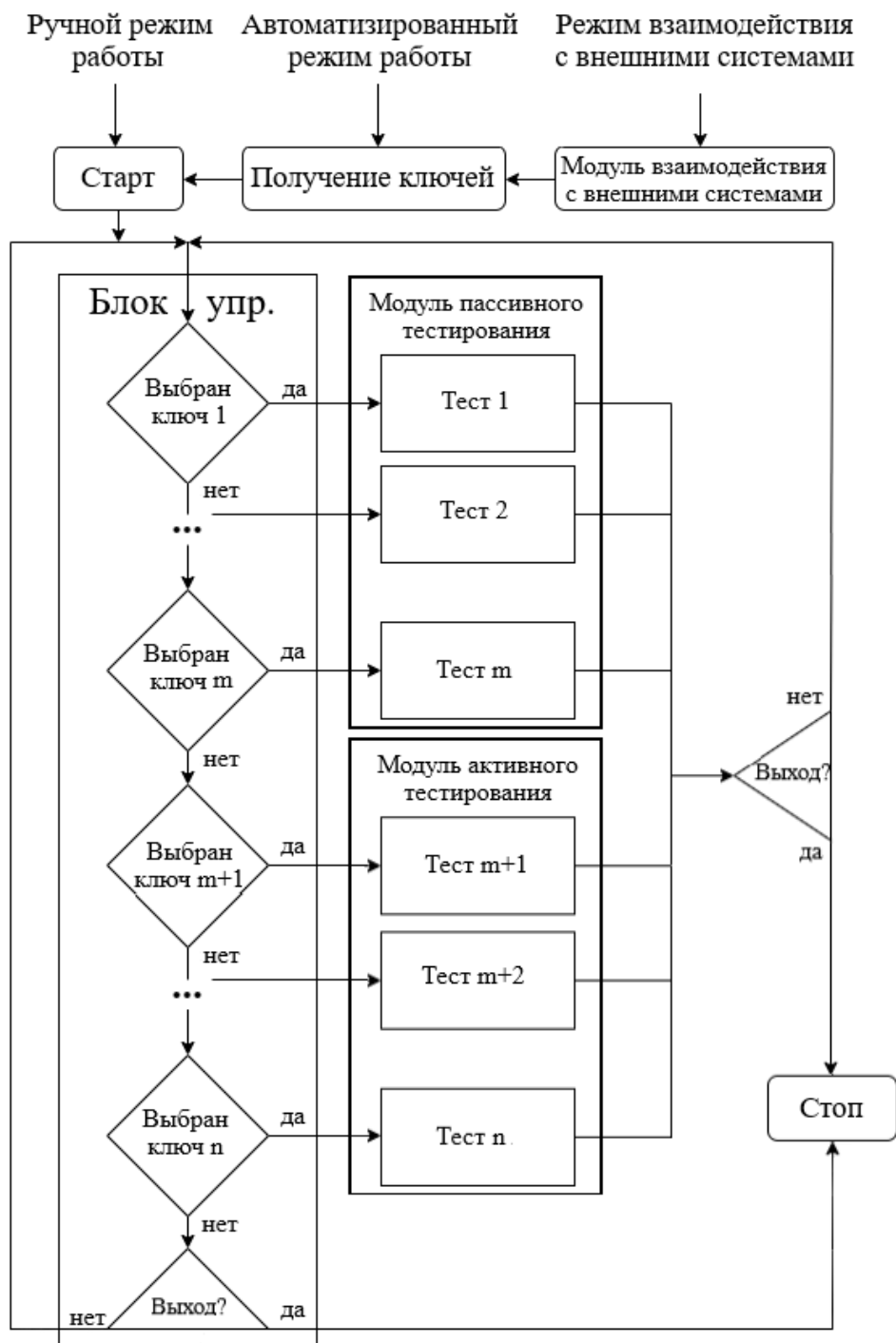


Рис. 1. Архитектура утилиты аудита безопасности

Также важно отметить, что проектируемое программное обеспечение может быть размещено как на отдельном устройстве, например Raspberry Pi, так и совмещено с другим программным обеспечением на персональном компьютере специалистов информационной безопасности или элементах систем wIPS, wIDS.

В общем случае для функционирования программы необходимы:

- среда функционирования: операционная система linux и python 3.9 и старше;
- беспроводные сетевые адаптеры, поддерживающие режим монитора;

– для загрузки утилиты и необходимых библиотек может понадобиться выход в Интернет.

Архитектура информационной системы, включающей один из способов размещения программного обеспечения (ПО), представлена на рис. 2.

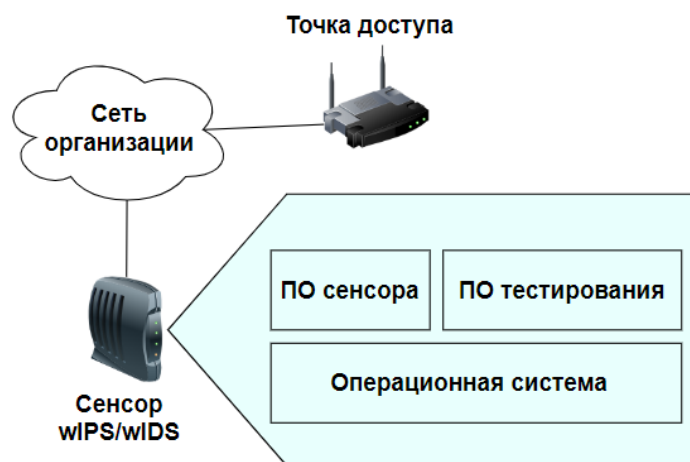


Рис. 2. Архитектура информационной системы

Таким образом, на основании требований и классификации утилит, была разработана архитектура для модуля автоматизированного аудита безопасности беспроводных сетей. В дальнейшем предстоит реализация описанного модуля и экспериментальная оценка эффективности его работы.

Список используемых источников:

1. Волкогонов В.Н. Казанцев А. А., Катасонов А. И., Орлов Г. А. Анализ безопасности Wi-Fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VIII Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 27-28 февр. 2019 г. СПб. : СПбГУТ, С. 270-275.
2. Ушаков И. А., Красов А. В., Мулладжанов Д. Д. у. Методика обнаружения аномалий в сетевом трафике с использованием IPS на основе security onion // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. N 1. С. 5-11. DOI 10.46418/2079-8199_2022_1_1. EDN DSQONB.
3. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 – ФСТЭК России: [Электронный ресурс], URL: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702> (дата обращения: 15.10.2022).
4. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 – ФСТЭК России [Электронный ресурс], URL: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21> (Дата обращения: 15.10.2022).
5. Карельский П. В., Зуев И. П., Ковцур М. М., Миняев А. А. Разработка методики тестирования IPS модуля // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. N 1. С. 25-31. DOI 10.46418/2079-8199_2021_1_4. EDN HRYGSZ.
6. Ворошнин Г. Е., Ковцур М. М., Юркин Д. В. Анализ и классификация программных инструментов для тестирования на проникновение беспроводных сетей семейства IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы XI Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 15–16 фев. 2022 г. Том 1. СПб. : СПбГУТ, 2022. С. 310-314. EDN MNROEN.

Voroshin G., Zebzeev E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Architecture of the device for automated security audit of IEEE 802.11 networks.

Today, wireless Wi-Fi networks are used almost everywhere: they can be found both in residential premises, shops, cafes, subways, and in the offices of most organizations. It is difficult for a modern person to imagine life without wireless Internet access. An ordinary user rarely thinks about the security of the method used to access the World Wide Web. How secure is the data it sends and receives? Every year there are many cases of violation of information security of networks of the IEEE 802.11 family. One of the main vulnerabilities of wireless networks is the public data transmission medium, which allows attackers to intercept and transmit any data. Given the constant improvement of attack methods, it can be argued that it is necessary to regularly monitor information security tools. Even the most advanced wireless network security tools cannot protect it from elementary attacks that degrade or disrupt the operation of network and client equipment. Taking into account this factor, there is a need to develop a device that performs regular checks of information security tools. Such a device will allow you to check the resistance of a wireless network to attacks, the readiness of information security specialists for emergency situations, and also to identify network vulnerabilities.

Key words: *information security, wireless network security, IEEE 802.11, penetration testing, wireless network testing device.*

УДК 004.056.5

ГРНТИ 81.96

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ SIEM MAHPATROL ПРИ ВЫЯВЛЕНИИ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ю. С. Данилова, С. И. Штеренберг

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В России в последние годы резко возросло количество преднамеренных вмешательств в работу информационных систем государственных и коммерческих организаций. Лучший подход для предотвращения киберугроз - организация Security Operation Center. Стоит отметить, что в качестве базовой платформы для организации SOC, как правило, покупается SIEM-система (Security Information and Event Management). В данной статье будет исследована эффективность SIEM Maxpatrol

SOC, SIEM, MaxPatrol, автоматизация, корреляция событий, инциденты

В России в последние годы резко возросло количество преднамеренных вмешательств в работу информационных систем государственных и коммерческих организаций. Согласно статистическому отчету PositiveTechnologies [1] «Актуальные киберугрозы: II квартал 2022 года» чаще всего атакам подвергались государственные учреждения. Главным образом действия злоумышленников приводили к утечкам конфиденциальной информации и нарушению деятельности госучреждений. Практически во всех случаях, после осуществления кибератак, работа организаций была заблокирована от нескольких часов до нескольких дней, что влечет большие потери, как финансовые, так и репутационные. Поэтому от степени безопасности используемых информационных технологий сейчас зависят не только стабильность и надёжность функционирования государственных институтов и коммерческих организаций, но зачастую и жизнь многих людей [2].

Лучший подход для предотвращения киберугроз - организация Security Operation Center (SOC). Лучше предотвратить возникновение атак, чем реагировать на нарушение после того, как оно произойдет. Стоит отметить, что в качестве базовой платформы для организации SOC, как правило, покупается SIEM-система (Security Information and Event Management) [3]. SIEM - это решение для мониторинга информационных систем, анализа событий безопасности и обнаружения событий информационной безопасности. Интеллектуальные системы справляются с разбором событий в разы лучше человека. Во-первых, SIEM-системы способны рассматривать и оценивать риски с разных аспектов. Это важно, так как игнорирование даже одного аспекта может нарушить стабильность и целостность анализа. Во-вторых, SIEM-системы способны с большой скоростью анализировать данные, полученные с разных источников. Интеллектуальные решения могут справиться с большинством задач в разы быстрее, чем человек [4].

В текущей статье будет рассмотрено SIEM решение MaxPatrol от компании Positive Technologies и продемонстрировано, каким образом данная система способна выявлять инциденты из тысячи событий, поступающих из разных систем.

Работа с группами активов в MaxPatrol SIEM

Актив в контексте ИБ – это сущность, имеющая ценность для организации, используемая для достижения целей организации, являющаяся объектом защиты и атаки с целью нарушения свойств безопасности. Защита активов информационной безопасности – основная обязанность данного направления. В MaxPatrol SIEM используется иерархическая структура групп активов [5], в которой предусмотрены следующие типы групп:

- системные группы;
- пользовательские группы, которые могут быть динамическими или статическими.

Группировку активов рекомендуем использовать для решения следующих задач процесса управления активами:

- систематизация сведений об активах;
- присвоение значимости активам;
- автоматизация поиска и аудита активов;
- мониторинг состояния активов

Автоматизация активного сбора событий. Активные методы сбора событий требуют формирования пары «метод сбора событий – цель сбора событий (источник)» [6]. По аналогии с аудитом активов для автоматизации сбора событий рекомендуем операторам MaxPatrol SIEM в качестве целей использовать группы активов, имеющие в своем составе источники событий. При этом стоит учитывать, что методы сбора событий непосредственно связаны с ПО, с которого происходит сбор, а значит формирование групп во многом зависит от источников событий, подключаемых к MaxPatrol SIEM. Если после аудита будет выявлен источник событий на активе, то он автоматически попадет в соответствующую ему группу источников, и MaxPatrol SIEM будет собирать события с данного источника без дополнительных действий со стороны оператора.

Корреляция событий по группам активов. Тонкая настройка правил корреляции снижает количество ложных срабатываний, тем самым снижая нагрузку на операторов в части разбора событий, ошибочно признанных инцидентами. Ниже приведена часть алгоритма правила корреляции, определяющего тип заражения вредоносным ПО (внутреннее, внешнее) и порядок создания инцидента (рис. 1).

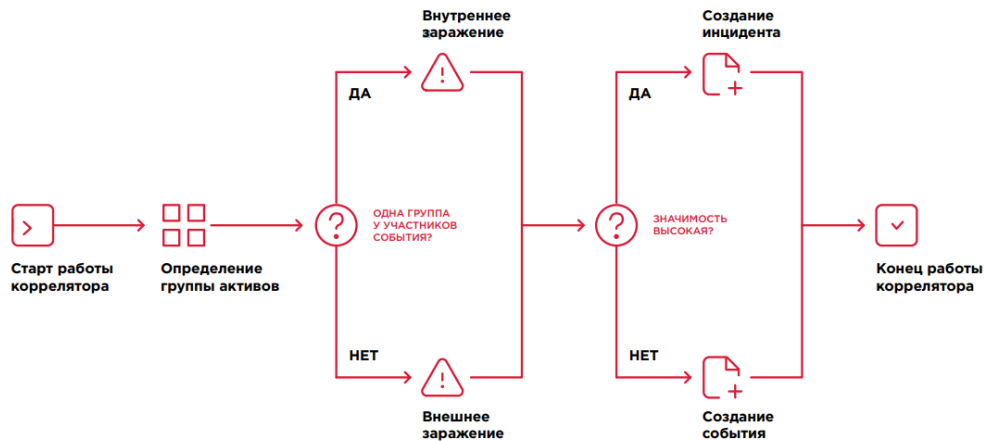


Рис. 1. Правило корреляции, определяющее тип заражения вредоносным ПО

Отчетность по итогам разбора эскалации инцидентов. Доступ к сведениям об активах, событиях и инцидентах обеспечивается на основе созданных групп активов. Это позволяет предоставлять оператору доступ к информации, связанной только с выбранными группами, а значит отдельные категории пользователей не смогут ознакомиться с недоступной для них информацией. MaxPatrol SIEM позволяет формировать отчетность по процессам управления активами, событиями и инцидентами ИБ. Функция группировки активов обеспечивает возможность предварительной фильтрации информации, поступающей в отчет (рис. 2).

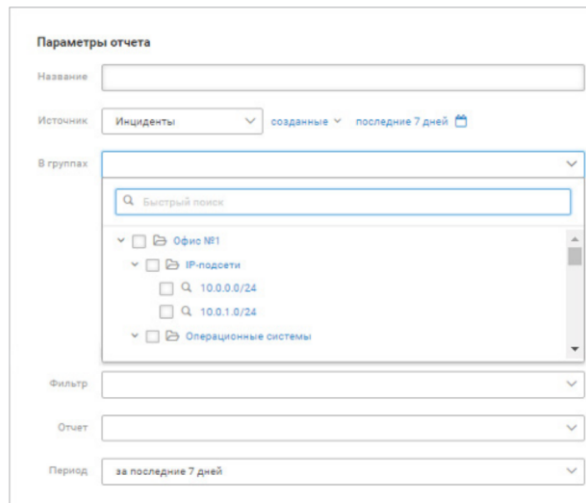


Рис. 2. Отчетность по инцидентам

Примеры выявления инцидентов

Пример №1 – Обнаружение вредоносного ПО.

Вредоносное ПО – одна из самых актуальных угроз информационной безопасности. Причем большинство из них (порядка 85%) связаны с фишинговыми рассылками. MaxPatrol SIEM использует внутренние сигнатуры для выявления вредоносной активности. То есть с некой регулярность система способна проводить сканирования, выявлять вредоносное ПО, фиксировать

информация о самом выявленном вредоносном ПО, хосте, на котором оно было обнаружено, и иную другую информацию, указанную на рис. 3.

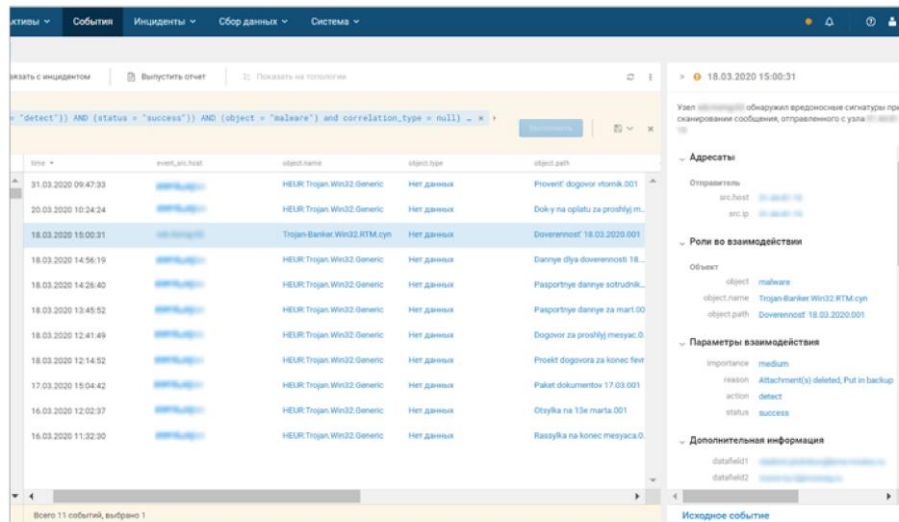


Рис. 3. Инцидент обнаружения вредоносного ПО

Пример 3. Нарушение политик ИБ

Еще одна категория инцидентов — это нарушения политик ИБ. Речь идет о выявлении фактов несоответствия требованиям нормативных документов, таких как PCI DSS, приказ ФСТЭК № 21, а также корпоративным политикам ИБ. Как правило, компаниям рекомендуется ограничить список узлов, на которых может использоваться ПО для удаленного доступа. Соответственно, ниже в примере рассмотрен инцидент ИБ, связанный с установкой ПО, запрещенного политиками (Рис. 4). В качестве такого ПО выступает TeamViewer - ПО, используемое для удаленного подключения к серверам и ПК.

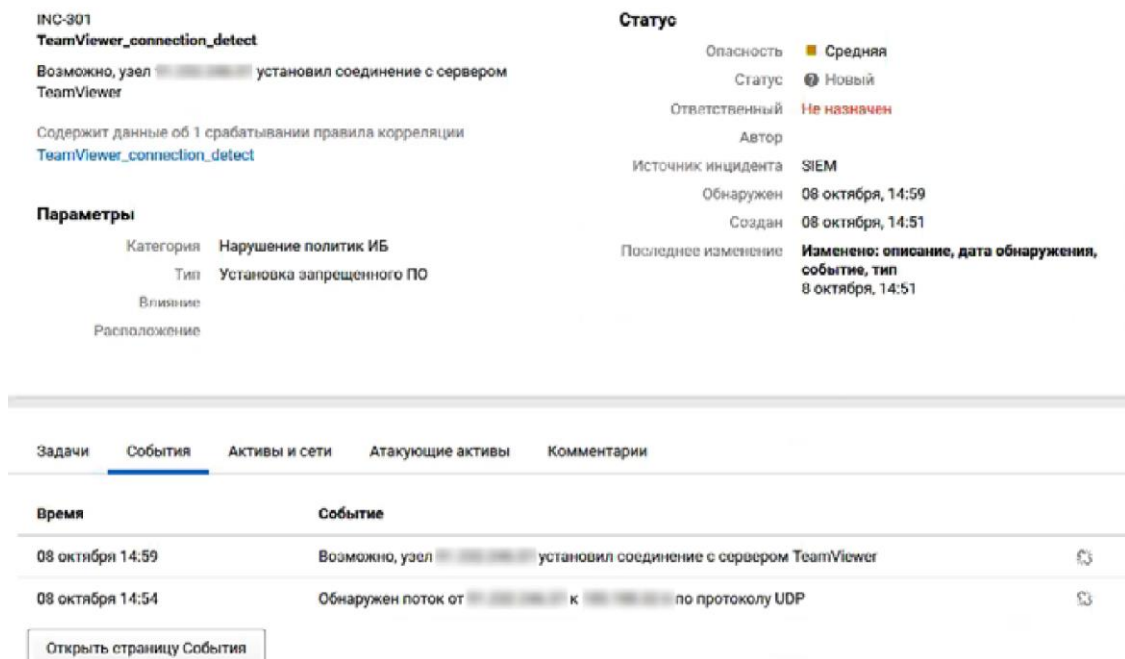


Рис. 4. Выявление инцидента по установке запрещенного ПО

В данной статье представлено лишь несколько примеров инцидентов, на основании которых проводился анализ эффективности SIEM решения MaxPatrol. Проведенный анализ позволил выявить, что MaxPatrol SIEM, благодаря встроенным правилам корреляции, позволяет выявлять актуальные техники атак без дополнительной настройки. Кроме того, MaxPatrol SIEM обладает правилами детектирования популярных техник атак (используется классификация MITRE ATT&CK), что позволяет обнаружить активность злоумышленников на ранних этапах.

Благодаря такому внедрению, компания сможет оценить эффективность инвестиций в развитие IT-инфраструктуры и обеспечить контроль за эффективностью работы систем информационной безопасности. Более того технические специалисты начинают работать эффективнее за счет того, что периодический мониторинг миллионов событий будет автоматизирован.

Список используемых источников:

1. Актуальные киберугрозы: III квартал 2021 года: [Электронный ресурс] // Positive Technologies. 29 ноября 2021. URL: <https://www.ptsecurity.com/ru-ru/research/analytics>. (дата обращения: 13.09.2022).
2. Хлестова Д.Р. Анализ актуальности использования SIEM систем на предприятиях // Символ науки. 2016. №7. 2016. С. 33-36
3. Бочкарев О.И. Создание собственного SOC в условиях международной изоляции // Информационная безопасность и международная коммуникация в контексте цифровой трансформации. С. 129-137
4. Штеренберг С. И. Разработка методики внедрения и выявления эффективности SIEM-системы // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 40-45.
5. MaxPatrol SIEM: [Электронный ресурс] // Positive Technologies. 2002-2022. URL: <https://www.ptsecurity.com/ru-ru/products/mpsiem> (дата обращения: 13.09.2022).
6. Как использовать механизм табличных списков в MaxPatrol SIEM: [Электронный ресурс] // Positive Technologies. 23 июня 2021. URL: <https://www.ptsecurity.com/upload/corporate/ru-ru/products/mpsiem/Mechanism-of-table-lists-mpsiem-a4-rus-0002-01-jun-23-2021.pdf> (дата обращения: 13.09.2022)

Danilova J., Shterenberg S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Researching the capabilities of SIEM MAXPATROL in detecting information security incidents. In Russia, the number of deliberate intrusions into the information systems of government and commercial organizations has increased dramatically in recent years. The best approach to prevent cyber threats is to organize a Security Operation Center. It is worth noting that, as a rule, SIEM (Security Information and Event Management) system is purchased as a basic platform for SOC organization. This article will investigate the effectiveness of MaxPatrol SIEM.

Key words: SOC, SIEM, MaxPatrol, automation, event correlation, incidents.

УДК 004.051
ГРНТИ 20.53.23

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ПОСТРОЕНИЯ DMVPN ПРИ ПЕРЕХОДЕ НА ОТЕЧЕСТВЕННОЕ ОБОРУДОВАНИЕ

Р. И. Дементьев, Д. Я. Держко, И. А. Ушаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На текущий момент времени остро стоит проблема импортозамещения в российских ИТ компаниях. В приведенной ниже статье рассматриваются аспекты настройки динамической виртуальной частной сети при переходе предприятия на отечественное оборудование на примере компании «Eltex». Решение вопроса реализуется через настройку идентичных топология сети, а также проверку пропускной способности в динамических туннелях при максимальной загрузке устройств. Существует потенциал для проверки реализации других сетевых технологий, не вошедших в статью.

информационная безопасность, импортозамещение, производительность, отказоустойчивость, DMVPN, IPsec, NHRP, маршрутизация, GRE-туннели

В настоящее время повсеместно используется технология многоточечных частных сетей (DMVPN) [1], так как она позволяет существенно снизить нагрузку на оборудование при организации работы удаленных офисов. Данный «overlay» VPN сокращает участие провайдера в организации соединения с большим количеством пользователей по сравнению с аналогами типа «peer-to-peer» [2].

Остро стоит вопрос о потенциале импортозамещения, так как производительность отечественных сетевых технологий играет не последнюю роль в безопасности государственных учреждений, а также в развитии внутреннего рынка страны с выходом на международный. В частности, крайне важны маршрутизаторы и коммутаторы, которые являются основой для построения любой современной сети. В связи с ростом количества атак на критические информационные инфраструктуры (КИИ) в 2020 году был опубликован приказ президента РФ. В нем утверждается, что лицам, владеющим КИИ, необходимо перейти на отечественное ПО до 1 января 2024 года, и еще на оборудование российского производства до 1 января 2025 года [3]. Оттого, на текущий момент времени крайне важен вопрос о нюансах перехода на отечественные сетевые решения.

Также актуально иметь представления о производительности российского оборудования в условиях приближенных к офисным по сравнению с популярными мировыми аналогами.

Цель статьи и ее выполнение.

Цель данной статьи – проверить возможность импортозамещения сетевых устройств Cisco на решения от компании Eltex. Она достигается через разработку двух сегментов сети, использующих популярную технологию обеспечения сетевой безопасности, а именно DMVPN. Это поможет определить нюансы

импортозамещения на практике, в том числе проверить как поведет себя оборудование при большой нагрузке.

Многоточечная виртуальная частная сеть (DMVPN).

Многоточечная виртуальная частная сеть (англ. Dynamical MultiPoint Virtual Private Network) представляет собой технологию overlay VPN, которая позволяет строить соединения основываясь на протоколах преобразования адресов NHRP [4] и построения туннелей mGRE. Безопасность передачи данных обеспечивает стек IPsec [5].

Разработка сегментов ИВС.

Разработка сегментов ИВС [7, 8, 9] проводилась на физическом оборудовании, предоставленном кафедрой ЗСС университета СПбГУТ. Модель топологии сети отражает несколько удаленных филиалов офиса, подключенных к головному. В таблице 1 отражены роли, выполняемые устройствами в сети.

ТАБЛИЦА 1. Описание ролей узлов, использующихся в топологии проектируемой сети

Имя узла	Роль
Hub	NHRP server
Spoke1	Удаленные площадки
Spoke2	
Spoke3	
PC1	Клиенты сетевых услуг
PC2	
PC3	
PC4	
Switch	Промежуточная незащищенная сеть

На рис. 1 представлена топология, реализуемая в рамках опыта.

На рис. 1 изображены удаленные филиалы офиса 1, 2 и 3 (маршрутизаторы Spoke1-3), головной офис (маршрутизатор Hub), выполняющий роль NHRP-сервера. Обе схемы идентичны по структуре, для корректности проверок.

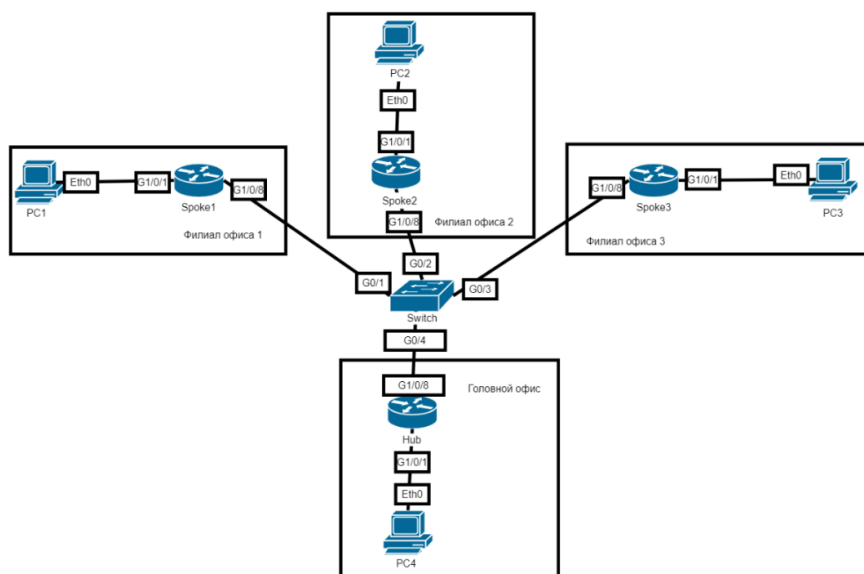


Рис. 1. Топология проектируемой сети.

Проведение проверок.

Для демонстрации работы оборудования был использован ряд команд в рамках утилиты «Iperf», позволяющий отобразить скорость передачи шифрованного трафика, с целью выявления разницы в производительности между устройствами разных компаний при максимальной загрузке процессоров.

Для наглядного представления один из результатов эксперимента был выведен в таблице 2.

ТАБЛИЦА 2. Результат выполнения команд по отправке информации

Eltex		
Команда на получателе	Отправитель /получатель	Результат выполнения команды
Передача данных с использованием TCP		
.\iperf3.exe -s -f k -p 5201	PC1/PC4	----- [ID] Interval Transfer Bandwidth [5] 0.00-141.38 sec 0.00 Bytes 0.00 Kbits/sec sender
		[5] 0.00-141.38 sec 2.00 GBytes 121504 Kbits/sec receiver -----

Рассмотрены две ситуации. В первой одновременно были запущены 3 сеанса передачи шифрованного трафика. В каждом из них передавались данные объемом 2 Гбайт, с использованием протокола TCP. После были проверены одиночные сеансы с применением UDP, так как было установлено, что при увеличении количества одновременных передач без гарантированной доставки соединение разрывалось. Опыт был проведен для обеих рассматриваемых схем. Стоит также отметить, что при тестировании прохождения зашифрованной информации по протоколу UDP некорректно отобразился процент потерянных пакетов в случае Cisco. Путем расчетов был установлен реальный процент потерь – около 80%. Далее в форме графиков на рис. 2 и рис. 3 приведена зависимость пропускной способности от времени при передаче 2 Гбайт зашифрованных данных.

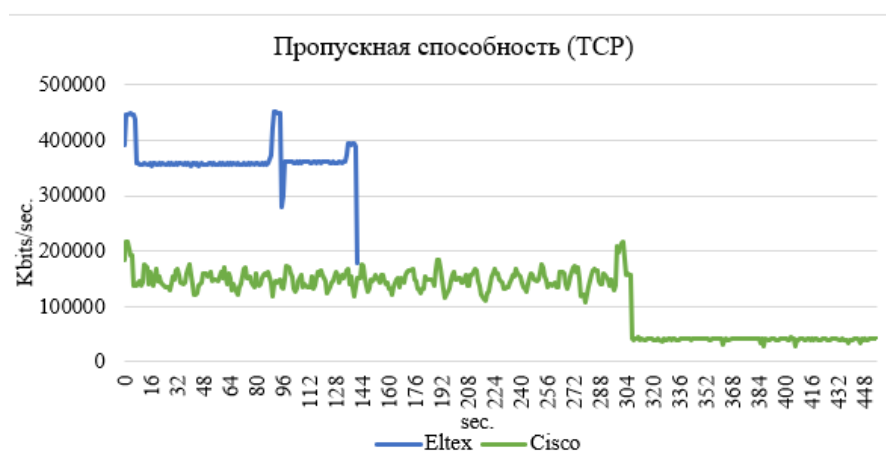


Рис. 2. Пропускная способность (TCP)

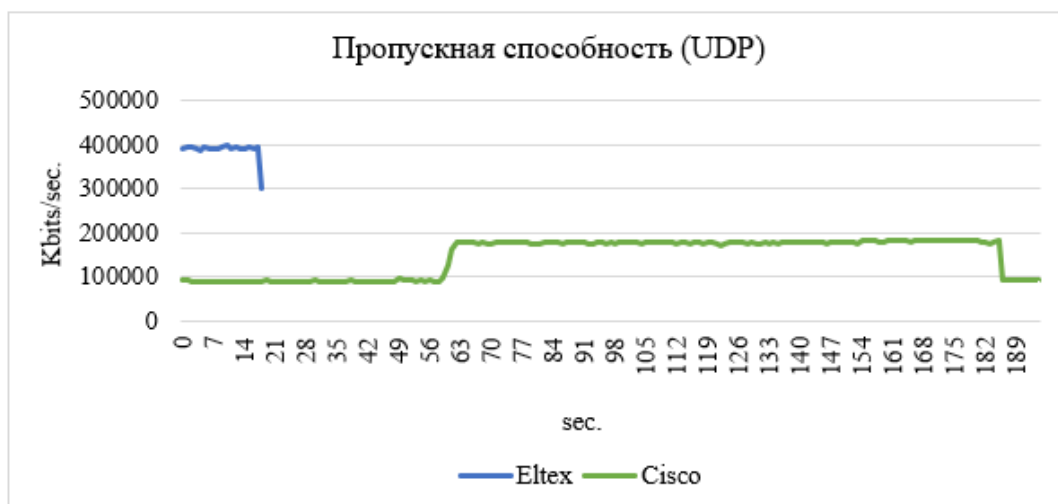


Рис. 3. Пропускная способность (UDP)

В целом, Eltex потребовалось гораздо меньше времени для передачи 2 Гбайт зашифрованного трафика из-за показателей пропускной способности. Ступенчатый характер графиков вероятно обусловлен загруженностью оборудования. Ядра процессоров устройств во время тестирования использовались на 100%.

При использовании протокола TCP, согласно расчетам, российское оборудование в среднем показало результат суммарной пропускной способности 365178 кбит/с., когда как у иностранного 133335 кбит/с. Разница составила 173%.

При передаче с применением UDP, устройства Eltex показали пропускную способность в среднем 385366 кбит/с., а Cisco 146543 кбит/с. (разница 163%), однако сильно пострадала целостность трафика. Процент потерь в обоих случаях был в районе 80%.

Очевиден вывод, что защитная технология многоточечных сетей может свободно применяться на Российском оборудовании.

К тому же CISCO1941/K9 довольно долго являлся востребованным сетевым устройством, отчего его замена на рассмотренный ESR-200 является более чем оправданной. На момент написания статьи, отечественный аналог имеет статус «ТОРП», с соответствующими сертификатами.

Беря в расчет результаты моделирования, можно сделать вывод, что маршрутизаторы компании Eltex имеют схожие с Cisco команды для настройки, отчего процесс перехода с одного решения на другое является довольно быстрым и понятным. Все поставленные задачи моделирования выполнены.

Список используемых источников:

1. Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T// Cisco Systems, Inc, 2020.
2. Красов А.В., Сахаров Д.В., Ушаков И.А., Лосин Е.П. Обеспечение безопасности передачи multicast-трафика в ip-сетях // Защита информации. Инсайд. 2017. № 3 (75). С. 34-42.
3. П. Князев, Д.В. Шалимов, В.С. Зияутдинов Особенности технологии VPN в сборнике: Информационные технологии в процессе подготовки современного специалиста: межвузовский сборник научных трудов, 2018.

4. Указ Президента Российской Федерации от 30.03.2022 № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации".

5. Сахаров Д.В., Красов А.В., Ушаков И.А., Бирих Э.В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе ipv6 // Защита информации. Инсайд. 2020. № 1 (91). С. 51-57..

6. Нестеров С. А. Основы информационной безопасности. // учебник для вузов / СПб. : Лань, 2021.

7. В. Anastasoff, M. Bernard. CCNP Security Senss 300-206 Official Cert Guide // Cisco Press, 2015.

8. ESR-Series_User_manual_v1.14.5 (от 16.02.2022)

9. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap // RFC. URL: <https://tools.ietf.org/html/rfc6071>.

10. NBMA Next Hop Resolution Protocol (NHRP) // RFC. URL: <https://tools.ietf.org/html/rfc2332> (дата обращения 28.10.2020).

Dementiev R., Derzhko D., Ushakov I.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

DMVPN tunnels.

At the current time, the problem of import substitution in Russian IT companies is acute. This article discusses aspects of setting up a dynamic virtual private network when an enterprise switches to domestic equipment using the example of Eltex. The solution to the issue is implemented through setting up identical network topologies, as well as checking throughput in dynamic tunnels at maximum device load. There is potential to test the implementation of other networking technologies not included in the article.

Key words: Information Security, dynamic tunnels, import substitution, performance, DMVPN, IPsec, NHRP, routing, GRE-tunnels.

УДК 004.627
ГРНТИ 20.23.25

ИССЛЕДОВАНИЕ МЕТОДОВ СЕТЕВОЙ СТЕГАНОГРАФИИ STEGTORRENT И SKYDE

П. С. Демидов, И. А. Ушаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Стеганография - термин, обычно описываемый как средство сокрытия секретной информации, смысл которого в том, что неосведомленная сторона не знает о ее существовании и извлекает эту информацию по месту назначения.

StegTorrent, SkyDe, сетевая стеганография

Стеганография (в узком смысле) — это часть стеганографии (в широком смысле), которая имеет трудно переводимое англоязычное название Information Hiding. Второй частью стеганографии (в широком смысле) являются цифровые водяные знаки [1].

Для каждого типа данных разрабатываются свои подходы к сокрытию. Так, в текстовой стеганографии используются предположения о расположении и количестве символов в тексте, которые не учитываются при чтении человека. Например, один из приемов - форматирование. Суть его в разделении строк за счет увеличения пробелов между словами, когда один пробел соответствует, например, биту 0, а два пробела - биту 1. Например, в сетевой стеганографии, скрытая информация передается через компьютерные сети с использованием особенностей передачи данных. Типичные методы сетевой стеганографии включают изменение свойств одного из сетевых протоколов.

В данный момент разработано большое число методов стеганографии например:

- Использование смещения слов, предложений, абзацев
- Выбор определенных позиций букв
- Скрытие информации в неиспользуемых местах гибких дисков
- Скрытие информации на основе распределения по спектру
- Скрытие на основе использования кода документов и файлов
- Скрытие информации на основе использования эхо-сигнала

Актуальность данной темы заключается в том, что по мере того, как производство, хранение и обмен информацией становятся все более обширными и важными для функционирования общества, проблема защиты информации от непреднамеренного и нежелательного использования становится все более сложной. В современных обществах защита информации включает множество взаимозависимых политических и технологических вопросов, касающихся конфиденциальности, целостности, анонимности, аутентичности, полезности.

Методы сетевой стеганографии подразделяются на:

1. Метод модификации пакетов:

Суть метода заключается в изменении свойств передаваемых сетевых пакетов. При помощи модификации определенных полей заголовка протоколов, изменением их содержимого, становится возможным инкапсулировать определенную информацию, при этом не внося изменения в пользовательские данные, содержащиеся в пакете. Также метод модификации пакетов включает в себя:

- Вложения в специальные поля протоколов
- Вложения в Payload (полезную нагрузку)
- Методы, объединяющие два предыдущих пункта

2. Метод изменения структуры потока пакетов

Второй метод основан на изменении структуры блоков данных протокола путем переупорядочивания этих блоков данных соответственно. Изменение структуры потока пакетов включает в себя:

Влияние на порядок пакетов, изменение задержки между пакетами или введение преднамеренных потерь

- Влияние на порядок пакетов
- Влияние на порядок следования пакетов
- Введение преднамеренных потерь
- Изменение меток времени

Плюсом данного метода является сложность обнаружения.

3. Гибридный метод

Данный метод основывается на объединении подходов, которые включают в себя два предыдущих метода. Рассматриваемый метод реализуется при помощи изменения содержимого пакетов, сроков доставки пакетов и порядка их передачи.

Метод StegTorrent.

StegTorrent новый сетевой стеганографический метод для популярного P2P-сервиса передачи файлов - BitTorrent. Он основан на изменении порядка пакетов данных в протоколе однорангового обмена данными. В отличие от других существующих стеганографических методов, которые изменяют порядок пакетов, он не требует синхронизации. Экспериментальные результаты, полученные в результате реализации прототипа, доказали, что он обеспечивает высокую стеганографическую пропускную способность до 270 б/с, внося при этом небольшие искажения передачи и обеспечивая сложную обнаруживаемость.

BitTorrent - система передачи файлов, первоначально выпущенная в июле 2001 года, в настоящее время является самой популярной сетевой системой P2P (Peer-to-Peer) во всем мире, которая позволяет пользователям делиться определенными ресурсами в виде файлов.

Отправитель скрытых данных использует модифицированный клиент BitTorrent - клиент StegTorrent - для совместного использования ресурса, который загружается вторым клиентом StegTorrent, который состоит из группы контролируемых клиентов BitTorrent.

Для описания и анализа предлагаемого метода определяется термин пакет данных как набор IP-адресов, который отправляется в IP-пакетах в заранее определенном порядке, а термин размер пакета данных как общее количество элементов в этом наборе. Предположим, что размер пакета данных равен 2. В этом случае два пакета с двумя разными IP-адресами (например, IP1 и IP2) используются для отправки битов скрытых данных. В этом простом сценарии, если порядок пакетов изменен для стеганографических целей, BitTorrent-клиент получает пакет, который был отправлен с IP1, а затем с IP2, то он будет интерпретироваться как двоичный "0", в другом случае двоичный "1". Пакет данных и его размер являются общим секретом между передачей и приемом клиентов StegTorrent.

Следует отметить, что производительность этого метода зависит от размера пакета данных, в то время как последний зависит от количества доступных принимающих IP-адресов (получение клиентов BitTorrent под контролем).

Метод SkyDe.

SkyDe (Skype Hide) представляет собой один из новейших стеганографических методов, суть которого заключается в использовании зашифрованных пакетов Skype с молчанием, для предоставления средств для тайной связи. Пакеты, которые не содержат голосовых сигналов, можно повторно использовать для стеганографических целей, поскольку Skype не использует никаких механизмов подавления пауз. Экспериментальная реализация метода и первые экспериментальные результаты доказывают, что этот метод осуществим и предлагает стеганографическую пропускную способность до 2,8 кбит/с.

Передача голоса по IP (VoIP) или IP-телефония — это одна из услуг в мире IP, которая позволяет пользователям совершать телефонные звонки через сети передачи данных, использующие протокол IP. В настоящее время одной из самых популярных систем IP-телефонии, потрясших мировой рынок телефонии за последнее десятилетие, является Skype (www.skype.com). Это проприетарный сервис P2P-телефонии. Из-за своей популярности и объема трафика Skype-трафик является идеальным кандидатом на роль секретного носителя данных.

Skype использует криптографические средства для обеспечения конфиденциальности для каждого типа сообщений пользователей, которыми обмениваются. Но скрытая связь не обязательно должна осуществляться сквозным образом, т. е. скрытые данные могут быть отправлены с использованием сторонних VoIP-вызовов. В последнее время возникла дискуссия о том, оказывает ли Skype, звонки которого, как считалось, очень сложно прослушать, правоохранительным органам услуги законного прослушивания. Кроме того, Skype является закрытым программным обеспечением, и поэтому ему нельзя доверять.

Эксперименты, проведенные с реальным трафиком Skype, доказывают, что метод — SkyDe (Skype Hide) — выполним и предлагает высокую стеганографическую пропускную способность и разумную стоимость стеганографии с точки зрения необнаруживаемости.

Весь трафик в Skype зашифрован; ни сигнальные сообщения, ни пакеты, несущие голосовые данные, не могут быть обнаружены. Как правило, предпочтительным транспортным протоколом Skype является протокол пользовательских дейтаграмм (UDP).

SkyDe предназначен для использования зашифрованных голосовых потоков Skype для обеспечения тайной связи. Этот секретный обмен данными может осуществляться между: двумя пользователями Skype.

ТАБЛИЦА 1. Сравнение методов SkyDe и StegTorrent

Стоимость	Сложность реализации	Обнаруживаемость	Пропускная способность
SkyDe	SkyDe	SkyDe	SkyDe
StegTorrent	StegTorrent	StegTorrent	StegTorrent

В таблице 1 приведены результаты сравнение методов сетевой стеганографии по их основным характеристикам. Исходя из данных, продемонстрированных в таблице, можно сделать вывод, что показатели метода SkyDe выше, чем у StegTorrent.

Подводя итоги, хотелось бы сказать, что в связи с постоянно возрастающей сложностью протоколов связи растет и потребность в сетевой стеганографии. Нет сомнений в том, что новые, более совершенные методы будут созданы и, по сути, риск того, что они будут использованы в злонамеренных целях, будет увеличиваться. Эта проблема добавляет новые проблемы к сложному вопросу построения сети и обеспечения информационной безопасности.

Список используемых источников:

1. Коржик В. И., Небаева К. А., Герлинг Е. Ю., Догиль П. С., Федянин И. А. Цифровая стеганография и цифровые водяные знаки. Т. 1. СПб. : СПбГУТ, 2016. 226 с.
2. Костырин А. С., Красов А. В. Обзор возможностей реализации канальной стеганографии на основе протоколов сетевого и транспортного уровней модели OSI // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VI Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 01-02 марта 2017 г. СПб. : СПбГУТ, 2017. Т. 2.С. 437-443.
3. Красов А. В., Степанов Е. И. Практическое применение сетевой стеганографии на примере протокола icmp // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VII Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 28 февр.-01 марта 2018 г. СПб. : СПбГУТ, 2018. Т. 2.С.510-513.
4. Mazurczyk W, Szczypiorski K. Steganography of VoIP Streams. In OTM 2008, Part II Lecture Notes in Computer Science (LNCS) 5332, Meersman R, Tari Z(eds). Springer-Verlag: Berlin Heidelberg, Proceedings of The 3rd International Symposium on Information Security (IS'08), Monterrey, Mexico, 10–11 November 2008, P. 1001–1018.
5. Mazurczyk W, Lubacz J. LACK—a VoIP stegano-graphic method. In Telecommunication Systems: Modelling, Analysis, Design and Management, Vol. 45, N 2–3, 2010, ISSN: 1018-4864 ISSN: 1572-9451 Springer US, Journal N 11235.
6. J. Zhai G., Liu Y. Dai. Detection of TCP covert channel based on Markov Model. Telecommun Syst. 2013. P. 333-343.

7. Dittmann J, Hesse D, Hillert R. Steganography and steganalysis in voice-over IP scenarios: operational aspects and first experiences with a new steganalysis tool set. In: Proc SPIE, Vol 5681, Security, Steganography, and Watermarking of Multimedia Contents VII, San Jose. 2005. P. 607–618.

Demidov P., Ushakov I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Research of network steganography methods StegTorrent and SkyDe.

Steganography is a term usually described as a means of hiding secret information, the meaning of which is that the unconscious party does not know about its purpose and extracts this information for its intended purpose.

Key words: StegTorrent, SkyDe, network steganography.

УДК 004.056
ГРНТИ 81.93.29

СЛОЖНОСТИ ПРИ ПРОВЕДЕНИИ ОЦЕНКИ СООТВЕТСТВИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ТРЕБОВАНИЯМ ГОСТ Р 57580.1-2017

А. А. Дятченко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В связи с увеличением количества инцидентов информационной безопасности и изменениями в требованиях к защите информации в платежной системе Банка России в статье рассматриваются недостатки инфраструктуры, выявленные в результате проведения оценки соответствия требованиям национального стандарта Российской Федерации о защите информации финансовых организаций, а также структура его требований.

защита информации, ГОСТ Р 57580.1-2017, оценка соответствия систем защиты информации

С 2019 года системы защиты информации ряда организаций должны удовлетворять требованиям ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (ГОСТ Р 57580.1-2017), к таким организациям, на основании Положений Центрального Банка Российской Федерации 683-П, 757-П, 747-П и 719-П, относятся соответственно кредитные организации, некредитные финансовые организации, участники платежной системы Банка России и операторы услуг платежной инфраструктуры [1].

Кроме того, по данным аналитиков Ростелеком-Солар во втором квартале текущего года был зафиксирован трехкратный рост подтвержденных инцидентов высокой степени критичности, что говорит об увеличении количества кибератак в целом и активизации злоумышленников [2]. На рис. (рис. 1) представлено распределение инцидентов, зарегистрированных в течение первых двух кварталов 2022 г., в зависимости от уровня их критичности.

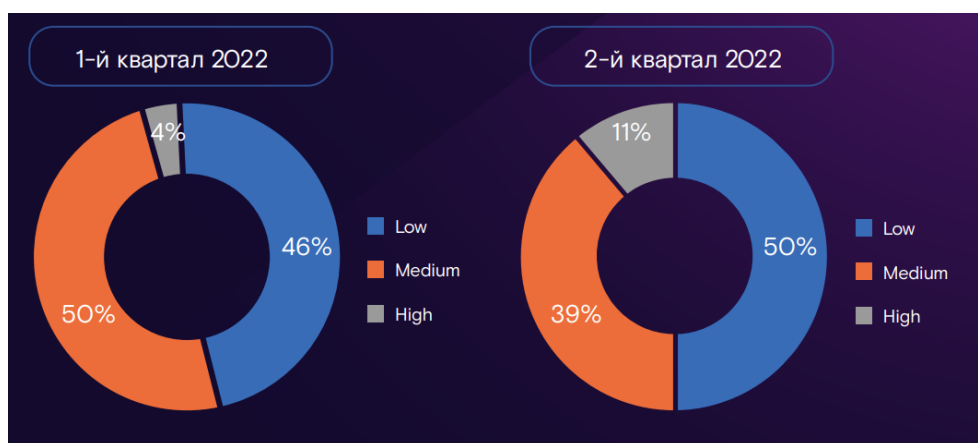


Рис. 1. Распределение инцидентов по критичности

Требования ГОСТ Р 57580.1-2017 объединяют в себе не только технические меры, но и организационные, реализация которых поможет выстроить слаженную систему защиты финансовой организации (ФО).

Рассматриваемый международный стандарт определяет 3 уровня защиты информации (уровень ЗИ): минимальный, стандартный и усиленный. В зависимости от установленного уровня ЗИ, ФО должна организовывать аудит, который проводится проверяющей организацией, с периодичностью, варьирующейся от одного до трех лет.

В ГОСТ Р 57580.1-2017 требования разделены на 3 раздела:

- 7-й отвечает за требования к системе ЗИ;
- 8-й за организацию и управление ЗИ;
- 9-й за ЗИ на этапах жизненного цикла автоматизированных систем и приложений.

Самый объемный 7-й раздел состоит из 8 процессов, некоторые из которых в свою очередь подразделяются на подпроцессы. Процессы и подпроцессы содержат перечень мер системы ЗИ, для каждой из которых в зависимости от уровня ЗИ определен один из трех возможных способов реализации:

- «О» – организационный;
- «Т» – технический;
- «Н» – реализация не обязательна.

Структура мер ГОСТ Р 57580.1-2017 приведена на рис. (рис. 2).

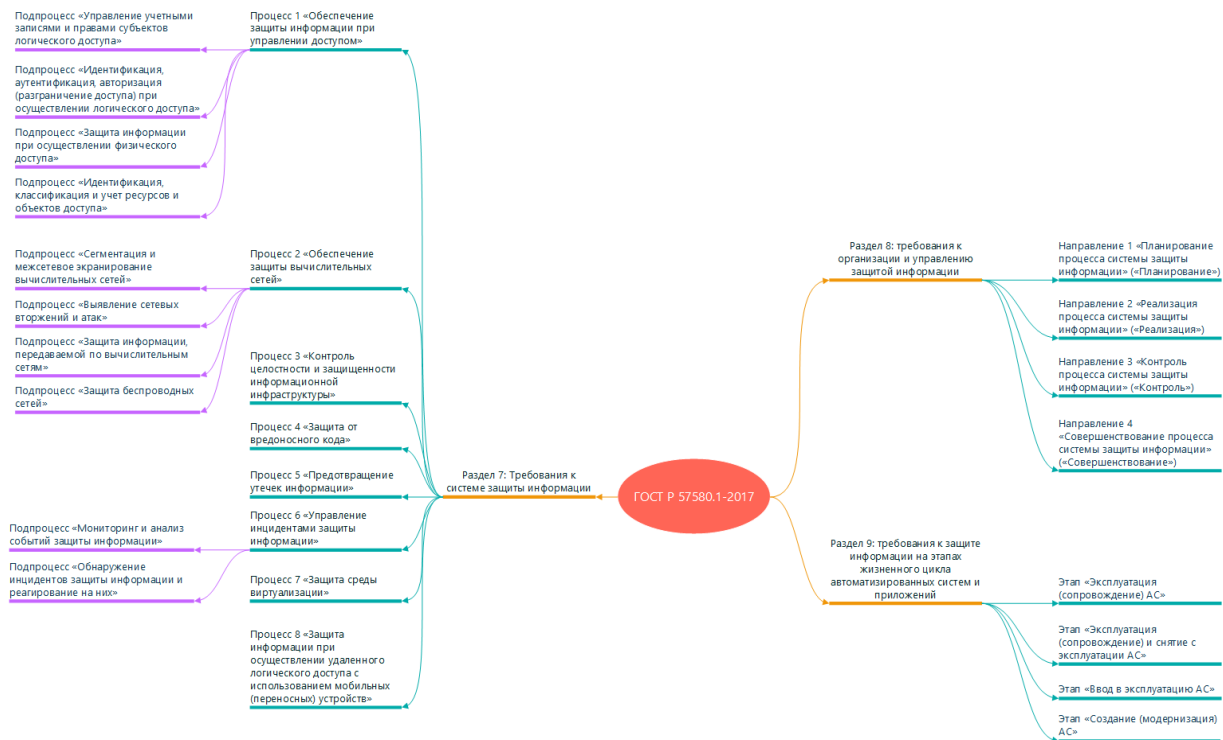


Рис. 2. Структура мер ГОСТ Р 57580.1-2017

Оценка соответствия требованиям ГОСТ Р 57580.1-2017 проводится в соответствии с методикой, определенной в ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» [3].

В данной работе представлены некоторые часто встречающиеся недостатки инфраструктуры, выявленные в результате проведения оценки соответствия требованиям ГОСТ Р 57580.1-2017.

1. Недостаточность организационно-распорядительной документации.

В процессе разработки и модернизации инфраструктуры ФО могут пренебрегать необходимостью документировать и описывать реализуемые функции и актуальную архитектуру, обновлять сетевые и структурные схемы, не поддерживая их в актуальном состоянии, в результате чего при проведении аудита могут возникнуть сложности в оценке инфраструктуры на уровнях аппаратного обеспечения и сетевого оборудования.

Зачастую процесс документирования отсутствует или недостаточно качественно реализован, при этом могут отсутствовать паспорта АС, регламенты, описывающие внутренние процессы обеспечения безопасности и взаимодействие структурных единиц, положения, касающиеся порядка реализации мер защиты информации и другие документы.

Также при наличии внутренней нормативной документации на момент проверки она может быть неактуальной, что помешает достоверно оценить состояние и слаженность выстроенных внутренних процессов.

Помимо формального закрепления и определения внутренних процессов и правил, наличие и полнота внутренней документации позволят повысить оценку по некоторым процессам на несколько сотых единиц.

2. Использование облачных сервисов.

Одной из сложностей при проведении корректной оценки инфраструктуры является полное или частичное размещение объектов доступа у провайдера облачных услуг. В таком случае затруднительно оценить фактическую реализацию мер, относящихся к процессу 7 «Защита среды виртуализации» и направленных в частности на регистрацию различных операций над виртуальными машинами и связанных с доступом к виртуальным машинам и серверным компонентам виртуализации, а также мер физической безопасности. Такая ситуация может складываться в силу отсутствия разграничения зон ответственности между клиентом и провайдером облачной инфраструктуры относительно реализуемых мер ЗИ, выполнение которых он обязуется обеспечивать в своей инфраструктуре [4].

Также сложность в оценке инфраструктуры ФО, расположенной на стороне облачного провайдера, может возникнуть в случае обеспечения провайдером недостаточного уровня соответствия процессов системы защиты информации, что может повлечь за собой возникновение финансовых, репутационных и производственных рисков для ФО [5]. Итоговый показатель и уровень соответствия должны быть представлены в выданном провайдеру заключении об оценке соответствия требованиям ГОСТ Р 57580.1-2017.

Кроме того, в процессе моделирования угроз для систем, расположенных в облачной инфраструктуре, часто возникают противоречия, в силу различия итогового перечня угроз, которые провайдер признает актуальными для своей инфраструктуры. Например, в случае, когда для провайдера актуальны угрозы, связанные с недекларированными возможностями программного обеспечения или программно-аппаратных средств, клиент должен также учитывать эти угрозы для своих информационных систем, размещенных в такой инфраструктуре, и соответственно адаптировать компенсирующие меры для нейтрализации угроз безопасности информации.

3. Выстраивание процессов системы защиты информации.

Раздел 8, направленный на оценку организации и управления защитой информации, требует структурированности выстроенных в ФО процессов для оценки их реализации на следующих стадиях: планирование, реализация, контроль и совершенствование. При этом более половины мер, оценка по которым должна быть выставлена для каждого из 8 процессов, определенных в предыдущем разделе, являются организационными, т.е. предусматривают установление временных, территориальных, правовых и иных ограничений на объекты информатизации и режимы их функционирования. Другими словами, планирование предполагает документарное определение мер защиты, реализуемых в ФО; реализация – периодическое проведение инвентаризации, определение ответственных лиц и проведение обучений работников; контроль – проведение разносторонних проверок с определенной периодичностью; совершенствование – проведение регулярного анализа необходимости совершенствования системы защиты информации. Эти с должны учитываться во всех реализованных процессах защиты, однако часто исполняются выборочно, например, при планировании порядка реагирования на инциденты безопасности или процедуры выявления и устранения уязвимостей.

В результате исследования были обозначены инфраструктурные и организационные проблемы, рекомендации по устранению которых будут представлены в дальнейших публикациях.

Список используемых источников:

1. ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. М. : Стандартинформ, 2020.
2. Отчет Ростелеком-Солар «Атаки на российские компании во 2-м квартале 2022 года»: [Электронный ресурс]. URL: https://rt-solar.ru/upload/iblock/de4/d56d2ff6f2xcqm3702kza3bqd4u5t19c/otchet_ataki_na_rossiyskie_kompanii_vo_2_m_kvartale_2022_goda.pdf. (Дата обращения 05.11.2022).
3. ГОСТ Р 57580.2-2018. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия. М. :Стандартинформ, 2018.
4. Сахаров Д. В., Левин М. В., Фостач Е.С., Виткова Л. А. Исследование механизмов обеспечения защищенного доступа к данным, размещенным в облачной инфраструктуре // Научные технологии в космических исследованиях Земли. 2017. Т. 9. N 2. С. 40–46.
5. Ли Н. И., Русяева М. С., Богданова В. А. Снижение рисков информационной безопасности облачных сервисов // «Подготовка киберэкспертов» : материалы регион. научно-практич. конф., Санкт-Петербург, 7-8 июля 2022 г. СПб. : СПбГУТ, 2022. С. 48 – 52.

Dyatchenko A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

The cyber security audit difficulties

Due to the increase in the number of information security incidents and changes in the requirements for information protection in the payment system of the Bank of Russia, the article examines the shortcomings of the infrastructure identified as a result of the assessment of compliance with the requirements of the national standard of the Russian Federation on the protection of information of financial organizations, as well as the structure of its requirements.

Key words: *cyber security, GOST R 57580.1-2017, information security audit*

УДК 004.01
ГРНТИ 81.93.29

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ НА БАЗЕ ОБЛАЧНОГО РЕШЕНИЯ

А. Л. Егорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Все чаще организации решают построить свою информационную инфраструктуру на базе облачных решений, таких как Amazon Web Services, Яндекс.Облако, Oracle Cloud. Облачные решения представляют ряд преимуществ по сравнению с привычными технологиями обработки данных, но способы построения такой инфраструктуры отличается от привычной, в связи с чем к оценке рисков информационной безопасности следует подходить иначе.

оценка рисков, информационная безопасность, облачные решения, ИТКС, конфиденциальность

Сейчас крупные вычислительные облака состоят из тысяч серверов, находящихся в центрах обработки данных. Они обеспечивают ресурсами десятки тысяч клиентов. Облачные решения несут в себе выгоду для предприятий с небольшим бюджетом, которым дорого развёртывать собственную инфраструктуру для содержания собственных серверов.

Предоставление облачных сервисов можно сравнить с предоставлением всем привычных ресурсов – воды, газа и электричества. Потребители просто получают желаемый ресурс, не думая о его источнике. Облачные технологии внедрили ту же концепцию в мир информационных технологий. С помощью модели облачных вычислений программное обеспечение, платформы и инфраструктуры становятся доступными как веб-сервисы через Интернет, а потребители облачных сервисов не знают о физическом местоположении, в котором эти службы выполняются. Компаниям больше не требуется наличие физических активов для выполнения желаемых задач, они получают аппаратные и программные ресурсы в качестве услуг от поставщиков облачных услуг.

Существует много разнообразных определений термина «риск», но в контексте данной работы целесообразно обратить внимание на определения, представленные в таблице 1.

ТАБЛИЦА 1. Определение риска

Источник	Определение
ISO/IEC 27005:2011 [2011]	«Потенциальная возможность того, что данная угроза будет использовать уязвимости актива или группы активов и тем самым нанесёт ущерб организации. Может быть измерено исходя из

	комбинации вероятности события и его последствия.»
SANS 27002:2008/ISO/IEC 27002:2005 [2008:2]	«Сочетание вероятности события и его последствий.»
NIST [2009:1]	«Мера степени, в которой субъекту угрожает потенциальное обстоятельство или событие, и, как правило, функция: (i) неблагоприятных последствий, которые могут возникнуть в случае возникновения обстоятельств или событий; и (ii) вероятность возникновения».
ENISA [2011]	«Потенциал того, что данная угроза будет использовать уязвимости актива или группы активов и тем самым нанесет ущерб организации».
FAIR [Jones, 2005:5]	«Вероятная частота и вероятная величина будущих потерь»

Таким образом, риск – потенциальное возникновение инцидента, вызванного наличием уязвимостей в облачной сети, что может привести к причинению вреда системе или организации [1].

Процесс по управлению рисками в свою очередь состоит из набора действий, направленных на отслеживание и контроль рисков. Этот процесс нацелен на повышение стратегической и тактической безопасности и включает в себя проведение оценки рисков, реализацию стратегии снижения рисков и применение методов и процедур контроля рисков для непрерывного мониторинга состояния безопасности информационной системы. Облачные информационные системы, как и традиционные информационные системы, требуют, чтобы риски управлялись на протяжении всего жизненного цикла разработки системы (System Development Life Cycle).

В соответствии с принципами безопасности риски ИБ облачных ИТКС могут быть классифицированы как:

– Риски нарушения доступности. Облачная ИТКС должна обеспечивать достаточный уровень предсказуемости с приемлемым уровнем производительности вычислительных ресурсов. Доступность обеспечивает авторизованным подписчикам облачного сервиса надежный и своевременный доступ к данным и ресурсам облачной ИТКС. На доступность облачной ИТКС может повлиять сбой или нарушение динамической балансировки ресурсов облачного сервиса и программно- аппаратного обеспечения. Атаки DDoS и EDoS являются наиболее популярной методикой злоумышленников для нарушения доступности облачных ИТКС.

– Риски нарушения целостности. Целостность обеспечивает гарантии точности и полноты, как информации обрабатываемой в облачном сервисе, так

и ресурсов предоставляющей ее облачной ИТКС. Целостность защищает информацию от несанкционированных изменений и уничтожения. Если злоумышленник запустит на исполнение разрушающее программное воздействие - целостность ИТКС и ее ресурсов будет нарушена. Такое воздействие негативно повлияет на обеспечение целостности конфиденциальной информации, обрабатываемой и хранящейся в облачной ИТКС, что может привести к мошенничеству, несанкционированным изменениям облачной среды, краже снимков виртуальных машин и баз данных.

– Риски нарушения конфиденциальности. Конфиденциальность обеспечивает недоступность информации или обеспечивает секретность ее содержания для неавторизованных лиц в каждой точке обработки информации и предотвращает ее несанкционированное раскрытие.

Конфиденциальность в облачной ИТКС должна обеспечиваться, как в процессе обработки, так и в процессе хранения и передачи информации. Атакующие могут нарушить конфиденциальность, перехватывая сетевой трафик между виртуальными машинами облачной ИТКС, похищать снимки виртуальных машин, целевую информацию о состоянии облачной ИТКС [2]. Кроме этого, пользователи облачной ИТКС могут преднамеренно или случайно разглашать конфиденциальную информацию. Общие риски для облачных ИТКС рассмотрены в работе альянса CSA «Security Guidance for critical areas of focus in cloud computing». К характерным рискам для облачных вычислений можно отнести:

- кража учетных записей;
- атаки на гипервизор;
- атаки на виртуальную инфраструктуру;
- блокирование сегмента облачной ИТКС;
- кража вычислительных ресурсов облачной ИТКС;
- нарушение механизма динамической балансировки ИТКС.
- В целом вектор угроз определяется, как:
 - Потеря/утечка данных - 26,5%
 - Неправомерное использование, нарушение правил пользования - 19,4%
 - Использование небезопасных интерфейсов - 14,2%
 - Кража и прослушивание аккаунтов - 12,3%
 - Неизвестные угрозы - 8,4%
 - Уязвимости технологии виртуализации - 6,5%

Таким образом, более 70% угроз негативного воздействия на ИТКС и ее ресурсы связаны с влиянием человеческого фактора [3].

Список используемых источников:

1. Машкина И. В. Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий : автореф. дис. ...д-ра техн. наук : 05.13.19 / Машкина Ирина Владимировна. Уфа. 2009. С. 10-12.
2. Бирюков А. Информационная безопасность: защита и нападение. М. : ДМК, 2017. 2013.

3. NIST. Managing Risk in Cloud Ecosystem: [Электронный ресурс]. URL: <https://www.nist.gov/publications/managing-risk-cloud-ecosystem> (Дата обращения 18.05.2018).

Egorova A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

IPTV Service Delivery Models.

Increasingly, companies decide to build their information infrastructure based on cloud solutions, such as Amazon Web Services, Yandex.Cloud, Oracle Cloud. Cloud solutions present a number of advantages over conventional data processing technologies, but the ways of building such an infrastructure differs from the usual one, and therefore the assessment of information security risks should be approached differently.

Key words: *risk assessment, information security, cloud solutions, ITS, confidentiality.*

УДК: 004.056
ГРНТИ 81.93.29

КЛАССИФИКАЦИЯ ОБЛАСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПРИМЕНЕНИЕМ КАТЕГОРИАЛЬНОГО ДЕЛЕНИЯ

Л. Р. Елизарова, К. Е. Израилов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обеспечение информационной безопасности является актуальной задачей современного мира. Для этого, в частности, необходимо корректное выделение соответствующих областей в данной сфере. В статье предлагаются авторские классы областей информационной безопасности, полученные применением аппарата категориального деления. Приводятся примеры сущностей сферы для каждого из классов.

информационная безопасность, категориальное деление, классификация

Важность информационной безопасности (далее – ИБ) обосновывается критичностью последствий ее нарушения, ведущих не только к финансовым потерям, но даже к человеческим жертвам [1]. Для обеспечения полноценной ИБ важно определить ее область и применять в ней соответствующие меры. Поэтому первой задачей логично является разработка классификации областей ИБ.

Современные классификации не всегда корректны, потому что области могут пересекаться между собой или же охватывают не все классифицируемые объекта. Причина такого рода «неудачных» классификаций состоит в том, что для их построения применяются не методологические аппараты, а эвристические подходы.

В статье предлагается авторская классификация областей ИБ, использующая методологически корректный аппарат категориального деления.

Аппарат категориального деления.

Суть категориального деления состоит в том, что выделяются пары категорий взаимно противоположных сущностей, комбинируя которые можно получить классы и как результат разделить по ним области ИБ [2].

Категориальные пары встречаются в каждой области, такой, как физика – «горячее vs холодное», математика – «положительный vs отрицательный», философия – «объект vs субъект», психология – «интроверт vs экстраверт» и т.п.

Аналогично, для области информационных технологий можно выделить такие категориальные пары, как «человек vs машина», «статический vs динамический», «аппаратный vs программный».

Поскольку категориальное деление применяется для известных областей, значит его можно применить и для области ИБ [3].

Классификация областей ИБ.

Выделим категориальные пары для области ИБ, используя следующие предпосылки (а также вводя индексы для будущего использования).

ИБ обеспечивает защиту данных, которые могут храниться или перемещаться [4], что дает первую категориальную пару – «статика (индекс S, сокр. от англ. Static) vs динамика (индекс D, сокр. от англ. Dynamic)».

Особенность ИБ в том, что она завязана на информационных технологиях, которые представляют собой программно-аппаратные комплексы – значит категориальная пара может быть следующей: «аппаратный (индекс H, сокр. от англ. Hardware) vs программный (индекс S, сокр. от англ. Software)».

Также, часть данных непосредственно участвуют во взаимодействии с пользователем и другими обработчиками, а часть – представляют собой встроенный информационный слой; таким образом, третья категориальная пара может быть следующей – «внешний (индекс E, сокр. от англ. External) vs внутренний (индекс I, сокр. от англ. Internal)».

Приведем интерпретацию всех указанных элементов категориальных пар.

Статические данные – это набор данных определенной формы и содержания [5], которые не модифицируются при обработке. Динамические данные, наоборот, могут изменяться после сохранения, а также подвержены изменению.

Аппаратное обеспечение – это физическая часть компьютера, которая обеспечивает его физические вычисления. Программное обеспечение – это набор инструкций, которые описывают алгоритмы вычисления и данные для них.

Внешние данные – информация, которая хранится на сервере. Внутренние же данные, наоборот, хранятся в локальных системах.

Таким образом, комбинация 3-х категориальных пар дает $2 \times 2 = 8$ классов областей ИБ:

1) K_{SHE} – образован пересечением статических данных, аппаратного обеспечения и внешнего доступа; например, защита портативных устройств хранения информации, таких, как USB-Flash или аппаратная система распознавания отпечатка пальца на мобильном телефоне.

2) K_{SHI} – образован пересечением статических данных, аппаратного обеспечения и внутреннего доступа; например, защита внутренних устройств хранения данных, таких как жесткий диск.

3) K_{SSE} – образован пересечением статических данных, программного обеспечения и внешнего доступа; например, защита Интернет-ресурсов.

4) K_{SSI} – образован пересечением статических данных, программного обеспечения и внутреннего доступа; например, защита базы данных.

5) K_{DHE} – образован пересечением динамических данных, аппаратного обеспечения и внешнего доступа; например, использование аппаратной системы обнаружения вторжений.

6) K_{DHI} – образован пересечением динамических данных, аппаратного обеспечения и внутреннего доступа; например, аппаратные средства

обеспечения резервного хранения и обработки данных, такие, как, дополнительные RAID-массивы;

7) K_{DSE} – образован пересечением динамических данных, программного обеспечения и внешнего доступа; например, обеспечение конфиденциальности обмена информацией между абонентами в процессе телефонного разговора.

8) K_{DSI} – образован пересечением динамических данных, программного обеспечения и внутреннего доступа; например, технология электронно-цифровой подписи.

Наглядное деление классов по категориальным парам представлено в таблице 1.

ТАБЛИЦА 1. Деление классов ИБ по категориальным парам

Статика				Динамика			
Аппаратный		Программный		Аппаратный		Программный	
Внеш.	Внутр.	Внеш.	Внутр.	Внеш.	Внутр.	Внеш.	Внутр.
K_{SHE}	K_{SHI}	K_{SSE}	K_{SSI}	K_{DHE}	K_{DHI}	K_{DSE}	K_{DSI}

Применение к существующим областям.

Попытаемся применить классификацию, полученную полностью корректным методологическим аппаратом, к наиболее распространенным областям ИБ:

1) *Компьютерная безопасность* заключается в защите компьютерных систем и сетей – одновременно относится к классам K_{SHE} и K_{DHE} .

2) *Безопасность инфраструктуры* обеспечивает защиту внутренних сетей, лабораторий, центров обработки данных, серверов, настольных компьютеров и мобильных устройств [6] – относится к классу K_{SHE} .

3) *Безопасность баз данных* с помощью средств ИБ обеспечивает защиту баз данных от нарушения их конфиденциальности, целостности и доступности – относится к классу K_{SSI} .

4) *Операционная безопасность* обеспечивает идентификацию и защиту критически важной информации [7] – относится к классам K_{SSI} и K_{DSI} .

5) *Безопасность приложений* заключается в разработке и улучшении методов обеспечения ИБ приложений – относится к классу K_{DSE} .

6) *Физическая безопасность серверов* обеспечивает защиту серверных помещений, по авторской классификации относится к классу K_{SHE} .

7) *Сетевая безопасность* занимается обеспечением ИБ компьютерной сети и ее ресурсов [8] – относится к классу K_{DSI} .

8) *Криптография* заключается в разработке методов шифрования информации [9] – относится к классу K_{DSI} .

Как видно, предложенная классификация не всегда хорошо ложится на типовые области ИБ. Это как раз и можно обосновать различиями применяемых для классификации подходов – теоретического и практического.

В работе с помощью аппарата категориального деления получена новая классификация из комбинации 3 элементов пар (статика vs динамика, аппаратный vs программный, внешний vs внутренний), для которых предложены примеры их интерпретации, а также произведена попытка классификации существующих областей ИБ.

Применение аппарата категориального деления обосновывает корректность полученного деления – классы гарантированно не пересекаются и покрывают всю область ИБ.

Дальше планируется разработка метода анализа статистики научных исследований и публикаций для каждого из классов с целью выявления наиболее актуальных и/или малоизученных из них в рамках выполнения выпускной квалификационной работы.

Список используемых источников:

1. Абдуллин Т.И., Баев В.Д., Буйневич М.В., Бурзунов Д.Д., Васильева И.Н., Галиуллина Э.Ф. и др. Цифровые технологии и проблемы информационной безопасности: монография. СПб: СПГУ 2021. 163 с.
2. Буйневич М.В., Израйлов К.Е. Категориальный синтез и технологический анализ вариантов безопасного импортозамещения программного обеспечения телекоммуникационных устройств // Информационные технологии и телекоммуникации. 2016. Т. 4. № 3. С. 95-106.
3. Израйлов К.Е. Обобщенная классификация уязвимостей интерфейсов транспортной инфраструктуры Умного города // Информационные технологии. 2021. Т. 27. № 6. С. 330-336. DOI: 10.17587/it.27.330-336.
4. Агамирова Т.Д. Метод обеспечения информационной безопасности // Матрица научного познания. 2021. № 12-2. С. 19-23.
5. Израйлов К.Е., Татарникова И.М. Подход к анализу безопасности программного кода с позиции его формы и содержания // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2019): сборник научных статей VIII Международной научно-технической и научно-методической конференции (Санкт-Петербург, 27-28 февраля 2019 г.). 2019. С. 462-467.
6. Красов А.В., Гельфанд А.М., Коржик В.И., Котенко И.В., Петрив Р.Б., Сахаров Д.В., Ушаков И.А., Шариков П.И., Юркин Д.В. Построение доверенной вычислительной среды: учебное пособие. СПб: Индивидуальный предприниматель Петрив Роман Богданович, 2019. 108 с.
7. Никулин В.В. Безопасность Windows и Windows defender // Вестник образовательного консорциума Среднерусский университет. Информационные технологии. 2021. № 2 (18). С. 7-13.
8. Лаврова Д.С., Попова Е.А., Штыркина А.А., Штеренберг С.И. Предупреждение dos-атак путем прогнозирования значений корреляционных параметров сетевого трафика // Проблемы информационной безопасности. Компьютерные системы. 2018. № 3. С. 70-77.
9. Кушнир Д.В., Шемякин С.Н., Исследование возможных методов аутентификации согласования данных в классическом канале в протоколах квантовой криптографии // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 4. С. 63-67.

Elizarova L., Izrailov K.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Classification of information security areas using categorical division.

Ensuring information security is an urgent task of the modern world. For this, in particular, it is necessary to correctly identify the relevant areas in this area. The article proposes the author's classes of information security areas obtained by using the apparatus of categorical division. Examples of sphere entities for each of the classes are given.

Key words: information security, categorical division, classification.

УДК 004.056.53
ГРНТИ 49.33.35

ПРИНЦИП ОРГАНИЗАЦИИ ЗАЩИТЫ ПОЛЬЗОВАТЕЛЬСКИХ ТЕРМИНАЛОВ ОТ АТАКИ ТИПА MAC-SPOOFING

Г. Ю. Емельяненко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современное развитие телекоммуникационных технологий сегодняшнего дня находится на высоком уровне, в связи с этим необходимо обращать внимание на борьбу с угрозами, исходящими как от внешнего, так и от внутреннего нарушителя. Для решения проблемы противодействия одной из угроз, при помощи которой внутренний нарушитель может успешно реализовать инцидент информационной безопасности, в рамках данной статьи будет рассмотрено применение технологии Cisco port security.

Cisco port security, корпоративная сеть, MAC-spoofing, ARP таблица, трафик

Сегодня информационные технологии достигли широкого развития и распространяются повсеместно на все отрасли жизни и деятельности человечества. Обработка информации при помощи персональных электронно-вычислительных машин носит повсеместный характер, и как следствие, возникает проблема защиты этой информации от различных атак и угроз. На сегодняшний день существует множество методов и средств защиты информации, в основном они направлены на защиту от нелегитимных действий нарушителя, располагающегося за пределами периметра корпоративной вычислительной сети (внешнего нарушителя), но существует и вероятность реализации угроз, исходящих от внутреннего нарушителя, обладающего определенными правами и решившего по своим мотивам реализовать угрозу информационной безопасности.

Одним из способов, который может стать инструментом для реализации атаки внутренним нарушителем является атака типа MAC-spoofing. Это атака, при которой злоумышленник выдает себя за целевой хост, используя его MAC-адрес. Таким образом, кадры, предназначенные для целевого хоста, попадают на хост злоумышленника.

Для выполнения атаки требуется узнать MAC цели, после чего установить такой же на сетевом интерфейсе нарушителя. Идея данной атаки заключается в том, что при смене уникального MAC адреса с одного порта на другой коммутатор идентифицирует, как верный, только адрес, подключенный по времени последним. Соответственно, если злоумышленник узнает MAC адрес жертвы и заменит его на своем интерфейсе, при этом они будут подключены к одному и тому же коммутатору, вычислительная машина жертвы будет изолирована от информационного обмена.

Для того, чтобы нарушитель со своего узла узнал MAC адрес жертвы, для он, зная IP адрес узла жертвы пользуется утилитой «Ping» и получает ответ от жертвы, в котором содержится IP адрес узла жертвы, а также MAC адрес данного

узла. Принцип вычисления MAC адреса жертвы по ARP таблице после выполнения команды «Ping» приведен на рис. 1.

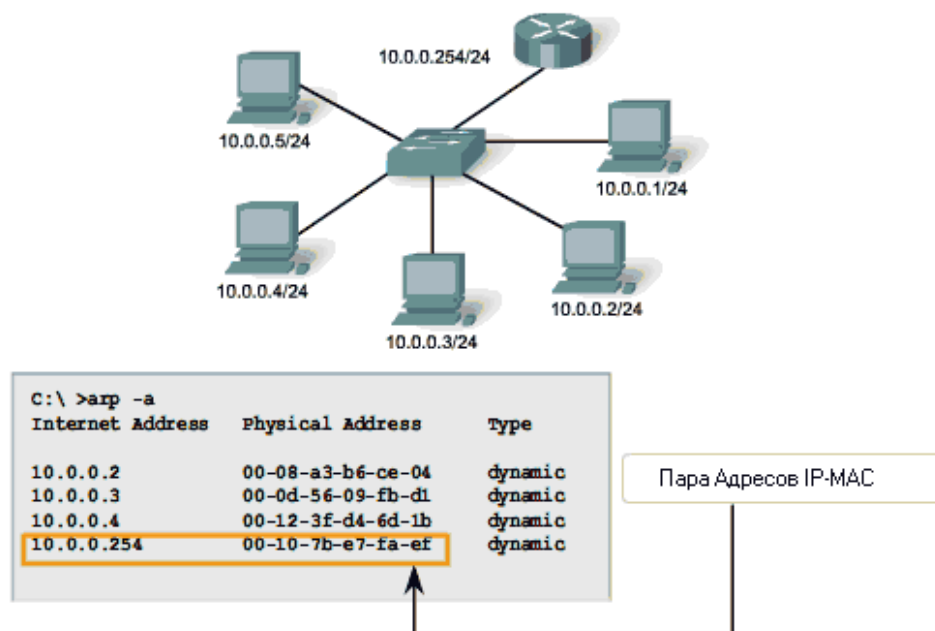


Рис. 1. Принцип вычисления MAC адреса узла жертвы нарушителем для подмены

В рамках настоящего исследования необходимо провести эксперимент. Для этого в программном симуляторе корпоративных сетей Cisco packet tracer будет построена схема простейшей корпоративной сети, приведенная на рис. 2.

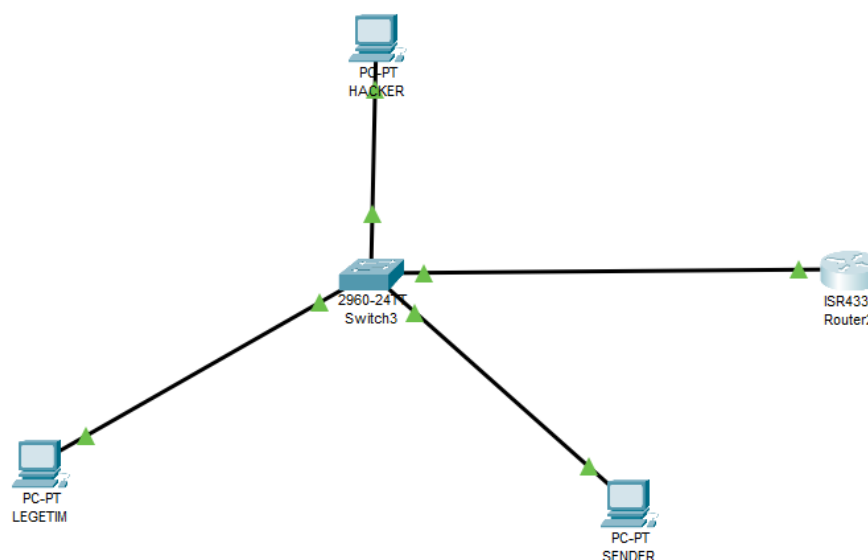


Рис. 2. Собранная схема корпоративной сети для проведения эксперимента

На данном этапе можно однозначно говорить, что для эксперимента сегмент сети настроен и все узлы функционируют штатно, соответственно трафик идет

на все эти адреса, так как распределение потоков трафика на канальном уровне осуществляет коммутатор, анализируя MAC адреса.

После этого злоумышленник, зная MAC адрес жертвы, меняет свой адрес на адрес жертвы, тем самым направляя весь трафик, который предназначен жертве, на себя. Процесс подмены MAC адреса приведен на рис. 3.

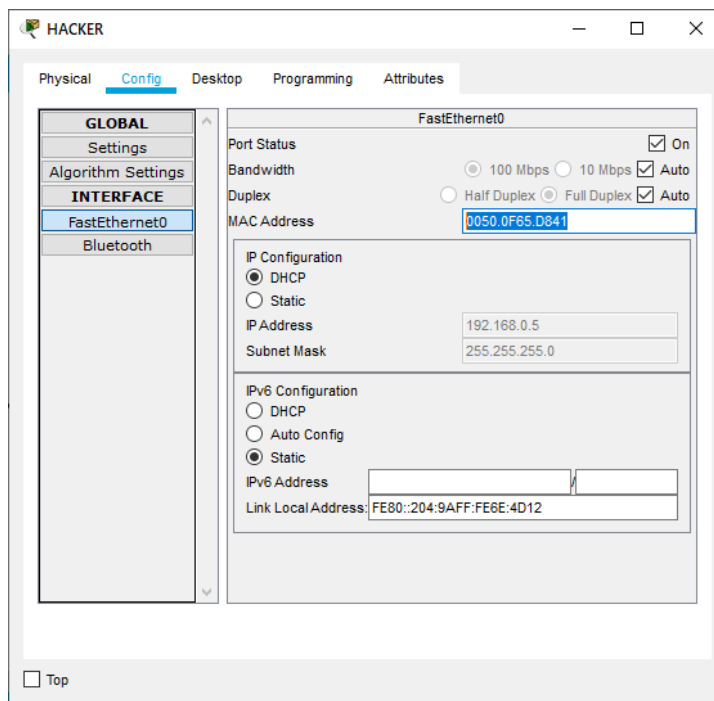


Рис. 3. Процесс подмены MAC адреса нарушителем на своем узле

Теперь выполняется попытка проверить доступность всех узлов при использовании утилиты «Ping» все компьютеры с маршрутизатора. Компьютер жертвы находится в сети, но на тестовые пакеты утилиты он не отвечает, так как все пакеты уходят на компьютер злоумышленника. То же самое произойдет с любым другим трафиком любого протокола, так как именно на канальном уровне решается вопрос доставки трафика до конкретного узла.

Существует достаточно простое решение, которое необходимо внедрить для защиты от подобной атаки. В оборудовании Cisco это решение носит название «Cisco port security», его настройка будет произведена в рамках настоящего исследования. Данное решение позволяет защищаться от атак, реализуемых по принципу MAC Spoofing.

Настройки Cisco port security приведены ниже.

```
Switch(config)#interface range f0/2-4
```

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#switchport port-security
```

```
Switch(config-if-range)#switchport port-security mac-address sticky
```

После этого необходимо симитировать подмену MAC адреса на компьютере хакера, поставив MAC адрес компьютера жертвы. В результате порт немедленно уходит в состояние административного выключения, так как mac-

address sticky является конструкцией, которая разрешает только один MAC адрес, который первый был подключен к порту коммутатора.

Результат блокировки порта приведен на рис. 4.

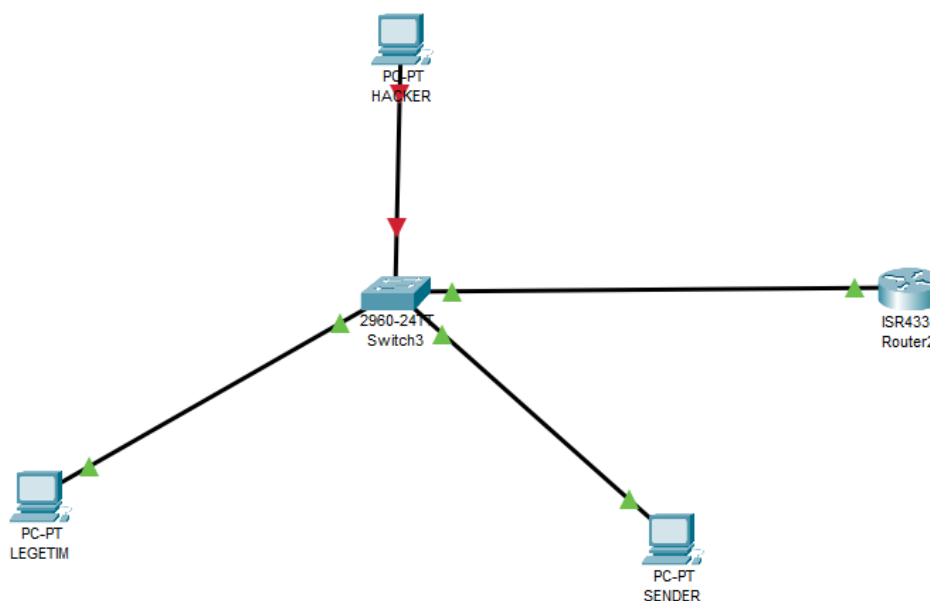


Рис. 4. Процесс подмены MAC адреса нарушителем на своем узле

В результате исследования можно сделать вывод, что оказавшись в корпоративной сети завербованным, легитимный пользователь легко превращается в злоумышленника, способного перехватывать и, впоследствии, анализировать трафик жертвы, в роли которой может выступать любой легитимный пользователь. Простая, но в то же время реально работающая технология «port security» способна эффективно противостоять этому.

Список используемых источников:

1. Хилл Б. Полный справочник по Cisco: [Электронный ресурс] // Издательский дом "Вильямс". М., 1992-2019. URL: <https://www.williamspublishing.com/Books/5-8459-0589-3.html> (Дата обращения 25.10.2022)
2. Подмена MAC адресации: [Электронный ресурс] // SPY-SOFT.NET. 2010-2022. URL: <https://spy-soft.net/mac-starvation-mac-spoofing/> (Дата обращения 27.10.2022)
4. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: [Электронный ресурс] // Издательский дом «Питер». СПб., 2022. URL: <https://www.piter.com/collection/top-prodazh/product/kompyuternye-seti-printsipy-tehnologii-protokoly-yubileynoe-izdanie> (Дата обращения 24.10.2022)
5. Протокол ARP: [Электронный ресурс] // Microsoft Learn. 2022. URL: <https://learn.microsoft.com/ru-ru/windows-server/networking/technologies/dhcp/dhcp-top> (Дата обращения 23.10.2022)
6. Уэнделл Одом. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101: [Электронный ресурс] // Издательский дом "Вильямс". М., 1992-2019. URL: <https://www.williamspublishing.com/Books/978-5-8459-1906-9.html> (Дата обращения 25.10.2022)

7. Что такое MAC Spoofing: [Электронный ресурс] // Timeweb.com. 2006-2022. URL: <https://timeweb.com/ru/community/articles/что-такое-dhcp-protokol> (Дата обращения 25.10.2022)

Emelyanenko G.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Principle of organizing protection of user terminals against MAC-spoofing attack.

The modern development of telecommunication technologies today is at a high level, in this regard, it is necessary to pay attention to the fight against threats emanating from both external and internal intruders. To solve the problem of countering one of the threats, with the help of which an insider can successfully implement an information security incident, this article will consider the use of Cisco port security technology.

Key words: Cisco port security, corporate network, MAC-spoofing, ARP table, traffic.

УДК 004.056.53
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ПРЕДОТВРАЩЕНИЯ DDOS АТАК НА МАРШРУТИЗАТОРЕ ELTEX ESR200

Ю. А. Иванилова, В. А. Кравцова, И. А. Ушаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются виды DDoS атак и методы их предотвращения. Приведены результаты реализации защиты от DDoS атак.

атака DDoS, HTTP-flood, SYN-flood, GRE-flood, ICMP-flood, Smurf-атака

Каждый день тысячи устройств подвергаются кибератакам. Один из видов таких атак – распределенная атака типа «отказ в обслуживании» (DDoS). Результатом этого метода является ограничение доступности ресурсов для легитимных пользователей, вследствие загруженности канала передачи данных бесполезным трафиком. В отличие от DOS атаки, распределенная атака предполагает заблаговременное заражение устройств, для сбора их в ботнет, который будет осуществлять нападение на ресурс в заданное время. DDoS-атаки занимают второе место по популярности среди киберпреступных услуг, продаваемых в мессенджере Телеграм. Одна из крупнейших атак «Mantis» реализовала скорость 26 млн запросов в секунду.

На рис. 1 представлены самые популярные типы DDoS-атак, согласно статистике Лаборатории Касперского.

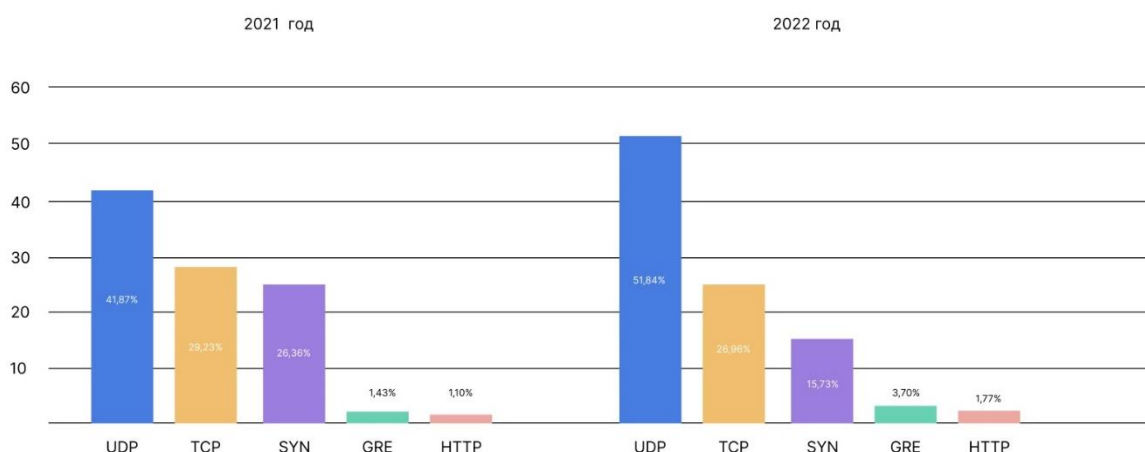


Рис. 1. Распределение DDoS-атак по типам, 2021/2022 год

Их можно разделить на 2 вида:

1. Атаки низкого уровня (сетевой и транспортный уровни OSI). Среди них выделяют:

- ICMP-flood. Использует утилиту ping, проверяющую доступность устройства в сети, отправляя на него эхо-запрос и получая эхо-ответ.

Злоумышленник перегружает целевое устройство ICMP-запросами. Один из методов реализации флуда – использовать минимальное время между отправкой ICMP-пакетов, что приводит к загруженности устройства.

- GRE-flood. Атака осуществляется путем отправки инкапсулированного пакета большого размера, при деинкапсуляции которого жертва получает полезную нагрузку, исчерпывающую ее ресурсы. Для выполнения атаки злоумышленнику необходимо использовать реальные устройства, так как источник пакетов GRE невозможно подделать.

- UDP-flood. Во время атаки жертва получает UDP пакеты одновременно от множества IP-адресов, что приводит к переполнению сервера ненужными UDP запросами.

- SYN-flood. Протокол TCP для установления сеанса связи использует syn-запросы, без ответа на которые невозможно обеспечить гарантированную доставку пакетов. Атакующий может отправить множество syn-запросов, загрузив сервер полуоткрытыми соединениями, так как указанный обратный адрес будет не действующим [1].

2. Атаки высокого уровня (прикладной уровень OSI).

-HTTP-flood. Атакующий отправляет запросы (GET,POST) небольшого размера, которые требуют ответы в пакетах большего объема, что вызывает заполнение полосы пропускания и отказ работы сервисов.

-NTP Используется для усиления DDoS атаки на жертву путем отправки NTP-серверу запросов get monlist, на которые он должен отправить 600 последних IP-адресов, подключенных к серверу. Также может быть реализовано множество запросов к NTP-серверу, с которыми он не сможет справиться, что приведет к отказу в обслуживании.

-DNS. К DNS-серверам формируется короткий запрос, а ответ отправляется на адрес жертвы и во много раз превосходит запрос[2].

В рамках противодействия DDoS атакам рассматриваются методы предотвращения и обнаружения. Главная цель предотвращения атаки – остановить ее до момента нанесения ущерба. Для этого может быть использована фильтрация входящего трафика - незаконным пакетам отказывается в доступе. Использование протоколов Save и HCF позволяет установить достоверность исходного IP адреса пакета и, на основании таблицы хопов, определить несоответствие ожидаемому количеству переходов и реальному[3].

Главной задачей обнаружения атаки является своевременное ее выявление. Для этого можно использовать метод Детектирования атак с помощью математических моделей. Так как модель может адаптироваться к постепенно наращиваемой нагрузке во время DDoS атаки, может быть использован аппарат нечеткой логики и нейронных сетей. Нейронная сеть может обучаться в процессе существования, поэтому она может выступать в качестве инструмента прогнозирования DDoS-атаки. Различают многослойные прямые нейронные сети и самоорганизующиеся карты Кохонена. Нейронная сеть способна определить новую атаку по неизвестным закономерностям [4].

В отличие от этого, сигнатурный метод заключается в быстром определении уже известных атак. Это достигается благодаря распознаванию глубоких взаимосвязей элементов системы. Одним из источников сигнатур являются матрицы MITRE ATT&CK, содержащие сотни вариантов развития событий.

Следующий метод детектирования атак основан на аномалиях и предполагает создание базового профиля сетевого поведения, который будет отражать нормальную пользовательскую активность в системе. Этот метод требует большого количества заранее собранных статистических данных.

Высокую эффективность показывает метод обнаружения DDoS-атаки с помощью SIEM-системы. Есть два варианта реализации: с помощью случайно сгенерированных captcha или выполнения блокирующего bash-скрипта, при превышении разрешенных запросов с одного IP-адреса [5].

Для защиты от DDoS-атаки в первую очередь необходимо осуществить настройку правил межсетевого экрана [6]. Файрвол запускается локально внутри маршрутизатора и блокирует атаку, что представлено на рис. 2.

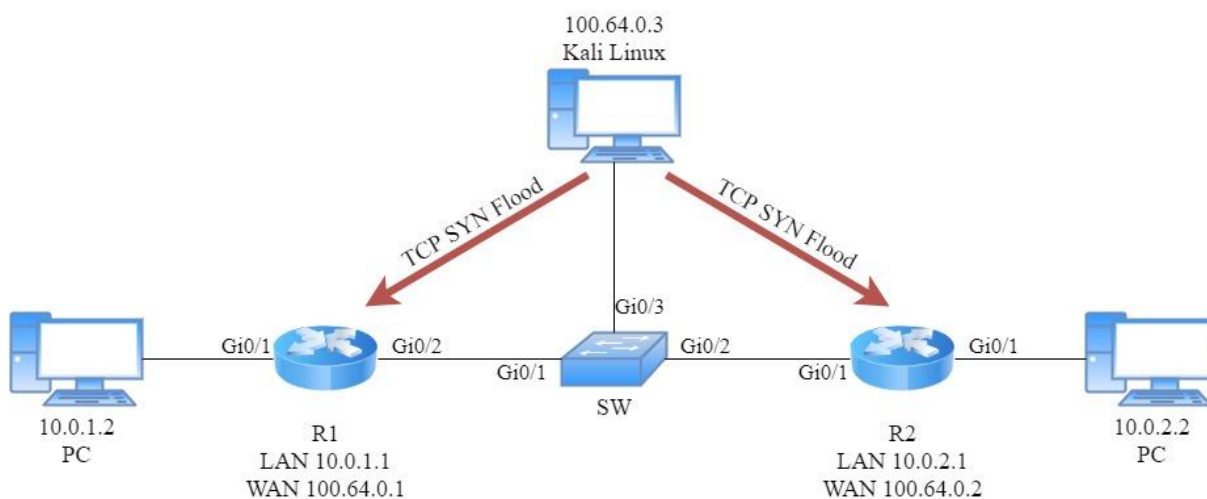


Рис. 2. Топология сети

Первыми настраиваются локальные и глобальные зоны безопасности, принадлежность интерфейсов к зонам. Затем списки IP-адресов, номеров портов и т.д.; взаимодействие между зонами безопасности для пропуска трафика из зоны LAN в зону WAN; настройка правил.

Настройка оборудования подразумевает создание следующих правил [7].

```
ip firewall screen dos-defence syn-threshold 10
ip firewall screen dos-defence land
ip firewall screen dos-defence winnuke
ip firewall screen spy-blocking icmp-type <ICMP_TYPE>
<ICMP_TYPE> – тип icmp, принимает значения:
– destination-unreachable
– echo-request
– reserved
– source-quench
– time-exceeded
ip firewall screen spy-blocking ip-sweep 10 5000
ip firewall screen spy-blocking port-scan 10 15000
ip firewall screen spy-blocking spoofing
```

При проведении настройки файервола Eltex, была обнаружена возможность осуществления TCP-SYN Flood-атаки с виртуальной машины KALI Linux посредством утилиты hping3 и подмены IP-адреса на легитимный, использующийся внутри сети. Тогда, файервол не разрывает сессию и отображает её в панели. При изменении IP-адреса на нелегитимный, сессия не была создана. Эту уязвимость сети можно исправить благодаря функции контроля динамических ARP. Она позволяет проверять легитимность пакетов в соответствии с базой данных легитимных IP и MAC-адресов.

Заявление о финансировании:

Проект реализуется победителем грантового конкурса для преподавателей магистратуры 2021/2022 Стипендиальной программы Владимира Потанина.

Список используемых источников:

1. Катасонов, А. И. Эффективность встроенной защиты Microsoft Windows server от DDOS-атак на основе TCP syn / А. И. Катасонов, А. В. Красов, А. Ю. Цветков // Сборник статей Круглого стола «Безопасность в профессиональной деятельности», в рамках II Всероссийской научно-практической конференции «Инновационные технологии и вопросы обеспечения безопасности реальной экономики» ITES-2020, СПб, 27.03.2020. – СПб: СПбГЭУ, 2020. – С. 68-78.
2. Ушаков, И. А. Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных : специальность 05.13.19 "Методы и системы защиты информации, информационная безопасность" : диссертация на соискание ученой степени кандидата технических наук / Ушаков Игорь Александрович. – Санкт-Петербург, 2020. – 215 с.
3. Zeb K., Baig O., Asif M.K. DDoS Attacks and Countermeasures in Cyberspace. // IEEE 2nd World Symposium on Web Applications and Networking (WSWAN). – 2015. – Mar. – P.1-6.
4. Довгаль, В. А. Анализ уязвимостей и угроз безопасности роя дронов с поддержкой Wi-Fi, противостоящего атакам злоумышленников / В. А. Довгаль, Д. В. Довгаль // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2020. – № 3(266). – С. 67-73.

5. Котенко, И. В. Технологии больших данных для мониторинга компьютерной безопасности / И. В. Котенко, И. А. Ушаков // Защита информации. Инсайд. – 2017. – № 3(75). – С. 23-33.

6. Масштабируемое Honeypot-решение для обеспечения безопасности в корпоративных сетях / А. В. Красов, Р. Б. Петрив, Д. В. Сахаров, Н.Л. Сторожук, И.А. Ушаков // Труды учебных заведений связи. – 2019. – Т. 5. – № 3. – С. 86-97. – DOI 10.31854/1813-324X-2019-5-3-86-97.

7. Управление логированием и защитой от сетевых атак // docs.eltex-co URL: <https://docs.eltex-co.ru/pages/viewpage.action?pageId=108069779> (дата обращения: 15.10.2022).

Ivanilova Y., Kravtsova V., Ushakov I.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Study of mechanisms to prevent DDoS-attacks on the router Eltex ESR200.

The article discusses the types of DDoS attacks and methods for their prevention. The results of the implementation of protection against DDoS attacks are given.

Key words: DDoS-attack, HTTP-flood, SYN-flood, GRE-flood, ICMP-flood, Smurf-attack.

УДК 004.056.53
ГРНТИ 49.33.35

РАЗРАБОТКА PLAYBOOK ANSIBLE ДЛЯ МОДУЛЯ ОБНАРУЖЕНИЯ НЕЛЕГИТИМНЫХ ТОЧЕК ДОСТУПА СЕМЕЙСТВА IEEE 802.11 В ПРОВОДНОЙ КОРПОРАТИВНОЙ СЕТИ

Н. И. Казаков, Т. В. Петрова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире компании работают с большими объемами различных данных. Поэтому в жизни каждого предприятия немаловажную роль играет защита информации. Чтобы защитить сеть от построенного вмешательства, компании в зависимости от объёмов работы необходимо нанять одного или нескольких квалифицированных специалистов по безопасности. К сожалению, в настоящее время большой дефицит таких кадров, так как они очень востребованы. Вследствие чего начала повышаться потребность использования автоматизированных процессов, которые «самостоятельно» решают задачи, основанные на предопределённых правилах и шаблонах.

автоматизация, Ansible, безопасность, нелегитимная точка доступа

В компаниях по мере развития и увеличения размеров сети, настройка и управление традиционными ручными методами становятся более сложной. Возникает необходимость в автоматизации. С помощью автоматизации сетевых задач и функций, а также с помощью повторяющихся процессов с автоматическим контролем и управлением, повышается доступность сетевых служб. Благодаря автоматизации сети, увеличивается эффективность сети, уменьшаются эксплуатационные расходы, а также сокращается возможность возникновения ошибок, которые может совершить человек.

Автоматизация сети – это процесс автоматизации настройки, управления, тестирования, развертывания и эксплуатации физических и виртуальных устройств в сети [1, 2]. На данный момент решения для автоматизации сети позволяют выполнить большой ряд задач:

– Мониторинг сети и ее сервисов. Позволяет быстро реагировать на различные инциденты, исправлять и предотвращать их будущее появление.

– Управление конфигурацией устройств. Позволяет настраивать аналогичную конфигурацию на нескольких устройствах сразу, что значительно экономит время специалиста.

– Управление потреблением сетевых ресурсов пользователями и группами пользователей. Позволяет отслеживать и регулировать ресурсы, которые потребляют пользователи или группы пользователей, тем самым осуществляется поддержка уровня обслуживания клиентов.

– Планирование и проектирование сети. Позволяет планировать различные сценарии, управлять запасами.

– Сбор данных устройств, программного обеспечения (ПО), различных систем, сетей и прочего в реальном времени. Позволяет за пару действий собрать все нужные данные, что очень сильно экономит время по сравнению с тем, если

бы специалист заходил на каждое устройство в сети и собирал нужные ему данные ручным способом.

- Тестирование устройств. Позволяет производить различные тесты сразу на нескольких устройствах одновременно по определенному сценарию.

- Обновление ПО. Позволяет своевременно и одновременно обновить ПО на всех устройствах, находящихся внутри сети.

- Защита данных с помощью контроля доступа к сетевым устройствам и их ресурсам. Позволяет защищать данные в сети путем заранее установленной политики безопасности и уведомления администратора сети о попытке ее нарушения, а также путем настройки определенных сценариев, которые не будут позволять нелегитимным устройствам проникать в сеть.

На данный момент существует несколько способов защиты от нелегитимных точек доступа семейства IEEE 802.11 [3], часть из которых применяется в информационной безопасности, а часть имеет большой потенциал, но применяется не в полной мере или еще не изучена до конца. В исследовательской области не так много работ, связанных с автоматизированным обнаружением и отключением нелегитимных точек доступа семейства IEEE 802.11, а главное нет готовых модулей, которые могли бы осуществить это отключение без помощи человека [4, 5, 6]. Поэтому будет целесообразно разработать скрипт для модуля обнаружения нелегитимных точек доступа в проводной корпоративной сети.

Для разработки скрипта будет использована система автоматизации Ansible. Ansible – это система управления конфигурациями, использующая декларированный язык разметки для описания конфигураций [7, 8]. Для описания конфигураций используется `playbook`. `Playbook` – это описание состояния ресурсов системы, в котором она должна находиться в конкретный момент времени, включая установленные пакеты, запущенные службы, созданные файлы и многое другое. Вместо того, чтобы индивидуально использовать команды для удалённой настройки компьютеров из командной строки, можно настраивать целые сложные среды, передавая скрипт одной или нескольким системам.

Листинг `playbook` для модуля обнаружения нелегитимных точек доступа семейства IEEE 802.11 в проводной корпоративной сети показан на рис. 1. Работа данного скрипта направлена на выявление в проводной сети MAC-адресов нелегитимных устройств. Вначале с помощью протокола SNMP со всех коммутаторов в сети собирается информация об устройствах, подключённых к коммутаторам, и записывается в SQL-таблицу «switching» (таблица 1). Из вышестоящих систем заполняется SQL-таблица «verification» (таблица 2), в которую помещаются MAC-адреса точек доступа, находящихся на предприятии. Флаг «R» (Rogue) обозначает нелегитимную точку доступа, а флаг «V» (Verified) – легитимную. Поэтому из SQL-таблицы «verification» необходимо получить значения MAC-адресов устройств с флагом «R» и найти те же значения в SQL-таблице «switching». Если значения MAC-адресов в таблицах совпали, то можно сделать вывод о том, что MAC-адреса найденных устройств являются нелегитимными.

```

---
- hosts: localhost
  connection: local
  gather_facts: yes

tasks:
  - name: host
    debug: msg="{{ item }}"
    with_items:
      - "{{ groups['switch'] }}"

  - name: Get MAC address
    command: snmpwalk -v 2c -c pr_snmp -OXsq {{ item
}} \1.3.6.1.2.1.17.4.3.1.1
    with_items: "{{ groups['switch'] }}"
    register: oid1

  - set_fact:
    _tmp: "{{ _tmp|d([]) + [item|combine({'item':
items.split()})] }}"
    loop: "{{ oid1.results }}"
    vars:
      _count: "{{ item.stdout_lines|length }}"
      _item: "{{ item.item }}"
      _items: "{{ _item * _count|int }}"

  - set_fact:
    result: "{{ _tmp }}"

- name: Result
  debug:

var: result| map(attribute='stdout_lines')

- name: MAC address (sql)
  debug:
    var: sql.query_result.0|map(attribute='macadd')

- name: OID MAC
  debug:
    var: oid1.results|map(attribute='stdout_lines')

- set_fact:
  mac: "{{ oid1.results|map(attribute='stdout_lines')|
flatten|
map('regex_replace', _regex, _replace)|
map('trim')|
map('split')|
map('join', ':')|
list }}"

- name: IP
  debug:
    var: oid1.results|map(attribute='item')

- set_fact:
  mac_rogue: "{{
mac|intersect(sql.query_result.0|map(attribute='macadd')
)}}"

- name: MAC address (rogue)
  debug:
    var: mac_rogue

- set_fact:
  mac_sql: "{{ result | map(attribute='stdout_lines') |
flatten }}"

- set_fact:
  ip_sql: "{{ result | map(attribute='item') | flatten }}"

- name: Writing to the table "switching"
  community.mysql.mysql_query:
    login_db: cisco
    query: "INSERT INTO switching(ipadd, oid_mac,
port_index) VALUES ('{{ item.0 }}', '{{ item.1 }}')"
  with_together:
    - "{{ ip_sql }}"
    - "{{ mac }}"

- name: Get mac from table "verification" (SQL)
  community.mysql.mysql_query:
    login_db: cisco
    query: "SELECT macadd FROM verification WHERE
flag=R"
  register: sql
  
```

Рис. 1. Листинг playbook

ТАБЛИЦА 1. Пример заполнения SQL-таблицы «switching»

ipadd	mac
192.168.176.143	00:50:79:66:68:03
192.168.176.144	00:50:79:66:68:04
192.168.176.140	00:50:79:66:68:05
192.168.176.141	00:50:79:66:68:06
192.168.176.147	00:50:79:66:68:08
192.168.176.142	00:50:79:66:68:07

ТАБЛИЦА 2. Пример заполнения SQL-таблицы «verification»

name	ipadd	macadd	flag
ubuntu	192.168.176.128	00:0c:29:dc:5b:c2	V
unknown	-	00:50:79:66:68:04	R
unknown	-	00:50:79:66:68:06	R

Результатом данной работы является разработанный скрипт для модуля обнаружения нелегитимных устройств в проводной сети, который автоматически обнаруживает беспроводное нелегитимное устройство в корпоративной сети с помощью таблицы коммутации и протокола SNMP. Данное решение позволяет автоматически обнаруживать нелегитимную точку доступа, которая подключена к коммутатору, что позволяет уменьшить вероятность взлома корпоративной сети. Работа playbook была проверена экспериментально на виртуальных устройствах и физическом оборудовании.

Список используемых источников:

1. Что такое автоматизация сети? Juniper Network: [Электронный ресурс] // Juniper.net. 2022. URL: <https://www.juniper.net/ru/ru/research-topics/what-is-network-automation.html> (Дата обращения 13.09.2022)

2. Что такое автоматизация сети?: [Электронный ресурс] // Cisco.com. 2022. URL: https://www.cisco.com/c/ru_ru/solutions/automation/network-automation.html#~:text=Путь%20к%20автоматизации (Дата обращения 13.05.2022)
3. Александрова Е. С., Ковцур М. М. Разработка модели нарушителя в беспроводных сетях стандарта IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VI Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 01-02 марта 2017 г. СПб. : СПбГУТ, 2017. Т. 2. С. 24–28.
4. Красов А. В., Петрив Р. Б., Сахаров Д. В., Сторожук Н. Л., Ушаков И. А. Масштабируемое Honeypot-решение для обеспечения безопасности в корпоративных сетях // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 86-97.
5. Миняев А. А., Третьяков И. В. Автоматизированная система контроля сетевого доступа в инфокоммуникационной среде // Международная конференция по мягким вычислениям и измерениям. 2009. Т. 1. С. 215-217.
6. Ковцур М. М., Герлинг Е. Ю., Коновалова В. В., Киструга А. Ю. Исследование способов удаленного перехвата трафика в корпоративных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 4. С. 68-75.
7. Красов А. В., Косов Н. А., Холоденко В. Ю. Исследование методов провизионинга безопасной сети на мультивендорном оборудовании с использованием средств автоматизированной конфигурации // Colloquium-journal. 2019. № 13-2 (37). С. 243-247.
8. Ansible: [Электронный ресурс]. URL: <https://docs.ansible.com/ansible/latest/index.html> (Дата обращения 15.09.2022)

Petrova T., Kazakov N.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Development of Ansible playbook for the IEEE 802.11 family of rogue access points detection module in a wired corporate network.

In today's world, companies work with large volumes of different data. Therefore, information protection plays an important role in the life of every company. To protect the network from the interference built, the company, depending on the amount of work needs to hire one or more qualified security specialists. Unfortunately, nowadays there is a big deficit of such specialists, as they are in great demand. As a consequence, the need to use automated processes that "independently" solve problems based on predefined rules and templates has begun to increase.

Key words: *automation, Ansible, security, rogue access point.*

УДК 004.057.5
ГРНТИ 20.53.23

ИССЛЕДОВАНИЕ БЕЗОПАСНОГО РАЗВЁРТЫВАНИЯ ВЕБ-ПРИЛОЖЕНИЯ В ОБЛАЧНОЙ ИНФРАСТРУКТУРЕ

И. А. Ковалев, А. Э. Фёдорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В связи с современными тенденциями развития в мире информационных технологий инженеры и архитекторы, обеспечивающие работу веб-приложений, были вынуждены отойти от традиционного развёртывания инфраструктуры на физических серверах из-за ряда недостатков, которые исходят в данном случае из невозможности контролировать распределения ресурсов. Для решения проблемы контроля ресурсов, масштабируемости и обработки ошибок стал использоваться Kubernetes.

оркестрация контейнеров; облачные технологии; kubernetes; terraform; веб-приложения

В производственной среде необходимо управлять контейнерами, которые запускают приложения, и гарантировать отсутствие простоев. Например, если контейнер выходит из строя [1], необходимо запустить другой контейнер.

Kubernetes — это портативная расширяемая платформа с открытым исходным кодом для управления контейнеризованными рабочими нагрузками и сервисами, которая облегчает как декларативную настройку, так и автоматизацию. У платформы есть большая, быстро растущая экосистема. Сервисы, поддержка и инструменты Kubernetes широко доступны.

Для дальнейших действий необходимы следующие инструменты:

- kubectl;
- yc;
- terraform.

В связи с быстрым ростом [2] актуальности импортозамещения и отсутствием альтернатив, было принято решение разворачивать инфраструктуру на инфраструктуре провайдера Яндекс.

После успешной инсталляции клиента потребуется небольшая настройка.

Для обращения к кластеру kubernetes необходим консольный клиент kubectl.

Для обращения к облачному провайдеру и автоматизированному созданию ресурсов в каталоге облака существует решение под названием Terraform. Это утилита, призванная упростить и автоматизировать принцип Infrastructure as a Code (IaaS) – Инфраструктура как Код, что отражает концепцию современных проектов в сфере информационных технологий. Terraform позволяет быстро создать облачную инфраструктуру в Yandex Cloud и управлять ею с помощью

файлов конфигураций. В файлах конфигураций хранится описание инфраструктуры на языке HCL (HashiCorp Configuration Language). Terraform и его провайдеры распространяются под лицензией Mozilla Public License.

При изменении файлов конфигураций Terraform автоматически определяет, какая часть вашей конфигурации уже развернута, что следует добавить или удалить.

В командной строке необходимо перейти в каталог, в котором создан конфигурационный файл.

Если конфигурация описана верно, в терминале отобразится список создаваемых ресурсов и их параметров. Если в конфигурации есть ошибки, Terraform на них укажет. Это проверочный этап: ресурсы не будут созданы.

Для получения файла контекста kubernetes необходимо сгенерировать его и подписать. Далее можем подключаться к кластеру, проверив подключение.

В данном ресурсе имеются настройки безопасности, например, настройка сервисного аккаунта (Service Account) – ресурса, позволяющего управлять и разграничивать доступ отдельных пользователей, к которому привязывается такой аккаунт, к использованию ресурсов и управлением кластером kubernetes. Реализована возможность назначения нескольких категорий прав доступа, таких как list, read, write, delete и другие.

Также в приведенном примере [3] проиллюстрировано управление ID внутреннего пользователя в контейнере для ограничение такого опасного вида атак как эскалация привилегий (Privilege Escalation). Ниже более подробно рассматривается безопасность в системе Kubernetes.

Kubernetes поддерживает такие базовые принципы как обеспечение контроля доступа на основе ролей, но не имеет возможностей для защиты приложений от уязвимостей. Для этого придется использовать дополнительные программы или системы безопасности от сторонних вендоров. Для защиты контейнеров в Kubernetes нужно обратить внимание на следующее:

- конфигурации по умолчанию;
- среда выполнения;
- образы контейнеров;
- безопасность хостов;
- взаимодействие между подами.

Один из аспектов, который при обеспечении безопасности необходимо учитывать в первую очередь, – это конфигурации по умолчанию. Перед использованием их нужно проверять, чтобы свести к минимуму риск того, что атака на один из подов может распространиться на другие.

Хотя в Kubernetes есть некоторые защитные средства для контроля доступа, большинство из них по умолчанию не активированы. Кроме того, их настройки могут не включать в себя принцип наименьших привилегий, поэтому

пользователи могут получить полные права доступа к информации, которая им не требуется для дела. Из-за этого появляется вероятность того, что к конфиденциальной информации могут получить доступ злоумышленники.

Среда выполнения – это специальное программное обеспечение, благодаря которому работают контейнеры. Kubernetes не предоставляет средств для защиты от атак на среду выполнения или для обнаружения вторжений.

Если в работающем контейнере [4] обнаружится уязвимость или он будет взломан, придется окончательно его остановить и заново запустить неskomпрометируемую версию этого контейнера. Информацию, которую использовали для устранения первопричин этой угрозы, также следует использовать и для исправления ошибок конфигурации компонента в рассматриваемой среде.

Образы также могут стать источником рисков безопасности. При неправильной конфигурации они оказываются удобной отправной точкой для проникновения в сеть, а если в образах есть ключи для аутентификации, злоумышленники могут воспользоваться ими в последующих атаках.

Чтобы обнаружить вредоносный код внутри образа, необходимо сканировать на уязвимости образы в реестре контейнеров и в среде эксплуатации. В Kubernetes такой функции нет.

Kubernetes выполняет [5] контейнеры на тех серверах, которые ему предоставлены. Поскольку он не может защитить сами серверы, необходимо обеспечивать их безопасность другими способами.

Многие компании используют традиционные средства защиты для обнаружения подозрительного использования ресурсов систем, однако при компрометации хостов последствия могут быть намного серьезнее. Для предотвращения атак необходимо осуществлять мониторинг на наличие утечек и потенциально опасную активность.

По умолчанию Kubernetes не применяет сетевые политики к каждому отдельному поду, а это означает, что поды в среде Kubernetes могут взаимодействовать друг с другом. Взаимодействие контейнеров и подов выгодно для правильного функционирования в рамках развертывания. Однако это может стать лазейкой для киберпреступников, которым достаточно взломать один контейнер, чтобы затем атака распространилась внутри среды.

Применение сетевой политики к отдельному поду ограничивает его связь с определенными [6] ресурсами, что похоже на применение правил межсетевого экрана и защитных средств.

Таким образом, из-за популярности Kubernetes крайне важно предпринять меры по предотвращению взломов и атак, направленных на эту платформу. Интеграция защитных средств в каждый этап жизненного цикла контейнеров позволит компаниям быть уверенными в своей безопасности.

Утилита `kubectl` сканирует директорию на наличие файлов разметки `json`, удовлетворяющим требованиям ресурсов `kubernetes`, после чего обращается к созданному кластеру, указанному в контексте `kube-config` и начинает развёртывание приложения, после которого все указанные в директории ресурсы отображаются в кластере. Также в `kubernetes` реализована возможность удобно и быстро посмотреть, что развёрнуто в системе на данный момент времени [7].

В настоящей статье был описан современный способ развёртывания инфраструктуры для веб-приложения в облачной среде с использованием фреймворка `Kubernetes`, что позволило убедиться в таких преимуществах системы оркестрации контейнеров как удобство, декларативная структура, оптимизированная утилизация ЦПУ и RAM, ролевая система управления доступом для обеспечения безопасности и возможность автоматизированного использования в процессах CI/CD.

Список используемых источников:

1. Александрова Е. С., Ковцур М. М. Разработка модели нарушителя в беспроводных сетях стандарта IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VI Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 01-02 марта 2017 г. СПб. : СПбГУТ, 2017. С. 24-28.

2. Александрова Е. С., Иванов Г. Н., Ковцур М. М. Анализ механизмов защиты WI-FI сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VII Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 28 февр.-01 марта 2018 г. СПб. : СПбГУТ, 2018. С. 47-51.

3. Габуев А. Г., Красов А. В., Оценков Ф. Д., Тарасов Н. М. Анализ защищённости современных средств передачи информации посредством портативной лаборатории на основе микрокомпьютера Raspberry Pi // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы IX Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 26-27 февр. 2020 г. СПб. : СПбГУТ, 2020. С. 295-298.

4. Завражнова М. В., Родкина Э. А., Шошина А. В. Разработка базы данных и веб-интерфейса научной электронной библиотеки // Colloquium-journal. 2019. N 19-1 (43). С. 31-34.

5. Ахрамева К. А., Ковцур М. М., Михайлова А. В. Обеспечение информационной безопасности баз данных web-приложений // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы IX Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 26-27 февр. 2020 г. СПб. : СПбГУТ, 2020. С. 107-110.

6. Ковцур М. М., Луеке П. Э. Разработка системы учёта посещаемости студентов масштаба ВУЗа // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VIII Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 27-28 февр. 2019 г. СПб. : СПбГУТ, 2019. С. 532-537.

7. Герлинг Е. Ю., Горлов С. Е., Кириллов Д. И. Обеспечение информационной безопасности при разработке web-приложений // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы IX Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 26-27 февр. 2020 г. СПб. : СПбГУТ, 2020. С. 326-330.

Kovolev I., Fedorova A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Research of secure deployment of web application in cloud infrastructure

Due to forward-looking development trends in the information technology world, engineers and architects who provide web applications have been forced to move away from statistical deployments to physical databases due to a number of disadvantages that come with the use case due to the inability to control the allocation of resources. To solve the problems of resource control, scalability and error handling, Russian Kubernetes has become.

Key words: container orchestration; cloud technologies; kubernetes; terraform; web applications.

УДК 004.056
ГРНТИ 81.93.29

ВНУТРЕННИЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОРГАНИЗАЦИИ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ

Р. К. Коломийцев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Благополучие организации напрямую связано с честностью ее работников. Однако организации также угрожает злоупотребление информацией со стороны ее агентов, таких как бывшие и нынешние сотрудники, поставщики или деловые партнеры. Такого рода угрозы, исходящие изнутри организации, известны как инсайдерские угрозы. Для их выявления в организациях используется множество подходов. Одним из таких подходов является использование технологий обмана. Этот метод дополняет существующие системы обнаружения инсайдерской информации, улучшает их производительность с точки зрения уменьшения ложноположительных результатов, а также позволяет выявить инсайдеров на стадии намерений.

внутренние угрозы, инсайдеры, технологии обмана, кибербезопасность

Самыми уязвимыми местами в безопасности системы являются люди, которые работают в защищенных сетях с авторизацией. Они могут представлять опасность для компании, если намеренно или непреднамеренно повредят сетевую инфраструктуру или украдут важную информацию. Кевин Митник утверждает, что компании тратят миллионы долларов на брандмауэры, шифрование и устройства защищенного доступа, и эти деньги тратятся впустую, потому что ни одна из этих мер не направлена на самое слабое звено в цепочке безопасности [1]. Это дает полное представление о ситуации, с которой сталкиваются профессионалы в области сетевой безопасности в наши дни.

Влияние внутренних угроз на безопасность организации.

Когда дело доходит до угроз безопасности компаний и борьбы с утечками данных, всеобщей огласке придаются внешние угрозы, они привлекают к себе гораздо больше внимания, чем внутренние угрозы, при этом, число последних из-за злонамеренных или непреднамеренных действий сотрудников растет с каждым годом (53% в 2018 году, 60% в 2020 году, 67% в 2022 году) [2]. Подавляющее большинство организаций (90%) чувствуют себя уязвимыми перед внутренними атаками, а 83% хотя бы раз столкнулись с утечкой информации по вине инсайдера. 68% организаций отмечают, что инсайдерские атаки стали более частыми за последние 12 месяцев [3]. Эти данные свидетельствуют о том, что риск внутренних угроз продолжает расти, это значит, что необходимо внедрять эффективные меры по борьбе с внутренними угрозами.

Внутренняя угроза или инсайдерский риск – это угроза, в результате которой интеллектуальная собственность, чувствительные и ценные данные могут быть раскрыты пользователями, имеющими легитимный доступ к сети, приложениям или базам данных. С каждым днем угрозы кибербезопасности

становятся все более сложными, а безопасность данных – еще более хрупкой. Инциденты с участием инсайдеров ежегодно обходятся компаниям в миллионы долларов и могут негативно повлиять на финансовую состоятельность компании, а также на репутацию.

С точки зрения защиты не имеет значения, является ли потеря данных результатом атаки внешнего злоумышленника или действий сотрудника. Критически важные данные должны быть защищены независимо от того, кто получает к ним доступ. Выявить внутренние угрозы бывает непросто, так как инсайдер имеет законный доступ к конфиденциальным данным и к чувствительным активам компании, поэтому всегда существует риск того, что сотрудники могут злоупотреблять этим доступом к данным в каких-либо злонамеренных целях [4]. Более того, злоумышленник может знать, как защищена эта информация, что существенно облегчает ему обход мер безопасности.

Для борьбы с внутренними угрозами первоначально следует провести оценку потенциальных рисков, которые могут исходить от инсайдеров. Использование мессенджеров для обмена короткими сообщениями по работе многие считают очень удобным инструментом, так как через них можно передавать текстовые и голосовые сообщения, файлы и видео. Но мессенджеры, как и любые другие электронные средства коммуникации, могут обладать уязвимостями с точки зрения возможных утечек.

Согласно данным исследования «Ростелеком-Солар», более 33% мошеннических схем реализуются через мессенджеры, 25% – через съемные носители и 8% – через облачные хранилища, личную и корпоративную почту соответственно [5], что показано на рис. 1.

Существует множество причин, по которым количество инцидентов, связанных с внутренними угрозами, увеличивается. Растущее использование технологии облачных вычислений и концепции «принеси свое устройство» (BYOD) способствует росту числа внутренних угроз. Пандемия COVID-19 ускорила процесс перехода к удаленному и гибриднему формату работы и способствовала распространению как облачных инструментов для совместной работы и хранения файлов, так и теневых информационных технологий, то есть программного обеспечения, не одобренного организацией. Как следствие, все большему числу сотрудников предоставляется расширенный доступ к сети. Все это приводит к общей нехватке контроля, что в итоге увеличивает возможности злонамеренных инсайдеров остаться незамеченными системами безопасности.

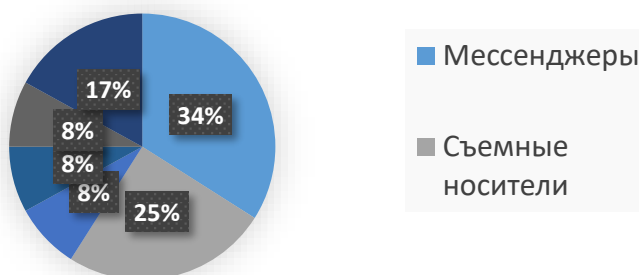


Рис. 1. Каналы мошеннических схем

Методы противодействия.

Подготовка организации к предотвращению внутренних угроз – это важная и последовательная задача. Для того чтобы сделать это правильно, необходимо внедрять правильные технологии и методы. В таблице 1 отображены основные типы внутренних угроз в организации, на которые следует обратить внимание и меры по их локализации.

ТАБЛИЦА 1. Типы внутренних угроз и меры защиты

Угроза	Описание	Меры защиты
Угроза со стороны беспечного персонала	Сотрудники, имеющие доступ к конфиденциальным данным, редко проводят полноценные инсайдерские атаки. Тем не менее они могут случайно выложить в свободный доступ данные или скомпрометировать корпоративную инфраструктуру, либо по ошибке, либо став жертвой фишинга	Проведение тренингов и учений
Угроза со стороны потенциальных злонамеренных инсайдеров	Это шпионы, разведчики внутри компании, те кто интересуется активами сети, которые им по работе не нужны (стадия вероятных намерений)	Организационные меры контроля, применение политик безопасности, использование обманок в корпоративных сетях
Угроза со стороны злонамеренных инсайдеров	Сотрудники, которые незаконно применяют или злоупотребляют своим доступом для хищения, продажи, утечки или удаления конфиденциальных данных из злонамеренных побуждений	Организационные меры контроля, технологии обманок в сочетании с оперативными мероприятиями

Одним из способов защиты от внутренних угроз является использование технологий обманок. Это категория простых и эффективных средств защиты кибербезопасности, которые обнаруживают угрозы на ранней стадии с низким количеством ложных срабатываний и минимальным воздействием на производительность сети. Технология заключается в создании реалистичных активов-приманок (например, ими могут быть домены, базы данных, активные каталоги, серверы, приложения, файлы, учетные данные, учетные записи, сеансы), которые будут развернуты в сети наряду с реальными активами. Злоумышленники, которые проникают в сеть, не имеют возможности отличить подделку от реальной сетевой сущности, и в тот момент, когда они

взаимодействуют с приманкой, система-приманка начинает регистрировать и отслеживать используемые векторы атаки на протяжении всего времени взаимодействия. Чтобы функционировать должным образом, технология обмана не должна быть очевидной для сотрудников, подрядчиков или клиентов предприятия. Преимущество данного способа заключается в возможности выявлять инсайдеров на стадии намерения, а также в дополнении существующих системы обнаружения инсайдерской информации, улучшая их производительность за счет уменьшения ложноположительных результатов.

При анализе внутренних угроз было выявлено, что инсайдерские угрозы оказывают наибольшее негативное воздействие на безопасность организаций. Приведенные статистические исследования подтверждают необходимость использования дополнительных методов защиты. В результате, в статье предложен метод применения обманных технологий в корпоративных сетях, который поможет выявлять инсайдеров на ранних стадиях. Дальнейшее изучение эффективности метода позволит разработать более совершенные меры противодействия.

Список используемых источников:

1. Yamin M. M. et al. Implementation of insider threat detection system using honeypot based sensors and threat analytics // Future of information and communication conference. – Springer, Cham, 2019. – С. 801-829.
2. 2022 Cost of insider threats global report / Ponemon institute // Proofpoint. – 2022. – С.45.
3. 2021 Insider threat report / Cybersecurity insiders // Gurukul. – 2021. – С. 24.
4. Trzeciak R. F. Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model // The 1st International Workshop on Managing Insider Security Threats (MIST2009). – 2009. – С. 1-21.
5. Мошенничество и слив в российских организациях: исследование / Ростелеком Солар. – 2022.–С.10.

Kolomiycsev R.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Organizational Information Security Internal Consequences and Countermeasures.

This article deals with the problem of internal threats in an organization. Particular attention is paid to insiders and incidents involving them. Various types of insiders and methods of dealing with them are considered. As a result, a countermeasure method is proposed using deception technologies in corporate networks.

Key words: internal threats, insiders, deception technologies, cybersecurity.

УДК 004.5
ГРНТИ 81.93.29

МОДЕЛЬ ДАННЫХ ДЛЯ ЗАЩИТЫ УСТРОЙСТВ УМНОГО ДОМА ОТ ВНЕШНЕГО НАРУШИТЕЛЯ

Н. А. Крестьяшин¹, В. В. Пучков^{1,2}

¹Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

²Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН).

В настоящее время растет популярность систем умного дома или умного офиса. В связи с этим задачи информационной безопасности расширяются на новый класс систем и устройств, связанных такими системами. При этом умные (Smart) ТВ, аудио-колонки, бытовая техника с доступом к сети Wi-Fi постоянно устанавливаются пользователями, внедряются в локальные сети без какой либо защиты. А иногда взломанные «умные» устройства сами становятся частью распределенной атаки. Необходимы новые модели защиты. В текущей работе для повышения уровня защищенности сетей Умного дома предлагается модель данных, которая может стать частью методики защиты киберфизических систем от известных уязвимостей.

умный дом, информационная безопасность, тестирование, база данных, киберфизические системы

Умный дом – система автоматизаций, позволяющая облегчить рутинные бытовые задачи в доме, здании, офисе, квартире и т.д. Умный дом позволяет пользователям создавать сценарии поведения для умных устройств, например, «выключить свет, если дома никого нет», «включить чайник вместе с будильником».

Возможности умного дома включают в себя следующие функции:

- Управление освещением;
- Видеонаблюдение;
- Управление электричеством;
- Управление шторами и/или жалюзи;
- Управление теплым полом, радиатором отопления;
- Управление вентиляцией, кондиционированием;
- Детектирование короткого замыкания, протечек воды, дыма;
- Обнаружение движения и/или присутствия человека, животных;
- Охрана;
- Голосовое управление посредством программ – голосовых помощников;
- Дистанционное управление через приложение на телефоне.

Согласно исследованию Научно-технического центра Главного радиочастотного центра (НТЦ ГРЧЦ) [1] количество умных домов в России выросло с 1,7 млн в 2017 г. до 3,7 млн в 2021 г., также прогнозируется рост до 8,3 млн в 2025 г, что представлено на рис. 1. В связи с этим растет актуальность проблемы обеспечения информационной безопасности устройств данной сферы.

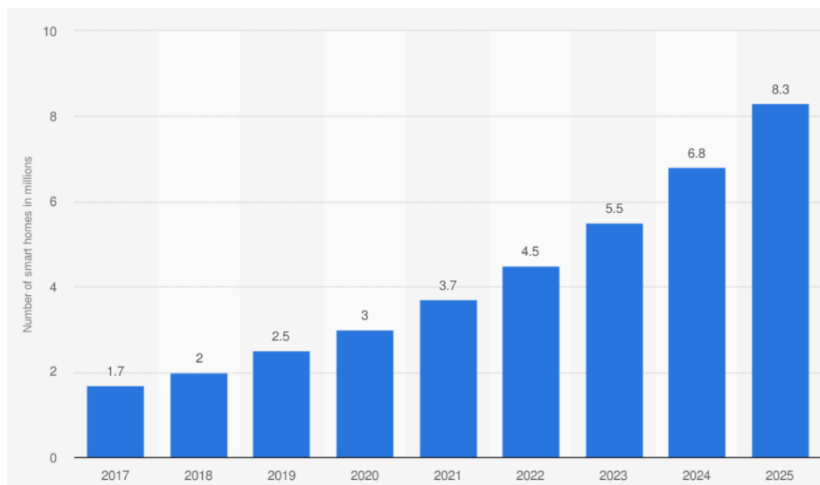


Рис. 1. Количество умных домов в России, прогноз до 2025 г.

Статьи [2, 3] приводят следующие распространённые проблемы безопасности умного дома:

1. Слабое шифрование данных внутри системы «Умный дом»;
2. Отсутствие механизма аутентификации санкционированного пользователя.
3. Необходимость наличия защищенных каналов связи
4. Потенциальные уязвимости системы «Умный дом» ввиду функционирования в ней устройств от разных производителей
5. Наличие свойственных определенным устройствам уязвимостей информационной безопасности.

Для защиты сетей Умного дома и устранения части проблем информационной безопасности предлагается база, представленная на рис. 2.

Модель данных киберфизической системы «Умный дом».

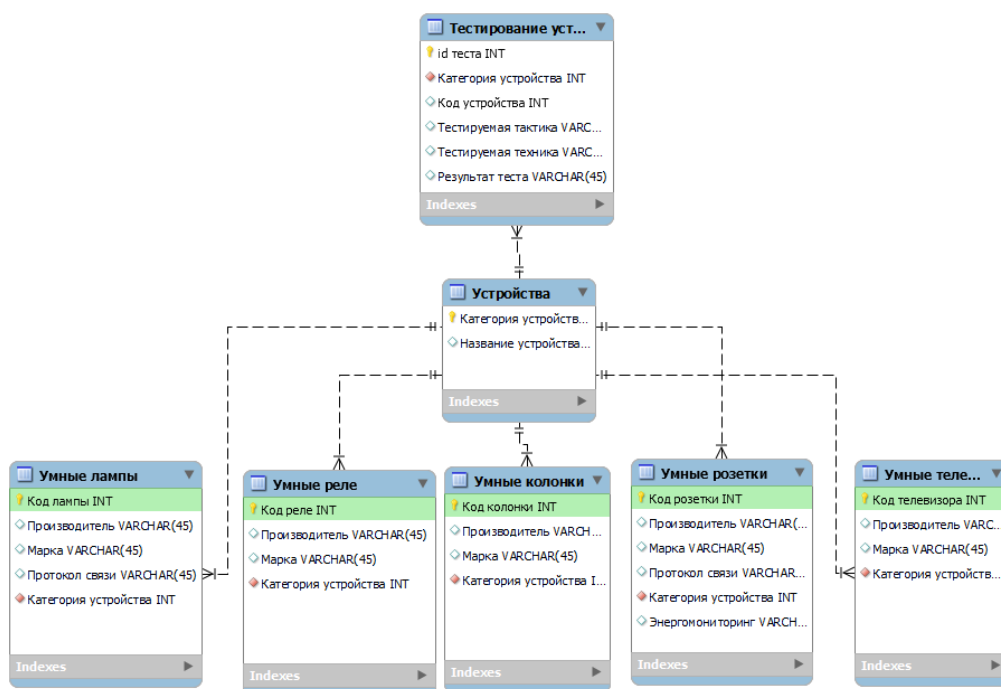


Рис. 2 Модель данных киберфизической системы «Умный дом»

Предложенная модель состоит из 7 таблиц. Главной таблицей является таблица «Устройства», данная таблица, представленная на рис. 3, содержит такие поля как «Категория устройства» и «Название устройства».

	Категория устройства	Название устройства
▶ 1		Умная колонка

Рис. 3 Пример содержимого таблицы «Устройства»

Далее в модели находятся таблицы для каждой категории устройств, они обладают схожей структурой: «Код устройства», «Производитель», «Марка», «Категория устройства», также некоторые таблицы содержат поля «Протокол связи», «Энергомониторинг». На рис 4. изображен пример таблицы «Умные колонки».

	Код колонки	Производитель	Марка	Категория устройства
▶ 1		Яндекс	Станция	1

Рис. 4 Пример содержимого таблицы «Умные колонки»

Таблица «Тестирование устройств» будет содержать в себе результаты тестирования устройств умного дома с использованием уязвимостей CVE из базы MITRE ATT&CK [4].

MITRE ATT&CK – база знаний, разработанная компанией Mitre в 2013 году. MITRE ATT&CK содержит техники и тактики, которые используют злоумышленники для реализации инцидентов информационной безопасности. Отличительная особенность данной матрицы состоит в том, что она составлена на основе анализа совершенных инцидентов.

Экспериментальный стенд.

Для тестирования и эксплуатации уязвимостей из базы MITRE ATT&CK разработан экспериментальный стенд (рис 5).

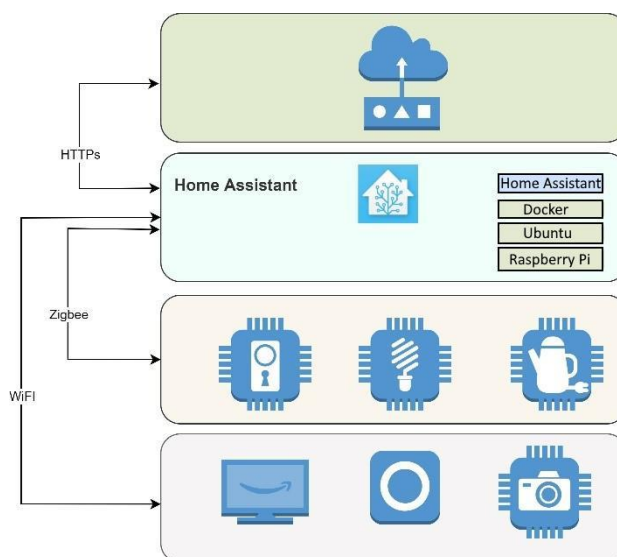


Рис. 5 Схема стенда Умный дом.

Стенд учитывает возможные протоколы связи между устройствами киберфизических системы и состоит из следующих компонентов:

- умный замок;
- умная лампа;
- умная бытовая техника;
- голосовая колонка;
- телевизор;
- видеокамера.

Для управления устройствами на плате Raspberry подключены датчики ZigBee, Wi-Fi, установлена ОС Ubuntu, запущена программа Home Assistant в контейнере Docker. Для сбора данных используется ОС Kali Linux из контейнера Docker. В ОС Kali встроены сканеры CVE уязвимостей устройств.

В текущей статье авторами было дано определение технологии «Умный дом», рассмотрены функциональные возможности и актуальные проблемы безопасности данной системы. Далее была предложена модель данных, предназначенная для тестирования устройств умного дома на наличие уязвимостей и описан экспериментальный стенд.

Статья является продолжением текущего исследования авторов [5, 6]. На следующем этапе исследования планируется выбрать вектора атак, провести атаки, собрать наборы данных для разработки методики защиты киберфизической системы от внешнего нарушителя.

Список используемых источников:

1. Рынок технологий Умного дома 2021 г. [Электронный ресурс]. URL: https://rdc.grfc.ru/2022/02/smart_home_market/ (дата обращения 10.10.2022).
2. Анализ уязвимостей системы «Умный дом» / А. М. Сливин, А. П. Иванов // Инжиниринг и технологии. – 2018. – Vol. 3(2). – DOI 10.21685/2587-7704-2018-3-2-3.
3. Виткова Л.А., Едемская Е.Д. Изучение уязвимостей в системе «умного» дома и методов их обнаружения. //В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. С. 267-270.
4. MITRE ATT&CK [Электронный ресурс]. URL: <https://attack.mitre.org/> (дата обращения 10.10.2022).
5. Виткова Л.А., Пучков В.В. Архитектура системы обнаружения аномального трафика в IoT. // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 4. С. 76-81.
6. Виткова Л.А., Крестьяшин Н.А. Классификация источников угроз SQL- инъекций. // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. С. 274-278.

Krestyashin N.A.¹, Puchkov V. V^{1,2}

¹The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

²St. Petersburg Federal Research Center of the Russian Academy of Sciences

A data model for protecting smart home devices from an external intruder.

Currently, the popularity of smart home or smart office systems is growing. In this regard, the tasks of information security are expanding to a new class of systems and devices connected by such systems. At the same time, Smart TV, audio speakers, household appliances with access to Wi-Fi are constantly installed by users, embedded in local networks without any protection. And sometimes hacked "smart" devices themselves become part of a distributed attack. New protection models are needed. In the current work, a data model is proposed to increase the security level of Smart Home networks, which can become part of the methodology for protecting cyber-physical systems from known vulnerabilities.

Key words: smart home, information security, testing, database.

УДК 004.71
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ СИСТЕМ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ КЛИЕНТОВ БЕСПРОВОДНЫХ СЕТЕЙ СЕМЕЙСТВА IEEE 802.11

О. И. Кузьмина, В. Е. Дрепа

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современных сетях беспроводного доступа важную роль занимают сервисы определения местоположения. Для решения задачи позиционирования существуют специализированные системы, разработанные ведущими вендорами в отрасли связи. Определяя местоположение и отслеживая перемещение объектов, компаниям удается контролировать работу людей и техники, обеспечивать безопасность производственных процессов и повышать эффективность бизнеса. В данной работе представлено исследование существующих систем позиционирования клиентов беспроводных сетей семейства IEEE 802.11.

беспроводные сети, определение местоположения, Wi-Fi, IEEE 802.11

Системы определения местоположения широко распространены в настоящее время, они используются в сфере экономики, медицины, медиасфере, а также в сфере информационной безопасности. Данные о геолокации пользователя используются в мобильных приложениях для вызова такси, браузеров, социальных сетях и т.д. Сети беспроводного доступа используются повсеместно и количество возможных атак [1] каждый день увеличивается. Определение местоположения устройства, с которого производится атака на беспроводную сеть, может быть одной из возможностей системы позиционирования.

Существует большое количество производителей беспроводного оборудования, однако, не у всех из них разработаны решения по определению местоположения беспроводных клиентов. Ниже приведена таблица 1, в которой представлены системы позиционирования, исследованные в данной работе.

ТАБЛИЦА 1. Системы позиционирования клиентов беспроводных сетей

Производитель	Продукт позиционирования	Принцип работы
Cisco	CMX (Connected Mobile Experience)	Используется беспроводная инфраструктура на базе точек доступа Cisco, управляется через базовый контроллер Cisco. На платформе Cisco CMX или Cisco Spaces Connector (в зависимости от системы позиционирования) устанавливается программный интерфейс. Требуется подписка Cisco Prime.
	DNA (Digital Network Architecture) Spaces	
Aruba	ALE (Analytics and Location Engine)	Используются точки доступа Aruba и виртуальная машина ALE, подключенная к модулю VisualRF.

Ekahau	Ekahau Real-Time Location System	Система базируется на любой Wi-Fi сети, используются специальные метки Ekahau и ПО Ekahau Vision.
Huawei	iMaster NCE-CampusInsight	Используется платформа iMaster NCE-CampusInsight для определения местоположения клиентов Wi-Fi сети, точки доступа должны быть совместимы с данной платформой. Требуется подписка.

Возможности Cisco CMX (Connected Mobile Experience) предоставляются с помощью трех компонентов: Location, CMX Connect и CMX Analytics [2].

Location: CMX использует существующую беспроводную инфраструктуру для расчета местоположения устройств Wi-Fi и источников помех, например, маяков BLE, микроволновых печей и др. в сети.

CMX Connect предоставляет целевые, контекстно-зависимые услуги посетителям на месте. Он предоставляет простой способ создания настраиваемых авторизованных порталов и сбора информации о посетителях с помощью нескольких вариантов регистрации. Благодаря собранным данным CMX Connect позволяет организациям взаимодействовать с посетителем на авторизованном портале или через внешние средства массовой информации, такие как мобильные приложения, цифровые вывески или офлайн-маркетинг.

CMX Analytics генерирует информацию об устройствах Wi-Fi посетителей в месте проведения на основе их местоположения и моделей движения. Существует два вида аналитики — аналитика присутствия и аналитика местоположения.

Cisco DNA (Digital Network Architecture) Spaces использует существующую сеть, а также физические пространства Wi-Fi и проводной инфраструктуры, включая людей (посетителей, гостей, сотрудников) и объекты (сенсоры, интеллектуальные устройства).

Унифицированное решение Cisco DNA Spaces для определения местоположения получает данные от многочисленных сенсоров, фильтрует и очищает их, предоставляет инструментарий для работы с этими данными, а также делает эти данные доступными для партнеров – независимых поставщиков программного обеспечения, а также партнеров по решениям для достижения бизнес-результатов.

Сравнение решений позиционирования Cisco представлено в таблице 2.

ТАБЛИЦА 2. Сравнение особенностей систем позиционирования Cisco

Особенность	Cisco DNA Spaces	Cisco CMX
Расчет местоположения устройства	Облачное обнаружение и расчет местоположения	Локальное обнаружение и расчет местоположения

Расчёт местоположения, используя технологию Hyperlocation или FastLocate	Да	Да
Беспроводное подключение Wi-Fi	Да	Нет
API-мониторинг	Да	Нет
Партнерский центр приложений	Да	Нет

Технология Cisco Hyperlocation – это решение для определения местоположения, которое позволяет отслеживать местоположение беспроводных клиентов с точностью до одного метра. Решение использует метод расчета местоположения подключённых устройств по углу прибытия (Angle of Arrival) сигналов Wi-Fi.

Технология Cisco FastLocate повышает скорость обновления данных о местоположении подключенных беспроводных клиентов, благодаря чему система позиционирования захватывает больше точек данных о местоположении. Для расчета местоположения устройства используется метод по уровню мощности принимаемого сигнала RSSI из пакетов данных. Точность данной технологии – до 10 метров, но при частоте обновления, которая для активных устройств составляет более одного раза в 30 секунд, результат улучшается до значения менее 10 метров [3].

Aruba Analytics and Location Engine (ALE) – это виртуальный механизм агрегации контекста и определения местоположения, который собирает данные о мобильных устройствах с поддержкой Wi-Fi, находящихся поблизости или подключенных к сети Aruba WLAN [4].

Контекстные данные позволяют внешним системам аналитики собирать информацию о людях, устройствах и приложениях, используемых в и извлекать полезные бизнес-аналитические данные. Данные о структуре трафика, включая время пребывания и частоту повторных посещений, соотносятся с другими источниками данных, такими как базы данных постоянных клиентов и системы продаж. Это позволяет предприятиям оценить эффективность маркетинга, предложить гостям и сотрудникам более персонализированную рекламу и повысить общую эффективность работы.

ALE устанавливается в виде образа виртуальной машины (VM): один образ VM, поставляемый в виде OVA-файла, может быть развернут с различными аппаратными конфигурациями, в зависимости от требований масштаба сети. CentOS 6.4 предустановлена со всеми необходимыми зависимостями. Поддерживается на VMware ESX/ESXi 5.0 или выше.

ALE требует подключения к модулю VisualRF для управления сетью Aruba AirWave и отображения карты площадки с расположением точек доступа. VisualRF автоматически генерирует карту радиочастотной среды и топологии сети, включая состояние устройств. VisualRF строит эту карту, используя

радиочастотные измерения, собранные с авторизованных беспроводных точек доступа, контроллеров и клиентов. VisualRF показывает, кто именно находится в сети, где они находятся и как работает сеть и связанные с ней клиентские устройства.

Для небольших помещений с 1-2 точками доступа, где необходимо присутствие, но не требуется триангуляция местоположения, ALE поддерживает функцию без карты при использовании с точками доступа Aruba Instant.

EkaHau Real-Time Location System (RTLS) – это беспроводное радиочастотное решение, которое постоянно отслеживает и сообщает в реальном времени местоположение отслеживаемых объектов.

Технология радиочастотного моделирования EkaHau использует стандартные точки доступа Wi-Fi, поэтому нет необходимости в специальной инфраструктуре. Любая сеть Wi-Fi может работать как сеть датчиков для системы определения местоположения в реальном времени. Это позволяет ускорить установку системы и значительно понизить затраты. EkaHau RTLS не требует аутентификации WLAN, для передачи данных используются недорогие Wi-Fi метки, работающие от батарей и перезаряжаемые [5]. Такие метки EkaHau прикрепляются к вещам или надеваются на людей. Метки передают радиочастотные сигналы стандарта 802.11b на точки доступа Wi-Fi, а затем в программное обеспечение EkaHau Vision для анализа и отображения. Алгоритмы EkaHau интерпретируют данные радиочастотного сигнала, вычисляя ряд вероятных местоположений и присваивая уровни уверенности каждому вероятному местоположению, а также отфильтровывают естественные колебания радиочастотного сигнала.

Huawei iMaster NCE-CampusInsight – технология Huawei для определения местоположения клиентов Wi-Fi основана на методе уровней принимаемой мощности беспроводного сигнала. Точки доступа сообщают собранную информацию о сигнале от клиента серверу определения местоположения. Сервер местоположения вычисляет местоположение клиента и точки доступа, а затем отображает местоположение устройства пользователю сети. В качестве сервера местоположения выступает механизм определения местоположения iMaster NCE-CampusInsight. Точки доступа должны быть доступны для iMaster NCE-CampusInsight [6], чтобы данные о местоположении могли быть отправлены в его систему позиционирования. Для синхронизации часов устройства клиента с часами сетевой системы рекомендуется использовать NTP-сервер.

В данной работе были исследованы существующие системы определения местоположения клиентов беспроводных сетей семейства IEEE 802.11, разработанные вендорами сферы связи. Рассматривая данные решения, был сделан вывод, что их реализация труднодоступна для среднего и малого бизнеса из-за необходимости специализированного программного и аппаратного обеспечения высокой стоимости. Создание более бюджетной системы позиционирования является актуальной задачей, в том числе в рамках программы импортозамещения.

Список используемых источников:

1. Киструга А. Ю., Ковцур М. М., Оганесян А. Г. Исследование устойчивости точек доступа в режиме PSK к DOS атакам на беспроводную сеть // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы X Юбилейной Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 24-25 февр. 2021 г. СПб. : СПбГУТ, 2021. Т. 1. С. 485–489.
2. Cisco Connected Mobile Experiences Data Sheet: [Электронный ресурс]. URL: <https://www.cisco.com/c/en/us/products/collateral/wireless/mobility-services-engine/datasheet-c78-734648.html> (Дата обращения 22.10.2022)
3. Cisco Spaces: Detect and Locate Configuration Guide: [Электронный ресурс]. URL: <https://www.cisco.com/c/en/us/td/docs/wireless/cisco-dna-spaces/detectandlocate/b-cisco-cle.html> (Дата обращения 22.10.2022)
4. Aruba Analytics and Location Engine: [Электронный ресурс]. URL: https://www.arubanetworks.com/assets/ds/DS_ALE.pdf (Дата обращения 23.10.2022)
5. The Ekahau Real-Time Location System: [Электронный ресурс]. URL: <https://www.ayscom.com/wordpress/wp-content/uploads/2016/03/Ekaha-RFID-over-WiFi-RTLS-Solutions.pdf> (Дата обращения 30.10.2022)
6. CloudCampus Solution Design and Deployment Guide: [Электронный ресурс]. URL: <https://support.huawei.com/enterprise/en/doc/EDOC1100193623/36bd9a12/wireless-location-design> (Дата обращения 05.11.2022)

Kuzmina O., Drepa V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Research of the location systems of IEEE 802.11 family wireless networks clients.

Location services play an important role in modern wireless access networks. To solve the problem of positioning, there are specialized systems developed by vendors in the communications industry. Companies manage to control the work of people and equipment, ensure the safety of production processes and improve business efficiency, using location and tracking of the movement of objects. This article presents a study of existing systems for positioning clients of wireless networks of the IEEE 802.11 family.

Key words: *wireless networks, positioning, Wi-Fi, IEEE 802.11.*

УДК 004.056
ГРНТИ 81.93.29

ПОДРОБНЫЙ АНАЛИЗ КЛАССОВ УЯЗВИМОСТЕЙ В VOIP СЕТЯХ

А. К. Макарова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современный мир характеризуется непрерывной коммуникацией участников всех областей жизнедеятельности. В период начала пандемии упал общий уровень защищенности из-за адаптации к новым условиям работы, быстрого внедрения технологий удаленного доступа, отзыва лицензий, в следствии санкций, а соответственно отсутствия поддержки оборудования иностранными фирмами. Все это спровоцировало рост атак на VoIP коммуникации.

В рамках данной статьи будут сформированы классы уязвимостей технологии VoIP. Описание класса будет включать подробный его анализ: описание, проблематика и меры по устранению уязвимостей.

VoIP, уязвимости, классификация уязвимостей

Многие сетевые компоненты, участвующие в развертывании технологии VoIP, имеют уязвимые места, прямо или косвенно влияющие на ее безопасность. Так, использование злоумышленником нескольких уязвимостей, может привести к реализации более сложны (многоходовых) атак [1]. Для формирования структуры рассуждения были выделены классы уязвимостей, чтобы охватить большую их часть. По компонентам, составляющим VoIP технологию, на основе данных собранных в информационных ресурсах, сформированы классы уязвимостей. Например: уязвимости протоколов VoIP, уязвимости внешних протоколов и устройств, уязвимости сетевой инфраструктуры и так далее. Сокращенные обозначения классов: ку_1, ку_2, ..., ку_8. Рассмотрим Топ-8 выделенных мной классов.

КУ_1. Уязвимости протоколов VoIP.

1. Суть: приложения VoIP работают в основном с открытыми протоколами сигнализации (H323, SIP, IAX) и используют протоколы передачи мультимедиа (RTP, RTCP). Все эти протоколы уязвимы для различных видов атак.

2. Как проявляется или используется: Протокол SIP - осуществляет открытую передача данных, пароль хэшируется алгоритмом MD5 – не безопасен, легко взломать.

3. Используется атакой: перехват регистрации SIP, Модификация SIP-сообщения.

КУ_2. Уязвимости внешних протоколов и устройств.

1. Суть: сетевая структура VoIP строится на основе протокола IP, следовательно использует его протоколы (пример: OSPF, ARP), те передают свои уязвимости сети VoIP.

2. Как проявляется или используется: например, у протокола ARP отсутствует проверка подлинности запросов и ответов. Отправляя поддельные пакеты ARP, можно выдать себя либо за регистратора SIP, либо за конечную точку.

3. Используется атакой: ARP Poisoning.

КУ_3. Уязвимости сетевой инфраструктуры.

1. Суть: VoIP-трафик будет подвержен уязвимостям IP-сети, в случае отсутствия отдельного WLAN [2]. В большинстве случаев это связано с неправильной конфигурацией сетевого устройства (коммутатора, маршрутизатора, брандмауэра и т. д.) или ошибкой в одном из задействованных протоколов (IP, UDP и т. д.).

2. Как проявляется или используется: злоумышленники могут проникнуть в медиа-поток RTP между двумя узлами с намерением изменить полезную нагрузку (или содержимое) голосового сообщения.

3. Используется атакой: MITM.

КУ_4. Уязвимости интерфейса управления.

1. Суть: VoIP устройств имеют различные сервисные интерфейсы, такие как SNMP, SSH, Telnet и HTTP. Сервисный интерфейс может быть источником уязвимости, особенно в случаях, когда при настройке интерфейса управления идентификатор/пароль оставляют по умолчанию.

2. Как проявляется или используется: из-за отсутствия надежного пароля, взломать интерфейс становится весьма простой задачей.

3. Используется атакой: фрикерская атака.

КУ_5. Уязвимости в передаче данных (незашифрованное соединение).

1. Суть: Большинство протоколов инициализации передают данные и голос в открытом виде, поэтому при передаче следует использовать дополнительные методы шифрования (протоколы TLS, SRTP) [3]. Данные следует шифровать на обеих сторонах передачи.

2. Как проявляется или используется: перехватив не зашифрованные данные, злоумышленник получает доступ к голосовому IP-трафику клиентов.

3. Используется атакой: подслушивание, утилита VOMIT.

КУ_6. Уязвимость полосы пропускания.

1. Суть: Сервис должен выдерживать нагрузку на сеть, даже если все абоненты звонят одновременно. Обычно используют резервированные полосы (протокол RSVP) [4].

2. Как проявляется или используется: генерация большого числа инициаций вызовов, может перегрузить сервер и помешать ему обрабатывать законные вызовы. Это классическая техника DoS, применяемая к SIP.

3. Используется атакой: DoS, UDP Flood.

КУ_7. Уязвимость обработки ошибок.

1. Суть: при обработке неправильной регистрации SIP Сообщение о регистрации с недопустимым номером телефона может привести к коду ошибки «404», тогда как действительный номер телефона приведет к ошибке «401» [5].

2. Как проявляется или используется: позволяет сузить область атаки, чтобы попытаться атаковать методом грубой силы только действительные учетные записи.

3. Используется атакой: рассылки спама по интернет-телефонии (SPIT).

КУ_8. Ошибки аутентификации и сертификата.

1. Суть: все пользователи и устройства должны проходить обязательную аутентификацию. Кроме того, в устройствах VoIP существуют другие службы, такие как управление устройствами, для которых требуется проверка подлинности пользователя [6].

2. Как проявляется или используется: система регистратора не аутентифицирует пользователя или устройство, но позволяет злоумышленникам подделывать регистрационные сообщения и повторно регистрироваться в качестве действительного пользователя.

3. Используется атакой: перехват регистрации в SIP.

Таким образом, в рамках исследования было получено Топ-8 классов уязвимостей:

1. Уязвимости протоколов VoIP;
2. Уязвимости внешних протоколов и устройств;
3. Уязвимости сетевой инфраструктуры;
4. Уязвимости интерфейса управления;
5. Уязвимости в передаче данных;
6. Уязвимость полосы пропускания;
7. Уязвимость обработки ошибок;
8. Ошибки аутентификации и сертификата.

К каждому классу представлено краткое описание, пример проявления, пример атаки, использующей данную уязвимость и методы противодействия. Предполагается, что данная классификация поможет в дальнейшей работе при создании расширенной модели атак, которая будет формироваться на основе данных классов уязвимостей сети VoIP и автоматизации подхода по ее защите.

Список используемых источников:

1. Mentsiev, A. U. VoIP security threats / A. U. Mentsiev, A. I. Dzhangarov // *Engineering Journal of Don*. – 2019. – No 1(52). – P. 75. – EDN QBNDIH.
2. Говор, Т. А. Обеспечение безопасности современных voip-сетей / Т. А. Говор // *Радиопромышленность*. – 2011. – № 4. – С. 37-43. – EDN ONPSXL.
3. Ковцур, М. Протоколы обеспечения безопасности IP-телефонии / М. Ковцур // *Первая миля*. – 2012. – Т. 32. – № 5. – С. 18-27. – EDN PGGBIX.
4. Яремчук, С. Атаки на VoIP и методы защиты / С. Яремчук // *Системный администратор*. – 2011. – № 6(103). – С. 62-64. – EDN RFVGGJ.
5. Peter Thermos; Ari Takanen, “Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures”, Addison-Wesley Professional, August 2007, ISBN-10: 0-321-43734-9
6. Никитин, И. Ю. Исследование и анализ уязвимостей систем IP телефонии на базе протокола SIP / И. Ю. Никитин // *Проблемы передачи информации в инфокоммуникационных системах : сборник докладов и тезисов VIII Всероссийской научно-практической конференции*, Волгоград, 26 мая 2017 года. – Волгоград: Волгоградский государственный университет, 2017. – С. 93-98. – EDN ZBYOPP.

Makarova A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Detailed analysis of vulnerability classes in VoIP networks.

The modern world is characterized by continuous communication of participants of all areas of life. During the start of the pandemic, the overall level of security fell due to adaptation to new working conditions, the rapid introduction of remote access technologies, the revocation of licenses as a result of sanctions, and, accordingly, the lack of support for equipment by foreign firms. All this provoked the growth of attacks on VoIP communications. Within the framework of this article, classes of vulnerabilities in VoIP technology will be formed. The description of the class will include its detailed analysis: description, issues and measures to eliminate vulnerabilities.

Key words: *VoIP, vulnerabilities, classification of vulnerabilities.*

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ УЯЗВИМОСТЕЙ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS

Н. А. Макеев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Компьютеры произвели революцию во всех отраслях промышленности. Компьютеры стали самой важной частью успеха любого предприятия. Компьютеры — это лучшее средство для надлежащего хранения и управления данными. Они могут использоваться в качестве баз знаний и для финансовых операций благодаря своей вычислительной мощности и объему памяти. Компьютеры обрабатывают и хранят данные, которые являются очень конфиденциальными и важными для организации. Поэтому обеспечение безопасности этих компьютеров является очень важной задачей. Осознание этого привело к разработке методов, которые пытаются обнаружить проблемы или лазейки в программных системах. Однако существуют некоторые программные сбои, которые могут быть использованы для намеренной попытки нанести серьезный ущерб системам. Эти программные сбои, обычно обозначаемые как компьютерные уязвимости, обладают особыми свойствами, которые отличают их от других программных сбоев. Детальный анализ каждой уязвимости классифицирует ее характеристики, политики, нарушаемые при ее эксплуатации, и приводит к пониманию мер, необходимых для устранения этих уязвимостей в будущих программах

патчи, безопасность, уязвимость, операционная система Windows

В 2000 году насчитывалось более 50 000 компьютерных вирусов. В 2002 году количество известных вирусов, троянских программ, червей и их вариаций достигло 60 000. Сегодня известно более 1000 000 компьютерных вирусов. А. Джеймс Кларк из Университета Мэриленда показал, что каждые 39 секунд происходит атака на компьютер, подключенный к Интернету. В современном мире, где программное обеспечение стало очень важной частью нашей жизни, нам стало очень важно иметь безопасное программное обеспечение. Компьютерные программы все глубже проникают в нашу жизнь. Они практически контролируют все - от онлайн-образования до бизнеса. На сайте показано, что Соединенные Штаты являются целью большинства НТТР-атак на стороне сервера. Существует несколько источников и несколько пунктов назначения этих атак. Китай является вторым по величине источником атак после США. Соединенные Штаты занимают первое место по количеству таких атак.

Чтобы противостоять лазейкам в безопасности программного обеспечения, которые технически можно назвать "уязвимостями", существует огромный спрос на анализаторы уязвимостей и другое программное обеспечение, связанное с безопасностью. Уязвимость можно определить как слабое место конструкции или ошибка в реализации, которая может привести к неожиданному, нежелательному событию, ставящему под угрозу безопасность соответствующей компьютерной системы, сети, приложения или протокола. Для

уязвимостей существуют общедоступные базы данных. Эти уязвимости служат основой для крупных нарушений безопасности, связанных с системой, которые являются наиболее вредными. Эти нарушения очень трудно проверить, поскольку данные поступают нечасто. Уязвимости классифицируются в соответствии с классом активов, к которому они относятся, например, аппаратное обеспечение, программное обеспечение - операционная система, приложение, сеть, персонал, сайт и организация. Распространенными типами дефектов программного обеспечения, которые приводят к уязвимостям, являются: Нарушения безопасности памяти, ошибки проверки ввода, метасимволы, неправильная обработка оболочки, поэтому они интерпретируются как SQL-инъекция, инъекция кода, инъекция электронной почты, обход каталога, межсайтовый скриптинг в веб-приложениях, инъекция HTTP- заголовка, расщепление HTTP-ответа и т.д., условия гонки, ошибки путаницы в привилегиях, эскалация привилегий, сбои пользовательского интерфейса. Уязвимости внедряются в программы несколькими способами, некоторые из них:

- Кодеры внедряют уязвимый код в программное обеспечение неосознанно. Это происходит из-за недостаточного понимания и осведомленности в безопасности;

- Разработчики не имеют соответствующих инструментов для оценки уязвимости кода и скомпилированных приложений.

Поставщики программного обеспечения предоставляют исправления и обновления для системы, чтобы устранить эти уязвимости. Однако хакеры используют эти уязвимости для установки вредоносного кода на компьютеры пользователей с целью кражи секретных данных для получения денежной выгоды. Взломанные компьютеры могут быть в дальнейшем используются для проведения атак типа "отказ в обслуживании" на серверы. Эти машины могут быть использованы для посягательств на компьютеры правительственных ведомств. Согласно процесс обнаружения уязвимостей можно разделить на три различные фазы. Фаза 1 включает в себя сбор достаточных знаний о системе. Эта фаза выполняется тестировщиками, что позволит им скомпрометировать систему. Фактическое обнаружение уязвимостей происходит на фазе 2. Наконец, на фазе 3 усилия по обнаружению уязвимостей начинают смещаться в сторону последующей версии программного обеспечения. Эти фазы образуют форму буквы «S». Предполагается, что она следует принципу уязвимости, согласно которому скорость обнаружения соответствует импульсу, полученному в результате принятия продукта рынком. Она также линейна по отношению к насыщению обнаружения уязвимостей. Модель также предполагает, что существует ограниченное количество уязвимостей, которые могут быть обнаружены. которая связывает количество уязвимостей со всеми усилиями, затраченными на обнаружение уязвимостей.

Уязвимости операционной системы. Существует огромное количество разновидностей операционных систем; только четыре центральных семейства существуют в основной массе - Windows, OS X, Linux и UNIX. По данным сайта

Microsoft Windows доминирует на мировом рынке операционных систем, занимая почти 90% рынка, а Apple и Linux делят оставшиеся 10% с множеством других доступных операционных систем. В анализ пяти операционных систем показывает, что среднее время между раскрытием уязвимостей для операционной системы Windows примерно в два раза больше, чем для MAC OSX и операционных систем с открытым исходным кодом. С другой стороны, "программных строк кода" в операционных системах Windows меньше, чем в MAC OSX и Debian 3.1 Каждая операционная система имеет свой собственный пакет уязвимостей, начиная от локальных эксплойтов и заканчивая удаленно доступными векторами атак. Что касается условий "прямо из коробки", то и Windows от Microsoft, и OS X от Apple полны удаленно доступных уязвимостей. Еще до развертывания серверов машины на базе Windows содержат множество уязвимостей, которые позволяют хакерам получить доступ к системе, а также выполнить произвольный код.

Когда речь идет о корпоративных системах, большинство систем полагается на обученных администраторов и ИТ-отделы, которые часто ставят исправления и обновляют операционные системы и их службы. Сценарий для домашних компьютеров отличается. Более ориентированные на потребителя операционные системы от Microsoft и Apple "закалены" каждая по-своему. Как только пользователь начинает субъективно позволять себе возиться с настройками по умолчанию, системы сразу же становятся восприимчивыми к вторжению. Если не включены соответствующие патчи или автоматические обновления, владельцы компьютеров с Windows и OS X наиболее подвержены быстрым и тщательным удаленным нарушениям со стороны хакеров. Согласно бюллетеню безопасности Microsoft MS08-067 в 2009 году более 90% целевых атак Microsoft были атаками на уязвимость переполнения буфера. Большинство этих атак на операционные системы Microsoft Windows было совершено червем Conficker/Downadup и его разновидностями. Даже такие черви, как Sasser и Blaster, печально известные в 2003-2004 годах, также были активны в этот период. Упомянутые выше атаки характерны как для операционных систем, так и для приложений. В связи с этим поставщики часто выпускают исправления и обновления. Системные уязвимости быстро устраняются производителями в первые две недели их жизни. Уязвимости, обнаруженные в приложениях, получают меньше внимания и исправляются медленно. Широко используемые приложения, такие как Microsoft Internet Explorer, Microsoft Office и Adobe Reader, более уязвимы для угроз.

Уязвимость автозапуска. Функция автозапуска появилась в Windows XP. Эта функция проверяет съемные носители / устройства, затем определяет и запускает соответствующее приложение на основе его содержимого. Эта функция полезна для аутентичных пользователей, но является шлюзом для злоумышленника. Разработанная программа смогла получить доступ и выполнить произвольный код, вставив USB, используя эту функцию. Эта уязвимость может быть использована локально. Сложность атаки в этом случае невелика. Конфиденциальность и целостность системы полностью утрачены.

Уязвимость буфера обмена. Разработанное программное обеспечение могло получать доступ к данным буфера обмена и изменять их. Эта уязвимость может позволить злоумышленнику получить доступ к конфиденциальным данным буфера обмена. В Windows буфер обмена является общим для всех приложений. Это может привести к доступу и изменению буфера обмена всех приложений в операционной системе.

Уязвимость реестра. MS-Windows хранит свои параметры конфигурации и опции в иерархической базе данных, которая известна как реестр Windows. Реестр используется для низкоуровневых настроек операционной системы и для настроек приложений, запущенных на платформе. Все жизненно важные компоненты операционной системы, такие как ядро, пользовательский интерфейс, драйверы устройств, SAM и т.д., используют реестр. Редактор реестра Windows не является защищенной программой. Это позволяет редактировать реестры без разрешения владельца. Как перед редактированием реестра с помощью программного обеспечения исполняемых файлов специально не отображается сообщение, поэтому злоумышленники могут легко изменить значение DWORD реестра, что представляет серьезную угрозу.

Уязвимость PNG. Программное обеспечение смогло вызвать отказ в обслуживании DoS-атака. В этой уязвимости Windows позволяет злоумышленнику использовать переносное сетевое графическое изображение (PNG) с должным разрешением в Блок IHDR, который приводит к 100% потреблению процессора. Операционная система Windows не приспособлена для обработки вредоносных PNG-файлов. Эта уязвимость может привести к чрезмерному использованию ресурсов и вызвать сбой системы. Таким образом, отказывая пользователям в обслуживании. Эта уязвимость не приводит к потере конфиденциальности или целостности и оказывает влияние на частичную доступность.

С появлением технологий каждый день обнаруживаются новые уязвимости или слабые места. В этой статье были рассмотрены основы атаки с использованием разработанной системы. Был проведен эксперимент, который продемонстрировал, что обновленные версии операционной системы Windows по-прежнему имеют ряд уязвимостей, которые могут привести к компрометации системы. Существуют определенные уязвимости, для которых нет доступных исправлений. PNG — это такая уязвимость. Window-очень популярная операционная система, но все же она подвержена атакам. Разработанная система была способна использовать уязвимости, такие как реестр, автозапуск и буфер обмена, чтобы получить доступ к системе. Эти уязвимости в Microsoft Windows делают ее более подверженной атакам. Пользователь должен знать об этих уязвимостях и использовать дополнительные меры безопасности для защиты системы. Поставщик операционной системы должен заблаговременно протестировать свой продукт и обеспечить безопасную среду.

Список используемых источников:

1. Бирюков, А. А. Информационная безопасность. Защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2016. - 474 с.
2. Лебедев, Алексей Защита компьютера от вирусов, хакеров и сбоев. Понятный самоучитель / Алексей Лебедев. - М.: Питер, 2013. - 160 с.
3. Бабин, С.А. Лаборатория хакера / С.А. Бабин. - М.: БХВ-Петербург, 2018. - 951 с.
4. Кевин, Мандиа Расследование компьютерных преступлений / Мандиа Кевин. - М.: ЛОРИ, 2013. - 143 с.
5. Аграновский А. В., Девянин П. Н., Хади Р. А, Черемушкин А. В. – Основы компьютерной стеганографии. – Радио и связь. – 2003. – 5-33.

Makeev N.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Windows operating system vulnerabilities.

This article deals with the problem of vulnerabilities in operating systems. Particular attention is paid to the development of operating systems. Various vulnerabilities, especially Windows operating system vulnerabilities are discussed and as well as the troubleshooting is presented.

Key words: *Patches, Security, Vulnerability, Windows Operating System.*

УДК 004.773
ГРНТИ 49.33.31

СТЕГАНОГРАФИЧЕСКИЕ ВЛОЖЕНИЯ В «STREAM CONTROL TRANSMISSION PROTOCOL»

М. Д. Масютин, А. С. Салита

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Протокол передачи с управлением потоком (SCTP) является новым протоколом транспортного уровня, который должен заменить TCP (Transmission Control Protocol) и UDP (User Datagram Protocol). Протокол управления потоком (SCTP) — это новый протокол транспортного уровня, который должен заменить протоколы TCP (Transmission Control Protocol) и UDP (User Datagram Protocol) в будущих IP сетях. В настоящее время он реализован в таких операционных системах, как BSD, Linux, HP-UX или Sun Solaris. Он также поддерживается в сетевых устройствах Cisco (Cisco IOS) и может быть использован в операционной системе Windows. В данной статье описываются потенциальные стеганографические методы, которые могут быть применены к SCTP и могут представлять угрозу для сетевой безопасности.

SCTP, стеганография, сети, информационная безопасность

Последняя тенденция в стеганографии заключается в использовании сетевых протоколов в качестве носителя стеганограммы путем изменения содержимого пакетов, которые используются протоколами, временных отношений между этими пакетами или гибридных решений. Все методы сокрытия информации, которые могут быть использованы для обмена стеганограммами в телекоммуникационных сетях, описываются термином "сетевая стеганография", который был первоначально введен Кшиштофом Щипиорски в 2003 году [8]. Многие стеганографические методы были предложены и проанализированы, например, [1],[2],[3],[4]. Они должны рассматриваться как угроза для сетевой безопасности, поскольку они могут привести, например, к утечке конфиденциальной информации.

SCTP [5] был определен рабочей группой IETF Signaling Transport (SIGTRAN) в 2000 году и поддерживается рабочей группой IETF Transport Area (TSVWG). Он разрабатывался для одной конкретной цели - транспортировки телефонной сигнализации по сетям на базе IP. Однако его особенности позволяют ему быть протоколом транспортного уровня общего назначения ([5], [6]). SCTP, как и TCP, обеспечивает надежную, последовательную передачу данных с контролем перегрузки, но при этом устраняет ограничения TCP. SCTP позволяет также установить доставку данных в порядке прибытия (порядковый номер не имеет значения). Расширение частичной надежности SCTP, определенное в [7], представляет собой механизм, позволяющий передавать не все данные, если в этом нет необходимости, т.е. данные, которые не были правильно получены, а устарели. Эта особенность делает приложения на базе SCTP более простыми в разработке, чем на базе TCP. Каждое SCTP-соединение (которое в SCTP называется ассоциацией) может использовать один или

несколько потоков, которые представляют собой однонаправленные логические каналы между конечными точками SCTP. Доставка данных в порядке передачи или в порядке прибытия осуществляется в пределах каждого потока отдельно, а не глобально. Если один из потоков блокируется (т.е. пакет потерян, а получатель ожидает его), это не влияет на другие потоки. Преимущество использования нескольких потоков показано на рис. 1.

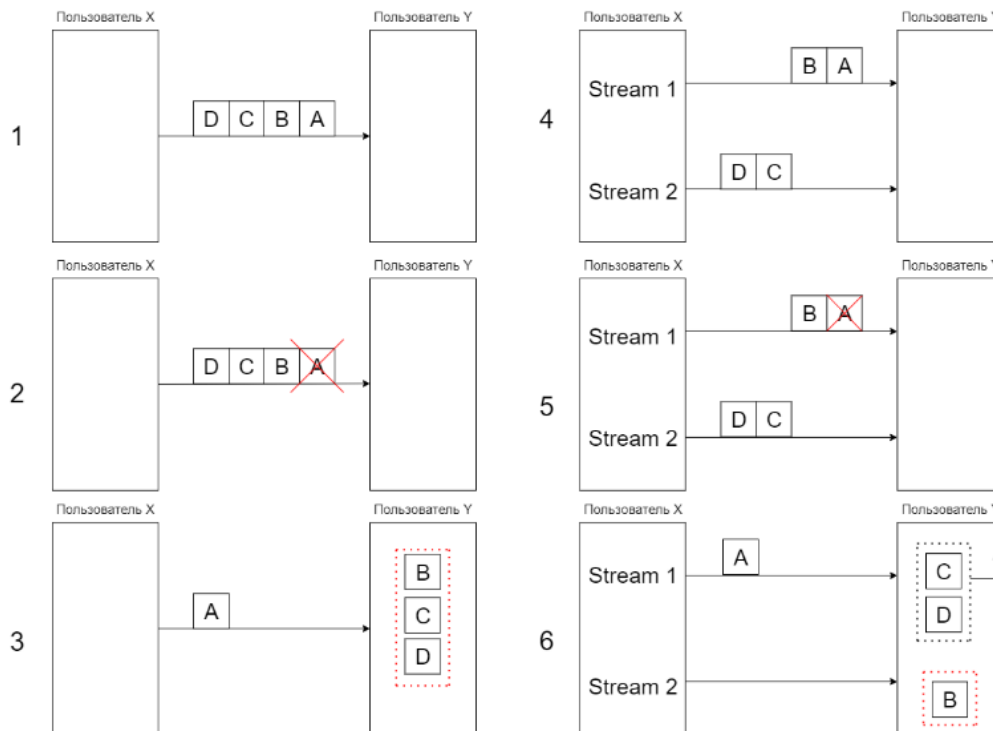


Рис. 1. Сравнение передачи данных TCP и SCTP с использованием нескольких потоков

Пользователь X посылает четыре сообщения (A, B, C, D) пользователю Y. Есть два требования относительно порядка доставки этих сообщений. Сообщение A должно быть доставлено раньше сообщения B, а сообщение C должно быть доставлено до сообщения D. В TCP сообщения отправляются в следующем порядке: A, B, C, D (1). Если сообщение A потеряно (2), другие сообщения, несмотря на правильный прием, не могут быть отправлены на верхний уровень, пока сообщение A не будет повторно передано и успешно получено пользователем Y (3). В SCTP, использующем многопоточность, сообщения могут быть разделены на два потока. Сообщения A и B могут быть отправлены в потоке 1, а сообщения C и D могут быть отправлены в потоке 2 (4). Если сообщение A потеряно (5), только сообщение B не может быть передано на верхний уровень, пока не будет получено сообщение A. Сообщения C и D могут быть доставлены на верхний уровень, поскольку они отправлены в другом потоке, чем сообщения A и B (6).

Еще одной особенностью SCTP является возможность расширения протокола. Каждый пакет SCTP состоит из основного заголовка и одного или нескольких блоков (рис. 2).

Заголовок
Чанк 1
Чанк 2
...
Чанк n

Рис. 2. Формат пакета SCTP

Существует два типа чанков: чанки данных, которые содержат пользовательские данные, и управляющие чанки, которые используются для управления передачей данных. Каждый чанк состоит из полей и параметров, характерных для типа чанка (рис. 3). Поля являются обязательными, а параметры могут быть как обязательными, так и необязательными. Структура пакета SCTP позволяет определять не только новые типы чанков, но и расширять функциональность существующих типов чанков за счет определения новых параметров.

Тип чанка	Флаг чанка	Длина чанка
Данные чанка		
Параметры		Длина параметров
Значение параметров		

Рис. 3. Формат фрагментов и параметров SCTP

SCTP поддерживает мультинаведение, т.е. способность хоста быть видимым в сети через более чем один IP-адрес, например, если хост оснащен несколькими сетевыми картами (NIC). Мультинаведение в SCTP используется для обеспечения более надежной передачи данных. Если нет потерь пакетов, все сообщения передаются с использованием одного адреса источника и одного адреса назначения (первичный путь). Если пакет передается повторно, он должен быть отправлен по другому пути (по другим адресам источника и назначения), чем первичный путь. Еще одним преимуществом мультинаведения в SCTP является возможность отказоустойчивой передачи данных, если первичный путь не работает. SCTP использует четырехстороннее рукопожатие с cookie, что обеспечивает защиту от атаки синхронизации (тип атаки "Отказ в обслуживании"), известной из TCP. Помимо описанных возможностей, SCTP обеспечивает встроенное обнаружение MTU пути, механизм фрагментации данных и, в целом, считается более безопасным, чем TCP.

Специфические для SCTP стеганографические методы можно разделить на три группы:

- Методы, изменяющие содержимое SCTP-пакетов;
- Методы, изменяющие способ передачи пакетов SCTP;
- Методы, которые изменяют как содержимое SCTP, так и способ обмена - гибридные методы.

Методы, изменяющие содержимое пакетов SCTP. Каждый пакет SCTP состоит из чанков, и каждый чанк может содержать переменные параметры. Далее представлены стеганографические методы, которые изменяют содержимое SCTP-пакетов в следующих кусках и параметры:

1. Чанки INIT и INIT ACK - используются во время инициализации SCTP ассоциации;
2. DATA чанки - которые содержат пользовательские данные;
3. SACK чанки - используются для подтверждения полученных DATA чанков;
4. Чанк AUTH - используется для аутентификации чанков;
5. Чанк PAD - используется для заполнения пакетов;
6. Переменные параметры - используются в определенных чанках.

Методы, изменяющие способ обмена пакетами SCTP. MULTI-HOMING или функция мультинаведения SCTP может быть использована для осуществления скрытой связи. Суть реализации этого метода заключается в наличии двух пользователей, имеющих несколько сетевых карт. Если пользователь 1 хочет отправить стеганограмму, он ждет, пока произойдет ошибка передачи на основном пути, а затем повторно передает чанк через другой путь. Перед отправкой стеганограммы необходимо установить, какие из ретранслированных пакетов несут скрытые данные. Пользователи могут предположить, что все ретрансляции несут биты стеганограммы, или должны отметить начало скрытой коммуникации, например, последовательностью инициации (последовательность ретранслируемых пакетов по заранее согласованным путям).

Многопоточная передача в SCTP реализуется с помощью двух идентификаторов: Stream Identifier (SI) для уникальной маркировки потока и Stream Sequence Number (SSN) для обеспечения правильного порядка пакетов в приемнике. Несмотря на эти два идентификатора, каждый чанк DATA содержит также номер последовательности передачи (TSN), который присваивается каждому чанку независимо. Стеганографический метод, использующий многопоточную передачу, основан на определенном назначении TSN для каждого куска, распределенного по разным потокам. SI в последующих DATA-кусках будут представлять скрытые биты данных.

Гибридный метод реализуется в протоколе SCTP при помощи отказа от передачи повторно определенных данных. Это возможно через чанк FORWARD TSN (FT), в который вставляется новое подтверждение TSN. После получения такого сообщения принимающая сторона рассматривает недостающие фрагменты с равными или меньшими TSN как правильно доставленные. Идея предлагаемого метода схожа по концепции с LACK, который был разработан для мультимедийных услуг реального времени Мазурчиком и Щипиорски [9].

Таким образом, можно сделать вывод, что протокол SCTP предоставляет пользователю достаточно возможностей для передачи стеганографических сообщений.

Список используемых источников:

1. Роулэнд К., "Скрытые каналы в пакете протоколов TCP/IP" // Первый понедельник, рецензируемый журнал об Интернете, 1997
2. Мердок С. Дж., Льюис С., Встраивание скрытых каналов в TCP/IP. Скрытие информации. 2005. С. 247
3. Зандер С., Г. Армитаж, П. Бранч, "Обзор скрытых каналов и контрмер в протоколах компьютерных сетей" IEEE Communications Surveys & Tutorials. 2007. V. 9. Issue 3, P. 44-57. ISSN: 1553-877X
4. Petitcolas F., Anderson R., Kuhn M., Information Hiding - A Survey: Специальный выпуск IEEE по защите мультимедийного контента, июль 1999 г.
5. Стюарт Р.: Протокол передачи управления потоком. RFC 4960, 2007 г.
6. Стюарт Р, Кси Кью.: Stream Control Transmission Protocol (SCTP): Справочное руководство. Addison-Wesley, 2002 г
7. Стюарт Р., Рамальхо М., Кси Кью., Конрад П.: Расширение частичной надежности протокола передачи управления потоком (SCTP). RFC 3758, 2004 г.
8. Щипиорски К., Стеганография в сетях TCP/IP. Состояние техники и предложение новой системы - HSCUPS, семинар Института телекоммуникаций, Варшавский технологический университет, Польша, 2003 г
9. Мазурчик В, Щипиорски К (2008) Стеганография потоков VoIP, в: Р. Меерсман и З. Tari (ред.): OTM 2008, Часть II - Конспекты лекций по информатике (LNCS) 5332, Springer-Verlag Berlin Heidelberg, Материалы 3-го Международного симпозиума по информационной безопасности (IS'08), Монтеррей, Мексика, 2008, стр. 1001-1018

Masyutin M., Salita A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Steganographic investments in "STREAM CONTROL TRANSMISSION PROTOCOL". SCTP is a new transport layer protocol to replace TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) in future IP networks. SCTP is a new transport layer protocol to replace TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) in future IP networks. It is currently implemented in operating systems such as BSD, Linux, HPUX or Sun Solaris. It is also supported in Cisco networking devices (Cisco IOS) and may be used in Windows operating systems. This article describes potential steganographic techniques that can be applied to SCTP and may pose a threat to network security.

Key words: *SCTP, steganography, networks, information security.*

УДК 004.056
ГРНТИ 81.93.29

УЯЗВИМОСТИ ИОТ-УСТРОЙСТВ ПОД УПРАВЛЕНИЕМ ОС LINUX

А. Д. Нагаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Идея интернета вещей играет ключевую роль в развитии ИТ индустрии по всему миру. Сфера применения интернета вещей очень широка. Она упрощает нашу жизнь и позволяет автоматизировать необходимые процессы. Именно поэтому возрастают и угрозы обеспечения информационной безопасности при передачи данных IoT-устройствами. Основными целями исследования являются выявление различного рода уязвимостей IoT-устройств, функционирующих на ОС Linux, и представление рисков для их пользователей.

интернет вещей, несанкционированные воздействия, защита информации, информационная безопасность

IoT - это широко используемый термин для обозначения набора технологий, систем и принципов проектирования, связанных с появляющейся волной подключенных к Интернету устройств, которые основаны на физической среде. [1]. Применение Интернета вещей безгранично. IoT-решения закрывают пробелы в различных индустриях и сферах жизни. Данные технологии позволяют с помощью интеллектуальных возможностей оптимизировать бизнес процессы компаний и облегчать жизнедеятельность пользователей. Ожидается, что рынок IoT вырастет до более чем 75 миллиардов устройств в 2025 году [2].

Рост IoT создает большие риски безопасности для их пользователей. С увеличением подключений устройств между собой появится и проблема их защиты. Всё оборудование, используемое ПО и подключение должны быть защищены для эффективной работы IoT. Без должного уделения внимания защите IoT любой объект, от бытовых устройств до производственных механизмов, может быть взломан. При получении контроля над функциональностью злоумышленники могут украсть цифровые данные пользователя с дальнейшим материальным или финансовый ущербом для пользователя. Самая высокая оценка риска связана с кибер-или информационными активами, такими как учетные данные пользователей, мобильные персональные данные и приложения пользователей [3].

Linux является наиболее распространенным компонентом: более 90% облачных рабочих нагрузок и 70% веб-серверов работают на нем.

По данным отчета SophosLabs за 2016 год, подразделения по анализу угроз производителя средств информационной безопасности Sophos, частота и сложность вредоносных программ для Linux росли с каждым годом. [4].

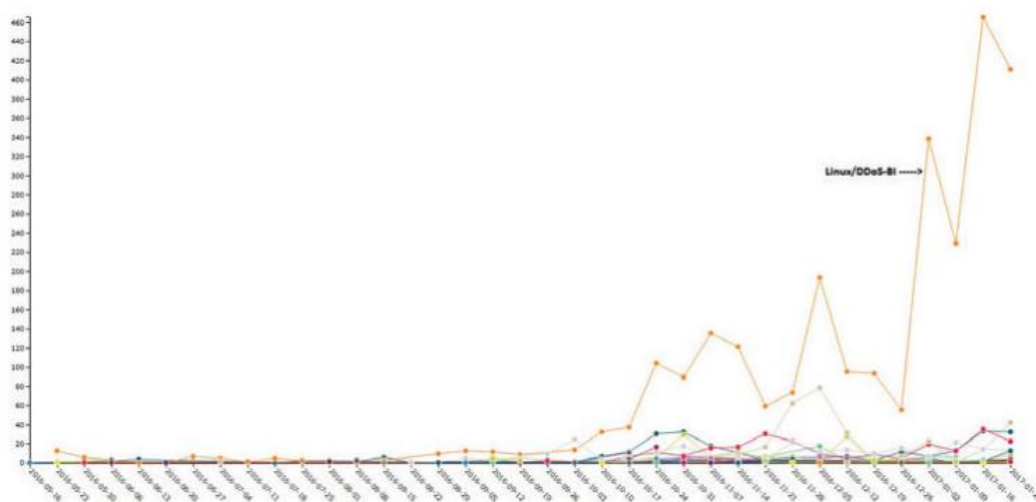


Рис. 1. Рост применения вредоносных программ для Linux

Согласно отчету CrowdStrike, в 2021 году количество вредоносных программ, нацеленных на устройства на базе ОС Linux, выросло на 35% по сравнению с прошлым годом, а семейства XorDDoS, Mirai и Mozi ответственны за 22% всех вредоносных программ для Интернета вещей на базе Linux.

На сегодняшний день можем выделить основные угрозы IoT-устройств на базе ОС Linux.

XorDdos известен тем, что использует атаки грубой силы Secure Shell (SSH) для получения удаленного контроля над целевыми устройствами. Как только XorDdos идентифицирует действительные учетные данные SSH, он использует привилегии root для запуска сценария, который загружает и устанавливает XorDdos на целевом устройстве. XorDdos использует механизмы уклонения, которые позволяют его операциям оставаться незаметными. Его возможности уклонения включают в себя запутывание действий вредоносных программ, обход механизмов обнаружения на основе правил и поиск вредоносных файлов на основе хэшей. XorDdos скрывает вредоносные действия от анализа, перезаписывая конфиденциальные файлы нулевым байтом.

Mirai был создан с использованием двоичных файлов ELF (Executable and Linkable Format), распространенного формата файлов для систем на базе Linux и UNIX. Этот формат используется в прошивке многих устройств IoT, включая маршрутизаторы, цифровые видеорегистраторы и IP-камеры. Mirai нацелен на сетевые протоколы SSH или Telnet, используя стандартные учетные данные для компрометации устройств на базе Linux. Mirai также шифрует трафик, который проходит между зараженными устройствами и серверами, используемыми для выдачи команд зараженных устройств, чтобы предотвратить мониторинг.

Mozi — это одноранговый (P2P) ботнет, использующая систему распределенной хеш-таблицы (DHT) для реализации собственного расширенного DHT. механизм распределенного децентрализованного поиска, предоставляемый DHT, позволяет Mozi скрывать трафик C2 за большим объемом законного трафика DHT. DHT позволяет Mozi быстро развивать сеть P2P. Кроме того, поскольку он использует расширение DHT, он не связан с обычным трафиком,

что затрудняет обнаружение трафика C2. Mozi заражает системы, взламывая порты SSH и Telnet. Затем он блокирует эти порты, чтобы они не были перезаписаны другими злоумышленниками или вредоносными программами.

Для дальнейшего рассмотрения предотвращения уязвимостей, необходимо их классифицировать. [5]

ТАБЛИЦА 1. Классификация уязвимостей безопасности

Категория	Угрозы безопасности	Уязвимости системы
Конфиденциальность	Прослушивание данных, атака «человек посередине», сниффинг	Утечка конфиденциальных данных
	Зомби-устройства, атаки типа «отказ в обслуживании» (DDoS), фишинг, фарминг	Утечка пользовательских данных, Вторичный ущерб, вызванный заражением вредоносным ПО
	Атаки с использованием уязвимости веб-интерфейса	Данные и захват контроля над устройством
	Неправильное обновление программы, аппаратный интерфейс и физическое поглощение флэш памяти	Захват привилегий администратора
Целостность	Прослушивание данных, атака «человек посередине», незаконная модификация сообщений	Утечка конфиденциальных данных
	Атаки на интерфейсы и системы уязвимости посредством незаконного проникновения к доступу	Захват прав доступа к прошивке и операционной системе
Доступность	Заражение вредоносным программным обеспечением	Нарушение исправности
	Физическое удаление и уничтожение данных	Захват устройств и данных
	Постоянные попытки атак на контроль над доступом, атака отказа в обслуживании	Исправная работа системы
	Потеря или кража устройств и данных	Захват устройств и данных
	Смишинг атака сетевых платформ	Заражение вредоносным ПО
Аутентификация/авторизация	Неавторизованный пользователь и несанкционированный доступ	Устройства доступа
	Устройство репликация, изменение, присвоение данных	Захват устройств и данных

Исходя из данной классификации, можем выделить основные требования для обеспечения безопасности:

Конфиденциальность

– Сообщения, передаваемые между устройствами IoT, должны передаваться в зашифрованном виде для предотвращения незаконного прослушивания или перехвата.

– IoT-устройства должны обеспечивать возможность обнаружения и защиты от заражения вредоносным ПО, чтобы предотвратить утечку информации.

Целостность

– Когда питание впервые подается на устройство, IoT-устройства должны обеспечивать функцию безопасной загрузки, чтобы гарантировать надежность устройства за счет подлинности и целостности программного обеспечения.

Доступность

– IoT-устройство должно обеспечивать соответствующую функцию ведения журнала для пользователя, системы, события безопасности.

– IoT-устройство должно обеспечивать возможность реагирования на внешние атаки, такие как атаки типа "отказ в обслуживании" и атаки с постоянными попытками установить соединение.

– IoT-устройство должно обеспечивать безопасное и надежное обновление программного обеспечения. Надежность системы обновления имеет решающее значение.

– IoT-устройства должны обеспечивать безопасность программного обеспечения с помощью функции ограничения доступа, несмотря на сбой или неисправность программного обеспечения из-за заражения вредоносным ПО.

Аутентификация/авторизация

– IoT-устройство устанавливает безопасный и надежный пароль и должно обеспечивать функцию периодического обновления.

– IoT-устройство должно обеспечивать взаимную аутентификацию между устройствами для создания безопасной, автономной среды связи.

– IoT-устройство должно обеспечивать функции контроля полномочий, такие как контроль прав для предотвращения утечки информации и защиты конфиденциальности.

В данной статье были представлены наиболее опасные уязвимости устройств IoT на базе ОС Linux и методы их предотвращения. Также была произведена классификация уязвимостей в целях категоризации решений и требований безопасности к различным классам устройств IoT. Уязвимости IoT-устройств несут за собой большие риски для безопасности данных. По мере увеличения объема хранимых и создаваемых данных возрастает и важность их защиты. В случае их утечки угрозе подвергнутся конфиденциальные данные пользователей. Утечки данных могут привести к разрушительным последствиям, в связи с этим пользователи и производители IoT-устройств должны уделять большое внимание их защите.

Список используемых источников:

1. Holler, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Avesand, S., Boyle, D. From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence // Elsevier, 1st edn. 2014. С. 14.
2. В. Фридман. (2018) На грани: решение проблем граничных вычислений в эпоху Интернета вещей [Электронный ресурс] // <https://data-economy.com/on-the-edge-solving-the-challenges-of-edge-computing-in-the-era-of-iot/>
3. Гельфанд А. М., Казанцев А. А., А. В. Красов, Орлов Г. А. Оценка рисков и угроз безопасности в среде «умный дом» // Апино. 2020. С.316-320.
4. Looking ahead: SophosLabs 2017 malware forecast. С. 3-4.
5. Yoon S., Jeongnyeo K., Yongsung J. Security considerations based on classification of IoT device capabilities. 2017. С. 14.

Nagaeva A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Vulnerabilities of IoT devices running linux OS.

The idea of the Internet of Things plays a key role in the development of the IT industry around the world. The scope of the Internet of things is very wide. It simplifies our lives and allows us to automate the necessary processes. That is why the threats to information security in the transmission of data by IoT devices are also increasing. The main objectives of the study are to identify various kinds of vulnerabilities in IoT devices operating on the Linux OS and present the risks for their users.

Key words: Internet of Things, unauthorized influences, information protection, information security.

УДК 004.056.2
ГРНТИ 81.93.29

МЕТОДЫ ВНЕДРЕНИЯ САМОМОДИФИЦИРУЮЩЕГОСЯ КОДА В ИСПОЛНЯЕМЫЕ ФАЙЛЫ PE-ФОРМАТА

В. В. Нефедов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире большое количество пользователей используют устройства на базе операционных систем Windows и Linux. Любая операционная система требует дополнительных специальных средств защиты информации помимо тех, которые имеются в стандартном наборе операционной системы. В дополнение к имеющимся средствам защиты информации имеется возможность использовать самомодифицирующийся код, внедренный в исполняемые файлы [1]. Существует популярное мнение, что самомодифицирующийся код используется в качестве атакующего инструмента. Попадая в систему жертвы код в зараженном файле самостоятельно модифицировался, заставляя программу работать некорректно, но это можно использовать и в целях защиты информации.

самомодифицирующийся код, исполняемые файлы, PE-файлы, внедрение кода

Первым делом возникает вопрос: куда внедрять самомодифицирующийся код? В данной работе были рассмотрены методы внедрения самомодифицирующегося кода в исполняемые файлы PE-формата.

Исполняемый файл состоит из двух основных частей:

- Заголовки;
- Секции.

Заголовки содержат в себе технические детали об исполняемом файле (необходимые данные для загрузки программы), а секции – «начинку» исполняемого файла (код, виртуальные адреса функций, ресурсы и т.д.) [2].

Подробнее остановимся на заголовках исполняемых файлов.

DOS-заголовок. Данный заголовок, как и любой другой, состоит из множества полей, каждое поле хранит в себе определенное значение. Остановимся только на тех полях, которые необходимы для запуска исполняемого файла.

PE-заголовок. Данный заголовок состоит из трех частей: сигнатуры PE-заголовка, файлового заголовка и опционального заголовка. Каждая часть также состоит как минимум из одного поля [3].

Начнем с сигнатуры PE-заголовка. Данное четырехбайтовое поле является началом всего PE-заголовка и содержит в себе сигнатуру 50 45 00 00 («PE/x00/x00»), указывающую на то, что это действительно PE-файл.

Далее рассмотрим файловый заголовок. В нем хранятся базовые характеристики исполняемого файла.

Оptionальный подзаголовок является завершающим в PE-заголовке. В нем находится необходимая информация для запуска PE-файла [4].

Таблица секций. Завершающий заголовок, в котором хранится различная информация о секциях исполняемого файла.

После того, как были рассмотрены основные моменты, касающиеся структуры PE-файла, можно переходить к непосредственному рассмотрению наиболее популярных методов вложения в исполняемые файлы PE-формата.

1. Расширение заголовка. Важно понимать, что расширение заголовка является сложной задачей и вызывает большое количество трудностей, для решения которых приходится изменять структуру файла-носителя. Например, необходимо увеличить физический адрес начала всех секций до величины, кратной степени выравнивания, а также физически перенести конец файла, поместив тело внедряемого кода в образовавшееся место [5].

На рис. 4 приведена упрощенная схема, визуальную показывающую то, как происходит вложение кода с помощью расширения заголовка файла.

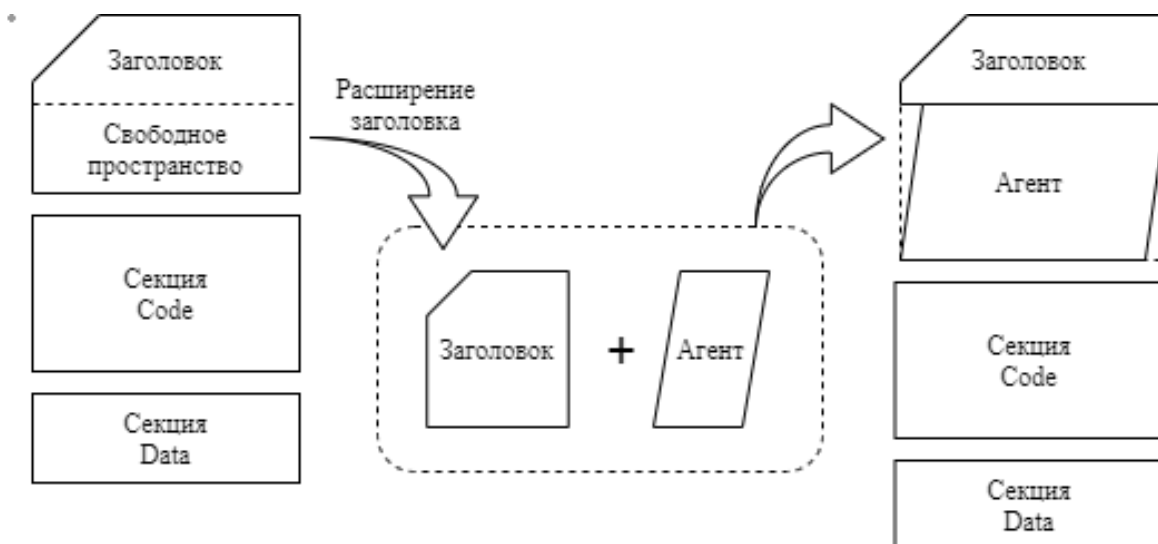


Рис. 1. Вложение кода с помощью расширения заголовка

Далее стоит обратиться к схеме, изображенной на рис. 5, на ней показан алгоритм, которому стоит придерживаться при осуществлении вложения внедряемого кода с помощью расширения заголовка.

Для начала стоит выяснить, присутствуют ли в DATA DIRECTORY структуры, которые привязаны к своему физическому смещению. Если же такие структуры есть, то придется сделать выбор: осуществить вложение, но вручную корректировать структуры, или же отказаться от вложения. Далее нужно проверить, равен ли размер заголовка виртуальному адресу первой секции, если равен, то отказываемся от вложения, так как вкладывать банально некуда, если же не равен, то нужно убедиться, что файл-носитель не содержит оверлей, так как после вложения в такой файл, он может перестать функционировать [6].

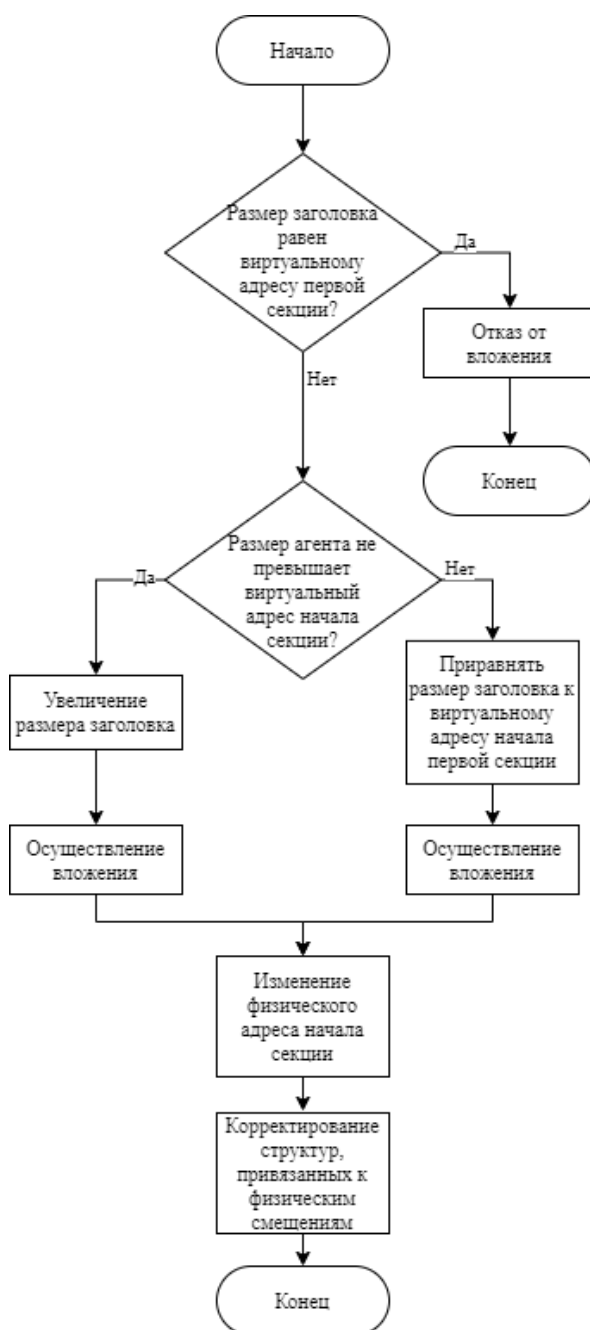


Рис. 2. Алгоритм вложения кода с помощью расширения заголовка

Следующим шагом следует проверить, меньше ли размер внедряемого кода виртуального адреса начала секции. Если да, то увеличиваем размер заголовка и добавляем необходимое количество байт (не стоит забывать про выравнивание) между концом заголовка и началом секции. Если же нет, то приравниваем размер заголовка к виртуальному адресу начала секции, после чего добавляем часть тела внедряемого кода в образовавшееся пространство. Важно понимать, что в таком случае системный загрузчик спроецирует только часть тела внедряемого кода, а все последующее ему придется подгружать самостоятельно.

Далее нужно увеличить физический адрес начала секции на величину физического расширения файла. После чего по необходимости привести в

порядок все структуры, которые привязаны к физическим смещениям внутри файла.

Список используемых источников:

1. Штеренберг С.И. Анализ работы алгоритмов защиты информации на основе самомодифицирующегося кода с применением стеговложений. // H&ES Research. – 2016. – № 2 – С. 86-90.
2. Исследуем Portable Executable (EXE-файл) [Формат PE-фала] [электронный ресурс] // CODEBY.NET. М., 2010 – 2021. URL: <https://codeby.net/threads/0x01-issleduem-portable-executable-exe-fajl-format-pe-fajla.65415/>
3. IMAGE_NT_HEADERS structure (winnt.h) [электронный ресурс] // Microsoft. М., 2021. URL: https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_nt_headers32
4. IMAGE_FILE_HEADER32 structure (winnt.h) [электронный ресурс] // Microsoft. М., 2021. URL: https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_optional_header32
5. Трегубенко В.В. ZeroAccess: полная биография // Хакер. 2013. №171.
6. Техника внедрения кода в PE-файлы и методы его удаления [Электронный ресурс] // URL: https://konyakov.ru/pubs/books/kris-kaspersky-r_i_p/kris-kaspersky-16.pdf

Nefedov V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Self-Defying Code Injection Methods into re-format executable files.

In the modern world, a large number of users use devices based on Windows and Linux operating systems. Any operating system requires additional special information security tools in addition to those that are available in the standard set of the operating system. In addition to the available information security tools, it is possible to use self-modifying code embedded in executable files [1]. There is a popular opinion that self-modifying code is used as an attacking tool. Getting into the victim's system, the code in the infected file was independently modified, forcing the program to work incorrectly, but this can also be used to protect information.

Key words: *self-modifying code, executable files, PE files, code injection.*

УДК 004.056
ГРНТИ 49.33.35

МОДЕЛИ И АЛГОРИТМЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРОЦЕССОВ DevSecOps

Е. А. Паршин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время Рынок переживает переломный момент, и предприятия ищут решения, позволяющие свести к минимуму время, необходимое для качественной разработки. При этом мир охватила волна огромная киберпреступлений, влекущая за собой огромные потери для корпораций. Это привело к мысли прибегнуть к DevSecOps. DevSecOps – это расширение DevOps, которое рассматривается как средство для объединения разработки, эксплуатации и безопасности. Некоторые компании, заботящиеся о безопасности, начинают принимать во внимание DevSecOps, когда речь идет о применении DevOps. В докладе рассмотрен процесс DevSecOps, как эффективная безопасная разработка. Приведены примеры статистики эффективной работы процессов DevSecOps и варианты решения

DevSecOps, Информационная безопасность, безопасная разработка, DevOps

«DevOps» - это сокращенная форма слова Development Operations. DevOps объясняет процедуры для ускорения процессов от разработки приложения до развертывания в производственном цикле. В коллективной модели DevOps безопасность предполагалась, но на практике численность комнаты безопасности была мала, и они играли роль надзорного органа, а не участника цепочки создания продукта, который выставлял требования и проверяли качество продукта. Основной проблемой такой разработки являлось то, что сотрудники отдела безопасности имели некоторое программное обеспечение, получали продукт или его код раз в полгода, а то и реже. Во время автоматического тестирования выявлялось большое количество уязвимостей, они отправлялись обратно разработчикам, которые принимались устранять их, выпуск продукта сдвигался, разработка затягивалась. Это привело некоторых к мысли придумать термин «DevSecOps» (рис. 1), чтобы подчеркнуть необходимость создания фронта безопасности во время работы DevOps. Одна из основных целей DevSecOps - автоматизация безопасности, направленной на формирование культуры «Безопасность как код», таким образом продвижение синергии между разработчиками и командой безопасности. Это решает задачи безопасности на протяжении жизненного цикла разработки программного обеспечения.

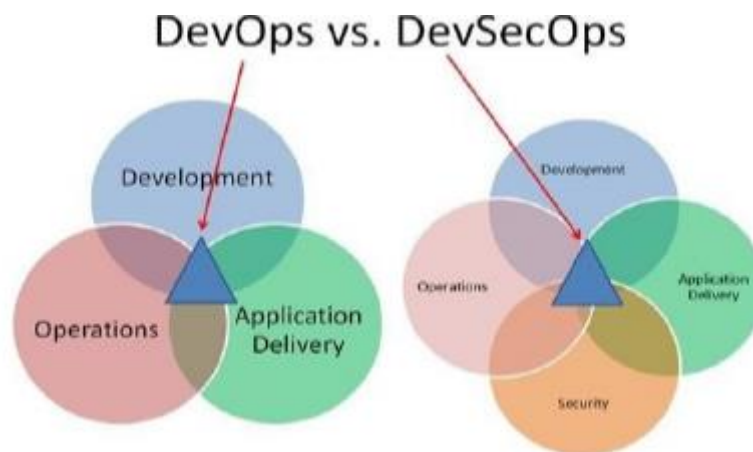


Рис. 1. Сравнение DevOps и DevSecOps

Подход DevSecOps включает 5 основных принципов, обеспечивающих эффективный процесс.

- A. Улучшение взаимодействия
- B. Повышение безопасности
- C. Непрерывное обучение
- D. Обмен информацией об угрозах
- E. Поощрение открытого сотрудничества

Предприятия думают о гибкой безопасности, и 88 [1] процентов респондентов заявили, что интеграция безопасности в DevOps в некоторой степени чрезвычайно важна. Они опасаются, что невыполнение этого требования приведет к проблемам, в том числе:

- Увеличение затрат (78 процентов)
- Более медленная доставка приложений (73 процента)
- Повышенные риски безопасности (71 процент)
- Респонденты также признают, что это непростой процесс, хотя препятствия различаются в зависимости от того, где находится организация.

Рассмотрим инструменты DevSecOps:

Jenkins предоставляет простой и легкий способ к среде непрерывной доставки (CD) и непрерывной интеграции (CI) практически для любого сочетания языков. Jenkins достигает непрерывной интеграции с помощью плагинов. Это позволяет интегрировать различные этапы DevOps [2].

SonarQube- это инструмент, который упрощает интеграцию результатов или статистики в конвейер сборки. Он используется для непрерывной проверки качества кода и руководства разработчиками при проверке кода.

Проверка зависимостей OWASP - Это инструмент, который распознает зависимости проекта и определяет наличие уязвимостей любого типа. Этот плагин может независимо выполнять исследование Dependency Check и наблюдать за результатами.

Docker - Это утилита, используемая для сборки, развертывания и запуска проекта через контейнеры. Это виртуальная машина, но она не похожа на виртуальные машины, на которых построена совершенно отдельная операционная система.

Это позволяет программам использовать ядро Linux той самой машины, на которой оно установлено, и, пользуясь этим преимуществом, может привести к тому, что программы будут готовы к отправке на другие машины, которые работают под той же ОС Linux с разными конфигурациями.

Отдельные предприятия уже смогли достигнуть успехов, связывая команды разработчиков и безопасников, уменьшая циклы обратной связи, минимизируя киберинциденты и повышая безопасность через общую ответственность. Райан О’Лири, главный специалист по исследованиям в области безопасности в White Hat, утверждает [3], что подобный путь помогает огромному числу компаний быстро реализовать безопасный код. По данным О’Лири, обыкновенный срок, требуемый для устранения уязвимости при применении динамического анализа в производстве, является 174 дня. Хотя организации, которые ввели DevSecOps, устраняют бреши за 92 дня. Что касается статического анализа — обычная организация исправляет бреши за 113 дней; а при использовании DevSecOps — всего за 51 день. достаточно сильная разница. Обычная фирма имеет 15 % уязвимостей от общей численности найденных проблем безопасности, ликвидированных за 10 дней, компании, использующие DevSecOps — устраняют 53 % проблем за 10 дней. В опубликованном отчете [4] DigiCert утверждается, что 98 % из 300 анкетированных фирм Соединённых Штатов заявили, что намереваются интегрировать безопасность в DevOps, или уже сделали это. Однако для похожей интеграции имеется препятствие. Специалисты обращают внимание на то, что DevOps и DevSecOps имеют разные операционные модели и задачи, на данном этапе существуют разногласия относительно ответственности разработчиков и недостатков навыков для решения задач.

Мы обнаружили, что DevSecOps определяется многими как интеграция процессов и практик безопасности в среды DevOps, что DevSecOps продвигает набор принципов, призванных изменить мышление всех участников процесса разработки программного обеспечения, чтобы все участвовали и делали все возможное, чтобы гарантировать безопасность в проекте, которые могут обеспечить безопасность в проекте, основанные на идее планирования и реализации безопасности с самого начала.

Выявленные нами преимущества указывают на то, что DevSecOps развивается, приводя к сокращению внеплановой работы и уменьшению ручного труда.

Список используемых источников:

1. Состояние DevOps в России: [Электронный ресурс]. М., 2021. URL: <https://habr.com/ru/company/oleg-bunin/blog/524556/> (Дата обращения 20.11.21)
2. What is Jenkins? The CI server explained: [Электронный ресурс]. 2020. URL: <https://www.infoworld.com/article/3239666/what-is-jenkins-the-ci-server-explained.html> (Дата обращения 18.11.21)
3. DigiCert Survey Shows Enterprises Integrating Security Teams into DevOps: [Электронный ресурс]. 2017. URL: <https://www.digicert.com/news/pr/survey-integrating-security-into-devops/> (Дата обращения 18.11.21)

4. Утечки данных: ущерб и борьба российских компаний: [Электронный ресурс] // Softline - IT-решения для бизнеса. М., 2018. URL: <https://softline.ru/about/news/utechki-dannyih-uscherb-i-borba-rossiyskih-kompaniy> (Дата обращения 21.11.21)
5. Дэвис Д. Философия DevOps. Искусство управления IT. СПб. : ПИТЕР, 2017 416 с.
6. Форсгрэн Н., Хамбл Д., Ким Д. Ускоряйся! Наука DevOps : Как создавать и масштабировать высокопроизводительные цифровые организации. М. : Интеллектуальная литература, 2020. 216 с.

Parshin E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Models and algorithms for evaluating the effectiveness of DevSecOps processes.

The market is currently at a tipping point and businesses are looking for solutions to minimize the time required for quality development. At the same time, a huge wave of cybercrimes swept the world, entailing huge losses for corporations. This led to the idea of resorting to DevSecOps. DevSecOps is an extension of DevOps that is seen as a vehicle for integrating development, operations, and security. Some security companies are starting to take DevSecOps into account when it comes to implementing DevOps. The report discusses the DevSecOps process as an effective secure development. Examples of statistics of effective work of DevSecops processes and solutions are given.

Key words: *DevSecOps, Information security, secure development, DevOps.*

УДК 004.772
ГРНТИ 49.38.49

ОРГАНИЗАЦИЯ СТЕГАНОГРАФИЧЕСКИХ КАНАЛОВ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА HTTP

Н. В. Паскидов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На сегодняшний день набирают популярность технологии обеспечения конфиденциальности при использовании сети «Интернет». Наиболее популярный способ обеспечения конфиденциальности – криптография. Данная технология позволяет ограничить доступ к информации путём шифрования данных, однако имеет ряд недостатков и ограничений. Ввиду существования данных изъянов набирают популярность методы стеганографии. В данной статье рассматривается возможность использования стеганографии в Hypertext Transfer Protocol.

HTTP, информационная безопасность, сетевая стеганография, канальная стеганография, сокрытие информации, защита информации

Сетевая стеганография — раздел стеганографии, науки о защите информации использующей различные методы для сокрытия конфиденциальных данных внутри общедоступных данных [1]. Сетевая стеганография использует различные сетевые протоколы в качестве носителей, тем самым обеспечивая сокрытие факта наличия скрытой информации от сетевых устройств. Основа сетевой стеганографии — это построение скрытых каналов связи. Данные каналы могут использоваться для проведения атак на сети организаций, для удалённого управления заражённых хостов или для передачи конфиденциальной информации злоумышленниками. Методы сетевой стеганографии обычно разделяют на три основные группы по способу создания стеганографического канала [2].

К первой группе относятся методы, изменяющие содержимое сетевых пакетов интернет-протоколов. С помощью изменения содержимого некоторых полей заголовков пакетов или полезной нагрузки становится возможным вложение определенной информации.

Вторая группа включает в себе технологии, позволяющие изменять структуру передачи пакетов. Данные технологии достаточно сложны в реализации и обладают низкой полосой пропускания, но при этом детектирование таких систем затруднено.

Третья группа сочетает в себе различные методы организации скрытых каналов из двух предыдущих групп. Здесь может одновременно вкладываться информация в заголовки пакетов, а затем меняться порядок их передачи и интервалы задержки [3,4].

Для организации стеганографического канала необходимо выбрать метод, с помощью которого будет скрываться информация, а также так называемый контейнер, или покрывающий объект, внутрь которого будут помещаться

данные. На текущий момент существует большое число исследований, посвящённых вложениям в различные сетевые протоколы. В данной работе будет рассмотрена возможность сокрытия данных с использованием протокола передачи гипертекстовых документов HTTP.

Согласно модели OSI, HTTP является протоколом седьмого (прикладного) уровня. Данный протокол работает по клиент-серверной модели, итоговым результатом для клиента обычно является гипертекстовый документ, полученный в результате ответа на запросы к серверной стороне.

Любой запрос, осуществляемый по протоколу HTTP состоит из трех частей:

1. Стартовая строка – поле, определяющее тип сообщения. В ней указывается тип запроса; путь, по которому находится запрашиваемый документ (URI); используемая версия протокола.

2. Заголовок – набор строк, содержащий информацию о браузере клиента, сервере к которому происходит обращение, запрашиваемой странице и прочем.

3. Тело сообщения – поле, используемое для передачи тела объекта, например HTML страницы.

Формат данных значений регламентирован согласно [5], однако интересно, что отсутствуют ограничения на размеры URI строки, тела сообщения и заголовка. Несмотря на ограничения различных серверных реализаций, данные уязвимости подходят для создания скрытых каналов. Далее будут рассмотрены способы организации скрытых каналов.

Один из способов заключается в использовании DATA-фреймов в качестве стекоконтейнера. В HTTP/2 в целях безопасности для сокрытия размера сообщения используется заполнение кадров DATA, PUSH PROMISE и HEADERS. Согласно [6], при передаче запроса посредники должны сохранять заполнение для кадров DATA, но при этом могут удалять отступы для HEADERS и PUSH PROMISE. Исходя из этого можно считать что кадры DATA при передаче изменяться не будут, что можно использовать в качестве контейнера для скрытых данных.

Второй способ заключается в использовании кадров PING. Данные кадры используются для определения состояния установленной HTTP-сессии, а также для измерения минимального пути до отправителя. В случае если соединение активно, данный кадр должен быть подтверждён ответным кадром PING с установленным флагом ACK с идентичной по размеру полезной нагрузкой и с более высоким приоритетом. Полезной нагрузкой кадра может быть любое 64-битное число. Используя данный факт можно создать скрытый канал, обмениваясь кадрами PING с нужной полезной нагрузкой.

Третий способ заключается в использовании потоков с назначением приоритетов. HTTP/2 использует потоки с назначением приоритетов или без них, что делает их зависимыми или не зависящими от других потоков. При ограниченной возможности отправки отправитель сделает выбор потока для передачи кадра, исходя из приоритетов. Обычно каждой зависимости присваивается вес от 1 до 256. Открытие потока осуществляется кадром HEADERS, который дополнительно может назначить приоритет потоку. После

этого приоритет данного потока может быть изменен в любое время кадром PRIORITY.

Для новых каналов подробности о расстановке приоритетов и зависимостях не важны. Важно только то, что процесс приоритизации является только рекомендательным, а не обязательным. То есть нет никакой гарантии, что он будет выполнен. Таким образом, появляется возможность использовать приоритизацию для создания стеганографических каналов.

Если для флага PRIORITY кадра HEADERS установлено значение 1, то в полезных данных кадра присутствуют поля Exclusive Flag (E), Stream Dependency и Weight. Чтобы новый поток зависел от ранее созданного, можно использовать 9 бит на кадр HEADERS, 1 бит от флага E и 8 бит от поля Weight, для создания двунаправленного скрытого канала, не привлекая внимания. Таким образом, если одно соединение HTTP/2 имеет N потоков в одном направлении, то в течение «жизни» сессии можно отправить 9N бит в одном направлении.

Кадр PRIORITY необязателен и указывает приоритет потока, рекомендованный отправителем. Он может быть отправлен в любом состоянии потока и в любое время, за исключением последовательных кадров, которые составляют один блок заголовка. В данном случае можно использовать 9 бит на кадр PRIORITY, 1 бит от флага E и 8 бит от поля Weight для создания скрытого канала. При этом стоит учитывать, что количество кадров PRIORITY, отправляемых за одну сессию HTTP/2 не должно быть аномально большим.

Ещё одним способом является организация стеганографического канала с использованием полей заголовков cookie-файлов. С HTTP версии 2 для повышения эффективности сжатия появилась возможность разделения пар cookie из одного заголовка cookie в несколько полей, каждое из которых будет иметь одну или несколько пар cookie. Используя получающуюся двойственность можно создавать односторонние скрытые каналы от клиента, устанавливая наличие одного существующего поля как 1 и наличие более одного существующего поля заголовка cookie как 0. При этом для работы данного метода необходимо наличие минимум двух пар cookie. Пропускная способность данного метода напрямую зависит от количества открытых потоков HTTP сессии и равняется N битам при N потоках.

Последним рассмотренным методом будет использование алгоритма сжатия HPACK в HTTP. В первых версиях протокола HTTP не применялось сжатие полей заголовка HTTP, однако в связи с ростом использования сети Интернет и ростом объёма веб-страниц в спецификации HTTP/2 был объявлен так называемый компрессор HPACK, позволяющий устранить избыточные поля заголовков. Данный компрессор представляет поля заголовков как упорядоченную таблицу пар имя – значение, рассматриваемых как последовательности октетов. При этом строковые литералы могут быть закодированы данным компрессором с помощью статического кода Хаффмана, либо напрямую. Представление строкового литерала имеет три поля: первое используется для указания использования кодировки Хаффмана, второе поле содержит длину строки, третье поле содержит закодированную строку с

данными литерала. По аналогии с предыдущим методом можно использовать первое поле в качестве контейнера рассматривая наличие флага кодировки методом Хаффмана как 1 и отсутствие как 0. Пропускная способность такого метода зависит от количества строковых литералов в заголовке.

На основании рассмотренных выше методов можно сказать, что протокол HTTP однозначно может быть использован для организации стеганографических каналов. Также хочется отметить, что данный протокол активно используется, соответственно большое количество HTTP запросов не покажется подозрительным в случае анализа трафика.

Список используемых источников:

1. Коржик В. И. Цифровая стеганография и цифровые водяные знаки. СПб. : Санкт-Петербург, 2016. 225 с.
2. Салита А. С., Красов А. В. Создание стеганографического канала при помощи полей // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 2. С. 36–40.
3. Волгогонов В. Н., Гетьман Е. М., Салита А. С. Методы и способы создания стеганографических вложений в сетевых протоколах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. 2021. С. 178–183.
4. Диордица В. Н., Красов А. В., Таргонская А. И. Исследование современных методов сетевой стеганографии // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы IX Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 26–27 фев. 2020 г. СПб: СПбГУТ, 2020. С. 404-409.
5. RFC 2616. Hypertext Transfer Protocol. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee. Jun. 1999.
6. RFC 7540. Hypertext Transfer Protocol Version 2. M. Belshe, R. Peon, M. Thomson. May 2015.
7. RFC 9114. Hypertext Transfer Protocol Version 3. M. Bishop. Jun 2022.
8. Ушаков И. А., Красов А. В., Савинов Н. В. Организация, принципы построения и функционирования компьютерных сетей // Academia. 2019. С. 240.
9. Шелухин О. И., Канаев С. Д. Стеганография. Алгоритмы и программная реализация. // М. : Горячая линия – Телеком, 2017. 592 с.
10. Алексеев А. С. Методика противодействия сетевым стеганографическим угрозам // Вестник современных исследований, Омск 2019.

Paskidov N.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunications

Creating steganographic channels using the http protocol.

To date, privacy technologies are gaining popularity when using the Internet. The most popular way to ensure confidentiality is cryptography. This technology allows you to restrict access to information by encrypting data but has several disadvantages and limitations. Due to the existence of these flaws, steganography methods are gaining popularity. This article discusses the possibility of using steganography in Hypertext Transfer Protocol.

Key words: *HTTP, information security, network steganography, channel steganography, information concealment, information protection.*

УДК 004.492.2
ГРНТИ 81.93.29

СИНТЕЗ МЕТОДА ВЫЯВЛЕНИЯ ФИШИНГОВЫХ САЙТОВ ДЛЯ АНТИФИШИНОВОЙ СИСТЕМЫ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ

П. Е. Петров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С развитием технологий и популяризацией киберпреступности данный метод обнаружения угроз стал неэффективным. Теперь каждое новое фишинговое электронное письмо редко совпадает с предыдущим, поскольку преступники стремятся обойти спам-фильтры, используя различные системы искусственного интеллекта и недочёты спам-фильтров для нахождения оптимальных вариантов текстовых ловушек. Фишинговые сообщения или веб-страницы зачастую отправляются и создаются из ботнета (сети с множеством устройств, на которых запущены автономные программы – боты, созданные для написания писем или генерации вредоносных веб-страниц). Количество устройств в такой сети постоянно меняется, что делает списки блокировок малополезными. URL-адреса также будут уникальными, что позволяет обойти проверку адресов спам-фильтрами.

фишинг, киберпреступление, безопасность, веб-браузер, машинное обучение

Изучив статью [8] за авторством Калахарша П. и Метре Б. М., можно прийти к заключению, что на данный момент существует четыре основных способа выявления фишинговых сайтов, они описаны на рис. 1.



Рис. 1. Способы выявления фишинговых сайтов

Метод на основании списков заключается в разделении URL-адресов по базам легитимных (белый список) и фишинговых (черный список) сайтов. При использовании данного метода каждый URL-адрес, запрошенный пользователем, проверяется и сравнивается с адресами из списков, после чего выводится вердикт, является ли сайт опасным или пользователь может на нем работать без угрозы потери данных. На сегодняшний день существует большое количество баз данных чистых и фишинговых URL-адресов.

Недостатком метода на основе списков является вероятность ложного пропускания фишингово сайта, так как на момент его запроса пользователем, он может не находиться ни в одном из списков.

Метод визуальной схожести является наименее популярным из всех. Суть данного способа заключается в создании снимка веб-страницы и сохранении его в базе данных, после чего создается экспертное заключение о легитимности сайта. Если в базе появляются сайты со схожим изображением, то данная страница маркируется как потенциально опасная. Минусами данного подхода являются высокая ресурсозатратность для хранения данных и ошибочность срабатывания. Так, к примеру, первым в базу может быть записан снимок фишингово сайта с ложной пометкой о его легитимности.

Суть эвристического анализа заключается в анализе характеристик веб-страницы, таких как URL-адрес и содержимое сайта. Далее контент сравнивается между другими сайтами. При нахождении совпадения, считается, что новый сайт может являться фишинговым. Данный метод является улучшенным принципом спискового разделения и обладает большей точностью определения, однако его недостаток заключается в долгой обработке страниц.

Передовым методом анализа является применение методик машинного обучения. На основе различных наборов исходных данных, собранных в процессе обнаружения и изучения фишинговых страниц, происходит обучение моделей машинного обучения с последующим тестированием на различных классификаторах, таких как дерево решений (Decision tree Classifier), логистическая регрессия (Logistic Regression), метод опорных векторов (Support Vector machines) и другие. Готовые обученные классификаторы позволяют определять потенциально опасный контент практически сразу при его появлении, таким образом решая проблему уязвимости нулевого дня (то есть позволяют обнаружить фишинговую страницу до того, как она была использована по назначению). Точность определения зависит от наборов данных, на которых была обучена система.

Таким образом, выделяются четыре основных способа выявления фишинговых сайтов: на основании списков, визуальный анализ, эвристический анализ и применение машинного обучения. Были выделены особенности каждого способа, а также рассказано о преимуществах и недостатках каждого из них.

Изучив существующие методы выявления фишинговых сайтов, разработаем свой метод, который будет состоять из композиции уже имеющихся с определенной доработкой. В нашем случае общая последовательность метода будет состоять из двух комплектов шагов: подготовительные (6 шагов) и основные (5 шагов):

Подготовительные шаги:

1. Создать систему работы с Blacklist/Whitelist;
2. Собрать базу данных фишинговых сайтов;
3. Выбрать признаки подозрительных страниц для модели МО;

4. Собрать набор данных для обучения модели МО;
5. Создать и обучить модель МО;
6. Протестировать адекватность модели МО;
 - a. Модель настроена адекватно – переход к шагу 7;
 - b. Модель настроена некорректно – переход к шагу 3.

Основные шаги:

7. Проверить URL-адрес на наличие в Blacklist/Whitelist;
 - a. URL в Blacklist – переход к шагу 11;
 - b. URL в Whitelist – переход к шагу 9;
 - c. URL нет в листах – переход к шагу 8.
8. Применить МО;
 - a. Оценка сайта «подозрительный» – переход к шагу 10;
 - b. Оценка сайта «чистый» – переход к шагу 9.
9. Открыть страницу, пропустить шаги 10 и 11;
10. Открыть страницу и предупредить об угрозе, пропустить шаг 11;
11. Заблокировать доступ к странице;

Схема метода выявления фишинговых сайтов показана на рис. 2.

Подготовительные шаги включают все этапы, которые необходимо выполнить непосредственно до работы основной части программы. Так, создание списков Blacklist и Whitelist будет влиять на то, какие из полученных страниц будут проходить дополнительную проверку через модель машинного обучения, а определение признаков будет всецело влиять на итоговую оценку модели. Также необходимо заранее собрать базу фишинговых сайтов, так как она будет нужна для корректного определения признаков. Для прототипа было принято решение использовать базу данных ресурса PhishTank, так как она бесплатная, имеет простой в обращении API и постоянно обновляется [5]. По ранее определенным признакам собирается набор данных и выставляется итоговая оценка. Далее данный набор разделяется на обучающий и тестовый наборы для первоначальной подготовки модели к работе.

Основные шаги работы являются основой рабочей части прототипа, на них будет построено функционирование всей программы. Последовательность шагов строго закреплена, а их определенное количество позволяет полноценно обрабатывать веб-страницы, на которых работает пользователь. Также стоит заметить, что применение машинного обучения в прототипе зависит, в первую очередь, от решения, представленного на шаге обработки сайта на его наличие в Blacklist/Whitelist.

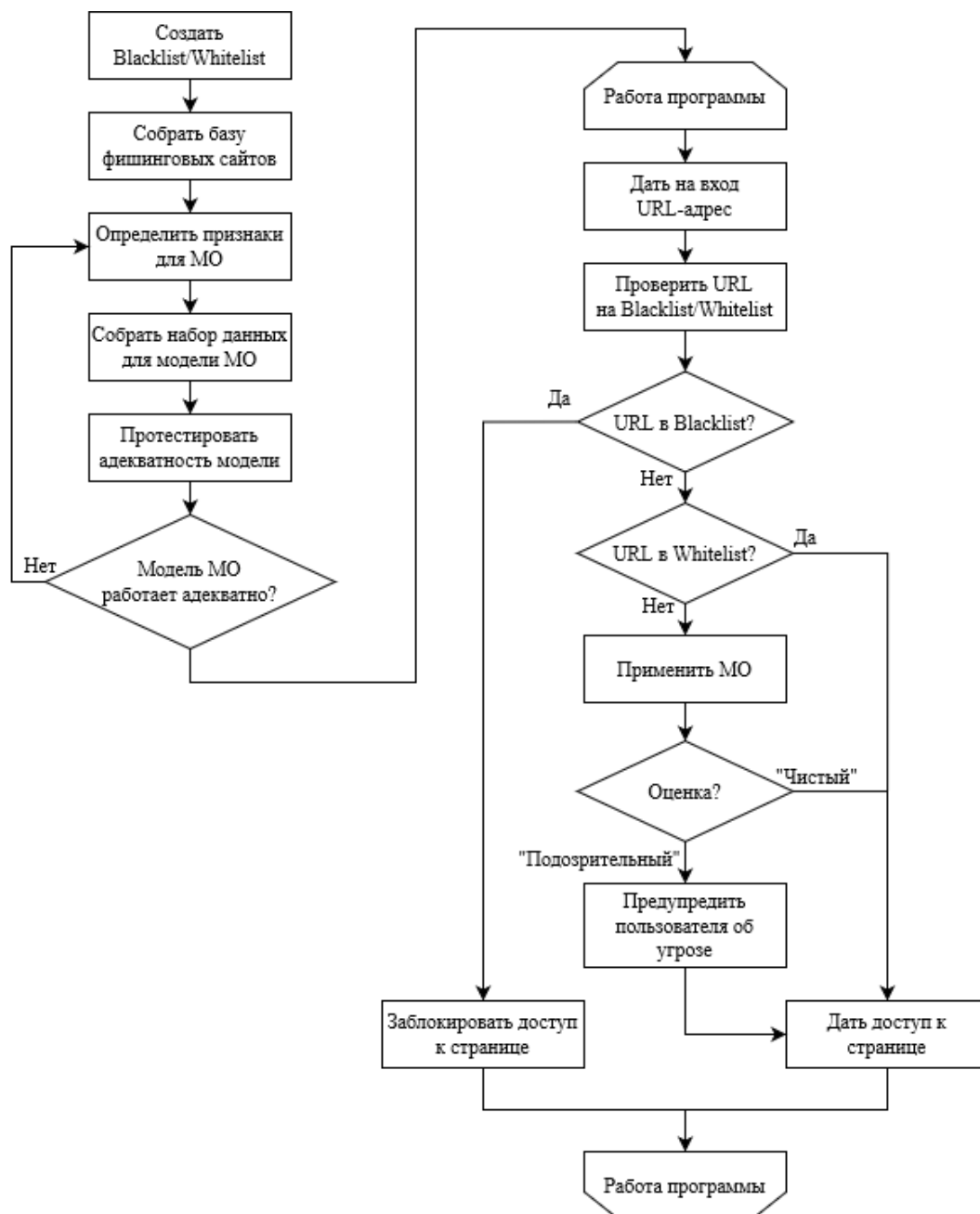


Рис. 2. Общая схема метода

Таким образом, были выделены шаги метода выявления фишинговых сайтов и составлена его общая схема. Из 11 полученных шагов, первые 6 являются подготовительными, они отвечают за сбор необходимых данных и за обучение модели машинного обучения. Оставшиеся 5 шагов относятся к подгруппе «основные», в них разбирается общая логика работы прототипа.

Список используемых источников:

1. Абитов А. А., Тхакахов Р. А., Хачмахова М. З., Сунгуров К. Ш. Защита от фишинга // Цифровая трансформация науки и образования : материалы междунар. научно-практич. конф., Нальчик, 25–28 сент. 2020 года. Нальчик: Кабардино-Балкарский государственный университет им. Х. М. Бербекова, 2020. С. 13-17.
2. Защищаемся от фишинга: [Электронный ресурс] // Изд-во “Открытые системы”, М., 1992-2022. URL: <https://www.osp.ru/pcworld/2011/08/13009731> (Дата обращения 20.05.2022)

3. Израйлов К. Е. Система критериев оценки способов поиска уязвимостей и метрика понятности представления программного кода // Информатизация и связь. 2017. № 3. С. 111-118.

4. Израйлов К. Е., Обрезков А. И., Курта П. А. Подход к выявлению последовательности одноцелевых сетевых атак с визуализацией их прогресса эксперту // Методы и технические средства обеспечения безопасности информации. 2020. № 29. С. 68-69.

5. База данных PhishTank: [Электронный ресурс]. URL: <https://phishtank.org/> (Дата обращения 20.05.2022)

6. Как идентифицировать фишинговый веб-сайт: [Электронный ресурс]. - URL: <https://www.egress.com/resources/cybersecurity-information/phishing/how-to-identify-a-phishing-website> (Дата обращения 20.05.2022)

7. Как обнаружить фишинговое электронное письмо или поддельную целевую страницу и спасти свой бизнес: [Электронный ресурс] // Small Business Trends LLC. 2003-2022. URL: <https://smallbiztrends.com/2018/05/how-to-spot-a-phishing-email.html> (Дата обращения 20.05.2022)

8. Малолетко Н. Е. Классические фишинг-атаки, вирусы и "тройанские Кони" как угрозы экономической безопасности предприятий // Актуальные проблемы и перспективы развития экономики: российский и зарубежный опыт. 2017. № 12. С. 48-51.

9. Обнаружение Фишинговых Сайтов - Обзор: [Электронный ресурс]. URL: <https://arxiv.org/pdf/2103.12739.pdf> (Дата обращения 20.05.2022)

Petrov P.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Synthesis of a method for detecting phishing sites for an anti-phishing system based on machine learning.

With the development of technology and the popularization of cybercrime, this method of detecting threats has become ineffective. Now every new phishing email rarely coincides with the previous one, as criminals seek to bypass spam filters by using various artificial intelligence systems and spam filter flaws to find the optimal options for text traps. Phishing messages or web pages are often sent and created from a botnet (a network with many devices running autonomous bot programs designed to write emails or generate malicious web pages). The number of devices in such a network is constantly changing, which makes blocking lists of little use. The URLs will also be unique, which allows you to bypass the spam filters checking the addresses.

Key words: *phishing, cybercrime, security, web browser, machine learning.*

УДК 004.415.25
ГРНТИ 50.41.25

СРАВНЕНИЕ СКОРОСТИ ИСПОЛНЕНИЯ КОДА В НАТИВНОЙ СРЕДЕ И СРЕДЕ WASM

А. А. Попов, О. В. Федорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В наше время существуют возможность быстрого исполнения кода в браузере. Данная технология позволяет получить прирост в скорости исполнения относительно Java Script, однако уступает скорости в нативной среде. В данной статье будет произведено сравнение нативной среды и WebAssembly.

webassembly; веб-технологии; программирование; go lang

На данный момент все большая часть разработчиков выбирают кроссплатформенные web фреймворки для разработки приложений, что позволяет унифицировать кодовую базу под большое количество конечных платформ. Данные фреймворки позволяют быстро и эффективно разрабатывать пользовательские интерфейсы используя высокоуровневые языки программирования, такие как *JavaScript*, *TypeScript* и *Dart*, утилизируя единую кодовую базу. В случае с *JavaScript* и *TypeScript*, данные языки используют *just-in-time* компиляцию, виртуальную машину *Dart VM* и транскомпиляцию в *JavaScript* в случае с *Dart*. Данные решения заметно уступают в производительности компилируемым языкам программирования, такими как *C*, *C++* и *Go*. Для решения данной проблемы был создан *WASM*. В данной статье будет проведено сравнение скорости исполнения кода в нативной среде исполнения и среде исполнения *WASM*(*WebAssembly*). *WASM* - это двоичный формат команд для виртуальной машины на основе стека. *WASM* так же может быть описан, как низкоуровневая виртуальная машина или результат компиляции с языка высокого уровня, позволяющая развертывать клиентские и серверные приложения в сети интернет. Данная технология предназначена для решения проблем с быстродействием исполнения кода в браузере. Ранее код выполнялся при помощи *JavaScript*, *HTML5*, но их быстродействие не всегда удовлетворяет современные запросы. Новая технология получила широкую поддержку. 88% браузеров поддерживают *WASM*, особенно в последних версиях. Без поддержки остаются *IE*, *Opera Mini* и несколько других устаревших браузеров. Так же *LLVM* теперь поддерживает *WASM*, как цель компиляции, что привело к появлению еще большего количества языков, компилирующихся в *WASM*. В данный момент этот список включает в себя такие популярные языки как *C/C++*, *Rust*, *Java*, *Kotlin*, *Go* и *C#*. Все эти языки активно используются для разработки современных приложений.

Целью данной работы является определение деградации производительности при работе в нативной среде и популярных средах исполнения WASM, таких как V8 и Spidermonkey.

Для сравнения скорости работы был написан код на Go, который реализует расчет числа Pi используя алгоритм братьев Чудновских. Данный алгоритм основывается на формуле Сриниваса Рамануджана для расчета числа Pi . В своем классическом виде алгоритм выражается в виде следующей формулы:

$$\frac{1}{\pi} = 12 \sum_{k=0}^{\infty} \frac{(-1)^k (6k)! (13591409 + 545140134k)}{(3k)! (k!)^3 640320^{\frac{3k+3}{2}}}$$

В данном случае для расчётов будет использоваться упрощенная версия формулы, имеющая следующий вид:

$$\frac{(640320)^{\frac{3}{2}}}{12\pi} = \frac{426880\sqrt{10005}}{\pi} = \sum_{k=0}^{\infty} \frac{(6q)! (545140134q + 13591409)}{(3q)! (q!)^3 (-262537412640768000)^q}$$

Данное выражение можно разложить на члены следующим образом:

$$\pi = C \left(\sum_{q=0}^{\infty} \frac{M_q * L_q}{X_q} \right)^{-1}, \text{ где}$$

$$C = 426880\sqrt{10005}$$

$$M_q = \frac{(6q)!}{(3q)! (q!)^3}$$

$$L_q = 545140134q + 13591409$$

$$X_q = (-262537412640768000)^q$$

Члены M_q , L_q , X_q можно рассчитывать следующим образом:

$$M_{q+1} = M_q * \left(\frac{(12q + 2)(12q + 6)(12q + 10)}{(q + 1)^3} \right), \text{ где } M_0 = 1$$

$$L_{q+1} = L_q + 545140134, \text{ где } L_0 = 13591409$$

$$X_{q+1} = X_q * (-262537412640768000), \text{ где } X_0 = 1$$

Член M_q можно рассчитывать следующим образом:

$$K_{q+1} = K_q + 12, \text{ где } K_0 = -6$$

$$M_{q+1} = M_q * \left(\frac{K_{q+1}^3 - 16K_{q+1}}{(q + 1)^3} \right), \text{ где } M_0 = 1$$

Данный алгоритм был выбран для проведения тестов так как он и работает с большими целыми числами и большими числами с плавающей запятой. Данный алгоритм имеет время работы $O(M(n)n)$.

Изначальная поддержка платформы *wasm* была добавлена в *go* в версии 1.11. При сборке будет использоваться версия *go* 1.19.3. При проведении всех тестов будет использоваться компьютер с *Intel® Core™ i5-7300HQ @ 3.00Ghz* с запущенной операционной системой *Microsoft Windows 10* версии 19044.2130. При сборке будут использованы дополнительные флаги для компоновщика, отключающие информацию для отладки и генерацию таблицы символов *Go*. Полученные результаты после 20 тестов для 10000 итераций алгоритма для каждой из сред исполнения приведены в таблице 1.

ТАБЛИЦА 1. Время исполнения теста

Spidermonkey (Firefox Nightly 108.0a1), с	V8 (Google Chrome 107.0.5304.107), с	Linux x64 (WSL), с	Windows 10, с
5.499000064	6.074799616	0.335218	0.327145
5.507000064	6.195699968	0.373599	0.330637
5.500999936	6.284100096	0.335189	0.329019
5.482000128	6.0784	0.330948	0.328855
5.470999808	6.074100224	0.338238	0.327056
5.496	6.224599808	0.350016	0.327056
5.502000128	6.084699904	0.340584	0.330541
5.492	6.096199936	0.336262	0.330943
5.496999936	6.396399872	0.331573	0.333067
5.510000128	6.380599808	0.333296	0.334449
5.472	6.117299968	0.334722	0.328226
5.557999872	6.126399744	0.331294	0.330058
5.464	6.574800128	0.333073	0.328829
5.461999872	6.431600128	0.339452	0.330573
5.470000128	6.17209984	0.337526	0.330422
5.480999936	6.18089984	0.334322	0.327477
5.517999872	6.168499968	0.338411	0.329084
5.476	6.12409984	0.331808	0.330034
5.468	7.969299968	0.338888	0.328353
5.481000192	6.121200384	0.338051	0.329585

Таким образом, мы наглядно продемонстрировали различия во времени исполнения кода в нативной среде и в среде *WASM*. Отличие, полученное в описанных условиях приблизительно равно 15. Таким образом мы можем сказать, что при использовании *WASM* мы значительно теряем в скорости исполнения.

Список используемых источников:

1. David Chudnovsky and Gregory Chudnovsky. The computation of classical constants. Proceedings of the National Academy of Science USA. 1989. P. 8178-8182.
2. Lorenz M, A detailed proof of the Chudnovsky formula with means of basic complex analysis. Cornell University, 2018. 60 p.

Popov A., Fedorova O.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Comparison of code execution speed in native environment and WASM environment.

Nowadays, it is possible to quickly execute code in the browser. This technology allows you to get an increase in execution speed relative to Java Script, but is inferior to the speed in the native environment. This article will compare the native environment and WebAssembly.

Key words: webassembly; web technologies; programming; golang.

УДК 004.5
ГРНТИ 81.93.29

ПРИНЦИПЫ ВЗАИМОДЕЙСТВИЯ КОМПОНЕНТОВ СЕТИ «УМНЫЙ ДОМ»

В. В. Пучков^{1,2}, Л. А. Виткова^{1,2}, Е. Д. Едемская¹

¹Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

²Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН)

Успешное сочетание времени и активного развития прогресса позволило появиться интеллектуальной технологии «умный дом», которая в современном варианте может слаженно управлять в автоматическом режиме всевозможными инженерными устройствами дома и здания в целом. Чтобы предоставлять владельцу наиболее оптимальные решения, система собирает большое количество пользовательской информации, которая передается другим компонентам сети. Для предотвращения реализации угроз безопасности «умного дома» необходимо понимать, какую информацию собирает каждый компонент «умной» сети и куда эти данные передаются. Данная статья описывает процесс взаимодействия устройств друг с другом.

умный дом, пользовательская информация, общение устройств, передача данных

Интеллектуальная технология «умный дом» может слаженно управлять в автоматическом режиме всевозможными инженерными устройствами дома и здания в целом, исключая необходимость постоянного контроля со стороны владельца. Несмотря на быстрый рост и удобное применение, системы «умного дома» также подвергают владельцев рискам безопасности, т.к. они собирают и передают по сети огромное количество пользовательской информации [1, 2].

1. Основные компоненты «умного дома»

Для выявления возможных векторов атак на «умную» инфраструктуру необходимо понимать принципы взаимодействия устройств друг с другом, а именно: какую информацию собирает каждое устройство и куда ее отправляет. На рис. 1 показана упрощенная схема взаимодействия основных составных частей сети «умного дома».

Система «умный дом» состоит из четырех основных элементов: пользовательского интерфейса, встроенного в управляющее устройство, шлюза, облачного сервера и различных «умных» устройств, которые легко подключаются через компьютерную сеть [3, 4].

Пользовательский интерфейс является средством общения владельца с компонентами дома. Пользователи могут контролировать устройства с помощью специального приложения, которое необходимо предварительно установить на смартфон или любое другое управляющее устройство. Однако в последнее время наиболее популярным является применение голосовых ассистентов. Благодаря этой технологии пользователь может контролировать «умные» устройства с помощью голосовых команд, что дает возможность отказаться от ручного управления.

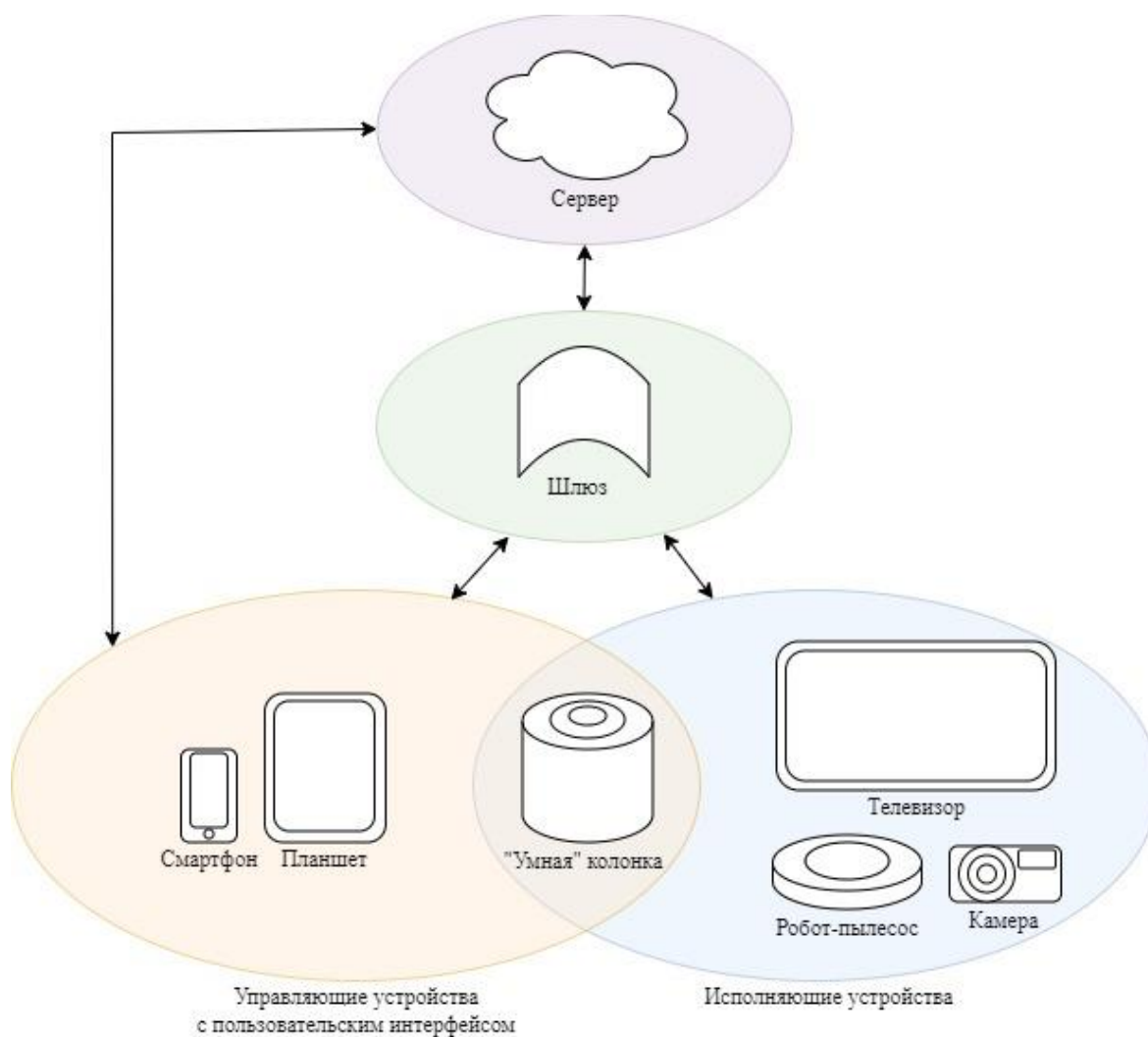


Рис. 1. Упрощенная схема взаимодействия компонентов системы «умный дом»

В среде Интернета вещей шлюз выступает в роли «мозга» беспроводной сети. Обычно он поддерживает различные стандарты связи, поскольку к нему подключаются разнородные устройства. Кроме того, шлюз служит соединителем с серверным облаком, в котором хранится логика агрегации для различных устройств. Как правило, шлюз получает пакеты от датчиков, отправляет информацию в облако и управляет другими подключенными устройствами в соответствии с сообщением, возвращаемым облаком.

В экосистеме «умного дома» облачный сервер берет на себя большинство вычислительных задач. В частности, облачный сервер отвечает за выполнение логики управления различными устройствами с целью снижения энергопотребления устройств с ограниченными ресурсами.

«Умные» исполняющие устройства являются ключевыми строительными блоками всей инфраструктуры. В отличие от традиционных электронных устройств, «умные» поддерживают сетевую связь с помощью различных беспроводных протоколов, информация о самых распространенных, применяемых при построении сети «Умный дом» приведена в таблице 1.

ТАБЛИЦА 1. Беспроводные протоколы связи

Протокол	Преимущества	Недостатки
Wi-Fi	<ul style="list-style-type: none"> • Возможность развернуть сеть без прокладки кабеля. • Широкое распространение оборудования, поддерживающего Wi-Fi. • Высокая скорость передачи данных. • Частоты, на которых работает протокол, не создают помех и безопасны для людей. 	<ul style="list-style-type: none"> • Высокая стоимость модулей. • Большая энергоемкость и отсутствие возможности длительной работы оборудования от автономных источников питания.
Bluetooth	<ul style="list-style-type: none"> • Высокая скорость передачи данных. • Простота в использовании. • Отсутствие кабелей. • Небольшое потребление энергии. 	<ul style="list-style-type: none"> • Маленький радиус действия.
Zigbee	<ul style="list-style-type: none"> • Низкое энергопотребление. • Возможность создания сложных сетевых решений с автоматической маршрутизацией. • Высокий уровень защиты данных. • Сеть может поддерживать до нескольких тысяч элементов. • Гибкая настройка узлов сети. 	<ul style="list-style-type: none"> • Отсутствие стандартизации, вследствие чего оборудование разных брендов редко оказывается совместимым. • Низкая скорость передачи данных.
Z-wave	<ul style="list-style-type: none"> • Низкое энергопотребление. • Возможность формирования сети с ячеистой топологией. • Низкая стоимость. • Простота в использовании, возможность расширения сети. • Безопасный уровень излучения 	<ul style="list-style-type: none"> • Низкая скорость передачи данных.
RF433	<ul style="list-style-type: none"> • Низкая стоимость. 	<ul style="list-style-type: none"> • Отсутствие обратной связи от устройства. • Очень загрязненный эфир.

Наиболее часто применяемыми устройствами являются «умные» колонки, камеры видеонаблюдения, телевизоры, различная бытовая техника (пылесосы, чайники и др.) и датчики (температуры, движения и др.). Сами «умные» устройства не хранят в себе информацию, они передают ее другим элементам системы. При этом шлюз выступает главным контролирующим элементом, через который проходит весь трафик.

2. Пользовательская информация и места ее передачи

«Умная» колонка позволяет проигрывать музыку, просматривать видео через телевизор или монитор, взаимодействовать с поиском в Интернете с использованием голосового управления, ставить будильники, напоминания и т.д. Она представляет собой объединение пользовательского интерфейса и «умного» устройства. Информация, которую получает колонка передается на сервер, при этом отправляется только тот звуковой трафик, который фиксируется после активации колонки специальной командой. Таким образом колонка может общаться с большинством устройств в «умном доме», шлюзом и сервером, на

котором происходит обработка голосовых команд и хранение информации о пользователе (голос владельца, музыкальные предпочтения и др.).

Робот-пылесос с помощью своей навигационной системы строит карту помещения, которая хранится в облачном хранилище производителя. Техникой можно управлять как с помощью специального приложения, так и с помощью «умной» колонки. Таким образом, робот-пылесос может общаться с управляющим элементом, шлюзом и облачным хранилищем.

В свою очередь данные с камер видеонаблюдения (видео и звук) хранятся либо на физических картах памяти, которые находятся непосредственно в самой камере либо в облачном хранилище. Контроль камеры происходит также при помощи управляющего устройства. Исходя из вышесказанного, камера, как и большинство «умных» устройств может обращаться к управляющему устройству, шлюзу и облачному хранилищу.

Телевизоры с функцией SmartTV также собирают большое количество данных о владельце, которые в последствии используются для создания подробного профиля потребителя. Ежесекундно телевизор снимает «отпечаток» экрана. Он выглядит как десятки квадратных фрагментов пикселей, разбросанных по экрану, которые телевизор преобразует в строку чисел. Эту строку телевизор передаёт на сервер вместе с идентификаторами телевизора. На сервере происходит сравнение отпечатка с базой известного контента. Результатом является посекундный журнал просмотра пользователя.

В таблице 2 отображена информация, собираемая различными «умными» устройствами и места, куда они могут обращаться.

ТАБЛИЦА 2. Собираемая информация и места обращения

Устройство	Собираемая информация	Места обращения
«Умная» колонка	Музыкальные предпочтения пользователя, голос владельца, история голосовых запросов, вся голосовая информация, поступающая после активации колонки	Другие «умные» устройства, шлюз, сервер
Робот-пылесос	Карта помещения, состояние аккумулятора	Управляющее устройство, шлюз, облачное хранилище
Датчики	Информация об окружающей среде (в зависимости от типа датчика: температура, влажность, движение, наличие дыма и т.д.)	Управляющее устройство, шлюз
Камера видеонаблюдения	Видео, звук	Управляющее устройство, шлюз, облачное хранилище
Телевизор со SmartTV	Содержимое экрана	Управляющее устройство, шлюз, сервер

В результате, в статье были описаны различные компоненты «умного дома» и информация, ими собираемая. В работе подчеркивается разнообразие и большой объем пользовательской информации, передаваемой по сети, целью злоумышленника может стать получение этой информации. Исследование

позволяет понять важность и необходимость обеспечения защищенного хранения и передачи пользовательских данных в «умной» среде. На основе данной работы в дальнейших исследованиях будут строиться векторы атак на «умную» инфраструктуру.

Работа выполнена при частичной финансовой поддержке Гранта РФФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников:

1. Ogonji M. M., Okeyo G., Wafula J. M. A survey on privacy and security of Internet of Things //Computer Science Review. – 2020. – Т. 38. – С. 1-42.
2. Виткова Л.А., Едемская Е.Д. Изучение уязвимостей в системе «умного» дома и методов их обнаружения. // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. С. 267-270.
3. Min Lia, Wenbin Gub, Wei Chenc, Yeshen Hed, Yannian Wud, Yiying Zhange Smart home: architecture, technologies and systems [Электронный ресурс] // Procedia computer science. – 2018. – N. 131. – С. 393-400. URL: <https://clck.ru/32cPf8> (дата обращения 06.11.2022).
4. Zaidan A. A., Zaidan B. B., Qahtan M. Y., Albahri O. S., Albahri A. S., Mussab Alaa, Jumaah F. M., Mohammed Talal, Tan K. L., Shir W. L., Lim C. K. A survey on communication components for IoT-based technologies in smart homes [Электронный ресурс] // Telecommunication Systems. – 2018. – №. 1. – С. 1-25. URL: <https://clck.ru/32cQLq> (дата обращения 06.11.2022).

Puchkov V.^{1,2}, Edemskaya E.¹, Vitkova L.^{1,2}

¹The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

²St. Petersburg Federal Research Center of the Russian Academy of Sciences

Principles of interaction between components of the smart home network.

The successful combination of time and the active development of progress has allowed the emergence of intelligent technology "smart home", which in the modern version can smoothly manage in automatic mode all kinds of engineering devices of the house and the building as a whole. In order to provide the owner with the most optimal solutions, the system collects a large amount of user information that is transmitted to other network components. To prevent the implementation of smart home security threats, it is necessary to understand what information each component of the smart network collects and where this data is transmitted. This article describes the process of devices interacting with each other.

Key words: smart home, user information, device communication, data transmission.

УДК 004.056.55
ГРНТИ 81.93.29

АЛГОРИТМ МОНТГОМЕРИ УМНОЖЕНИЯ В ПОЛЯХ ГАЛУА

Д. А. Разумов, С. Н. Шемякин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Алгоритм Монтгомери широко используется в криптографии для модульных вычислений (умножение или возведение в степень по модулю). Однако его чаще всего используют для целочисленных вычислений. Новизна работы заключается в том, что в ней рассматривается алгоритм Монтгомери как способ умножения элементов конечных полей.

алгоритм Монтгомери, конечные поля, поля Галуа, алгоритмы умножения, модульные вычисления, криптография, информационная безопасность

Алгоритм Монтгомери широко используется для ускорения модульных вычислений. В то же время интересен вопрос о применении алгоритма Монтгомери для ускорения умножения в конечных полях. Как написано в [1] алгоритм Монтгомери существует в двух вариациях: первая используется для нахождения отображения $\varphi_R(x) = xR^{-1}(\text{mod}N)$, а вторая для нахождения отображения произведения множителей: $\varphi_R(xy) = xyR^{-1}(\text{mod}N)$. При этом для нахождения произведения множителей по модулю достаточно использовать второй вариант алгоритма (далее под словами «алгоритм» и «алгоритм Монтгомери» будет подразумеваться именно второй вариант алгоритма Монтгомери), поэтому здесь будет рассматриваться только он. Также не будем касаться того, как используется алгоритм Монтгомери для ускорения модульного умножения, т. к. это тоже описано в [1].

Описание алгоритма.

По аналогии с [1] был сформирован следующий алгоритм Монтгомери для конечных полей. Пусть даны: поле Галуа $GF(p^n)$; модуль (1), который образует конечное поле $GF(p^n)$; множители (2) и (3).

$$N(x) = \sum_{i=0}^n N_i x^i \quad (1)$$

$$a(x) = \sum_{i=0}^{n-1} a_i x^i \quad (2)$$

$$b(x) = \sum_{i=0}^{n-1} b_i x^i \quad (3)$$

Определим вспомогательный модуль как $R(x) = x^n$ и предварительно вычислим коэффициенты разложения $R(x)R'(x) - N(x)N'(x) = 1$ (4) и (5).

$$N'(x) = -N^{-1}(x)(\text{mod} R(x)) = \sum_{i=0}^n N'_i x^i \quad (4)$$

$$R^{-1}(x) = R^{-1}(x) \pmod{N(x)} = \sum_{i=0}^{n-1} R_i^{-1} x^i \quad (5)$$

Тогда для вычисления отображения $\varphi_R(a(x)b(x)) = a(x)b(x)R^{-1}(x) \pmod{N(x)}$ необходимо вычислить последовательность $z_0(x), \dots, z_n(x)$, где элементы последовательности вычисляются рекуррентно следующим образом:

1. вычислить полином по формуле (6);

$$u(x) = z_i(x) + a_i b(x) \pmod{x} \quad (6)$$

2. используя уже вычисленное значение, вычислить полином по формуле (7);

$$v(x) = u(x)N^{-1}(x) \pmod{x} \quad (7)$$

3. получить следующий элемент последовательности по формуле (8).

$$z_{i+1}(x) = (z_i(x) + a_i b(x) + v(x)N(x)) / x \quad (8)$$

При этом $z_0(x) = 0$. И полагается, что $\varphi_R(a(x)b(x)) = z_n(x)$. Нетрудно заметить, что в отличие от алгоритма для целых чисел, в этом алгоритме отсутствует последний шаг, в котором проверяется больше ли $z_n(x)$ чем $N(x)$ или нет. Это связано с тем, что при такой реализации алгоритма гарантированно будет выполняться условие $\partial(z_n(x)) < \partial(N(x))$. Приведем доказательство.

Очевидно, что $\partial(v(x)) = \partial(u(x)) = 0$ т. к. вычисления производятся по модулю x . Из этого следует что $\partial(z_{i+1}(x)) < \max\{\partial(z_i(x)), n\}$. Однако с учетом того, что $\partial(z_0(x)) = 0$, можно утверждать, что $\forall i \in \{0, \dots, n\}: \partial(z_i(x)) < n$. Из этого следует, что $\forall i \in \{0, \dots, n\}: z_i(x) \in GF(p^n)$, отсюда вытекает доказываемое неравенство.

Аналогично [1] отметим, что при делении в (8) остаток не образуется: (9).

$$z_i(x) + a_i b(x) + v(x)N(x) \equiv z_i(x) + a_i b(x) - a_i b(x) \pmod{x} \equiv 0 \pmod{x} \quad (9)$$

Доказательство корректности алгоритма.

Докажем, что этот алгоритм работает корректно. Доказательство будет схоже с тем, что приведено в [1]. Докажем индукцией то, что формула (10) верна.

$$x^i z_i(x) \equiv \left(\sum_{j=0}^{i-1} a_j x^j \right) b(x) \pmod{N(x)}, 1 \leq i \leq n \quad (10)$$

База индукции: при $i = 1$ получаем уравнение (11).

$$x^1 z_1(x) \equiv z_0(x) + a_0 b(x) \pmod{N(x)} \equiv a_0 b(x) \pmod{N(x)} \quad (11)$$

Индуктивный переход: при $i > 1$ получаем уравнение (12).

$$x^{i+1} z_{i+1}(x) \equiv x^i (z_i(x) + a_i b(x)) \pmod{N(x)} \equiv x^i z_i(x) + (a_i x^i) b(x) \pmod{N(x)} \quad (12)$$

Учитывая базу индукции и индуктивный переход, выводим формулу (10).

Подставив n вместо i в формуле (10) получаем связь между множителями и $z_n(x)$ (формула (13)). Следовательно $z_n(x) \equiv a(x)b(x)R^{-1}(x) \pmod{N(x)}$ – значит алгоритм работает корректно.

$$x^n z_n(x) \equiv \left(\sum_{j=0}^{n-1} a_j x^j \right) b(x) \pmod{N(x)} \equiv a(x)b(x) \pmod{N(x)} \quad (13)$$

Сравнение алгоритма Монтгомери и обычного алгоритма умножения.

Для определения эффективности алгоритма Монтгомери была написана программа, в которой реализовано умножение в полях Галуа с характеристикой 2 с помощью алгоритма Монтгомери и с помощью алгоритма обычного умножения. В программу был загружен набор неприводимых полиномов, которые образуют конечные поля. Программа вычисляла среднее время выполнения умножения для случайных множителей для каждого алгоритма умножения и для каждого неприводимого полинома. В результате ее работы была получена зависимости среднего времени выполнения умножения от степени конечного поля.

Зависимость времени выполнения обычного алгоритма умножения и алгоритма Монтгомери от степени поля Галуа представлена в таблице 1 (для однократных запусков и с усреднением по 10000 запускам). Графики этой зависимости представлены на рис. 1 (время выполнения однократных запусков) и на рис. 2 (усредненные значения по 10000 запускам).

ТАБЛИЦА 1. Среднее время выполнения умножения с помощью обычного алгоритма и алгоритма Монтгомери

Степень поля Галуа	Время выполнения умножения,нс		Среднее время выполнения умножения, нс	
	Обычный алгоритм	Алгоритм Монтгомери	Обычный алгоритм	Алгоритм Монтгомери
8	6	6	4,2787	3,3028
16	13	9	8,0882	5,4636
24	17	12	12,8971	7,5669
32	36	22	23,1891	12,5092
40	39	15	32,4468	15,4018
48	51	19	42,6862	18,2811
56	54	22	54,6592	21,0019
64	18	23	12,2276	12,9913
72	41	35	32,3219	26,8314

80	72	41	57,4711	30,4685
88	103	46	89,4526	33,5924
96	128	47	127,277	38,3915
104	171	52	149,984	41,808
112	183	46	170,507	48,196
120	189	49	194,609	48,1698
128	26	2	28,001	36,2987
136	86	78	82,2341	53,4994
144	163	60	150,212	65,5354
152	231	64	235,448	62,4923
160	343	69	317,164	75,6607

Можно заметить, что время выполнения умножения существенно падает при степенях кратных 64. Это скорее всего связано с оптимизацией вычислений для 64-битных значений. Но несмотря на эти спады, алгоритм Монтгомери все равно дает выигрыш по скорости выполнения умножения. В среднем алгоритм Монтгомери выполняется на 45 % быстрее, чем обычный алгоритм умножения.

Также можно заметить небольшие «пики» (в усредненном графике) по времени выполнения для конкретных степеней, которые особенно хорошо выделяются для значений больше 128. Это может быть связано со свойствами полиномов, которые образовывали поля Галуа.

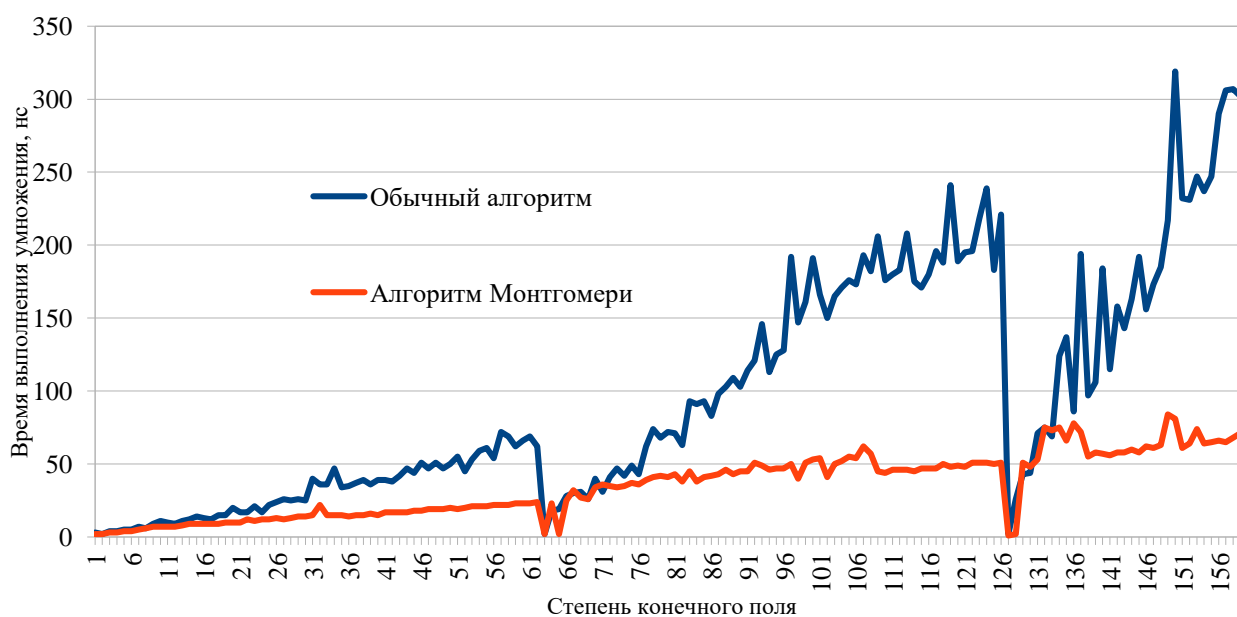


Рис. 1. Время выполнения умножения с помощью обычного алгоритма и алгоритма Монтгомери

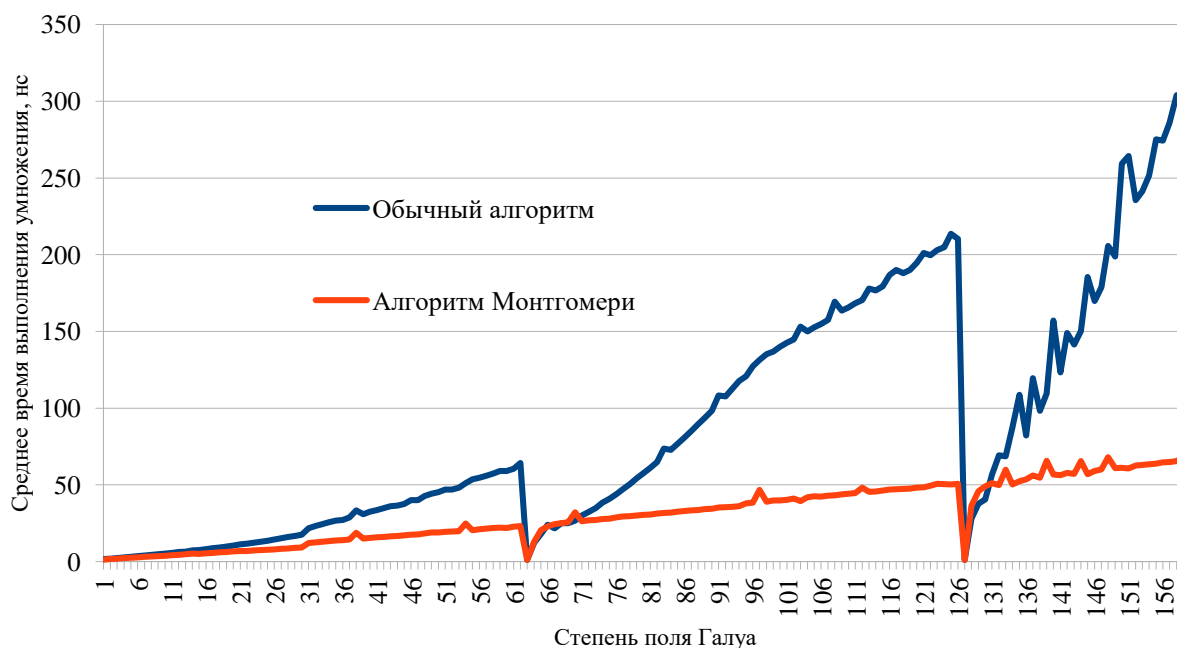


Рис. 2. Среднее время выполнения умножения с помощью обычного алгоритма и алгоритма Монтгомери (10000 запусков)

Список используемых источников:

1. Глухов М. М., Круглов И. А., Пикчур А. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии: учеб. пособие. СПб. : Лань, 2011. 400 с.

Razumov D., Shemyakin S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Montgomery algorithm for multiplication in Galois fields.

The Montgomery algorithm is widely used in cryptography for modular calculations (multiplication or exponentiation modulo). But largely it is used for integer calculations. The scientific novelty of the article is determined by the fact that it considers the Montgomery algorithm as a way to multiply elements of finite fields.

Key words: *Montgomery algorithm, finite fields, Galois fields, multiplication algorithms, modular calculations, cryptography, information security.*

УДК 004.773
ГРНТИ 49.33.31

СТЕГАНОГРАФИЧЕСКИЕ ВЛОЖЕНИЯ В ПРОТОКОЛ «DOMAIN NAME SYSTEM»

А. С. Салита

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Для упрощения жизни пользователям сети internet используется протокол системы доменных имен (Domain name system или DNS). В настоящее время все сложнее отследить утечку информации, тем более с использованием стеганографического канала. В данной статье описывается один из возможных методов использования протокола DNS для взаимодействия устройства со специальным DNS-сервером.

DNS, стеганография, сети, информационная безопасность

В современном мире остро встает вопрос о сокрытии данных и выявлении утечек информации [1-5]. Поэтому всю большую популярность набирает такой метод защиты информации, как стеганографические вложения [6-10]. Сетевая стеганография – это семейство методов, которые используют телекоммуникационные протоколы в качестве контейнеров для сокрытой передачи информации. Данные методы преобразуют телекоммуникационные протоколы заменяя информацию в некоторых служебных полях на полезную нагрузку, в результате протокол перестаёт выполнять свои первоначальные функции пользователь это может заметить или же полезная нагрузка помещается в поля, которые не влияют на работоспособность протокола, пользователь может не заметить вложений. Учитывая тот факт, что протокол системы доменных имен или сокращенно DNS, используется повсеместно на каждом рабочем устройстве с выходом в интернет, будь то компьютер, планшет, телефон или часы, а блокировка данного протокола в сети чаще всего парализует работу всего предприятия, было решено рассмотреть его для применения в качестве стегоконтейнера.

Протокол DNS состоит из следующих полей:

- ID — данное поле отвечает за идентификационный номер запроса и состоит из цельного числа, которое является одинаковым для запроса и ответа
- Flags — поле, в котором содержатся различные флаги;
- Question Count;
- Answer Record Count;
- Answer Authority Count;
- Answer Additional Count;
- Запросы DNS (Question) — поле, содержащее доменное имя, ip адрес которого хотим получить. Например: vk.ru;
- Ответов DNS (Answer) — поле, содержащее ip-адрес требуемого устройства или системы;

– Авторитетные серверы (Authority) — поле, работающее в итеративном режиме, содержит в себе ip-адреса серверов, отвечающих за DNS зону, которая интересует пользователя;

– Дополнительная информация (Additional) — поле содержит дополнительные комментарии, которые могут иметь пользу в будущем;

Стоит отметить, что в одном и том же DNS пакете могут быть несколько запросов и несколько ответов, в том числе несколько ответов на один запрос, если одному доменному имени соответствует несколько ip-адресов. Остановимся на поле Флаги, которое состоит из нескольких полей:

– QR (Query/Response Flag) — флаг, отвечающий за тип операции: запрос (0) или ответ (1).

– OPCODE (Operation Code) (4 бита) — флаг, отвечающий за тип запроса. На практике используются только 0-стандартный запрос.

– AA — флаг, указывающий на авторитетность ответа (1 – да, 0 – нет).

– TC — флаг, сигнализирующий о целостности пакета. Его значения: 1 – пакет был обрезан, 0 – манипуляций с пакетом не.

– RD — флаг, указывающийся только при запросах. Его наличие указывает просьбу о работе сервера в рекурсивном режиме.

– RA — флаг, указывающийся только при ответах. Его наличие указывает о готовности сервера к работе в рекурсивном режиме.

– Z — флаг, зарезервированный на будущее.

– RCODE (4 бита) — последние четыре бита — это статус выполнения операции. Значение 0 сообщает пользователю о том, что операция завершилась успешно, все остальные значению будут сигнализировать о сбое.

Произведя теоретический анализ, а также серию экспериментов было выявлено, что:

1) DNS-сервер, обрабатывающий запросы, игнорировал искаженные запросы, т.е. запросы, содержащие поля заголовка, заполненные нестандартным образом.

2) Редкие запросы обратного типа запроса или с неиспользуемым OPCODE сильно выделяются, что отрицательно сказывается на обнаруживаемости передачи дополнительной информации.

3) DNS-запросы (сообщения с флагом QR, установленным на 0) также могут получать ответы; такой запрос не рассматривается как беспрецедентный или искаженный; кроме того, при поступлении такого сложного сообщения оно корректно интерпретируется сервером — подготовленный ответ просто заменяется правильным.

4) В структуре ответа DNS поле «Длина данных ресурса» сообщает нам, сколько байтов занимает поле «Данные ресурса»; это значение, однако, может быть предсказано, например, для ответа на запись типа A это поле всегда будет занимать 4 байта, что достаточно для записи IPv4-адреса; поэтому в случае записи данного типа протоколом предусмотрена интерпретация только первых

четыре байта из поля Resource Data — остальные игнорируются, несмотря на определение их количества в поле Resource Data Length.

С учетом проведенного анализа наиболее перспективное представляется следующая модель сокрытия данных в DNS-сообщениях:

- 1) Стандартный (Opcode = 0) запрос (QR = 0) об одном домене (QDCount = 1, Query[1]);
- 2) Пакет должен содержать только один ответ (ANCCount = 1, Answer[1]), в случае если их больше DNS сервер отбрасывает пакет;
- 3) В поле запроса есть один запрос об IPv4 адресе (Query[1].Type = 2) существующего домена (например: Query[1].Name = zss.sut.ru).
- 4) В поле Answer[1].TTL служит для нумерации отправленных сообщений. Данное поле способно пронумеровать 32 768 сообщений (2 байта).
- 5) В поле Answer[1].IP помещается правильный IPv4-адрес, который будет предоставлен DNS-сервером на такой запрос.
- 6) После поля Answer[1].IP (где по спецификации протокола не должно быть данных) размещается конфиденциальная информация.
- 7) Поле Answer[1].ResourceDataLength содержит правильную информацию о длине данных (4 байта на подготовленный адрес IPv4 + длина конфиденциальных данных).

Данная теория была проверена на практике, действительно, сетевые устройства не замечают то, что пакет был изменен, считают его легитимным и не отбрасывают. Для выявления данного метода требуется более глубокий анализ пакетов, чем могут предложить стандартные межсетевые экраны. Необходимо писать специальные паттерны для систем обнаружения и предотвращения вторжений или писать специальные программы для выявления сетевой стеганографии, примером может быть обнаружение стеганографии на основе статического метода.

Список используемых источников:

1. Котенко И. В., Левшун Д. С., Чечулин А. А., Ушаков И. А., Красов А. В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров. Вопросы кибербезопасности. 2018. № 3 (27). С. 29-38.
2. Ушаков И. А., Котенко И. В., Овраменко А. Ю., Преображенский А. И., Пелёвин Д. В. Комбинированный подход к обнаружению инсайдеров в компьютерных сетях. Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 4. С. 66-71.
3. Никитин В. Н., Ковцур М. М., Юркин Д. В. Повышение защиты протоколов распределения ключей от атак вторжения в середину канала связи. Информационно-управляющие системы. 2014. № 1 (68). С. 70-75.
4. Shterenberg S. I., Krasov A. V., Ushakov I. A. Analysis of using equivalent instructions at the hidden embedding of information into the executable files. Journal of Theoretical and Applied Information Technology. 2015. Т. 80. № 1. С. 28-34
5. Штеренберг С. И., Красов А. В. Варианты вложения информации в исполнимый файл формата .INTEL HEX. Информационные технологии и телекоммуникации. 2013. Т. 1. № 4. С. 52-64.
6. Штеренберг С. И., Виткова Л. А., Андрианов В. И. Методы использования пустых секций исполнимого файла для стеговложения саморазвивающегося кода в распределенной

системе однозначного отождествления. Системы управления и информационные технологии. 2015. № 1-1 (59). С. 189-194.

7. Красов А. В., Сахаров Д. В., Ушаков И. А., Лосин Е. П. Обеспечение безопасности передачи multicast-трафика в ip-сетях. Защита информации. Инсайд. 2017. № 3 (75). С. 34-42.

8. Штеренберг С. И., Виткова Л. А., Андрианов В. И. Методы использования пустых секций исполнимого файла для стеговложения саморазвивающегося кода в распределенной системе однозначного отождествления. Системы управления и информационные технологии. 2015. № 1-1 (59). С. 189-194.

9. Ахрамева К. А., Герлинг Е. Ю., Ковцур М. М., Куликов И. А. Использование стеганографии в компьютерных играх. Телекоммуникации. 2020. № 10. С. 22-26.

10. Коржик В. И., Небаева К. А., Герлинг Е. Ю., Догиль П. С., Федянин И. А. Цифровая стеганография и цифровые водяные знаки. СПб. : СПбГУТ, 2016. 226 с.

Salita A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

The Domain name system (DNS) protocol is used to make life easier for internet users. Nowadays it is more and more difficult to trace information leaks, especially with the use of steganographic channel. This article describes one possible method of using the DNS protocol to communicate between the device and a special DNS-server.

Key words: *DNS, steganography, networks, information security.*

УДК 004.056.57
ГРНТИ 81.93.29

ПРОБЛЕМНЫЕ ВОПРОСЫ ОБНАРУЖЕНИЯ БОТНЕТ-СЕТЕЙ НА БАЗЕ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

М. А. Скорых, К. Е. Израилов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире большое распространение получили компьютерные атаки, использующие устройства Интернета вещей для построения вредоносных ботнет-сетей. Задача обнаружения такого рода атак не имеет классических решений по ряду существенных причин. В статье приводится описание 6 таких проблемных вопросов, без которых построение полноценных систем противодействия распределенным атакам будет малоэффективно.

IoT, Интернет вещей, ботнет-сеть, компьютерные атаки, Threat Intelligence

В настоящее время количество компьютерных атак (далее – КА) имеет непрерывный рост и усложнение своих принципов воздействия [1]. В роли одного из наиболее опасных источников КА как правило выступают ботнет-сети. При этом последние могут основываться не на персональных или серверных компьютерах, имеющих, как правило, полноценную защиту, а использовать маломощные устройства Интернет-вещей, в которые физически не возможно встроить системы противодействия вторжениям. Данный факт подтверждается, в том числе, опубликованным в 2016 году исходным кодом крупнейшей ботнет-сети Mirai. Одним же из наиболее очевидных и действенных этапов защиты от такого рода атак является своевременное обнаружение устройств Интернета вещей, объединенных в ботнет-сети. Однако, классические методы обнаружения не всегда оказываются действенными по причине наличия ряда проблемных вопросов, требующих первостепенного решения; их описанию и посвящена данная статья.

Описание ботнет-сетей на базе устройств Интернета вещей

Для выделения проблемные вопросы, связанных с обнаружением устройств Интернета вещей [2], объединенных в ботнет-сети (далее – IoT-ботнет), укажем их основные особенности. IoT-ботнет – это набор скомпрометированных устройств Интернета вещей, зараженных вредоносным программным обеспечением (далее – ВПО) [3]. Как правило IoT-ботнеты состоят из таких устройств как беспроводные маршрутизаторы, IP-камеры, сетевые хранилища, сервера под управлением семейства операционных систем Linux и др. Ботнеты могут содержать в своем составе следующие типы узлов [4]: сервер управления и контроля, предназначенный для «администрирования» всеми ботами; сервер распределения ВПО, хранящий образцы вредоносных скриптов и программ, которые загружают на зараженные устройства; сервер отчетов, представляющий собой, как правило, базу данных, наполняемую деталями о всех устройствах в ботнете; непосредственно боты – устройства Интернета вещей, зараженные ВПО и, соответственно, выполняющие деструктивные воздействия.

КА, генерируемые IoT-ботнетами, могут включать в себя попытки подбора паролей к различным сервисам (FTP, Telnet, SSH и др.), эксплуатации различных видов уязвимостей, сетевое сканирование, DoS- и DDoS-атаки, рассылка спама и фишинговых сообщений.

Под обнаружением же IoT-ботнета авторами понимается выявление всех его узлов, для чего в основном применяются следующие технические решения и технологии [5]: системы обнаружения атак (аббр. IDS от англ. Intrusion Detection System), технология HoneyPot (использование подставных целей для злоумышленника), методы Threat Intelligence (анализ открытых источников с целью сбора информации об актуальных уязвимостях, группировках киберпреступников и индикаторах компрометации).

Проблемные вопросы обнаружения IoT-ботнетов

Исходя из особенностей IoT-ботнетов, а также авторского опыта в сфере сетевой безопасности, предположим следующие 6 проблемных вопросов, отсутствие или недостаточность решения которых не позволяет эффективно противодействовать данному роду атак.

Вопрос №1. Определение необходимого количества и места расположения в адресном пространстве IDS и HoneyPot систем

Беспроводные маршрутизаторы, IP-камеры, сетевые хранилища и другие устройства Интернета вещей располагаются по всему миру. Злоумышленники, управляющие ботнетами, могут осуществлять компьютерные атаки на любые страны и диапазоны IP-адресов. В связи с этим возникает необходимость определения пространства IP-адресов и географического расположения для установки IDS- и HoneyPot-систем [6] для обеспечения необходимого процента обнаружения узлов ботнет-сети.

Вопрос №2. Определение размера IoT-ботнетов

Одним из важных факторов при распознавании интенсивности угроз IoT-ботнетов является оценка их размеров. Чем больше зараженных устройств в своем составе содержит IoT-ботнет, тем более мощные атаки он может проводить. Очевидно, что зафиксировать все узлы ботсети при помощи IDS и HoneyPot-систем невозможно. Задача исследователя состоит в том, чтобы по частичным данным о функционировании ботнета с заданной точностью определить его размер, и как следствие – возможную мощность компьютерных атак [7]. Существующие же подходы к обнаружению обычно не обладают точностью измерения размера [5].

Вопрос №3. Обнаружение атак, производящих вредоносные действия вне защищаемой системы

Технологии обнаружения IoT-ботнетов, основанные на использовании IDS и HoneyPot, подразумевают, что средства обнаружения устанавливаются на стороне защищаемой организации, в связи с чем возникает проблема обнаружения специфических КА, не затрагивающих защищаемую сеть напрямую. В качестве примера, можно привести DDoS-атаку типа «DNS-resolver». В данной атаке генерируемый IoT-ботнетом трафик инициирует большое количество DNS-запросов от легитимных DNS-серверов к NS-серверу, что оказывает деструктивное воздействие на его работу, и как следствие,

невозможность разрешения доменного имени контролируемого сайта. Проблема заключается в том, что зловредный трафик не попадает на средства обнаружения атак [8], и следовательно, определить узлы IoT-ботнета не представляется возможным.

Вопрос №4. Определение принадлежности источника КА к IoT-ботнету

Как правило IoT-ботнеты могут осуществлять определенный перечень КА; обычно в него входит перебор пароля по протоколам Telnet и SSH, DDoS-атаки различного типа, а также применение эксплойтов, специфичных для устройств Интернета вещей. Однако, источниками вышеперечисленных КА могут быть не только IoT-ботнеты, но и другие виды ботнетов или одиночные хакеры. Исходя из этого возникает сложность в определении того, является ли источник деструктивных действий IoT-устройством или нет [9]. Например, IDS может зафиксировать атаку, связанную с уязвимостью CVE-2016-6563 в реализации протокола HNP в маршрутизаторах производства фирмы D-Link. Эксплуатация данной уязвимости характерна для IoT-ботнета, но ее может эксплуатировать и любой специалист в области информационной безопасности. Таким образом, при принятии решения о включении атакующего узла в список зараженных IoT-устройств возможно возникновение ошибок первого и/или второго рода.

Вопрос №5. Обнаружение источников КА, использующих подмену IP-адресов

IDS могут обнаруживать КА IoT-ботнетов, однако это не всегда позволяет выявить конкретные IP-адреса ботов. В качестве примера можно привести DDoS-атаки, основанные на подмене IP-адреса источника (DNS-Amplification, NTP-amplification). Исходные IP-адреса ботов будут выявлены только в том случае, если IoT-ботнет генерирует КА с целью получения несанкционированного доступа (подбор паролей, эксплуатация уязвимостей) или сканирования.

Вопрос №6. Обнаружение IoT-ботнетов методами Threat Intelligence

С ростом сообщества информационной безопасности, появляется все больше открытых ресурсов, содержащих информацию об источниках КА, базах репутации IP-адресов, актуальном ВПО и его центрах управления, базах результатов сканирований публичных IP-адресов. Агрегируя информацию из множества открытых источников, появляется возможность обнаруживать вредоносные узлы сети Интернет, в том числе входящие в IoT-ботнеты. Например, используя базу репутации AbuseIPDB можно находить атакующие IP-адреса, а далее с помощью поисковой системы Shodan определять принадлежность конкретного IP-адреса к определенному классу устройств (IP-камеры, сетевые хранилища и др.). Однако, на данный момент, авторами еще не найдено алгоритма, который позволял бы с использованием методов Threat Intelligence определить с заданной точностью, является ли атакующий IP-адрес частью IoT-ботнета или нет.

В работе выделены и описаны проблемные вопросы, игнорирование которых не позволит эффективно противодействовать ботнет-сетям, построенным на основе устройств Интернета вещей. Каждый проблемный вопрос обладает собственной спецификой, учет которой позволит строить

соответствующие методы противодействия. При этом, какого-либо наиболее первоочередного для решения вопроса на данном этапе выделить нельзя. Таким образом, продолжение исследования авторы видят в более глубокой проработке причин, мешающих противодействию распределенным атакам с применением IoT-ботнетов, а также разработка и тестирование соответствующих методов защиты от них.

Список используемых источников:

1. Абдуллин Т. И., Баев В. Д., Буйневич М. В., Бурзунов Д. Д., Васильева И. Н., Галиуллина Э. Ф. Цифровые технологии и проблемы информационной безопасности. СПб. : СПГЭУ, 2021. 163 с.
2. Kotenko I., Izrailov K., Buinevich M. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches // Sensors. 2022. Vol. 22. Iss. 4. PP. 1335. DOI: 10.3390/s22041335
3. Скорых М. А. Применение фреймворка Zeek и elk-стека для анализа рассылок вредоносного программного обеспечения // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы X междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 24-25 февр. 2021 г.. 2021. СПб. : СПбГУТ, 2021. С. 658-661.
4. Бухарев Д. А., Вагин С. В., Соколов А. Н. Защита устройств интернета вещей от Mirai-подобных вирусных программ-червей // Вестник УрФО. 2018. № 4(30). С. 11–19.
5. Ahmad Karim, Rosli Bin Salleh, Muhammad Shiraz, Syed Adeel Ali Shah, Irfan Awan, Nor Badrul Anuar Botnet detection techniques: review, future trends, and issues // Journal of Zhejiang University-SCIENCE C (Computers & Electronics). 2014. Vol. 15 Iss 11. PP. 943-983. ISSN: 1869-1951
6. Поляков В. В. Система honeypot как инструмент сбора информации для противодействия киберпреступности // Библиотека криминалиста. Научный журнал. 2017. № 1 (30). С. 250-254.
7. Тарасов Я. В. Методический подход к обнаружению DDOS-атак малой мощности // Информатика и системы управления : материалы Восьмой всерос. научно-технич. конф., Москва, 06–07 дек. 2017 г. М. : МГТУ им. Н.Э. Баумана, 2017. С. 479-482.
8. Скорых М. А., Израйлов К. Е., Башмаков А. В. Задачаориентированное сравнение средств анализа сетевого трафика // Теория и практика обеспечения информационной безопасности : материалы Всерос. научно-теоретич. конф., Москва, 03 дек. 2021 г.. М. : МТУСИ, 2021. С. 103-107.
9. Kotenko I., Izrailov K., Buinevich M. Analytical Modeling for Identification of the Machine Code Architecture of Cyberphysical Devices in Smart Homes // Sensors. 2022. Vol. 22. Iss. 3. PP. 1017. DOI: 10.3390/s22031017

Skorykh M., Izrailov K.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunications

Problematic issues of botnet detection based on IoT devices.

In the modern world, computer attacks that use Internet of Things devices to build malicious botnet networks have become widespread. The task of detecting such attacks does not have classical solutions for a number of significant reasons. The article provides a description of 6 such problematic issues, without which the construction of full-fledged systems to counter distributed attacks will be ineffective.

Key words: *IoT, Internet of Things, botnet network, computer attack, Threat Intelligence.*

УДК 004.056
ГРНТИ 81.93.29

РЕАЛИЗАЦИЯ МОДУЛЬНЫХ ВЫЧИСЛЕНИЙ С БОЛЬШИМИ ЧИСЛАМИ НА ОСНОВЕ АЛГОРИТМА МОНТГОМЕРИ

Е. В. Таров, С. Н. Шемякин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрен принцип работы алгоритма Монтгомери. Проведен сравнительный анализ обычного алгоритма деления в столбик и алгоритма модульного умножения с использованием алгоритма Монтгомери. Сравнение проводилось по результатам программы, написанной на языке программирования Python, которое показало эффективность алгоритма Монтгомери.

криптография, информационная безопасность, алгоритм Монтгомери, модульная арифметика, умножение по модулю

Многие криптографические методы защиты информации основываются на модульной арифметике [1, 2]:

- в RSA криптограмма формируется по правилу

$$c_i = M_i^{e_A} \bmod n_A,$$

где размер модуля n_A рекомендуется брать 1024 и 2048 бит;

- в алгоритме Диффи-Хеллмана для вычисления общего ключа применяют формулу

$$K = \alpha^{yx} \bmod p,$$

где p порядка 1024 бит, y и x порядка 2048 и более бит;

- в криптосистеме Эль-Гамала часть открытого ключа формируется по правилу

$$\alpha^a \bmod p,$$

где p имеет разрядность 1024 бит;

- в ГОСТ 34.10-2018 для формирования цифровой подписи используется модульное умножение для чисел разрядности 256 бит.

Выполнение модульных операций с числами большой разрядности (1024 и более бит) на 8/16/32/64 разрядных вычислительных системах при помощи стандартных методов, например, умножения и деления в столбик требует больших временных и вычислительных затрат [3]. Потому поиск вычислительно эффективных алгоритмов для работы с большими числами является актуальной задачей.

Для решения задачи умножения больших чисел следует воспользоваться алгоритмом Монтгомери. Использование данного алгоритма позволяет

избавиться от операций деления и умножения, заменяя их на более эффективные операции побитового сдвига [4].

В данной работе изложен принцип работы алгоритма Монтгомери, проведен сравнительный анализ времени выполнения обычного алгоритма деления в столбик и алгоритма модульного умножения с применением алгоритма Монтгомери для чисел больших размерностей.

Основная идея алгоритма Монтгомери заключается в замене приведения по исходному модулю N в кольце классов вычетов Z_N на определение остатка в другом кольце классов вычетов Z_R при помощи более удобного модуля R . Модуль R выбирается из соображений простоты выполнения операций умножения и деления с остатком. Кольцо Z_R называют кольцом Монтгомери [5, 6].

Модуль R задается следующим образом [7]:

$$R = \beta^m (1),$$

где m – количество разрядов в записи модуля N в β -ичной системе счисления, β – основание системы счисления. При этом $R > N$.

Далее при помощи расширенного алгоритма Евклида находится линейное разложение

$$Rr - Nn = 1 (2),$$

где $r = R^{-1} \bmod N$, $n = (-N)^{-1} \bmod R$.

И вычисляется значение $R^2 \bmod N$.

Для того чтобы произвести замену определения остатка в исходном кольце классов вычетов Z_N на определение остатка в кольце Монтгомери Z_R нужно произвести отображение числа из Z_N в Z_R . Обозначим данное отображение как $\varphi_R(z)$. Оно задается следующим равенством

$$\varphi_R(z) = zr \bmod N (3),$$

где z – целое положительное число, меньшее N .

Данное отображение вычисляют при помощи алгоритма 1.

Алгоритм 1: вычисление образа при отображении $\varphi_R(z)$ одного числа z из исходного кольца Z_N в кольцо Монтгомери Z_R [7].

Пусть дано целое положительное число $z \in Z_N$.

1. Вычислить значение

$$m = zn \bmod R (4);$$

2. Вычислить целое число

$$t = \frac{z+mN}{R} (5);$$

Результат отображения равен t , если t меньше N , иначе результат равен разнице чисел t и N .

Для случая, когда нужно отобразить не одно число, а произведение двух чисел x и y можно было бы умножить их в исходном кольце Z_N и применить к полученному результату алгоритм 1, но существует более эффективный способ.

Обозначим данное отображение как $\varphi_R(x, y)$. Оно задается следующим равенством

$$\varphi_R(x, y) = xyr \bmod N \quad (6),$$

где x, y – целые положительные числа, меньшие N .

Данное отображение вычисляются при помощи алгоритма 2 [7].

Алгоритм 2: вычисление образа при отображении $\varphi_R(x, y)$ произведения чисел x и y из исходного кольца Z_N в кольцо Монтгомери Z_R .

Пусть даны два целых положительных числа $x, y \in Z_N$. Алгоритм состоит в построении последовательности чисел z_0, \dots, z_m . Здесь $z_0 = 0$, и по найденному z_i следующее число z_{i+1} вычисляется последовательно следующим образом:

1. Вычислить значение

$$u = z_i + x_i y \bmod \beta \quad (7);$$

2. Вычислить значение

$$v = un \bmod \beta \quad (8);$$

3. Вычислить очередное значение последовательности

$$z_{i+1} = \frac{z_i + x_i y + vN}{\beta} \quad (9).$$

После того как был найден последний элемент z_m , положить, что результат отображения равен z_m , если z_m меньше N , иначе результат равен разнице z_m и N .

Рассмотрим реализацию вычисления умножения двух чисел x и y по модулю N с использованием алгоритма Монтгомери – алгоритм 3.

Алгоритм 3: вычисление модульного произведения двух чисел с применением алгоритма Монтгомери [7].

Пусть дан целый положительный нечетный модуль N и два целых положительных числа $x, y \in Z_N$.

1. При помощи алгоритма 2 вычислить

$$z_R = \varphi_R(x, y) \quad (10);$$

2. При помощи алгоритма 2 вычислить

$$\varphi_R(z_R, (R^2 \bmod N)) \quad (11).$$

В итоге получаем искомое значение $\varphi_R(z_R, (R^2 \bmod N)) = xy \bmod N$.

Корректность данного алгоритма следует из того, что $z_R = \varphi(x, y) = xyr \bmod N$ при этом $\varphi_R(z_R, (R^2 \bmod N)) = z_R R^2 r \bmod N = xy R^2 r^2 \bmod N = xy \bmod N$. Также учтем, что значение $R^2 \bmod N$ было вычислено заранее.

Рассмотрим пример использования алгоритма 3 с конкретными числами.

Дано: $x = 16, y = 21, N = 23, \beta = 10, m = 2$.

Нужно найти: $x * y \bmod N$.

Предварительные вычисления: $R = 10^2, r = 3, n = 13, R^2 \bmod N = 18$.

Запись числа x в системе счисления β имеет вид:

$$x = \sum_{i=0}^{m-1} x_i \beta^i = 6 * 10^0 + 1 * 10^1$$

Произведем модульное умножение $xy \bmod N$ по алгоритму 3.

На первом шаге алгоритма 3 вычислим $z_R = \varphi_R(x, y)$ при помощи алгоритма 2, где $x=16, y=21$.

$$1. u = 0 + 6 * 21 \bmod 10 = 6$$

$$v = 6 * 13 \bmod 10 = 8$$

$$z_1 = \frac{0 + 6 * 21 + 8 * 23}{10} = \frac{310}{10} = 31$$

$$2. u = 31 + 1 * 21 \bmod 10 = 2$$

$$v = 2 * 13 \bmod 10 = 6$$

$$z_2 = \frac{31 + 1 * 21 + 6 * 23}{10} = \frac{190}{10} = 19$$

$$\text{В итоге: } z_R = \varphi_R(xy) = z_2 = 19$$

На втором шаге алгоритма 3 вычислим $\varphi_R(z_R, (R^2 \bmod N))$ при помощи алгоритма 2, где $z_R=19, R^2 \bmod N=18$.

$$1. u = 0 + 9 * 18 \bmod 10 = 2$$

$$v = 2 * 13 \bmod 10 = 6$$

$$z_1 = \frac{0 + 9 * 18 + 6 * 23}{10} = \frac{300}{10} = 30$$

$$2. u = 30 + 1 * 18 \bmod 10 = 8$$

$$v = 8 * 13 \bmod 10 = 4$$

$$z_2 = \frac{30 + 1 * 18 + 4 * 23}{10} = \frac{140}{10} = 14$$

$$\text{В итоге: } \varphi_R(z_R, (R^2 \bmod N)) = z_2 = 14$$

Полученный результат $\varphi_R(z_R, (R^2 \bmod N)) = 14$ и будет являться искомым значением.

В настоящее время мною была разработана программа на языке программирования Python3, в которой был реализован обычный алгоритм деления в столбик и алгоритм модульного умножения с применением алгоритма Монтгомери. Данная программа позволила сравнить временные затраты данных алгоритмов. В результате запуска программы была получена диаграмма, представленная на рис. 1, а также сформирована таблица результатов – таблица 1.

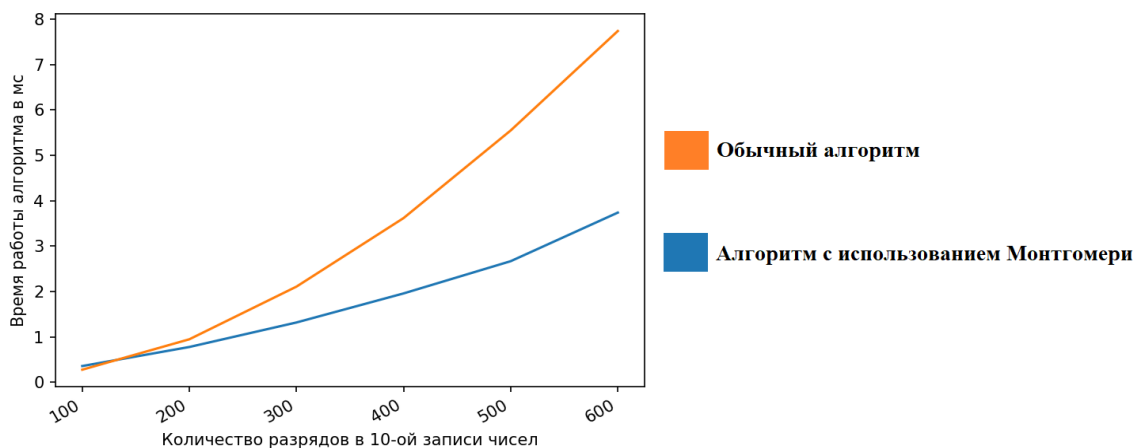


Рис. 1. Графическое представление результатов

ТАБЛИЦА 1. Результаты измерения

Количество разрядов в 10-ой записи чисел	Время работы обычного алгоритма, мс	Время работы алгоритма Монтгомери, мс	Отношение времени выполнения обычного алгоритма к Монтгомери
100	0,28	0,36	0,78
200	0,95	0,78	1,21
300	2,11	1,32	1,59
400	3,62	1,96	1,85
500	5,55	2,67	2,08
600	7,74	3,36	2,30

Алгоритм Монтгомери позволил получить выигрыш во времени вычисления модульного умножения в 1,21 (последний столбик) или на 21% при числе разрядов 200 (первый столбик) и в 2,30 или на 130% при числе разрядов 600 по сравнению с обычным алгоритмом деления в столбик.

В дальнейшем необходимо оценить выигрыш при использовании алгоритма Монтгомери в криптосистемах RSA, Эль-Гамала, в алгоритме Диффи-Хеллмана и ГОСТ 34.10-2018 при работе с большими числами (содержащих примерно 3000 двоичных разрядов).

Список используемых источников:

1. Коржик В.И., Яковлев В.А. Основы криптографии: учебное пособие. Санкт-Петербург: Интермедия, 2017. – 312 с.

2. Коржик В.И., Просихин В.П. Основы криптографии: учебное пособие по специальности 210403 "Защищенные телекоммуникационные системы связи". Санкт-Петербург: Линк, 2008.

3. Панкратова, И. А. Теоретико-числовые методы криптографии: учебное пособие / И. А. Панкратова ; Томский государственный университет. – Томск : Национальный исследовательский Томский государственный университет, 2009. – 120 с.

4. Кнут Д.Э. Искусство программирования. Том 1. Основные алгоритмы - М.: Мир, 1976. - 735 с.

5. Montgomery P.L. Modular multiplication without trial division. // Mathematics of computation. 1985. Vol. 44, No. 170. P. 519-521.

6. Лобес М.В., Червяков Н.И. Повышение скорости выполнения операции модульного возведения в степень многозначных чисел // Инфокоммуникационные технологии. 2009. № 7. С. 8-12.

7. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. -М.: Лань, 2011.-400 с.

Tarov E., Shemyakin S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunications

Implementation of modular calculations with large numbers based on the montgomery algorithm.

The principle of operation of the Montgomery algorithm is considered. A comparative analysis of the usual column division algorithm and the algorithm for calculating modular multiplication using the Montgomery algorithm is carried out. The comparison was based on the results of a program written in the Python programming language, which showed the effectiveness of the Montgomery algorithm.

Key words: *cryptography, information security, Montgomery algorithm, modular arithmetic, multiplication modulo.*

УДК 004.3
ГРНТИ 20.53.23

SDN ЦОД на базе Cisco ACI

Д. А. Ульянов, А. М. Гельфанд

Санкт-Петербургский государственный университет телекоммуникаций им. М. А. Бонч-Бруевича

Ключевые особенности SDN состоят в разделении процессов передачи и управления данными, централизации управления сетью при помощи унифицированных программных средств, виртуализации физических сетевых ресурсов. Главными преимуществами использования программно-конфигурируемых сетей является снижение финансовых и временных затрат, снижение трудозатрат, а также в увеличение надежности за счёт автоматизации низкоуровневых операций по управлению сетью. В статье рассматривается описание решения SDN для центров обработки данных на базе Cisco Application Centric Infrastructure.

ЦОД, SDN, ACI, Инфраструктура, топология, гипервизор

Cisco ACI (Application Centric Infrastructure) – Информационная инфраструктура, ориентированная на разворачивание приложений. Предоставляет целостную архитектуру с централизованной автоматизацией и профилями приложений на основе политик. ACI обеспечивает гибкость используемого программного обеспечения и масштабируемость аппаратных ресурсов.

Архитектура Cisco ACI с точки зрения топологии представляет собой 2-х уровневую маршрутизируемую фабрику, состоящую из Spine (ядро) и Leaf (доступ) коммутаторов. Коммутаторы Cisco Nexus 93180 в архитектуре представляют собой Leaf коммутаторы. Такая фабрика, вне зависимости от размеров, управляется с помощью кластера централизованных контроллеров: Cisco APIC. Управление осуществляется из графического интерфейса с помощью сервисных профилей в которых описываются связи между серверами приложений. Каждый коммутатор интерпретирует сервисный профиль в конкретную конфигурацию на коммутаторе, включая отдельные сегменты и связь между сегментами. Работа фабрики не нарушается, даже в случае, если представить невероятное событие - выход из строя всех контроллеров APIC кластера. Помимо бизнес-задач, архитектура Cisco ACI обладает дополнительными преимуществами:

- а) упрощение возможности автоматизации за счет модели применения политик;
- б) централизованный контроль с функцией мониторинга состояния работоспособностью приложений в режиме реального времени;
- в) открытое код ПО для гибкой интеграции с группами DevOps и партнерами по экосистеме;
- г) масштабирование производительности и многопользовательский режим оборудования;

д) поддержка виртуализации фабрики на проекты, подразделения, заказчиков и пр. то есть возможность монетизации услуг ЦОД в рамках группы компаний Ленэнерго;

е) встроенная безопасность, модель черного списка, когда только в случае соответствующих разрешений возможен трафик между приложениями и пользователями;

ж) поддержка всех видов гипервизоров; Возможность использования как физического, так и виртуализованного сервера при соблюдении технических параметров взаимодействий приложений;

Из-за ограничения оптических линий связи между ЦОД (2 оптические трассы), рекомендованной схемой является схемой с двумя фабриками в каждом из ЦОД. Другие возможные варианты дизайна подразумевают использование минимум 4 оптических трасс (рис.1).

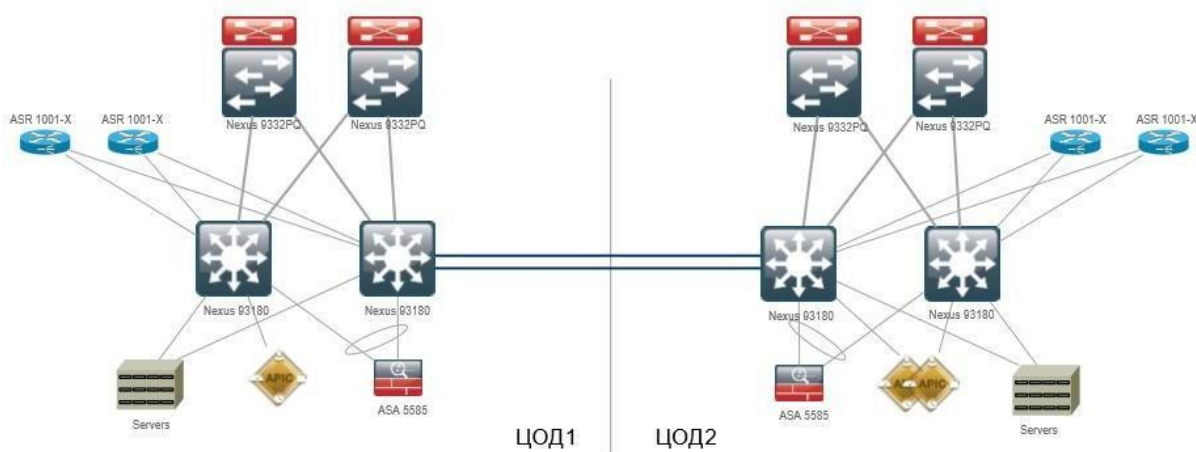


Рис.1. Целевая схема ЦОД ПАО «Ленэнерго» на основе архитектуры Cisco ACI

Применение центров обработки данных уже давно стало промышленным стандартом для больших телекоммуникационных инфраструктур, которое позволяет применять все современные механизмы обеспечения стабильности и надежности предоставления услуг для бизнеса.

Следующим этапом требуется виртуализировать сетевую инфраструктуру для обеспечения автоматизации эксплуатационных процессов, пуско-наладочных и аварийно-восстановительных работ, требующих больших изменений в сети связи.

Cisco Systems, является безоговорочным лидером в производстве решений для сетей связи. Имеет развитую систему технической поддержки своих решений. Имеет сеть филиалов сертифицирования и обучения специалистов по своим решениям.

Телекоммуникационная сеть ПАО «Ленэнерго» насчитывает более 1500 активных сетевых элементов, 95% из которых телекоммуникационное оборудование компании Cisco. Полная программно-аппаратная поддержка существующей телекоммуникационной инфраструктуры, а также безоговорочное лидерство в решениях по программно-определяемым сетям

компании Cisco Systems является определяющими факторами рассмотрения Cisco ACI (Application Centric Infrastructure).

Список используемых источников:

1. Красов А. В., Левин М. В. Возможности управления трафиком в рамках концепции SDN // Актуальные проблемы инфотелекоммуникаций в науке и образовании : IV Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 03–04 марта 2015 г. СПб. : СПбГУТ, 2015. С. 350-354.
2. Красов А. В., Гельфанд А. М., Коржик В. И. Построение доверенной вычислительной среды. СПб. : ИП Петрив Р. Б., 2019. 108 с. – ISBN 978-5-6043143-2-6.
3. Красов А. В., Левин М. В., Штеренберг С. И., Исаченков П. А. Модель управления потоками трафика в программно-определяемой сети с изменяющейся нагрузкой // Научные технологии в космических исследованиях Земли. 2016. Т. 8. N 4. С. 70-74.
4. Савинов Н. В., Токарева К. А., Ушаков И. А. Исследование модели сети ЦОД на основе политик Cisco ACI // Защита информации. Инсайд. 2019. N 4(88). С. 32-43.
5. Сахаров Д. В., Красов А. В., Ушаков И. А., Орлов Г. А. Защищенная модель программно-определяемой сети в среде виртуализации KVM // Электросвязь. 2020. N 3. С. 26-32. DOI 10.34832/ELSV.2020.4.3.004.
6. Исаченков П. А., Красов А. В., Левин М. В. Исследование эффективности метода управления потоками трафика на основе информации о нагрузке в программно-определяемой сети с неравными метриками маршрутов // Современная наука и инновации. 2017. N 2(18). С. 32-38.
7. Волкогонов В. Н., Волостных В. А., Гельфанд А. М., Катасонов А. И. Способы коммутации пакетов в сетях cisco // Национальная безопасность России: актуальные аспекты : материалы Всерос. научно-практич. конф., Санкт-Петербург, 28-31 мая 2018 г. СПб. : ГНИИ "Нацразвитие", 2018. С. 31-35.
8. Катасонов А. И., Цветков А. Ю., Андрианов В. И. CISCO TRUSTSEC // Информационные технологии и телекоммуникации. 2017. Т. 5. N 4. С. 85-95.
9. Krasov A., Vitkova L., Pestov I. Behavioral analysis of resource allocation systems in cloud infrastructure // Proceedings - 2019 International Russian Automation Conference, RusAutoCon 2019. 2019. С. 8867699.

Ulyanov D., Gelfand A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunications

SDN data center based on Cisco ACI SDN data center powered by Cisco ACI.

Key features of SDN are the separation of data transfer and management processes, centralization of network management using unified software tools, virtualization of physical network resources. The main advantages of using software-defined networks are reduced financial and time costs, reduced labor costs, as well as increased reliability due to the automation of low-level network management operations. This article describes an SDN solution for data centers based on the Cisco Application Centric Infrastructure.

Key words: *data center, SDN, ACI, Infrastructure, topology, hypervisor.*

УДК 004.75
ГРНТИ 81.93.29

МЕТОДИКА АНАЛИЗА MAX PATROL SIEM В ОРГАНИЗАЦИИ

А. А. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В стандартном понимании SIEM-системы исключительно забирают и обрабатывают данные, а также сигнализируют администратору о вероятной опасности. Блокировка процессов, вызывающих подозрение, карантин и прочие меры реагирования в задачи не входят. Однако, в последнее время под термином SIEM часто объединяют как системы сбора и обработки данных, так и системы, позволяющие реагировать на информацию и предпринимать действия. В данной статье методика анализа отечественного ПО MaxPatrol SIEM в организации.

SIEM-система, анализ SIEM-системы, MaxPatrol SIEM, информационная безопасность, отечественный производитель SIEM

Проблема наблюдения инцидентов информационной безопасности, обработки сбора огромного количества событий от различных источников и средств для защиты данных известна каждому IT-специалисту. В новейших системах защиты информации используются множества различных средств и каждое генерирует тысячи и миллионы событий ежедневно. Для решения проблемы отслеживания и мониторинга созданы решения, названные SIEM – система мониторинга и выявления событий информационной безопасности. Российская компания Positive Technologies создала собственный продукт для управления событиями – MaxPatrol SIEM [1].

MaxPatrol SIEM позволяет организовать цикл работы с событиями безопасности, который включает в себя следующие этапы [2]:

1. Сбор информации из различных источников - в стандартный комплект входит поддержка нескольких форматов и протоколов: Syslog, Windows Event log, Windows File log, Windows WMI log, NetFlow, ODBC log, SSH File log, CheckPoint LEA, SNMP Traps. Во время сбора поддерживается разбор текстовых файлов, форматов JSON, TABULAR, Windows EventLog.

2. Нормализация событий – каждый инцидент безопасности подвергается нормализации и преобразовывается в структурированный объект. У данных объектов есть несколько обязательных полей – дата, время, ID, актив (объект), к которому относится инцидент, тип действия и состояние. Формулы нормализации могут быть изменены или добавлены новые самим заказчиком либо вендором в рамках поддержки.

3. Фильтрация инцидентов – удаление событий, не относящихся к безопасности.

4. Агрегация – объединение инцидентов во избежание появления огромного количества ненужной лишней информации.

5. Корреляция – анализ связей между разными событиями по определенным правилам и автоматическое создание инцидентов в случае выявления нарушений.

6. Архивация – хранение событий и состояний наблюдаемых систем для осуществления глубокого анализа и расследования.

Корреляция инцидентов безопасности – главная функция SIEM-систем. Корреляция помогает значительно уменьшить работу администраторов безопасности по работе с журналами логирования и сосредоточиться исключительно на критических событиях. В состав продукта входит большая база с правилами для поиска инцидентов и поддерживается возможность обновления правил и их редактирование прямо в интерфейсе продукта. Каждое правило состоит из условий для поиска инцидентов, параметров глубины поиска, списка исключений и сценариев действий при срабатывании правил.

Работа с событиями безопасности в MaxPatrol SIEM выстроена как процесс, включающий в себя автоматическое создание инцидентов при срабатывании правил корреляции, а также возможность назначения ответственных сотрудников для обработки инцидентов и поддержкой разных этапов и стадий расследования.

Одна из особенностей MaxPatrol SIEM – это работа с активами и инфраструктурой – персональными компьютерами и оборудованием в локальной сети. Данный продукт автоматически собирает данные об IT-инфраструктуре, выстраивает топологию, проводит анализ версий операционных систем (ОС) и установленных программ, сканирует порты и службы, а также иные функции сканера безопасности.

MaxPatrol SIEM – это продукт состоящий из множества компонент (рис. 1):

- Core – центральный компонент, осуществляющий управление другими компонентами в системе и хранение конфигурации всех активов – данных о ПК и устройствах в сети.

- Server – второй компонент, выполняющий хранение, агрегацию, фильтрацию, нормализацию и корреляцию инцидентов и данных в трафике.

- Agent – модульная платформа для сканирования сети и сбора информации, включающий в себя:

- Scanner – компонент сканера для сбора данных о сети, поиска оборудования, проведения сканирования для выявления уязвимостей, открытых портов и запущенных служб.

- Log Collector – модуль для сбора инцидентов безопасности от внешних продуктов через протоколы взаимодействия.

- Storage – модуль хранения событий. Помимо “сырых” данных хранит нормализованные и коррелированные события.

- Knowledge Base – база знаний, хранящая формулы агрегации, нормализации, корреляции, обогащения и табличные списки. Именно через эту базу проходят пользовательские правила и формулы, которые затем проверяются и заносятся в центральный компонент Core.

– UCS (Update and Confirmation Service) – модуль обновления системы. Через него проходят обновления системы и её компонентов.

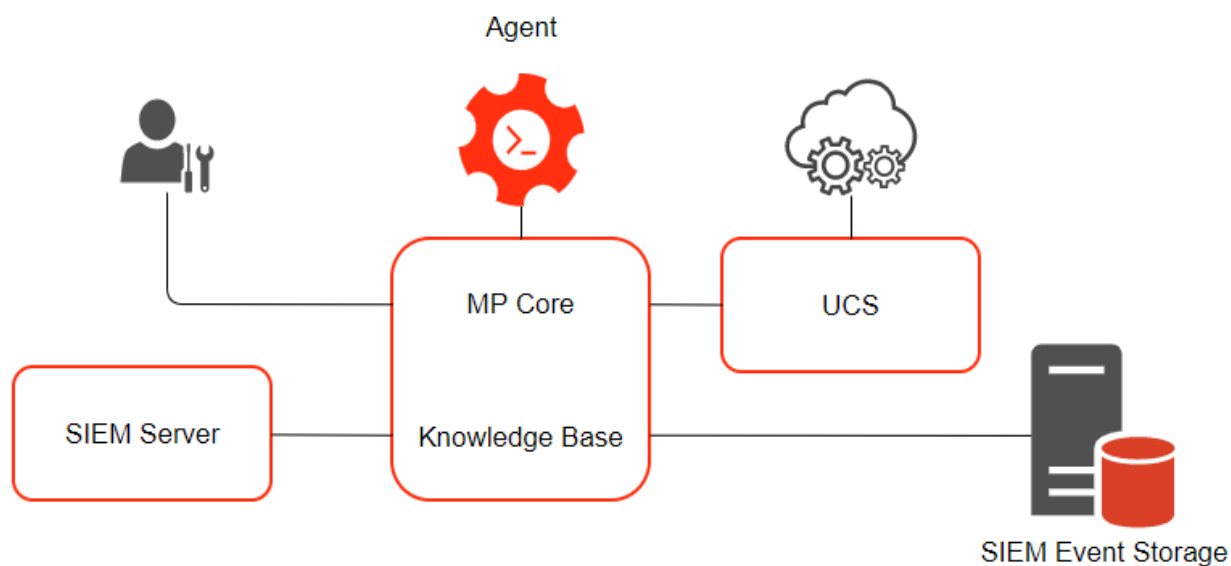


Рис. 1. Архитектура MP SIEM

Систему можно установить, как в программном режиме (виртуализация), так и в аппаратном (на физических серверах). Помимо этого, существует несколько вариантов развертывания системы, зависящие от EPS (количества регистрируемых событий в секунду) и особенностей организации [3].

Работа с продуктом выполняется посредством веб-интерфейса, подключением к компоненту Core. Доступ выдается на ролевой основе. Также отдельным пользователям доступ может быть ограничен по группам узлов сети – активам, разрешив управление только оборудованием в зоне ответственности.

Управление оборудованием в MaxPatrol SIEM осуществляется в разделе “Активы”. По каждому элементу существует информация о системе, список уязвимостей и история состояний. Дополнительно в продукте выстраивается топология сети с отображением коммутации сетевых узлов. Данные для построения графа связей берутся на основе сканирования хостов сети, анализа журналов логирования, сетевого трафика.

Настройка сбора событий содержит в себе 4 основных группы: учетные записи, профили сбора данных, управление задачами и корреляцией. Профили сбора данных представляют собой параметры и правила для реализации доступа к удаленному узлу и сбора данных с этих узлов. Продукт предоставляет множество предустановленных профилей сбора, но также предусмотрена возможность редактирования или создания собственных.

Активы могут быть распределены по группам, один актив может находиться в нескольких группах. Группы могут быть сформированы администратором или автоматически на основе правил. По каждому активу и группам настраиваются метрики контекста CVSS (Common Vulnerability Scoring System) – информация о параметрах, критичности оборудования, требования доступности, вероятность нанесения ущерба и другие.

Инциденты в MaxPatrol SIEM могут быть созданы двумя способами – вручную при помощи интерфейса или автоматически на основе специальных правил. К инцидентам могут быть привязаны задачи – рабочие элементы для проведения расследования операторами. Также практически для каждого элемента системы предоставляется функция отображения статистики, построения графиков и отчетов. Отчеты содержат описание, графики и разнообразную информацию об активах, инцидентах, задачах и событиях.

Раздел мониторинга позволяет на основе графиков отслеживать состояние системы сбора событий. Графики показывают количество полученных и обработанных событий из разных источников. Отдельно возможно вывести данных о числе исходных событий и сравнить с числом нормализованных и отфильтрованных. По графикам предусмотрены разнообразные настройки и фильтры.

Обработка инцидентов с различного оборудования в локальной сети – трудоёмкая задача, которая не может выполняться без автоматизации. Система безопасности MaxPatrol SIEM помогает IT-специалистам по безопасности взять под контроль функционирование защищаемых активов. В заключении можно выразить основные достоинства системы:

- Модульность продукта;
- Правила корреляции устойчивы к изменениям инфраструктуры;
- Система нормализации событий;
- Поддержка кастомизации продукта;
- Система задач;
- Но в данной системе также присутствуют и некоторые недостатки, такие как:
 - Меньшее число коннекторов к целевым системам “из коробки”;
 - Отсутствие эвристических механизмов анализа инцидентов, механизмов глубокого анализа инцидентов, поиска аномалий и других сложных технических методов обнаружения инцидентов;
 - Множество дополнительных функций доступны только за дополнительную покупку модулей, что значительно повышает стоимость продукта по сравнению с аналогами других производителей;

Список используемых источников:

1. Max Patrol SIEM. Обзор системы управления событиями информационной безопасности: [Электронный ресурс] // PVSM. М., 2010-2022. URL: <https://www.pvsm.ru/informatsionnaya-bezopasnost/351757> (Дата обращения 27.10.2022).
2. What is SIEM? How it works? Why it is required?: [Электронный ресурс] // ManageEngine. 2022. URL: <https://www.manageengine.com/log-management/siem/what-is-siem.html> (Дата обращения 25.10.2022).
3. MaxPatrol – система контроля защищенности и соответствия стандартам: [Электронный ресурс] // Positive technologies. М., 2022. URL: <https://www.ptsecurity.com/ru-ru/products/mp8/#architecture> (Дата обращения 20.10.2022).

Filippov A.

The Bonch-Bruевич Saint-Peterburg State University of Telecommunications

Methodology for the analysis of max patrol siem in the organization.

MaxPatrol SIEM analysis methodology in the organization In the standard sense, SIEM systems exclusively collect and process data, as well as signal the administrator about a possible danger. Blocking suspicious processes, quarantine and other response measures are not included in the tasks. However, recently, the term SIEM often combines both data collection and processing systems and systems that allow you to respond to information and take action. In this article, the methodology for analyzing the domestic MaxPatrol SIEM software in the organization.

Key words: *SIEM system, SIEM system analysis, MaxPatrol SIEM, information security, domestic SIEM manufacturer.*

УДК 004.056
ГРНТИ 81.93.29

БЕЗОПАСНЫЙ ОБМЕН ДАННЫМИ И СХЕМА ДОСТУПА ЧЕРЕЗ БЛОКЧЕЙН

Х. А. Джораев

Санкт-Петербургский государственный университет телекоммуникаций им. М. А. Бонч- Бруевича

С быстрым ростом сетевых устройств объем совместно используемых данных со временем продолжает увеличиваться, т. е. устройства Интернета вещей (IoT) могут генерировать зеттабайты данных в ближайшие несколько лет. Согласно последней версии Общего регламента по защите данных (GDPR), пользователи имеют право полностью контролировать свои личные данные. Многие поставщики веб-услуг также предоставляют пользователям некоторые возможности для управления данными. Тем не менее, по-прежнему сложно исследовать, как они осуществляют эти действия. Необходимо принять дополнительные меры для защиты доступа к данным. Сосредоточившись на этой проблеме, в этой работе мы разрабатываем схему, которая использует смарт-контракт и блокчейн для обеспечения безопасного обмена данными и среды доступа. В нашей схеме есть три основные стороны и каждая из них имеет свою пару ключей для шифрования и подписи данных. Мы также разрабатываем четыре основных смарт-контракта для разных сторон и обсуждаем, какие виды данных должны быть неизменными и размещаться в сети. В ходе оценки мы изучаем производительность нашей схемы на различных платформах, таких как Ethereum с EtHash, Ethereum с Clique и Hyperledger. Анализ нескольких потенциальных атак показал, что наша схема жизнеспособна и эффективна

шифрование данных, технология блокчейн, контроль доступа, безопасность и конфиденциальность данных, смарт-контракт

На ранней стадии компьютерной коммуникации обмен цифровой информацией ограничен либо в закрытой локальной сети, либо в обмене физическими носителями. Несколько вариантов пути ограничивают скорость распространения информации. Однако совершенствование телекоммуникационных технологий позволяет легко получать доступ как к людям, так и к услугам через обширную глобальную сеть, которая может быть сплетена из множества небольших локальных сетей. Хотя в 90-е годы узкополосное подключение к Интернету стало доступным, ограниченная пропускная способность сохраняла однонаправленность потока информации, поскольку загрузка контента из помещения клиента обходится гораздо дороже, чем загрузка. Для фирм, которые хотели бы собирать личные данные для анализа, может не быть благоприятной среды. Однако, когда наступила эра широкополосной связи, мгновенный скачок пропускной способности персональной сети стал поворотным моментом от однонаправленной среды к двунаправленной.

Блокчейн.

Хранение данных, как безопасное, так и децентрализованное, является одной из самых важных и сложных тем в децентрализованной системе. Например,

записи транзакций на криптовалютной платформе должны храниться децентрализованно, чтобы никто не мог доминировать в сети. Однако трудно гарантировать, что вся сеть совместно использует только одну правильную ветвь базы данных без полномочий или централизованной стороны [1]. Проблема в том, где доминирует технология децентрализованного реестра. Любая методология, относящаяся к категории технологий децентрализованного реестра, может иметь следующие характеристики. Блокчейн, как одна из технологий, удовлетворяющая всем требованиям, рассматривается как технология децентрализованного реестра. Название происходит от системного механизма хранения данных. Система может периодически собирать транзакции в блок и использовать алгоритм консенсуса для выбора запечатывающего устройства и защиты запечатанных данных [2]. Затем герметик рассылает блок каждому узлу в сети, чтобы обновить их базу данных. Силер может проверить блок, проверив хэш-данные в заголовке. Практика сформировала виртуальную цепочку, соединенную блоками. Именно благодаря этой процедуре блокчейн получает свое название.

Смарт-контракт.

Согласно словарю Merriam-Webster, контракт — это обязательное соглашение между двумя или более лицами или сторонами, особенно с одним из них, имеющим юридическую силу. Следовательно, существуют критерии и соответствующие действия. При исполнении договора результат необратим и признается законом [3]. Для блокчейна смарт-контракт — это небольшая программа, находящаяся в цепочке, которая обеспечивает ту же функциональность, что и традиционные поставщики контрактов. [4]. Когда кто-то внедряет смарт-контракт в цепочку, владелец не может изменить код в цепочке. Все состояния и переменные смарт-контракта хранятся в цепочке, как показано на рис. 1.

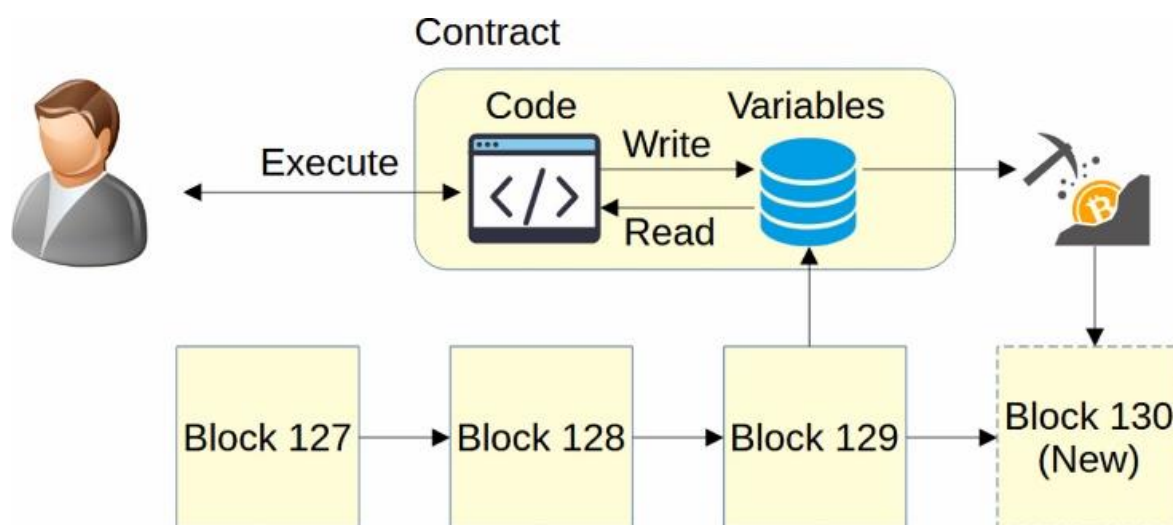


Рис. 1. Взаимодействие между смарт-контрактом и блокчейном.

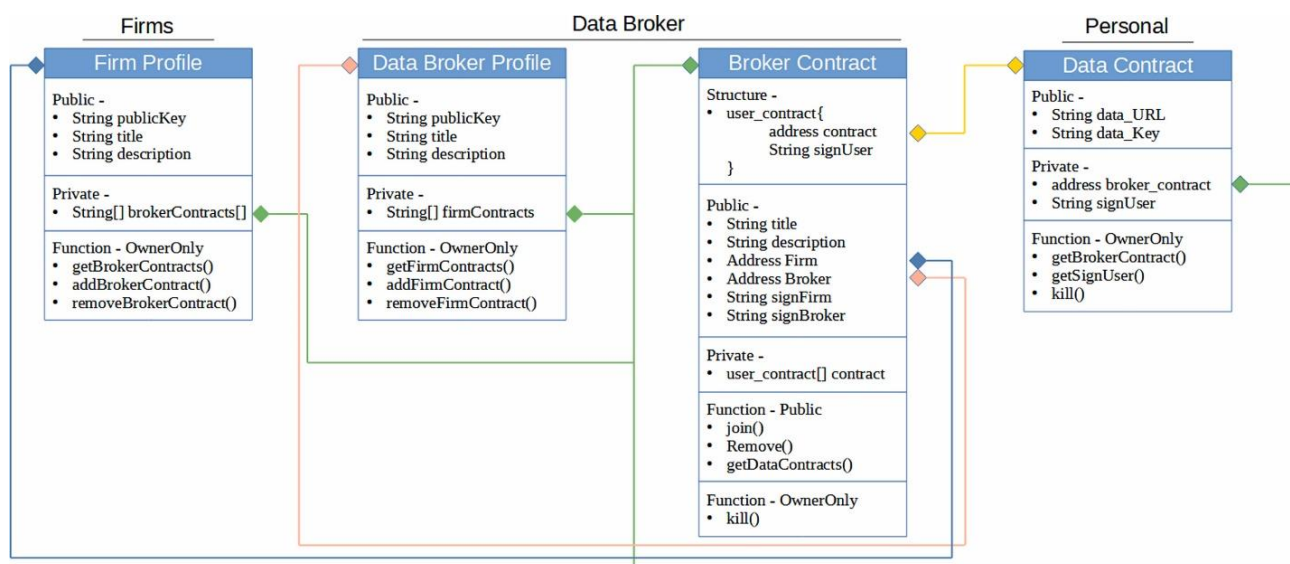


Рис .2. Обзор системы.

Случай атаки.

Брокер данных, который изменяет описание.

В предлагаемой нами системе брокер данных может изменить описание или политику предложения и загрузить их в цепочку. Однако только в том случае, если у брокера есть закрытый ключ фирмы для повторной подписи измененного описания; в противном случае фирма может отклонить контракт, когда фирма получит адрес контракта. Если брокер повторно загружает контракт, несмотря ни на что, пользователь может обнаружить несоответствие обеих подписей (SIGfirm (название + описание) и SIGbroker (название + описание)) и отклонить контракт с брокером. Вредоносный брокерский контракт, который не позволяет пользователям удалять. Брокер может злонамеренно изменить контракт брокера, то есть функция remove() не удаляет адрес контракта данных пользователя из контракта брокера, но это не повлияет на операцию пользователя по отзыву контракта данных [6]. Пользователь может уничтожить контракт данных, несмотря ни на что, и сделать контракт недействительным. С точки зрения брокера адрес контракта — не более чем бесполезно недействительный адрес контракта. Брокер не может извлечь из этого никакой выгоды. Если брокер намеренно сбрасывает цепочку, чтобы достичь этого недействительного контракта, в этом нет никакой выгоды, поскольку данные зашифрованы с помощью открытого ключа фирмы. Фирма, которая сбрасывает блокчейн из-за убитого контракта на данные. Пока пользователь удаляет данные из хранилища вне сети, фирме нечего получить. Даже если пользователь аннулирует контракт данных, фирма все еще может получить и расшифровать URL-адрес данных и одноразовый ключ, но это не принесет ей никакой пользы. Во-первых, если пользователь удаляет данные, значит, ему не к чему добираться [7]. Во-вторых, каждый фрагмент данных шифруется одноразовым ключом; и ключ можно использовать только для расшифровки конкретной записи. Это делает ключи бесполезными для фирмы.

Основываясь на нашем анализе, наша система может помочь защитить конфиденциальность данных пользователей, но в будущем еще предстоит решить некоторые проблемы. Наша система оставляет название и описание в брокерском договоре в виде простого текста. Хотя дизайн может показаться разумным, они могут вызвать интерес со стороны особых интересов, что приведет к нападению на фирму и пользователя. Размещение данных вне сети кажется отличным способом преодолеть возможную угрозу конфиденциальности и узкое место в производительности, которые могут быть вызваны платформой блокчейна [8]. Однако URL-адрес данных, указывающий на помещение клиента или онлайн-хранилище, может создать другую угрозу конфиденциальности. Необходимо изучить и обсудить этот вопрос.

Список используемых источников:

1. Директива 95/46/ЕС о защите физических лиц при обработке персональных данных и о свободном перемещении таких данных(1995).
2. The Times, 27 февраля 2018 г. [Онлайн] <https://www.thetimes.co.uk/article/businessman-sues-google-to-have-his-crime-forgotten-srdr8d0q8>. [По состоянию на 3 ноября 2020 г.]
3. Утц К., Дегелинг М., Фаль С., Шауб Ф., Хольц Т. (Не)информированное согласие: изучение уведомлений о согласии GDPR на местах. В: Конференция АСМ по компьютерной и коммуникационной безопасности. 2019. с. 973–90.
4. Кристенссон П.Определение цифрового следа(2014).TechTerms, 26 мая 2014 г. [Онлайн] Доступно: https://techterms.com/definition/digital_footprint. [По состоянию на 2 ноября 2020 г.]
5. Чан Р.Информатор Cambridge Analytica объясняет, как фирма использовала данные Facebook, чтобы повлиять на выборы(2019).
6. Business Insider, 5 октября 2019 г. [Онлайн] <https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10?r=US&IR=T>. [По состоянию на 2 ноября 2020 г.]
7. Исповедник Н.
8. Cambridge Analytica и Facebook: скандал и последствия на данный момент(2020).
9. The New York Times, 4 апреля 2020 г. [Онлайн] <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>. [По состоянию на 2 ноября 2020 г.]
10. Мэн В., Тишхаузер Э.В., Ван К., Ван Ю., Хан Дж.Когда обнаружение вторжений встречается с технологией блокчейнRev IEEE Access, 6 (1) (2018), стр. 10179–10188.
11. Чиу В.Я., В. Мэн. EdgeТС — схема ЕТС на основе блокчейна RBFT для умных городов. В: Одноранговые сети и приложения; Спрингер [в печати].
12. Молл Р., Годсифф П., Маллиган С., Браун А., Кьюэлл Б. Технология распределенного реестра: приложения и последствия. В: ФИНРА, Vol. 26, № 5, с. 481–9.

Jorayev H.

The Bonch-Bruевич Saint-Peterburg State University of Telecommunications

A secure data sharing and access scheme over blockchain

With the fast growth of networked devices, the shared data volume keeps increasing over time, i.e., the Internet of Things (IoT) devices may generate zettabytes of data in the coming few years. According to the recent version of General Data Protection Regulation (GDPR), users have the right

to fully control their personal data. Many web service providers also provide some options for users to control the data. However, it is still a challenge to investigate how they enforce these actions. There is a need to deploy additional measures to secure the data access. Focused on this challenge, in this work, we design a scheme that uses smart contract and blockchain to provide a secure data sharing and access environment. In our scheme, there are three major parties and each of them has its own key pair for encrypting and signing the data. We also develop four main smart contracts for different parties, and discuss what kinds of data should be immutable and placed on-chain. In the evaluation, we explore the performance of our scheme under different platforms such as Ethereum with EtHash, Ethereum with Clique, and Hyperledger. With the analysis of several potential attacks, our results indicate the viability and effectiveness of our scheme.

Key words: *data encryption, blockchain technology, access control, data security and privacy, smart contract.*

УДК 004.056.53
ГРНТИ 49.33.35

ИССЛЕДОВАНИЕ DoS АТАК НА БЕСПРОВОДНЫЕ СЕТИ НА ОСНОВЕ WPA-2 ENTERPRISE

Д. О. Храмцов, А. Ю. Киструга

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматриваются принципы стандарта IEEE 802.1x и представлены средства защиты от DoS-атак в соответствии с корпоративной матрицей MITRE ATT&CK для корпоративных сетей компаний. Определены методы защиты от представленных атак и исследованы способы их реализации на оборудовании различных производителей, таких как TP-LINK, ASUS, MikroTik.

IEEE 802.1x, Wi-Fi, безопасность беспроводной сети, RADIUS-сервер, DoS-атаки, механизмы защиты

В настоящее время всё чаще применяется технология беспроводного доступа в Интернет. Крупные государственные и частные компании из различных отраслей, образовательные учреждения, имеющие зачастую большой список работников, вместо проводной корпоративной сети используют беспроводную. Самым распространённым способом является передача данных с помощью Wi-Fi сетей, что позволяет работникам подключаться в любой точке зоны действия. Для выполнения контролируемого доступа к сети используется RADIUS сервер, который предназначен для обеспечения централизованной аутентификации, авторизации и учёта пользователей [1]. Однако, существуют проблемы безопасности, связанные с использованием сетей семейства стандартов IEEE 802.11. По данным компании Positive Technologies можно заметить, что в I квартале 2022 года количество атак увеличилось на 14,8% по сравнению с IV кварталом 2021 года. Стоит отметить, что 67% кибератак носили целенаправленный характер. Чаще всего атакам подвергались государственные и медицинские учреждения, промышленные предприятия.

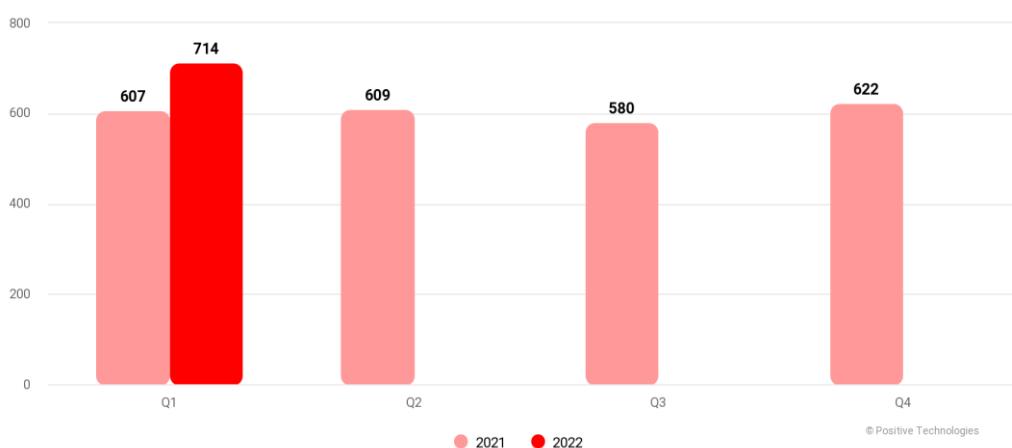


Рис. 1. Диаграмма атак за 2021 и 2022 года согласно исследованиям Positive Technologies

В рамках данной работы рассмотрим наиболее распространенный тип построения корпоративной сети. Для исследуемой информационной системы актуальным является внешний нарушитель, не имеющий доступ в контролируемую зону и к средствам вычислительной техники. Схема организации сети представлена на рис. 2. В ней есть 2 клиента: один из которых подключен через сетевой кабель, а другой по беспроводной сети. Установлена точка доступа на которой включен режим WPA2-Enterprise. Злоумышленник который отправляет фальшивые сообщения по беспроводной сети, установленный Radius сервер на операционной системе на ядре Linux и системный администратор который следит за беспроводным трафиком с помощью анализатора трафика [2].

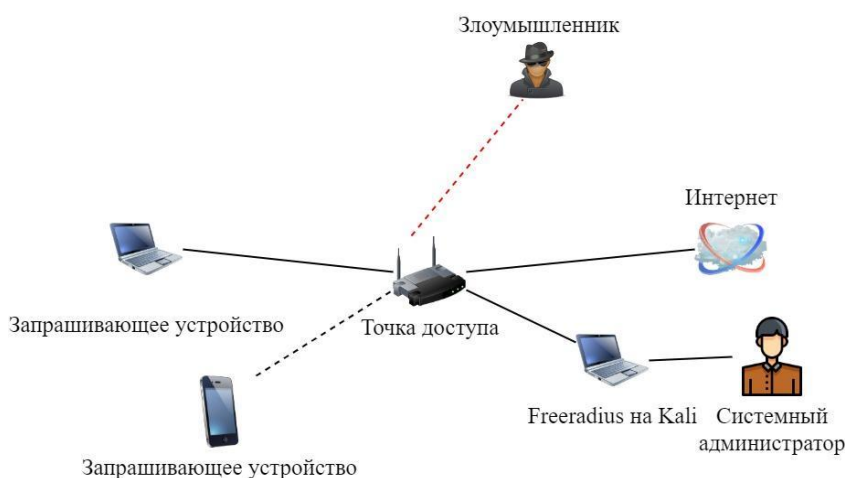


Рис. 2. Исследуемая модель беспроводной корпоративной сети

Корпоративные сети с шифрованием WPA2-Enterprise строятся на аутентификации по протоколу 802.1x через RADIUS-сервер. Протокол 802.1x (EAPOL) определяет методы отправки и приема запроса данных аутентификации и обычно встроен в операционные системы и специальные программные пакеты.

802.1x предполагает три роли в сети:

1. Клиент (supplicant) — клиентское устройство, которому нужен доступ в сеть;
2. Сервер аутентификации (обычно RADIUS);
3. Аутентификатор — роутер/коммутатор, который соединяет множество клиентских устройств с сервером аутентификации и отключает/подключает клиентские устройства.

Для организованной сети была разработана следующая методика для тестирования беспроводной сети:

1. АРМ атакующего (kali linux);
2. АРМ тестирования (kali linux);
3. Анализатор трафика (wireshark);
4. Перехват пакетов с помощью анализатора трафика;
5. Формирование большого количества пакетов и отправка их;
6. Обработка результатов и принятие решения.

На рис. 3 показан принцип работы протокола 802.1x, а также смоделированные DoS атаки: EAPOL-Start, EAPOL-Logoff, EAP-Failure, EAP-Success по MITRE ATT&CK matrix, которые состоят из одной матрицы и техники: TA0043(Reconnaissance)/T1595(Active Scanning)/Pre-compromise.

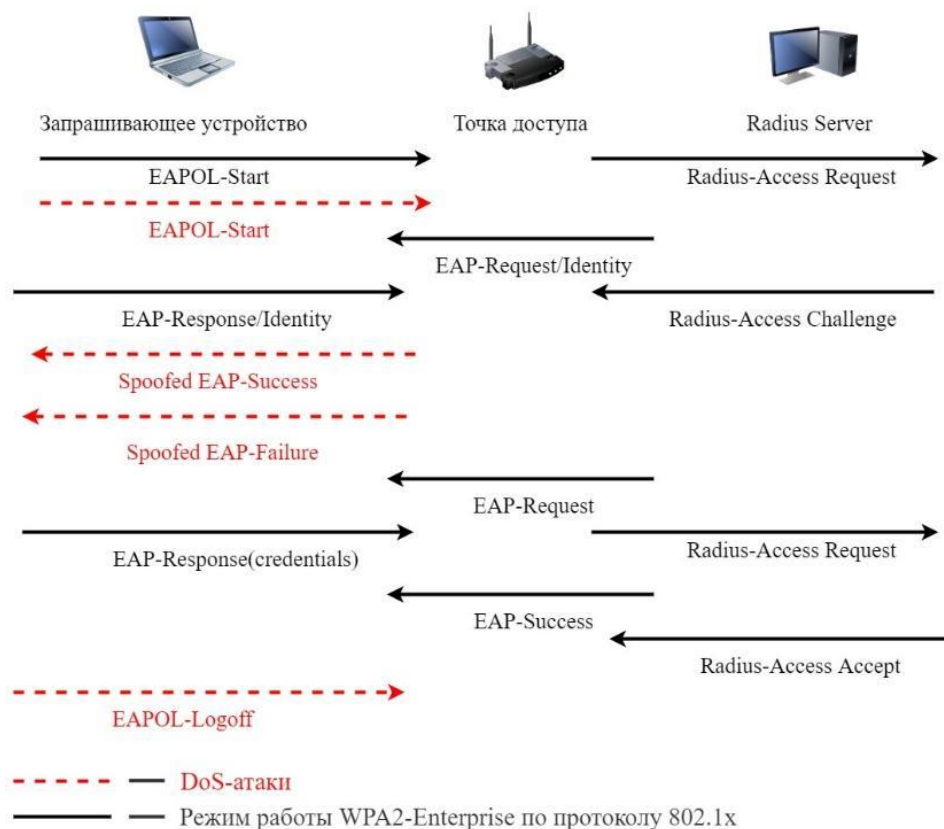


Рис. 3. Схема работы WPA2-Enterprise 802.1x

На трех точках доступа: TP-Link Archer AX50, ASUS WL-520 GU, MikroTik mAP lite RBMAPL-2ND исследовалось, при каком количестве пакетов в секунду запрашивающее устройство не может аутентифицироваться. Результаты представлены в таблице 1.

ТАБЛИЦА 1. Количество пакетов, отправленных в секунду, нужных для успешной DoS атаки

Точка доступа	EAPOL Logoff, кол-во пакетов в секунду	Premature EAP-Success, кол-во пакетов в секунду	Premature EAP-Failure, кол-во пакетов в секунду	EAPOL Start, кол-во пакетов в секунду
ASUS WL-520GU	1	5	10	1
TP-LINK Archer AX50	1	1	5	1
MikroTik mAP lite RBMAPL-2ND	1	5	1	1

Для данных DoS атак существуют следующие механизмы защиты [3]:

1. В настройках маршрутизатора вы можете изменить канал, по которому вещает сеть Wi-Fi. Это может помочь на короткое время, пока злоумышленник не обнаружит изменения и не изменит свои настройки.

2. Используется фильтрация MAC-адресов. Во время фильтрации к сети могут подключаться только устройства, MAC-адреса которых администратор ввел в таблицу доверенных в точке доступа.

3. Рекомендуются выбирать оборудование беспроводной сети, поддерживающее стандарт IEEE 802.11w. Этот стандарт защищает управляющий трафик между клиентом и точкой доступа.

4. Внедрение WIPS [4]. Это система, которая отслеживает окружающий радиоэфир с помощью датчиков. Они анализируют полученную информацию об источниках радиосигнала, их взаимодействиях и ненормальных (необычных) действиях и предотвращают действия, противоречащие настроенной политике предотвращения вторжений.

5. Ограничение радиовидимости беспроводной сети за пределами территории, где эксплуатируется беспроводная сеть.

6. Наличие протоколирования событий безопасности на беспроводном оборудовании, включая отражение ошибки авторизации сообщения и их обработка системой мониторинга и персоналом компании.

7. Скрытие имени SSID, но в настоящее время этот метод малоэффективен.

В этой статье типичная корпоративная среда была смоделирована с использованием беспроводных технологий IEEE 802.1x. Сценарии атак были разработаны с использованием тактики и приемов MITRE ATT&CK. Предложена методология тестирования и определены механизмы защиты от атак. Был представлен обзор атак типа "отказ в обслуживании" в беспроводных сетях. Экспериментально было установлено минимальное количество пакетов в секунду для успешной DoS-атаки. Влияние DoS-атаки на беспроводные сети были проведены для моделей: ASUS WL-520GU, TP-LINK Archer AX50 и MikroTik mAP lite RBMAPL-2ND. Текущие результаты показывают проблематичность существующих атак, поскольку для этого требуется низкая заполняемость канала. Это позволяет злоумышленнику, используя только один адаптер, атаковать несколько точек беспроводного доступа.

Список используемых источников:

1. Ковцур М. М., Поляничева А. В. Исследование механизма авторизации пользователей для доступа к IP-TV сервисам с применением RADIUS-сервера // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VII Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 28 февр. - 01 марта 2018 г.. СПб. : СПбГУТ, 2018. Т. 1. С. 466–471.

2. Александрова Е. С., Ковцур М. М. Разработка модели нарушителя в беспроводных сетях стандарта IEEE 802.11. // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VI Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 01 - 02 марта 2017 г. СПб. : СПбГУТ, 2017. Т. 2. С. 24-28.

3. Александрова Е. С., Иванов Г. Н., Ковцур М. М. Анализ механизмов защиты Wi-Fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы

VII Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 28 февр. - 01 марта 2018 г. СПб. : СПбГУТ, 2018. Т. 1. С. 47–51.

4. Зуев И. П., Карельский П. В., Ковцур М. М., Юркин Д. В. Разработка методики проведения испытания IPS модулей // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы IX Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 26-27 февр. 2020 г. СПб. : СПбГУТ, 2020. Т. 1. С. 492-496.

Khramtsov D., Kistruga A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Investigation of DoS attacks on wireless networks based on WPA2 enterprise

This article discusses the principles of the IEEE 802.1x standard and presents four DoS attacks in accordance with the enterprise matrix MITRE ATT&CK for corporate networks of companies. The methods of protection against the presented attacks are determined and the ways of their implementation on the equipment of various manufacturers, such as TP-LINK, ASUS, MikroTik are investigated.

Key words: IEEE 802.1x, Wi-Fi, wireless network security, RADIUS Server, DoS attacks, protection mechanisms.

УДК 004.3
ГРНТИ 20.53.23

ИЗМЕНЕНИЕ ЗАДЕРЖКИ В ЗАВИСИМОСТИ ОТ КОЛИЧЕСТВА УЗЛОВ В КЛАСТЕРЕ ONOS ПРИ ВКЛЮЧЕНИИ/ОТКЛЮЧЕНИИ КОММУТАТОРА

Я. К. Шабловский, А. М. Гельфанд

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Распространение облачных услуг, виртуализация серверов, а также резкий рост количества мобильных устройств явились одними из основных причин к возникновению новой сетевой архитектуры. Основным отличием SDN от традиционных сетей является централизованное интеллектуальное управление и мониторинг сети, которые обеспечивают проверку, контроль и модификацию потоков, передаваемых данных.

эксперимент, коммутатор, тест, задержка, ONOS

Сетевые события должны обрабатываться с низкой задержкой, чтобы минимизировать время, в течение которого приложения работают в устаревшем представлении топологии. Одним из основных событий топологии, которые важно измерить, считается: добавление/удаление коммутатора. Важно быстро распознать, что такие события произошли, и быстро обновить сетевой график в кластере, чтобы все экземпляры сходились к одному и тому же представлению топологии.

В данном тесте мы подключаем и отключаем коммутаторы и отслеживали время, которое понадобилось системе ONOS, чтобы изменить топологию сети.

Результаты эксперимента «подключения коммутатора» представлены на рис. 1:

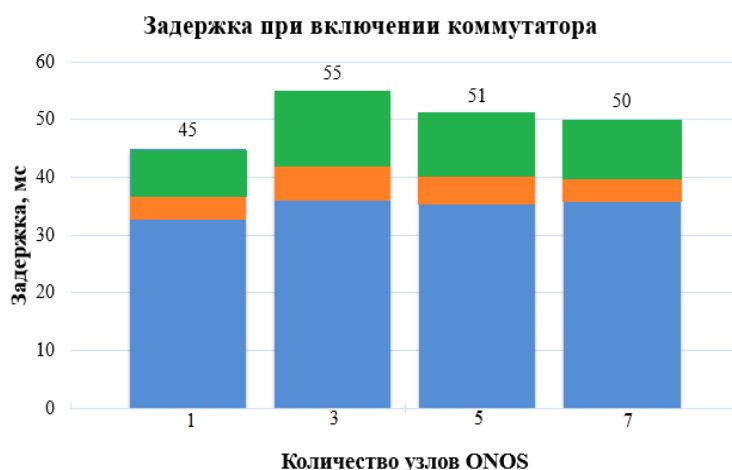


Рис. 1. Результаты теста «включение коммутатора»

Для всех установок с одним или несколькими устройствами задержка колеблется от 45 до 55 мс.

Каждая задержка делится на три измерения:

- время, потраченное с начала подключения устройства до отправки сообщения системе ONOS (выделено голубым цветом);
- время, затрачиваемое на избрание «главного» коммутатора (выделено оранжевым цветом);
- время, потраченное ONOS на генерацию графического события (выделено зеленым цветом).

Изучение результатов показывает, что задержки в основном обусловлены временем, которое требуется коммутатору для отправки сообщения системе ONOS. Это подтверждается постоянной задержкой ~ 35 мс, показанной в виде голубой части столбцов на рис. 2, которая не зависит от количества узлов кластера.

Совокупный вклад ONOS в задержку составляет от 10 до 20 мс. Это время, необходимое системе ONOS, для выбора коммутатора в качестве «главного». Оно немного увеличивается с повышением количества узлов ONOS.

Ожидается дополнительная небольшая координационная нагрузка, поскольку этот шаг требует полного консенсуса между всеми экземплярами кластера.

В остальном никаких дополнительных затрат при увеличении размера кластера нет.

Результаты эксперимента «отключение коммутатора»:

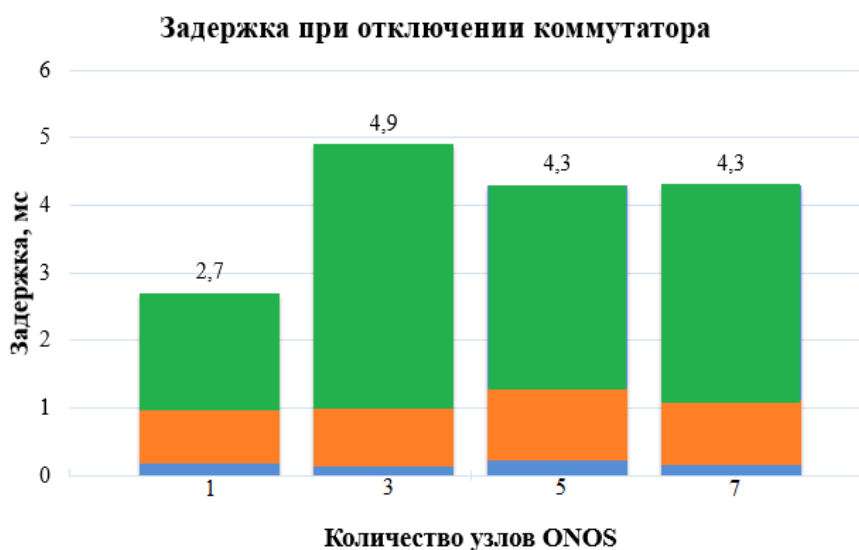


Рис. 2. Результаты теста «отключение коммутатора»

Для всех установок с одним и несколькими экземплярами задержка составляет от 3 до 5 мс.

Каждая задержка делится на три измерения:

- время, потраченное на разрыв сеанса TCP между ONOS и устройством (выделено голубым цветом);
- время, потраченное ONOS на генерацию события устройства (выделено оранжевым цветом);

– время, потраченное ONOS на генерацию графического события (выделено зеленым цветом).

Подобно разнице задержки при подключении и отключении порта, выключение коммутатора происходит значительно быстрее его подключения, потому что не тратится время на согласование. Как только соединение обрывается, ONOS может категорически объявить, что коммутатор недоступен и без задержки удалить его из сетевого графика.

Список используемых источников:

1. Красов А. В., Левин М. В. Возможности управления трафиком в рамках концепции SDN // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы IV Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 03–04 марта 2015 года. СПб. : СПбГУТ,, 2015. С. 350-354.
2. Красов А. В., Гельфанд А. М., Коржик В. И. Построение доверенной вычислительной среды. СПб. : ИП Петрив Р. Б., 2019. 108 с. ISBN 978-5-6043143-2-6.
3. Исаченков П. А., Красов А. В., Левин М. В. Исследование эффективности метода управления потоками трафика на основе информации о нагрузке в программно-определяемой сети с неравными метриками маршрутов // Современная наука и инновации. 2017. № 2(18). С. 32-38.
4. Красов А. В. Волконогов В. Н., Волостных В. А., Гельфанд А. М., Катасонов А.И. Способы коммутации пакетов в сетях cisco // Национальная безопасность России: актуальные аспекты : материалы Всерос. научно-практич. конф., Санкт-Петербург, 30 июля 2018. СПб. : ГНИИ “Нацразвитие”. 2018. С. 31-35.
5. Леснова Е. М. Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Региональная информатика и информационная безопасность : материалы межрегион. конф., Санкт-Петербург, 01-03 нояб. 2017 г. СПб. : СПОЙСУ, 2018. С. 236-240.

Shablovskiy Y., Gelfand A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Changing the delay depending on the number of nodes in the ONOS cluster when switching on/off the switch.

The spread of cloud servers, virtualization, as well as a sharp increase in the number of mobile devices were among the main reasons for a specific network architecture. The main difference between SDN and networks is dedicated intelligent network management and monitoring, which check, control and modify suspicious data flows.

Key words: experiment, switch, test, delay, ONOS.

УДК 004.056.53
ГРНТИ 49.33.35

РАЗРАБОТКА КОМПЛЕКСА ЛАБОРАТОРНЫХ РАБОТ ПО ФУНКЦИОНИРОВАНИЮ WLAN КОНТРОЛЛЕРОВ

М. В. Яссер, М. М. Ковцур

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Беспроводные сети имеют большую популярность в современном мире, зачастую из выбирают за счет их удобства по сравнению с проводными сетями. Главными преимуществами являются доступность и мобильность, также охват такой сети может достигать до нескольких тысяч километров. Одним из главных недостатков выступает уязвимость беспроводных сетей к различным типам атак. Проводная сеть при идеальных условиях и безопасному использованию может быть атакована только из интернета при подключении к нему, беспроводная сеть напротив – открыта всем, кто находится в зоне ее действия, а это не может не привлекать злоумышленников или же людей, которые захотят бесплатно пользоваться данной сетью. Появляется риск утечки конфиденциальной информации либо же документов, именно поэтому важно уделять безопасности беспроводных локальных сетей должное внимание. В работе представлен комплекс лабораторных работ, позволяющий изучить функционирование WLAN контроллера.

беспроводная локальная сеть, защита беспроводной локальной сети, WLAN-контроллер, 802.1х, лабораторная работа

В крупных компаниях достаточно сложно следить за безопасностью и правильной настройкой беспроводной локальной сети, а также всех точек доступа, поэтому есть необходимость использовать WLAN контроллер.

WLAN контроллер (Wireless LAN controller) – устройство применяемое при развертывании сетей семейства IEEE 802.11, позволяющее настраивать сразу несколько точек доступа одновременно, что намного упрощает администрирование локальной беспроводной сети. Большую популярность WLAN контроллеры приобретают на предприятиях, где установлено много точек доступа.

Рассмотрим WLAN контроллер на примере программного контроллера Eltex.

Контроллер выполняет также несколько дополнительных функций, например:

- авторизация пользователей WPA Enterprise, WPA Personal;
- мониторинг точек доступа;
- конфигурирование точек доступа, включая групповые политики;
- отображение текущего состояния всех Wi-Fi клиентов сети;
- сбор сервисной и аварийной информации.

Комплекс лабораторных состоит из двух работ. В первой рассматривается базовая настройка контроллера SOFTWLC для работы с точкой доступа и

авторизации на базе WPA2-PSK, во второй рассматривается организация беспроводной сети на базе IEEE 802.1x авторизация WPA2-Enterprise.

При выполнении первой работы необходимо настроить беспроводную сеть с режимом безопасности WPA2-PSK, осуществить привязку этой сети к точке доступа, как показано на рис. 1, проверить работоспособность организованной WLAN сети. Также осуществляется настройка такого функционала, как изоляция беспроводных клиентов и ограничение скорости сети семейства IEEE 802.11.

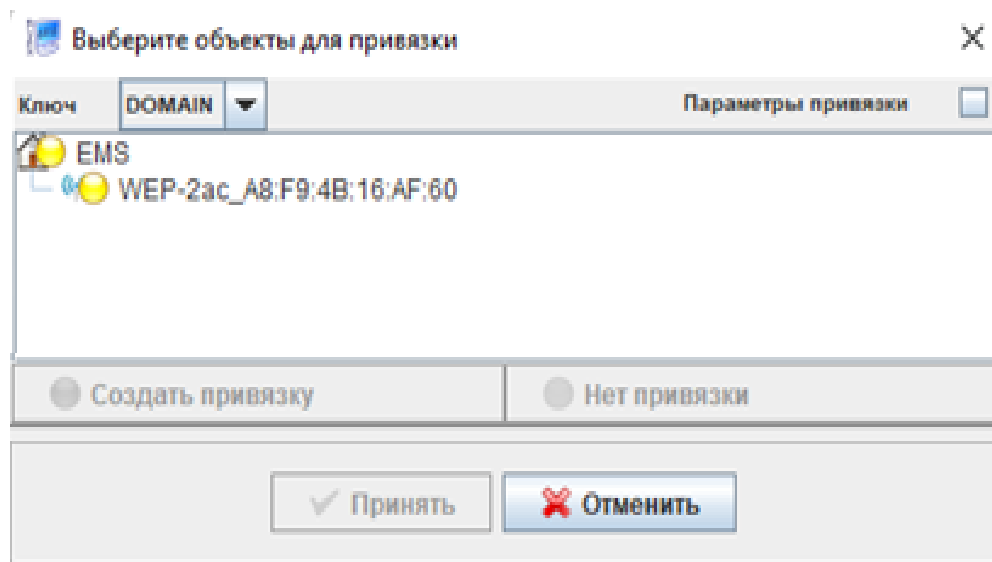


Рис. 1. Точка доступа, отражаемая в «Менеджер SSID»

В рамках второй лабораторной работы выполняется настройка IEEE 802.1x.

WPA2- Enterprise – режим безопасности беспроводной сети, в котором применяется IEEE 802.1x для аутентификации и авторизации пользователей WLAN. В данном режиме каждый пользователем имеет свою учетную запись и выполняет подключение к беспроводной сети с использованием персональных регистрационных данных, таких как имя и пароль. Данный механизм зачастую применяется в корпоративных беспроводных решениях. В данном режиме используются протоколы EAPoL и RADIUS, также потребуется наличие RADIUS-сервера для авторизации пользователей. Аутентификация производится между рабочей станцией и сервером аутентификации. Точка доступа проводит мониторинг пользователей и направляет аутентификационные запросы пользователей на сервер RADIUS в случае RADIUS сервер уже встроен в программный контроллер Eltex. На рис. 2 наглядно изображена схема беспроводной локальной сети организации.

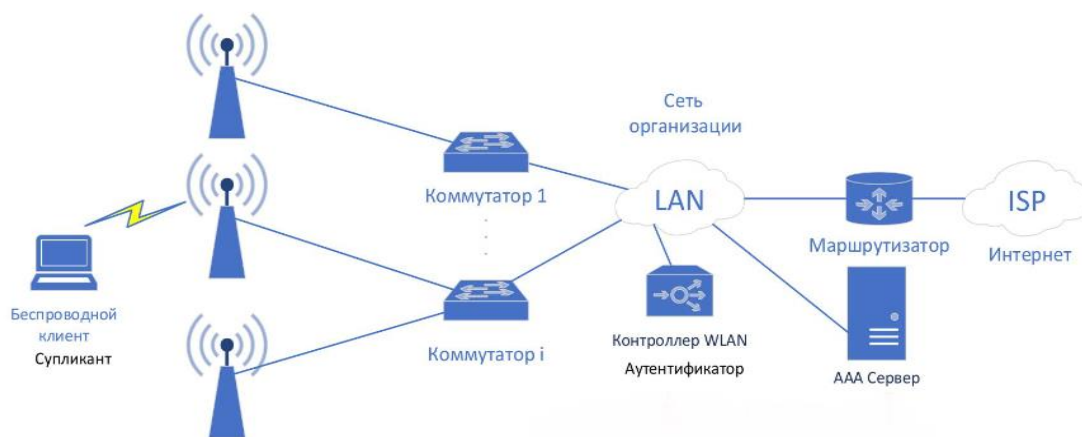


Рис. 2. Схема беспроводной локальной сети организации

Для выполнения второй лабораторной необходимо изменить созданную ранее WLAN и вручную выставить режим безопасности WPA2-Enterprise, а также тип шифрования WPA2-AES (рис. 3)

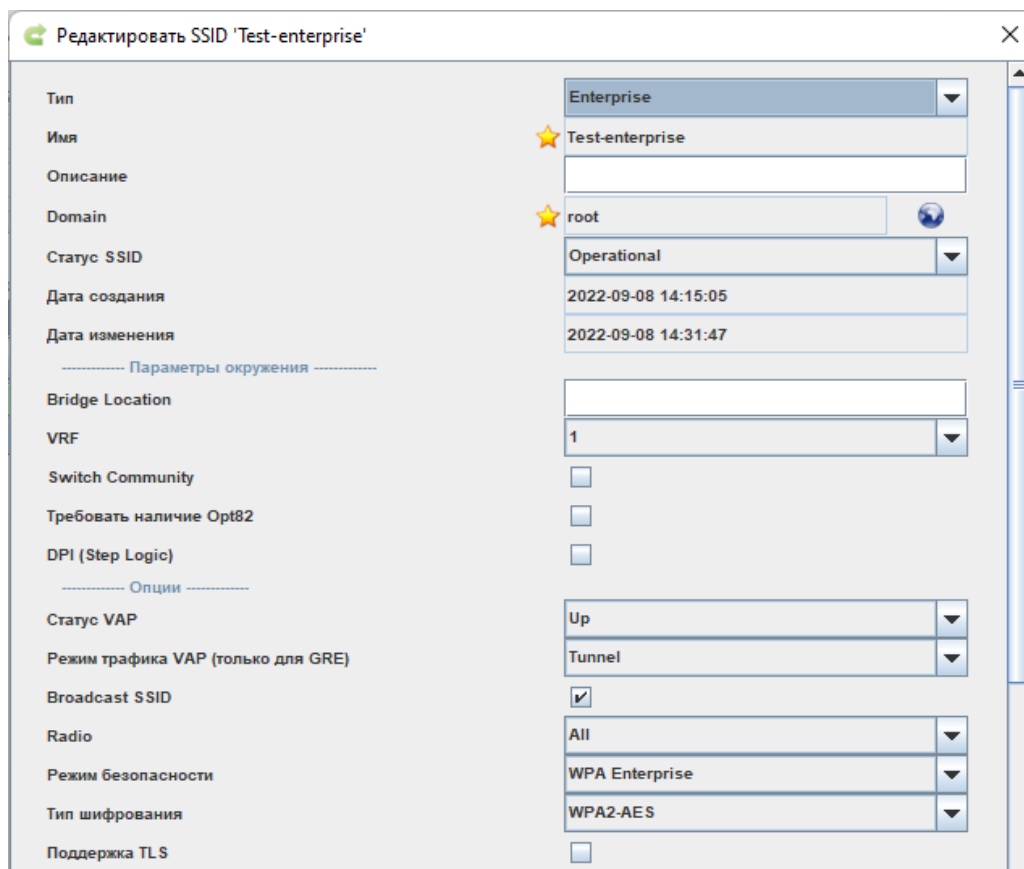


Рис. 3. Основная настройка беспроводной локальной сети на контроллере

Далее необходимо указать настройки RADIUS-сервера, а именно IP-адрес сервера и порт по которому будет происходить подключения, стандартно RADIUS-сервер прослушивает порт 1812 (рис. 4).

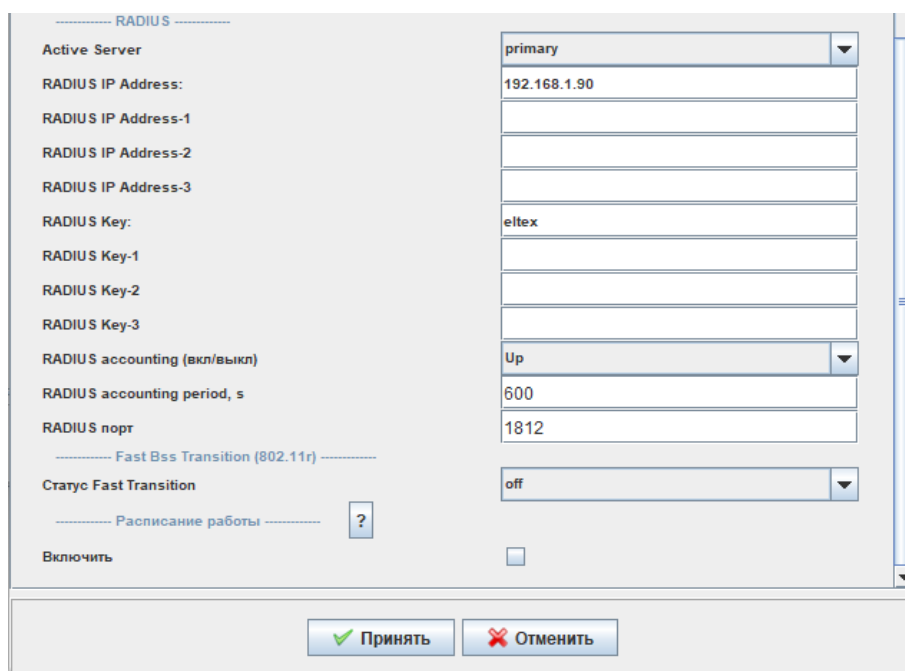
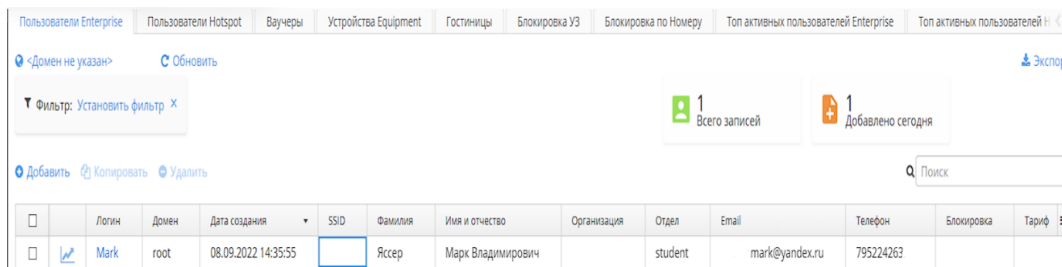


Рис. 4. Основная настройка беспроводной локальной сети на контроллере

Создание пользователя происходит через модуль управления пользователем, для того чтобы создать пользователя нужно указать всю необходимую информацию, а именно номер телефона, ФИО, выдать логин и пароль для успешной авторизации через RADIUS-сервер (рис. 5).



	Логин	Домен	Дата создания	SSID	Фамилия	Имя и отчество	Организация	Отдел	Email	Телефон	Блокировка	Тариф
<input type="checkbox"/>	Mark	root	08.09.2022 14:35:55		Яссер	Марк Владимирович		student	mark@yandex.ru	795224262		

Рис. 5 Пользователи Wi-Fi сети

После последнего пункта осуществляется подключение к беспроводной локальной сети посредством WPA2-Enterprise.

Результатом данной работы является комплекс лабораторных работ по функционированию WLAN контроллеров. Также в ходе данной работы была описана базовая настройка беспроводной локальной сети, а также настройка WPA2-Enterprise авторизации. Работа была проверена экспериментально на виртуальных устройствах и физическом оборудовании.

Список используемых источников:

1. Программный контроллер SOFTWLC [Электронный ресурс] URL - https://eltex-co.ru/catalog/wi-fi_kontroller/softwlc/ (Дата обращения 15.11.22).
2. Ковцур М. М., Юркин Д. В., Герлинг Е. Ю., Ахрамеева К. А. Безопасность беспроводных локальных сетей : [Электронный ресурс] : учебное пособие. СПб. : СПбГУТ, 2021. 71 с. (Дата обращения 11.01.2022).

3. Пошаговая настройка и установка SOWTWLC: [Электронный ресурс]. URL - <https://docs.eltex-co.ru/pages/viewpage.action?pageId=200704612>.

Yasser M., Kovtsur M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development of laboratory works on the functioning of WLAN controllers.

Wireless networks are very popular in our modern world, often chosen due to their convenience compared to wired networks. The main advantages are accessibility and mobility, and the coverage of such a network can reach up to several thousand kilometers. One of the main drawbacks is the vulnerability of wireless networks to various types of attacks. A wired network under ideal conditions and safe use can only be attacked from the Internet when connected to it, a wireless network, on the contrary, is open to everyone who is in its area of operation, and this cannot but attract intruders or people who want to use this network for free. There is a risk of leakage of confidential information or documents that is why it is important to pay due attention to the security of wireless local area networks. The paper presents a set of laboratory work that allows you to study the functioning of the WLAN controller.

Key words: *wireless LAN, wireless LAN protection, WLAN controller, 802.1x.*

Секция 3.2.
Интернет вещей и гетерогенные сети

УДК 004.772
ГРНТИ 49.01.73

АНАЛИЗ ТРАФИКА ОБЛАЧНОГО ГЕЙМИНГА

И. Д. Абитов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрен и проанализирован трафик облачного гейминга. На основе анализа полученных данных сделан вывод об возможности оказании услуг сервиса облачного гейминга на основе современной сети в России.

анализ трафика, облачный гейминг, сеть, Онлайн-игра

В настоящее время на игровом рынке одной из популярных тенденций является возможность удалённой игры через сеть интернет, поэтому всё больше крупных компаний внедряют сервис облачного гейминга, который основан на потоковой передаче видео по сети между двумя устройствами. Этому способствовало расширение пропускной способности сетей, а также спрос на видеоигры в условиях повышения цен на комплектующие для компьютера. При запуске данного вида услуг наблюдались проблемы в виде неудовлетворения качеством обслуживания из-за низкой пропускной способности.

В этой статье проанализированы и сравнены два типа трафика высокодинамичной многопользовательской игры Battlefield 1. Первый тип – это трафик между хостом и игровым сервером напрямую. Второй тип – это трафик облачного гейминга между хостом и сервером от GeForce, через приложение NVIDIA GeForce NOW. Для анализа и захвата трафика использовалась бесплатная программа Wireshark. Трафик фиксировался приблизительно в течение 15 минут.



Рис. 1. Структурная схема измерительного стенда

ТАБЛИЦА 1. Сравнение характеристик захваченного трафика

Характеристика	Нисходящий		Восходящий	
	Игровой трафик	Трафик облачного гейминга	Игровой трафик	Трафик облачного гейминга
Кол-во пакетов	57300	2427995	56973	150687
Интенсивность (Пакеты/с)	60,2	2648	59,9	164,3
Интенсивность (Кбайт/с)	26	3369	14	36
Объём трафика (Мбайт)	24,45	2946,43	12,77	31,73
Ср. размер пакета (Байт)	447	1272	235	221

Как видно по таблице 1, за приблизительно одинаковое время захвата, объём и интенсивность захваченного трафика между хостом и сервером облачного гейминга многократно превышает объём трафика между хостом и игровым сервером. Это связано с тем, что сервер облачного гейминга отправляет потоковое видео, в котором демонстрируется результат обработки команд между игровым сервером и сервером от GeForce, а игровой сервер отправляет файлы, которые состоят из команд и основная их обработка происходит на хосте клиента.

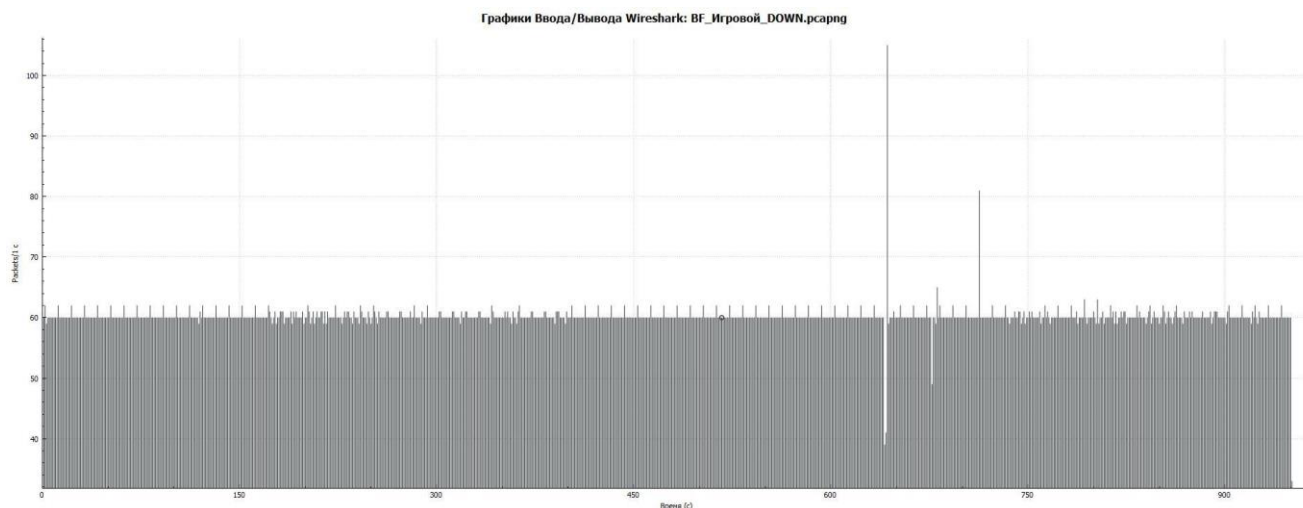


Рис. 2. График ввода/вывода нисходящего игрового трафика

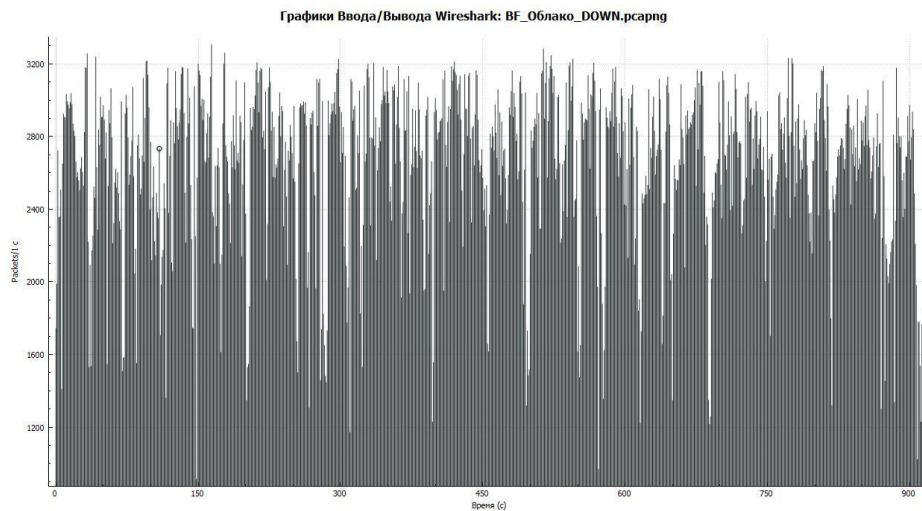


Рис. 3. График ввода/вывода нисходящего трафика облачного гейминга

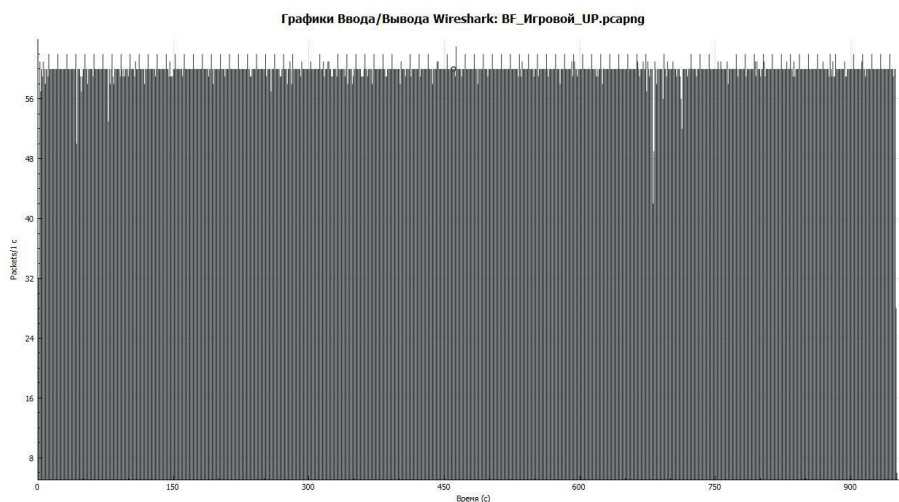


Рис. 4. График ввода/вывода восходящего игрового трафика

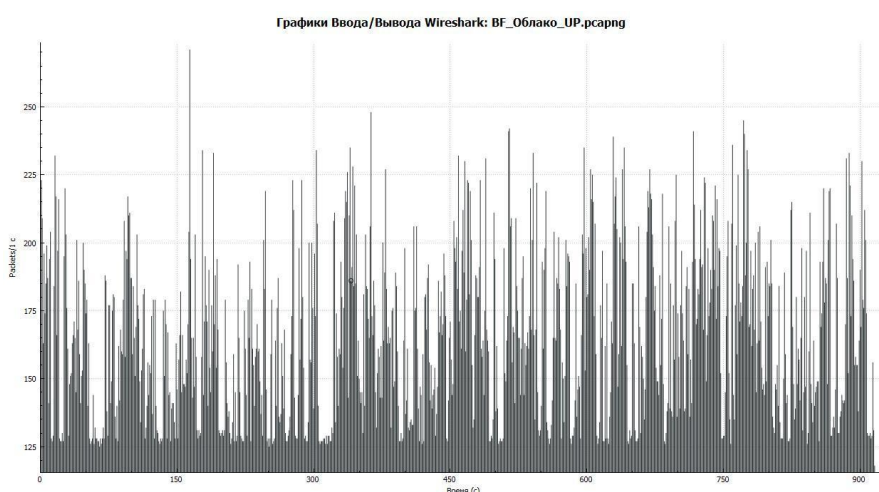


Рис. 5. График ввода/вывода восходящего трафика облачного гейминга

Как видно со второго по пятый рисунок, интенсивность игрового трафика равномерна на протяжении всего времени, что противоположно трафику облачного гейминга. Так как вовремя игры через сервис облачного гейминга

иногда наблюдались незначительные задержки в выполнении команд, то вероятно это было вызвано как раз неравномерной интенсивности данного трафика.

Таким образом, несмотря на значительные различия между игровым трафиком и трафиком облачного гейминга, через сеть интернет в России может обеспечить оказание услуги облачного гейминга, так как по сведениям от SPEEDTEST средняя нисходящая и восходящая скорость фиксированной широкополосной связи соответственно равна 73,26 Мбит/с и 79,71 Мбит/с, что подходит для трафика облачного гейминга, где скорость была равна 26,32 Мбит/с и 0,28 Мбит/с. Однако трафик облачного гейминга требует много ресурсов сети и это может сильно нагрузить сеть при массовом потреблении данной услуги.

Список используемых источников:

1. Сандерс К. Анализ пакетов: практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях. СПб. : ООО «Диалектика», 2019. 448 с.
2. Speedtest: [Электронный ресурс] // speedtest.net. 2006-2022. URL: <https://www.speedtest.net/global-index/russia#mobile> (Дата обращения 31.10.2022)

Abitov I.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Cloud gaming traffic analysis.

The article discusses and analyzes the traffic of cloud gaming. Based on the analysis of the data obtained, a conclusion is made about the possibility of providing cloud gaming services based on a modern network in Russia.

Key words: traffic analysis, cloud gaming, network, Online game.

УДК 004.021
ГРНТИ 49.33.35

АЛЬТЕРНАТИВНЫЕ РЕАЛИЗАЦИИ ($p - 1$) – МЕТОДА ПОЛЛАРДА

Н. С. Баталин, Г. П. Лапцевич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Из описания ($p - 1$) – метода Полларда следует, что для него отсутствует конкретизация в выборе используемых параметров. Это свидетельствует о случайности данного алгоритма. В настоящей работе рассмотрены варианты реализации алгоритма с целью определения оптимальных параметров.

факторизация, RSA, криптография

На сегодняшний день криптосистема RSA [1] является одной из наиболее распространённых. Криптографическая стойкость данной криптосистемы основывается на практической трудности решения задачи факторизации.

Факторизация в криптосистеме RSA является частным случаем задачи факторизации в общем виде и заключается в разложении модуля n на два простых сомножителя p и q :

$$n = p * q.$$

В 1974 году для решения задачи факторизации Поллардом был предложен алгоритм, получивший название ($p - 1$) – метод Полларда [2]. Данный алгоритм предполагает поиск таких значений $a^M - 1 \pmod{n}$, которые удовлетворяют условию:

$$\text{НОД}(a^M - 1, n) \neq 1. \quad (1)$$

Условие (1) может быть выполнено при:

$$a^M - 1 = p * k \pmod{n}$$

или

$$a^M - 1 = q * k \pmod{n},$$

где k – некоторое целое число.

В настоящей работе выбраны следующие подходы к реализации выражения

$$a^M - 1 \pmod{n}. \quad (2)$$

Способ 1: параметр a – константа равная 2; параметр M – задается функцией факториала некоторого числа k , принимающего на каждой итерации значения $k = 2, 3, \dots$. Таким образом, выражение (2) принимает вид:

$$2^{k!} - 1 \pmod{n}.$$

Способ 2: на первой итерации $k = 1$, параметр $a = 2$, а на каждой последующей принимает значение $a_{k+1} = a_k^{k+1} \pmod{n}$; параметр M принимается равным номеру итерации $k+1$. Таким образом, выражение (2) принимает вид:

$$a_k^{k+1} - 1 \pmod{n}.$$

Способ 3: параметр a – константа равная 2; параметр M – произведение первых j простых чисел p в степени зафиксированной степени $r = 2$, где количество простых чисел в произведении увеличивается на одно на каждой итерации k , при $p_1 = 2$. Таким образом, выражение (2) принимает вид:

$$2^{\prod_{j=1}^{j=k} p_j^2} - 1 \pmod{n}.$$

Для осуществления измерений был разработан аппаратно программный комплекс, включающий в себя:

- Физический процессор: AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx 2.10 GHz;
- Операционная система: Windows 10;
- Среда разработки: Visual Studio 2019;
- Язык программирования высокого уровня: C# v7.3;
- Целевая платформа: .Net Framework 4.72;
- Тип проекта: Windows Forms.

Обработка результатов измерений аппаратно-программного комплекса, а также построение графиков реализовано средствами Microsoft Excel.

Быстродействие алгоритма оценивалось количеством итераций. Для каждой длины модуля было проведено 10000 измерений для каждого способа реализации алгоритма, а итоговый результат вычислялся как среднее арифметическое результатов всех замеров итераций работы. Также, для каждого итогового результата посчитано среднеквадратическое отклонение.

В таблице с результатами измерений введены следующие условные обозначения:

- i – итоговое количество итераций;
- σ – среднеквадратическое отклонение;
- k – количество неудачных измерений;
- $нд$ – нет данных – измерения для данной величины не проводились.

В таблице 1 приведены результаты измерений для $(p - 1)$ – метода Полларда.

ТАБЛИЦА 1. Результаты измерений для $(p - 1)$ – метода Полларда

Длина модуля n , бит	Варианты реализации								
	Способ 1			Способ 2			Способ 3		
	i	σ	k	i	σ	k	i	σ	k
20	39	41	-	37	50	-	19	23	79
22	53	85	-	51	81	-	28	42	84
24	98	179	-	88	152	-	36	61	107
26	157	287	-	152	271	-	67	107	120
28	276	625	-	279	586	-	96	198	148
30	477	1017	66	426	1003	-	128	359	154
32	626	1296	131	855	1917	-	174	390	240
34	748	1339	344	1265	3520	-	243	496	449
36	<i>nd</i>	<i>nd</i>	<i>nd</i>	3436	9512	-	302	634	872
38	<i>nd</i>	<i>nd</i>	<i>nd</i>	5413	15471	-	412	812	1136
40	<i>nd</i>	<i>nd</i>	<i>nd</i>	10624	33594	-	576	1204	1324
$\sum k_i$	<i>nd</i>			-			4713		

При проведении измерений способом 1, при длине модуля n равной 36 бит, измерения были прекращены в связи с недостатком ресурсов аппаратно-программного комплекса. По результатам измерений заметно, что при увеличении длины модуля, количество итераций в способе 3 растёт значительно медленнее (рис. 1). Однако при использовании данного способа были зафиксированы неуспешные измерения уже при длине модуля равной 20 бит.

Несмотря на то, что общее число неуспешных тестов (рис. 1) для способа 3 значительно выше, для остальных способов данный параметр может расти быстрее на больших длинах модуля. Данное замечание требует дополнительных исследований.

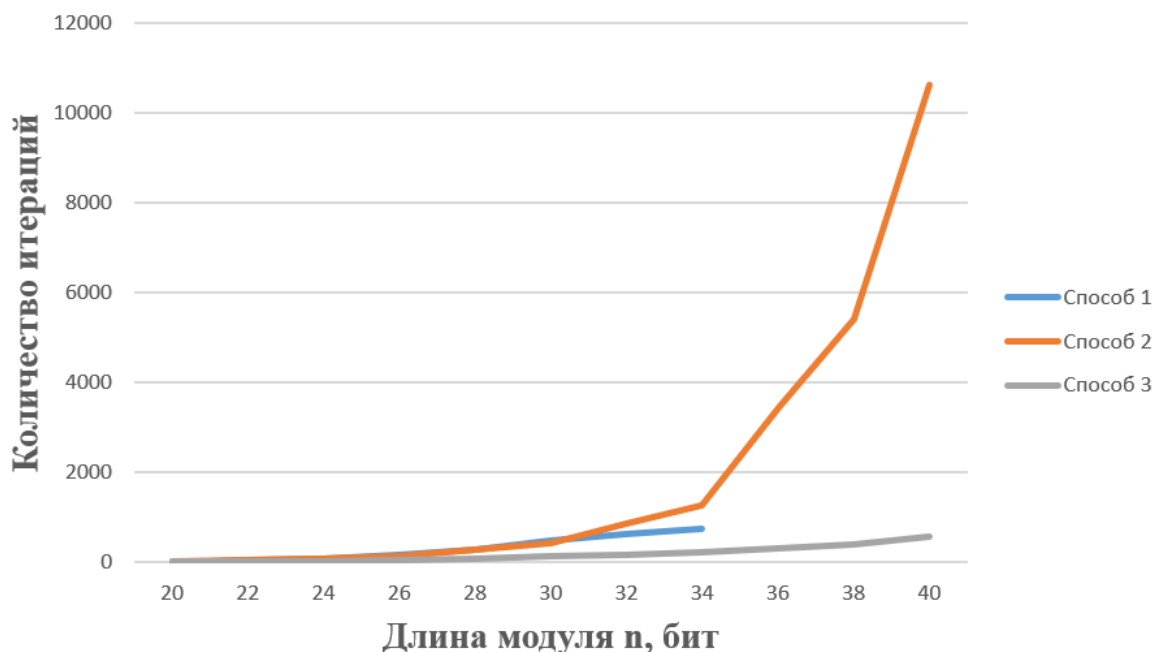


Рис. 1. Зависимость количества итераций от длины модуля n

Реализация $(p - 1)$ – метода Полларда с применением параметров, описанных в способе 3, является наиболее эффективной, поскольку, несмотря на несходимость, присущую данной реализации, обладает гораздо лучшим быстродействием относительно других способов. Для способа 3 общий процент неуспешных измерений составил 4.2 %.

Список используемых источников:

1. Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems // Commun. ACM — [New York]: Association for Computing Machinery, 1978. — Vol. 21, Iss. 2. — P. 120—126. — ISSN 0001-0782; 1557-7317 — doi:10.1145/359340.359342.
2. Pollard J. M. Theorems on factorization and primality testing // Mathematical Proceedings of the Cambridge Philosophical Society / B. J. Green — Cambridge University Press, 1974. — Vol. 76, Iss. 3. — P. 521—528. — 8 p. — ISSN 0305-0041; 1469-8064 — doi:10.1017/S0305004100049252.

Batalin N., Lapceovich G.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Pollard's $(p - 1)$ algorithm alternative implementations.

The article explores variations of the Pollard's $(p - 1)$ algorithm implementation for RSA modulus factorization in order to determine the optimal parameters. Optimal parameters evaluated by algorithm's speed and it's convergence. A hardware-software complex in a high-level language was developed for research. The comparison results and the conclusions are presented.

Key words: *factorization, RSA, cryptography.*

УДК 004.78
ГРНТИ 28.21.19

ПЕРСПЕКТИВЫ РАЗВИТИЯ КВАНТОВОЙ КРИПТОГРАФИИ В ИНТЕРНЕТЕ ВЕЩЕЙ НА ПРИМЕРЕ МЕТОДА КВАНТОВЫХ БЛУЖДАНИЙ

А. И. Выборнова, А. А. Григорьев, А. С. Толкачев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Разработка полноценного квантового компьютера значительно изменит всю вычислительную технику и многие сферы нашей жизнедеятельности, включая экономику, медицину, производство и быт. Классические методы шифрования информации станут бесполезны. Квантовая криптография может помочь защитить наши данные не только в очевидных сферах, но и в более узких, таких как Интернет вещей.

квантовая криптография, квантовые блуждания, интернет вещей

Введение

Квантового шифрование[1] - это первая в истории человечества система распределения ключей, для которой есть строгое математическое доказательство того, что она не взламывается — даже со всеми неограниченными вычислительными мощностями и технологиями, которые не запрещены законом физики. Есть передатчик и приемник, первый берет случайные числа, которые создает при помощи квантового генератора, и кодирует каждый бит информации, каждый бит ключа в состоянии одиночного фотона. Второй же в свою очередь измеряет эти состояния. Отличие одиночного фотона, от конверта с ключом состоит в том, что физика не запрещает вскрыть конверт, прочитать письмо и закрыть обратно. Но если перехватчик попытается посчитать состояние одиночного фотона, это неизбежно его изменит [2].

С учетом потерь фотонов их нужно принимать и передавать дальше каждые 100 километров, то есть создавать так называемый доверенный узел. Одной из самых сложных задач в квантовых коммуникациях является квантовый повторитель. Он совмещает в себе две технологии. Одна из них — это обмен запутанностью, или квантовая телепортация, вторая — квантовая память. Если научиться телепортировать квантовые состояния, сохраняя их, можно будет передавать квантовые ключи на очень большие расстояния. Сейчас предельное расстояние одного пролета квантовой криптографии в реальных условиях составляет 100–130 километров[3].

Квантовая криптография в интернете вещей

Многие устройства интернета вещей — сенсоры — могут быть как классическими, так и квантовыми. Скажем, у нас есть набор классических сенсоров, устройств интернета вещей, шлюзов контроля, которые обладают конфиденциальной информацией. Чтобы их соединить между собой, нужен протокол криптографической защиты — опять же квантовые коммуникации. В данном направлении пока существуют только прототипы, которые защищают отдельные элементы или устройства — говорить о промышленных масштабах

еще рано. Сперва миру необходимо понять ценность направления, выбрать устройство интернета вещей, которое нуждается в защите и эффективной реализации квантовой коммуникации. Кроме того, нужно преодолеть ряд технических барьеров.

На сегодняшний день не совсем ясно, что именно в интернете вещей нужно защищать на таком высоком уровне. Однако по мере распространения технологии интернета вещей будет расти и ценность информации, и ценность ее взлома. В теории взлом может быть особенно опасен на полностью автоматизированном производстве. Так, если сенсоры будут передавать в центр принятия решения некорректную информацию, решения будут приниматься неправильно, и экономический ущерб от такой атаки может быть достаточно ощутимым.[4]

Метод квантовых блужданий

Суть метода заключается в “случайных” неконтролируемых перемещениях, в которых объект периодически совершает шаги в произвольном направлении. Интересной особенностью тут является то, что в среднем объект удаляется от стартового положения на некоторое расстояние, причем это расстояние растет как квадратный корень из числа шагов. Данная модель[5] имеет огромное количество применений в математике и других сферах жизни. По этому же принципу существуют квантовые блуждания с одним исключением. Под перемещением подразумевается вероятность оказаться в тех или иных положениях для частицы в кольце состоящем из N вершин. Кольцо передвижения частицы построено на рис. 1.

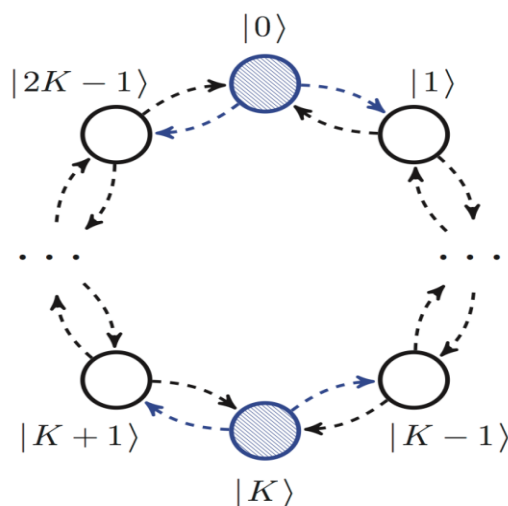


Рис. 1. Кольцо возможных положений частицы.

Перемещение в случайную точку происходит с помощью оператора так называемой “монетки”, показывающей где в какую сторону и насколько передвинется частица. Расчеты вероятностей могут происходить как в одномерном так и двумерном пространстве, что показано на рис. 2 и рисунке 3.

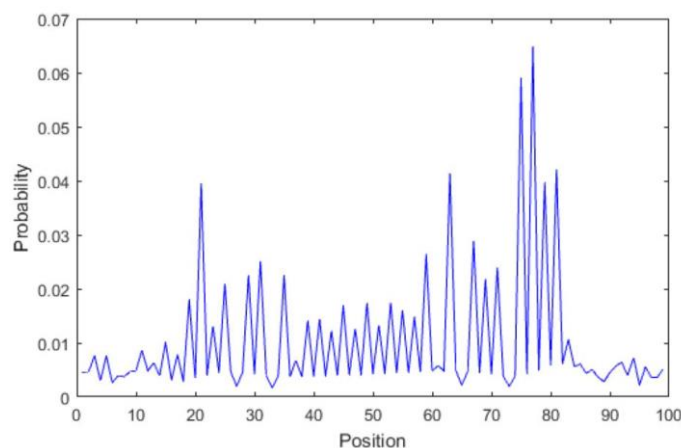


Рис. 2. График вероятностей в одномерном пространстве

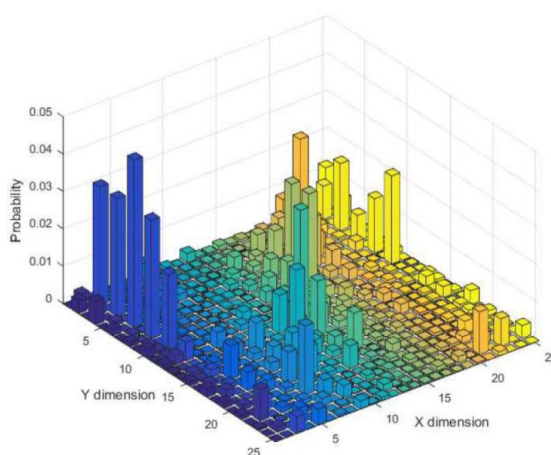


Рис. 3. График вероятностей в двумерном пространстве

Фундаментальным элементом блочных шифров является блок подстановок. Этот блок осуществляет нелинейное преобразование одной группы битов в другую. Конструирование S-блока из V элементов происходит по следующему алгоритму:

1. Запускаем квантовое блуждание, в результате чего получаем вектор вероятностей.
2. Изменяем размер вектора в соответствии с V .
3. Упорядочиваем по возрастанию.
4. В качестве последовательности для S-блока выбираем последовательность индексов элементов вектора из пункта 3 в итоговом векторе.

После выполнения алгоритма получаем S-блок для подстановки.

Преимуществом данного метода являются физические свойства квантовых частиц, которые оказываются в суперпозиции на каждом узле, что кардинально меняет вероятности нахождения в тех или иных положениях. Это свойство сильно укрепляет шифрование и делает минимальной вероятность кражи данных квантовым компьютером.

Квантовые блуждания в интернете вещей

[6] Вопрос безопасности шифрования в интернете вещей с каждым годом становится все более важным, так как практически все имеющиеся методы

сейчас будут с легкостью взломаны квантовым компьютером, поэтому требуются новые варианты защиты данных. Одним из таких является алгоритм шифрования файлов методом квантовых блужданий. Это могут быть файлы любого типа: изображение, аудио, видео, текст и т.д., так как алгоритм работает с ними как с битовыми наборами. Для шифрования битового набора ВF выполняются следующие действия:

1. Вычисляем матрицу вероятностей размера $N \times N$.
2. Переводим матрицу в вектор Z размером L (длина битового набора/8).
3. Переводим полученный вектор в битовый вектор K .
4. Выполняем операцию побитовое хог (исключающее или) между битовым набором и вектором K .
5. Конструируем S-блок размером 256.
6. Применяем блок к каждому элементу последовательности и получаем закодированный файл.

Весь алгоритм отражен на рис. 4.

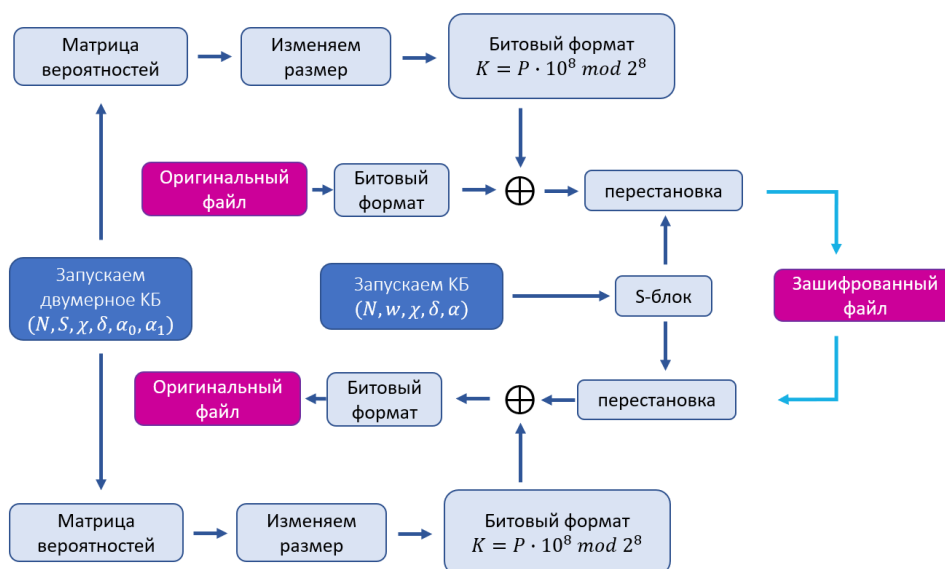


Рис. 4. Схема шифрования файла.

Расшифрование происходит путем выполнения данных действий в обратном порядке.

Заключение

Сейчас квантовая криптография в Интернете вещей используется лишь как подстраховка на будущее от возможных угроз, но даже в такой момент определенные методы выделяются по различным параметрам. Алгоритмы квантового блуждания являются эффективными и с точки зрения других криптографических метрик. Также данный метод позволяет узнать была ли попытка кражи по количеству ошибок в подстановках. Данный метод, как и в целом квантовая криптография, будет успешно развиваться в сфере Интернета

вещей в течении 8-10 лет.

Список используемых источников:

1. Технический комитет 194 «Кибер-физические системы» и Технический комитет 26 «Криптографическая защита информации» 2022. - [Электронный ресурс]. URL : <http://tc194.ru/> (дата обращения: 01.11.2022).
2. В.В. Яценко Введение в криптографию 2000.
3. Shor P.W., Preskill J. Simple proof of security of the BB84 quantum key distribution protocol // Phys. Rev. Lett. 2000. Vol. 85, 441.
4. Постнаука. 2022 - [Электронный ресурс]. URL : <https://postнаука.ru/longreads/156066> (дата обращения 9.11.2022).
5. Хабр. «Понимание квантовых вычислений через случайное блуждание людей» - [Электронный ресурс]. URL: <https://habr.com/ru/company/macloud/blog/552982/>.
6. Хабр. «Шифрование на основе квантовых блужданий для Интернета Вещей» 2022 –[Электронный ресурс] URL : <https://habr.com/ru/post/531774/>.

Vybornova A., Grigoriev A., Tolkachev A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Prospects for the development of quantum cryptography in the internet of things on the example of the method of quantum walks.

The development of a full-fledged quantum computer will significantly change all computing technology and many areas of our life, including the economy, medicine, production and eve-ryday life. Classical methods of encrypting information will become useless. Quantum cryp-tography can help protect our data not only in the obvious areas, but also in narrower areas such as the Internet of Things.

Key words: quantum cryptography, quantum walks, Internet of Things.

УДК 004.732
ГРНТИ 49.43.29

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ OFDMA В WI-FI 6

Я. А. Герасимова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С быстрым ростом числа устройств, подключенных к Интернету, беспроводные локальные сети (WLAN) стали важными из-за их разумной стоимости и подходящих характеристик. Соответственно, приложения WLAN стали разнообразными, и существует спрос на связь с ограниченной задержкой (например, беспроводное дистанционное управление) в WLAN. Для улучшения использования спектра и уменьшения задержки передачи в IEEE 802.11ax был введен множественный доступ с ортогональным частотным разделением каналов (OFDMA), при котором точка доступа (AP) может передавать кадры нескольким станциям (STA) одновременно. OFDMA используется в системах сотовых сетей и обеспечивает эффективное использование спектра при удовлетворении требований к задержке за счет соответствующего распределения ресурсов.

802.11ax, 802.11ac, OFDMA, AP, MU-MIMO, STA

Благодаря высокой скорости передачи данных, простоте установки и бесплатному доступу в Интернет, число пользователей и устройств Wi-Fi постоянно растет в течение последних нескольких лет. Результаты исследований показывают, что в РФ общее число беспроводных БС, включая домашние роутеры, вырастет (с 2018 года) в 6 раз и составит 30,8 млн. к 2023 году. В мире к 2023 году будет 5,3 млрд. пользователей Интернета (66% населения Земли). В России число пользователей глобальной сети через три года составит 113,3 млн человек (78% от общего числа граждан). Повышению эффективности передачи в восходящем направлении в Wi-Fi уделяется больше внимания в связи с разработкой разнообразных приложений, таких как одноранговые вычисления, потоковые сервисы, системы Интернета Вещей и облачные приложения. Учитывая эту тенденцию, легко представить, что сети Wi-Fi станут более плотными и будут страдать от серьезных проблем с перегрузкой. Это означает, что могут часто возникать коллизии кадров, пользователям придется очень долго ждать приема и передачи данных. Многопользовательская (Multi-User, MU) передача привлекает большое внимание как ключевая технология для решения этих проблем в системах Wi-Fi. За счет одновременной связи нескольких беспроводных узлов друг с другом не только увеличивается пропускная способность системы, но и уменьшается перегрузка сети. Для реализации многопользовательской передачи в Wi-Fi использовались две основные схемы связи: MU с несколькими входами и несколькими выходами (MU-MIMO) и множественный доступ с ортогональным частотным разделением каналов (OFDMA). IEEE 802.11ac— это первый стандарт Wi-Fi, использующий функциональность MU-MIMO, позволяющий выполнить одновременную передачу различных потоков данных для нескольких пользователей, что доступно только в нисходящем направлении. Стандарт IEEE 802.11ax поддерживает технологию OFDMA, которая выделяет непересекающиеся

подканалы нескольким пользователям, чтобы они могли одновременно передавать данные как в нисходящем, так и в восходящем направлениях.

Стандарт IEEE 802.11ax вносит значительные улучшения по сравнению с стандартом 802.11ac. В новом стандарте используется технология OFDMA, которая является одним из ключевых улучшений и представляет собой расширение технологии цифровой модуляции OFDM. Основная задача OFDMA – эффективное использование доступного частотного диапазона. Основным механизмом OFDMA заключается в разделении передачи на несколько подканалов, которые называются единицами ресурсов (RUs). В IEEE 802.11ax, который является первым стандартом Wi-Fi, использующим OFDMA, каналы с шириной 20, 40, 80 и 160 МГц можно разделить на 9, 18, 37 и 74 RUs соответственно. Разделение полосы пропускания канала позволяет нескольким пользователям получить доступ к каналу одновременно. 802.11ax использует гораздо больше поднесущих, чем его предшественник 802.11ac, примерно на 192 поднесущих в радиочастотном канале 20 МГц. OFDMA получает поднесущие OFDM через радиочастотный канал и распределяет группы для передач среди различных устройств. В рамках нисходящего канала OFDMA точка доступа может передавать пакеты различным клиентам, используя отдельные группы поднесущих. OFDMA может снизить частоту коллизий на этапах запроса на передачу. Одновременная передача кадров уменьшает чрезмерные накладные расходы на конкуренцию на уровне управления доступом к среде (MAC) и сводит к минимуму накладные расходы на физическую преамбулу (PHY). Появление OFDMA значительно изменило работу Wi-Fi, даже передачи по восходящему каналу теперь контролируются точкой доступа, а не самими клиентскими устройствами. Введение триггерного кадра (TF) является одной из новых функций 802.11ax. Рассылая TF, точка доступа может вызывать и синхронизировать пользователя восходящей линии связи. TF передает несколько форм информации, которые необходимы для передачи OFDMA, например, какие пользователи должны отправлять данные, какие RU должны использовать пользователи, продолжительность соответствующей передачи OFDMA и даже уровень мощности передачи каждого пользователя.

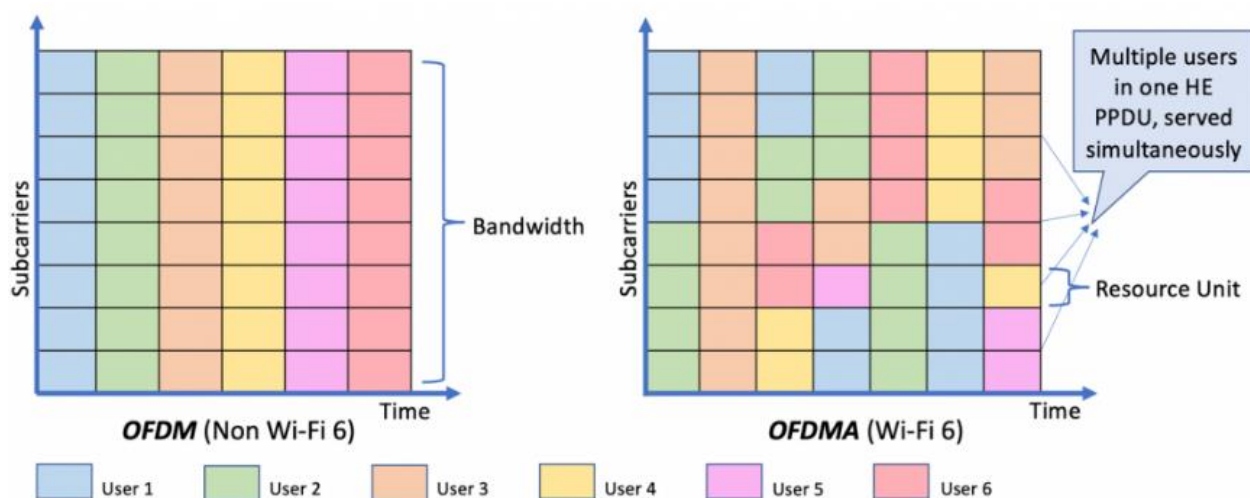


Рис. 1 Один пользователь, использующий канал с использованием OFDM (слева) и мультиплексирование различных пользователей в одном канале с использованием OFDMA (справа)

На рис. 1 в правой части показано, как OFDMA разделил канал и выделил поднесущие разным клиентам для одновременной передачи. OFDMA выделяет неиспользуемый канал другому клиенту. AP может выделить весь канал или только несколько поднесущих в зависимости от потребности. Таким образом, эффективно используется пропускная способность, и поэтому OFDMA лучше работает в среде с высокой плотностью.

В случае передачи DL OFDMA общее поле HE-SIG-B содержит подполя RU, в которых содержатся поля содержимого для каждого пользователя, указывающие RU, назначенные STA, и параметры передачи, которые должны использоваться STA.

802.11ax вводит четыре новых формата PPDU (HE SU, HE MU, HE SU EXT, HE TRIG) и добавляет новые требования к PPDU на основе триггера HE (HE TRIG). Эти новые требования необходимы, потому что восходящая линия OFDMA и многопользовательский MIMO зависят от точности передачи и синхронизации участвующих станций. В восходящей линии связи OFDMA несколько станций (STA) одновременно передают PPDU на основе триггера в точку доступа (AP). Передаче PPDU на основе триггера HE (в восходящей линии связи) предшествует кадр триггера, отправляемый точкой доступа (в нисходящей линии связи). Этот триггерный кадр отправляется всем станциям для координации передачи по восходящей линии связи. Кадр триггера включает в себя такую информацию, как длина полезной нагрузки, полоса пропускания, выделение RU, схема модуляции и т. д. Участвующие STA должны начать передачу сигнала восходящей линии связи через заданный интервал времени SIFS (короткий межкадровый интервал) после окончания кадра триггера. Поскольку в передаче PPDU на основе триггера HE участвуют несколько STA, требуется синхронизация времени передачи, частоты, тактовой частоты дискретизации и мощности участвующими STA для уменьшения помех. Предварительная коррекция мощности необходима для минимизации помех между различными передающими STA.

Кроме того, 802.11ax использует несколько дополнительных управляющих кадров, позволяющих точке доступа распределять ресурсы OFDMA пользователям надлежащим образом, например, опрос отчета о состоянии буфера (BSRP) и опрос отчета о запросе пропускной способности (BQRP). Используя их, точка доступа может отслеживать состояние буфера и качество сигнала пользователей OFDMA. В отличие от технологий MIMO, OFDMA сама по себе не обеспечивает увеличения пропускной способности, вместо этого скорость передачи данных каждого пользователя может уменьшиться, когда полоса пропускания канала используется совместно с другими, что приводит к увеличению времени передачи. Тем не менее, это значительно снижает конкуренцию и накладные расходы преамбулы, и эта экономия особенно эффективна и необходима, где серьезные конфликты каналов возникают из-за большого количества пользователей. Чтобы обеспечить более высокий выигрыш OFDMA, следует использовать соответствующее распределение ресурсов и планирование.

Список используемых источников:

1. WiFi moves to OFDMA [Электронный ресурс]. URL: <https://alethea.in/wifi-ofdma> (дата обращения 18.10.2022).
2. “The Wi-Fi market and the genesis of 802.11ax,” Aruba Netw., Santa Clara, CA, USA, White Paper 053018, 2018. [Электронный ресурс]. URL: https://www.arubanetworks.com/assets/wp/WP_802.11AX.pdf (дата обращения 24.10.2022).
3. IEEE Draft Standard for Information Technology – Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks – Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment Enhancements for High Efficiency WLAN, Standards 802.11ax 2017. [Электронный ресурс]. URL: https://standards.ieee.org/project/802_11ax.html (дата обращения 20.10.2022).
4. Статья: Cisco: число точек доступа Wi-Fi в мире к 2023 году составит 628 млн. [Электронный ресурс]. URL: Cisco: число точек доступа Wi-Fi в мире к 2023 году составит 628 млн (rspectr.com) (дата обращения 01.11.2022).
5. HE MU Transmission. [Электронный ресурс]. URL: HE MU Transmission - MATLAB & Simulink (turborpages.org) (дата обращения 03.11.2022).

Gerasimova Y.

The Bonch-Bruевич Saint- Petersburg State University of Telecommunications

Using ofdma technology in Wi-Fi 6.

With the rapid growth in the number of devices connected to the Internet, wireless local area networks (WLANs) have become important due to their reasonable cost and suitable characteristics. Accordingly, WLAN applications have become diversified, and there is a demand for limited delay communication (eg, wireless remote control) in a WLAN. To improve spectrum utilization and reduce transmission delay, IEEE 802.11ax introduced orthogonal frequency division multiple access (OFDMA), in which an access point (AP) can transmit frames to multiple stations (STA) at the same time. OFDMA is used in cellular network systems and ensures efficient use of spectrum while meeting delay requirements through appropriate resource allocation.

Key words: 802.11ax, 802.11ac, OFDMA, STA, AP, MU-MIMO.

УДК 004.71
ГРНТИ 49.33.29

АРХИТЕКТУРА СЕТИ INFINIBAND

В. К. Гераськин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С развитием нейросетей, аналитики и big data появилась необходимость в высокопроизводительной сети для надежной и быстрой передачи большого массива данных. Одним из решений стала сеть InfiniBand, разработанная компанией InfiniBand Trade Association (IBTA). В данной работе выполнен общий обзор принципов функционирования архитектуры сети, а также идей, вокруг которых она строится.

infiniband, точка-точка, высокоскоростная сеть, компьютерная сеть, RDMA

1. Введение

InfiniBand — коммутационная компьютерная сеть, которая обеспечивает высокоскоростную связь между взаимосвязанными узлами. Сеть *InfiniBand* обычно состоит из конечных узлов, таких как ПК, серверы, устройства хранения и периферийные устройства. Каждый узел оборудован канальным адаптером, и все передачи начинаются или заканчиваются этим адаптером. Эта сеть используется в таких сферах, как интеллектуальный анализ данных, *deep learning* и прогнозная аналитика [1].

2. Проблематика

Основная причина, по которой была начата разработка *IBA*, заключается в том, что вычислительная мощность существенно превышает возможности стандартных систем ввода-вывода, использующих шины. В то время как шины имеют главное преимущество в простоте и до сих пор хорошо служили отрасли, системы ввода-вывода на основе шин не используют должным образом лежащие в их основе технологии для обеспечения передачи данных (полосы пропускания) из системы на устройства. На это есть две причины.

В шинной архитектуре все коммуникации используют одну и ту же полосу пропускания. Чем больше портов добавлено в шину, тем меньше полоса пропускания доступна для каждого периферийного устройства. Существует ограничение на количество устройств на шину. Добавление моста может преодолеть лимит, и, хотя это позволяет подключать к системе больше устройств, данные по-прежнему проходят через центральную шину, когда происходит связь с другими устройствами. Тем более уровни задержки и перегрузки увеличиваются с каждым добавленным в систему мостом.

Поскольку стандартные шины отображаются в память, короткие последовательности, такие как передача команд и считывание состояния, выполняются с использованием операций загрузки (*load*) и сохранения (*store*) процессора. Загрузка, в отличие от сохранения, обычно не может продолжаться продолжительное время, не останавливая процессор для ожидания запрошенных данных. Это может быть очень серьезной проблемой эффективности. Почти 30%

времени работы процессора может быть затрачено на ожидание загрузки информации из ввода-вывода, а также ее обработку [1].

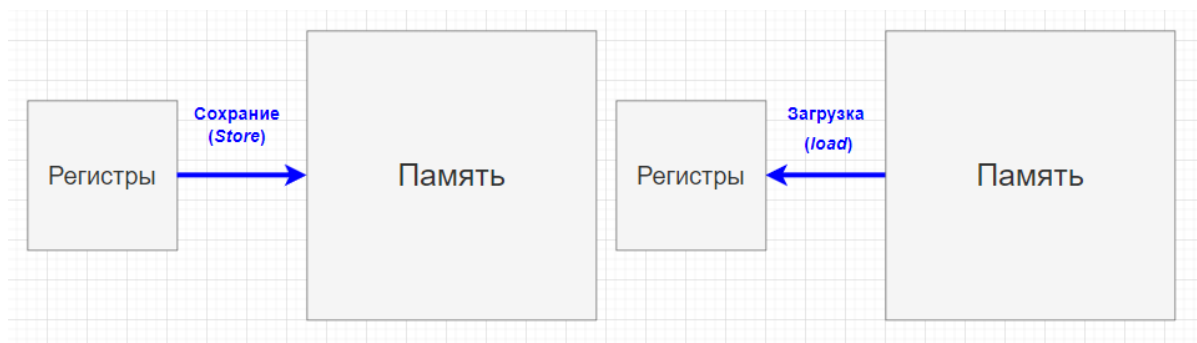


Рис. 1. Store/Load операции

3. Общая идея архитектуры *infiniband*

Проблема, упомянутая выше, была решена ранее отдельными поставщиками серверов различными способами. Однако, все такие решения были полностью или частично проприетарными, тем самым могли вызвать значительные расходы. Вместо этого *IBA* должна стать такой архитектурой, которая будет работать на широкий рынок и требовать меньших затрат. Архитектура строится на базе следующих двух принципов:

Infiniband использует принцип *RDMA* (англ. *Remote Direct Memory Access* — удалённый прямой доступ к памяти), при котором передача данных из памяти удалённого компьютера в локальную память инициатора запроса производится непосредственно сетевым контроллером, при этом исключается участие *CPU* удалённого узла. *RDMA* позволяет передавать данные без дополнительной буферизации и не требует активной работы ОС, библиотек или приложения на узле, к памяти которого производится обращение.

InfiniBand использует коммутируемую среду с соединениями точка-точка [2]. Коммутационная структура «точка-точка» означает, что к каждому каналу подключено ровно одно устройство на каждом конце. Такая архитектура обеспечивает масштабируемость, которая может быть достигнута путем добавления коммутаторов к сети и подключением дополнительных конечных узлов через коммутаторы.

4. Элементы *Infiniband*

Архитектура *InfiniBand* (рис. 2) определяет несколько устройств, необходимых для коммуникации: каналный адаптер, коммутатор, маршрутизатор и менеджер подсети. В подсети должен быть хотя бы один каналный адаптер для каждого конечного узла и диспетчер подсети для настройки и обслуживания каналов. Все каналные адаптеры и коммутаторы должны иметь агент управления подсетью (*Subnet Management Agent SMA*), необходимый для взаимодействия с диспетчером подсети [2].

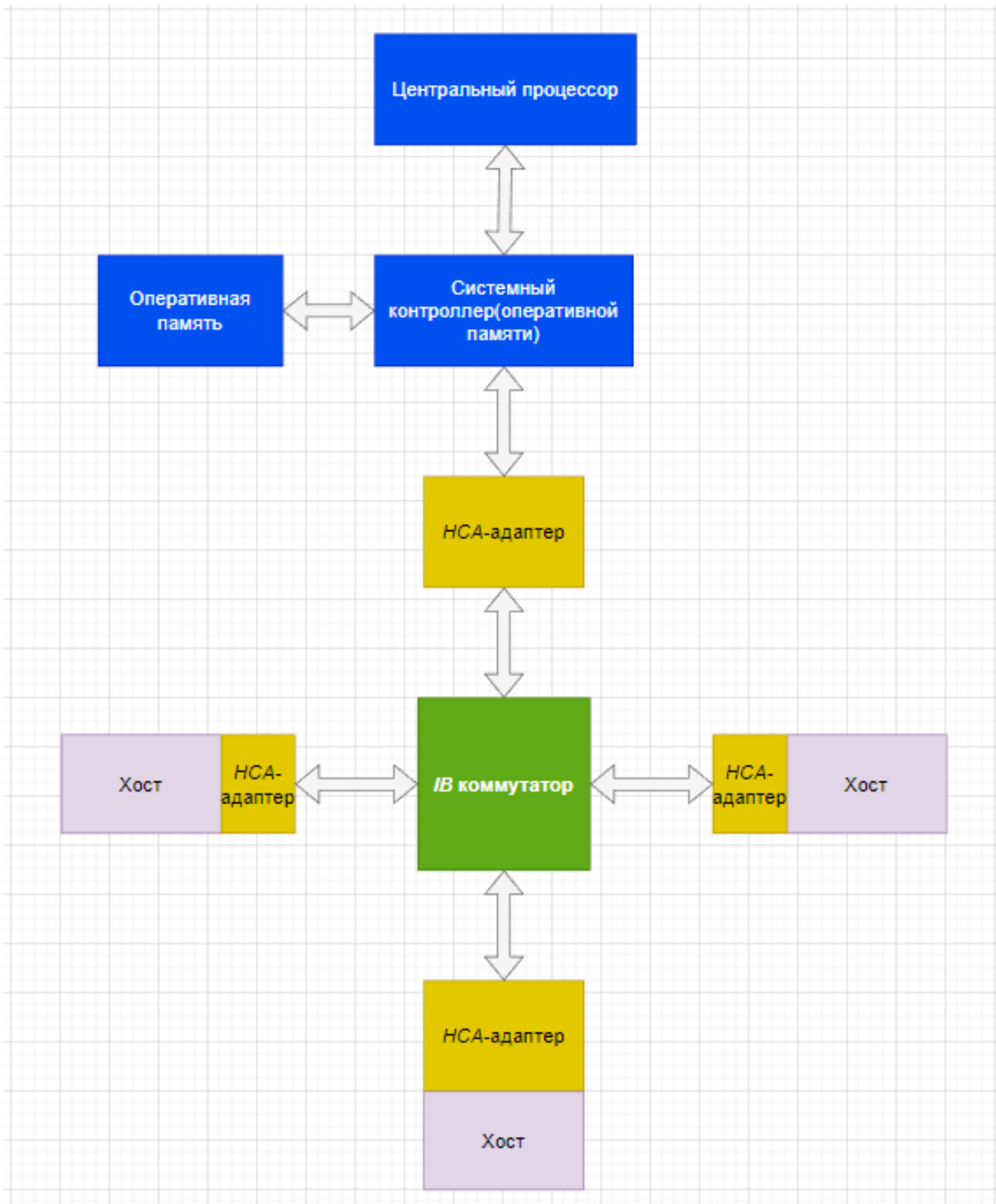


Рис. 2. Архитектура

Конечные узлы, такие как хосты и устройства, отправляют сообщения по каналам к другим конечным узлам; сообщения маршрутизируются коммутаторами. HCA обеспечивает интерфейс для хоста-устройства для взаимодействия с сетью, пример устройства можно увидеть на рис. 3.

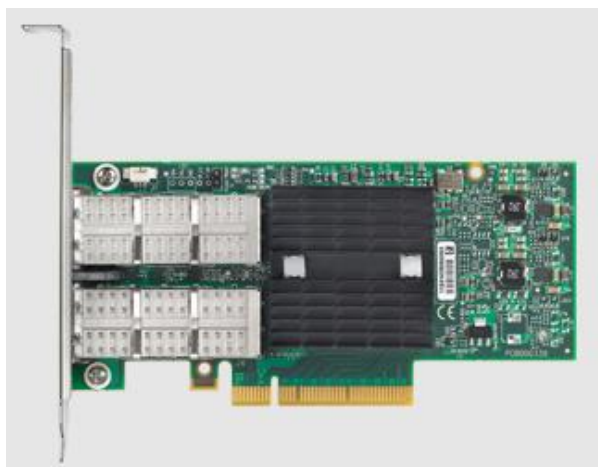


Рис. 3. 2-портовый адаптер HCA

Коммутатор содержит более одного порта *InfiniBand* и перенаправляет пакеты с одного своего порта на другой на основе *LID*, содержащегося в заголовке локального маршрута второго уровня. Все устройства внутри подсети имеют 16-битный локальный идентификатор (*LID*), назначенный диспетчером подсети. Все пакеты, отправленные внутри подсети, используют *LID* для адресации [3]. Помимо пакетов управления, коммутатор не получает и не генерирует пакеты. Подобно каналному адаптеру, коммутаторам необходим внедренный *SMA* для ответа на пакеты управления подсети.

Маршрутизаторы *InfiniBand* пересылают пакеты из одной подсети в другую. В отличие от коммутатора, маршрутизатор считывает *GRH* для пересылки пакета на основе его адреса сетевого уровня *IPv6*. Пакеты, отправляемые между подсетями, содержат заголовок глобального маршрута (*Global Route Header (GRH)*). Маршрутизатор перестраивает каждый пакет с подходящим для другой подсети *LID*.

Менеджер подсети управляет локальной подсетью и обеспечивает ее непрерывную работу. В подсети должен присутствовать хотя бы один менеджер для управления всеми настройками коммутаторов и маршрутизаторов, а также для реконфигурации подсети, в случае обрыва соединения или появления новых участников. Менеджер подсети может находиться внутри любого из устройств в подсети. Диспетчер подсети связывается с устройствами из подсети через каждый выделенный *SMA*.

В подсети может находиться несколько менеджеров подсети, однако активен может быть только один [4]. Неактивные менеджеры подсети (резервные) хранят копии сетевой таблицы активного менеджера и проверяют, что активный менеджер подсети работает исправно. Если активный менеджер подсети выйдет из строя, резервный менеджер возьмет на себя обязанности активного, чтобы не дать сети выйти из строя [4].

Как видно из выше сказанного, сеть *Infiniband* обладает достаточно простой структурой с понятной идеей. Благодаря технологии *RDMA* процессоры освобождаются от необходимости выполнения ненужной работы, что в условиях

обучения нейромоделей крайне важно, а высокая пропускная способность с топологией точка-точка позволяет быстро перемещать данные между серверами.

Список используемых источников:

1. Paul Grun. Introduction to InfiniBand for End Users : InfiniBand Trade Association, 2010.
2. Gregory F. Pfister. Aspects of the InfiniBand Architecture :CLUSTER, 2001.
3. An Integrated Tutorial on InfiniBand, Verbs, and MPI // IEEE Patrick MacArthur, Qian Liu, Robert D. Russell, Fabrice Mizero, Malathi Veeraraghavan, John M. Dennis. 2017..
4. Adaptive Routing in InfiniBand Hardware // IEEE José Rocher-González, Ernst Gunnar Gran, Sven-Arne Reinemo, Tor Skeie, Jesús Escudero-Sahuquillo, Pedro Javier Garcíaю. 2022.

Geraskin V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Architecture of the InfiniBand network.

With the development of neural networks, analytics and big data, there is a need for a high-performance network for reliable and fast transmission of a large amount of data. One of the solutions was the InfiniBand network, developed by the InfiniBand Trade Association (IBTA) specifically for areas where reliability and high bandwidth play a key role. This paper provides a general overview of the principles of the network architecture, as well as the ideas around which it is built.

Key words: *infiniband, point-to-point, high-speed network, computer network, RDMA.*

УДК 004.75
ГРНТИ 50.39.15

BIG DATA И ТУМАННЫЕ ВЫЧИСЛЕНИЯ

Е. Е. Ермолаев, Д. С. Кукунин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Интеллектуальные устройства нашли повсеместное применение в жизни общества и стали основным пластом компьютерных вычислений. Стало ясно, что распределенные вычисления необходимы для дальнейшего развития цифровой экономики. В данной работе выполнен общий обзор принципов функционирования туманных вычислений, а также какую роль играют в них большие данные и особенности баз данных.

большие данные, туманные вычисления, высокоскоростная сеть, интернет вещей, базы данных

1. Введение

Туманные вычисления — это развивающаяся парадигма вычислений, которая предлагает ресурсы, лежащие между пограничными устройствами и облачным центром обработки данных. Эта технология необходима для обработки больших объемов данных из Интернета вещей на высокой скорости с малой задержкой.

2. Предпосылки

Туманные вычисления актуальны в контексте глобальных распределенных систем, где многие клиенты находятся на границе Интернета. Такими клиентами могут быть мобильные или потребительские устройства (например, смартфон, смарт-часы, гарнитура виртуальной реальности (VR)), используемые людьми в интерактивном режиме, или устройства, являющиеся частью Интернета вещей (например, интеллектуальные счетчики, камеры дорожного движения и сигнализация, беспилотные автомобили) для машин.

Клиент может быть как потребителем данных или исполнительным механизмом, получающим управляющие сигналы (уведомление на умных часах, изменение сигнала на светофоре), так и производителями данных (частота сердечных сокращений со смарт-часов, видео с дорожных камер).

Существуют две современные модели вычислений для приложений и аналитики, которые используют данные или генерируют контент и элементы управления для таких клиентов на границе Интернета. [1]

Как показано на рис. 1 в облачно-ориентированной модели также называемые облачными вычислениями, данные от этих клиентов отправляются в центральный центр обработки данных, где обработка выполняется, а ответы, если таковые имеются, отправляются обратно тому же или другому клиенту или клиентам. [4]

В гранично-ориентированной модели или граничных вычислениях часть (или даже вся) обработка выполняется на устройстве источнике данных, а все остальное делается в облаке. [4]



Рис. 1. Связи между ресурсами в облачной, граничной и P2P-моделях

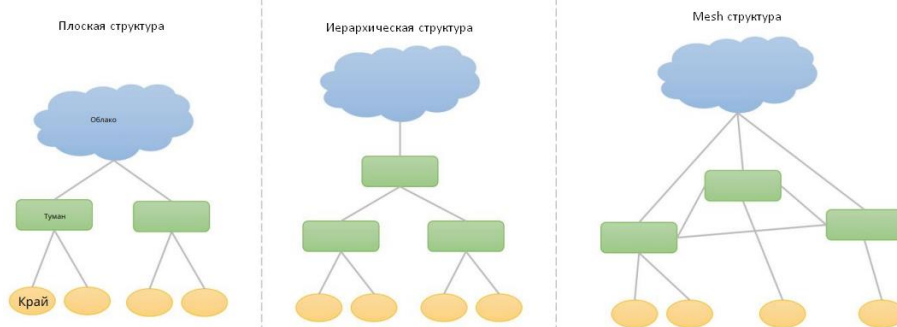


Рис. 2. Типы используемых туманных структур

3. Роль больших данных

Одним из основных причин развертывания и использования туманных вычислений являются большие данные, генерируемые на границе сети. Это ускоряется развертыванием IoT. Традиционные веб-клиенты, которые просто потребляют услуги и контент из Интернета создали рост сетей распространения контента (CDN), чтобы обслуживать их с низкой задержкой. Данные вместо того, чтобы генерироваться на датчиках и устройствах IoT генерируются на конечных устройствах клиента. В этом контексте туманные вычисления описываются как обратная CDN.

Большой объем данных IoT поступает в виде потоков наблюдений или данных временных рядов от широко разбросанных датчиков. Эти потоки данных различаются по своей скорости — один отправляет данные каждые 15 минут (счетчики коммунальных услуг), другой каждую секунду (сердечный ритм с фитнес-часов), и до 50 Гц с измерительных блоков в интеллектуальных электрических сетях — и количество датчиков может варьироваться до миллионов для развертывания в масштабе города.

Это высокоскоростные потоки данных, которые чувствительны к задержкам и требуют онлайн-аналитики и принятия решений, например, для предоставления предупреждений о работоспособности или управления поведением энергосистемы. Здесь туманные вычисления могут помочь перенести принятие решений ближе к краю, чтобы уменьшить задержку. Кроме того, они могут уменьшить пропускную способность, используемую по сети Интернет и ограничить передачу данных в локальную сеть. А также, предоставить более высокие вычислительные ресурсы и ускорители для развертывания сложной аналитики.

Существует три важных аспекта которые нужно учитывать при построении архитектур туманных вычислений со стороны баз данных [3]:

1) Поддержка гибридной базы данных: база данных Интернета вещей с гибкостью для обработки полу-структурированных, неструктурированных, геопространственных и традиционных реляционных данных. Различные типы данных могут сосуществовать в одной базе данных.

2) Встроенная база данных развертывания: базу данных IoT часто необходимо встраивать для обработки и сжатия данных, а также для передачи по сетям и между ними. Хорошими функциями являются минимальная настройка или ее отсутствие во время развертывания, самонастройка и автоматическое восстановление после сбоя.

3) Миграция в облако: сети IoT могут хранить и обрабатывать данные в масштабируемой и гибкой облачной инфраструктуре. Доступ к платформе можно получить с помощью веб-интерфейсов и вызовов API.

Платформы больших данных в облаках и кластерах быстро развиваются благодаря таким платформам, как Spark, Storm, Flink, HBase, Pregel и TensorFlow, помогающим хранить и обрабатывать большие объемы данных, высокоскоростные потоки и полу-структурированные данные. Облака также предлагают эти решения в формате платформы как услуга.

Примеры приложений

Приложения, стимулирующие развертывание и потребность в туманных вычислениях, разнообразны. Они охватывают приложения виртуальной и дополненной реальности (VR/AR) и игры, промышленный Интернет вещей. [2]

1) Умные города являются ключевым фактором для туманных вычислений, и они уже внедряются. Здесь используются датчики звука и окружающей среды, видеокамеры и мониторы энергоснабжения объединены вместе с вычислительными ресурсами и пропускной способностью сети в составе туманных комплексов, размещенных вдоль улиц. Они помогают собирать данные с датчиков, выполнять базовую аналитику, а также предлагают точки доступа Wi-Fi для общего пользования.

2) В здравоохранении носимые устройства играют большую роль не только в личном фитнесе, но и в качестве вспомогательных технологий. В рамках проектов изучалось использование таких устройств для наблюдения за человеком, чтобы определить, когда пациенты, перенесшие инсульт, упали и нуждаются в посторонней помощи. Может применяться и для прогностической аналитики сигналов мозга, отслеживаемых с помощью ЭЭГ-гарнитур, для определения психического состояния пациента в реальном времени.

3) Беспилотные автомобили и дроны — новые области применения, в которых туманные вычисления играют ключевую роль. Обе эти платформы имеют множество встроенных датчиков и аналитику в реальном времени для автономной мобильности. Автомобильные сети позволяют подключенным автомобилям и общаться друг с другом (V2V) для совместного обмена информацией для принятия решений о трафике и дорожных условиях.

Дальнейшие исследования

Последующие исследования в данной сфере будут сосредоточены на следующих аспектах работы:

1) Туманные архитектуры. Многие из предложенных архитектурных проектов туманных систем не применялись в больших масштабах и являются просто правдоподобными предложениями. В то время как развертывание в масштабе города с сотнями противотуманных устройств становится доступным, опыт их эксплуатации будет использоваться при проектировании будущих проектов.

2) Управление сетью, вероятно, станет ключевой технической проблемой, поскольку управление трафиком в городской сети (MAN) приобретает все большее значение. В отличие от статических ресурсов тумана, мобильные или специальные ресурсы, такие как автомобильный туман, будут создавать проблемы с обнаружением ресурсов, доступом и координацией.

3) Управление данными. Ключевой проблемой станет отслеживание и управление контентом через периферию, туман и облако. Частично это является результатом того, что устройства в IoT выступают в качестве источников данных и вычислительных платформ, что требует координации в киберпространстве и физическом мире. Обнаружение, репликация, размещение и сохранение данных потребуют тщательного изучения в контексте глобальных сетей и временных вычислительных ресурсов.

4) Модели программирования и платформы. Несмотря на рост периферийных и туманных ресурсов, не хватает общей программной абстракции или среды выполнения для определения и выполнения распределенных приложений на этих ресурсах.

5) Безопасность, Конфиденциальность, Доверие. В отличие от облачных вычислений, где существует определенная степень доверия к поставщику услуг, туманные вычисления могут содержать ресурсы от различных и разовых поставщиков. Кроме того, туманные устройства не могут быть физически защищены, как центр обработки данных, и могут быть доступны третьим сторонам [1].

Выводы

Парадигма туманных вычислений набирает все большую популярность благодаря способности дополнять облачные решения за счет масштабирования и оптимизации инфраструктуры IoT, что особенно эффективно при решении задач в реальном времени. Туманные вычисления рассматриваются как расширение облака в своей основе, которое имеет некоторые специфические вычислительные ресурсы и регистры хранения данных и располагается в узлах сетей. Благодаря своей гибкой способности обрабатывать данные ближе к месту их производства, туманные вычисления значительно решают проблему большого объема данных, разнообразия и скорости. Но перед тем, как туманные вычисления станут применяться повсеместно, необходимо решить еще несколько проблемных, но важных аспектов в их работе.

Список используемых источников:

1. Big Data Analytics with Fog Computing in integrated Cloud Fog and IoT Architecture for Smart Devices : Sultan Ahmad, June 2020.
2. Fog Computing with Distributed Database : Tsukasa Kudo, 2018 IEEE AINA.
3. Distributed Database Systems and Edge/Fog/Cloud Computing : McObject LLC 2019.
4. Towards Distributed Data Management in Fog Computing : Vasileios Moysiadis, Panagiotis G. Sarigiannidis, Ioannis D. Moscholios September 2018.

Ermolaev E., Kukunin D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Big data and fog computing.

Intelligent devices have found widespread use in society and have become the main layer of computing. It became clear that distributed computing is necessary for the further development of the digital economy. This paper provides a general overview of the principles of fog computing, as well as the role that big data and databases architecture play in them.

Key words: Big Data, fog computing, high-speed network, IoT, data bases.

УДК 004.722
ГРНТИ 49.33.29

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ

А. К. Зенченко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Появление новейших разработок в сфере информационных технологий, постоянная модернизация мобильных сетей, увеличение пользователей и соответственно увеличение объема трафика в сети, требуют менее ресурсоемкой и менее сложной в управлении и масштабировании сети, чем традиционная сетевая архитектура. Это привело к созданию принципиально нового подхода к построению сети, концепции «Программно-Конфигурируемых Сетей» – ПКС (англ. Software-defined Networking – SDN). С точки зрения обеспечения безопасности сети ПКС, существуют особенности, связанные с архитектурным подходом к разделению плоскостей и выделению централизованного управляющего устройства.

информационная безопасность, программно-конфигурируемые сети

Введение в ПКС

Программно-конфигурируемые сети представляют собой средство для реализации сети следующего поколения, так как данная концепция позволяет создавать динамичную, легко масштабируемую и гибкую в управлении сетевую архитектуру. К тому же ПКС позволил создать принципиально новый подход к программированию сети и открыл возможности для динамического управления элементами сети через различные интерфейсы и приложения. Главная особенность ПКС, это наличие контроллера ПКС, который является централизованным управляющим устройством, и разделение плоскости управления и плоскости передачи данных. Цель создания такой архитектуры сети, гибкость, автоматизация и снижение издержек.

Рассматривая обеспечение безопасности ПКС, контроллер как ключевой элемент в управлении всей ПКС является наиболее уязвимым местом, и в случае атаки на контроллер возникнут критичные последствия для всей ПКС [1].

Основными угрозами для ПКС, остаются уже давно знакомые вариации таких атак, как «отказ в обслуживании», а также подмена контроллера и т.д.

Цели данной статьи:

- рассмотреть основные проблемы связанные с защитой передачи данных в ПКС;
- описать решения проблем информационной безопасности в ПКС;

Основные векторы атак в ПКС

Так как инфраструктура ПКС может быть использована во многих областях, в центрах обработки данных, в облачных вычислениях, так же перспективным направлением использования является интернет вещей, важно чтобы такая

инфраструктура обеспечивала информационную безопасность, а именно: конфиденциальность данных, целостность.

Рассмотрим возможные атаки на сети ПКС. За счет упрощения конфигурации и управления сетевой архитектурой, появляются также и определенные потенциальные уязвимости. С учетом того, что ПКС имеет трехуровневую архитектуру, можно выделить следующие точки, для возможной атаки (рис. 1).

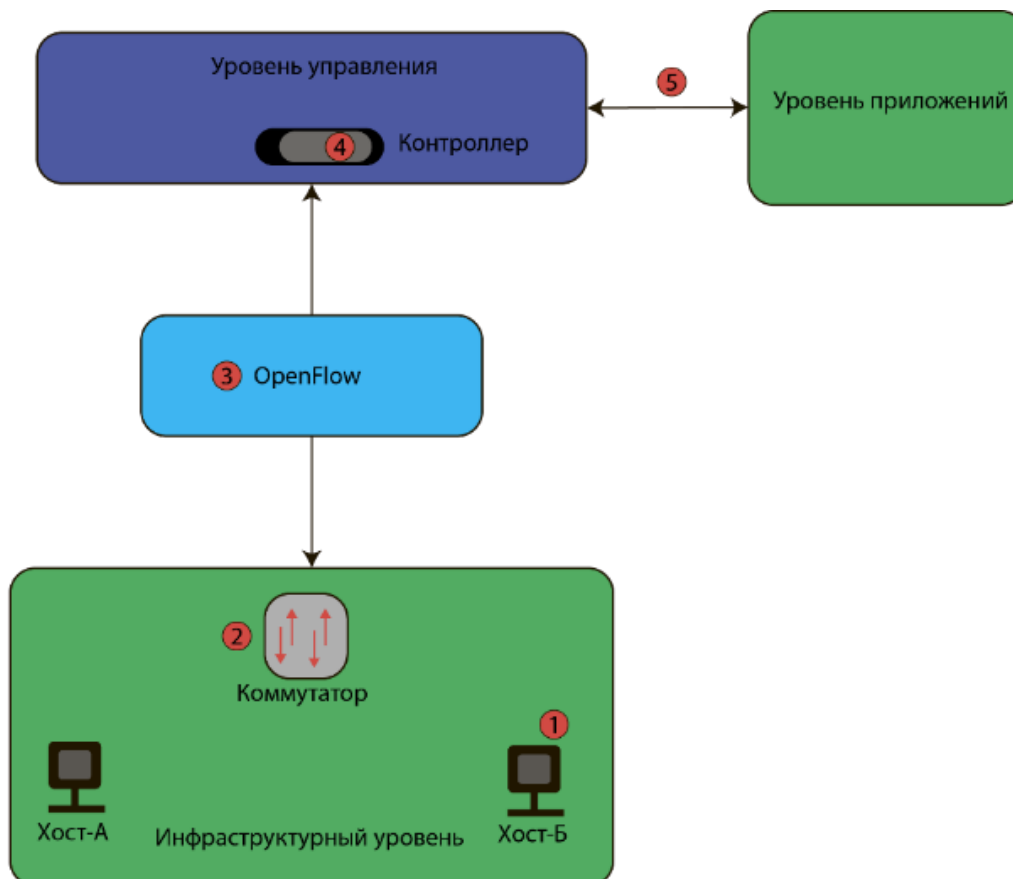


Рис. 1. Возможные точки атак на сеть ПКС

Следовательно, для обеспечения информационной безопасности ПКС, необходимо обеспечить безопасность на каждом уровне архитектуры, в особенности уровню управления, где находится контроллер, который является особо важным компонентом ПКС.

Рассмотрим основные типы атак на уровни архитектуры ПКС [2].

Атаки на инфраструктурный уровень:

- *ARP Poisoning*;
- *Fake topology*;
- *TCAM exhaustion*;

Атаки на уровень управления:

- *DoS* контроллера.

Атаки на уровень приложений:

- *HTTP spoofing*.

Атаки на канал связи:

- *MiTM (Man in the middle)*.

ARP Poisoning – атакующие машины, подменяют информацию о устройствах в сети при помощи ложных ARP-запросов. Из-за чего контроллер ПКС устанавливает вредоносные правила потоков, что позволяет перехватить трафик других пользователей.

Fake topology – создание поддельного звена в сети, с помощью линейной топологии. Позволяет нарушить маршрутизацию и правильное направление потоков в сети.

TSCAM exhaustion – атака направлена на память коммутатора, зараженное устройство отправляет множество сообщений, тем самым заставляя контроллер устанавливать большое количество правил к потокам, расходуя память, таким образом появляется высокая задержка и гарантированная потеря пакетов.

Атака «человек по середине» (*MiTM*) – это комплексная атака, которая включает в себя успешные атаки на *IP*-маршрутизацию или протоколы (например, *ARP*, *DNS* или *DHCP*), приводящие к перенаправлению трафика. Методом компрометации канала связи атака направлена на обход взаимной аутентификации злоумышленник устанавливает независимые связи с жертвами и передает сообщения между ними. Атака такого типа, скорее обобщенная концепция, которая может быть реализована во многих сценариях, в отличие от конкретных видов атак. Как правило, атакующий имеет возможность просматривать данные между двумя узлами сети. Атака «человек по середине» может быть пассивной или активной. В пассивном режиме злоумышленники похищают конфиденциальную информацию. При активных атаках злоумышленники модифицируют данные при передаче или вводят собственные данные.

HTTP spoofing – простые *HTTP*-запросы отправляются *GET* и *POST*, которые требуют огромного количества данных в ответ, потребляющих большой объем полосы пропускания, сбрасывая сервер.

Исследуя список возможных атак, можно сделать вывод о том, что для ПКС, ввиду видимого центра архитектуры, атаки с подменой данных и разновидности *DDoS* представляют большую опасность, чем в обычных сетях передачи данных.

Безопасность ПКС играет ключевую роль при использовании их в «облачных» сервисах, обеспечение безопасности необходимо как для дальнейшего развития самих ПКС, так и построенных на её основе сетей.

Методы обеспечения безопасности в ПКС

Рассмотрим методы обеспечения безопасности в ПКС.

Как уже говорилось ранее, основной целью атаки, чаще всего становится контроллер ПКС, следовательно необходимо обеспечить его безопасность и сделать невозможными атаки на уровень топологии, так как это влечет за собой следующим шагом, получение доступа к контроллеру. Для исключения возможности атак на контроллер ПКС, необходимо соблюсти требования к безопасности для контроллеров ПКС, представленные в таблице 1.

ТАБЛИЦА 1. Основные требования к безопасности контроллеров ПКС

Защита интерфейсов контроллера	Службы безопасности контроллера	Методы повышения надежности
1. безопасный канал связи 2. безопасность <i>API</i> (<i>Application Programming Interface</i>) <i>GUEST/REST</i> 3. контроль авторизации для вложенных приложений 4. учет и аудит авторизации	1. интеграция <i>IDS/IPS</i> (<i>Intrusion Detection System/Intrusion Prevention System</i>) 2. аутентификация и авторизация 3. мониторинг ресурсов 4. утилиты для изоляции приложений	1. репликация 2. механизмы самовосстановления 3. доверие между контроллерами, устройствами и прикладным программным обеспечением 4. домены безопасности

Контроллер ПКС обладает тремя интерфейсами *D-CPI*, *I-CPI* и *A-CPI*, для контроллера данных, промежуточного контроллера и контроллера приложений соответственно. Также существует еще графический интерфейс пользователя, называемый *GUI* (*graphical user interface*). Для всех интерфейсов, должна быть обеспечена защита конфиденциальности.

При обеспечении безопасности также необходимо обеспечивать устранение уязвимостей в протоколе *OpenFlow*, являющегося одним из самых используемых в ПКС на данный момент.

Для создания безопасного подключения в *OpenFlow* и проверки подлинности используются такие протоколы как:

- *Transport Layer Security (TLS)*;
- *Secure Shell (SSH)*;
- *IPSec*.

Так же существуют комплексные решения для обеспечения безопасности в ПКС, которые реализуются как программное обеспечение, дополнительные расширения для контроллеров, облачные платформы и сервисы [1], [3],[4],[5], [6].

– ***FORTNOX***: проверяет правила потока с цифровой подписью. Является расширением для контроллера *NOX*, представляет из себя систему контроля доступа на основе ролей, фокус данного решения направлен на плоскость управления.

– ***FlowVizor***: прозрачный прокси между контроллерами и переключателями. Делегирует управление срезами для разных контроллеров – один срез не может контролировать трафик другого.

– ***VeriFlow***: является системой проверки состояния сети при пересылке пакетов.

– *AvantGuard*: соединения *TCP* поддерживаются модулем подключения миграции чтобы избежать угроз атаки. С помощью управляющего триггерного модуля плоскость данных, имеет возможность сообщать о состоянии сети и активировать определенные правила потока.

– *OpenSec*: действует как виртуальный уровень между пользователем и контроллером *OpenFlow*. автоматически преобразует политики безопасности в набор правил, которые вставляются в сетевые устройства. *OpenSec* позволяет сетевым операторам определять, как автоматически реагировать при обнаружении вредоносного трафика.

– *SE-Floodlight*: Расширение для повышения безопасности ПКС с помощью проверки подлинности на основе ролей.

Рассматривая программируемую сеть со стороны обеспечения безопасности, можно заметить немало плюсов. Таких как возможность реализовать политику безопасности в виде файла данных, базы данных, таблиц или других структур данных [1].

К тому же можно применять правильную защиту к конкретному потоку, и идентифицировать те, которые требуют более глубоких проверок.

Так же возможность сравнивать трафик в реальном времени дает возможность выявлять отклонения и динамически перенаправлять трафик, вызвавший подозрения на дополнительную проверку или в изоляцию.

Заключение

Преимуществом технологии ПКС и её слабым местом является наличие центра управления и маршрутизации сети. Таким образом было выявлено, что изменение структуры сети с помощью ПКС, приводит к появлению новых угроз безопасности, кроме того, угрозы которые давно известны в традиционных сетях, также или даже в большей степени опасны в случае ПКС, но в противовес этому гибкость архитектуры, открывающая большое количество возможностей для развития инструментов безопасности. Следовательно, необходимо применять совокупность комплексных мер защиты как контроллера ПКС, так и устранять уязвимости протокола *OpenFlow* используя при передаче безопасные каналы, организованные с помощью протоколов *SSH* и *TLS*, следовательно цели данной статьи были выполнены, в последующих исследованиях планируется смоделировать сегмент сети ПКС с внедрением известных механизмов обеспечения информационной безопасности.

Список используемых источников:

1. Захаров А. А., Попов Е. Ф., Фучко М. М. Аспекты информационной безопасности архитектуры SDN // Вестник СибГУТИ. 2016. № 1 (33). С. 83-92.
2. Курочкин И. и др. Безопасность сетей SDN. Классификация атак // Современные информационные технологии и ИТ-образование. 2015. Т. 2. №. 11. С. 381-383.
3. Sherwood R. et al. Flowvisor: A network virtualization layer // OpenFlow Switch Consortium, Tech. Rep. 2009. Т. 1. С. 132.

4. Khurshid A. et al. Veriflow: Verifying network-wide invariants in real time // Proceedings of the first workshop on Hot topics in software defined networks. 2012. С. 49-54.
5. Klöti R., Kotronis V., Smith P. OpenFlow: A security analysis // 2013 21st IEEE International Conference on Network Protocols (ICNP). IEEE. 2013. С. 1-6.
6. Филатов Н. А. УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ В ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ СЕТЯХ // Перспективные информационные технологии (ПИТ 2018). 2018. С. 339-341.

Zenchenko A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Ensuring Information Security in Software-Defined Networks.

The advent of new developments in the field of information technology, the constant modernization of mobile networks, the increase in the number of users and the increase in the growth of traffic in the network, the need for fewer resources and less involvement in managing and scaling the network than traditional network architecture. This led to the conclusion about a fundamentally new approach to building a network, the discovery of "Software-defined networks" - SDN. From the point of view of the security of the SDN network, in the aggregate, the features associated with the architectural approach to the separation of planes and the allocation of a centralized control device.

Key words: *information security, software-defined networks.*

УДК 004.65
ГРНТИ 20.23.19

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ БАЗ ДАННЫХ

Д. С. Кукунин¹, К. А. Елисеева¹, И. О. Федотов²

¹Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
²ООО «Естественный интеллект»

С развитием big data и увеличением бизнеса e-commerce традиционные реляционные базы данных выходят из обихода по причине медленного поиска и обработки данных. В данной работе выполнен сравнительный анализ запросов в современных базах данных полнотекстового поиска и OLAP баз данных.

Big-data, e-commerce, Elasticsearch, ManticoreSearch, ClickHouse

Поездки на такси в Нью-Йорке (Нью-Йорк), вероятно, являются наиболее часто используемым эталоном в области анализа данных. Все началось с того, что Годд В. Шнайдер[1] решил в 2015 году подготовить первую подборку для анализа 1,1 миллиарда поездок на такси и Uber в Нью-Йорке. Затем Марк Литвинчик[2] продолжил тестирование множества баз данных и поисковых систем с использованием сбора данных. DB Benchmarks настроили подготовку сбора данных, чтобы упростить его использование, и сделали его доступным как часть самого прозрачного и открытого набора тестов базы данных с открытым исходным кодом. [3]

Сбор

данных

Сбор данных охватывает 1,7 миллиарда поездок на такси и арендованных транспортных средствах (Uber, Lyft и т.д.), Совершенных в Нью-Йорке с 2009 года. Большая часть необработанных данных поступает от Комиссии по такси и лимузинам Нью-Йорка.

Запись о сборе данных включает в себя множество различных атрибутов поездки на такси:

- *Дата и время получения товара*
- *Координаты посадки и высадки*
- *Названия мест получения и высадки груза*
- *Сумма комиссии и чаевых*
- *Скорость ветра, глубина снега*
- *И во многих других областях*

Его можно использовать в основном для тестирования аналитических запросов, но он также включает в себя пару полнотекстовых полей, которые можно использовать для тестирования возможностей свободного текста в базах данных.

Весь список полей и их типов данных выглядит следующим образом:

```
"properties": {  
  "vendor_id": {"type": "keyword"},
```



```
"pickup_datetime": {"type": "date", "format": "epoch_second"},
"dropoff_datetime": {"type": "date", "format": "epoch_second"},
"store_and_fwd_flag": {"type": "keyword"},
"rate_code_id": {"type": "integer"},
"pickup_longitude": {"type": "float"},
"pickup_latitude": {"type": "float"},
"dropoff_longitude": {"type": "float"},
"dropoff_latitude": {"type": "float"},
"passenger_count": {"type": "integer"},
"trip_distance": {"type": "float"},
"fare_amount": {"type": "float"},
"extra": {"type": "float"},
"mta_tax": {"type": "float"},
"tip_amount": {"type": "float"},
"tolls_amount": {"type": "float"},
"ehail_fee": {"type": "float"},
"improvement_surcharge": {"type": "float"},
"total_amount": {"type": "float"},
"payment_type": {"type": "keyword"},
"trip_type": {"type": "byte"},
"pickup": {"type": "keyword"},
"dropoff": {"type": "keyword"},
"cab_type": {"type": "keyword"},
"rain": {"type": "float"},
"snow_depth": {"type": "float"},
"snowfall": {"type": "float"},
"max_temp": {"type": "byte"},
"min_temp": {"type": "byte"},
"wind": {"type": "float"},
"pickup_nyct2010_gid": {"type": "integer"},
"pickup_ctlabel": {"type": "keyword"},
"pickup_borocode": {"type": "byte"},
"pickup_boroname": {"type": "keyword"},
"pickup_ct2010": {"type": "keyword"},
"pickup_boroct2010": {"type": "keyword"},
"pickup_cdeligibil": {"type": "keyword"},
"pickup_ntacode": {"type": "keyword"},
"pickup_ntaname": {"type": "text", "fields": {"raw": {"type": "keyword"}}},
"pickup_puma": {"type": "keyword"},
"dropoff_nyct2010_gid": {"type": "integer"},
"dropoff_ctlabel": {"type": "keyword"},
"dropoff_borocode": {"type": "byte"},
"dropoff_boroname": {"type": "keyword"},
"dropoff_ct2010": {"type": "keyword"},
```

```
"dropoff_boroc2010": {"type": "keyword"},
"dropoff_cdeligibil": {"type": "keyword"},
"dropoff_ntacode": {"type": "keyword"},
"dropoff_ntaname": {"type": "text", "fields": {"raw": {"type": "keyword"}}},
"dropoff_puma": {"type": "keyword"}
}
```

Базы данных

Тест доступен для 3 баз данных

- Clickhouse - мощная база данных OLAP,
- Elasticsearch - универсальная “поисково-аналитическая система”,
- Manticore Search - “база данных для поиска”, альтернатива Elasticsearch.

В этом тесте мы вносим **как можно меньше изменений в настройки базы данных по умолчанию**, чтобы не дать ни одному из них несправедливого преимущества. Тестирование на максимальной настройке не менее важно, но это тема для другого теста. Здесь мы хотим понять, какую задержку может получить обычный неопытный пользователь после простой установки базы данных и запуска ее с настройками по умолчанию. Но чтобы было справедливо сравнивать одно с другим, нам все же пришлось изменить несколько настроек:

- Clickhouse: без настройки, просто
- CREATE TABLE ... ENGINE = MergeTree() ORDER BY id
- стандартный образ clickhouse-server docker.
- Elasticsearch: здесь, чтобы было справедливо сравнивать с другими

базами данных, мы должны были помочь Elasticsearch,:

- позволяя ему создавать 32 фрагмента: ("number_of_shards": 32), в противном случае он не мог бы использовать процессор, который имеет 32 ядра на сервере, поскольку, как сказано в официальном руководстве Elasticsearch, “Каждый фрагмент выполняет поиск в одном потоке процессора”.

- bootstrap.memory_lock=true поскольку, как сказано в https://www.elastic.co/guide/en/elasticsearch/reference/current/docker.html#_disable_swapping это нужно сделать для повышения производительности.

- image docker является стандартным

- Manticoresearch также используется в виде их собственного образа docker + столбчатой библиотеки, которую они предоставляют:

- как и в случае с Elasticsearch, мы также используем 32 сегмента в виде 32 простых индексов

- и мы используем столбчатое хранилище Manticore, поскольку сравнение хранилища Manticore по умолчанию в виде строк с столбчатыми хранилищами Clickhouse и Elasticsearch было бы несправедливым для такого большого сбора данных.

Настройка баз данных

Мы также настроили базы данных так, чтобы они не использовали никаких внутренних кэшей. Почему это важно:

1. В этом бенчмарке мы проводим **точное измерение задержки**, чтобы выяснить, какое время отклика могут ожидать пользователи, если они запустят один из тестируемых запросов в случайный момент, а не после многократного выполнения одного и того же запроса.

2. Любой кэш - это кратчайший путь к низкой задержке. Как написано в Википедии, "кэш хранит данные, чтобы будущие запросы на эти данные можно было обслуживать быстрее". Но кэши бывают разные, их можно разделить на 2 основные группы:

- те, которые просто кэшируют необработанные данные, хранящиеся на диске. Например, многие базы данных используются mmap() для сопоставления данных, хранящихся на диске, с памятью, легкого доступа к ним и позволяют операционной системе позаботиться об остальном (считывать их с диска, когда есть свободная память, удалять их из памяти, когда это необходимо для чего-то более важного и т. Д.). Это нормально с точки зрения тестирования производительности, потому что мы позволяем **каждой** базе данных использовать преимущества использования кэша страниц ОС (или его внутреннего аналогичного кэша, который просто считывает данные с диска), **это именно то, что мы делаем в этом бенчмарке.**

- те, которые используются для сохранения результатов предыдущих вычислений. И это нормально во многих случаях, но с точки зрения этого бенчмарка позволять базе данных включать такой кэш - плохая идея, потому что:

- это нарушает правильное измерение: вместо измерения времени вычисления вы начинаете измерять, сколько времени требуется, чтобы найти значение по ключу в памяти. Это не то, что мы хотим делать в этом тесте (но в целом это интересно, и мы, возможно, сделаем это в будущем и опубликуем какую-нибудь статью "Бенчмарк кэшей").

- даже если они сохраняют не полный результат конкретного запроса, а результаты его подсчетов, это нехорошо, потому что это нарушает идею теста - "какое время отклика могут ожидать пользователи, если они запустят один из тестируемых запросов в случайный момент".

- некоторые базы данных имеют такой кэш (обычно его называют "кэш запросов"), другие - нет, поэтому, если мы не отключим внутренние кэши базы данных, мы дадим несправедливое преимущество тем, у кого это есть.

Поэтому мы делаем все, чтобы убедиться, что ни одна база данных не выполняет такого рода кэширование.

Что именно мы делаем для достижения этой цели:

- clickhouse:

- SYSTEM DROP MARK CACHE, SYSTEM DROP UNCOMPRESSED CACHE, SYSTEM DROP COMPILED EXPRESSION CACHE перед тестированием каждого нового запроса (а не каждой попытки одного и того же запроса).

- elasticsearch:

- "index.queries.cache.enabled": false в своей конфигурации

○ /_cache/clear?request=true&query=true&fielddata=true перед тестированием каждого нового запроса (а не каждой попытки выполнения одного и того же запроса).

- Manticoresearch (в файле конфигурации):

```
qcache_max_bytes=0
docstore_cache_size = 0
```

- Операционная система:

○ мы делаем `echo 3 > /proc/sys/vm/drop_caches; sync` это перед каждым **НОВЫМ** запросом (А НЕ перед каждой попыткой). Т.е. для каждого нового запроса мы:

- остановить базу данных
- удаление кэша ОС
- начните все сначала
- сделайте самый первый холодный запрос и измерьте его время
- и сделайте еще десятки попыток (до 100 или до тех пор, пока коэффициент вариации не станет достаточно низким, чтобы считать результаты теста качественными).

Запросы

Запросы в основном представляют собой аналитические запросы, которые выполняют фильтрацию, сортировку и группировку. Также включили один полнотекстовый запрос:

[
"SELECT count(*) FROM taxi where pickup_ntaname = '0'",
"SELECT pickup_ntaname, count(*) c FROM taxi GROUP BY pickup_ntaname ORDER BY c desc limit 20",
"SELECT cab_type, count(*) c FROM taxi GROUP BY cab_type order by c desc LIMIT 20",
"SELECT passenger_count, avg(total_amount) a FROM taxi GROUP BY passenger_count order by a desc LIMIT 20",
"SELECT count(*) FROM taxi WHERE tip_amount > 1.5",
"SELECT avg(tip_amount) FROM taxi WHERE tip_amount > 1.5 AND tip_amount < 5",
"SELECT rain, avg(trip_distance) a FROM taxi GROUP BY rain order by a desc LIMIT 20",
{
"manticoresearch": "SELECT * FROM taxi where match('harlem east') LIMIT 20",
"clickhouse": "SELECT * FROM taxi where match(dropoff_ntaname, '(?i)\WHarlem\WEast\W') or match(pickup_ntaname, '(?i)\WHarlem\WEast\W') LIMIT 20",
"elasticsearch": "SELECT * FROM taxi where query('harlem east') LIMIT 20"
}
"SELECT avg(total_amount) FROM taxi WHERE trip_distance = 5",
"SELECT avg(total_amount), count(*) FROM taxi WHERE trip_distance > 0 AND trip_distance < 5",
"SELECT count(*) FROM taxi where pickup_ntaname != '0'",
"select passenger_count, count(*) c from taxi group by passenger_count order by c desc limit 20",
"select rain, count(*) c from taxi group by rain order by c desc limit 20",
"SELECT count(*) from taxi where pickup_ntaname='Upper West Side'",
"SELECT * from taxi limit 5",
"SELECT count(*) FROM taxi WHERE tip_amount = 5",

<code>"SELECT avg(total_amount) FROM taxi"</code>

<code>1</code>

Результаты

Вы можете найти все результаты на странице результатов, выбрав “Тест: такси”. Помните, что **единственная метрика высокого качества - это “Fast avg”, поскольку она гарантирует низкий коэффициент вариации и большое количество запросов, выполняемых для каждого запроса.** Остальные 2 (“Самый быстрый” и “Самый медленный”) предоставляются без гарантии, поскольку:

- **Самый медленный** - результат одной попытки, в большинстве случаев самый первый самый холодный запрос. Несмотря на то, что мы очищаем кэш ОС перед каждым холодным запросом, он не может считаться стабильным. Таким образом, он может быть использован только в информационных целях (хотя многие авторы тестов публикуют такие результаты без каких-либо оговорок).

- **Самый быстрый** - просто самый быстрый результат, он должен быть в большинстве случаев похож на показатель “Fast avg”, но может быть более изменчивым от запуска к запуску.

Помните, что тесты, включая результаты, на 100% прозрачны, как и все в этом проекте, поэтому: вы можете использовать тестовый фреймворк, чтобы узнать, как они были созданы найдите необработанные результаты теста в каталоге результатов.

Результаты бенчмарков

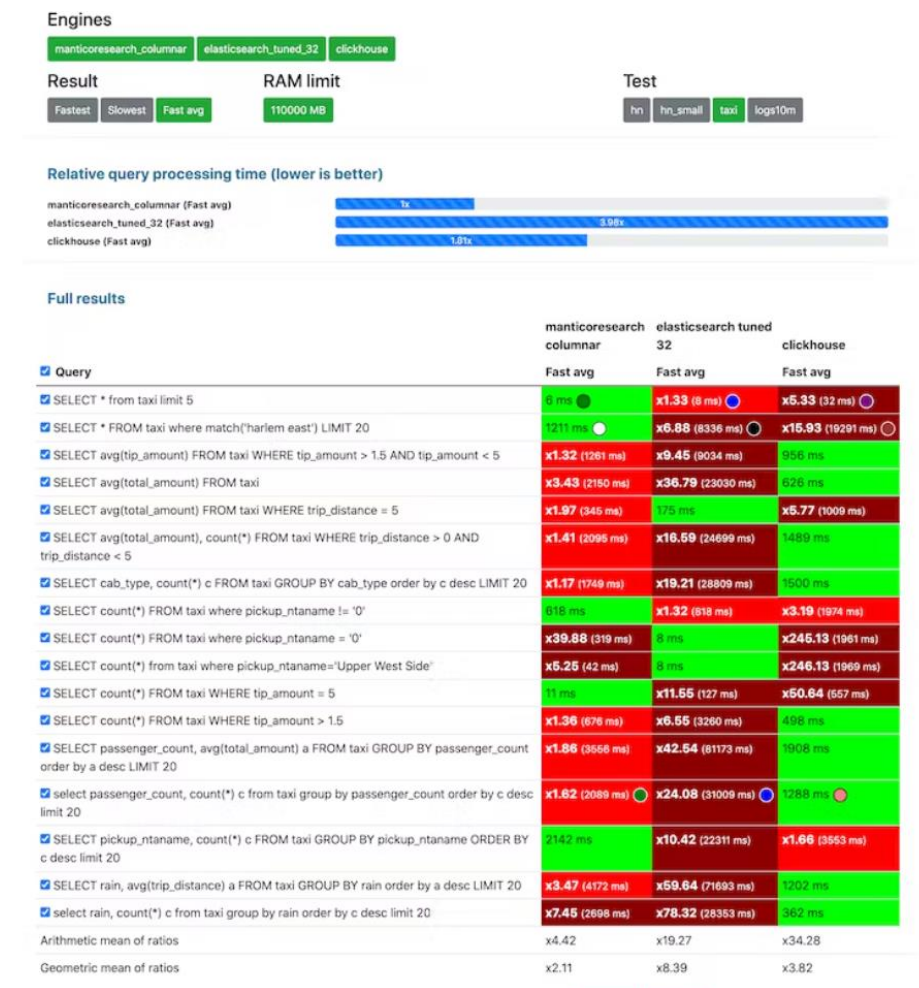


Рис 1. Результаты сравнения баз данных

Заключение

Использование каждой из баз данных предполагает и использование как и положительных, так и отрицательных сторон баз данных, т.е. Manticoresearch, являющаяся форком Sphinx наследует его проблемы. clickHouse – OLAP выигрывает в табличных операциях выборки

Kukunin D.¹, Eliseeva K.¹, Fedotov I.²

¹The Bonch-Bruевич St. Petersburg State University of Telecommunications
²Natural Intelligence

Comparative analysis of modern databases.

With the development of big data and the increase in e-commerce business, traditional relational databases are falling out of use because of slow data retrieval and processing. This paper performs a comparative analysis of queries in modern full-text search databases and OLAP databases.

Key words: *Big-data, e-commerce, Elasticsearch, ManticoreSearch, ClickHouse.*

УДК 621.396.49
ГРНТИ 47.05.17

ИССЛЕДОВАНИЕ ПРОЦЕССА РАСШИРЕНИЯ СПЕКТРА СИГНАЛА В СРЕДЕ МОДЕЛИРОВАНИЯ

Д. С. Кукунин, И. О. Петушков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе исследуются имитационные модели, которые расширяют спектр сигнала с помощью метода прямой последовательности, оценивается эффективность его моделирования и сам процесс расширения.

метод прямой последовательности, широкополосный спектр, моделирование

Предметом нашей работы является создание модели расширения спектра методом DSSS в среде моделирования Simulink программы Matlab.

Simulink – среда динамического моделирования сложных технических систем и основной инструмент для модельно-ориентированного проектирования.

Модель (рис. 1) представляет из себя набор различных блоков подсистем, отвечающих за генерацию случайных целых чисел и псевдослучайных последовательностей (ПСП) [1], модуляцию и демодуляцию сигнала, требуемые математические операции, вывод исследуемых сигналов, эта же система тестируется в канале с аддитивным белым гауссовским шумом (AWGN) [2].

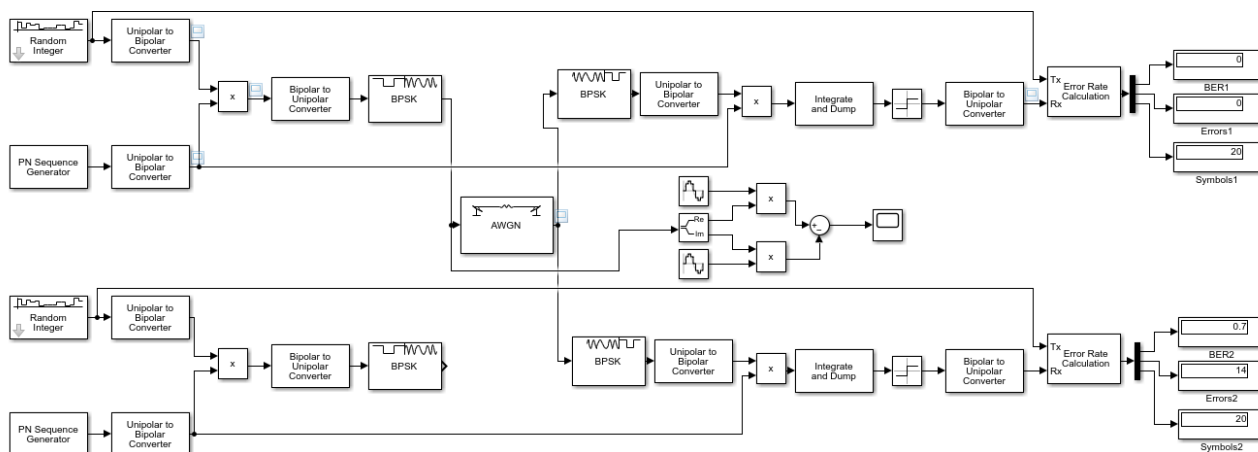


Рис. 1. Модель Matlab Simulink DSSS системы

Также для корректного отображения сигналов, следует уменьшить время симуляции до 0,02 и выставить время выборки на генераторах 1/32000 [3].

В ходе исследования данной модели на выходе генератора ПСП получаем последовательность двоичных чисел с помощью регистра сдвига с линейной обратной связью (LFSR) (рис. 2).

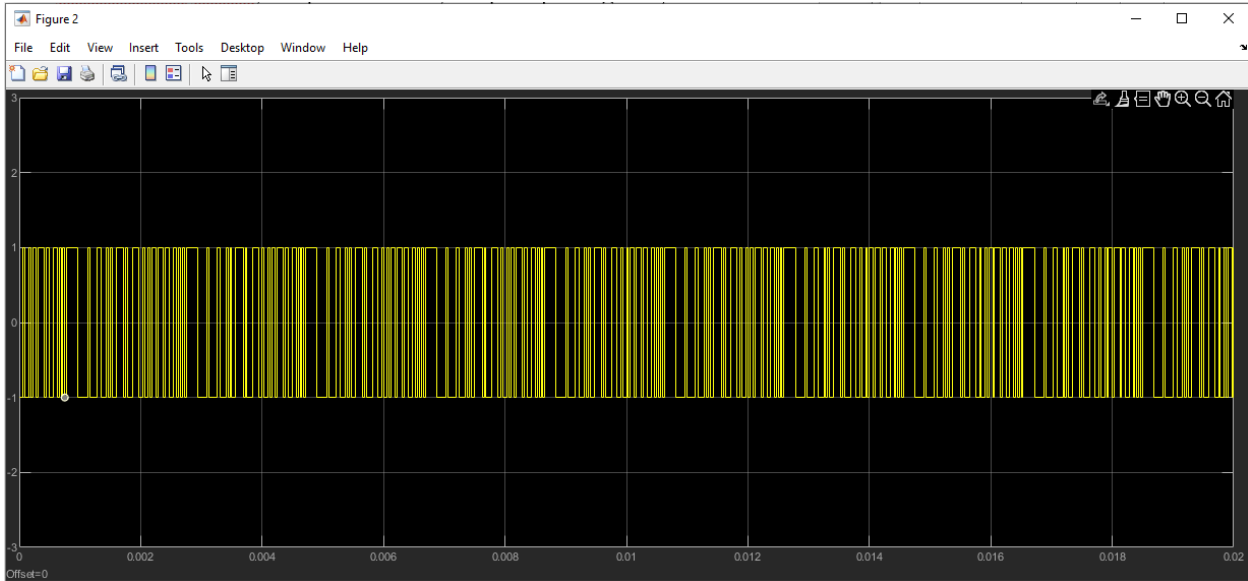


Рис. 2. Случайная полярная последовательность расширения со скоростью 100 кбит/с

Передаваемые данные со скоростью 1 кбит/с применяются к сумматору по модулю 2 с PN-последовательностью для получения данных расширения (рис. 3) [4].

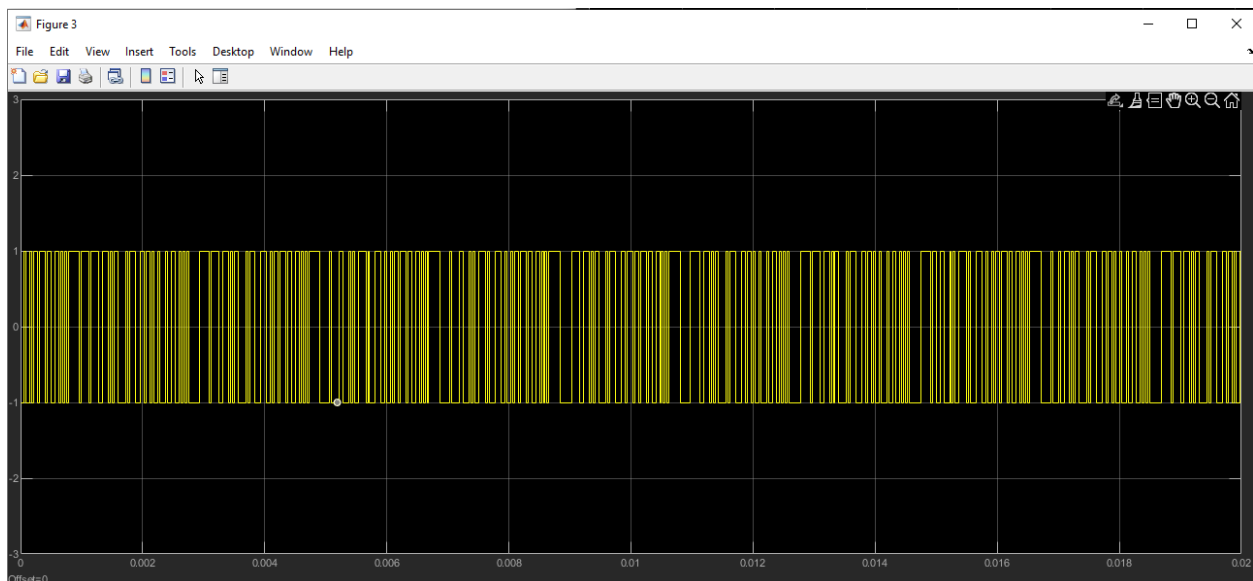


Рис. 3. Последовательность расширения на входе модулятора BPSK

BPSK модулятор преобразует данных расширения из однополярного в биполярный с обратной фазой (0 или 180) в зависимости от входа в BPSK модулятор. На рис. 4 показан передаваемый сигнал с наложением шума AWGN при SNR (отношение сигнал-шум) равном 10 дБ.

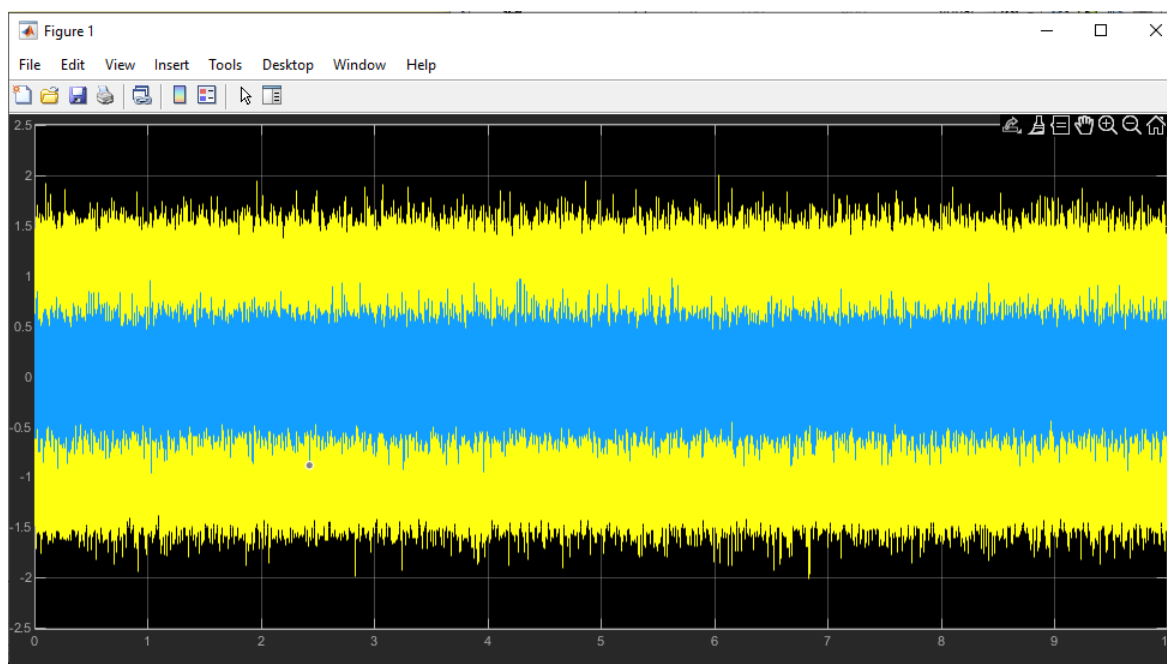


Рис. 4. Форма волны на выходе модулятора BPSK

Если в передатчике используется правильный PN-код, полученные данные от демодулятора BPSK по отношению к переданным данным, выглядят как на рис. 5, где принятая последовательность эквивалентна переданной.

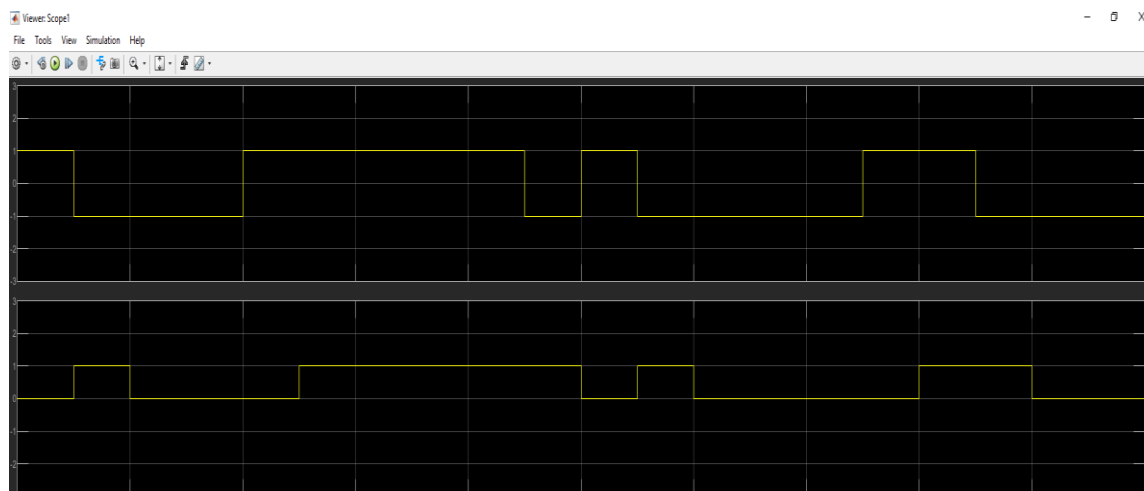


Рис. 5. Форма волны на выходе приемника, эквивалентная переданной последовательности

Благодаря исследованию в среде Simulink мы можем наблюдать процессы изменения сигналов при расширении спектра, влияние аддитивного белого гауссовского шума на сигнал, получение исходного сигнала при снятии шума, что очень удобно.

Вывод: исследования показали, что в программах для модельно-ориентированного проектирования также возможно исследовать расширение спектра сигнала, визуализировать его, что должно упростить работу с

широкополосными сигналами и использованием ПС шума для усложнения перехвата сигнала и уменьшения помех.

Список используемых источников:

1. Donald Schilling, Laurence B. Milstein, Marvin Kullback, Frank Miller “Spread spectrum for commercial applications”, IEEE communication magazine, April 1991.
2. Кукунин, Д.С. Использование фантомных каналов в качестве катализаторов усиления ортогональных свойств М-последовательностей в системе с кодовым разделением каналов: научная статья [Электронный ресурс] / Д.С. Кукунин, А.А. Березкин, Р.В. Киричек // Труды НИИР. – С. 24-25. URL: <https://www.elibrary.ru/item.asp?id=48193108>
3. ‘Wang Ding’, Zhao – Yi-Xuas, “multicarrier sub channel spread spectrum for antijamm communication, industrial conference on industrial control and electronics engineering 2012. 978-0-7695-4792-3/12, 2012 IEEE.
4. Manoj Barnela and Dr. Suresh Kumar,” Digital Modulation Schemes Employed in Wireless Communication: A Literature review”, International Journal of Engineering, Applied and Management Sciences Paradigms, Vol. 14, Issue 01, April 2014

Kukunin D., Petushkov I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

Investigation of a Spectrum Spreading using the Simulation Environment Simulink.

In this research, simulation models are investigated that expand the signal spectrum using the direct sequence method, the efficiency of its modeling and the expansion process itself are evaluated.

Key words: Spread Spectrum, modeling, signal.

УДК. 004.725.5
ГРНТИ 49.33.29

АНАЛИЗ ОСОБЕННОСТЕЙ БЕСПРОВОДНЫХ СЕТЕЙ СВЯЗИ С ВЫСОКОЙ ПЛОТНОСТЬЮ ПОЛЬЗОВАТЕЛЕЙ

Д. А. Лохов, А. И. Парамонов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С каждым годом технологии набирают всё больший оборот, что человек не успевает разобраться в одной, как появляется уже следующая со своими улучшениями и новыми возможностями. В этой статье рассматриваются тенденции развития беспроводных технологий связи: 5G, Интернет вещей, сети высокой плотности и их особенности.

5G, Интернет вещей, сети высокой плотности, беспроводные сети

Введение

Внедрение Интернета практически во все уровни человеческой жизни привело к огромному росту трафика в сетях по всему миру, а это в свою очередь привело к проблемам, связанным с обеспечением требуемого уровня QoS. Плотность устройств постоянно увеличивается и традиционные сети не могут соответствовать требованиям новых стандартов. Так, специалисты в области связи начали разрабатывать новые модели сети. Эти модели являются частью сетей будущего – Интернета вещей и 5G.

Развивающиеся Интернет вещей, а также сети подвижной связи и беспроводного доступа приводят к увеличению количества устройств из расчета на единицу площади. Увеличение плотности устройств приводит, в основном, к возникновению сложностей при обслуживании трафика.

Эти сложности могут проявляться как в росте трафика, общего количества устройств из расчета на одну точку доступа, в снижении отношения сигнал шум или в комплексных проблемах.

Структура сети Интернета вещей обусловлена инфраструктурой города, в частности его застройкой и параметрами строений этой застройки. Влияние городской застройки на структуру сети проявляется не только для сетей Интернета вещей, но и для других сетей беспроводной связи.

Анализ развития беспроводных технологий связи

На сегодняшний день самым основополагающим курсом телекоммуникаций, который заложит базу для дальнейшего развития и создания новых технологий являются сети пятого поколения (5G).

Появление сетей в нашей жизни в дальней перспективе способно изменить мироощущение, а также изменить общество. Это приведет к трансформации экономики сетей: издержки доставки уменьшаться в 30 раз, и в 40 раз увеличится средняя скорость передачи данных.

Ключевые показатели 5G определены в рекомендации 3GPP TR 38.913 [1]:

- пиковая скорость передачи данных на линии вниз — 20 Гбит/с (при спектральной эффективности 30 бит/с/Гц);
- пиковая скорость передачи данных на линии вверх — 10 Гбит/с (при спектральной эффективности 15 бит/с/Гц);
- минимальная задержка в подсистеме радиодоступа для сервисов URLLC — 0,5 мс, для сервисов eMBB — 4 мс;
- максимальная плотность подключенных к сети в городских условиях устройств IoT — 1 млн устройств/кв. км;
- автономная работа устройств IoT без подзарядки аккумулятора в течение 10 лет;
- поддержка мобильности при максимальной скорости передвижения объектов 500 км/ч.

5G нам открывают следующие технологии:

1. Потокоевое видео (4K- и 8K-видео)
2. Виртуальная и дополненная реальности
3. Тактильный Интернет
4. БПЛА (новое применение дронов)
5. Инфраструктура C-V2X [2]

Сети 5G могут стать технологией с самым быстрым развитием в истории мобильной связи. Главные бустеры роста — повышенный спрос на услуги в Китае и Северной Америке, он подогревается снижением цен на устройства пятого поколения. Об этом говорит статистика третьего квартала 2021 года, а именно появление 98 млн новых 5G-подключений и 48 млн новых подключений в сетях четвертого поколения. Таким образом, в 2027 году в зоне обслуживания 5G сетей будет жить 75% мирового населения. Порядка 50% мобильных подключений и 62% мирового трафика смартфонов будет приходиться на сети 5G [3].

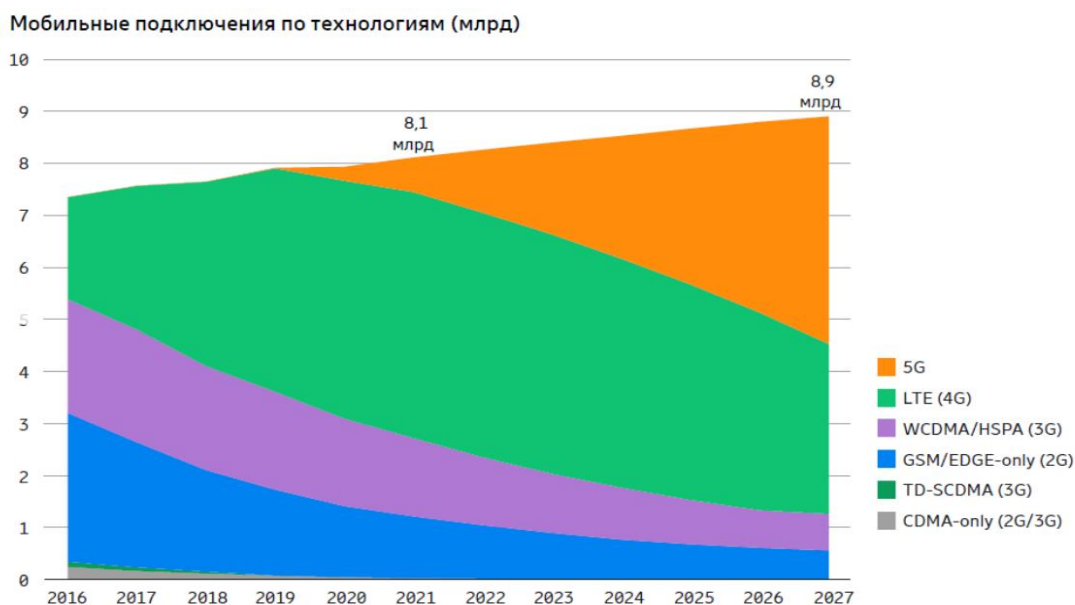
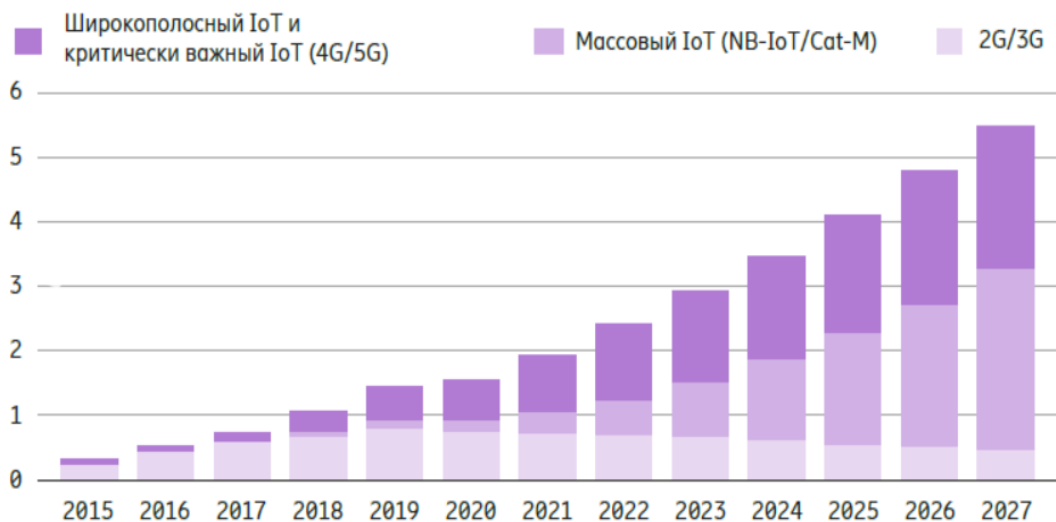


Рис. 1.1. Мобильные подключения по технологиям

Основными технологическими факторами, определяющими развитие IoT являются:

- обилие миниатюрных и дешевых сенсоров, контроллеров и передатчиков, позволяющих обеспечить экономичный процесс сбора различных данных;
- рост пропускной способности и всеобщее проникновение сетей, а также огромное увеличение IP-адресов, способствующее вовлечению в Интернет вещей новых устройств и участников;
- значительное снижение стоимости хранения и управления данными, определявшей на протяжении многих лет расходы на ИТ;
- появление мощных аналитических инструментов, которые позволяют управлять накопленными объемами данных в режиме, близком к реальному времени [4].

Бурно развивающийся интернет вещей (IoT) вносит весомый вклад в трафик. Самая большая часть IoT — устройства, которые подключены к широкополосному интернету. По прогнозам к концу 2021 года в секторе IoT доля широкополосного интернета должна была составлять 47%, доля 2G/3G — 37%, а доля технологий массового IoT (Massive IoT) — 16%.



Примечание: График показывает доступность функциональностей сети и наличие поддержки в устройствах.

Рис. 1.2. Мобильные IoT-подключения по секторам и технологиям

Особенности сетей ИВ и сетей с высокой плотностью устройств

Международный союз электросвязи определили в рекомендации МСЭ-Т У.2060 [5], что Интернет Вещей должен иметь следующие характеристики:

1. Связность

Каждый объект или вещь должен быть способен быть связанным с глобальной информационной инфраструктурой.

Условие связности сети при высокой плотности сети (1 устройство на 1 квадратный метр и радиусом около 10 метров) будет выполняться для сетей почти любого масштаба.

2. Обеспечение вещей услугами

ИВ отвечает за то, чтобы у любой вещи должны быть предоставлены услуги, которые относятся к ней, без каких-либо ограничений. Для этого ИВ должен использовать все свои возможности физического и информационного мира.

3. Гетерогенность

Не так давно произошла смена на гетерогенные конвергентные сети телефонной сети связи общего пользования (ТфОП), до этого они были гомогенными сетями. Устройства ИВ тоже могут быть гетерогенными, построенные на разных аппаратных, программных платформах и сетях. Такие устройства должны быть способны через различные сети взаимодействовать с другими устройствами или платформами услуг. Для этого нужно обеспечить совместимость технических средств, услуг, классов и параметров качества обслуживания в сетях, которые поддерживают Интернет Вещей.

4. Динамические изменения

Каждое современное устройство имеет ряд атрибутов:

- Статус, то есть спящее или активное устройство, связанное с сетью или изолированное;
- Число;
- Местоположение;

- Скорость и др.

Все эти атрибуты могут изменяться в зависимости от времени. Эта характеристика ИВ является фундаментом для требований о самоорганизации сети. Постепенное развитие Интернета Вещей изменит параметры трафика сети, а значит изменяться и требования к объему ресурсов сетей связи. Число вещей, которые могут быть подключены к сети, это показатель развития Интернета вещей, в отличии от развития Интернета [6].

Выводы:

Сети 5G будут с очень высокой плотностью устройств, которая будет только увеличиваться. Будут создаваться новые технологии, а значит и новые требования к сетям.

По разным оценкам и прогнозам интенсивность роста и количество Интернет Вещей будет стремительно увеличиваться и сильно будет превышать количество людей и абонентских терминалов. Одно устройство на один метр квадратный, именно такую высокую плотность стоит ожидать в ближайшее время.

Список используемых источников:

1. 3GPP TR 38.913 V0.4.0 (2016-06) «Study on scenarios and requirements for next generation access technologies», June 2016.
2. Батуев Батор «Технология 5G: поэтапное внедрение и элементная база для абонентского оборудования» // Журнал «Беспроводные технологии» апрель, 2019 (Дата обращения 10.11.2022)
3. Ericsson Mobility Report, November 2021.
4. «Интернет вещей: перспективы развития, создание инфраструктуры, обеспечение безопасности» Журнал «Рациональное Управление Предприятием» 04/2015.
5. Рекомендация МСЭ-Т Y.2060 (06/2012) «Сети последующих поколений – Структура и функциональные модели архитектуры», Июнь, 2012.
6. ТРУДЫ МФТИ. — 2013. — Том 5, № 3 В. Н. Бондарик, А. Е. Кучерявый Московский физико-технический институт (государственный университет) «Прогнозирование развития Интернета вещей на горизонте планирования до 2030 года».
7. Тонких Е.В. «Анализ беспроводной сети интернета вещей высокой плотности.» / Е.В. Тонких, А.И. Парамонов, А.Е. Кучерявый // М. Электросвязь – №1, 2020 – с.51-55.

Lokhov D., Paramonov A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of the features of wireless communication networks with high user density.

Every year, technologies are gaining more and more momentum, so that a person does not have time to figure out one, as the next one appears with its own improvements and new features. This article discusses the trends in the development of wireless communication technologies: 5G, the Internet of Things, high-density networks and their features.

Key words: 5G, Internet of Things, high-density networks, wireless networks.

УДК 004.7
ГРНТИ 49.33.29

АНАЛИЗ И ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ «УМНОГО ДОМА» ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ ТУМАННЫХ ВЫЧИСЛЕНИЙ

Е. С. Машошин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире всё чаще используются облачные сервисы и технологии, но нагрузка на них растёт, что может приводить к задержкам и ошибкам. Для того, чтобы избежать данную проблему, была разработана технология туманных вычислений.

информационные технологии, интернет вещей, облачные технологии, туманные вычисления, облачные сервисы, туманные вычисления, «умный дом»

Развитие современных IT технологий проходит довольно интенсивным темпом. Со временем повышается сложность задач, которые решаются с помощью IT технологий и инфокоммуникационных систем. При развитии информационных технологий меняются также способы и инструменты их взаимодействия с обществом.

Главные черты современных информационных систем:

- Возможность передачи данных на любые расстояния
- Скорость передачи данных
- Компьютерная обработка информации
- Возможность интеграции различных информационных технологий между собой
- Широкое использование компьютеризированного хранения и предоставления информации по мере необходимости

На сегодняшний день информационные технологии способны сделать неоценимый вклад для установки взаимосвязи роста производительности труда, инвестиций и объемов производства.

Благодаря эволюционному развитию IT технологий в течение последних нескольких десятилетий появились новые облачные сервисы, отвечающие потребностям современного бизнеса. Благодаря активному использованию данных технологий, стало возможным оптимизировать вычислительные ресурсы и сосредоточить внимание на вопросах управления бизнесом.

Туманные вычисления – это передовая концепция облачной архитектуры, которая предполагает, что данные будут обрабатываться на периферийных устройствах сети – персональных компьютерах, смартфонах и т.д., выводя их из облака [1].

Любое здание, вне зависимости от назначения, состоит из набора подсистем, каждая из которых отвечает за выполнение определённых функций, которые позволяют этому зданию нормально функционировать. Чем сложнее подсистема, тем сложнее её обслуживание, тем больше требуется средств и персонала для обслуживания каждой подсистемы, ремонт и наблюдения за

работоспособностью. Помочь решить данные проблемы может технология «Умного дома».

Современный «Умный дом» позволяет без участия человека выполнять контроль над работой подсистем, таких как включение и выключение света, регулировка отопления и кондиционера, пожарная сигнализация, контроль за входом и выходом. «Умный дом» рассматривают как частный случай интернета вещей, он связывает доступные через интернет домашние устройства.

Туманные вычисления — это расширение облачных вычислений, состоящее из нескольких пограничных узлов, непосредственно подключенных к физическим устройствам.

Такие узлы физически гораздо ближе к устройствам по сравнению с централизованными центрами обработки данных, поэтому они способны обеспечивать мгновенные соединения. Значительная вычислительная мощность периферийных узлов позволяет им самостоятельно выполнять вычисления большого объема данных, не отправляя их на удаленный сервер.

Туманные вычисления также включают в себя облачные вычисления – небольшие и довольно мощные центры обработки данных, расположенные в пограничном сегменте сети. Их цель - поддерживать ресурсоемкие приложения Интернета вещей, требующие низкой задержки.

Основное различие между туманными и облачными вычислениями заключается в том, что облако — это централизованная система, в то время как туман — это распределенная децентрализованная инфраструктура.

Туман является посредником между оборудованием и удаленными серверами. Туманные вычисления определяют, какая информация будет отправлена на сервер, а какая информация может быть отредактирована локально. Таким образом, туман — это интеллектуальный шлюз, который разгружает облака, обеспечивая более эффективную обработку и анализ данных.

Следует отметить, что туманная сеть не является отдельной архитектурой и не заменяет облачные вычисления, а скорее дополняет их, максимально приближая к источнику информации.

Как и просто облачные вычисления, применение технологии туманных вычислений имеет ряд своих преимуществ и недостатков.

Преимущества туманных вычислений:

Подход затуманивания имеет много преимуществ для Интернета вещей, больших данных и аналитики в реальном времени. Вот основные преимущества туманных вычислений перед облачными вычислениями:

Передача данных в режиме реального времени [2] - «Туман» находится ближе к пользователю, поэтому время на обработку и передачу информации снижается.

Низкое время отклика [3] связано с тем, что туман географически ближе к пользователям и способен обеспечить мгновенный ответ.

Нет проблем с пропускной способностью - часть информации агрегируется в разных точках, а не отправляется в один центр по одному каналу.

Невозможность потери соединения обеспечивается множеством подключенных каналов.

Высокий уровень безопасности - данные обрабатываются огромным количеством узлов в сложной распределенной системе.

Энергоэффективность – в периферийных узлах используются протоколы высокой эффективности, такие как Bluetooth, Zigbee.



Рис 1. Устройство Интернета вещей

Одной из самых серьезных проблем, с которыми продолжают сталкиваться умные дома, является огромное количество информации, генерируемой, собираемой и анализируемой каждый день. В сочетании с постоянно растущим числом устройств автоматизации Интернета Вещей объем собранных данных становится непосильным для управления и отслеживания, что требует больших вычислительных ресурсов для их обработки. Передача этого невероятно большого объема данных между облаком и источниками данных также требует много времени и затрат.

Туманные вычисления позволяют сократить объем данных, которые необходимо отправлять в облако для обработки, тем самым повышая эффективность [4]. Умные дома могут увидеть следующие преимущества благодаря туманным вычислениям:

Минимизация объема данных, отправляемых в облако

Главная цель туманных вычислений - сделать большие данные меньше и более управляемыми. Согласно прогнозу IDC на 2019 год, объем данных, собираемых подключенными устройствами, к 2025 году превысит 79 зеттабайт. Туманные вычисления способны сократить этот огромный объем данных за счет применения интеллектуального зондирования и фильтрации, которые позволяют

передавать только полезную информацию, основанную на знаниях, доступных локально на данном устройстве.

Низкая задержка передачи данных

Узлы туманных вычислений способны обрабатывать и загружать данные, не отправляя их на удаленные облачные серверы и не возвращая результаты обратно. Это позволяет значительно экономить время при передаче данных и получать ответы в режиме реального времени. Немедленная обработка данных станет только более важной для систем "умного дома", особенно когда решения или действия необходимо принимать быстро: например, при возникновении пожара очень важно передать сигнал об этом с минимальной задержкой.

Уменьшенная пропускная способность

Для передачи и обработки данных требуется огромная пропускная способность, которая может быть ограничена в случае облачных вычислений. Однако это не является проблемой, когда дело доходит до туманных вычислений, поскольку все данные распределяются между локальными устройствами и не передаются по беспроводной сети. Это позволяет значительно снизить потребление пропускной способности сети.

Повышенная безопасность данных

Безопасность данных - еще один важный фактор, заставляющий "умные дома" переключать свои ресурсы на облачные вычисления. Он сохраняет более конфиденциальные и конфиденциальные данные вне досягаемости уязвимых общедоступных сетей, тем самым предотвращая легкий доступ к ним любых киберпреступников. Туманные вычисления позволяют обнаруживать вредоносные программы и зараженные файлы на ранней стадии их цикла на уровне устройства задолго до того, как у них появится возможность заразить всю сеть.

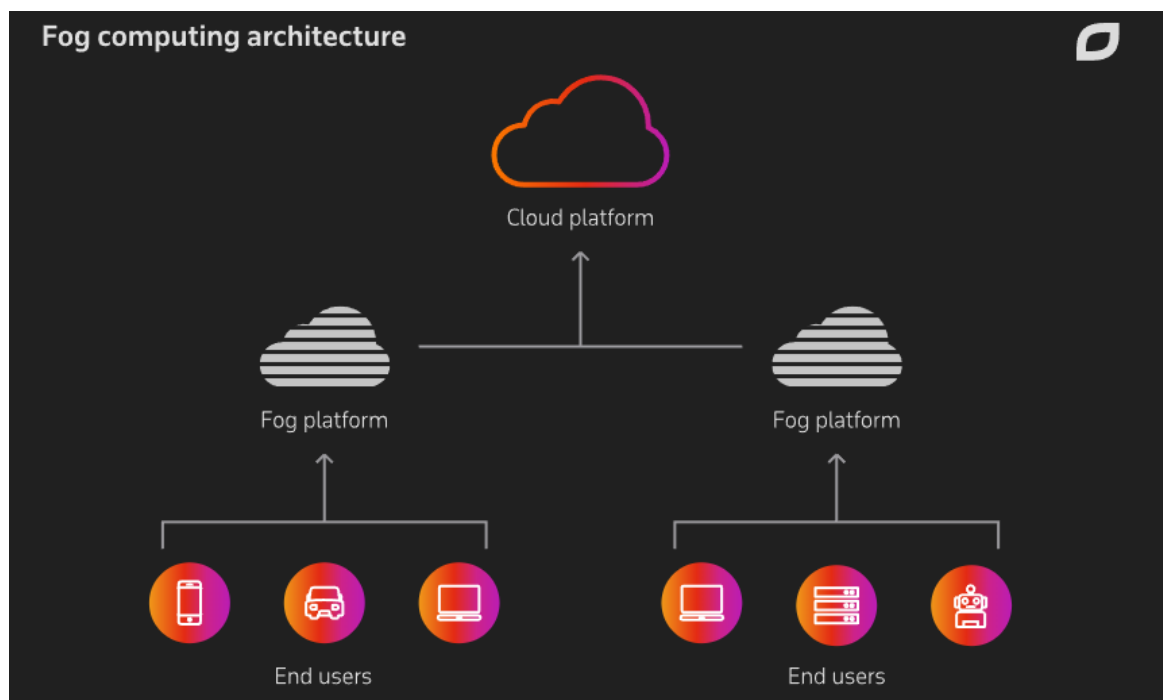


Рис 2. Архитектура туманных вычислений для «Умного дома»

В заключении отметим, что туманные вычисления, использованных в

технологии «Умного дома», смогут значительно ускорить работу умных устройств, благодаря тому что информация будет обрабатываться не в облаке на удалённом сервере, а в непосредственной близости к самому устройству. Также технология туманных вычислений позволит снизить нагрузку на облако, позволив тому обрабатывать только необходимые данные.

Список используемых источников:

1. Облачные, туманные и граничные вычисления: отличия и перспективы развития технологий [Электронный ресурс]. URL: <https://www.thefastcode.com/ru-rub/article/what-is-fog-computing> (дата обращения 12.11.2022).
2. Облачные, туманные и граничные вычисления: отличия и перспективы развития технологий [Электронный ресурс]. URL: <https://rb.ru/story/edge-computing/> (дата обращения 12.11.2022).
3. Сравнение облачных и туманных вычислений для создания проектов интернета вещей [Электронный ресурс]. URL: <https://oncloud.ru/blog/2019/06/05/oblachnye-i-tumannye-vychisleniya-dlya-IoT> (дата обращения 12.11.2022).
4. Общие принципы туманных вычислений [Электронный ресурс], <https://protei.ru>, 2010. URL: https://protei.ru/sites/default/files/media/2019-09LM_2_2018.pdf. (Дата обращения: 12.11.2022).

Mashoshin E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

Analysis and use of smart home capabilities to provide services using fog computing technology.

In the modern world, cloud services and technologies are increasingly used, but the load on them is growing, which can lead to delays and errors. In order to avoid this problem, the technology of fog computing was developed.

Key words: information technologies, internet of things, cloud technologies, fog computing, fog computing, cloud services, smart house.

УДК 004.056.55
ГРНТИ 49.33.35

ИСПОЛЬЗОВАНИЕ АССИМЕТРИЧНОЙ СИСТЕМЫ ШИФРОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ В СЕТИ WEB 3.0

В. Д. Минеева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается система асимметричного шифрования, которая применяется в основном для использования криптовалюты. При этом данный метод можно использовать для защиты информации при ее передаче для реализации сети третьего поколения WEB.

WEB 3.0, цифровая подпись, асимметричная система шифрования, криптография с открытым ключом

Реализация WEB 3.0 предполагает использование серверной и клиентских составляющих для корректной работы сети, а также для использования сервисов, таких как децентрализованные браузеры и системы децентрализованных финансов DeFi. При этом пользовательский запрос обрабатывается интегрированной блокчейн сетью. Для осуществления данного процесса принято использовать цифровую подпись и метод транзакций, так как данные открыты и могут быть прочитаны кем угодно. Отправка транзакции подтверждает, обновленные данные были внесены в определенный блокчейн, но для ее отправки обязательно требуется цифровая подпись инициатора транзакции.

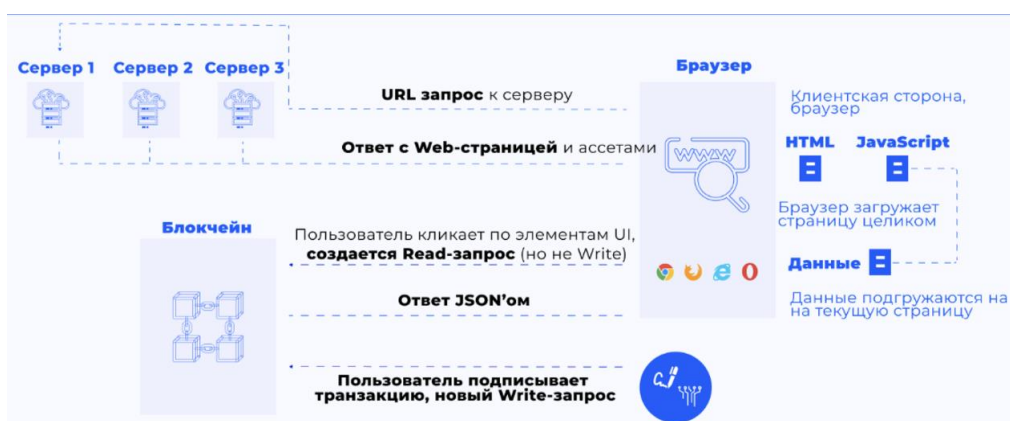


Рис. 1. Реализация пользовательского запроса в сети WEB 3.0

Реализация цифровой подписи в сети WEB 3.0 предполагает использование метода асимметричного шифрования. Криптография с открытым ключом направлена на создание двух ключей - приватного и публичного, описанных математической зависимостью, исходя из которой каждый публичный ключ

имеет только один приватный и наоборот. Созданная транзакция подписывается с помощью приватного ключа, который доступен только пользователю. Для валидации транзакции любой другой пользователь, который знает публичный ключ может удостовериться, что созданная транзакция, подписана его приватным ключом, а значит создана именно им.



Рис. 2. Процесс создания цифровой подписи с приватным и публичным ключом

Использование хэш-функций позволяет генерировать приватный ключ из случайной seed-фразы (seed phrase). Для генерации seed phrase необходимо 256 битное число. Путем умножения приватного ключа умножения на одну из точек эллиптической кривой можно также создать публичный ключ, из которого в дальнейшем генерируется сетевой адрес. Соответственно данный вид трансформации ключей является однонаправленным. Обратное преобразование является затруднительным поскольку требует 2^{256} вычислительных операций.

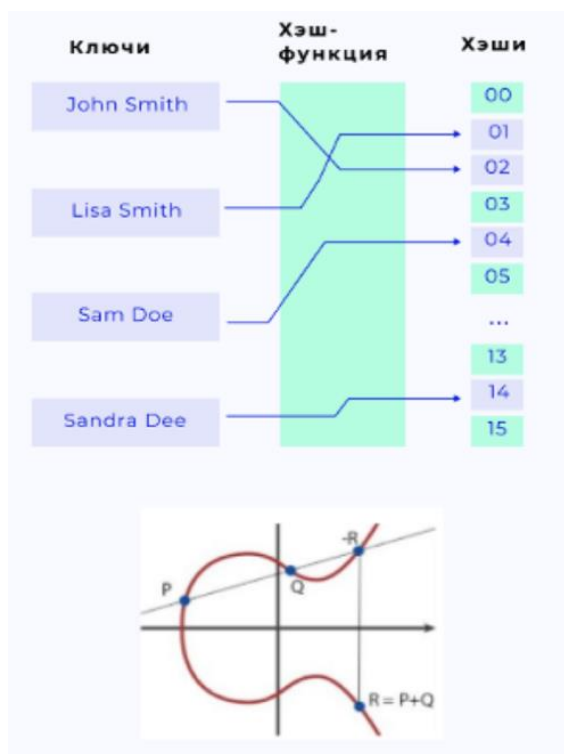


Рис. 3. Генерация публичного и приватного ключей

Хранение приватных ключей, seed-фразы, а также активов пользователя может быть реализовано с помощью программно-аппаратного комплекса. Одним из примеров такого комплекса может стать Ledger.

Ledger Nano — это аппаратный кошелёк, который генерирует приватные ключи в офлайн-среде, то есть за пределами интернета. Он полностью изолирован от интернет-подключения. Соответственно аппаратные устройства Ledger генерируют фразу восстановления непосредственно на устройстве, что также дает возможность внедрения двухфакторной аутентификации при проведении транзакции. Это значит, что для каждого перевода требуется подтверждение непосредственно с помощью устройства, на котором хранятся все данные пользователя.

Ledger Live — наше нативное приложение, которое работает в паре с устройствами Nano. Аппаратный кошелёк Ledger Nano отвечает за безопасность крипто активов. Приложение Ledger Live же позволяет контролировать происходящее с собственными крипто активами и легко управлять ими.

Заключение

В ходе анализа теоретических материалов об обеспечении безопасности передачи данных в сети WEB 3.0 были сделаны выводы о том, что на данный момент реализация хранения и передачи данных затрагивает только криптовалюту и цифровую экономику. Соответственно обеспечение безопасности передачи данных касается реализации безопасной отправки и получение транзакций внутри крипто экосистемы. Безопасное движение крипто финансов происходит благодаря использованию асимметричной системы шифрования, которая позволяет предоставлять публичный ключ всем пользователям в сети для отправки данных и приватный для сохранения пользовательских данных о конкретном крипто активе. При использовании онлайн кошелька генерирование seed-фразы происходит в онлайн-среде. Это означает компрометацию средств пользователя с первой секунды взаимодействия с кошельком. В связи с этим в настоящее время реализацией криптографии с открытым ключом на уровне аппаратного обеспечения активно занимаются крупные компании как Ledger, так как хранение приватных ключей, seed-фразы офлайн является более безопасным способом для пользователя.

Список используемых источников:

1. Спиридонов А.А., Филиппов Н.С., Додонова Н.Л. ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ АЛГОРИТМА АСИНХРОННОГО ШИФРОВАНИЯ ЭЛЬ-ГАМАЛЯ И ЕГО РЕАЛИЗАЦИЯ ДЛЯ ОБМЕНА СООБЩЕНИЯМИ // МОЛОДЕЖНЫЙ НАУЧНЫЙ ФОРУМ: ТЕХНИЧЕСКИЕ И МАТЕМАТИЧЕСКИЕ НАУКИ . - 2016. - №5(34). - С. 80-89.
2. Долова А.А., Константиныди А.Ю. ШИФРОВАНИЕ ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ // ПОЛИТЕХНИЧЕСКИЙ МОЛОДЕЖНЫЙ ЖУРНАЛ . - 2019. - №5(34). - С. 3.
3. Данилов И.А., Долотов П.С. ПРИМЕНЕНИЕ АСИНХРОННЫХ СХЕМ ДЛЯ ПОВЫШЕНИЯ ЗАЩИТЫ ОТ АТАК ПО СТОРОННИМ КАНАЛАМ // БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ . - 2022. - №2. - С. 112-127.

Mineeva V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Using an asymmetric encryption system to ensure secure data transmission on the WEB 3.0 network.

The article discusses the system of asymmetric encryption, which is used mainly for the use of cryptocurrencies. At the same time, this method can be used to protect information during its transmission for the implementation of a third-generation WEB network.

Key words: WEB 3.0, digital signature, asymmetric encryption system, public key cryptography.

УДК 004.85
ГРНТИ 28.23.29

АРХИТЕКТУРА ПРЕДОСТАВЛЕНИЯ СИСТЕМЫ УСЛУГ ТЕЛЕПРИСУТСТВИЯ И СФЕРЫ ПРИМЕНЕНИЯ ТАКТИЛЬНОГО ИНТЕРНЕТА В РОБОТИЗИРОВАННЫХ СИСТЕМАХ

А. С. А. Мутханна, М. Д. Леонова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Тактильный интернет является одной из важнейших частей эволюции сетей связи и представляет собой взаимодействие человека и машины на уровне ощущений. Такими ощущениями могут быть: прикосновения, визуальные и слуховые эффекты. С началом революции искусственного интеллекта мы можем наблюдать широкий спектр применения робототехники. Интеллектуальные роботизированные системы применяются повсеместно. Телеприсутствие — это идея присутствия в удаленном месте виртуально или с помощью роботов-аватаров. Аналогично, идея управления роботом из удаленного места для выполнения различных задач называется телеоперацией. Всё это влечёт за собой потребность в обеспечении высокой доступности, надежности, безопасности, а также задержек, не превышающих уровень 1000 мкс.

тактильный интернет (ТИ), роботизированные системы, искусственный интеллект (ИИ), услуги телеприсутствия, приложения роботизированных систем, H2M, требования к тактильным сетям, режимы работы роботизированных систем, архитектура услуг телеприсутствия, робот-аватар, робототехника

Определение роботизированных систем

Роботизированные манипуляторы, в общем своём понимании, представляют собой устройства, запрограммированные на выполнение четко поставленных задач быстро, эффективно и исключительно точно.

Требования к сетям

Требования реального времени составляют основную часть успеха, когда речь идет о роботах, представляющих человека в удаленном месте. Постоянная связь между человеком и роботом просто необходима. Критические по времени задачи, такие как аудиовизуальная передача между пользователем и роботом, навигационные инструкции и команды взаимодействия (такие как речь и визуальные сигналы), требуют надежного протокола связи с низкой задержкой (по UDP) на прикладном уровне. В случае передачи визуальных данных со стороны пользователя на сторону робота, иногда видео может быть передано неправильно и не полностью, если пропускная способность и мощность сети низкая.

Поэтому требуются более низкие задержки и максимальная надежность, уже сложились представления о некотором разделении этих пониманий, которые представлены в таблице 1, где представлен сравнительный анализ требований приложений [1].

ТАБЛИЦА 1. Требование к сетям приложений для реализации ТИ

Тип приложения	Задержки (мс)	Надёжность (%)	Скорость передачи данных	Размер передачи информации нагрузки	Плотность передачи данных	Плотность абонентов	Область обслуживания (м)
Тактильные взаимодействия	0,5	99,999	мал.	мал.	мал.	мал.	любая 1
Удалённое управление	50	99,9999	1-100 Мбит/с	любой	100 Гбит/км ²	1000 км ²	300x300x50
Мониторинг	50	99,9	1 Мбит/с	мал.	10 Гбит/км ²	10 000 км ²	300x300x50
Смарт транспорт	10	99,9999	10 Мбит/с	любой	10 Гбит/км ²	1 000 км ²	2 км вдоль дороги

Режимы работы: автоматический и мануальный (ручной) и обобщенная архитектура услуг телеприсутствия

Телероботы могут работать в двух режимах - ручном и автоматическом. В ручном режиме робот выполняет точные инструкции пользователя в удаленном месте, будь то навигация, планирование пути, выбор и размещение, следование за кем-то и т. д. В автоматическом режиме робот выполняет почти все действия с помощью собственного интеллекта и возможностей. В ручном режиме пользователь полностью контролирует робота и его действия, но основной проблемой является окружающая среда.

Иногда восприятие пользователем удаленной среды может быть ошибочным или неправильным, что может привести к нежелательным действиям робота. Например, расстояние от робота до человека в ситуации может быть неверно оценено пользователем, в результате чего робот может столкнуться с ним. В автономном режиме полный контроль находится у робота, он воспринимает окружающую среду и действует в соответствии со своим интеллектом. Но проблема заключается в том, что, если какой-либо модуль выходит из строя это может привести к нежелательному поведению робота, вплоть до причинения вреда людям в сцене.

Кроме того, в ручном режиме, если возникнут проблемы с сетью связи, команда пользователя может быть передана роботу ненадежно. Поэтому последние исследования сосредоточены на логике совместной автономии, где робот не является полностью автоматическим, а пользователь может выбирать между ручным и автоматическим режимами в зависимости от ситуации. Такая

гибридная модальность может улучшить опыт пользователя, а также восприятие роботов с точки зрения зрителей [2].

На рис. 1 показана целостная архитектура обобщённой системы телеприсутствия и телеоперации с когнитивными возможностями, которая ориентируется на граничных вычислениях [3]. Робот-аватар, как говорилось ранее, может управляться в двух режимах – ручном и автоматическом. В случае удаленной навигации пользователь может выбрать и изменить свой режим в любое время использования. Выбранный режим сохраняется на граничном устройстве, который запускает выбранный модуль управления навигацией устройства.

Пользователь отправляет команду роботу-аватару только тогда, когда он получает подтверждение, что предыдущая команда завершила выполнение и робот-аватар подключен к граничным вычислениям. В нашей системе телеприсутствия два аспекта: манёвренность робота и мультимедийная коммуникация поддерживаются параллельно и синхронизировано.

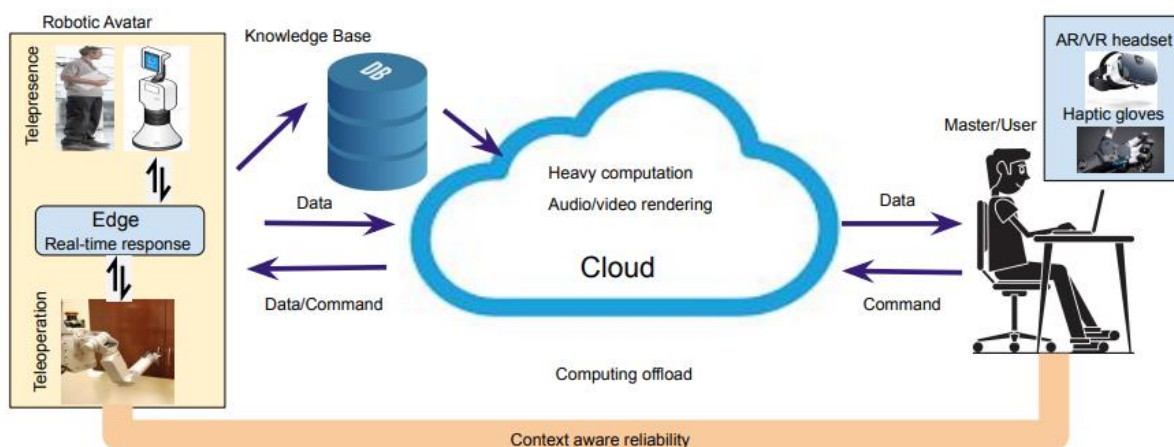


Рис. 1. Архитектура предоставления системы услуг телеприсутствия

Область применения

Интеллектуальные роботизированные системы применяются как в промышленности, так и в быту. Роботизированное телеприсутствие или телеоперация может оказать огромное влияние на модернизацию общества.

1. Применение в гибких удаленных совещаниях или конференциях: сегодня мы участвуем в совещаниях из разных географических точек, используя систему аудио- и видеоконференций. Но роботизированное решение делает их более интерактивными, используя когнитивные возможности. Это также сокращает расходы на транспорт, питание и проживание во время конференций за рубежом.

2. Медицинские роботы — это результат междисциплинарных усилий по автоматизации здравоохранения. Основной целью использования робототехники в медицине являются следующее:

1) Имплантирование чипов людям с болезнями мозга, а также животных с целью отслеживания и обработки биометрических данных.

2) Подключение роботизированных устройств-конечностей людям с ограниченными возможностями.

3) Выполнение операций высокого уровня в микроскопическом масштабе.

4) Дистанционный анализ и рекомендации по улучшению здоровья пациента.

Решение для дистанционного телеинспектирования в больницах — это следующая большая вещь. Робот может не участвовать в критических операциях в последнее время, но он может обеспечить живое руководство от удаленного врача, когда роботизированный аватар присутствует в операционной. Также он может быть использован для удаленного осмотра врачом (который физически не присутствует в удаленном месте) в различных медицинских центрах в сельской местности.

3. Особая роль в деле обеспечения национальной безопасности и обороны. Вооруженные силы, оснащенные перспективными типами и образцами робототехнических комплексов завтрашнего дня, будут обладать неоспоримым интеллектуально-технологическим превосходством над противником. Они увеличивают возможности стратегической тактики и обороны, используя автономных роботов обороны с искусственным интеллектом и роботов разведчиков с высокой маневренностью.

4. Изучение пород космоса и различных ресурсов на нашей планете: аватары могут работать в многокилометровых глубинах океана в подводных предприятиях по добыче природных ресурсов (нефть, газ, редкие металлы и т. д.), будут работать в местах ликвидации последствий стихийных бедствий и технических катастроф, в местах с крайне низкими и высокими температурами, высоким радиационным фоном, в условиях химического заражения. В будущем аватары позволят людям без риска исследовать планеты, астероиды.

5. Телеобразование в школах или университетах: роботизированное решение откроет новую эру в телеобразовании, представляя специализированного преподавателя дистанционно, например, в неблагополучных районах, где его присутствие не может реализоваться физически.

6. Удаленное теленаблюдение: архитектура телеприсутствия может быть реализована и с помощью беспилотника, который будет использоваться полицией для удаленного мониторинга и инспекции в районах, подверженных преступности.

7. В сфере культуры могут тоже применяться такие технологии: дистанционный гид в библиотеках — роботизированный аватар может перемещаться по книжным стеллажам и записывать существующие названия от имени человека, чтобы сократить его усилия и время.

Заключение

Реализация роботизированных систем в тактильном интернете включает в себя приложения из различных областей: робототехника, электроника, виртуальная реальность, дополненная реальность, искусственный интеллект, здравоохранение и другие. Были рассмотрены роботизированные системы в их

общем понимании, какие предъявляются требования к сетям для реализации таких технологий, описаны автоматический и мануальный режимы работы, а также приведён обзор области повсеместного применения. И несмотря на всю прогрессивность технологий, все еще остаются вопросы об их зрелости, надежности и безопасности.

Список используемых источников:

1 Кузнецов К. А., Мутханна А. С. А., Кучерявый А. Е. Тактильный Интернет и его приложения // Информационные технологии и телекоммуникации. 2019. Том 7. № 2.

С. 12–20. DOI 10.31854/2307-1303-2019-7-2-12-20.

2. A Perspective on Robotic Telepresence and Teleoperation using Cognition: Are we there yet? // arXiv URL: <https://arxiv.org/ftp/arxiv/papers/2203/2203.02959.pdf> (дата обращения: 10.11.2022).

3. A. Sau, R.D. Edge-centric telepresence avatar robot for geographically distributed environment, / A. Sau, R.D. Roychoudhury, H.B. Barua, C. Sarkar, S. Paul, B. Bhowmick, A. Pal // 2020, arXiv preprint arXiv:2007.12990

Leonova M., Muthanna A.S.A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Architecture of telepresence service delivery system and application areas of tactile internet in robotic systems.

Haptic Internet is one of the most important parts of the evolution of communication networks and represents the human-machine interaction on the level of sensations. Such sensations can be touch, visual and auditory effects. With the beginning of the artificial intelligence revolution, we can observe a wide range of robotic applications. Intelligent robotic systems are used everywhere. Telepresence is the idea of being present in a remote location virtually or with robotic avatars. Similarly, the idea of controlling a robot from a remote location to perform various tasks is called teleoperation. All this entails the need for high availability, reliability, security, and delays not exceeding 1000 μ s.

Key words: tactile Internet (TI), robotic systems, artificial intelligence (AI), telepresence services, robotic system applications, H2M, requirements for tactile networks, modes of operation of robotic systems, telepresence service architecture, robot avatar, robotics.

УДК 004.7
ГРНТИ 49.33.29

ОПРЕДЕЛЕНИЕ И КЛАССИФИКАЦИЯ НАНОСЕТЕЙ. МОЛЕКУЛЯРНЫЕ НАНОСЕТИ И ИХ ПРИМЕНЕНИЕ. ЭЛЕКТРОМАГНИТНЫЕ НАНОСЕТИ И ИХ ПРИМЕНЕНИЕ.

Е. Д. Никитин, М. А. Харламов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследования в области Интернета Вещей показывают, что число подключенных устройств продолжает расти и доходит до 50 триллионов единиц. Однако, эти прогнозы не учитывают еще одну категорию устройств – нановещей, которые задействованы в наносетях.

IoT, IoNT, наносети, электромагнитные наносети, молекулярные наносети

Исследования по развитию в области концепции Интернета Вещей [1] показывают, что число Интернета Вещей может составлять до 50 триллионов единиц [2]. Кроме того, отмечается, что составляющие этой концепции – «вещи», подразделяются на физические и виртуальные (вещи информационного мира) [3], а в плане приложений – персональные и автономные вещи, вещи специального назначения, летающие вещи и т.д. Однако эти прогнозы не учитывают еще одну категорию вещей — тех, которые могут быть элементами сетей связи в наном мире. Эти вещи получили название нановещей, а их сетевые структуры — наносетей [4]. В данной работе речь пойдет об определении и классификации наносетей, их применении и приложениях.

Наносеть является самоорганизующейся сетью, в которой в качестве узлов сети используются наномашинны, а информация и сигнализация могут быть переданы, в том числе и путем перемещения вещества. Наномашинна — это устройство, состоящее из компонентов наноуровня, способное выполнять такие специфические задачи на наноуровне, как телекоммуникации, вычисление, хранение, измерение и воздействие.

Наномашинны и наносети образуют новую ветку развития Интернета Вещей – Интернет Нановещей (IoNT – Internet of Nano-Things). IoNT может применяться во множестве сфер деятельности человека, к примеру:

- 1) Медицина:
 - a) «Умные» имплантаты;
 - b) On-line мониторинг уровня сахара в крови у больных диабетом;
 - c) Мониторинг сердца;
 - d) «Умные» лекарства (доставляются непосредственно к патогенным организмам).
- 2) Производство:
 - a) Контроль качества пищи;
 - b) Тотальный контроль процессов производства.
- 3) Окружающая среда:

- a) Контроль состояния водных ресурсов;
- b) Контроль состояния почвы;
- c) Контроль загрязнения воздуха.

В настоящее время классифицируют и выделяют два вида наносетей:

- Электромагнитные, в которых информация передается с помощью электромагнитных волн с использованием графеновых антенн, работающих в диапазоне 0,1—1 ТГц;
- Молекулярные, в которых информация передается с помощью перемещения вещества.

Концепция наносетей, её типы и примеры практического применения во всех случаях подразумевают централизованный сбор и обработку информации. Для такой задачи необходим микрошлюз, с которым взаимодействуют составные части сети [5]. В общем виде эта структура изображена на рис. 1.

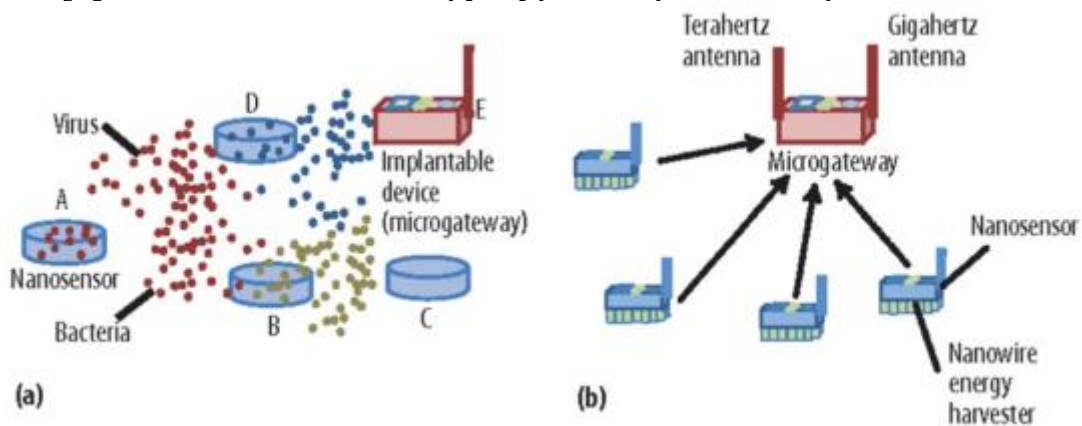


Рис. 1. Взаимодействие молекулярных (а) и электромагнитных (б) наносетей с микрошлюзом.

Как уже говорилось ранее, электромагнитные наносети используют для передачи информации антенны, работающие в диапазоне 0,1—1 ТГц (рис. 2).

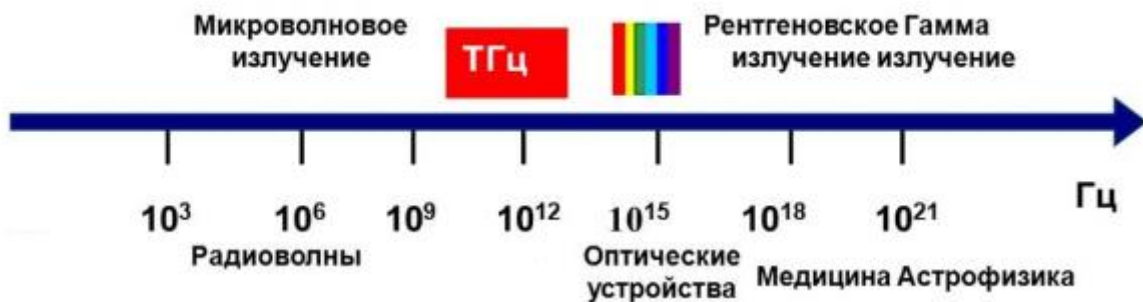


Рис. 2. Терагерцовый диапазон частот.

Передача происходит в так называемых «окнах прозрачности» (рис. 3) - наиболее подходящих (с наименьшими потерями) полосах частот в ТГц диапазоне по формуле: $P_{Rx}(f, d) = P_{Tx}(f) - L_P(f, d) - L_A(f, d)$, где

- $P_{Rx}(f, d)$ – СПМ принятого сигнала;
- $P_{Tx}(f)$ – спектральная плотность мощности переданного сигнала (СПМ);
- $L_P(f, d)$ – потери сигнала в пространстве;

- $L_A(f, d)$ – потери из-за молекулярной абсорбции.

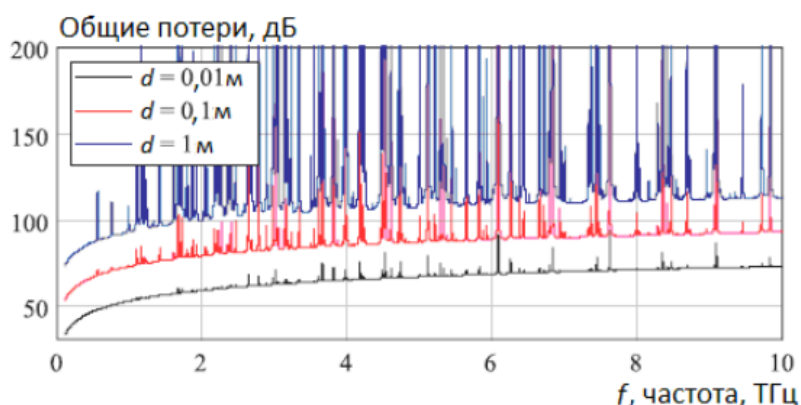


Рис. 3. Окна прозрачности в диапазоне ТГц.

Для определения взаимодействия между частями сети используют аббревиатуру ЭМКН (Электромагнитные коммуникации в наносетях) – передача и прием электромагнитного излучения с использованием компонентов на основе новейших наноматериалов.

ЭМКН происходят путем передачи информации между антеннами из графена, т.к. уменьшение до наноуровня классических металлических антенн потребует использования очень высоких резонансных частот (более 100 ТГц).

Антенна располагается на корпусе наномашинки совместно с другими составными частями (рис. 4).

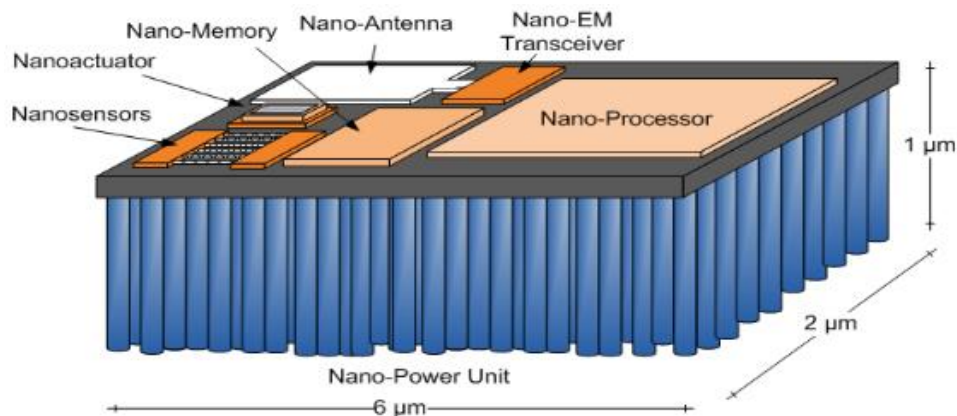


Рис. 4. Пример наномашинки.

В силу размеров привычные способы зарядки или замены батареи не представляются возможным. Для решения данного вопроса используют, к примеру, нанопроволоки из оксида цинка, располагающиеся на корпусе устройства (рис. 4, Nano-Power Unit), или используют метод питания от внешних устройств, по аналогии с пассивными RFID метками.

Молекулярные наносети, в свою очередь, классифицируются на наносети, в которых информация передается на расстояния:

- нано и микрометры,
- микро- и миллиметры,

- метры и более.

В первом случае для передачи информации исследуются возможности, например, положительных ионов кальция. Вторая группа молекулярных наносетей характеризуется использованием для передачи информации, например, жгутиковых бактерий. Для третьей же группы предусматривается проведение исследований по передаче информации с помощью феромонов, пыльцы и спор растений, трансдукции (сенсорного преобразования) света [4]. Кроме того, в последнее время пристальное внимание уделяется созданию наносетей на основе нейронов, несущих в себе свойства электромагнитных и молекулярных наносетей.

Чтобы сеть работала, каждая составляющая должна быть способна передавать информацию на определенные расстояния. Поэтому в молекулярной наносети (во всех ее видах) есть определенная концепция передачи информации (молекулярная коммуникация), подобно обычным сетям, так называемая «молекулярная теория связи» (рис. 5).

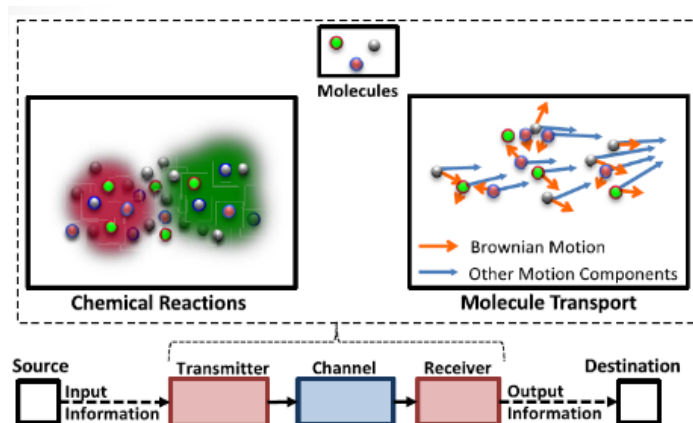


Рис. 5. Молекулярная теория связи.

В зависимости от того, как молекулы переправляются передатчиком и приёмником, молекулярные коммуникации делятся на два основных типа. Первый тип называется пассивной молекулярной коммуникацией (ПМК), а второй тип - активной молекулярной коммуникацией (АМК) [7].

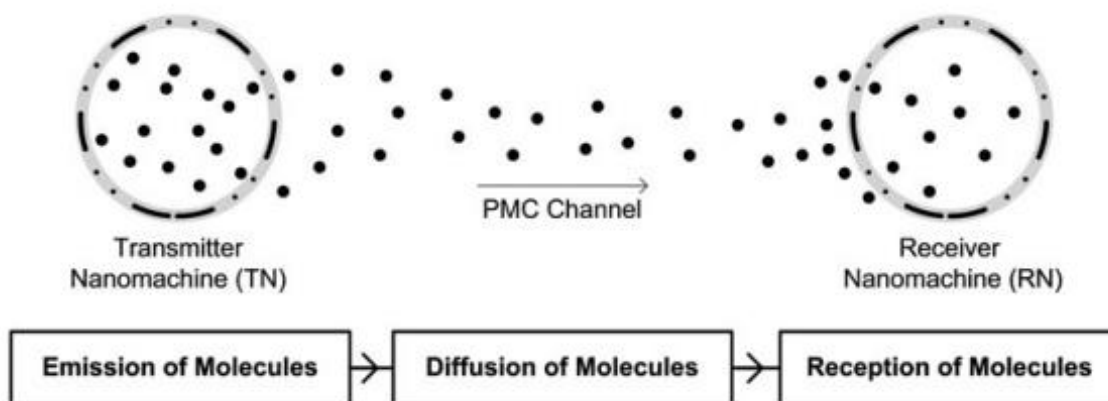


Рис. 6. Абстрактная схема для ПМК (РМС) между наномашинной-передатчиком (TN) и наномашинной-приемником (RN).

В ПМК молекулы пассивно перемещаются от передатчика и приёмнику без необходимости в промежуточной транспортной системе, которая бы занималась направлением и транспортировкой (рис. 6). В зависимости от того, как приёмник получает молекулы, пассивная молекулярная коммуникация классифицируется на два типа:

- ПМК с поглощением;
- ПМК со связкой рецептора и лиганда.

ПМК с поглощением подразумевает, что молекула-приемник принимает молекулы в себя всякий раз, когда они вступают в контакт с её поверхностью. Во втором же случае, молекула-приемник имеет поверхностные рецепторы для приема молекул в непосредственной близости от него посредством лиганд-рецепторного механизма связывания.

В активной молекулярной коммуникации после того, как молекулы испускаются передатчиком, они нуждаются в промежуточной транспортной системе, которая направляет и транспортирует их к приёмнику (рис. 7). Таких систем в АМК выделяют 4:

- В первой системе для переноса молекул от передатчика к приёмнику используются молекулярные двигатели;
- Во второй системе предполагается, что передатчик и приёмник контактируют, а GJCs (Gap junction channels) каналы являются посредниками в диффузии молекул.
- В третьей системе передатчики движутся к приемнику, следуя за молекулами аттрактора, испускаемыми приемником.
- В четвертой системе предполагается, что передатчик и приёмник являются подвижными. Молекулы передатчик остаются прикрепленными на его поверхности. При каждом столкновении эти молекулы и рецепторы на поверхности приёмника взаимодействуют, передавая информацию.

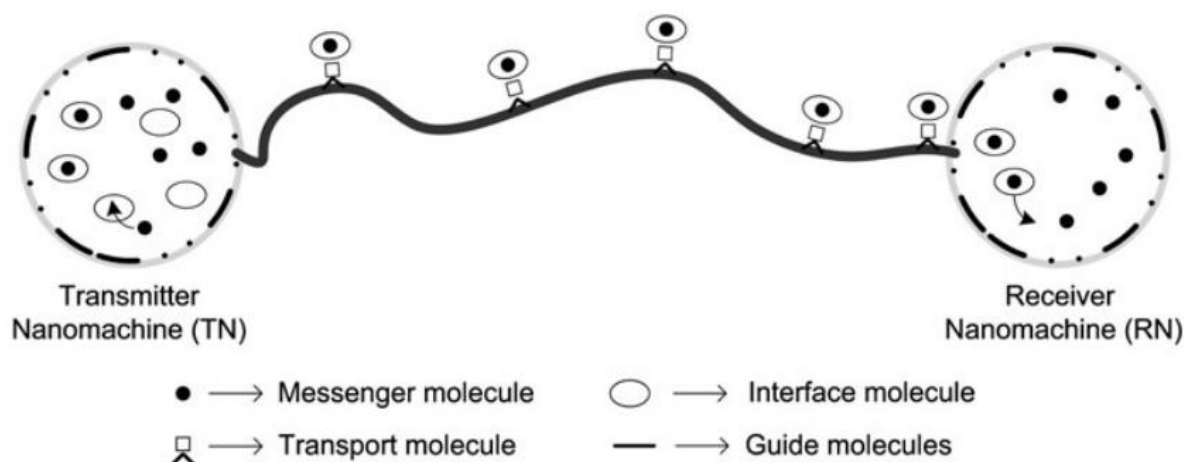


Рис. 7. Пример АМК с помощью молекулярных моторов. Молекулы, инкапсулированные в везикулы, переносятся молекулярными двигателями по белковым нитям.

Получение информации в наносетях требует контроля за частицами, находящимися на нано-уровне. Решением в данном вопросе выступает использование спектрометра – аналитического прибора, принцип работы которого основан на накоплении, обработке и анализе спектра излучения. Получают этот спектр методом облучения образца и регистрации появляющейся флуоресценции. Замеряется длина, частота волн, интенсивность излучения. В результате работы данного прибора получают данные о составе исследуемого объекта – те самые нано-частицы, которые используются как транспорт в наносетях.

Таким образом, наносети в данный момент времени подразделяются на молекулярные и электромагнитные. Каждая из этих концепций уникальна, так как использует различный транспорт и способы передачи информации. Электромагнитные наносети используют нанороботов с графитовыми антеннами, передающими и принимающими информацию в терагерцовом диапазоне частот в окнах прозрачности, а молекулярные наносети используют молекулы для передачи информации. В зависимости от используемого вещества, передача информации происходит на различные расстояния.

Список используемых источников:

1. Кучерявый А. Е. Интернет Вещей // Электросвязь.— 2013.— № 1.
2. Waldner J.-B. Nanocomputers and Swarm Intelligence / ISTE, Wiley&Sons, London.— 2008.
3. Recommendation Y.2060. Overview of Internet of Things. ITU-T, Geneva — February 2012.
4. Кучерявый А.Е., Баласубраманиям С. Интернет нановещей и наносети // Электросвязь.— 2014.— № 4.
5. Valerie K., Daniel B. Cyborgs R Us: The Bio-Nano Panopticon of Injected Bodies? // International Journal of Vaccine Theory, Practice, and Research 2(2), August 12, 2022.
6. Koucheryavy Y., Kara O., Balasubramaniam S. et. al. An Experimental Investigation into Utilizing Neurons for Wireless Nano Communication // IEEE Transactions on NanoBioScience.— 2014 (в печати).
7. Atakan B. Molecular Communications and Nanonetworks From Nature To Practical Systems // Department of Electrical and Electronics Engineering Izmir Institute of Technology Urla, Izmir, Turkey – Книга – 2014.

Nikitin E., Kharlamov M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Definition and classification of nanonetworks. Molecular nanonetworks and their applications. Electromagnetic nanonetworks and their applications. Research in the field of the Internet of Things shows that the number of connected devices continues to grow, reaching up to 50 trillion units. However, these projections do not take into account another category of devices - the nano-things that are involved in nano-networks.

Key words: IoT, IoNT, nanonets, electromagnetic nanonets, molecular nanonets.

УДК 621.319
ГРНТИ 49.33.29

РАЗРАБОТКА МЕТОДИКИ СУБЪЕКТИВНОЙ ОЦЕНКИ КАЧЕСТВА ВОСПРИЯТИЯ ДЛЯ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

Е. Ю. Никонова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Дополненная реальность является одной из самых перспективных и актуальных технологий. Количество приложений и услуг Дополненной реальности постоянно растет. А появление новых услуг предъявляет, соответственно, новые, более строгие требования к сетям, и их так же необходимо оценивать. Поэтому была создана методика субъективной оценки качества восприятия для голографических изображений на основе рекомендации ВТ.500-14. Методика экспериментально проверена, а результаты представлены в таблице.

дополненная реальность (ДР), субъективная оценка, методика, требования к сетям связи, голографические изображения

Введение

Дополненная реальность является одной из самых перспективных технологий 21, а количество приложений, использующих дополненную реальность, постоянно растет, и результаты очевидны во многих областях, например, в развлечениях, здравоохранении, образовании, коммерция, маркетинге, рекламе и т.д.

В тоже время расширяется количество устройств, используемых в ДР. В последнее время стали популярны голографические вентиляторы.

Услуги дополненной реальности стремительно развиваются, например, появляются такие услуги как телеприсутствие, которое обширно везде используется. Наглядный пример представлен на рис. 1.



11 марта 2020
Живое танцевальное шоу от компании
Panasonic



Лаборатория цифрового искусства в
Нью-Йорке

Рис. 1. Примеры телеприсутствия

Актуальность ДР

Количество активных пользователей мобильной дополненной реальности (AR) по всему миру к 2024 году вырастет почти в 3 раза. Объем мирового рынка гарнитур для дополненной реальности в 2021 году достиг 11,2 млн штук,

увеличившись на 92,1% в сравнении с показателем годичной давности, по данным исследователей эти цифры с каждым годом будут все больше расти [4]. А значит, тема дополненной реальности есть и будет одной из самых актуальных тем еще долгое время.

Требования к сетям связи

С каждым годом новых услуг появляется все больше. А появление новых услуг предъявляет, соответственно, новые, более строгие требования к сетям.

Высококачественная и реалистичная обратная связь возможна при очень высокой частоте пропускания (> 10 кГц) и низкой задержке (~1 мс). Этого можно достичь с помощью сети 5G.

По представленному ниже рис. 2, мы получаем подтверждение вышесказанному. Если приложения видео стриминга требуют пропускную способность от 10 Мбит до 100 Мбит, то приложения дополненной и виртуальной реальности уже от 100 до 1Гбит с задержкой около 1 мс [3].

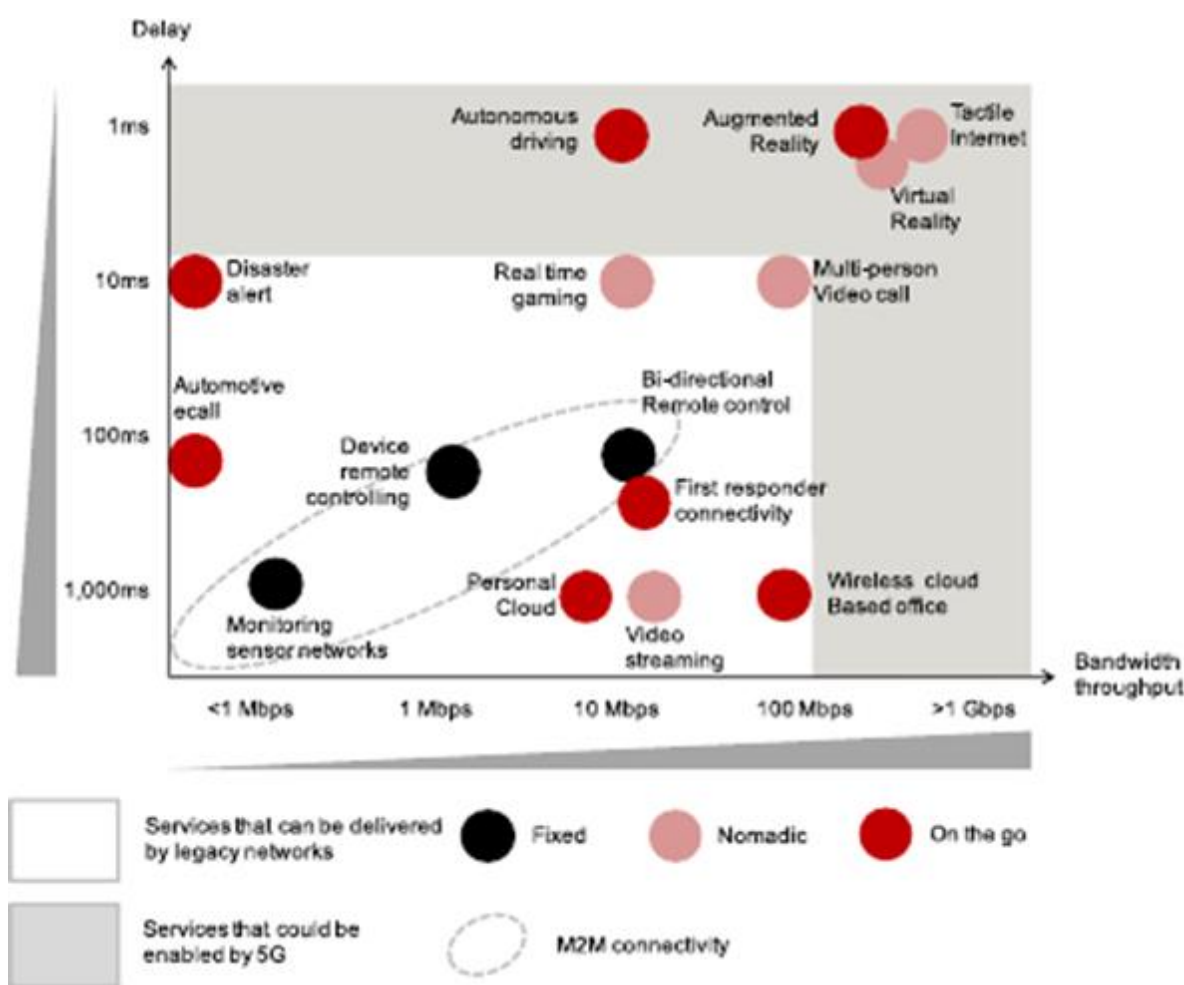


Рис. 2. Требования к пропускной способности и задержке при использовании 5G

Методика субъективной оценки качества восприятия для дополненной реальности (голографических изображений)

Так как появляются новые устройства, их так же необходимо оценивать.

Поэтому, в данной работе я предлагаю новую методику субъективной оценки качества восприятия для дополненной реальности конкретно для голографических изображений. Данная методика создана на основе рекомендации ВТ.500-14 [1].

Условия для проведения испытания.

Рекомендуется выбирать помещение с низкой освещенностью, шумоизолированное.

Угол обзора должен быть ограничен таким образом, чтобы при отклонении от вентилятора не появлялось искажений цвета изображения. Угол обзора не должен превышать 45 градусов, иначе изображение сливается и перестает быть видимым. Оптимальный горизонтальный угол просмотра испытываемой системы изображения должен учитываться при определении угла обзора.

Оценщики могут быть или не быть экспертами, что определяется задачами испытания. Рекомендованное число наблюдателей более 15.

До начала эксперимента необходимо оценить световосприятие экспертов.

Исходный сигнал представляет собой эталонное изображение с разрешением в диапазоне от 240 до 1080 пикселей. Для данного эксперимента необходимо подобрать 5-7 видеороликов с различным форматом и качеством 3D изображения.

Продолжительность сеанса испытания 20 минут. Время для просмотра одного видеоролика – 60 секунд. В данном эксперименте необходимо запустить 5-7 видеороликов с различным качеством 3D- изображения. Между каждым видеороликом необходимо сделать минутную паузу, таким образом дав наблюдателям возможность выставить оценку по представленной шкале оценивания. В начале первого сеанса следует провести примерно пять "тренировочных демонстраций" для стабилизации мнения оценщиков.

Вариант испытания- Сравнение пары вентиляторов.

Для данной методики используется 7-бальная шкала от 8- неразличимые ухудшения до 1- сильные ухудшения везде.

ТАБЛИЦА 1. Шкала оценивания пары голографических вентиляторов

Оценка	Параметры	ухудшение
8	Большая палитра цветов; Изображение четкое; Стереоскопический эффект присутствует; Изображение яркое; Звук и видео синхронизированы;	нигде
7	Большая палитра цветов; Изображение менее четкое;	кое-где
6	Стереоскопический эффект присутствует; Яркость снизилась; Звук и видео синхронизированы;	везде
5	Палитра цветов снизилась; Изображение мутноватое;	кое-где
4	Стереоскопический эффект присутствует; Изображение неяркое;	везде

	Звук и видео иногда не совпадают;	
3	Палитра цветов большая; Изображение размытое; Стереоскопический эффект присутствует не всегда; Изображение бледное; Заметно отставание звука от видео;	кое-где
2		езде
1	Палитра цветов узкая; Изображение мутное, неразборчивое; Стереоскопический эффект отсутствует; Изображение тусклое; Звук и видео не синхронизировано;	кое-где

Экспериментальное исследование методики

В соответствии с требованиями оценщики были размещены на расстоянии приблизительно 6Н от вентиляторов, голографические вентиляторы были размещены на светло-серой стене, кабинет полностью был изолирован от постороннего шума.

Перед тестированием метода участникам был объяснен метод и выдана распечатанная на листах А4 шкала оценивания.

На оба вентилятора были одновременно поданы видеоизображения в разном формате, а по завершении эксперимента бланки со шкалами были собраны и проанализированы.

В результате эксперимента получились следующие итоги:

ТАБЛИЦА 2. Результаты эксперимента

Р	а	Н	Номер участника														Ср. значение			
			В	1	2	3	4	5	6	7	8	9	10	11	12	13		14	15	16
1	0	1	1	7	8	8	7	8	8	8	8	8	8	7	7	7	8	8	7	7
			2	5	5	6	5	6	6	5	6	6	6	6	5	6	6	6	6	6

80																			
720	2	1	5	6	6	5	6	6	7	5	6	5	6	5	6	6	5	5	6
		2	4	5	4	4	4	4	5	4	4	3	3	4	5	4	4	4	4
480	3	1	5	5	5	4	5	5	6	4	5	5	5	5	5	5	4	5	5
		2	3	4	4	4	4	4	3	3	3	4	4	4	4	4	3	4	4
360	4	1	4	5	4	4	4	4	4	4	4	4	4	5	4	4	4	5	4
		2	3	3	3	4	3	3	3	3	4	4	3	3	3	4	3	4	3
240	5	1	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3
		2	2	2	2	2	3	2	2	3	3	3	2	2	2	3	3	3	2

Вывод:

В данной работе была создана методика субъективной оценки качества восприятия для дополненной реальности для голографических изображений. Экспериментально проверено и доказано, что она подходит для оценки на голографических вентиляторах.

Список используемых источников:

1. Recommendation ITU-R BT.500-14 « Methodology for the subjective assessment of the quality of television pictures». ITU-T, Geneva, January, 2019
2. Развитие приложений и услуг дополненной реальности, А. А.Рочев, М.А. Маколкина, СПбГУТ, Санкт-Петербург, 2018
3. Virtual and Augmented Reality on the 5G Highway, Virtual and Augmented Reality on the 5G Highway, Feb. 2017
4. Рынок устройств виртуальной и дополненной реальности [Электронный ресурс]:URL:Tadviser.2022.URL:https://www.tadviser.ru/index.php/Статья:Рынок_устрой.(дата обращения 15.09.22)
5. Augmented Reality Trends of 2022 [Электронный ресурс]: URL: <https://mobidev.biz/blog/augmented-reality-trends-future-artechnologies> (дата обращения 11.05.22)

Nikonova E.U.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Development of a methodology for subjective assessment of perception quality for augmented reality.

Augmented reality is one of the most promising and relevant technologies. The number of Augmented Reality applications and services is constantly growing. And the emergence of new services imposes, accordingly, new, more stringent requirements for networks, and they also need to be evaluated. A technique for subjective assessment of the quality of perception for augmented reality was created based on the recommendation BT.500-14. The technique has been experimentally verified, and the results are presented in the table.

Key words: augmented reality (AR), subjective assessment, methodology, requirements for communication networks, holographic images.

УДК 004.732
ГРНТИ 49.43.29

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ТЕХНОЛОГИИ ЯВНОГО ФОРМИРОВАНИЯ ЛУЧА В СЕТЯХ WI-FI

С. А. Скоробогатова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается технология явного формирования луча, исследуется эффективность её применения в сетях стандарта IEEE 802.11ac. Проведено сравнение полученных в ходе эксперимента характеристик передачи данных с применением и без применения данной технологии. Сделано заключение о работоспособности технологии, эффективности ее применения на практике и предположение о том, что могло повлиять на полученные результаты.

явное формирование луча, TxBF, 802.11ac, Wi-Fi

Формирование луча (Transmit Beamforming, TxBF) – это технология, в которой за счет измерений характеристик канала, расчета и изменения фаз, сигнал с разных антенн передающего устройства приходит на сторону клиента синфазно [1]. Устройство, формирующее передаваемый сигнал в сторону клиента, называется формирователем луча (beamformer), а устройство принимающее сигнал – получателем луча (beamformee). При явном формировании луча и beamformer, и beamformee поддерживают технологию TxBF, beamformee активно участвует и помогает в формировании луча. Результатом применения технологии TxBF является увеличение мощности сигнала на стороне клиента и, соответственно, более высокое соотношение сигнал/шум [2,3]. Увеличение соотношения сигнал/шум позволит использовать более сложную модуляцию, где приходится больше бит на один символ, и более простое кодирование. Следовательно, ожидается более высокая скорость передачи данных и меньше повторных передач.

Как правило, устройства с технологией TxBF стоят дороже. Если взять два роутера от компании TP-Link: Archer A5 и Archer C50, одинаковых по характеристикам во всем, кроме наличия технологии TxBF, то разница в стоимости будет составлять около четырехсот пятидесяти рублей. С более дорогостоящим и сложным оборудованием разница в стоимости может быть более значительной. Оптимальным способом для определения целесообразности переплаты за TxBF является проведение эксперимента с такими устройствами, что не всегда представляется возможным.

В данном исследовании использовались два устройства: Wi-Fi роутер TP-Link Archer AX73 и адаптер Linksys WUSB6300. Wi-Fi роутер был подключен к персональному компьютеру сетевым Ethernet-кабелем. Через 2 стены, на расстоянии 20 метров от роутера, находился ноутбук с подключенными внешними адаптерами NETGEAR A6210, который участвовал в перехвате трафика, и Linksys WUSB6300, который подключался к сети Wi-Fi роутера

стандарта IEEE 802.11ac в диапазоне 5 ГГц. Схема стенда представлена на рис. 1.

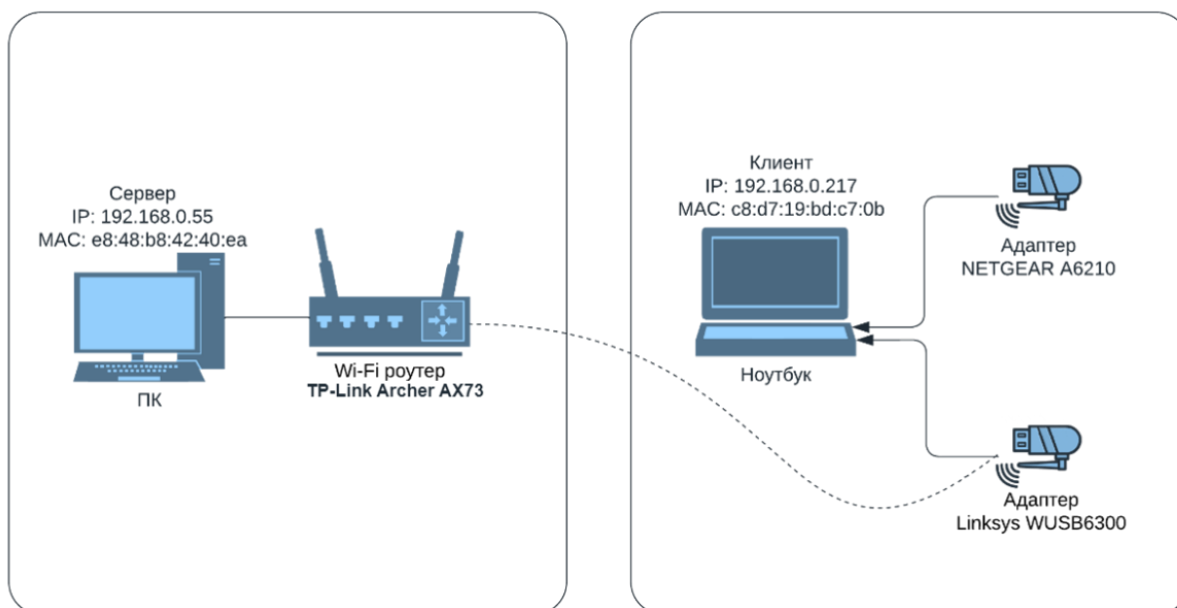


Рис. 1. Организация стенда

Трафик перехватывался на ширине канала 20 МГц при включенном и при выключенном TxBF, аналогично на ширине 40 МГц: по 3 перехвата для каждого случая, в общей сумме 12 перехватов.

На основе перехваченного трафика, произведен расчет средней скорости передачи кадра, уровня мощности сигнала и процента повторных. Результаты расчетов представлены в таблице 1. На ширине 20 МГц случай с явным формированием луча не отличается по средней мощности сигнала от случая без явного формирования. Процент повторных передач с TxBF в 1,8 раза больше, чем без него, а средняя скорость передачи кадров с TxBF увеличилась на 4,4 Мбит/с. На ширине канала 40 МГц совершенно противоположные результаты. С включенным TxBF среднее значение мощности сигнала улучшилось всего на 2,4 дБм, доля повторных передач стала в 1,6 раз меньше, но средняя скорость передачи без явного формирования луча больше на 31,9 Мбит/с.

ТАБЛИЦА 1. Результаты расчета средней скорости передачи, уровня сигнала и доли повторных передач

Средняя скорость передачи кадров, Мбит/с				
№ измерения	Ширина канала 20 МГц		Ширина канала 40 МГц	
	TxBF вкл.	TxBF выкл.	TxBF вкл.	TxBF выкл.
1	92,9	96,4	145,8	174,6

2	78,3	83,6	166,1	182,7
3	103,1	81,2	144,9	194,9
среднее	91,5	87,1	152,2	184,1
Уровень сигнала, дБм				
№ измерения	Ширина канала 20 МГц		Ширина канала 40 МГц	
	ТхBF вкл.	ТхBF выкл.	ТхBF вкл.	ТхBF выкл.
1	-57,5	-58,6	-61,3	-57,0
2	-60,7	-59,1	-57,8	-58,4
3	-57,6	-58,1	-62,6	-57,5
среднее	-58,6	-58,6	-60,6	-57,6
Доля повторных передач, %				
№ измерения	Ширина канала 20 МГц		Ширина канала 40 МГц	
	ТхBF вкл.	ТхBF выкл.	ТхBF вкл.	ТхBF выкл.
1	14,8	15,5	5,8	15,4
2	10,6	6,2	10,6	9,1
3	22,0	5,2	3,2	6,7
среднее	15,8	9,0	6,5	10,4

Во всех случаях, за исключением третьего измерения на ширине канала 20 МГц, скорость передачи с выключенным ТхBF лучше, чем с включенным. Из рис. 2 видно, что именно в этом измерении разброс значений уровня сигнала с включенным ТхBF меньше всего.

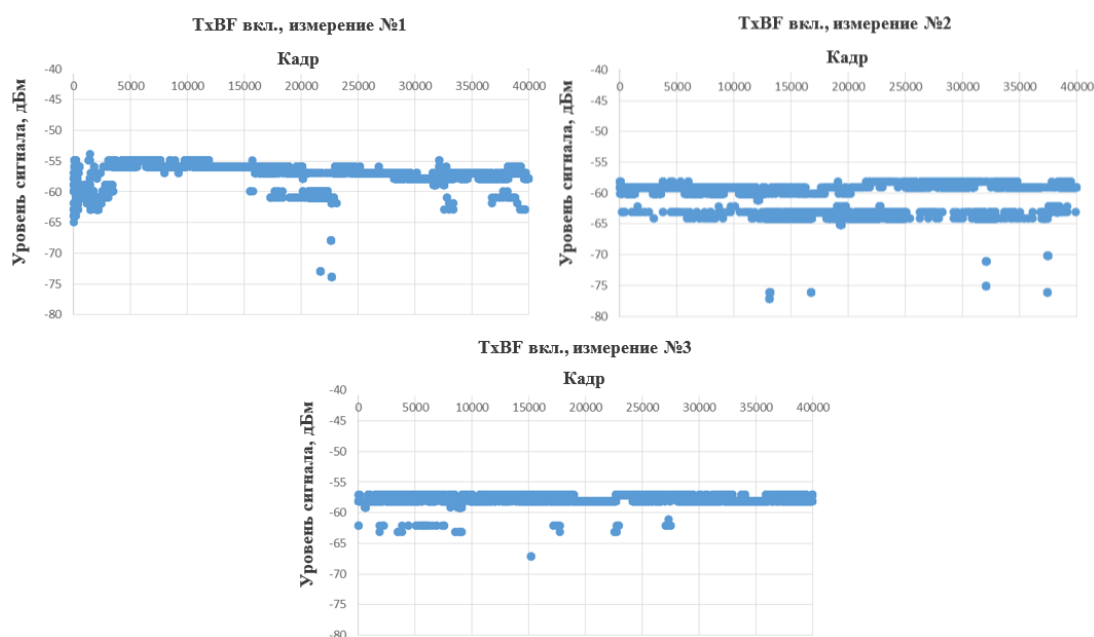


Рис. 2. Графики изменения уровня сигнала для трех измерений с включенным TxBF на ширине канала 20 МГц

Исходя из результатов расчетов, приведенных в таблицах 1 и 2, можно сделать вывод о соответствии доли повторных передач количеству пространственных потоков. Чем больше потоков используется, тем больше повторных передач. Например, на ширине 20 МГц, при выключенном TxBF во втором и третьем измерении, передача осуществлялась в основном в один поток и соответственно доли повторных передач ниже. А вот в первом измерении передача большинства кадров осуществлялась в два потока и доля повторных передач в этом измерении значительно выше, чем в других двух. Важно отметить, что большая доля повторных передач при явном формировании луча в третьем измерении не помешала получить скорость выше, чем без TxBF.

ТАБЛИЦА 2. Процент кадров с одним или двумя пространственными потоками

Ширина канала, МГц	TxBF	Кол-во пространственных потоков	№ измерения			Среднее
			1	2	3	
20	Вкл.	1	14,2%	37,6%	0,1%	17,3%
		2	85,8%	62,4%	99,8%	82,7%
	Выкл.	1	6,6%	97,9%	84,7%	63,1%
		2	93,4%	2,1%	15,3%	36,9%
40	Вкл.	1	87,9%	6,0%	95,1%	63,0%
		2	11,6%	93,6%	4,6%	36,6%
	Выкл.	1	50,3%	95,9%	96,3%	80,8%
		2	49,4%	3,7%	3,3%	18,8%

Предполагалось, что технология явного формирования луча повысит уровень принимаемого сигнала, увеличит скорость передачи кадров и сократит количество повторных передач. Но данная технология не показала однозначного преимущества. Есть либо незначительные изменения в характеристиках, либо без явного формирования трафик передается лучше. Такие результаты могли быть получены из-за условий, в которых проводились опыты: ошибок в прошивке Wi-Fi адаптера или Wi-Fi роутера, препятствий на пути распространения сигнала, ориентации устройств по отношению друг к другу или расстояния между ними.

Список используемых источников:

1. Matthew S. Gast. 802.11ac: A Survival Guide: O'Reilly Media, 2013. – 154 p. ISBN 978-1-449-34314-9.
2. Смирнова Е. В., Пролетарский А. В. и др. Технологии современных беспроводных сетей Wi-Fi : учебное пособие. М : МГТУ им. Н. Э. Баумана, 2017. 446 с.
3. Aruba Networks, White paper 802.11 ac in-depth [Электронный ресурс]. URL: https://www.arubanetworks.com/assets/wp/WP_80211acInDepth.pdf (дата обращения 4.11.2022).

Skorobogatova S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunications

A study of the efficiency of beamforming technology in Wi-Fi networks. The article reviews explicit beamforming and explores the efficiency of its application in IEEE 802.11ac networks. The comparison of the data transmission characteristics obtained in the experiment with the use of explicit beamforming and without it is presented. The conclusions about the technology performance in practice and assumptions about what might have influenced the obtained results are made.

Key words: *explicit beamforming, TxBF, 802.11ac, Wi-Fi.*

УДК 004.732
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ КОДИРОВАНИЯ LDPC В СЕТЯХ WI-FI

А. А. Смирнова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена исследованию эффективности применения кодирования LDPC в сетях Wi-Fi. Актуальность темы заключается в необходимости сокращения процента повторных передач для удобства и быстрого подключения к сети Wi-Fi. В статье рассматривается метод исследования эффективного уменьшения значения процента повторных передач при использовании кодирования с малой плотностью проверок на четность по сравнению со стандартным двоичным сверточным кодированием в сетях Wi-Fi. В статье представлены результаты экспериментального сравнения этих двух способов.

Wi-Fi, IEEE 802.11, помехоустойчивое кодирование, LDPC

Wi-Fi – это стандарт широкополосной беспроводной связи семейства IEEE 802.11, работающий на физическом и канальном уровне модели ISO/OSI (см. рис. 1).



Рис. 1. Уровни модели OSI, на которых работает стандарт IEEE 802.11

Одним из способов борьбы с ошибками, возникающими при передаче данных по каналам с шумами, является применение методов помехоустойчивого кодирования. Существует несколько методов, применяемых в разных поколениях технологии Wi-Fi. Одним из них является использование кодов с малой плотностью проверок на четность Low Density Parity Check, LDPC [1]. Спрос на использование данного типа кодирования возник с развитием телекоммуникационных технологий [2].

Для выполнения работы по исследованию эффективности применения кодирования LDPC в сетях Wi-Fi был создан экспериментальный стенд,

содержащий следующие элементы: ноутбук в качестве клиентского устройства, Wi-Fi роутер с поддержкой стандартов IEEE 802.11a/b/g/n/ac, внешний адаптер Wi-Fi с подключением через USB, настольный компьютер в качестве сервера (см. рис. 2). С помощью программы TamoSoft Throughput Test генерировался поток TCP-трафика как со стороны клиента (IP-адрес 192.168.31.208), так и со стороны сервера (IP-адрес 192.168.31.14). Wi-Fi роутер и сервер располагались в несмежной аудитории с клиентским устройством и подключенным внешним адаптером Wi-Fi. Препятствием на пути распространения сигнала были 2 внутренние стены.

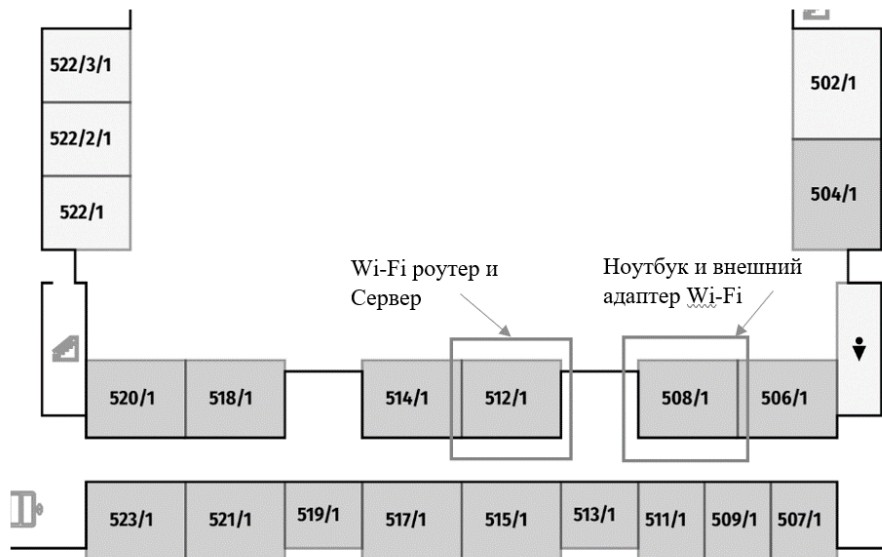


Рис. 2. Схема расположения компонентов экспериментального стенда

Экспериментальная часть работы заключается в исследовании статистики повторно переданных кадров с разделением по размеру в режимах с и без использования кодирования LDPC на каналах диапазона 5 ГГц. Данная статистика была выбрана по причине того, что кодирование LDPC является более помехоустойчивым (по сравнению со способом кодирования на основе Binary Convolutional Coding, BCC) в условиях большего шума в эфире [3]. Теоретически его использование предполагает меньший процент ошибочных кадров и их последующую повторную передачу. перехват трафика был организован при помощи программы Savvius Omnipcap, а обработка полученных результатов производилась в Wireshark.

В рамках исследования были выбраны каналы 52, 56, 60 и 64, на которых собиралась статистика в восходящем (Upstream) и нисходящем (Downstream) направлениях. Проверка на наличие постоянных помех в эфире перед постановкой эксперимента показала то, что данные каналы были наименее зашумлены в текущий момент времени (см. рис. 3). Для получения статистики по количеству повторно переданных использовался фильтр Wireshark `ip.src == 192.168.31.14 and ip.dst == 192.168.31.208` для нисходящего потока, `ip.dst ==`

192.168.31.14 and ip.src == 192.168.31.208 для восходящего. Данные фильтры применялись в меню Wireshark «Беспроводной - Трафик WLAN».

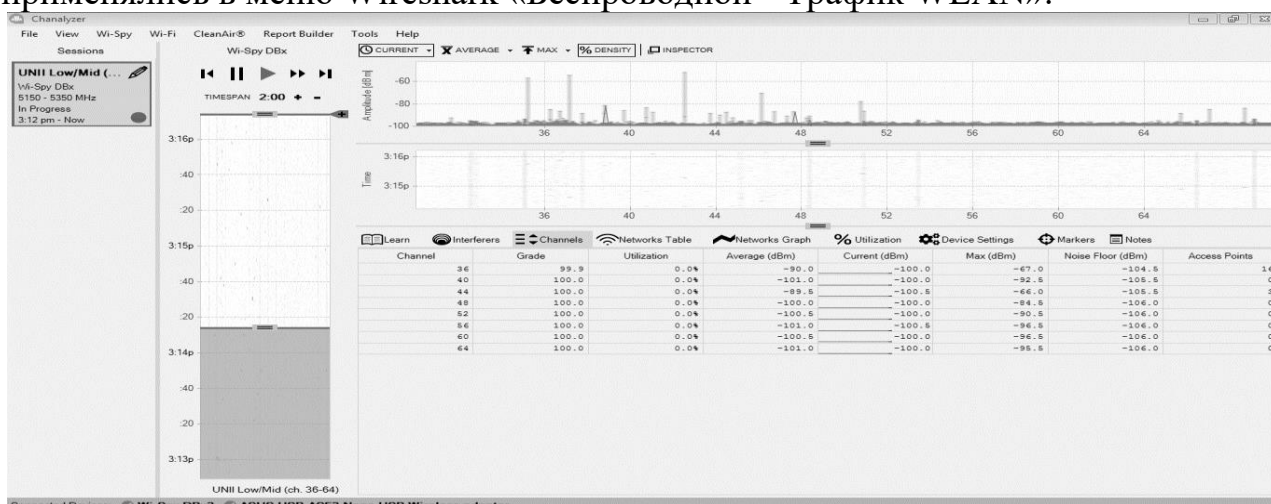


Рис. 3. Проверка эфира на наличие помех при помощи программы Chanalyzer

Для анализа полученных результатов были составлены таблицы 1 и 2. В них отражена статистика повторных передач кадров с учетом размера кадра в байтах и направления передачи трафика. Общий процент повторных передач по двум направлениям наиболее наглядно отображает эффективность применения кодирования LDPC в рамках поставленного эксперимента.

ТАБЛИЦА 1. Статистика повторно переданных кадров для канала 52

Размер кадра, байт	LDPC включен		LDPC выключен	
	Downstream	Upstream	Downstream	Upstream
≤ 240	0,07%	29,27%	0,14%	33,19%
≥ 1024	0,04%	35,35%	0,07%	38,69%
По всем размерам	0,06%	32,31%	0,11%	35,94%
По двум направлениям	7,75%		13,01%	

Для канала 52 значение процента повторных передач при включенной опции кодирования LDPC в 1,5 раза меньше, чем при выключенном LDPC (см. таблицу 1). Наиболее эффективно передавались кадры в нисходящем потоке. Данная статистика наблюдалась на всех четырех исследуемых каналах в рамках поставленного эксперимента. Это явление можно объяснить наличием у Wi-Fi роутера внешних антенн с большим коэффициентом усиления и высокой мощности передатчика. Когда процент повторно переданных кадров близок к нулю, это означает, что нагрузка на канал в виде дублирования потерянной информации практически отсутствует.

В таблице 2, представленной ниже, отражена информация по общим значениям процента повторных передач для каналов 56-64.

ТАБЛИЦА 2. Статистика повторно переданных кадров для каналов 56, 60, 64

Тип статистики	LDPC включен	LDPC выключен
----------------	--------------	---------------

По двум направлениям (56 канал)	8,74%	12,24%
По двум направлениям (56 канал)	7,88%	8,22%
По двум направлениям (56 канал)	10,01%	10,32%

По мере перехода от канала 52 к каналу 64 разница между значением процента повторных передач при включенном и отключенном LDPC становится меньше (см. рис. 4). Данную зависимость можно объяснить наличием временных помех, которые могли появиться в течение проведения эксперимента. На рис. 3 видно, что перед постановкой эксперимента более подвержен влиянию внешних помех канал 52, а менее всего – канал 64.

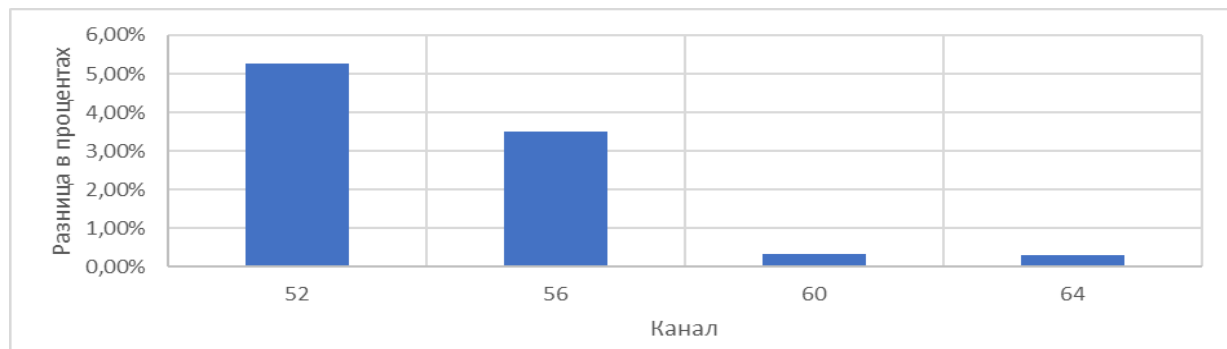


Рис. 4. Разность между долей повторных передач при включенной и отключенной опциях кодирования LDPC

Таким образом, несмотря на незначительное уменьшение процента повторных передач в собранной статистике, применение кодирования LDPC в сетях Wi-Fi оказалось эффективным. Данная тематика заслуживает отдельного внимания и дальнейшего исследования.

Список используемых источников:

1. Теория помехоустойчивого кодирования. Часть 2. Сверточные коды. Турбокоды // О.С. Когновицкий, В.М. Охорзин, И.А. Небаев; СПбГУТ. – СПб., 2015 – 64 с.
2. Панкратов, А. В. Исследование LDPC декодеров / А. В. Панкратов. — Текст: непосредственный // Молодой ученый. — 2011. — № 7 (30). — Т. 1. — С. 39-42.

Smirnova A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunications

A study of the efficiency ldpc coding in wi-fi networks.

The article is devoted to the study of the effectiveness of LDPC encoding in Wi-Fi networks. The relevance of the topic consists in the need to reduce the percentage of retransmissions for convenience and quick connection to the Wi-Fi network. The article discusses a method for investigating the effective reduction of the percentage of retransmissions when using encoding with a low density of parity checks compared to standard binary convolutional encoding in Wi-Fi networks. The results of an experimental comparison of these two methods are presented.

Key words: *Wi-Fi, IEEE 802.11, error-correcting coding, LDPC.*

УДК 621.319
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ВЗАИМОСВЯЗИ СУБЪЕКТИВНЫХ ОЦЕНОК QoE И ПАРАМЕТРА ХЁРСТА ДЛЯ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

А. М. Степанов, М. А. Маколкина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Дополненная реальность - одна из самых перспективных технологий 21 века. На сегодняшний день технология дополненной реальности широко распространена в различных областях: Интернете, маркетинге, туризме, науке, медицине и телекоммуникациях. Для определения удовлетворенности пользователем качеством контента в дополненной реальности используются качество обслуживания и качество восприятия.

дополненная реальность, качество обслуживания, качество восприятия, параметр Хёрста

В настоящее время услуги передачи видео очень разнообразны и включают в себя различные форматы, которые зависят от способа организации самой услуги. Трафик дополненной реальности в большинстве приложений содержит в себе передачу видеотрафика с низким разрешением и невысокой скоростью, это связано с тем, что и беспроводные сети, и терминальное оборудование дополненной реальности, а также их совместимость ещё активно исследуются [1, 2].

Методы субъективных оценок необходимы для определения качества телевизионных систем и доставки видео, так как они выражают реакцию людей, которые в свою очередь и являются получателями видеоконтента [3][4]. Но оценить полностью систему можно только используя субъективную и объективную оценку совместно [5, 6]. Одним из возможных параметров объективной оценки является параметр Хёрста [7]. В данном докладе приведены результаты исследования параметра Хёрста и его возможность включения в методы объективной оценки качества передачи видео.

Чтобы показать явную зависимость параметра Хёрста и субъективных оценок были проведены многочисленные эксперименты и выбран трафик панорамного видео 360 градусов.

Для исследования особенностей панорамного видео при трансляции через Интернет был выбран трафик видеохостинга «YouTube», доступ к видеоконтенту осуществлялся по ссылке «<https://www.youtube.com/watch?v=hndfrDНIB-0>». Трафик захватывался на ПК через кабель Ethernet и по сети Wifi, когда как субъективная оценка просматриваемому контенту давалась при просмотре видеоконтента через смартфон.

В ходе проведения эксперимента использовался канал доступа с пропускной способностью 60 Мбит/с. Видео исследовалось в форматах LQ, SD, HD, FHD.

ТАБЛИЦА 1. Общие характеристики видеотрафика «YouTube»

N	Характеристика	Ед. измерения	Скорость потока, Кбит/с			
			380/317	680/496	990/970	2090/1900
1	Протокол	-	IP/TCP	IP/TCP	IP/TCP	IP/TCP
2	Интенсивность пакетов	Пакетов/с	56,9/40,5	91/58	143,9/110,7	292,2/210,6
3	Средняя длина пакета	байт	828/1084	812/1070	863/1096	896/1133
4	Средняя скорость передачи	Мбит/с	0,38/0,32	0,68/0,49	0,9/0,9	2,1/1,9
5	Коэффициент Хёрста (Ethernet/Wi-Fi)	-	0,78/0,74	0,785/0,76	0,79/0,77	0,8/0,775
6	Сравнительная оценка качества по пятибалльной шкале	-	2/1,8	2,5/2,3	3/2,8	4,5/4,3

При анализе полученных данных, очевидно, что статистические свойства видеотрафика, получаемого пользователем от одного источника, но при разных скоростях потока видео, отличаются. Это происходит из-за особенностей передачи по пакетным сетям, а именно маршрутами доставки и их загруженностью на момент передачи видеотрафика.

Оценка параметра Хёрста производится методом анализа изменения дисперсии и показана на рис. 1.

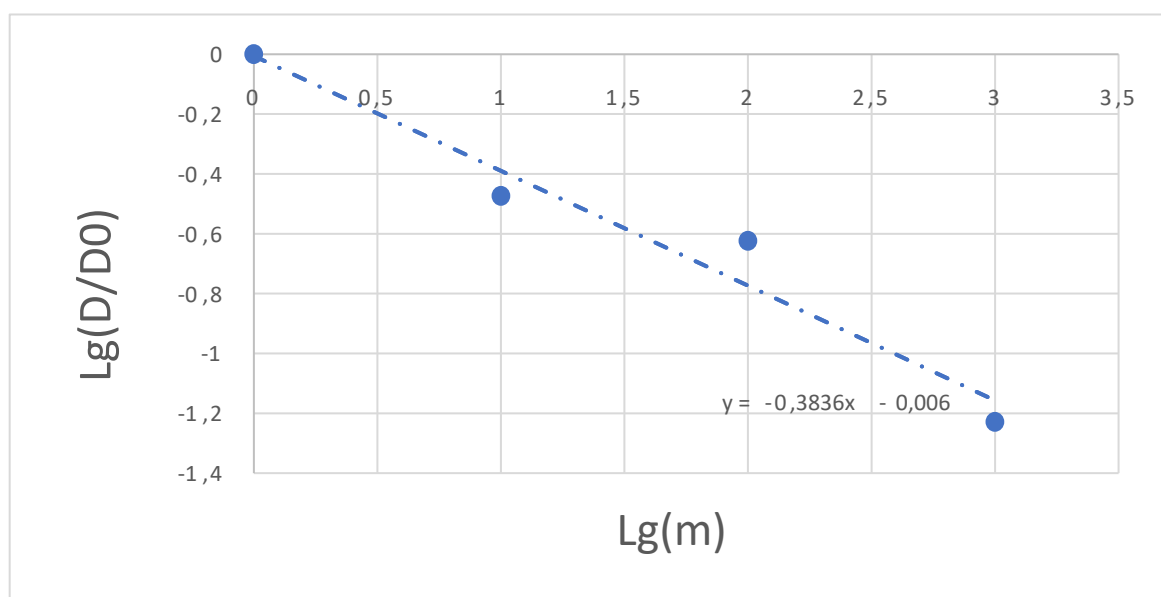


Рис. 1. Пример оценки параметра Хёрста методом анализа изменения дисперсии для видеохостинга «YouTube»

Данные, приведенные в таблице 1, характеризуют единичный поток трафика от сервера к пользователю, т.е. поток, который может передаваться на уровне абонентского доступа (в случае, если пользователь в данный момент получает только одну услугу) или на уровне агрегации, при условии отсутствия других активных пользователей.

Для установления взаимосвязи между значениями параметра Хёрста и субъективными оценками качества передачи видео был выбран метод SSCQE (Single Stimulus Continuous Quality Evaluation, Метод непрерывной оценки качества при одном источнике воздействия). Данный метод применяется для оценки качества передачи видео в условиях отсутствия эталонного источника видео, что максимально подводит эксперимент к реальным условиям предоставления видеослуг. Метод SSCQE предполагает непрерывную оценку качества видеопотока, что дает возможность оценивать каждый фрагмент тестируемого материала. Эксперты могут просматривать видеофрагмент только один раз, не имея при этом эталонного изображения. Для выставления оценок применяются бланки с непрерывной шкалой. Экспертам предлагают оценить общее впечатление от качества видео, и поставить ему отметку на вертикальной шкале. В данном случае для определения уровня качества использовались термины, хорошо знакомые и понятные экспертам, а именно: отлично, хорошо, удовлетворительно, плохо, неприемлемо [8].

В таблице 2 представлены субъективные оценки и значения параметра Хёрста для панорамного видео.

ТАБЛИЦА 2. Значения параметра Хёрста и оценки SSCQE панорамного видео на платформе «YouTube»

N	Оценки SSCQE, Ethernet	Параметр Хёрста через Ethernet	Оценки SSCQE, Wi-Fi	Параметр Хёрста через Wi-Fi
1	2	0,780	1,8	0,740
2	2,5	0,785	2,3	0,760
3	3	0,790	2,8	0,768
4	4,5	0,800	4,3	0,775

Проанализировав результаты в таблице 2 можно утверждать, что существует взаимосвязь между значениями параметра Хёрста и субъективными оценками качества передачи видео методом SSCQE.

Данные были аппроксимированы и была составлена логистическая кривая на рис. 2.

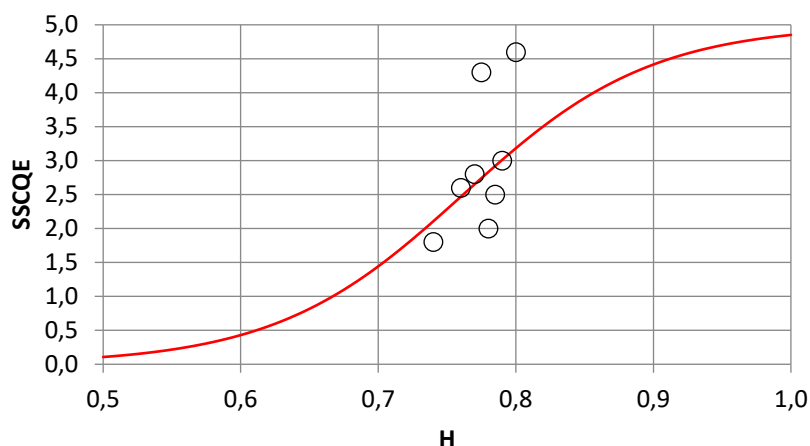


Рис. 2. График логистической кривой

Сравнивая результаты характеристик панорамного видео 360 градусов и параметра Хёрста можно утверждать, что трафик панорамного видео самоподобен при всех рассматриваемых качествах изображения.

Так же можно сделать вывод, что при большей нагрузке на сеть, трафик становится более самоподобным.

Очевидно, что взаимосвязь параметра Хёрста и субъективных оценок качества восприятия видеоизображений аналогична установленной взаимосвязи субъективных оценок метода MOS и объективных оценок R-фактора, применяемой для оценки качества передачи речи в пакетных сетях.

Следовательно, при широкомасштабных исследованиях зависимости параметра Хёрста от изменения состояния сети и взаимосвязанности с субъективными оценками, можно включить параметр Хёрста в метод объективной оценки качества передачи видео, что приведет к увеличению точности оценок качества восприятия.

В дальнейших исследованиях планируется изучение применения параметра Хёрста различных областях, таких как приложения дополненной реальности, очки дополненной реальности, голографические вентиляторы и т. д. В будущем, при реализации сетей 5G на территории Российской Федерации, так же нужно будет исследовать параметр Хёрста относительно новых параметров сети.

Список используемых источников:

1. Прокопьев, А. В. Самоподобие нагрузки в беспроводных сенсорных сетях для приложения сбора данных / А. В Прокопьев // 65-я научно-техническая конференция, посвященная Дню радио, Апрель 2010.
2. Кучерявый, А.Е. Сети связи общего пользования. Тенденции развития и методы расчета / А.Е. Кучерявый, А.И. Парамонов, Е.А. Кучерявый. – М.: ФГУП ЦНИИС. 2008.
3. Recommendation ITU-T P.10/G.100 «Vocabulary for performance, quality of service and quality of experience». ITU-T, Geneva, November, 2017.
4. Recommendation ITU-T G.1080 « Quality of experience requirements for IPTV services». ITU-T, Geneva, December, 2008.
5. Recommendation ITU-T G.1010 « End-user multimedia QoS categories». ITU-T, Geneva, November, 2001.

6. Recommendation ITU-T E.804 « QoS aspects for popular services in mobile networks». ITU-T, Geneva, September, 2014.
7. Маколкина, М.А. Параметр Хёрста как средство выявления аномальных изменений при передаче видеотрафика / М.А. Маколкина, А.В. Прокопьев, А.Е. Кучерявый // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании II Международная научно-техническая и научно- методическая конференция. 2013. С. 158-162.
8. Recommendation ITU-R BT.500-13 « Methodology for the subjective assessment of the quality of television pictures». ITU-T, Geneva, January, 2012.

Stepanov A., Makolkina M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Investigation of the relationship between subjective estimates of QoE and the Hearst parameter for augmented reality.

Augmented reality is one of the most promising technologies of the 21st century. Today, augmented reality technology is widely used in various fields: Internet, marketing, tourism, science, medicine and telecommunications. To determine user satisfaction with the quality of content in augmented reality, the quality of service and the quality of perception are used.

Key word: augmented reality, Quality of service, Quality of perception, Hearst parameter.

УДК 004.7
ГРНТИ 49.33.29

ЗАДАЧИ ИССЛЕДОВАНИЯ ТРАФИКА И КАЧЕСТВА ОБСЛУЖИВАНИЯ В САМООРГАНИЗУЮЩИХСЯ СЕТЯХ С ПОДВИЖНЫМИ ПОЛЬЗОВАТЕЛЯМИ

А. М. Тихонов, А. И. Парамонов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются вопросы совершенствования самоорганизующихся сетей с мобильными пользователями. На основе обзора технологий, используемых в существующих самоорганизующихся сетях, определены характеристики для исследования, такие как пропускная способность, задержка и надежность. В данной работе также рассматривается вопрос об изменении режима работы узлов с симплексного на дуплексный для обеспечения более рационального использования частотного диапазона сети.

самоорганизующиеся сети, сетевая модель, трафик и качество обслуживания

Введение

С каждым годом количество устройств, использующих беспроводные сети связи значительно увеличивается. Чтобы удовлетворить запросы современного общества, желающего в любое время суток оставаться на связи, в настоящее время можно заметить значительный рост и развитие технологий беспроводной передачи данных. Ежегодно появляются новые устройства, позволяющие передавать данные на более высоких скоростях, с меньшими задержками и с большей надежностью. Это ведет как к совершенствованию текущих моделей сетей связи, но и к поиску новых вариантов применения беспроводных технологий. Частным случаем являются самоорганизующиеся сети с подвижными пользователями (MANET-Mobile Ad-Hoc Network) [2, 3].

Описание технологии

В последнее время вырос интерес к мобильным одноранговым сетям (MANET), архитектура которых состоит из подвижных узлов. Сети MANET реализуют полностью децентрализованное управление при отсутствии базовых станций или опорных узлов. Данные сети способны к самоорганизации по причине того, что все их узлы являются не только конечными пользователями, а также являются маршрутизаторами-ретрансляторами, передавая пакеты других пользователей от узла к узлу и участвуя в определении местонахождения маршрутов к ним. Такие сети могут состоять из десятков, сотен и даже тысяч узлов [2]. Топология сети быстро меняется и не имеет фиксированного количества соединения узлов. В связи с этим, площадь покрытия самоорганизующейся сети не обязана быть постоянной [1].

В отличие от сетей с иерархической структурой и централизованным управлением, одноранговые сети без инфраструктуры состоят из узлов одного типа. Каждый узел имеет набор программно-аппаратных средств, позволяющих

напрямую организовать передачу данных от источника к приемнику, при наличии такого пути. Данный метод позволяет распределить нагрузку на сеть и повышает общую пропускную способность сети. Даже, в случае, если исходный и целевой мобильные узлы не находятся в зоне охвата друг друга, пакеты данных пересылаются на целевой мобильный узел путем ретрансляции передачи через промежуточные мобильные узлы. [1] На рис. 1 представлена структурная схема модели непосредственного взаимодействия узлов сети.

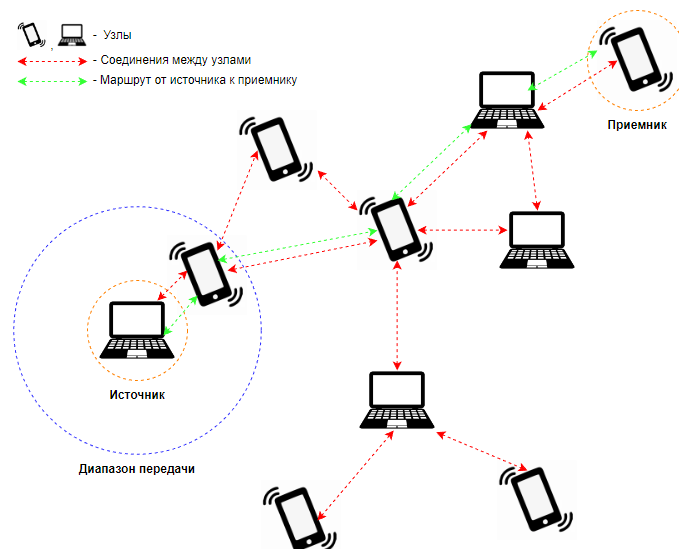


Рис. 1. Структура модели непосредственного взаимодействия узлов

Несмотря на то, что данная технология полностью не раскрыла свой потенциал, она уже используется во многих сферах. В ближайшем будущем данная технология найдет применение в таких концепциях как умный дом, VANET, FANET и др.

Особенности самоорганизующихся сетей с подвижными пользователями

Сети класса MANET (Mobile Ad-Hoc network) имеют определенные особенности, которые необходимо учитывать при моделировании сети:

- в связи с высокой мобильностью узлов необходимо учитывать стремительное изменение топологии сети [3];

- поскольку сеть не имеет базовой станции и площади ее покрытия, необходимо учитывать расстояние между узлами;

- невозможность одновременного приема/передачи на одной частоте.

Так как пропускная способность достаточно ценный ресурс в таких сетях, хорошим тоном будет минимизировать служебный трафик. Следует конфигурировать сеть таким образом, чтобы отсутствовали периодические сообщения для выявления соседних узлов. Новые узлы следует подключать к сети по запросу [1].

Постановка задачи

В данной работе проводится постановка задач для исследования имитационной модели сети ad-hoc в качестве узлов которой представлены подвижные устройства. Поскольку особенностью данных узлов является симплексный режим работы, данный режим вносит ограничение по пропускной способности сети.

Основной задачей на исследование самоорганизующейся сети с подвижными пользователями является разработка ее имитационной модели в которой произойдет смена симплексного режима работы на дуплексный. Данный режим позволит не только параллельно передавать и принимать информацию, а также увеличит пропускную способность сети.

Так же второй задачей является сравнительный анализ задержек и потерь в сетях с симплексным режимом работы и дуплексным.

Заключение

Подводя итоги можно сказать, что самоорганизующиеся сети в будущем могут быть использованы в большом количестве концепций. Их должное развитие позволит быстро развертывать сети с подвижными пользователями без использования базовых станций.

В данной работе был приведен обзор на технологию MANET, рассмотрены особенности и поставлены задачи на исследование модели самоорганизующейся сети с подвижными пользователями.

Список используемых источников:

1. k Nearest Neighbor Search for Location-Dependent Sensor Data in MANETs. [Электронный ресурс] / Yuka Komai; Yuya Sasaki; Takahiro Hara; Shojiro Nishio; IEEE, 2015. URL: <https://ieeexplore.ieee.org/document/7126920> (Дата обращения 08.11.2022).
2. Что такое MANET или почему WiFi не решение всех телекоммуникационных проблем. [Электронный ресурс] // habr.com, 16.10.2013. URL: <https://habr.com/ru/post/197860/>. (Дата обращения 09.11.2022).
3. Дорохова А. А., Парамонов А. И. Исследование трафика и качества обслуживания в самоорганизующихся сетях на базе БПЛА // Информационные технологии и телекоммуникации. 2016. Том 4. №2. С.12-25.

Tikhonov A., Paramonov A.

The Bonch-Bruевич Saint Petersburg State University of Telecommunications

Tasks for traffic and quality of service research in self-organizing networks with mobile users. The article deals with the issues of improvement of self-organizing networks with mobile users. Based on the overview of technologies used in existing self-organizing networks, characteristics for study such as throughput, latency, and reliability are defined. In addition to this, the article discusses the issue of changing the operating mode of nodes from simplex to duplex to provide more rational use of the network frequency range.

Key words: *self-organizing networks, network model, traffic and quality of service.*

УДК 621.391
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ПАРАМЕТРОВ ТРАФИКА УСТРОЙСТВ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ В СЕТЯХ СВЯЗИ

В. А. Хасанова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Дополненная реальность с каждым годом все активнее проявляется в нашей повседневной жизни. С помощью новых устройств и приложений меняется наша жизнь, а также общее представление о сетях связи. Исследование параметров трафика входит в комплекс моделей и методов для дополненной реальности. Были исследованы параметры трафика устройств дополненной реальности, проектора LG HF85LSR и смартфона. Анализ трафика проведен с использованием 3D-видео и трех приложений с функциями дополненной реальности. Результаты продемонстрированы с помощью графиков, подведены итоги исследования.

дополненная реальность (ДР), пропускная способность, трафик, исследование трафика, параметры трафика, Wireshark

Определение ДР

Дополненная реальность (AR, Augmented Reality) позволяет с помощью различных устройств накладывать виртуальные объекты на реальную среду в режиме реального времени.

Актуальность ДР

Приложения, использующие технологию ДР, приобрели огромную популярность у пользователей смартфонов. На рис. 1 видно, что количество пользователей мобильной дополненной реальности неуклонно растет от года к году. Так, предположительно, к 2024 году количество активных пользователей ДР на смартфонах будет составлять 1,73 миллиарда человек [1].

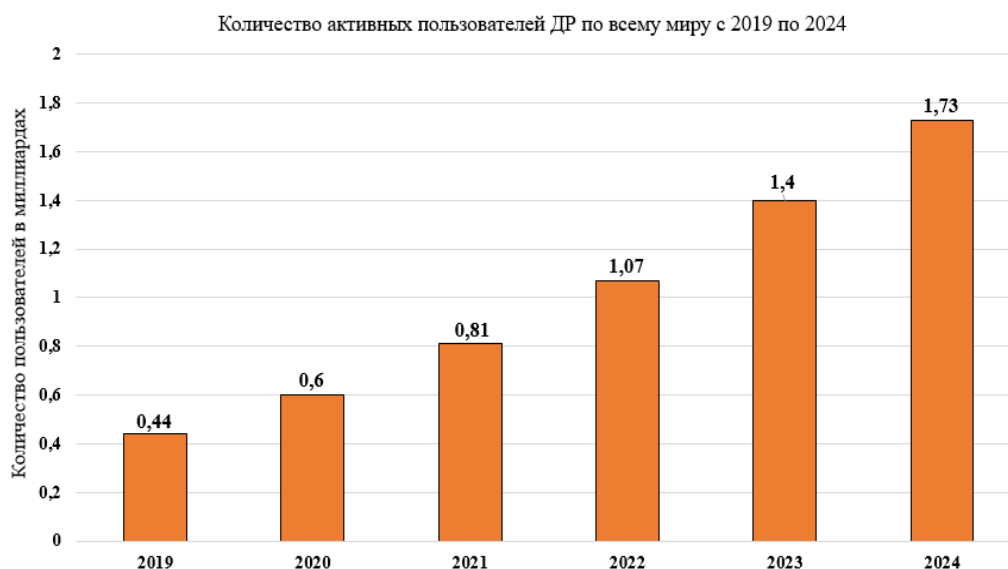


Рис. 1. Статистика активных пользователей мобильной дополненной реальности по всему миру с 2019 по 2024 года

На российском рынке ДР также наблюдается стремительный рост. По данным отчета аналитического агентства «ТМТ Консалтинг» совместно с компанией Huawei, рынок AR/VR с 2020 года по 2025 год должен увеличиться в 5 раз [2]. Прогноз увеличения российского рынка AR/VR показан на рис. 2.

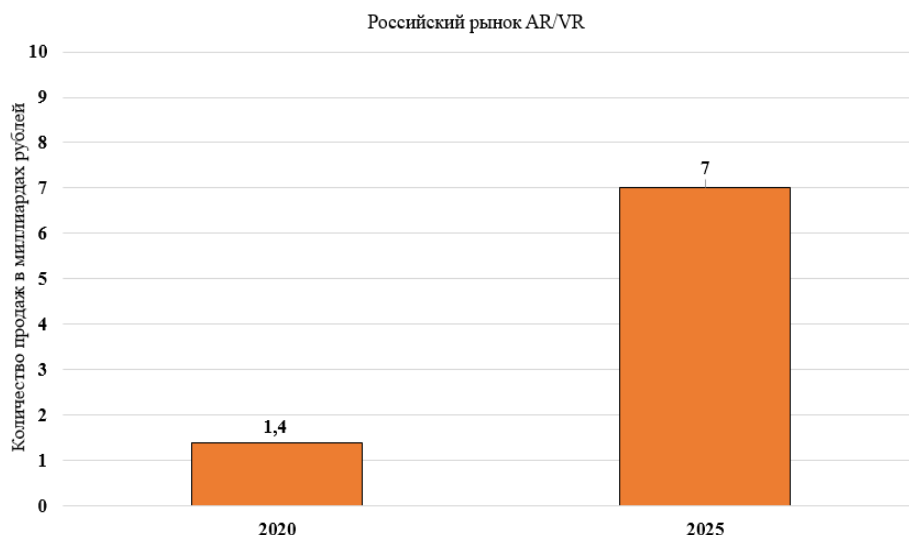


Рис. 2. Прогноз увеличения российского рынка AR/VR с 2020 по 2025 года

Перехват и анализ трафика 3D-видео в различных разрешениях

Исследование трафика проводилось с использованием 3D-видео, найденном на видеохостинге «YouTube», в лаборатории Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича. Трансляцию видеоматериала осуществлял проектор LG HF85LSR. В качестве сетевой технологии был выбран Wi-Fi 802.11ac. Захват трафика производился при помощи программы Wireshark, так как в нем есть функции, необходимые для сбора и анализа данных [3]. Модель сети, осуществляющая трансляцию видеоматериала на проектор, показана на рис. 3.

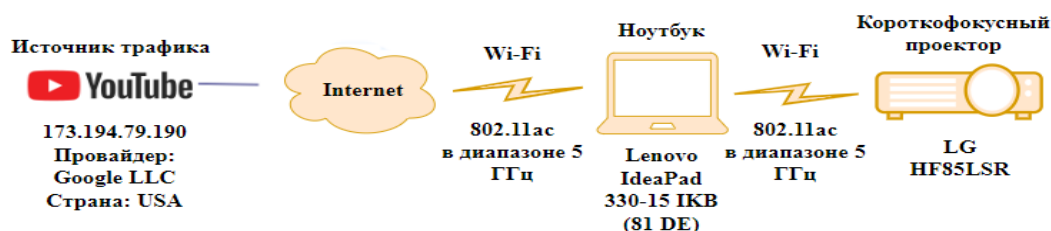


Рис. 3. Модель сети, осуществляющая трансляцию видеоматериала на проектор

В ходе выполнения эксперимента воспроизводились видео в разрешениях 144p, 720p и 1080p в течение 5 минут. Захватив пакеты в Wireshark, был проведен анализ полученных данных. Все данные были сопоставлены на одном графике для точной оценки результатов. Полученный график показывает, что при разрешении 144p было захвачено минимальное количество пакетов, в остальных

же случаях разница была несущественной. Максимальный объем информации был предоставлен в первые 15 секунд, после чего каждые 5-10 секунд загружались новые пакеты, среднее количество которых оставалось практически на одном уровне. Данное правило действовало для всех разрешений. Обобщенный график количества пакетов в единицу времени показан на рис. 4.

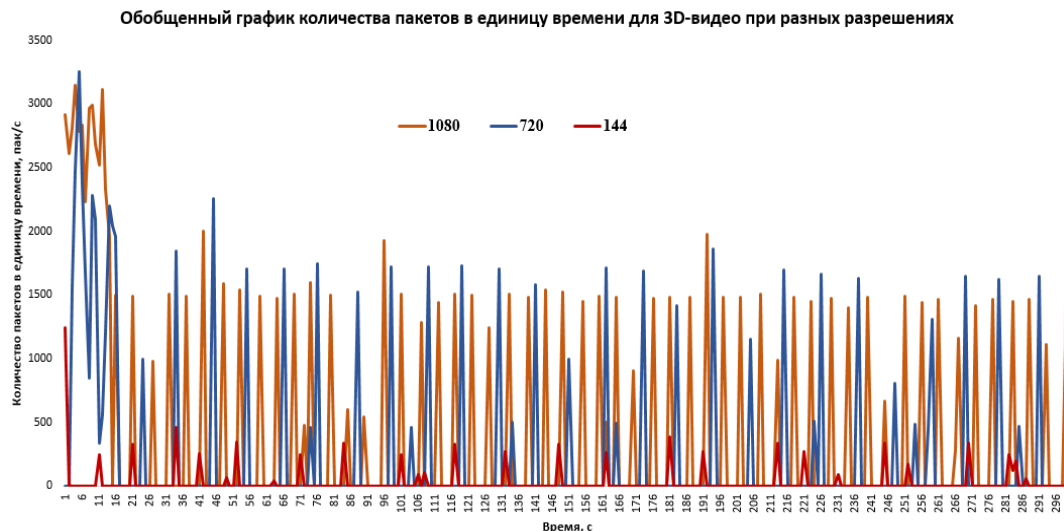


Рис. 4. Обобщенный график количества пакетов в единицу времени для 3D-видео при разных разрешениях

Захватив данные о пропускной способности для различных разрешений, был построен обобщенный график, объединяющий все результаты. Он представлен на рис. 5. Самый низкий показатель пропускной способности выявился у 3D-видео с разрешением 144р. Графики пропускной способности для 3D-видео с разрешением 720р и 1080р идут практически на одном уровне. Это говорит о том, что качество изображения у видео с такими разрешениями примерно идентично, что и подтверждалось при просмотре.

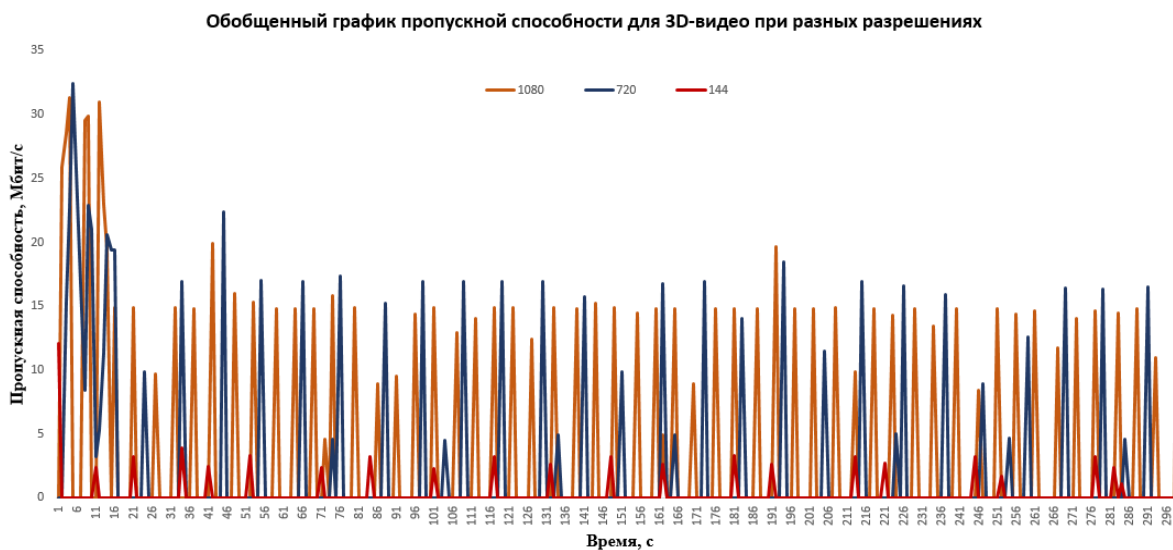


Рис. 5. Обобщенный график пропускной способности для 3D-видео при разных разрешениях

Перехват и анализ трафика приложений дополненной реальности

Следующий эксперимент проводился с использованием ноутбука в роли «захватчика» трафика, при этом целью стали не устройства, а приложения дополненной реальности на смартфоне. Структура сети, осуществляющая передачу данных приложений ДР, представлена на рис. 6.

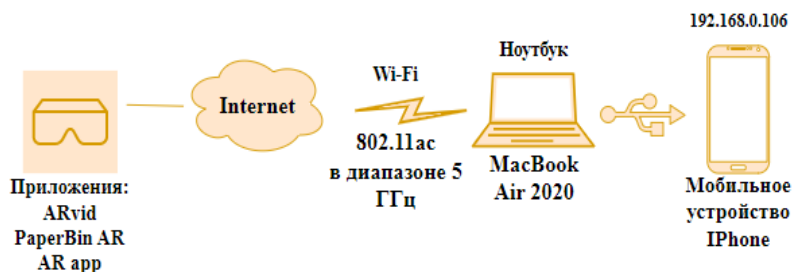


Рис. 6. Структура сети, осуществляющая передачу данных приложений дополненной реальности

Обобщенный график количества пакетов в единицу времени показан на рис. 7. Всплески количества пакетов наблюдались при активном использовании приложения, совершении различных действий. Другими словами, в определенный промежуток времени происходил обмен данными между устройством и пользователем. Более частый обмен данными был в приложении «PaperBin AR», так как оно является игровым, то есть в нем происходит постоянное взаимодействие с виртуальными объектами. В приложении «ARvid» есть возможность добавлять виртуальные объекты в реальный мир, но сам процесс использования был скорее визуальным, нежели игровым. Поэтому обмен данными происходил реже, но всплески были больше. Требовалось прогрузить объекты дополненной реальности, а затем наблюдать за их взаимодействием с реальным миром.

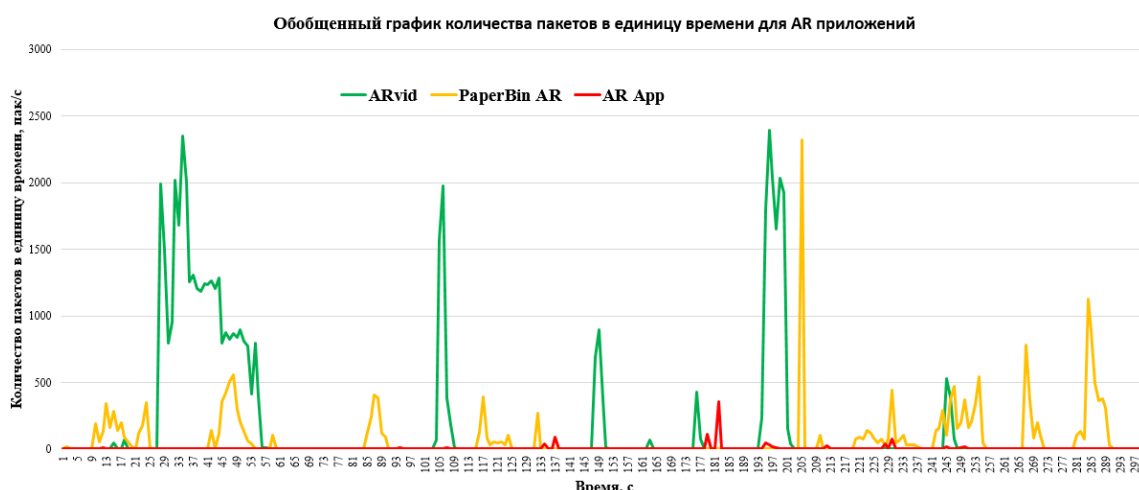


Рис. 7. Обобщенный график количества пакетов в единицу времени для AR приложений

На рис. 8 показан обобщенный график пропускной способности приложений ДР. Больше всего данных было получено из приложения «ARvid».

На практике оно являлось самым проработанным, насыщенным и наполненным различными функциями. «ARapp» показало себя, как менее содержательное приложение, что также подтверждается при просмотре графика пропускной способности.



Рис. 8. Обобщенный график пропускной способности для AR-приложений

Заключение

Низкое разрешение (144p) у видео не позволяло обнаружить желаемый 3D-эффект изображения, так как оно было значительно размыто, зрение было расфокусировано, а также была видна раскадровка. При высоком разрешении (720p и 1080p) 3D-эффект отчетливо проявлялся, происходило полное погружение в происходящее на экране. При сравнении характеристик 3D-видео можно подтвердить увиденное при просмотре. К примеру, пропускная способность 3D-видео - 293000 бит/с для 144p, 4085000 бит/с для 1080p.

Более высокая нагрузка на сеть создается приложениями, использующими более детальные виртуальные объекты и более обширные функции. Рост качества приложений и предоставляемых ими услуг приводит к увеличению значений всех параметров трафика [4].

Увеличение пропускной способности – естественное следствие при повышении качества как приложений, так и видео. Профессионально разработанные приложения и видео с насыщенными эффектами и детальными виртуальными объектами позволяли загружать и анализировать гораздо большее количество данных.

Список используемых источников:

1. Number of mobile augmented reality (AR) active users worldwide from 2019 to 2024 [Электронный ресурс] // Statista. URL: <https://www.statista.com/statistics/1098630/global-mobile-augmented-reality-ar-users/> (дата обращения: 1.10.22).
2. TMT Consulting. Российский рынок дополненной и виртуальной реальности (AR/VR) / TMT Consulting, Huawei // TMT Consulting, Huawei - 2021. - С.1-2.
3. Wireshark – приручение акулы [Электронный ресурс] // Хабр. URL: <https://habr.com/ru/post/204274/> (дата обращения: 11.10.22).

4. М.А. Маколкина. Разработка и исследование комплекса моделей трафика и методов оценки качества для дополненной реальности/ Маколкина М.А. // Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича» на кафедре сетей связи и передачи данных - 2019. - С.1-40.

Hasanova V.A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Research on the traffic parameters of augmented reality devices in communication networks. Augmented reality is becoming more and more active in our daily lives every year. With the help of new devices and applications, our lives are changing, as well as the general idea of communication networks. The study of traffic parameters is part of the set of models and methods for augmented reality. The traffic parameters of augmented reality devices, LG HF85LSR projector and smartphone were investigated. The traffic analysis was conducted using 3D video and three augmented reality apps. The results are shown in graphs, and the results of the study are summarized.

Key words: *augmented reality (AR), throughput, traffic, traffic research, traffic measurement, Wireshark.*

УДК 621.396.99
ГРНТИ 49.33.29

ОБЗОР ТЕХНОЛОГИИ ONAP ДЛЯ СЕТЕЙ БУДУЩЕГО ПОКОЛЕНИЯ

Ю. С. Шипицын, М. А. Котов, А. С. А Мутханна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Сфера услуг телекоммуникаций постоянно прогрессирует, сети нового поколения требуют высокий уровень обслуживания с использованием автоматизации процессов. В связи с этим предлагается рассмотреть ONAP - проект с открытым исходным кодом, реализуемый Linux Foundation Networking (LFN), целью которого является разработка широко используемой платформы для оркестровки и автоматизации физических и виртуальных элементов сети с полным управлением жизненным циклом. ONAP может принести еще больше пользы, если его использовать для создания новых услуг, поддерживающих новые бизнес-модели в различных вертикалях, которые появятся в результате внедрения 5G [1].

виртуализация сетевых функций, Контейнеры, ONAP, сотовая связь

В последние годы облачные вычисления стали одним из ключевых направлений в сфере ИТ. Виртуализация инфраструктуры сыграла важнейшую роль в оптимизации использования ресурсов и обеспечила беспрецедентную гибкость управления.

Контейнеризация - это технология, которая предоставляет средства для инкапсуляции приложений без использования виртуальных машин. Наиболее распространенным решением является запуск контейнеров поверх уже работающих виртуальных машин, что не требует дополнительного времени загрузки ОС.

Технология использования контейнеров повлекла за собой развитие различных механизмов их оркестрации для автоматизации развертывания, масштабирования и управления приложениями, например, Kubernetes.

Первоначально телекоммуникации были просто средством, обеспечивающим связь с облачным вычислениями (для пользователей или для объединения центров обработки данных). С тех пор многие телекоммуникационные компании сами стали поставщиками услуг облачных технологий, пытаясь использовать присущие им преимущества (например, большую пропускную способность сети) для выхода на новый рынок. Тем не менее, реальное воздействие на сектор телекоммуникаций началось с "софтверизации" сети. Стандартные сетевые функции начали переходить с проприетарного оборудования на компьютеры Commercial-Off-The-Shelf (COTS), упрощая такие задачи, как обновления функционала, исправление ошибок или масштабирование услуг. Следующим логическим шагом является виртуализация этих сетевых функций путем превращения сетевого оборудования в виртуальные объекты. Именно это является движущей силой концепции Network Function Virtualization (NFV). Новые виртуальные

устройства, отвечающие парадигме NFV, могут быть созданы по запросу или развернуты в любом облаке с достаточным количеством доступных ресурсов и масштабироваться в зависимости от нагрузки.

Software Defined Networking (SDN) - это еще одна родственная технология, которая разделяет плоскости управления и данных и централизует решения в контроллере. Эти уровни разделяются с помощью четко определенного API между коммутаторами и контроллером. Наиболее популярным API в настоящее время является OpenFlow. SDN позволяет управлять потоками трафика из централизованной точки, упрощая создание новых и перемещение существующих инстансов NFV без прекращения обслуживания конечных пользователей [2].

Инфраструктура NFV, поддерживаемая сетью с поддержкой SDN, представляет собой сложную среду, которая также требует архитектуры для управления и оркестрации. Для этой цели группа ETSI NFV определила структуру управления и оркестрации (MANO). Она стандартизирует функциональные возможности для обеспечения конфигурации VNF, а также включает в себя оркестрацию и управление физическими и виртуальными ресурсами, которые требуются VNF.

ONAP - это набор ETSI MANO с дополнительными возможностями. Она появилась в результате слияния ECOMP (Enhanced Control, Orchestration, Management and Policy) и Open-O и находится под эгидой Linux Foundation. В настоящее время она имеет сильный импульс с участием поставщиков, которые охватывают более 60% мобильных клиентов по всему миру.

Это делает ONAP интересной платформой для анализа того, как контейнеры могут помочь в построении инфраструктуры NFV [1]. В данной статье рассматриваются архитектурные особенности платформы ONAP и сферы её применения.

Проект Open Network Automation Platform (ONAP) направлен на удовлетворение растущей потребности в платформе автоматизации различных процессы жизненного цикла сетевого оборудования, чтобы предоставлять различные сетевые услуги, используя при этом существующие инвестиции.

До появления ONAP операторы телекоммуникационных сетей были вынуждены поддерживать масштаб и стоимость ручных изменений, необходимых для внедрения новых услуг, начиная с установки нового оборудования в центре обработки данных и заканчивая модернизацией оборудования клиентов.

В настоящее время многие операторы стремятся использовать Software Defined Network (SDN) и Network Function Virtualization (NFV) для повышения скорости предоставления услуг, упрощения совместимости и интеграции оборудования, а также снижения общих капитальных и операционных затрат [3].

ONAP решает проблемы путем разработки возможностей автоматизации в огромных масштабах для физических и виртуальных элементов сети. Это способствует повышению гибкости услуг за счет поддержки моделей данных для быстрого развертывания услуг и ресурсов, предоставления общего набора

открытых и совместимых REST API Northbound, а также поддержки интерфейсов к сетям на основе моделей. Такой подход позволяет операторам сетей и облаков оптимизировать физическую и виртуальную инфраструктуру с точки зрения стоимости и производительности; в то же время использование стандартных моделей ONAP снижает затраты на интеграцию и развертывание разнородного оборудования, сводя к минимуму фрагментацию управления.

ONAP ориентирован на моделирование информации и соответствующих функций управления на уровнях услуг и ресурсов, в то время как вся его экосистема охватывает множество отраслей и бизнес-сценариев, от продуктов конечного пользователя до уровня инфраструктуры.

На рис. 1 представлено упрощенное функциональное представление архитектуры, которое показывает роль нескольких ключевых компонентов:

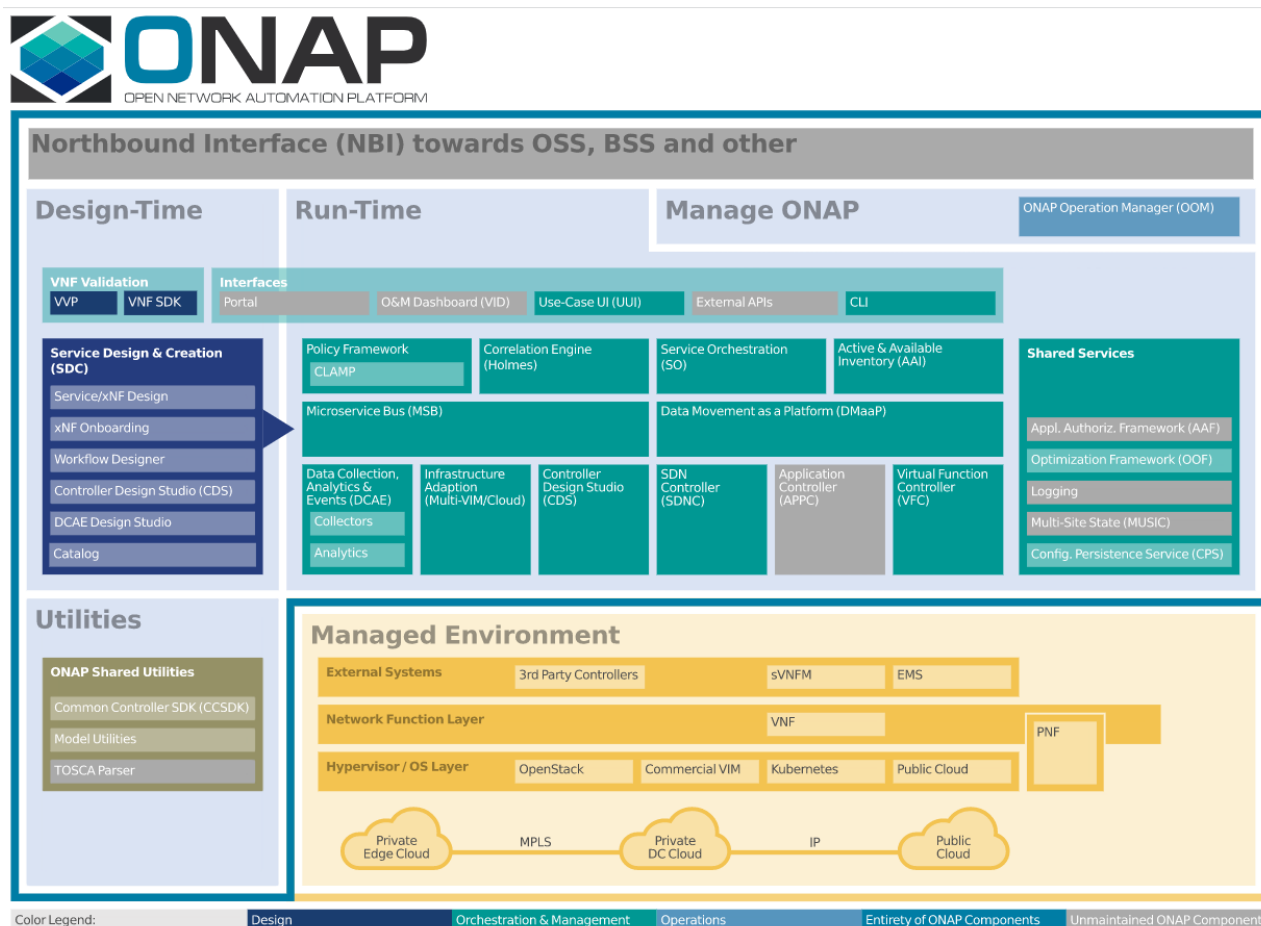


Рис. 1. Обзор архитектуры

- Design time environment предоставляет услуги и ресурсы для внедрения в ONAP
 - External API обеспечивает функциональную совместимость для платформы ONAP.
 - Runtime environment предоставляет структуру оркестрации и контроля для автоматизированного создания и конфигурирования сервисов и ресурсов. Multi-VIM/Cloud обеспечивает взаимодействие с облаком для рабочих нагрузок

ONAP. Структура мониторинга обеспечивает управление замкнутым контуром управления для динамического восстановления, масштабирования и обновления.

- ONAP Operations Manager обеспечивает возможность развёртывания облачных решений в средах, управляемых Kubernetes.

- ONAP Shared Services предоставляет общие возможности для модулей ONAP. ONAP Optimization Framework (OOF) предоставляет декларативный подход для создания и запуска приложений оптимизации, таких как Homing/Placement и Change Management Scheduling Optimization. Общие утилиты ONAP предоставляют утилиты для поддержки компонентов ONAP. [4]

Высокоуровневая архитектура ONAP состоит из различных программных подсистем, которые в целом разделены на среду времени проектирования и среду времени исполнения для выполнения того, что разработали платформы. Сообщество ONAP определяет шаблоны для различных вариантов использования, например:

- Voice Over LTE (VoLTE)
- Customer Premise Equipment (CPE)
- 5G
- Cross Domain and Cross Layer VPN (CCVPN)
- Broadband Service (BBS)

Таким образом, способность сетевых операторов использовать возможности, возникающие благодаря новым технологиям, таким как облако и 5G, требует значительного сокращения фрагментации и сложности в области поддержки эксплуатации. Open Networking Automation Platform (ONAP) - это инициатива с открытым исходным кодом, направленная на решение этой проблемы путем внесения ясности в отраслевые ожидания. Она обеспечивает модульную архитектуру и общую среду для ряда операционных процессов, а также сквозное управление жизненным циклом услуг в различных сетях и технологиях. ONAP может принести еще больше пользы, если его использовать для создания новых услуг, поддерживающих новые бизнес-модели в различных вертикалях, которые появятся в результате внедрения 5G. [5]

Список используемых источников:

1. Artem Volkov, Kovalenko Vadim, Ibrahim A. Elgendy, Ammar Muthanna, and Andrey Koucheryavy. "DD-FoG: Intelligent Distributed Dynamic FoG Computing Framework." *Future Internet* 14, no. 1 (2022): 13.

2. Khakimov Abdukodir, Ibrahim A. Elgendy, Ammar Muthanna, Evgeny Mokrov, Konstantin Samouylov, Yassine Maleh, and Ahmed A. Abd El-Latif. "Flexible architecture for deployment of edge computing applications." *Simulation Modelling Practice and Theory* 114 (2022): 102402.

3. Fernández-Nandín, A., Gil-Castiñeira, F., & González-Castaño, F. J. ONAP Architectures for Network Function Virtualization // *Broadband Communications, Networks, and Systems*. 2018. С. 62–71.

4. ONAP Architecture Overview [Электронный ресурс]. URL: <https://docs.onap.org/en/latest/platform/architecture/index.html> (дата обращения 10.11.2022).

5. ONAP and the telecom industry's open-source journey [Электронный ресурс]. URL: <https://www.ericsson.com/en/reports-and-papers/white-papers/onap-and-the-telecom-industrys->

open-source-journey

(дата

обращения

10.11.2022).

Shipitsyn Y., Kotov M., Muthanna A. S. A*The Bonch-Bruевич Saint-Petersburg State University of Telecommunication**An Overview of ONAP technology for next-generation networks.*

The field of telecommunication services is constantly progressing, with next-generation networks requiring a high level of service using process automation. In this context, it is proposed to consider ONAP, an open-source project implemented by Linux Foundation Networking (LFN), which aims to develop a widely used platform for orchestration and automation of physical and virtual network elements with full lifecycle management. ONAP can bring even more value when used to create new services that support new business models in the various verticals that will emerge from the 5G implementation. [1]

Key words: Network Functions Virtualization, Containers, ONAP, Cellular.

УДК 004.732
ГРНТИ 49.43.29

ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК БЕСПРОВОДНОЙ ЛОКАЛЬНОЙ СЕТИ ОБЩЕЖИТИЯ СПБГУТ «ДАЛЬНЕВОСТОЧНОЕ»

С. А. Щеглов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В ходе выполнения данной работы были исследованы характеристики беспроводной локальной сети общежития СПбГУТ «Дальневосточное». С помощью программных средств был осуществлён анализ беспроводной локальной сети, выявлены её проблемные места. По завершению анализа были даны рекомендации по устранению обнаруженных недостатков.

радиообследование, радиоинспектирование, беспроводная локальная сеть, Wi-Fi.

Быстрое развитие технологий беспроводных сетей Wi-Fi привело к повсеместному их применению. Причина этого – мобильность технологии, то есть свобода от проводов. Увеличение количества устройств, требующих интернет-соединения, растёт с каждым годом также, как и растёт потребность в беспроводных сетях. Однако чтобы обеспечить стабильное соединение и хороший уровень сигнала беспроводной сети, пользователю недостаточно просто купить точки доступа и включить их. Требуется правильно провести планирование желаемой сети.

Для проведения радиообследования было выбрано общежитие "Дальневосточное", в котором проживает значительное количество студентов СПбГУТ.

Сначала был произведен визуальный осмотр общежития на наличие точек доступа. В процессе обхода было обнаружено семьдесят девять точек доступа WEP-12ac компании Eltex стандарта IEEE 802.11ac [2]. Далее проведено радиообследование общежития, начиная с первого этажа и заканчивая пятнадцатым. В ходе данного обследования, для детального анализа был выбран девятый этаж. Первоочередную важную роль имел сигнал от точек доступа до устройств, находящихся в жилых комнатах, однако из-за того, что заход в комнаты, где проживают студенты не представлялся возможным, было решено построить компьютерную модель беспроводной локальной сети, предварительно определив где находятся, на каких каналах и в каких диапазонах работают точки доступа.

На плане этажа отмечены такие препятствия на пути распространения сигнала, как стены с соответствующим им коэффициентом затухания:

- сухая стена, выделенная коричневым цветом, с коэффициентом затухания 3 дБ;
- кирпичная стена, выделенная красным цветом, с коэффициентом затухания 10 дБ;
- бетонная стена, выделенная светло-коричневым цветом, с коэффициентом затухания 12 дБ;

- стена из шлакоблоков, выделенная серым цветом, с коэффициентом затухания 5 дБ;
- окна, выделенные голубым цветом, с коэффициентом затухания 3 дБ;
- шахта лифта, выделенная черным цветом, с коэффициентом затухания 30 дБ.

С помощью программы Nomedale были нанесены на план точки доступа и распределены их каналы в соответствии с измерениями. Конечная компьютерная модель была создана и получена в программе Ekahau Pro. Было выявлено, что точки доступа работают одновременно в двух частотных диапазонах.

На рис. 1 ниже представлен готовый план девятого этажа общежития «Дальневосточное». Фиолетовым цветом показан номер канала, на котором работают точки доступа в частотном диапазоне 2,4 ГГц, красным – в диапазоне 5 ГГц.

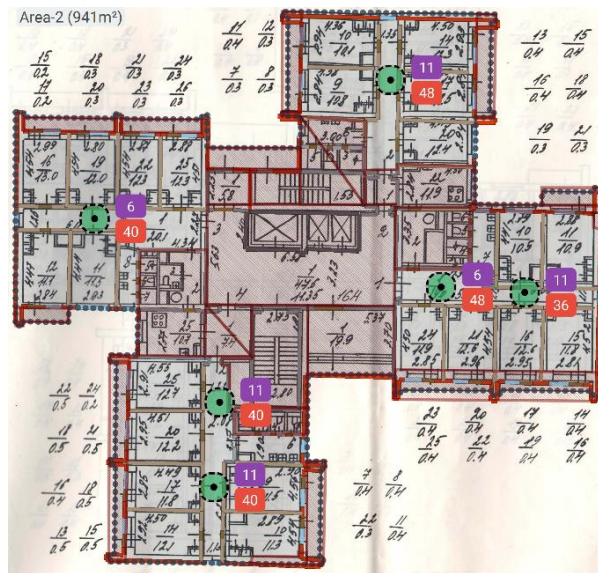


Рис. 1. Готовый план девятого этажа

Прежде чем собирать данные, следует определиться с требованиями к покрытию. В табл. 1 наглядно показаны требования к беспроводной сети для обеспечения стабильного соединения, а также бесперебойной работы в двух частотных диапазонах.

ТАБЛИЦА 1. Требования к беспроводной сети

Требования к сети		
2.4 ГГц	Минимальный уровень сигнала	-67.0 дБм
	Минимальная скорость передачи данных	12 Мбит/с
	Максимальная канальная интерференция	2
5 ГГц	Минимальный уровень сигнала	-67.0 дБм
	Минимальная скорость передачи данных	12 Мбит/с
	Максимальная канальная интерференция	1

Во-первых, рассмотрим уровень сигнала. На рис. 2 показаны уровни сигналов в двух частотных диапазонах.



Рис. 2. Уровень сигнала в частотном диапазоне 2,4 ГГц (а) и 5 ГГц (б)

Можно убедиться, что мощность сигнала в двух частотных диапазонах соответствует выставленным требованиям. В среднем уровень сигнала варьируется от -65 дБм до -45 дБм, что является хорошим показателем.

Во-вторых, следует обратить внимание на скорость передачи данных от точек доступа. Для замера скорости был выбран интернет-ресурс SpeedTest. После замера выяснилось, что скорость на скачивание составляет примерно 13 Мбит/с, а на загрузку данных около 25 Мбит/с, что удовлетворяет выставленному требованию к сети.

В-третьих, надо проанализировать канальную интерференцию беспроводной сети. Она бывает как межканальной, так и внутриканальной [3]. В данном случае проблема проявляется в виде внутриканальной интерференции. Если в диапазоне 2,4 ГГц существует всего три непересекающихся канала: 1, 6 и 11, то в 5 ГГц все каналы являются непересекающимися. В данном случае интересно, что канальная интерференция встречается только в частотном диапазоне 5 ГГц, потому что точки доступа находятся на близком друг от друга расстоянии и имеют одинаковые каналы. В другом же диапазоне тоже встречаются точки доступа с одинаковыми каналами, однако они находятся не слишком близко друг к другу. Чтобы решить данную проблему достаточно лишь провести верное радиочастотное планирование, проще говоря, распределить каналы между точками доступа так, чтобы каналы не пересекались. На рис. 3 представлен итоговый вариант локальной беспроводной сети.

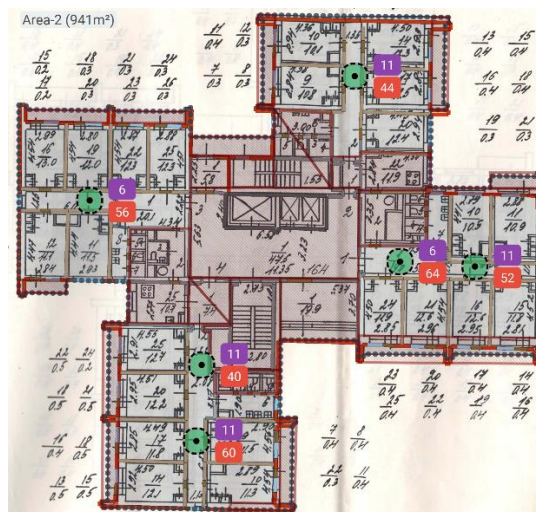


Рис. 3. Итоговый вариант локальной беспроводной сети

В данной работе была рассмотрена беспроводная локальная сеть в общежитии «Дальневосточное». С помощью визуального осмотра в этой сети было найдено 79 точек доступа. При помощи программ Ekahau Pro и Homedale была подробно проанализирована работа сети девятого этажа. Этими же программными средствами удалось выявить проблему внутриканальной интерференции точек доступа и исправить её посредством правильного распределения каналов.

Список используемых источников:

1. David D. Coleman; David A. Westcott. CWNA Certified Wireless Network Administrator Study Guide Exam CWNA-108 Sixth Edition – Copyright © by John Wiley & Sons, Inc., Indianapolis, Indiana – 2021. – 1091 с.
2. Matthew S. Gast. 802.11ac: A Survival Guide – Copyright © Matthew S. Gast. Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472. – 2013. – 154 с.
3. Викулов А. С., Парамонов А. И. Анализ основных видов помех в задаче планирования сетей Wi-Fi с высокой плотностью пользователей // Информационные технологии и телекоммуникации. – 2018. Том 6. № 1. – С. 21–31.
4. Основы построения беспроводных локальных сетей стандарта 802.11: Пер. с англ. - М.: Издательский дом "Вильямс", 2004. - 304 с.
5. Пролетарский А.В., Баскаков И.В., Федотов Р.А. Бобков А.В. Чирков Д.Н. Платонов В.А. Беспроводные сети Wi-Fi – НОУ «ИНТУИТ» - 2016. – 284 с.

Shcheglov S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Study of the characteristics of the wireless local area network of the «Dalnevostochnoe» dormitory of St.Petersburg State University of Technology.

In the course of this work we investigated the characteristics of the wireless local area network of St. Petersburg State University of Telecommunications "Dalnevostochnoe" dormitory. Using software tools the analysis of the wireless local area network was carried out, its problem areas were identified. Upon completion of the analysis, recommendations were given to eliminate the problems.

Key words: radio survey, radio inspection, wireless local area network, Wi-Fi.

Секция 3.3.**Мультисервисные телекоммуникационные системы и технологии**

УДК 654.1
ГРНТИ 50.41.23

АНАЛИЗ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ АППАРАТА ТЕОРИИ ИГР ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССОВ В ИНФОКОММУНИКАЦИЯХ

К. В. Белозеров, С. В. Кисляков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья - это обзор найденных исследовательских работ, касающихся применения теории игр для решения задач в различных областях человеческой деятельности. Особое внимание уделено работам в области инфокоммуникаций. Анализируется возможность использования аппарата теории игр для задач управления и эксплуатационной поддержки сетей связи.

теория игр, инфокоммуникационные системы, информационная безопасность, многоагентные системы.

В последние годы игровые модели получили широкое применение для описания сложных систем. Теория игр (ТИ) — раздел прикладной математики, с помощью которого можно исследовать поведение нескольких “игроков” и принятые ими решения в условиях следования собственным интересам. ТИ находится на стыке компьютерной науки и направлена на изучение и создание алгоритмов для стратегий. Результаты таких исследований нашли свое применение в различных сферах, таких как: социология, экономика, экология, бизнес-управление и др.

В инфокоммуникациях она пока применялась редко, хотя некоторые задачи, такие, например, как балансировка трафика или маршрутизация трафика, могли бы решаться через применение этого математического аппарата. Основываясь на природе ряда процессов, имеющих место в инфокоммуникациях, можно надеяться на успешное применение ТИ в задачах управления инфокоммуникациями - управлении неисправностями, конфигурацией, техническим учетом, производительностью и безопасностью, эксплуатацией инфраструктуры.

Применение теории игр

ТИ – это средство для моделирования и изучения взаимодействия между субъектами, заинтересованными «в себе» [1]. Она изучает проблемы, связанные с разработкой стратегий взаимодействия, которые позволят максимизировать благосостояние агента в случае взаимодействия нескольких агентов. В [1] выработка рекомендаций для агентов является главной задачей, решаемой при помощи ТИ. Стратегия агента – это система правил, которая определяет поведение агента на каждом ходе. Когда стратегии агентов пересекаются, образуется ситуация, в которой каждый агент получает определенный результат. Результат может быть как положительным так и отрицательным. Выбор стратегии основан на получении желаемого в самый короткий срок, но нельзя забывать про шаги противоположного агента, так как они тоже влияют на ситуацию в целом.

В инфокоммуникационных системах очень актуальна проблема защиты информации от различных угроз. Многие исследователи предлагают использовать ТИ в качестве математической основы при анализе и построении систем защиты информации. В [2] говорится, что в любой системе защиты информации есть две стороны, сторона защиты и сторона нападения. Для ТИ типична такая модель, когда присутствует две или более сторон. Если известны варианты стратегий каждой из сторон, а также положительные и отрицательные варианты действий, то существует возможность сформулировать математическую модель ситуации, а на основе этой модели можно получить оптимальные стратегии каждой из сторон. Например, для стороны защиты, можно найти решение для минимальной траты ресурсов при защите информации или для достижения максимальной вероятности предотвращения атак.

Сегодня связь является необходимым ресурсом для каждого человека. Чем лучше качество связи, тем лучше коммуникация. Но для улучшения ее требуется огромное количество ресурсов и времени. Математические методы, применяемые для решения задач управления инфокоммуникациями помогают в развитии и улучшении связи. С помощью теории игр можно найти наилучшие пути решения задачи оптимального количества перемещаемых сервисов сети в условиях ограниченного количества вычислительных ресурсов. Например, можно применить ТИ с целью поиска наилучших путей решения задачи оптимального количества перемещаемых сервисов сети пятого поколения в условиях ограниченного количества вычислительных ресурсов. Многие крупные компании используют ТИ для разделения пропускной способности между различными пользователями. В [3] изучается общая топология сети, и проблема заключается в том, какая полоса пропускания или дополнительная мощность, должна быть выведена сетью каждому пользователю на каждом канале. В [3, 4] предлагается концепция торга по Нэшу для распределения этой пропускной способности.

Также концепция Нэш используется в [5] для целей ценообразования, где концепция решения используется для определения стратегии ценообразования, в которой два игрока являются поставщиком услуг и совокупностью всех пользователей. Например, с пользователя никогда не взимается плата больше, чем его заявленный бюджет, но может взиматься меньшая плата, если перегруженность сетевых каналов, используемых соединением, низкая. Все агенты будут доброжелательны, то что они будут иметь общие цели и поэтому будут рады «помочь», когда нужна будет помощь. Однако в [6] показано, что агенты могут проявлять «эгоистичность». Так как каждый агент имеет «личные интересы», то «доброжелательность» является исключением. В большинстве встреч с несколькими агентами общий результат зависел от выбора каждого агента в сценарии. Получается, чтобы агент сделал выбор, который оптимизирует его результат, он должен рассуждать стратегически. То есть он должен учитывать решения, которые может принять другой агент, и должен предполагать, что они будут действовать таким образом, чтобы оптимизировать свой собственный результат. ТИ дает нам возможность формализовать и проанализировать такие проблемы.

Заключение и выводы

ТИ вошла в литературу по многоагентным системам в основном благодаря работам Джеффри Розенштейна и коллег. В своей докторской диссертации 1985 года [7] Розенштейн использовал теоретические методы игр для анализа ряда сценариев многоагентного взаимодействия. Например, он показал, как определенные виды сотрудничества и заключения сделок могут осуществляться без связи: оба агента просто вычисляют наилучший результат и знают, что сторона, с которой они имеют дело, сделает то же самое. Поскольку агенты могут использовать теоретические методы игры для прогнозирования того, что будут делать другие, это устраняет необходимость в явном общении - координация возникает из-за предположения о взаимной рациональности. Область переговоров в многоагентных системах заняла особое место. Так как благодаря переговорам агенты могут достичь соглашения по вопросам представляющим общий интерес. ТИ чрезвычайно убедительна как инструмент для переговоров из-за своих концепций.

С помощью ТИ, судя по исследуемым работам, были получены хорошие результаты в различных сферах. Но в инфокоммуникационной тематике очень мало работ по ТИ. Применимость ТИ недостаточно хорошо исследована применительно к инфокоммуникациям, хотя природа многих процессов позволяет говорить о применении ТИ для их моделирования.

Список используемых источников:

1. Simon Parsons., Michael Wooldridge. Game Theory and Decision Theory in Multi-Agent Systems // Department of Computer Science, University of Liverpool, Liverpool L69 7ZF, United Kingdom
2. Г. В. Басалов. Применение методов теории игр в системах обнаружения вторжения // Известия ТулГУ. Технические науки. 2016. Вып. 11. Ч.1
3. H. Yaiche, R. Mazumdar, C. Rosenberg. A game theoretic framework for bandwidth allocation and pricing of elastic connections in broadband networks: Theory and algorithms. IEEE/ACM Transactions on Networking. 2000. С. 667-678.
4. A. Muthoo Bargaining theory with applications.
5. X. R. Cao and U. X. Shen. Internet pricing: comparison and examples. In Proceedings of IEEE Conference on Decision and Control, Sydney, Australia, December 2000.
6. J. S. Rosenschein. Rational Interaction: Cooperation Among Intelligent Agents. PhD thesis, Computer Science Department. Stanford University, Stanford, CA 94305, 1985.
7. J. S. Rosenschein and M. R. Genesereth. Deals among rational agents. In Proceedings of the Ninth International Joint Conference on Artificial Intelligence (IJCAI-85), pages 91–99, Los Angeles, CA, 1985.

Belozarov K., Kislyakov S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunications

Analysis of the possibility of using the game theory apparatus for automating processes in infocommunications.

This article is a review of the research papers found concerning the application of game theory to solve problems in various fields of human activity. Special attention is paid to works in the field of infocommunications. The possibility of using the game theory apparatus for control tasks and operational support of communication networks is analyzed.

Key words: game theory, infocommunication systems, information security, multi-agent systems.

УДК 004.7
ГРНТИ 49.34.06

АНАЛИЗ ТЕХНОЛОГИИ NFV (ВИРТУАЛИЗАЦИЯ СЕТЕВЫХ ФУНКЦИЙ) ДЛЯ ПОСТАВЩИКОВ ТЕЛЕКОММУНИКАЦИОННЫХ УСЛУГ

А. Ю. Божедомов, Е. Е. Гончаров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Для того, чтобы справиться с растущим использованием сети, вызванным появлением новых мобильных клиентов, удовлетворить спрос на новые сетевые услуги и гарантии производительности, поставщики телекоммуникационных услуг используют виртуализацию в своей сети. Виртуализация сетевых функций, считается ключевым фактором «программного обеспечения» сети, которая обещает снизить капитальные и эксплуатационные расходы сетевых операторов за счет переноса обработки пакетов со специализированного оборудования на программное обеспечение, работающее на обычных серверах.

NFV, виртуализация, телекоммуникации, сетевой трафик

В современном мире наблюдается колоссальный рост интернет-пользователей, передаваемого трафика, количества персональных устройств, межмашинных соединений и так далее. Согласно прогнозному отчету Cisco VNI (Visual Networking Index) «Наглядный индекс развития сетевых технологий», распределение трафика по типам устройств будет выглядеть так:

- 71 % – беспроводные и мобильные, из них 44 % на смартфоны;
- 29 % - проводные, из них 19 % на ПК;
- 82 % от мирового трафика займет видео и 17 % придется на онлайн-видео;
- интернет-видео на ТВ вырастет втрое, до 27 % от фиксированного видео-трафика;
- трафик интернет-игр вырастет на 55 %;
- трафик виртуальной и дополненной реальности – на 65 %.

Ожидаемый объем глобального интернет-трафика составит 4,8 ZB в год (1,9+ трлн ГБ). Ежемесячный IP-трафик на душу населения вырастет с 16 ГБ до 50 ГБ.

Исходя из вышеперечисленных данных можно сделать вывод, расширяется полоса пропускания, повышается доля мобильного трафика, а интернет захватывает все сферы жизни, и становится все более безграничным, а операторам связи и поставщикам телекоммуникационных услуг необходимо как можно быстрее расширять свои сети, а сделать это не так просто. Современные телекоммуникационные сети содержат большое количество специализированного оборудования, каждое из которых необходимо для выполнения определённых задач [1].

В связи с ростом передачи растущего объема трафика и подключения к сети все большего числа устройств, традиционная архитектура сетей требует

существенных инвестиций, а именно в покупке большего количества оборудования, которое является дорогостоящим и часто имеет неполную совместимость сетевых решений. Традиционные методы развития сетей заключаются в «аппаратном» принципе: «устройство – функция», в большинстве случаев для того, чтобы ввести очередную функцию, надо установить другое устройство. Однако, такие методы развития сетей и вывода на рынок новых услуг при помощи новых физических устройств сталкиваются с рядом ограничений, что впоследствии ведет к несоответствию потребностей клиентов и предлагаемых на рынке телекоммуникаций решений. Возникает вопрос: а как бороться с такими ограничениями? Решение данной проблемы – виртуализация сетевых функций, технология NFV (Virtual Functions Virtualization).

Виртуализация сетевых функций NFV – это архитектурная концепция, которая используется в качестве виртуализированного метода для проектирования, развертывания и управления сетевыми службами. NFV позволяет использовать сетевые функции не аппаратной базе, а в программном обеспечении, как виртуальные машины. Примером таких сетевых функций являются: NAT, Firewall, DPI, балансировки нагрузки, функционал роутеров, коммутаторов, маршрутизаторов (MME, DHCP, EPC, SGW) и так далее [2].

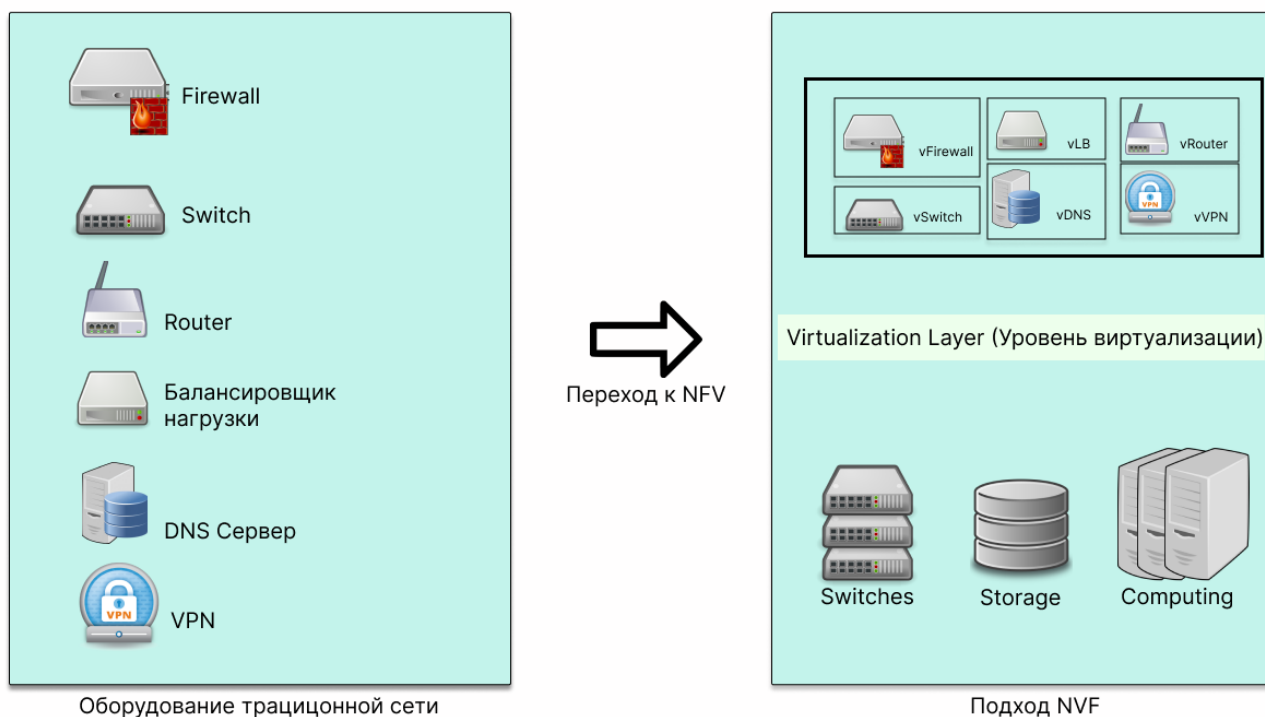


Рис. 1. Переход от традиционной сети к NFV

Архитектурная структура ETSI NFV ISG стандартизирует NFV, определяя различные элементы, необходимые для виртуализации сетевых функций.

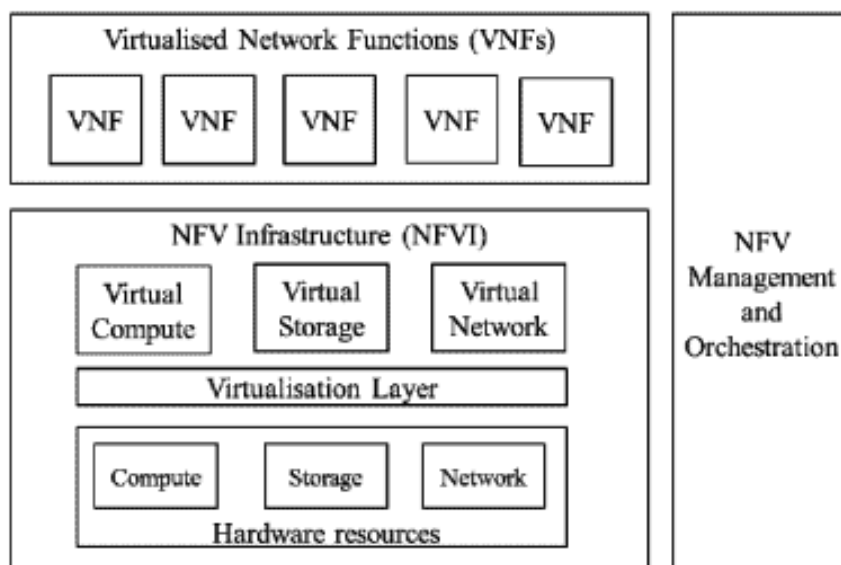


Рис. 2. Эталонная модель NFV, предложенная ETSI (основные элементы)

NFVi (NFV Infrastructure) – инфраструктура, которая реализует концепцию виртуализации сетевых функций это сетевая и вычислительная платформа, на которой базируется виртуализация. Данная инфраструктура включает в себя: Hardware resources (физические ресурсы), данная часть использует оборудование серверов (Compute) – систем хранения (Storage), сетевых интерфейсов (Network)

Virtual Computer, Storage, Network, в данном случае физические ресурсы превращаются в абстрактные виртуальные ресурсы, которые будут использоваться виртуальными сетевыми функциями;

Virtualization Layer (Уровень виртуализации) – гипервизор, в котором физические ресурсы абстрагируются в виртуальные.

VNFs (Virtualized Network Functions) – виртуальная сетевая функция – это виртуализированный сетевой элемент, который используется при развертывании виртуализации сетевых функций, то есть сами виртуализированные функции представляют свою программную реализацию. Если бы вы виртуализировали маршрутизатор, тогда маршрутизатор стал бы виртуальной сетевой функцией. Ряд элементов, которые можно превратить в виртуальную сетевую функцию, включает IP-адреса, брандмауэры, анализаторы трафика, балансировщики нагрузки и так далее.

NFV Management and Orchestration – это система комплексного управления и мониторинга, то есть отвечает за управление всеми ресурсами в инфраструктуре, определяет структуру предоставления VNFs, их конфигурацию, а также развертывание инфраструктуры при ее запуске [3,4,5].

После краткого разбора самой технологии NFV, можно сделать сравнительную таблицу, которая отметит преимущества виртуализации перед традиционными физическими устройствами (TFD). В таблице приведены основные характеристики, которые подразумевает под собой переход к виртуализации.

ТАБЛИЦА 1. Сравнительны таблица NFV и TFD

Характеристика	NFV	TFD
Оборудование общего назначения	Стандартные сервера на базе x86	Специальные устройства
Программно-аппаратная реализация	ПО отделено от аппаратного обеспечения и используется в виде модулей	Аппаратное и программное обеспечение тесно связано. Функции ПО зависят от выделенного оборудования
Открытость	Использует универсальную платформу и стандартные интерфейсы	Может происходить несовместимость устройств различных производителей
Гибкость сети	Имеется возможность динамически настраивать программные и аппаратные ресурсы, согласно требованиям к их обслуживанию	Устройства могут не поддерживать технологии виртуализации для совместного использования ресурсов и эластичного масштабирования
Обновления и развертывание	Обновление и развёртывание систем происходит быстро, так как в основном связано с ПО. Систему можно полностью автоматизировать, без привлечения технического персонала	Обновление и развёртывание систем отнимает много времени, поскольку необходима работа как с аппаратной частью, так и с программным обеспечением
Обслуживание	Сами сети развёртываются по необходимым параметрам для определенных сервисов.	Требования к сети не могут быстро перестроиться к требованию сервиса, что приводит к медленной реакции.

Можно заметить, что технология NFV, убирает ограничения традиционных сетей, что полностью поможет решить проблемы массового роста сетевого трафика и снимет ограничения традиционных сетей, например, такие как:

- сокращение операционных капитальных затрат и операционных расходов за счет снижения стоимости оборудования и снижения потребления энергии;
- сокращение «выхода на рынок» для развертывания новых сетевых сервисов, улучшение отдачи от инвестиций в новые услуги;
- большая гибкость для увеличения, уменьшения или развития услуг; открытость для рынка виртуальных устройств и «чистых» участников.

В итоге рассмотрения вопроса об использовании виртуализации сетевых функций для поставщиков телекоммуникационных услуг следует подчеркнуть,

что рост полосы пропускания и передаваемых по сети данных в целом подразумевает под собой переход к сетям пятого поколения 5G. Телекоммуникационным оператором непросто трансформировать инфраструктуру своих сетей, чтобы создавать новые сервисы, получать дополнительные источники доходов и улучшать операционную эффективность.

Возникает еще много вопросов о других технологиях и принципах их работы, которые в совокупности позволят поставщикам телекоммуникационных услуг развивать, улучшать, развивать их архитектуры, но эти вопросы будут обязательно рассмотрены в следующих статьях.

Список используемых источников:

1. К. Иванов // News Mobile Review [Электронный ресурс]: По прогнозам Cisco, мировой объем IP-трафика к 2021 г. превысит три зеттабайта – Режим доступа URL: <https://mobile-review.com/news/po-prognozam-cisco-mirovoj-obem-ip-trafika-k-2021-g-prevysit-tri-zettabajta> (дата обращ. 2021 г.)
2. Ю. Ковалевский Потенциал создания российских базовых станций для сетей 5G // Электроника, Наука, Технология, Бизнес: Информационные и телекоммуникационные системы. –2021. – №2. – С. 94-99.
3. ETSI GS NFV 006 (2022-06) Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Architectural Framework Specification
4. В. Ефимушкин, Т. Ледовских, Д. Корабельников, Д. Языков Обзор решений SDN/NFV Зарубежных производителей // Т-Comm: Телекоммуникации и транспорт. – 2015. – Том 9. – №8. – С. 5-13.
5. Anti-Malware [Электронный ресурс]: Как работает виртуализация сетевых функций (NFV, Network Functions Virtualization)
6. K. Jang, M. Walls, S. Ratnasamy, S. Shenker NetBricks: Talking the V out of NFV // USENIX Symposium on Operating Systems Design and Implementation. –2016. – №12, pp. 203-2016.
7. Chowdhury, Shihabur Rahman; Salahuddin, Mohammad A.; Limam, Noura; Boutaba, Raouf Re-Architecting NFV Ecosystem with Microservices: State of the Art and Research Challenges. IEEE Network. –2019. – №33(3). – pp. 168–176.
8. Cziva, R. and Pezaros, D. P. (2017) Container network functions: bringing NFV to the network edge. IEEE Communications. –2017.– №55(6) – pp. 24-31.

Bozhedomov A., Goncharov E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of NFV technology (Virtualization of network functions) for telecommunication service providers.

In order to cope with the increasing network usage caused by new mobile customers, to meet the demand for new network services and performance guarantees, telecom service providers are using virtualization in their network. Network function virtualization, considered a key driver of network "software" that promises to reduce capital and operating expenses for network operators by moving packet processing from specialized hardware to software running on common servers.

Key words: *NFV, virtualization, telecommunications, network traffic.*

УДК 654.1
ГРНТИ 50.41.23

АНАЛИЗ СОВРЕМЕННЫХ ИНСТРУМЕНТОВ DEVOPS

М. В. Градовский, С. В. Кисляков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Модель объединения двух сфер, работавших порознь, в единый механизм становится важным вектором развития в истории IT индустрии. В данной статье предлагается рассмотреть основные принципы, назначение и инструменты DevOps.

DevOps, IT, kubernetes, docker, контейнеризация, автоматизация

До начала 2000-х годов цикл выпуска программного обеспечения был очень долгим. Даже если разработчики могли быстро написать или усовершенствовать продукт, команда эксплуатации опасалась за стабильность его работы. Из-за этого выпуск продукта или его новой версии мог затянуться на месяцы, а иногда и больше.

DevOps описывает процесс разработки приложения и его непрерывного внедрения за счет автоматизации и объединения усилий команд разработки и поддержки – двух групп, которые работали отдельно друг от друга.

DevOps - это сочетание культурных философий, практик и инструментов, которые повышают способность организации предоставлять приложения и услуги с высокой скоростью: разрабатывать и совершенствовать продукты более быстрыми темпами, чем организации, использующие традиционные процессы разработки программного обеспечения и управления инфраструктурой. В рамках модели DevOps команды разработки и эксплуатации больше не изолированы друг от друга.

Для того, чтобы ускорить разработку и повысить качество, команды разработчиков начали внедрять гибкие методологии разработки программного обеспечения, или Agile, которые, в отличие от традиционных методов, являются скорее итеративными [1], чем линейными, и сосредоточены на более частых и менее объемных обновлениях кода. Главными среди этих методологий являются непрерывная интеграция и непрерывная доставка, или CI/CD.

DevOps был порожден культурой и методологиями Agile, которая за последние десятилетия выявила необходимость более целостного подхода к жизненному циклу доставки программного обеспечения. Идеалы DevOps [2] расширяют практику гибкой разработки за счет дальнейшей оптимизации процесса изменения программного обеспечения на этапах сборки, тестирования, развертывания и доставки.

Этапы разработки программного обеспечения, которые затрагивает DevOps, показаны на рис. 1.

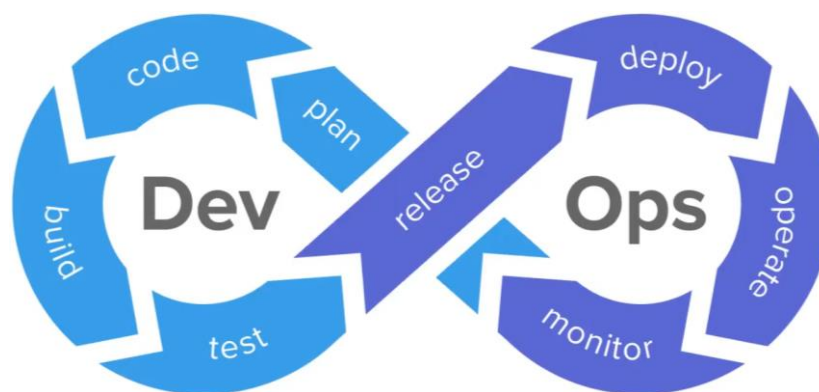


Рис. 1. Этапы DevOps

DevOps от своего зарождения до сегодняшнего дня претерпел некоторые фазы развития [2], а именно:

- **Waterfall Deployment**

Командам разработчиков приходилось бы писать код на протяжении нескольких месяцев, затем они объединяли бы свой код, чтобы выпустить его, но разные версии кода были бы настолько разными, что этап интеграции мог бы занять месяцы. Этот процесс был очень непродуктивным.

- **Continuous Integration**

Непрерывная интеграция – это практика быстрой интеграции недавно разработанного кода с основной частью кода, который должен быть выпущен. С точки зрения DevOps этот процесс включает в себя проверку кода, компиляцию его в пригодный для использования код и выполнения некоторого базового валидационного тестирования.

- **Continuous Delivery**

Непрерывная доставка — это расширение непрерывной интеграции. При выполнении непрерывной доставки добавляется дополнительная автоматизация и тестирование, так что происходит не просто объединение кода с основной частью кода, но и получается код, практически готовый к развертыванию, почти без вмешательства человека. Это практика постоянного поддержания базы кода в режиме готовности к развертыванию.

- **Continuous Deploy**

Непрерывное развертывание — это практика полного развертывания в производство без какого-либо вмешательства человека. Команды, использующие непрерывную доставку, не развертывают непроверенный код. Вместо этого созданный код проходит автоматическое тестирование, прежде чем он будет запущен в производство. Обычно, выпуск кода распространяется на небольшой процент пользователей, и, благодаря автоматическому циклу обратной связи, отслеживается качество и использование, прежде чем код будет распространен дальше.

В сфере DevOps существует множество различных технологий и инструментов [3]. И когда речь заходит о технологиях контейнеризации, возникают лишь два названия [4]: Docker и Kubernetes – самые популярные среди

технологий контейнеризации. Их сравнение будет не совсем корректно, поэтому рассмотрим преимущества и недостатки каждой.

Контейнер – это исполняемый модуль программного обеспечения, который упаковывает код приложения с его зависимостями, позволяя ему работать в любой IT-инфраструктуре.

Docker – это среда выполнения контейнеров с открытым исходным кодом, которая позволяет разработчикам программного обеспечения создавать, развертывать и тестировать контейнерные приложения на различных платформах.

Его преимущества:

- **Легкая переносимость:** приложения могут перемещаться из одной среды в другую, и они будут работать независимо от операционной системы.
- **Гибкая разработка приложений:** контейнеризация упрощает внедрение процессов CI/CD и использование преимуществ DevOps. Благодаря контейнеризации, приложения могут быть протестированы в одной среде и развернуты в другой.
- **Масштабируемость:** контейнеры докер могут быть созданы быстро, и несколькими контейнерами можно управлять эффективно и одновременно.

Kubernetes – это популярный оркестратор контейнеров с открытым исходным кодом, который разработчики программного обеспечения используют для развертывания, масштабирования огромного количества микросервисов и управления ими.

Его преимущества:

- **Автоматическое развертывание:** планирует и автоматизирует развертывание контейнеров на нескольких вычислительных узлах.
- **Балансировка нагрузки:** использует балансировку нагрузки при возникновении скачков трафика для поддержания стабильности.
- **Функции автоматического масштабирования:** автоматически запускает новые контейнеры для обработки больших нагрузок.
- **Возможности самовосстановления:** перезапускает, заменяет или перепланирует контейнеры, когда они выходят из строя или когда узлы умирают.

Технологии Docker и Kubernetes не конкурируют между собой, а на деле могут и дополнять друг друга.

В дальнейших целях стоит развернуть полигон при помощи Kubernetes под задачи и на серверах компании-разработчика OSS-систем.

Направление DevOps на сегодняшний день является очень актуальным. Многие организации внедряют его методологии в свою жизнь, и их число растет. Это говорит о том, что методологии DevOps приносят выгоду организациям, автоматизируя их процессы, ускоряя выпуск продукта и улучшая стабильность его работы. Но, кроме этого, DevOps меняет культуру.

Список используемых источников:

1. DevOps [Электронный ресурс]. URL: <https://www.ibm.com/cloud/learn/devops-a-complete-guide> (дата обращения 10.11.22).

2. DevOps Concepts [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/devops-concepts/viewer> (дата обращения 10.11.22).
3. Kubernetes vs Docker: Why Not Both? [Электронный ресурс]. URL: <https://www.ibm.com/cloud/blog/kubernetes-vs-docker> (дата обращения 11.11.22).
4. Джей Вьяс, Крис Лав Kubernetes изнутри: пер. с англ. А. Н. Киселева. М.: ДМК Пресс, 2022. 29 с.

Gradovsky M., Kislyakov S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of modern DevOps tools.

The model of combining two spheres that worked separately into a single mechanism is becoming an important vector of development in the history of the IT industry. This article proposes to consider the basic principles, purpose and tools of DevOps.

Key words: DevOps, IT, kubernetes, docker, containerization, automation

УДК 004.725.4
ГРНТИ 49.33.29

АНАЛИЗ МОБИЛЬНЫХ СЕТЕЙ В ДВУХРЕЖИМНОЙ ПРОГРАММНО-ОПРЕДЕЛЯЕМОЙ СЕТЕВОЙ ПЛАТФОРМЫ SD-CORE

В. С. Елагин, С. М. Тураев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

SD-Core, проект с открытым исходным кодом для создания дезагрегированного мобильного ядра 5G/4G, оптимизированного для новых частных и корпоративных вариантов использования 5G, начинается с предварительно интегрированной двухрежимной плоскости управления. Плоскость управления SD-Core одновременно поддерживает автономное развертывание 5G (SA), неавтономное развертывание 5G (NSA) и 4G/LTE, оптимизируя тем самым гибкость и готовность сетей к будущему.

сети 4G/5G, SD-Core, API-интерфейс, UPF, агент PCF

Введение

SD-Core - это открытое, гибкое, масштабируемое и настраиваемое двухрежимное мобильное сетевое решение 4G / 5G с открытым исходным кодом от Open Networking Foundation (ONF), которое обеспечивает возможность подключения как услуги на основе облака. SD-Core дополняет и расширяет 4G Open Mobile Evolved Core (OMEC) компании ONF, а также базовую сетевую платформу free5GC для создания двухрежимного решения, которое поддерживает сервисы LTE, 5G NSA и 5G SA, оптимизированные для многооблачных сред [1].

Обзор проекта SD-Core

SD-Core ONF представляет собой полностью настраиваемую платформу с открытым исходным кодом и богатым набором API для двухрежимного подключения 4G и 5G. Как показано на **рис. 1**, SD-Core использует OMEC и free5GC в качестве базовых компонентов, объединяет их для двухрежимной работы и предоставляет новые важные функции для оптимизации доставки Connectivity-as-a-Service из гибридного облака [1].

Чтобы оптимизировать гибридное облако и поддерживать новые сценарии использования Индустрии 4.0, SD-Core включает несколько функций плоскости пользователя (UPF) для обработки различных классов корпоративного трафика [2].

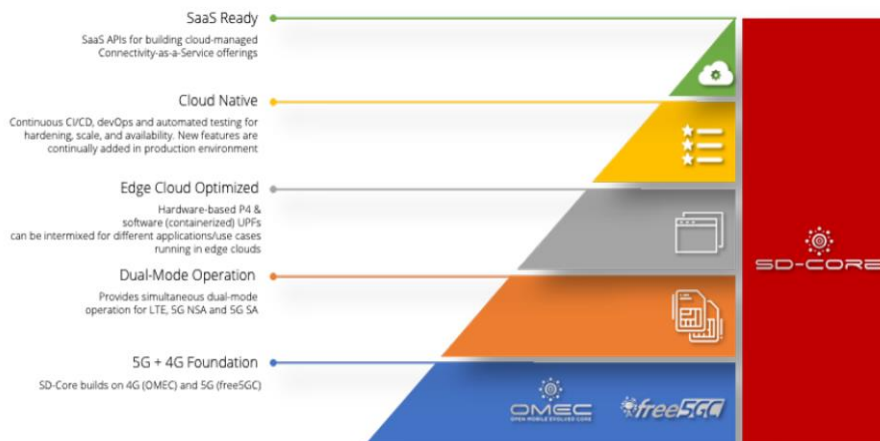


Рис. 1. SD-Core

SD-Core, обеспечивающий подключение 4G и 5G в качестве управляемой облачной услуги

Чтобы включить управляемую облачную службу подключения 4G / 5G, SD-Core предоставляет богатый набор API. Как показано на рис. 2, эти API-интерфейсы предназначены для предоставления данных телеметрии и приема обновлений конфигурации от сторонних приложений и порталов. Следовательно, сторонние приложения могут разрабатывать автоматизированные процессы управления с обратной связью, непрерывно отслеживая состояние подключения и изменяя конфигурацию SD-Core с помощью простых регуляторов для поддержания желаемого качества работы.

Как показано на рис. 2, ROC ONF включает встроенные адаптеры для SD-Core для трансляции своих API-интерфейсов мониторинга и конфигурации на порталы клиентов и операторов, а также сторонние приложения с соответствующими уровнями абстракции. ROC использует RBAC для управления доступом к API мобильного ядра [3].

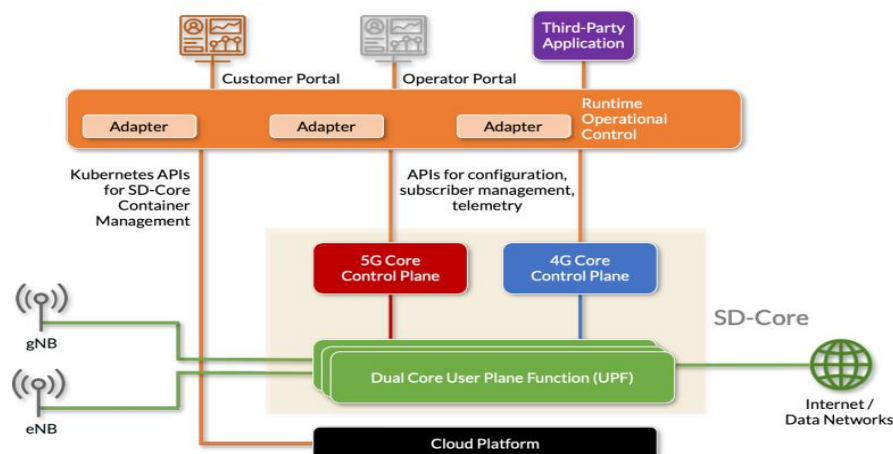


Рис. 2. Архитектура SD-Core высокого уровня

SD-Core Архитектура

Архитектура SD-Core обеспечивает следующие отличительные особенности:

- Архитектура полностью дезагрегирована и состоит из контейнерных компонентов.
- Решение поддерживает 4G, 5G Standalone (SA) и 5G Non-Standalone (NSA).
- Решение поддерживает 4G, 5G Standalone (SA) и 5G Non-Standalone (NSA).
- Решение обеспечивает подключение 4G, 5G Standalone (SA) и 5G Non-Standalone (NSA).
- Платформа настраивается во время выполнения с помощью расширяемого набора API.
- Решение можно использовать как облачную управляемую услугу.

Детали двухрежимной архитектуры SD-Core показаны на **рис. 3**. В частности, функции базовой сети 5G SD-Core соответствуют требованиям 3GPP версии 15.3 и включают функцию управления доступом и мобильностью (AMF), функцию управления сеансом (SMF), Функция сервера аутентификации (AUSF), функция управления политикой (PCF), унифицированное управление данными (UDM), унифицированный репозиторий данных (UDR), функция сетевого репозитория (NRF), функция выбора сетевого сегмента (NSSF), функция приложения (AF) и в ближайшем будущем - функция хранения неструктурированных данных (UDSF) для поддержки облачных технологий. Эти функции используют интерфейсы на основе служб (SBI) для связи друг с другом.

Функции уровня управления 4G SD-Core совместимы с 3GPP версии 13 и включают объект управления мобильностью (MME), управление шлюзом сети обслуживания и пакетных данных (SPGW-C), сервер домашнего абонента (HSS) и функцию правил политики и тарификации (PCRF). Ядро 4G SD-Core разработано с учетом архитектуры, совместимой с CUPS (разделение плоскости управления и пользователя), и использует протокол управления пересылкой пакетов (PFCP) 3GPP для реализации CUPS.

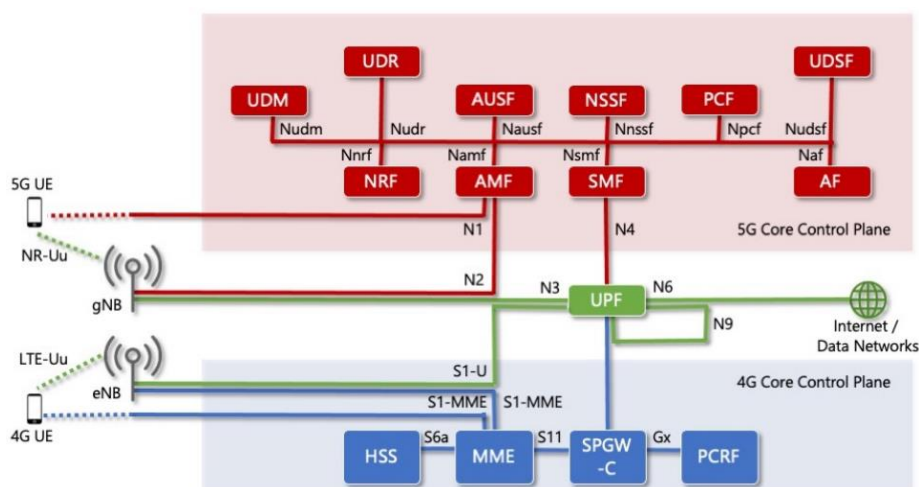


Рис. 3. 5G Standalone (SA) и 4G / LTE с SD-Core

Плоскость управления 4G SD-Core была улучшена для обеспечения функциональной поддержки неавтономной работы 5G с совместимыми eNB и

gNB в соответствии со спецификациями 3GPP. Работа SD-Core 5G NSA показана на **рис. 4**. Усовершенствования, связанные с 5G NSA, включают поддержку расширенных скоростей передачи на требуемых интерфейсах, а также атрибутов 5G NSA в HSS. [3]

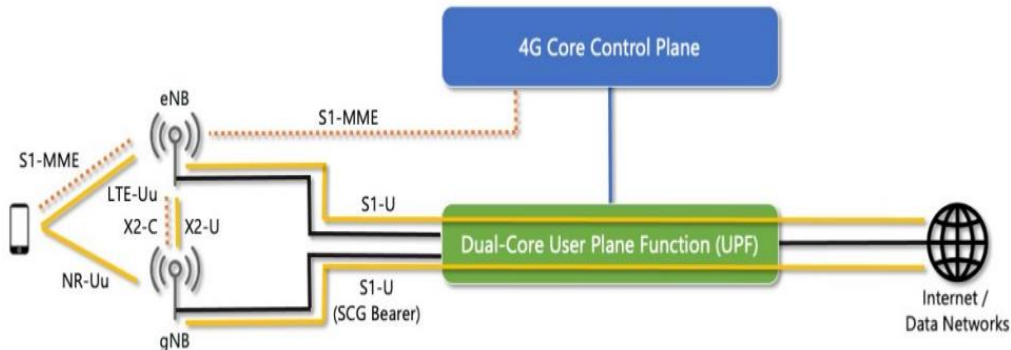


Рис. 4. 5G Non-Standalone с SD-Core

Заключение

SD-Core оптимизирован для развертывания гибридного облака. Его централизованная двухрежимная мобильная базовая плоскость управления была разработана для управления множеством UPF, распределенных по множеству граничных облаков по всему миру. Это делает SD-Core идеальной платформой с открытым исходным кодом, чтобы предлагать предприятиям облачные частные услуги подключения 4G / 5G в качестве инструмента преобразования Индустрии 4.0. Благодаря множеству опций UPF, включая реализацию на основе P4, SD-Core обеспечивает превосходную производительность и детальную видимость трафика сотовой сети. В сочетании с программируемостью это позволяет операторам обеспечивать проверяемые возможности отказоустойчивости, безопасности и конфиденциальности для своих развертываний 4G и 5G.

Список используемых источников:

1. <https://opennetworking.org/>
2. <https://docs.sd-core.opennetworking.org/sdcore-1.1/overview/introduction.html>
3. <https://docs.sd-core.opennetworking.org/sdcore-1.1/overview/architecture.html>

Elagin V., Turaev S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Mobile network analysis in a dual-mode software-defined SD-Core network platform.

SD-Core is the Open Networking Foundation (ONF)'s open source, flexible, agile, scalable, and configurable dual-mode 4G/5G mobile core network solution that enables a cloud-based Connectivity-as-a-Service. SD-Core builds and enhances on ONF's 4G Open Mobile Evolved Core (OMEC) as well as the free5GC core network platform to create a dual-mode solution that supports LTE, 5G NSA and 5G SA services optimized for hybrid-cloud environments.

Key words: ONF, 4G/5G, OMEC, 5G NSA, 5G SA.

УДК 004.891.2
ГРНТИ 49.34.06

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В БИЗНЕС-ПРОЦЕССАХ

М. П. Заяц

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья посвящена использованию искусственного интеллекта в бизнесе. В ней рассмотрено, как искусственный интеллект может повлиять на ход работы ряда компаний. В статье представлено, какие функции может иметь бизнес-процесс при использовании искусственного интеллекта.

искусственный интеллект, бизнес-процессы, функции, IDEF0, элементы иерархии механизмов

Использование искусственного интеллекта в бизнесе – одно из направлений, которое активно внедряется в различные сферы компаний. Уже сегодня примерно треть мировых брендов активно занимаются разработкой собственного программного решения из сферы искусственного интеллекта.

Искусственный интеллект возможно применять для различных бизнес-процессов, обеспечив эффективную работу во всех сферах компаний (рис. 1).



Рис. 1. Применение информационных систем с элементами ИИ в бизнес-процессах

- Использование ИИ для сбора, анализа и обработки данных

Применение аналитических инструментов повышает эффективность работы организаций. Технологии ИИ способны выполнять осуществлять сбор и работать со статическими данными, определяя различные факторы, стимулирующие клиентов совершать повторные действия.

- Использование ИИ для улучшения организации бэкенда

Инструменты ИИ полностью изменяют сферу бэкенда. Таким образом, технологии избавляют сотрудников от рутинных и монотонных задач, позволяя сфокусироваться на главном. После обучения сети качество данных может возрасти, а инфраструктура упроститься (рис. 2).



Рис. 2. Процесс машинного обучения

- Использование ИИ в сфере маркетинга

Бизнес всегда заинтересован в появлении новых клиентов. Однако не исключен риск привлечения нецелевой аудитории, используя дополнительные траты компаний. Поэтому программные решения с машинным обучением способны составить «портрет» идеального клиента, а также отыскать его на различных площадках (рис. 3).

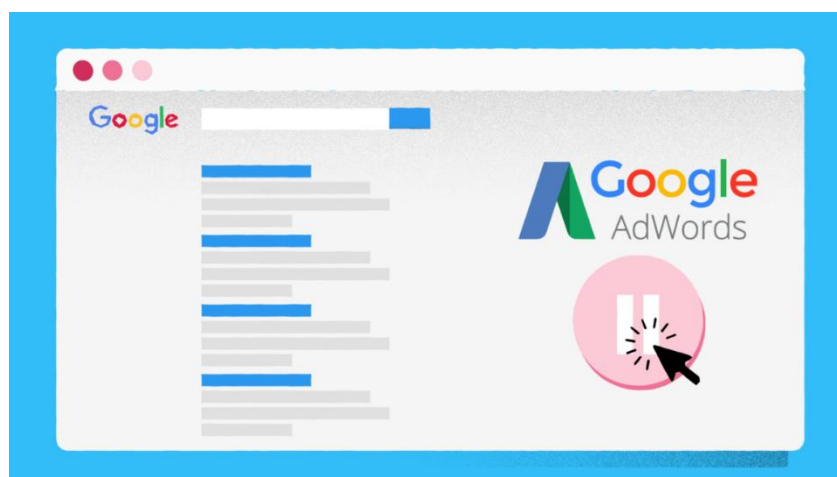


Рис. 3. Использование ИИ Google для оптимизации показа рекламы

- Использование ИИ для повышения уровня качества сервиса

ИИ способен сделать бизнес более клиентоориентированным. Уже сейчас активно используются чат-боты и виртуальные помощники для проведения консультаций и поддержки клиентов. Таким образом, системы ИИ способны предоставить решения по базовым вопросам и обеспечить непрерывную работу с клиентами.

- Использование ИИ для подбора персонала

Используя ИИ, бизнес может уменьшить нагрузку на отдел кадров или вовсе обойтись без него. Алгоритмы машинного обучения способны выделять лучшую стратегию для найма, сортировать полученные данные из анкет, систематизировать информацию об опыте и задачах конкретного кандидата. Однако в данном случае требуется сотрудник, который будет взаимодействовать с кандидатами, оформляя и передавая данные о них ИИ.

Таким образом, ИИ способен полностью изменить структуру компаний, заменив полностью человеческий труд, что, в первую очередь, может уменьшить количество ошибок, которые могут допускаться сотрудниками в связи с человеческим фактором.

Бизнес-процесс может быть представлен в виде совокупности функций. Каждая функция получает определенные данные на входе, которые она преобразует под управляющим воздействием, с помощью определенного механизма осуществления. Преобразованные данные являются исходными данными для входов других функций в рамках бизнес-процесса.

Необходимо определить, чем ИИ является при моделировании и реинжиниринге бизнес-процессов - механизмом осуществления или управляющим воздействием?

Рассмотрим с точки зрения нотации IDEF0 ИИ в качестве управляющего воздействия на процесс.

Управляющей информацией являются сведения о условиях и правилах преобразования объекта на входе в объект на выходе блока.

Управление - особый вид процесса, операции, действия. По методологии IDEF0 в каждом блоке на диаграмме должна присутствовать хотя бы одна управляющая стрелка, информирующая условия правильного функционирования блока. Это требование является следствием положения системотехники, согласно которому управление есть такое воздействие (преимущественно информационное) на систему, которое стимулирует ее функционирование в направлении достижения некоторой цели. В связи с этим можно сформулировать ряд определений и методических положений, которыми следует руководствоваться при отражении управлений на функциональных моделях.

По методологии IDEF0 в каждом блоке на диаграмме должна присутствовать хотя бы одна управляющая стрелка, информирующая условия правильного функционирования блока.

Управление деятельностью - процесс, состоящий, из операций:

- установка целей;
 - оценивание необходимых ресурсов и сопоставление с имеющимися;
 - сбор информации об условиях протекания и фактическом состоянии деятельности;
 - выработка и принятие решений, в том числе решений о распределении ресурсов по процессам;
 - оформление решений в виде директив;
 - реализация решений и оценка их результатов;
 - корректировка ранее сформулированных целей (в случае выявленной потребности).
- Именно решения и их реализация - основная часть мотивирующего воздействия на систему. В свою очередь управление процессом - операция, состоящая из следующих:

- анализ директивы на управление процессом, ее декомпозиция на директивы управления операциями;
- сбор информации о ходе выполнения операций, ее обобщение и формирование сведений о состоянии процесса;
- передача данных в подсистему управления деятельностью;
- сопоставление информации о ходе операций с данными директив и выработка локальных решений, направленных на устранение отклонений;
- корректировка директив на выполнение операций.

Таким образом, ИИ и технологии на его основании не могут быть рассмотрены в разрезе IDEF0 в качестве управляющего воздействия. При этом вполне возможен вариант использования в качестве механизма осуществления.

В соответствии с методологией IDEF0 каждая функция выполняется посредством механизма. В большинстве систем, анализируемых при помощи функциональных моделей такими механизмами, служат организационно-технические структуры. Вместе с тем анализ показывает, что между иерархией функций и иерархией механизмов существует соответствие.

Используя приведенные выше понятия системного анализа, определим элементы иерархии механизмов следующим образом. Организационно-техническая система - организационная структура, персонал и комплекс технических средств, необходимые для осуществления деятельности. Организационно-техническая подсистема - часть организационно-технической системы, обеспечивающая протекание процесса. Организационно-технический модуль - часть организационно-технической подсистемы, предназначенная для выполнения операции. Организационно-технический блок - часть организационно-технического комплекса, обеспечивающая выполнение действия.

Следовательно, при корректном построении модели появляется возможность связать ее блоки на разных уровнях декомпозиции с объектами организационно-технической структуры, выступающими в качестве механизмов. В этом случае организационно-техническая структура становится результатом функционального моделирования.

Список используемых источников:

1. Роль искусственного интеллекта в бизнесе [Электронный ресурс]. URL: <https://www.simbirsoft.com/blog/rol-iskusstvennogo-intellekta-v-biznese/> (дата обращения: 06.11.2022).
2. Как работает искусственный интеллект в бизнесе [Электронный ресурс]. URL: <https://ratenger.com/hi-tech/ai/iskusstvenniy-intellekt-v-biznese/> (дата обращения: 06.11.2022).
3. Искусственный интеллект в бизнес-процессах [Электронный ресурс]. URL: https://revolution.allbest.ru/programming/00986815_0.html (дата обращения: 06.11.2022).
4. Бизнес и искусственный интеллект [Электронный ресурс]. URL: <https://vc.ru/services/324966-biznes-i-iskusstvennyy-intellekt-gde-primenyat-i-kak-ispolzovat> (дата обращения: 06.11.2022).
5. Нейросети: как искусственный интеллект помогает в бизнесе и жизни [Электронный ресурс]. URL: <https://habr.com/ru/post/337870/> (дата обращения: 06.11.2022).

6. Искусственный интеллект в действии: как умные алгоритмы помогают улучшить бизнес-процессы [Электронный ресурс]. URL: <https://www.esphere.ru/blog/iskusstvennyij-intellekt-v-dejstvii> (дата обращения: 06.11.2022).

Zaiats M.

The Bonch-Bruевич Saint- Petersburg State University of Telecommunications

Artificial intelligence in business processes.

This article is devoted to the use of artificial intelligence in business. It examines how artificial intelligence can affect the course of work of a number of companies. The article presents what functions a business process can have when using artificial intelligence.

Key words: *artificial intelligence, business processes, functions, IDEF0, elements of the hierarchy of mechanisms.*

УДК 004.7
ГРНТИ 49.34.06

АНАЛИЗ ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ СЛАЙСИНГА В СЕТЯХ 5G

И. О. Казаченко, А. Ю. Просветов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье речь пойдет о технологиях, которые обеспечивают процессы создания и управления виртуальными сетями. Были рассмотрены программно-определяемые сети, туманные вычисления, пограничные вычисления с множественным доступом, виртуализация сетевых функции, виртуальные машины и контейнеры. Представленные технологии рассматривались с точки зрения совместимости в рамках обеспечения работы сетей пятого поколения.

5G, слайсинг, виртуализация, виртуализация сетевых функций, программно-определяемые сети, облачные вычисления, пограничные вычисления, туманные вычисления

Программно-определяемые сети

SDN или программно-определяемые сети – это новая парадигма, которая упрощает управление сетью и делает ее более гибкой. Сетевой интеллект управляется централизованно сетевым контроллером, где последний создает более эффективные правила управления маршрутизацией потоков для различных сетевых устройств. Контроллер может взаимодействовать с другими сетевыми уровнями через два интерфейса – северный и южный. [1-3].

В контексте сетевого слайсинга, технология SDN способна обеспечивать гибкую, ориентированную на обслуживание и масштабируемую поддержку широкого спектра бизнес-задач. Каждая такая задача будет обслуживаться одновременно в общей инфраструктуре и совместно использовать ресурсы. Как показано на рис. 1, стандартная архитектура «SDN Network Slicing» предоставляет сетевой фрагмент для каждого слайса [4].

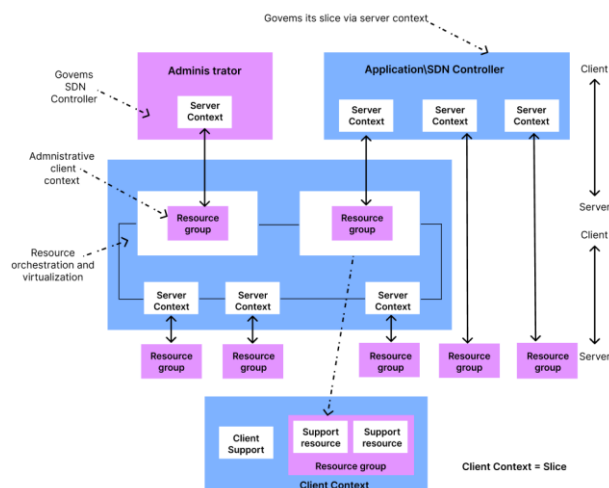


Рис. 1. Абстракция слайса на основе SDN

Cloud-fog computing

Хотя «туман» и превосходит облако по быстродействию и общей осведомленности о местоположении, его простых возможностей недостаточно для выполнения сложных и многоэтапных задач. Таким образом, туманные вычисления могут дополнять облачные вычисления, а не заменят их. Другими словами, более сложные и комплексные задачи обслуживаются облаком, в то время как массово развертываемые Fog обрабатывают облегченные вычисления и недолговечный обмен контентом, зависящим от местоположения.

Поскольку запросы и контент будут часто мигрировать между туманом и облаком, для скоординированного представления услуг следует организовать взаимодействие типа «облако-туман» на высоком уровне [5]. Однако, требования к сервису в сетях пятого поколения динамичны и изменяются во времени, следовательно, появляется необходимость в местном координаторе, который будет осуществлять предварительную обработку запросов, распределять поступающие задачи по доступным ресурсам, собирать и анализировать информацию о состоянии сети в реальном времени.

Для решения поставленных задач, предлагается интегрировать программно-конфигурируемые сети для организации взаимодействия между облаком и туманом. Показанная на рис. 2 архитектура включает мобильных пользователей, облачные и Fog сервера, где хранилище и вычислительные ресурсы за пределами сети доступа называются облаком. Таким образом, информация о локальной сети непрерывно передается между контроллерами, что приводит к созданию логического контроллера с групповым интеллектом. Контроллеры оценивают запросы пользователей и выдают соответствующие ответы либо по средством взаимодействия «туман-туман» либо «облако-туман».

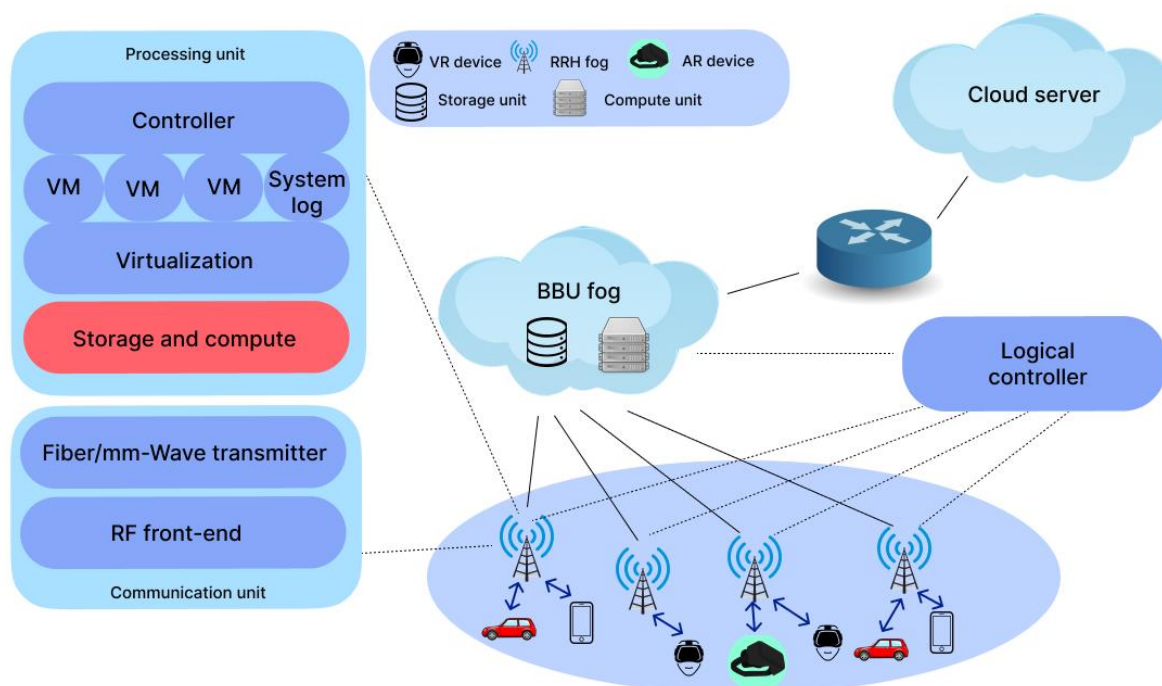


Рис. 2. Взаимодействие облака и тумана через SDN

Multi-access edge computing

Концепция пограничных вычислений с множественным доступом (MEC) внедряется для оптимизации работы различных промышленных вертикалей, которые требуют различные и строгие показатели качества обслуживания (QoE). В таком случае, возможностей, предоставляемых программно-определяемыми сетями в паре с «NFV» не обязательно будет достаточно для необходимых гарантий. Например, приложения дополненной реальности должны иметь сверхнизкие задержки, чего очень трудно достичь, если сервер расположен в центре обработки данных за тысячи километров от конечных пользователей. Следовательно, вычислительные ресурсы необходимо разместить на границе сети и организовать работу с сетевыми ресурсами и функциями, а также поддержку нескольких технологий доступа.

Сети пятого поколения, в отличие от четвертого, были целостно разработаны с использованием MEC (рис. 3). Таким образом, вместе с SDN и NFV – MEC является ключевым элементом 5G сетей [6].

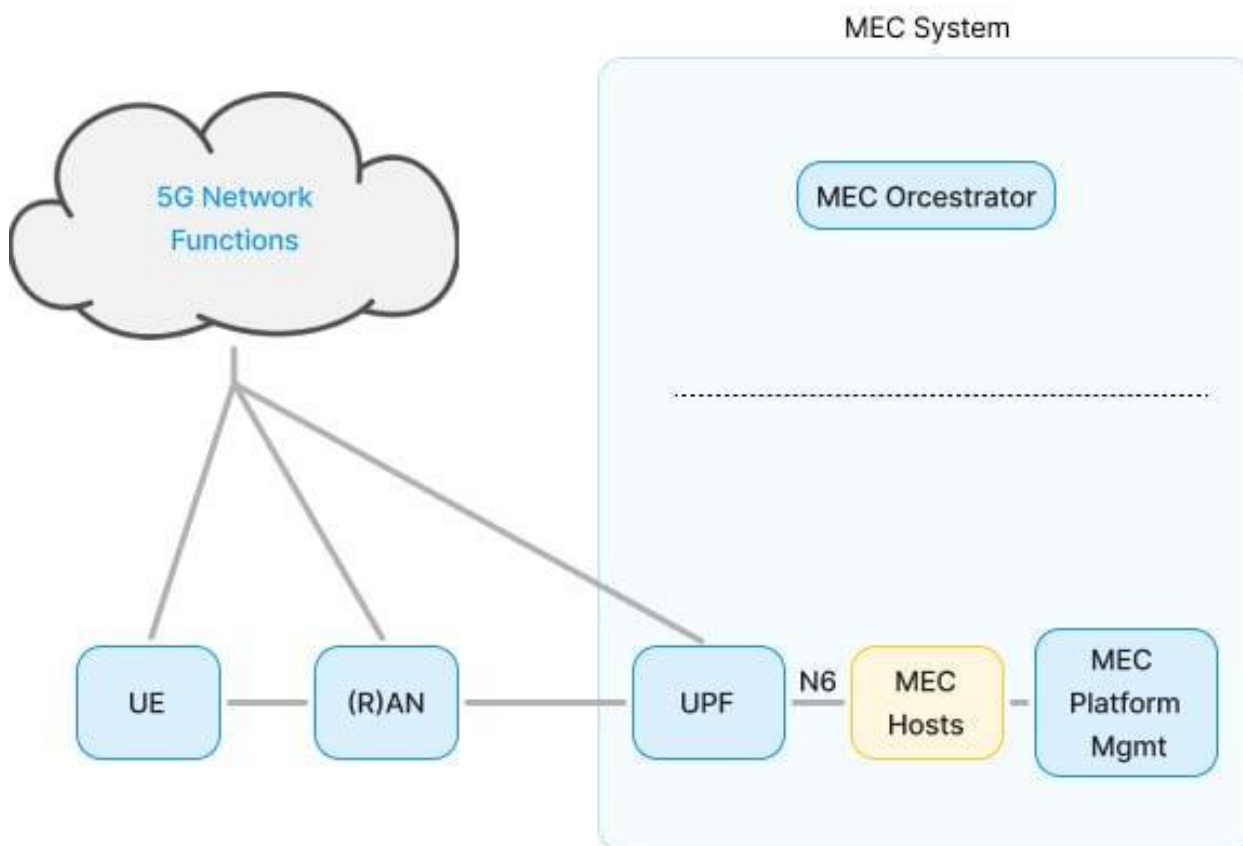


Рис. 3. MEC с 5G

Network Virtualization Technologies

NFV использует технологию виртуализации для построения виртуальной сети и элементов виртуальной сети. В то время как построенная сеть и форма стратегии изменяются, производительность сети остается прежней. Ключевой характеристикой NFV являются сетевые функции (NFs), которые реализованы в

программных пакетах, а виртуальные машины используются для запуска таких пакетов. Архитектура NFV описана на рис. 4.

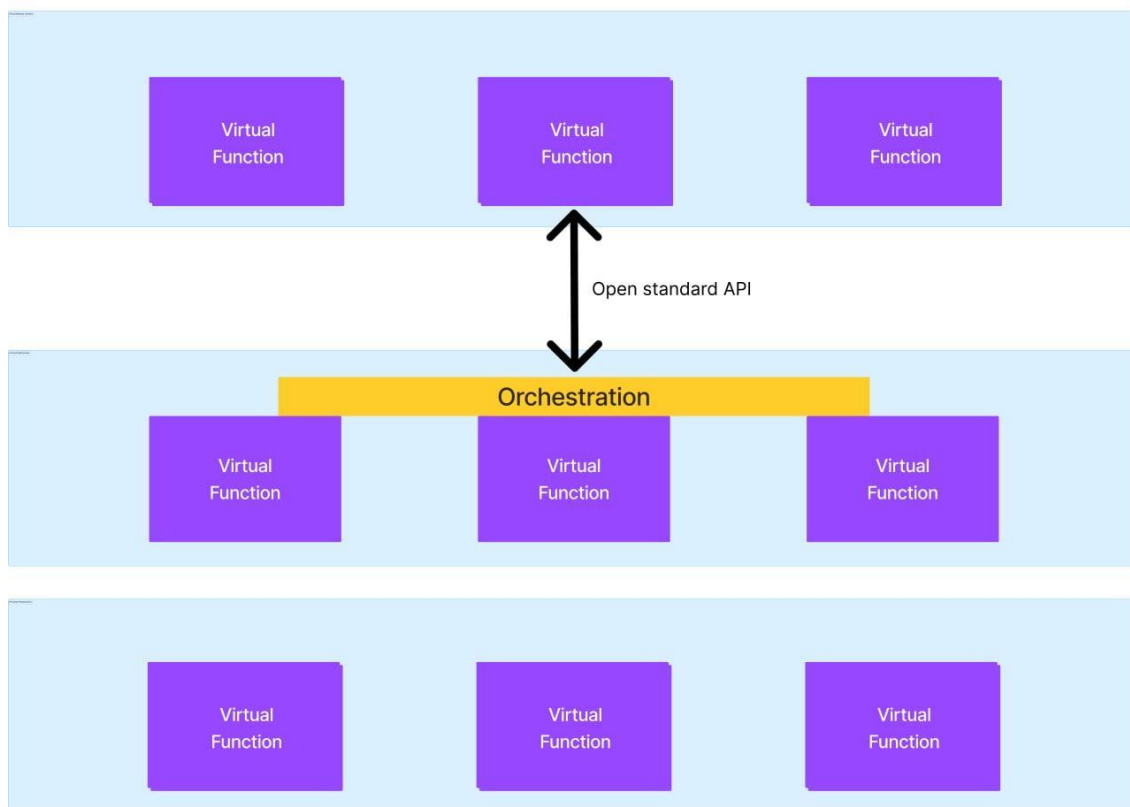


Рис. 4. Архитектура NFV

Virtual machines and containers

Создание виртуальной машины (VM) обеспечивает виртуализацию физического ресурса, в то время как экспериментатор может запускать свою операционную систему. Ключевым принципом виртуальной машины является совместное использование ресурсов, таких как память, хранилище и сеть, изолированным образом. Следовательно, функциональность виртуальной машины полностью изолирована от хоста и других гостевых виртуальных машин, где несколько виртуальных машин также могут быть запущены на одной физической машине одновременно.

В свою очередь контейнер, является облегченной альтернативной виртуальной машины на основе гипервизора. Контейнер создается с использованием виртуализации на уровне операционной системы, где физический сервер виртуализируется и создаются экземпляры изолированных служб и приложений.

По прогнозам, к 2024 году к 5G подключится 1,5 миллиарда человек. Но пока единого стандарта 5G нет – ведется ряд тестирований инфраструктуры и технологий, многие из которых еще разрабатываются. Однако, виртуализация с самых ранних концептов была признана как одно из важнейших направлений, практикуемых в сетях пятого поколения. Таким образом совместная реализация технологий, которые были названы в этой статье, поможет упростить процесс создания, сегментирования и дальнейшего управления, и обслуживания виртуальных сетей, которые, как уже говорилось, занимают ключевую роль в

обеспечении слайсинга и упрощения эксплуатации сети со стороны конечного арендатора.

Список используемых источников:

1. Chen Q., Wang X., Lv Y. An overview of 5G network slicing architecture //AIP Conference Proceedings. – AIP Publishing LLC, 2018. – Т. 1967. – №. 1. – С. 020004.
2. Maaloul R. et al. Energy-aware routing in carrier-grade Ethernet using SDN approach //IEEE Transactions on Green Communications and Networking. – 2018. – Т. 2. – №. 3. – С. 844-858.
3. Jmal R., Fourati L. C. Emerging applications for future internet approach based-on SDN and ICN //2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA). – IEEE, 2017. – С. 208-213.
4. TR-526 Applying SDN Architecture to 5G Slicing Issue 1 April 2016
5. Yang P. et al. Catalyzing cloud-fog interoperation in 5G wireless networks: An SDN approach //IEEE Network. – 2017. – Т. 31. – №. 5. – С. 14-20
6. Spinelli F., Mancuso V. Toward enabled industrial verticals in 5G: A survey on MEC-based approaches to provisioning and flexibility //IEEE Communications Surveys & Tutorials. – 2020. – Т. 23. – №. 1. – С. 596-630.

Kazachenko I., Prosvetov A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of virtualization technologies to provide slicing in 5g networks.

This article will focus on technologies that provide the processes for creating and managing virtual networks. Software-defined networks, fog computing, multi-access edge computing, network function virtualization, virtual machines, and containers were covered. The presented technologies were considered from the point of view of compatibility within the framework of ensuring the operation of fifth generation networks.

Key words: *5G, slicing, virtualization, network function virtualization, software-defined networking, cloud computing, edge computing, fog computing*

УДК 654.1
ГРНТИ 50.41.23

АДАПТАЦИЯ СИСТЕМ NRI И WFM К ОТКРЫТОЙ ЦИФРОВОЙ АРХИТЕКТУРЕ TM FORUM

С. В. Кисляков, Е. А. Лочкарев, Д. И. Сухомлинов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Мир управления инфокоммуникациями движется в сторону реформирования подходов к разработке систем поддержки операций и управления. Осуществляется плавный переход концепции NGOSS/Framework к открытой цифровой архитектуре построения информационных систем автоматизации. В данной работе проведено сравнение инструментов новой и старых систем поддержки операций и систем поддержки бизнеса.

Open Digital Architecture, OSS/BSS системы, NGOSS/Framework, TM Forum, eTOM, Functional Architecture, Functional Framework

Реализация проекта ODA основывается на использовании концепции NGOSS/Framework международной некоммерческой организации TM Forum, предлагает свой набор инструментов:

- Функциональная архитектура бизнес-функций FA (Functional Architecture), приходит на замену Business Process Framework [1], необходимой для проектирования и разработки решений OSS/BSS;
- Функциональная структура программных приложений поставщика цифровых услуг FF (Functional Framework) появляется вместо карты приложений телекоммуникационной компании TAM (Telecom Applications Map), содержащей в себе классификацию функций, выполняемых используемыми в компании программными приложениями, в том числе системами OSS/BSS [2];
- Модель SID (Shared Information and Data model), которая выступает в качестве эталонной информационной модели информационной системы;
- Open APIs – набор стандартных API, обеспечивающих быструю, повторяемую и гибкую интеграцию между операциями и системами управления.

Функциональная архитектура хранит в себе основную идею карты Business Process Framework – совокупность структурированных бизнес-функций, из которых можно формировать бизнес-процессы. В основу архитектуры закладывается ряд принципов методологии TOGAF [3], которая является более высоким уровнем абстракции. Её использование позволяет выявлять дублирование функций и нерациональное использование ресурсов при автоматизации бизнес-процессов. Благодаря чему, данную архитектуру можно будет применить не только в сфере телекоммуникаций, но и в любой другой.

Помимо перераспределения бизнес-функций, открытая цифровая архитектура предлагает поделить ПО на небольшие самостоятельные компоненты. Предполагается, что весь более сложный продукт должен состоять из независимых друг от друга элементов. Преимущество в том, что программное

обеспечение собирается как «пазл», внедряется в ландшафт какого-либо IT-поставщика цифровых услуг, а когда появляется необходимость замены одной из частей, то можно исключить этот компонент, слабо связанный с другими компонентами стандартными программными интерфейсами и заменить в зависимости от потребностей. Можно сказать, что компоненты ODA – это автономные программные неделимые модули, предназначенные для реализации конкретных бизнес-целей.

Переход к ODA подразумевает изменение бизнес- и программных приложений цифрового предприятия, сохраняя идею модели SID, смену монолитных программных продуктов на платформу с ODA компонентами, взаимодействующими через открытые стандартные API. В отличие от NGOSS/Frameworkx, ODA нацелена на автоматизацию не только операторов связи, но и на любую другую сферу, где предоставляются цифровые услуги. Во многом эта универсальность достигается согласованием с TOGAF. Вместо «монолита» [4] OSS/BSS каждый сервис будет представлять собой четко определенный функционально самодостаточный компонент, взаимодействующий с другими компонентами.

Если смотреть с точки зрения разработки, то нужно определиться: какие ключевые функции должны быть у ODA компонентов? как их формировать, отталкиваясь от задач разработчика ПО? как определить минимальную функциональность, но при этом достаточную для описания системы? В планы дальнейшей работы включено исследование двух OSS-систем (из большой продуктовой линейки) НТЦ АРГУС - WFM, NRI с целью разделения этих монолитных систем на ODA-компоненты.

Одна из анализируемых систем – NRI (Network Resource Inventory) (рис. 1). АРГУС NRI (Технический учет) призван автоматизировать процессы учета, обработки и анализа информации по линейно-техническим объектам, сооружениям и услугам с помощью современных информационных технологий [5]. Функциональность по Application Process Framework (TAM) представлена на рис.. Функциональность отражена группировками функций программных приложений:

- Resource Process Management (Управление процессами уровня ресурсов) предоставляет взаимодействие с системами NMS;
- Resource Inventory Management (Учет ресурсов) дает возможность получать консолидированные отчетности по всей инфраструктуре и оборудованию на сети Оператора;
- Location Management (Управление местоположением ресурса) позволяет проводить поиск местоположения ресурса на карте;
- Capability Specification Management (Управление возможностями ресурсов) дает контроль и упрощение внесения данных за счет использования шаблонов;
- Service Inventory Management (Учет услуг) подразумевает учёт услуг, связанных с соответствующим ресурсом;

- Network number Inventory Management (Учёт номерной емкости сети) дает автоматизированный подбор номера и предоставление пула номеров для выбора номера клиентом;
- Resource Order Management (Управление заказами на ресурсы) позволяет проводить автоматическую проверку технической возможности предоставления услуги.

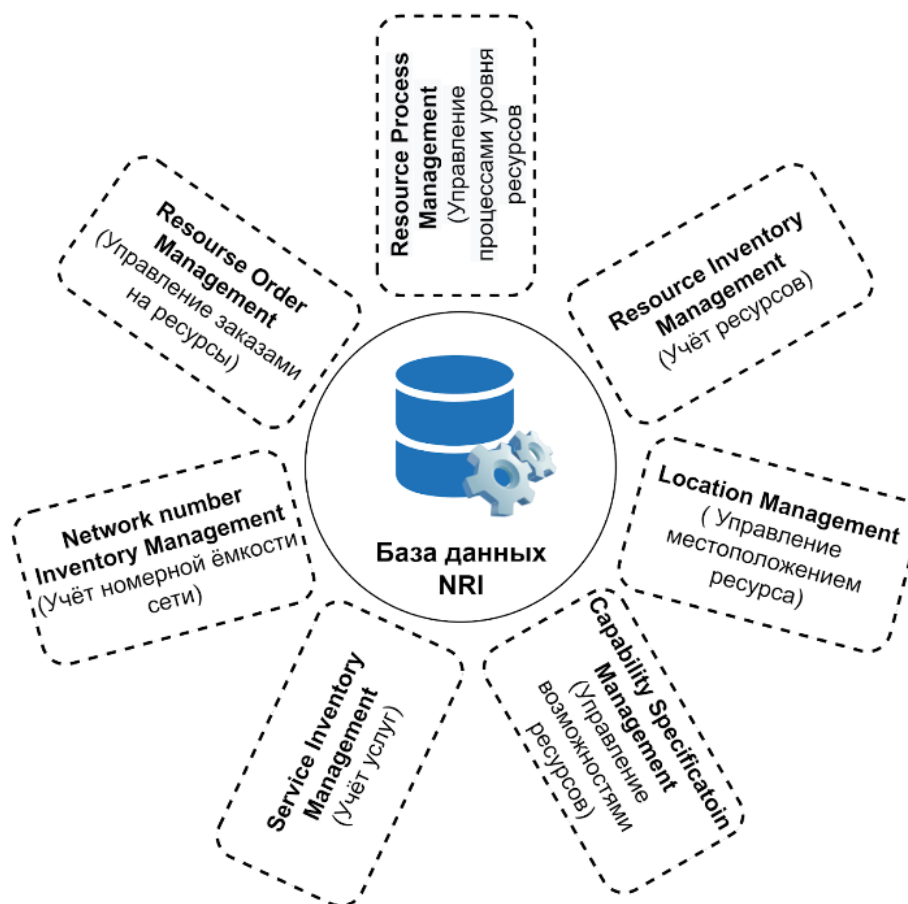


Рис. 1. Возможности Network Resource Inventory

Система управления рабочей силой АРГУС Workforce Management (WFM) автоматизирует бизнес-процессы управления персоналом, имеет целый ряд удобных и полезных инструментов для управления расписаниями и маршрутами.

Функциональность по Application Process Framework (TAM) представлена на рис. 2. Функциональность отражена группировками функций программных приложений:

- Workforce Schedule Management (Управление рабочими расписаниям)
- Work Order Analysis (Анализ заказов на работы)
- Work Order Assignment & Dispatch (Распределение и назначение заказов на работы)
- Work Order Tracking & Management (Контроль выполнения работ)
- Workforce Configuration and Setup (Настройка зон обслуживания и навыков рабочих)

• Workforce Management Reporting (Формирование отчётности об управлении рабочими ресурсами)

WFM лежит на пересечении областей Fulfillment и Assurance. Assurance позволяет производить прием обращений и установление неисправностей, а Fulfillment дает возможность подключать услуги и обрабатывать клиентские заказы. Данная система позволяет более эффективно управлять рабочей силой, устранять неисправности сети и оптимизировать рабочие процессы, повышая результативность работы сотрудников.

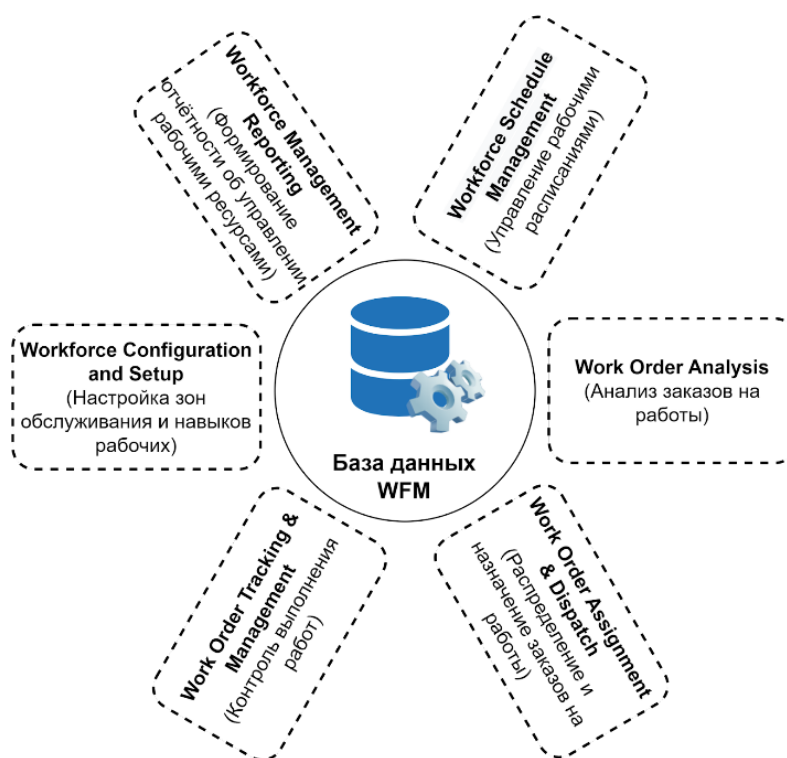


Рис. 2. Возможности Workforce Management

Таким образом, чтобы адаптировать системы NRI и WFM к открытой цифровой архитектуре TM Forum необходимо разделить данные продукты на ODA-компоненты - самодостаточные единицы, взаимодействующий с другими такими же единицами. Для этого требуется провести анализ функциональности NRI и WFM систем и исследовать их границы на Functional Architecture и Functional Framework. Это будет целью исследования в дальнейших работах.

Список используемых источников:

1. Современные подходы к автоматизации бизнес-процессов операторов связи : учебное пособие / А. Б. Гольдштейн, С. В. Кисляков ; СПбГУТ. – СПб., 2020. – 84 с.
2. Самуйлов, К. Е. Бизнес-процессы и информационные технологии в управлении телекоммуникационными компаниями / К. Е. Самуйлов, А. В. Чукарин, Н. В. Яркина. – М. : Альпина Паблишер, 2016. – 512 с.
3. Гольдштейн А.Б., Кисляков С.В. Концепция открытой цифровой архитектуры: эволюция или революция? // Вестник связи. - 2022. - №6.
4. Кисляков С.В., Майоров В.В. Разработка бизнес-процесса подключения услуги на основе TM FORUM OPEN DIGITAL ARCHITECTURE // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). - Санкт-Петербург: 2022.

5. Продукты и решения // argustelecom URL: <https://argustelecom.ru/> (дата обращения: 13.11.2022).

Kislyakov S., Lochkarev E., Sukhomlinov D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Adapt NRI and WFM systems to the open digital architecture of the TM Forum.

The world of infocommunication management is moving towards reformatting approaches to the development of operations and management support systems. The NGOSS/Frameworks concept is moving smoothly to an open digital architecture for building automation information systems. This paper compares the tools of the new and old operations support systems and business support systems.

Key words: Open Digital Architecture, OSS/BSS системы, NGOSS/Frameworks, TM Forum, eTOM, Functional Architecture, Functional Framework.

УДК 004.624
ГРНТИ 20.51.19

РАЗРАБОТКА ПРИЛОЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ МИКРОСЕРВИСНОЙ АРХИТЕКТУРЫ ДЛЯ СОСТАВЛЕНИЯ ПРОГНОЗА ЛАВИННОЙ ОПАСНОСТИ И РАСПРОСТРАНЕНИЕМ ЕГО ПОСРЕДСТВОМ ТЕЛЕГРАММ БОТА

Д. А. Коничев, А. В. Ткачук

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современные телекоммуникационные услуги охватывают широкий спектр деятельности человека, с помощью данных услуг мы получаем информацию о прогнозе погоды, ценах акций, расписании работы заведений, а также с предоставлением данных услуг можно распространять информацию об опасных природных явлениях. Например – лавины в горных местностях. Для этого необходимо реализовать приложение, которое в автоматизированном режиме собирает информацию, рассчитывает и производит составление прогноза на основе данных, доступных в открытых источниках. На основе данного расчета идет рассылка прогнозов пользователям. Это позволит увеличить информированность населения об опасных погодных явлениях и решит проблему ручной разработки прогнозов т.е. автоматизирует процесс работников лавинных служб.

микросервисная архитектура, математическая модель, контейнеризация, база данных, телеграм бот, парсинг

Для такого приложения необходимо разработать схему работы, найти источники данных, на основе математики составить программный код, а также подготовить базу данных и написать телеграм бота для распространения данной информации (рис. 1).

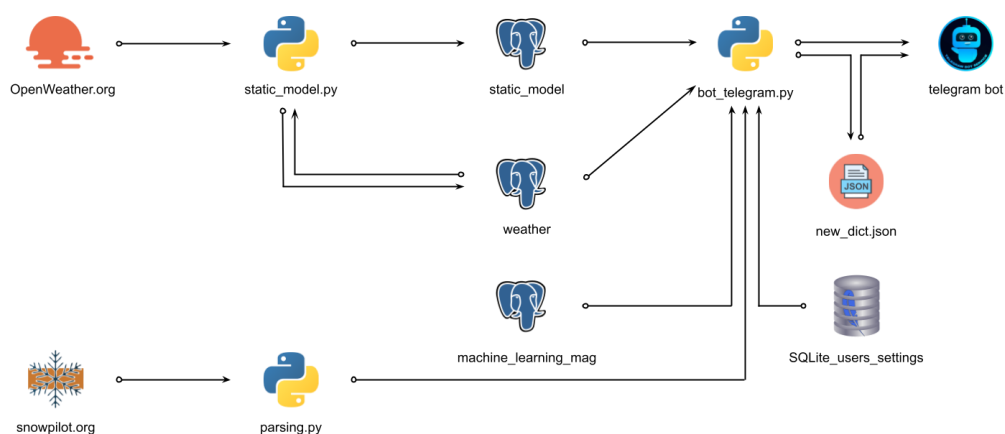


Рис. 1. Взаимодействие микросервисов

С целью автоматизации расчета лавинной опасности был выбран горный массив Хибины, т.к. в городе Кировск существует муниципальная лавинная служба, которая ежедневно формирует лавинный бюллетень. Это позволит

анализировать точность получаемого прогноза по расчету лавинной опасности разработанной автоматической системы.

Чтобы рассчитывать уровень лавинной опасности необходимо получать такие метеоданные, как температура, скорость ветра, направление ветра, количество осадков за определенный промежуток времени в виде снега или дождя и т.д. Такие данные можно брать с сайтов прогноза погоды, имеющих API (*Application programming interface*). Одним из таких сайтов является openweathermap.org (рис. 2). Для получения информации с этого сайта необходимо пройти регистрацию и получить собственный API Key [1]. Обращаясь к API через запрос GET, можно получить полный список погодных данных в формате JSON, с которым дальше будет удобно работать и использовать нужную нам информацию.

```
{
  "coord": {"lon": 33.6727, "lat": 67.6148},
  "weather": [{"id": 803, "main": "Clouds", "description": "broken clouds", "icon": "04d"}],
  "base": "stations",
  "main": {
    "temp": -6.22, "feels_like": -9.59, "temp_min": -6.22, "temp_max": -6.22, "pressure": 1024, "humidity": 93, "sea_level": 1024, "grnd_level": 981, "visibility": 10000, "wind": {"speed": 1.93, "deg": 325, "gust": 2.06}, "clouds": {"all": 51}, "dt": 1668340197, "sys": {"country": "RU", "sunrise": 1668321740, "sunset": 1668341817}, "timezone": 10800, "id": 548391, "name": "Kirovsk", "cod": 200}
}
```

Рис. 2. Пример ответа сайта openweathermap.org на запрос GET

Рассмотрим математическую составляющую прогнозирования лавинной опасности. Для расчета количества перенесенного снега на конкретную экспозицию, используем интеграл по времени, на протяжении которого скорость ветра больше 3 м/с, для этого вводим переменную $time_wind(t)$. Интеграл $snow_transfer$ рассчитывается для каждого румба отдельно.

$$snow_transfer = \int_0^t C * windSpeed^3 * k$$

где C - коэффициент пропорциональности, размер которого зависит от плотности снега в метелевых сугробах, для горного массива Хибин составляет $= 0.00031$, $windSpeed$ – скорость ветра м/с, k – коэффициент доступного для переноса снега, t – время.

Поддерживать сервис необходимо бесперебойно 24 часа в сутки, для этого используются вычислительные ресурсы компьютеров, на которых разворачивается инфраструктура. Каждый микросервис упаковывается в отдельный docker контейнер, что позволяет изолировать их друг от друга. Контейнеризация упрощает процесс мониторинга за отдельными частями всего сервиса, а также повышает отказоустойчивость системы [2].

Для хранения данных, полученных с сайта openweathermap.org, и результатов расчета данной проблемы была выбрана система управления реляционными базами данных PostgreSQL. Для взаимодействия python скриптов и PostgreSQL нужно установить модуль `psycopg2`. Данная библиотека позволяет устанавливать соединение с базой данных, создавать нужные нам таблицы, записывать и забирать рассчитанные данные [3, 4].

С целью предоставления информации по расчету пользователю было принято решение написать телеграм бота, используя библиотеку aiogram [5]. Задача бота состоит в информировании пользователя о фоновом уровне лавинной опасности, расчётных данных лавинных проблем и прогнозе погоды. Также можно получить сведения о шурфах. И всё это поможет пользователю оценить местность на безопасность.

Чтобы осуществить рассылку, была использована библиотека aioschedule. Она позволяет настроить точное время рассылки сообщений пользователям при помощи метода `“day.at('9:00')”` [6].

Для критических явлений, которые рассчитываются в таблице по “расчётным данным лавинных проблем”, будет присылать отдельное уведомление информирующие пользователя об опасности. В этой таблице есть столбец “Danger”. где от 1 до 4 определяется степень опасности лавины: 1 - лавины маловероятны, 2 - вероятны небольшие лавины, 3 - очень вероятно лавины, 4 - очень вероятно большие лавины.

В телеграм боте есть кнопка “Настроить рассылку”, благодаря которой, пользователь может задать боту, какие данные он хочет получать в рассылке (рис. 3). Для этого функционала было принято решение создать легкую файловую базу данных SQLite, так как к этой базе будет обращаться сам пользователь, и есть вероятность, что запросов будет много и база данных будет постоянно изменяться. В коде, для данного функционала, используется библиотека sqlite3 [7]. В эту базу будут записываться условия рассылки в виде ответов “Да”, “Нет”. Также в ней прописываются id пользователей, чтобы рассылки работали только для определённого пользователя. Эти настройки можно заново прописать, но перед этим нужно удалить данные с базы при помощи кнопки “Удалить настройки рассылки”.

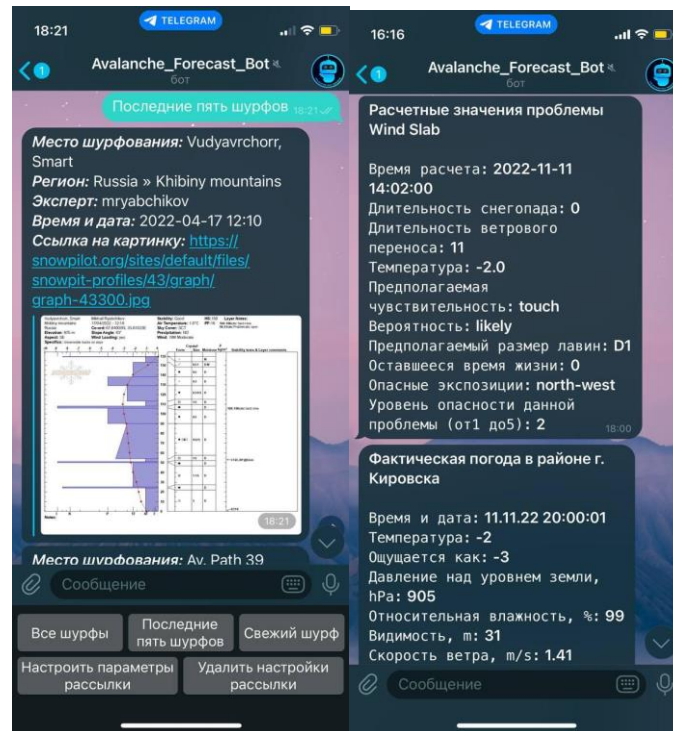


Рис. 3. Пример рассылки телеграм бота

Сведения о шурфах берутся прямо из сайта “snowpilot.org”. Это осуществляется при помощи парсинга (считывания) html страницы сайта. Для пайтона использовались библиотеки requests и bs4. Данные, которые были считаны будут записываться в JSON файл, как в словарь. Решение записывать данные в файл было основано на том, чтобы у пользователя была возможность просмотреть все шурфы или шурфы за неделю. В качестве словаря был выбран формат файла JSON, так как он является самым простым по заполнению и очень мало весит. Парсинг и запись данных в словарь происходит по нажатию кнопки “Свежий шурф”. Если такого шурфа ещё нет, то бот выдаст сообщение “Свежих шурфов ещё нет”. Но для того, чтобы пользователь постоянно не нажимал данную кнопку и не отслеживал появление нового шурфа, в коде прописан запрос к сайту раз в день через библиотеку asynscore, где идет обращение к последней записи шурфа и проверяется его id со всеми id, которые прописаны в словаре. Если такого id нет в словаре, то бот выдаст сообщение “Появился новый шурф”, иначе аналогично предыдущему сообщению. Также у нас осуществляется отбор по парсингу, нам требуются шурфы только определенных регионов, а именно: Khibiny mountains, Hibirny Mtns, Kirovsk.

В заключение можно сказать, что на сегодняшний день современные телекоммуникационные услуги играют немаловажную роль в жизни человека и имеют обширный функционал, которым мы можем пользоваться и развивать.

Список используемых источников:

1. Документация "How to make an API call". [Электронный ресурс]. // openweathermap.org., 2022. URL: <https://openweathermap.org/current/> (Дата обращения: 11.11.2022)

2. Документация "Docker". [Электронный ресурс]. // docs.docker.com., 2022. URL: <https://docs.docker.com/get-started/overview/> (Дата обращения: 11.11.2022)
3. Документация "PostgreSQL". [Электронный ресурс]. // www.postgresql.org., 2022. URL: <https://www.postgresql.org/docs/14/intro-what-is.html> (Дата обращения: 11.11.2022)
4. Документация "Psycopg 2.9.5 documentation". [Электронный ресурс]. // <https://www.psycopg.org/>, 2022. URL: <https://www.psycopg.org/docs/> (Дата обращения: 11.11.2022)
5. Документация aiogram "Quick start". [Электронный ресурс]. // docs.aiogram.dev/en/latest/, 2022. URL: https://docs.aiogram.dev/en/latest/quick_start.html (Дата обращения: 11.11.2022)
6. Сайт вопросов и ответов для программистов "Stack Overflow". [Электронный ресурс]. // [ru.stackoverflow.com.](https://ru.stackoverflow.com/), 2022. URL: <https://ru.stackoverflow.com/questions/1144849/Как-совместить-работу-aiogram-и-schedule-на-Telegram-bot> (Дата обращения: 11.11.2022)
7. Документация "sqlite3 — DB-API 2.0 interface for SQLite databases" [Электронный ресурс]. // python.org., 2022. URL: <https://docs.python.org/3/library/sqlite3.html> (Дата обращения: 11.11.2022)

Konichev D., Tkachuk A.

The Bonch-Bruевич Saint - Petersburg State University of Telecommunications

Development of an application using a microservice architecture for making an avalanche hazard forecast and distributing it via bot telegrams.

Modern telecommunication services cover a wide range of human activities, with the help of these services we receive information about the weather forecast, stock prices, opening hours of establishments, and with the provision of these services, information about natural hazards can be disseminated. For example, avalanches in mountainous areas. To do this, it is necessary to implement an application that automatically collects information, calculates and makes a forecast based on data available in open sources. Based on this calculation, forecasts are being sent to users. This will increase the awareness of the population about dangerous weather events and solve the problem of manual development of forecasts, i.e. automates the process of avalanche services.

Key words: *micro service architecture, mathematical model, containerization, database, telegram bot, parsing*

УДК 621.3911
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ТРАФИКА УЗЛА ДОСТУПА С ПОМОЩЬЮ СИСТЕМЫ АМС

Б. Я. Лихтциндер, А. С. Садкова

Поволжский государственный университет телекоммуникаций и информатики

В работе рассмотрена система АМС моделирования параметров трафика мультисервисных сетей. Система базируется на принципах интервального метода анализа потоков общего вида систем массового обслуживания. Рассмотрена структурная схема программного обеспечения. Показана возможность определения коэффициентов аппроксимации.

СМО, трафик, узлы доступа, система анализа, потоки заявок

Система АМС предназначена для анализа характеристик стационарных ординарных потоков заявок, представляющих пакеты или кадры мультисервисных сетей связи.

В процессе моделирования программа определяет характеристики, потоков заявок, представленные ниже [1].

«Входной поток (I)» – отображает нарастающий график суммарного времени, от начального момента до момента прихода очередной заявки.

«A(I)» – отображает числа заявок, поступающих в систему в течение последовательных интервалов времени τ , равных среднему времени обработки одной заявки.

«mA(ρ)» – график отображает зависимость среднего числа заявок, поступающих в течение интервалов времени τ , от коэффициента загрузки ρ . Если λ – средняя интенсивность поступления заявок, то коэффициент загрузки $\rho = \lambda\tau$.

«dispA(ρ)» – график отображает зависимость дисперсии числа заявок, поступающих в течение интервалов времени τ , от коэффициента загрузки ρ .

«q(t)» – числа заявок в очереди, на интервалах τ , соответствующих моментам времени t и коэффициенту загрузки ρ .

«mq(ρ)» – график отображает зависимость среднего числа заявок, в очереди, от коэффициента загрузки ρ .

«dispq(ρ)» – график отображает зависимость дисперсии числа заявок, в очереди, от коэффициента загрузки ρ .

«P(i)» – вероятности прихода i -заявок, в течение интервалов времени τ , соответствующих коэффициенту загрузки ρ .

«P0(i)» – условные вероятности прихода i -заявок, в течение интервалов времени τ , соответствующих коэффициенту загрузки ρ .

«mE(ρ)» – зависимость значения числителя обобщенной формулы Хинчина-Поллячека от коэффициента загрузки ρ .

« $dq(\rho) = \alpha(\rho - \rho_0)^2 + \beta(\rho - \rho_0)$ » – аппроксимация зависимости среднего значения дисперсии размеров очереди q от коэффициента загрузки ρ .

« $\sigma(\rho)$ » – зависимость среднеквадратичного отклонения размеров очереди от коэффициента загрузки ρ .

« $\rho(q) = aq + b\sqrt{q} + \rho_0$ » – аппроксимация зависимости коэффициента загрузки ρ от среднего значения размеров очереди q .

« $K(I)$ » – числа приборов, занятых обработкой на текущем интервале времени.

« $PK(I)$ » – вероятности чисел приборов, занятых обработкой.

« $M(t)$ » – нормированная корреляционная функция потока, при заданном значении коэффициента загрузки, в зависимости от интервала сдвига по времени.

$I(t)$ – интеграл от нормированной корреляционной функции потока, при заданном значении коэффициента загрузки.

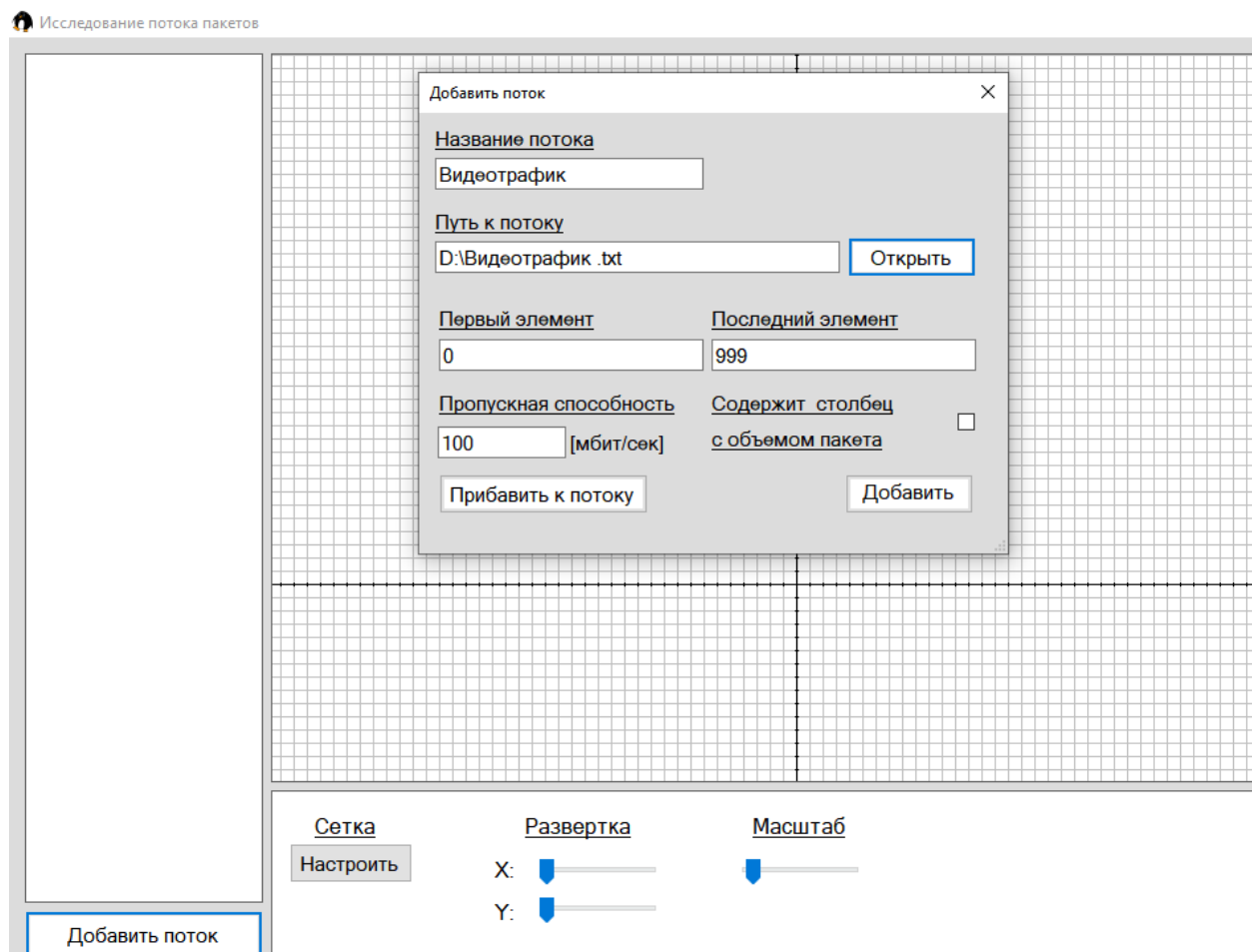


Рис. 1. Добавление нового потока

Для начала исследования в программу необходимо добавить информацию об исследуемом потоке, рис. 1. Система позволяет поочередно ввести на обработку нескольких одноименных или различных потоков. Для каждого из потоков появляется своя иконка с названием потока. Графики,

предоставляющие собой результаты обработки, могут выводиться по одному, то есть для каждого потока отдельно, или одновременно и совмещаться. На рис. 2 представлены четыре графика зависимости дисперсии от коэффициента загрузки для потоков видео кодеков H.264. Демонстрация каждого графика может отключаться и включаться нажатием правого поля на иконке с соответствующим потоком, рис. 2. Каждый из потоков может быть удален из системы нажатием поля со знаком «x» на соответствующей иконке. Также может быть произведено суммирование нового потока с предыдущим. Для этого служит кнопка «Прибавить к потоку», и в этом случае анализируется суммарный поток (моделируется мультиплексирование потоков).

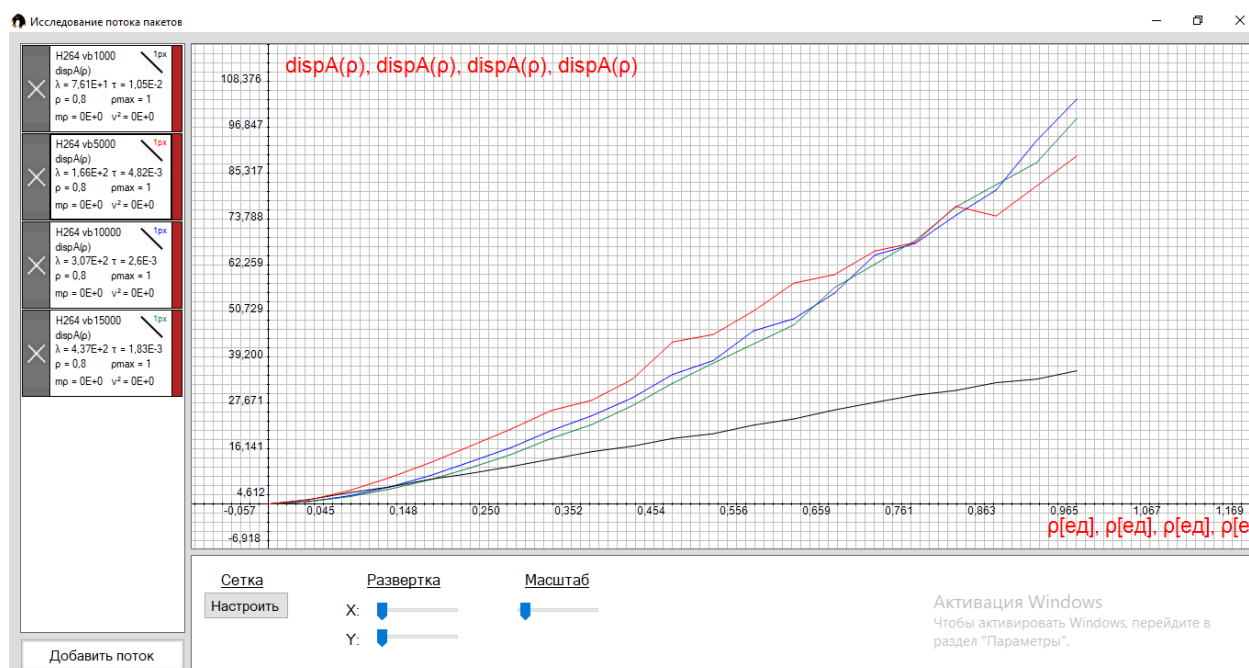


Рис. 2. Представление графиков

С помощью системы АМС возможно выполнение комплекса исследовательских работ:

1. Изучение характеристик простейшего потока заявок.
2. Изучение потоков заявок с различными распределениями интервалов между заявками.
3. Анализ характеристик потоков пакетов от видео кодеков.
4. Анализ характеристик потоков пакетов видео трафика.
5. Изучение мультиплексирования потоков.
6. Анализ СМО с ограничением очереди.

Таким образом, разработанное программного обеспечение имеет практическую ценность для специалистов при анализе потока МСС. Дальнейшее ее развитие предполагает автоматический сбор информации о потоке и обработку трафика в реальном времени, что позволит получать усредненные значения коэффициентов обобщенной формулы Хинчина-Полячека, которые будут точнее описывать поток МСС.

Список используемых источников:

1. Лихтциндер Б. Я. Трафик мультисервисных сетей доступа (интервальный анализ и проектирование): учебное пособие. Самара: ПГУТИ, 2018. С. 206-215.

Likhttsinder B., Sadkova A.

The Povolzhskiy State University of Telecommunications and Informatics

Access Node Traffic Examination Using AMS Systems.

The paper considers the AMS system for modeling traffic parameters of multiservice networks. The system is based on the principles of the interval method for analyzing flows of a general type of queuing systems. The block diagram of the software is considered. The possibility of determining the approximation coefficients is shown.

Key words: *queuing system, traffic, access nodes, analysis system, request flows.*

УДК 004.724.3
ГРНТИ 49.38.49

ИССЛЕДОВАНИЕ МИКРОСЕРВИСНОЙ АРХИТЕКТУРЫ ДЛЯ ПОДДЕРЖКИ ЭКСПЛУАТАЦИОННЫХ ПРОЦЕССОВ

А. В. Моисеева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч Бруевича

Микросервисная архитектура, также известная как «микросервисы», определяется как метод разработки, который разбивает программное обеспечение на модули со специализированными функциями и детализированными интерфейсами. В данной статье речь пойдет о микросервисной архитектуре, а именно системе, где каждый продукт системы (кеш-платформа, биллинг, инвентори система, система хранения клиентских аккаунтов и т.д.) может развиваться независимо от смежных систем, обеспечивая повышенную гибкость эксплуатации.

микросервисы, API, REST

Микросервисы — это архитектурный и организационный подход к разработке программного обеспечения, при котором ПО состоит из небольших независимых сервисов, взаимодействующих через четко определенные API, которые принадлежат небольшим автономным командам.

Такой подход к архитектуре делает сервисы самодостаточными единицами с разным стеком технологий, которые общаются между собой посредством обмена сообщений в виде REST-запросов. Каждый сервис отвечает за одну бизнес-логику и имеет свою базу данных, а группа сервисов объединяется в один API-продукт. Таким образом один пользовательский запрос может порождать пять, а то и десятки каскадных вызовов смежных сервисов. Такие запросы могут выполняться синхронно и асинхронно [1].

Синхронный сценарий - это такой поток выполнения бизнес логики, в котором выполнение идет сверху вниз, но когда запросов десятки, такой подход может значительно снизить скорость обработки. Для таких случаев используют асинхронные сценарии, которые позволяют реализовать механизм параллельной передачи сообщений между сервисами, образуя древовидный поток. При этом не нужно беспокоиться, что какой-то запрос потеряется и так и не дойдет до получателя, для решения таких проблем существуют брокеры, благодаря которым вы можете отправлять сообщения с одной стороны, а с другой стороны подписываться на эту очередь и получать их. Такое ПО гарантирует, что сообщения останутся в очереди, даже если пользователь по какой-то причине недоступен, он сможет получить их после восстановления. Сообщения, помещенные в очередь, сохраняются до тех пор, пока потребитель не извлечет их [2].

Важно отметить, что сервисы, передавая сообщения друг другу в действительности ничего не знают друг о друге. Микросервисную архитектуру можно рассматривать, как конструктор Lego, где каждая деталь

(сервис) является независимым продуктом, эксплуатация и выход из строя которого не влияет на работу всей системы в целом. При отказе одного из сервисов перестает работать только та бизнес-логика, за которую он отвечает [3].

Парадигма микросервисов предоставляет командам разработчиков более децентрализованный подход к созданию программного обеспечения. Каждая служба может быть изолирована, перестроена, повторно развернута и управляться независимо. Например, если программа неправильно создает отчеты, ИТ-персонал может отследить проблему до конкретной службы, а затем протестировать, перезапустить, исправить и повторно развернуть эту службу по мере необходимости, независимо от других служб [4].

Давайте представим, что вы создаете приложение по подключению услуг связи, где клиент имеет возможность выбрать красивый номер за дополнительную плату. В микросервисной архитектуре приложение будет состоять из нескольких компонентов, включая StoreFrontUI, который реализует пользовательский интерфейс, а также компоненты, хранящие пользовательские аккаунты, учета коммерческих сущностей и бронирований. Каждый такой компонент будет представлять собой отдельный API-продукт, объединяющий в себе сервисы обработки запросов и сервисы баз данных. На рис. 1 представлено упрощенное функциональное представление архитектуры, которое показывает как будет организовано взаимодействие в таком приложении.

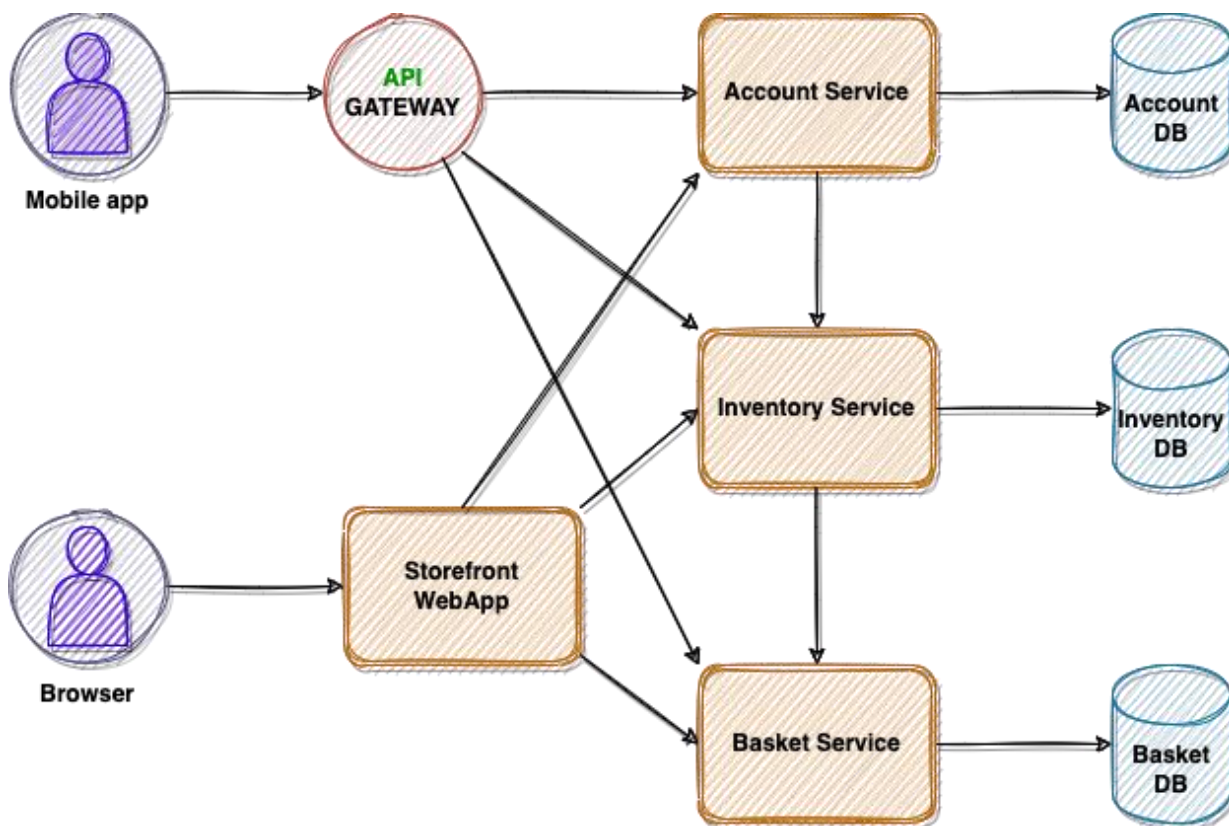


Рис. 1. Упрощенное функциональное представление архитектуры

Это решение будет иметь ряд преимуществ:

- Обеспечение непрерывной доставки и развертывания больших и сложных приложений.
 - Улучшение ремонтпригодности — каждый сервис относительно небольшой, поэтому его легче понять и изменить.
 - Лучшая тестируемость — сервисы меньше по размеру и быстрее тестируются.
 - Улучшенная развертываемость — сервисы можно развертывать независимо.
 - Возможность организовать усилия по разработке вокруг нескольких автономных команд. Каждая команда владеет и отвечает за один или несколько сервисов. Каждая команда может разрабатывать, тестировать, развертывать и масштабировать свои сервисы независимо от всех других команд.
- Каждый микросервис относительно мал:
 - Легче понять разработчику.
 - IDE работает быстрее, делая разработчиков более продуктивными.
 - Приложение запускается быстрее, что повышает продуктивность разработчиков и ускоряет развертывание.
- Улучшенная изоляция неисправностей. Например, если в одной службе есть утечка памяти, то затронута будет только эта служба. Другие службы продолжают обрабатывать запросы. Для сравнения, один неисправный компонент монолитной архитектуры может вывести из строя всю систему.
- Устраняет любые долгосрочные обязательства перед стек технологий. При разработке нового сервиса вы можете выбрать новый стек технологий. Точно так же при внесении серьезных изменений в существующую службу вы можете переписать ее, используя новый стек технологий.

Микросервисы разбивают монолитные приложения на более мелкие, более управляемые компоненты, с которыми проще работать. Конечная цель перехода на микросервисы — реализовать распределенную, слабосвязанную и независимую структуру, которая позволит сделать процессы эксплуатации гибкими и легкоуправляемыми. Таким образом, нажатая клиентом кнопка заказа какой-либо услуги будет направлять REST-запрос от одного API к другому до эксплуатации, а по завершению этой цепочки у клиента будет успешно подключенный сервис.

Список используемых источников:

1. Конференция HighLoad++ Весна 2021 [Электронный ресурс]. URL: <https://www.youtube.com/watch?v=eI1QQUrFUZI> (дата обращения 11.10.2022).
2. Part 1: RabbitMQ for beginners - What is RabbitMQ? [Электронный ресурс]. URL: <https://www.cloudamqp.com/blog/part1-rabbitmq-for-beginners-what-is-rabbitmq.html> (дата обращения 12.10.2022).

3. Современная микросервисная архитектура: принципы проектирования [Электронный ресурс]. URL: <https://habr.com/ru/company/innotech/blog/683550/> (дата обращения 09.11.2022).

4. What are microservices, and what is a microservices architecture? [Электронный ресурс]. URL: <https://www.techtarget.com/searchapparchitecture/definition/microservices> (дата обращения 12.10.2022).

Moiseeva A.

The Bonch-Bruевич Saint- Petersburg State University of Telecommunications

Microservice architecture research to support operational processes.

Microservice architecture, also known as ‘microservices,’ is defined as a development method that breaks down software into modules with specialized functions and detailed interfaces. This article will focus on microservice architecture, namely, a system where each product of the system (cash platform, billing, inventory system, client account storage system, etc.) can depend on adjacent systems, increasing the flexibility of operation.

Key words: Microservices, API, REST.

УДК 004.716
ГРНТИ 49.34.39

АНАЛИЗ РЫНКА И АКТУАЛЬНОСТЬ СИСТЕМ ВИДЕОКОНФЕРЕНЦСВЯЗИ (ВКС)

В. Н. Некрасов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире сложно представить корпоративную среду без систем видеоконференцсвязи, она используется почти так же часто, как и телефония, при этом имеет множество преимуществ. ВКС позволяет оперативно решать деловые вопросы и экономить денежные средства компании.

видеоконференцсвязь, Н.323, SIP

Введение

Видеоконференцсвязь (ВКС) — это технология, обеспечивающая одновременную передачу видео и звука между двумя и более пользователями, с помощью аппаратно-программных средств коммуникации [1]. Американская компания Gartner, специализирующаяся на исследованиях рынка информационных технологий, в своём отчете от 7 октября 2021 года пишет, что к 2025 году более 50 % всех корпоративных встреч будут проводиться в формате видеоконференций [2].

Актуальность

Рассмотрим, какие задачи решают современные системы видеоконференцсвязи.

- преодоление географических барьеров для коммуникаций внутри организации. В следствии чего, сокращение количества командировок;
- поддержка работы из домашнего офиса, возможность удаленно провести собеседование и оценить навыки соискателя;
- повышение вовлеченности и контроль удаленных работников;
- отсутствие необходимости в большинстве деловых командировок и снижение сопутствующих расходов;
- обучение студентов без привязки к региону;
- автоматизация расшифровки и записи дискуссий в рамках видеоконференций.

На самом деле это совсем не полный список задач, решение которых упрощает ВКС. Использование видеоконференцсвязи увеличивает эффективность работы и взаимодействия людей из разных точек мира, а так-же заметно снижает расходы за счет возможности решать большинство вопросов on-line [3].

Думая о будущем, можно ожидать дальнейший рост ВКС-рынка, занятого отечественными вендорами. Дмитрий Одинцов, директор по развитию в компании TrueConf уверен, что российские системы видеоконференцсвязи способны полностью заменить зарубежные аналоги. Отечественные решения

ВКС систем уже полноправно конкурируют с иностранными в части стандартного функционала, характерного для профессиональных продуктов, а также имеют уникальный, собственный функционал, ориентированный российских заказчиков.

Универсальные зарубежные ВКС-продукты не всегда подходят под задачи заказчиков из государственного сектора или корпоративной сферы, которым необходим определенный функционал системы и высокие требования к ее безопасности. Например, российские ВКС могут похвастаться успешно реализованными решениями обеспечения безопасности в виде криптомаршрутизаторов и VPN [2].

Анализ рынка

Основной объём внедрений ВКС охватывает государственный сектор и сфера образования, а так же значительную часть занимает средний и крупный бизнес, особенно компании имеющие множество филиалов. С помощью систем видеоконференцсвязи очень удобно обмениваться информацией и контролировать региональные подразделения. В отраслевом разрезе, ВКС системы внедряются чаще в госструктурах, образовании, ИТ и торговле [2].

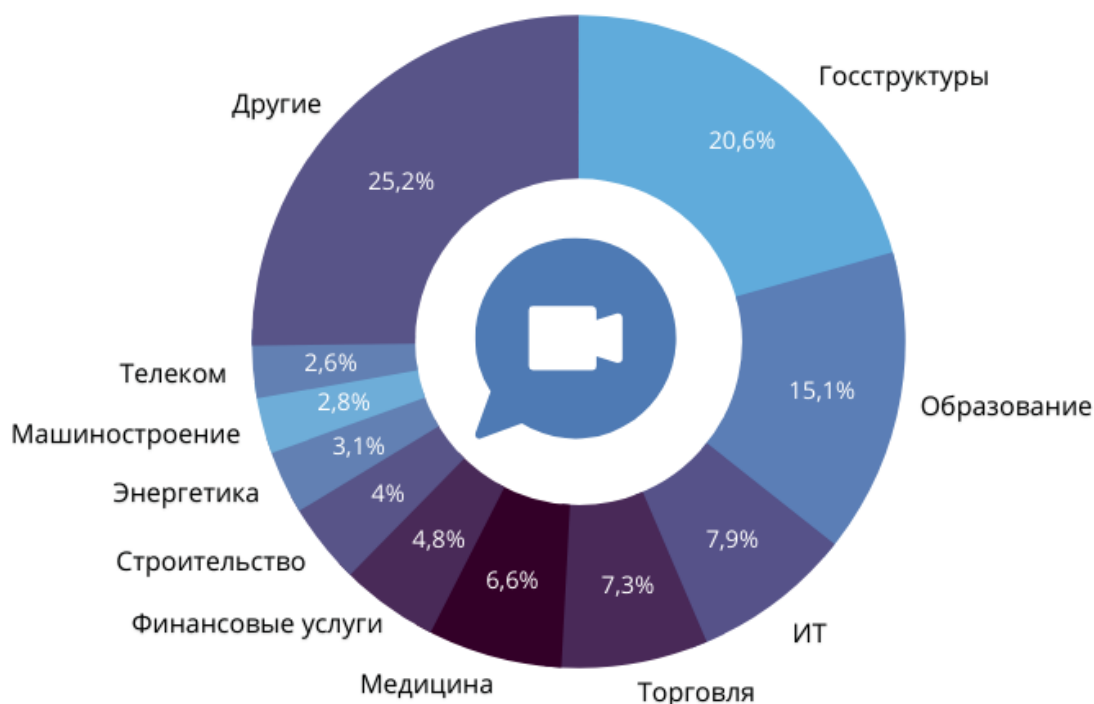


Рис. 1. Отраслевое распределение проектов внедрения систем видеоконференцсвязи.

На мировом рынке лидируют такие гиганты, как Zoom, Microsoft, Google, Cisco и др., но мне бы хотелось посмотреть, как обстоят дела в России.

Цитата Бориса Попова, директора по развитию компании Vinteo: «В 2000-х годах системы ВКС были очень дорогими и достаточно сложными, мало кто мог себе их позволить. Крупные коммерческие и государственные структуры стали основными заказчиками видеоконференцсвязи» Около 90% ВКС сетей были построены с помощью оборудования зарубежных компаний. Среди которых

наиболее популярными были Avaya, Polycom, Cisco Systems, а выход на рынок отечественных производителей произошёл в 2014 году в рамках программы импортозамещения [2].

Пандемия дала сильный толчок развитию видеоконференцсвязи и в 2022 году рост продолжается. На данный момент в России реализовано более 5 тыс. проектов по внедрению систем ВКС.

Среди разработчиков по количеству реализованных проектов, лидирующие позиции занимают компании Spirit (VideoMost) и TrueConf, вместе они забирают около 70% рынка [2].

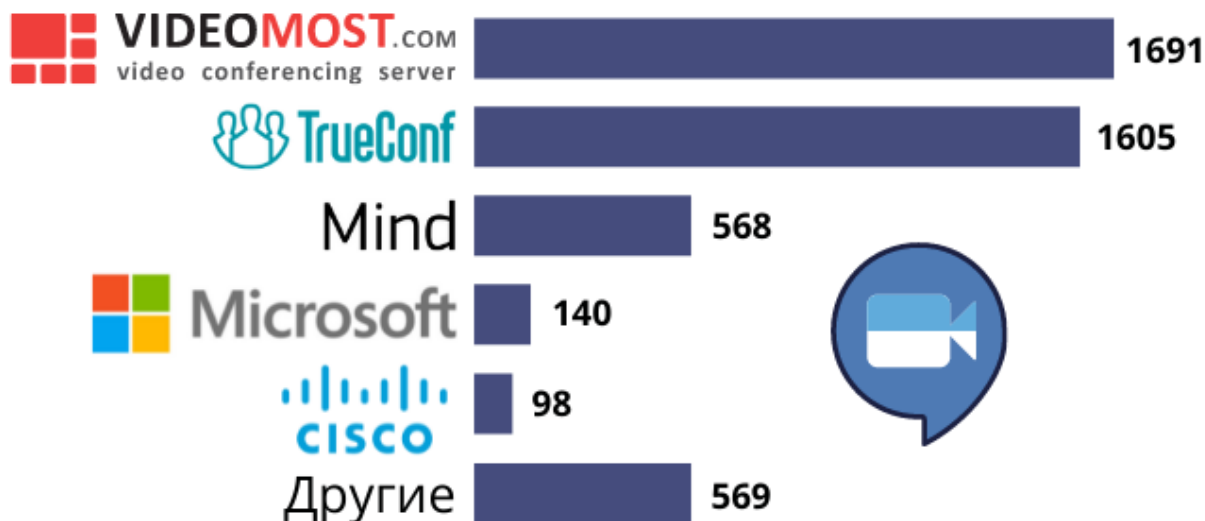


Рис. 2. Вендоры систем видеоконференцсвязи, лидирующие на российском рынке по количеству реализованных проектов. Согласно данным TAdviser за период наблюдений с 2005 по ноябрь 2021 г.

Здоровая конкуренция толкает рынок, но есть свои нюансы. Некоторые компании, или не поддерживают, или имеют ограничения по интеграции с внешними системами по протоколам SIP и H.323. Из-за чего, дистанционное образование, телемедицина и другие важные направления очень медленно развиваются, потому как системы ВКС в разных ведомствах, которые должны работать вместе, в одной сети, оказываются несовместимы друг с другом.

Заключение

Проведенный анализ показывает актуальность и востребованность систем видеоконференцсвязи для решения коммуникативных задач органов государственной власти, крупных корпораций, а так же средних и малых предприятий. Необходимо отметить, что отечественные решения систем ВКС отлично справляются с этой задачей.

Список используемых источников:

1. Труконф. Видеоконференцсвязь [Электронный ресурс]. URL: <https://trueconf.ru/videokonferentssvyaz.html#070>
2. Российский рынок видеоконференцсвязи 2021: тренды, барьеры, перспективы [Электронный ресурс]. URL: <https://www.tadviser.ru/index.php>

3. Denstadli J.M., Julsrud T.E., Hjortol R.J. *Videoconferencing as a Mode of Communication: A Comparative Study of the Use of Videoconferencing and Face-to-Face Meetings // Journal of Business and Technical Communication*, 07.12.2011. С. 65-90.

Nekrasov V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Market analysis and relevance of videoconferencing systems (VCS).

In today's world, it is hard to imagine a corporate environment without video conferencing systems, it is used almost as often as telephony, while it has many advantages. Videoconferencing allows you to quickly resolve business issues and save money for the company.

Key words: videoconferencing. H.323, SIP.

УДК 004.94
ГРНТИ 20.53

ПРИМЕНЕНИЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ В РЕШЕНИИ РАЗЛИЧНОГО РОДА ЗАДАЧ

Д. О. Якупов¹, С. В. Малахов²

¹Федеральное государственное бюджетное образовательное учреждение высшего образования

²«Поволжский государственный университет телекоммуникаций и информатики»

В статье рассматривается применение предсказательного и виртуального имитационного моделирования в решении различного рода задач. Для примера, смоделирована виртуальная сеть передачи данных. Сеть включает в себя кэширующий прокси-сервер и общий канал доступа в Интернет. Освещается роль и необходимость их дальнейшего развития.

виртуальное моделирование, имитационное моделирование, модели, Anylogic, абонент, прокси-сервер

В современных условиях со стремительным развитием общества накапливается большой объем данных в процессе различной деятельности человека, которые возможно рационально использовать. В информационной индустрии появилось целое направление, получившее название «хранилище данных (Data Warehouse)», где хранятся и эффективно обрабатываются данные. Собранные данные представляют собой основу для управленческих методов в области коммерческих систем. Полученные правильно организованные экспериментальные данные преобразуются в полезную информацию, на основе которой возможно создать компьютерную модель и проверить её работоспособность в различных критических и некритических ситуациях, с целью выявления проблемных областей, что позволит впоследствии улучшить модель. В этом и заключается актуальность рассматриваемой темы. Моделирование позволяет упрощать и сокращать время, а также автоматизировать процесс работы и поиска решения для различного рода задач.

В данной работе более подробно рассматривается предсказательное и виртуальное имитационное моделирование [1].

Модели предсказательного вида могут использоваться для того, чтобы спрогнозировать значение ответа функций без организации вспомогательных глобальных экспериментов или сложных технических расчетов. По своему существу, модели предсказательного вида – это ничто иное, как сложный полином, описывающий слой отклика функций модели.

Предсказательное моделирование может использоваться для восстановления и прогнозирования информации о событиях, которые принципиально невозможно наблюдать. На основе данной теории научной командой университета ПГУТИ было предложено использовать предсказательное моделирование в основе решения задачи по прогнозированию числа заболевших вирусом COVID-19 по Самарской области. Используя в

основе метод предсказательного имитационного моделирования, стало возможным подсчитать, сколько будет заболевших через определенный промежуток времени, а также смоделировать, сколько всего было носителей инфекции, зная данные о первоначальном количестве заболевших людей. Разработанная модель успешно позволяет спрогнозировать динамику распространения заболевания.

Моделирование виртуального типа способствует выполнению построения разных определенных признаков пространств и представление их изменений во времени. Также, данное моделирование способно показывать движение обозревателя в самом виртуальном пространстве, которое отображает изменение важных свойств предметов.

На основе виртуального имитационного моделирования работает имитационная система Any Logic, которая позволяет разработать любое бизнес-предприятие в виртуальной среде и симулировать различные риски или успехи для данного предприятия, для того чтобы выявить слабые стороны в стратегических решениях и защитить предприятие от банкротства [2].

С помощью виртуального моделирования, была построена сеть передачи данных, в которой абоненты подключены к общему каналу доступа в Интернет, и использующие кэширующий прокси сервер. Данная модель имеет назначение анализировать, насколько загружен канал связи. Смоделированная сеть передачи данных имеет следующие характеристики:

1. Абонент имеет свою отдельную линию, скорость передачи данных которой составляет 33 Мбит/с. Так, как не учитываются ошибки, возникающие на линии, скорость передачи материалов, которые получает пользователь равна 4,125 МБайт/с.

2. Затраченное количество времени для передачи запроса на материал от пользователя к серверу, и от сервера в сеть Интернет, не принималось во внимание.

3. Объем данных канала связи будет считаться без ограничений. Благодаря этому, материалы и файлы от разных абонентов будут иметь возможность отправляться из Интернета на сервер синхронно и параллельно.

4. Ресурсы прокси сервера, затраченные для обновления файлов, которые хранятся в буфере сервера – не берутся во внимание.

5. Длительность поиска данных в буфере сервера не зависит от нахождения данных в памяти прокси сервера.

Передача данных из сети Интернет с заданной скоростью зависит от следующих факторов:

1. Скорость передачи данных по коммутируемому каналу связи.
2. Длительность зондирования файлов в кэше сервера.
3. Скорость обмена в сети передачи данных.

Четыре элемента, составляющие образец сети:

- абонент, который запрашивает данные;
- кэширующий прокси сервер;
- интернет-сервер;

- сеть передачи данных.

Абонент имеет один токен, который моделирует запрос. Данный токен имеет в своем составе два атрибута: порядковый номер и номер запроса. После того, как произошло инициирование модели, возникает еще один токен, который отправляется дальше. После этого токен получает атрибуты, которые включают в себя порядковые номера абонентов, и отправляются на сервер без задержки. В заключительной стадии, созданный ранее токен идет обратно к нужному абоненту с определенным порядковым номером.

Сервер принимает токены от абонентов. После получения происходит отправка в ряд ожиданий, для поиска файлов в кэше сервера. Поиск файлов в кэше происходит по однородно разбитым интервалам времени в промежутке от 2 до 8 секунд. В результате каждому из токенов устанавливается свой атрибут, содержащий размер одного пакета. Размер пакета также однородно разбит в интервале от 10 Кб до 100 Кб. Вероятность того, что токен дойдет до линии связи равна p . Вероятность передачи токена на сервер Интернет равна $(1-p)$.

Результат виртуального моделирования с вероятностью успешных передачи пакетов на сервер 35% приведен в таблице 1.

ТАБЛИЦА 1. Виртуальное моделирование передачи данных на сервер

Размер одного пакета данных (Кб)	64,41
Число отправленных пакетов (шт.)	1597000
Нагрузка на канал (Кб/с)	2350

Результат передачи данных для трех клиентов приведен в таблице 2.

ТАБЛИЦА 2. Моделирование передачи пакетов для пользователей

	Пользователь 1	Пользователь 2	Пользователь 3
Размер одного пакета (Кб)	50,64	53,51	54,05
Число пакетов	829000	869000	865000
Нагрузка на клиента	1200	1460	1320

В заключение необходимо сказать, что роль имитационного моделирования на сегодняшний день велика. Необходимость дальнейшего развития в этом направлении востребовано и перспективно. При помощи данных методов можно моделировать различные системы в разных средах, подвергать их разным критическим ситуациям, предсказывать поведение модели в этих критических ситуациях, выявлять недочеты модели, чтобы в итоге улучшить систему модели и избежать нежелательных последствий в реальной жизни.

Список используемых источников:

1. Акопов А. С. Имитационное моделирование: учебник и практикум для академического бакалавриата : М. : Юрайт, 2018. 389 с. ISBN 978-5-534-02528-6.
2. Боев В. Д. Моделирование в среде AnyLogic : учебное пособие для вузов: М. : Юрайт, 2022. 298 с. ISBN 978-5-534-02560-6.

Yakupov D., Malakhov S.

Povolzsky State University of Telecommunications and Informatics

Application of simulation modeling in solving various problems.

The article discusses the use of predictive and virtual simulation modeling in solving various kinds of problems. For example, a virtual data network is modeled. The network includes a caching proxy server and a public Internet access channel. The role and necessity of their further development is highlighted.

Key words: virtual simulation, simulation, models, Anylogic, subscriber, proxy server.

**Секция 3.4.
Оптоэлектронные технологии (фотоника) в инфокоммуникациях**

УДК 621.39
ГРНТИ 49.33.29

МОДЕЛИРОВАНИЕ ВОСС С КОГЕРЕНТНЫМ ПРИЕМОМ И МОДУЛЯЦИЕЙ DP-16-QAM

П. С. Агоштиню, С. Э. Какусилумезо

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная работа является продолжением ранее опубликованной работы [1], где подробно описана схема, принцип действия и работа одноканальной схемы ВОСС с когерентным приемом и скоростью передачи полезной информации $B=100$ Гбит/с с модуляцией DP-16QAM. Реальная скорость в линии за счет использования помехозащищенного кодирования (FEC) составляет $B=112$ Гбит/с. Статья посвящена детальному исследованию процессов в двухканальной ВОСС с одним и двумя пролетами.

волоконно-оптическая система связи, формат модуляции, кодирование, квадратурная амплитудная модуляция, когерентный прием, энергетический прием

Введение.

Данная работа посвящена исследованиям двухканальных волоконно-оптических систем связи (ВОСС) для магистральных и транспортных сетей с плотным мультиплексированием в волновой области (DWDM) с 16-уровневой квадратурно-амплитудной модуляцией DP-16QAM. Информационная скорость передачи полезной информации $B=100$ Гбит/с, а реальная скорость в линии за счет использования помехозащищенного кодирования (FEC) составляет $B=112$ Гбит/с. Для увеличения пропускной способности в 2 раза два независимых потока сигналов передаются на двух состояниях поляризации (условно горизонтальной и вертикальной). Скорость передачи на каждой поляризации будет вдвое меньше $B/2=56$ Гбит/с, а символьная скорость составит $B_c=14$ Гбод.

Схемы и результаты исследований будут использованы в методических указаниях к виртуальной лабораторной работе по изучению ВОСС с технологией DWDM и когерентным приемом для студентов, обучающихся по соответствующим направлениям бакалаврской и магистерской подготовки.

Схема моделирования двухканальной ВОСС с когерентным приемом

Схема моделирования приведена на рис. 1. Одноканальная схема подробно описана в [1]. Там можно получить более подробные сведения о работе основных элементов схемы. В двухканальной схеме в качестве источников сигнала используются два анализатора ошибок (BER Test Set). На их выходах формируются бинарные псевдо случайные последовательности (ПСП) импульсов в формате NRZ со скоростью $B=112$ Гбит/с. На входы анализаторов поступают восстановленные последовательности после прохождения через всю моделируемую ВОСС, которая работает в режиме тестирования (Back-to-Back) и может содержать много пролетов. Побитовое сравнение входных и выходных сигналов анализаторов позволяет определить и вывести на дисплей количество

битовых ошибок на каждой поляризации и результаты расчетов коэффициентов ошибок (BER) в первом и втором каналах.

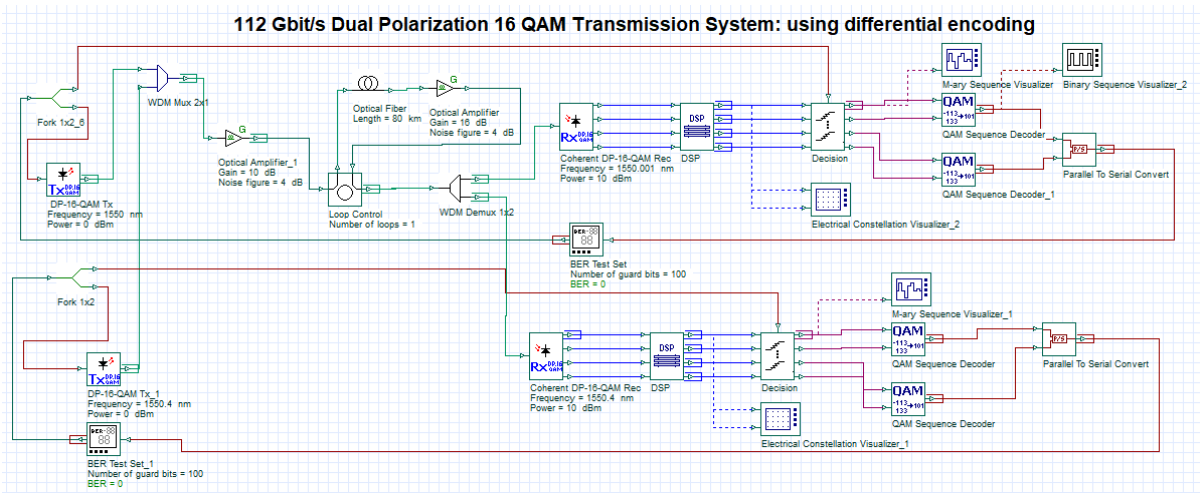


Рис. 1. Схема двухканальной ВОСС с когерентным приемом и модуляцией DP-16-QAM

Сигналы от анализаторов поступают на входы передатчиков T_x , которые осуществляют линейное FEC кодирование, разделение ПСП на две последовательности для каждой поляризации с битовой скоростью 56 Гбит/с. и формируют каналные сигналы с модуляцией 16QAM на каждой поляризации с символьной скоростью 14 Гбод. Сигналы двух передатчиков объединяются в одном одномодовом оптическом волокне (ОВ) с помощью мультиплексора WDM Mux 2x1, усиливаются в эрбиевом оптическом усилителе (ОУ-Optical Amplifier) и поступают в многопролетный волоконно-оптический линейный тракт (ВОЛТ). Каждый пролет содержит ОВ длиной l_p и линейный ОУ с коэффициентом усиления $G = \alpha l_p$ равным затуханию в пролете.

На приеме двухканальный сигнал разделяется на отдельные каналы с помощью демультиплексора WDM Dmux 1x2. В каждом канале используются интрадинные фотоприемные устройства (ФПУ- R_x) с интрадинным приемом. ФПУ включает два поляризационных расщепителя для излучения сигнала, пришедшего из ВОЛТ, и излучения оптического гетеродина – лазерного диода (ЛД), который имеет частоту ν_g близкую к несущей частоте принимаемого оптического сигнала ν_s . Оптическая схема ФПУ также содержит два 90° гибрида, которые объединяют излучения сигнала с мощностью P_s и гетеродина P_g с одинаковыми поляризациями. На выходе каждого гибрида формируются оптические сигналы соответствующие синфазной и квадратурной составляющим для соответствующей поляризации. С помощью четырех балансных фотоприемников с усилителями фототока (УФТ) и аналого-цифровыми преобразователями (АЦП) формируются цифровые сигналы в параллельном коде для ввода в быстродействующий цифровой сигнальный процессор (DSP). Процессоры осуществляют электронную компенсацию хроматической (ХД) и поляризационно-модовой дисперсии (ПМД). При обработке восстанавливается исходное состояние поляризации, синхронизация, тактовая частота. Решающее устройство (Decision) преобразует выходные

сигналы DSP в четырехуровневые цифровые сигналы для каждой поляризации. Далее эти сигналы с помощью двух декодеров QAM преобразуются в бинарные сигналы для каждой поляризации, которые с помощью преобразователя двух параллельных кодов в один последовательный код.

Для контроля за качеством связи используют приборы для регистрации сигнальных созвездий для каждой поляризации (Electrical Constellation Visualizer). Кроме визуализации сигнальных созвездий эти приборы позволяют оценивать BER, Q -фактор и количество битовых ошибок до FEC декодирования. Это позволяет детально анализировать изменения качества связи при изменении параметров исследуемой ВОСС.

Результаты моделирования одно- и двухпролетных ВОСС с когерентным приемом

Уточним некоторые исходные данные для исследования ВОСС с когерентным приемом: дифференциальное кодирование; стандартное ОВ; длины волн каналов $\lambda_1=1550$ нм, $\lambda_2=1550.4$ нм; мощность гетеродина $p_g=10$ дБм; p-i-n ФД с чувствительностью $S_{ph}=1$ А/Вт и спектральной плотностью теплового шума $S_T=100 \cdot 10^{-24}$ Вт/Гц; усилитель мощности (бустер) с коэффициентами усиления $G=10$ дБ и шума $NF=4$ дБ, ширина полосы пропускания мультиплексора и демультиплексора $\Delta\nu_{mux}=20$ ГГц. Изменяемые параметры: уровень выходной мощности передатчика p_u , количество пролетов n и длина одного пролета ВОСС l . Коэффициент усиления линейного усилителя определяется выражением $G=\alpha l_p$.

Измерялись: средние мощности p_0 и p_l , дБм, оптические отношения сигнала к шуму $OSNR_{in}$ и $OSNR_{out}$ на входе и выходе ВОЛТ, а также коэффициент символьных ошибок BER и символьный Q -фактор.

Исходные данные и результаты измерений приведены в таблицах 1 и 2.

ТАБЛИЦА 1. Результаты исследования однопролетных ВОСС при изменении уровня входных сигналов и длины пролета

№ изм	Устан. парам.		Измеряемые параметры						
	p_u , дБм	l , км	p_0 , дБм	p_l , дБм	$osnr_{in}$, дБ	$osnr_{out}$, дБ	BER расчет	Q	BER измер.
1	-10	80	-10.3	-3.73	23/28	18/18.5	10^{-4}	3.3	$7 \cdot 10^{-4}$
2	-6	80	-7.59	-4.69	24/32	22/25	$7 \cdot 10^{-9}$	5.8	0
3	0	80	-2.39	-1.3	24/38	24/31	$2 \cdot 10^{-16}$	8.2	0
4	3	80	0.36	0.98	23/40	23/33	10^{-18}	8.8	0
5	6	80	3.31	3.63	24/44	24/37	$2 \cdot 10^{-20}$	9.3	0
6	10	80	7.31	7.44	24/48	24/41	$2 \cdot 10^{-13}$	7.3	0
7	12	80	9.29	9.38	24/50	24/43	$7 \cdot 10^{-9}$	5.8	0

8	13	80	10.3	10.37	23/50	23/43	10^{-6}	4.8	$3 \cdot 10^{-5}$
9	6	100	3.35	4.12	24/44	24/32	$4 \cdot 10^{-17}$	8.4	0
10	6	120	3.34	5.06	24/44	24/30	$4 \cdot 10^{-14}$	7.6	0
11	6	140	3.36	6.82	24/44	22/26	$2 \cdot 10^{-9}$	6.0	0
12	6	150	3.37	10.2	24/44	19/21	$5 \cdot 10^{-4}$	3.5	$5 \cdot 10^{-4}$

Выводы по таблице 1.

Введение второго канала DWDM приводит к ухудшению качества связи. Для однопролетной линии длиной 80 км уровни входных сигналов могут изменяться в диапазоне от -6 до +12 дБм. При этом Q -фактор до FEC декодирования больше 5.8, а максимальное его значение составляет $Q=9.3$. Для оценки OSNR использовалась спектрограмма двухканального сигнала на выходе ВОЛТ (рис. 2, строка 4 таблицы 1), зарегистрированная оптическим спектроанализатором (OSA). Отметим, что в таблицы 1 и 2 записывались два числа, первое это разность между максимальным значением и минимальным значением, лежащим посередине между двумя пиками (A-B), а второе это разность между максимальным значением и уровнем УСИ (A-C).

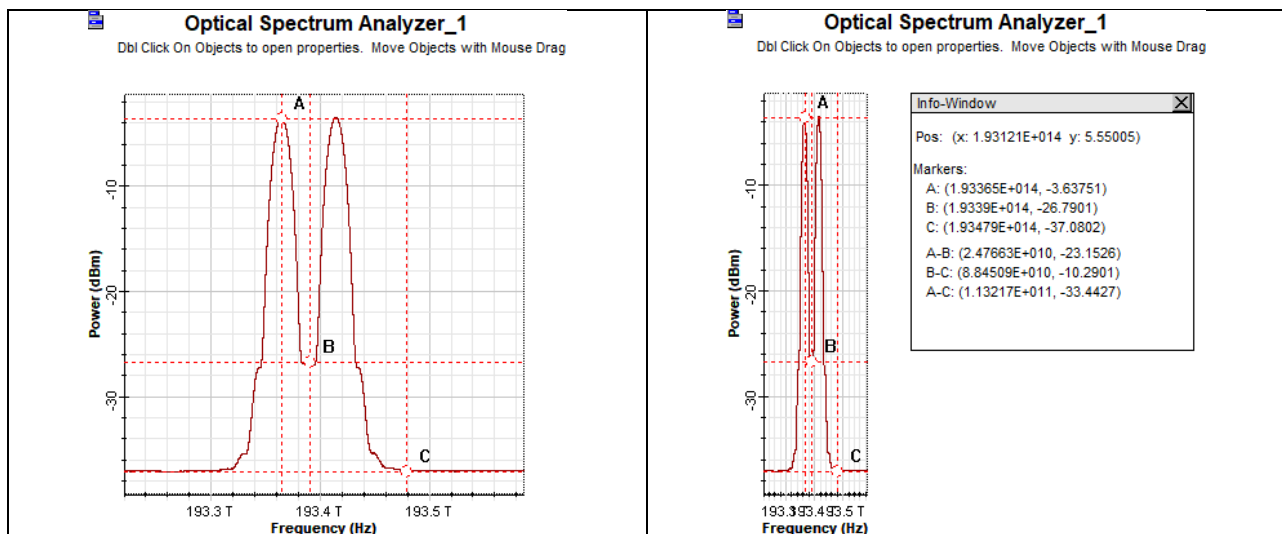


Рис. 2. Спектрограмма сигнала в OSA для определения OSNR

Можно отметить, что длина однопролетной ВОСС может быть увеличена до 140 км при сохранении качества связи.

ТАБЛИЦА 2. Результаты исследования двухпролетных ВОСС

№ изм	Устан. парам.		Измеряемые параметры						
	p_u , дБм	l , км	p_o , дБм	p_l , дБм	$osnr_{in}$, дБ	$osnr_{out}$, дБ	BER расчет	Q	BER измер.
1	-8	2x80	-9.05	-3.43	24/30	19/20	10^{-4}	3.8	$3 \cdot 10^{-5}$

2	-6	2x80	-7.59	-2.98	24/32	19/22	10^{-6}	4.9	0
3	0	2x80	-2.41	-0.44	24/37	22/28	$2 \cdot 10^{-12}$	7.0	0
4	3	2x80	0.43	1.57	24/41	23/34	$2 \cdot 10^{-14}$	7.7	0
5	8	2x80	5.33	5.72	23/45	23/35	$3 \cdot 10^{-11}$	6.6	0
6	10	2x80	7.29	7.55	23/47	23/37	$2 \cdot 10^{-5}$	5.2	$3 \cdot 10^{-5}$
7	3	2x100	0.398	2.85	23/39	22/27	$2 \cdot 10^{-12}$	7.0	0
8	3	2x120	0.423	5.05	24/40	21/24	10^{-7}	5.3	0

Выводы по таблице 2.

Увеличение количества пролетов приводит к ухудшению качества связи. Однако оно остается достаточно высоким.

Заключение.

1. Схема исследования и их результаты будут использованы для разработки методических указаний к виртуальной лабораторной работы по изучению ВОСС с когерентным приемом.
2. Исследования когерентных систем связи с другими форматами модуляции будут продолжены.

Список используемых источников:

1. Агоштиньо П. С. Моделирование одноканальной ВОСС с когерентным приемом и модуляцией DP-16-QAM // “Студенческая весна - 2022” : материалы 76-ой регион. научно-технич. конф. студентов, аспирантов и молодых ученых, Санкт-Петербург, 24-25 мая 2022 г. СПб. : СПбГУТ, 2022.
2. Трещикова В. Н., Листвин В. Н., DWDM – системы. М. : Техносфера, 2021. 420 с.
3. Agrawal G. P. Lightwave technology : telecommunication systems. 2005. p. 461.
4. Былина М. С., Глаголев С. Ф., Дюбов А. С. Сравнительный анализ методов энергетического и когерентного приема цифровых информационных оптических сигналов. Часть 2. Когерентный прием // Труды учебных заведений связи. 2017. Том 3. № 4. С. 21-28.
5. OptiSystem. Tutorials - Volume 1. Version 13: [Электронный ресурс]. URL: <https://optiwave.com> (Дата обращения 15.11.2022).

Agostinho P, Kakusilumezo S.

The Bonch-Bruевич St. Petersburg State University of Telecommunications

Voss modeling with coherent reception and modulation DP-16-QAM.

This work is a continuation of the previously published work [1], which describes in detail the scheme, principle of operation and operation of a single-channel VOSS circuit with coherent reception and transmission rate of useful information $I_n = 100$ Gbit/s with DP-16QAM modulation. The real line speed due to the use of noise-proof coding (FEC) is $B = 112$ Gbit/s. The article is devoted to a detailed study of the processes in a two-channel VOSS with one and two spans.

Key words: *fiber-optic communication system, modulation format, coding, quadrature amplitude modulation, coherent reception, energy reception.*

УДК 621.39, 530.182

ГРНТИ 49.29.14

ПРИМЕНЕНИЕ ОПТИЧЕСКИХ СОЛИТОНОВ ДЛЯ СОЗДАНИЯ ИЗМЕРИТЕЛЬНЫХ ИСТОЧНИКОВ ИЗЛУЧЕНИЯ

Е. И. Андреева, Н. В. Яковлев, Е. С. Константинов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследованы методы формирования в волоконном световоде импульсов субпикосекундной и фемтосекундной длительности. Проведено компьютерное моделирование солитонного самосжатия оптического импульса в волоконном световоде. Полученные результаты согласуются с численными оценками.

волоконно-оптические сети, волоконный световод, сверхкороткие оптические импульсы, лазеры, синхронизация мод, оптические солитоны

Нелинейные свойства волоконных световодов активно используются для самых различных применений [1-4]. Наиболее ярко нелинейные свойства кварц-кварцевых волоконных световодов проявляются в области аномальной дисперсии, где возможно формирование оптических солитонов – стабильных волновых пакетов. После 1998 г., когда была создана и протестирована первая дуплексная система спектрального уплотнения с четырьмя каналами, использующая блок генераторов солитонных импульсов, данные системы стали активно внедряться в магистральные сети передачи данных. Уже не одно десятилетие оптические солитоны используются в системах передачи данных на большие расстояния – long-haul systems – в системах с большой длиной пролета [4]. Благодаря данной концепции возможно существенно сократить влияние хроматической дисперсии на потоки оптических импульсов в высокоскоростных линиях волоконно-оптических систем связи. Несмотря на явные проблемы использования этой концепции в телекоммуникационных системах, как, к примеру, проблемное взаимодействие соседствующих в потоке солитонных импульсов, высокая стабильность данного типа импульсов демонстрирует состоятельность их использования в современных ВОСС.

Солитонные эффекты используются также в устройствах фотоники [1-3]. Важным направлением является создание источников излучения с заданными рабочими параметрами. Примером могут служить источники сверхкоротких оптических импульсов субпикосекундного и фемтосекундного диапазона, комб-генераторы и источники белого шума. Источники фемтосекундных импульсов находят самое широкое применение самых разных областях: в системах синхронизации, медицине, технике.

Высокостабильные комб-генераторы, используются для высокоточных спектральных оптических измерений. Оптические комб-генераторы, использующие, нелинейные эффекты в волоконном световоде, позволяют перекрыть весь спектр ближнего ИК диапазона, используемого для передачи данных по ВОЛС.

Источники белого шума генерируют мощное излучение в широком спектральном диапазоне и используются для измерения спектральных характеристик различных волоконно-оптических компонентов и устройств фотоники.

В основе функционирования таких устройств, как правило, задействованы нелинейные свойства волоконных световодов.

В ходе исследования проведено моделирование эволюции солитонного импульса длительности τ в волоконном световоде, сопровождающееся самосжатием и уширением спектра [5]. В ходе компьютерного моделирования показано, что важное значение имеет выбор типа волоконного световода. В волоконном световоде с большой дисперсией β'' процесс самосжатия происходит с большей скоростью, так как дисперсионная длина, определяемая как $L_D = \tau^2 / \beta''$, в таком световоде меньше. Преимущество – меньшее влияние потерь. Недостаток – степень самосжатия меньше, чем в волоконном световоде с малой дисперсией. В волоконном световоде с малой дисперсией точка максимального самосжатия оказывается более удаленной, так что потери могут ослабить оптический импульс.

Техническим решением может служить гибридный световод, в котором вначале дисперсия принимает высокое значение, а затем уменьшается. При использовании гибридного решения удается уменьшить длительность оптического импульса.

Предположим, что на вход стандартного SSMF световода с дисперсией β_1'' и коэффициентом нелинейности \mathcal{C}_1 подается импульс длительности τ мощности P_o , соответствующий солитону порядка N_1 .

$$P_o = N_1^2 P_{s1} \beta_1'' \quad (1)$$

где P_{s1} – соответствует мощности фундаментального солитона в световоде с указанными параметрами:

$$P_{s1} = \frac{\beta_1''}{\gamma_1 \tau_1^2} \quad (2)$$

При переходе во второй световод с меньшей дисперсией β_2'' и большим коэффициентом нелинейности \mathcal{C}_2 (световод со смещенной дисперсией DSF) будет формироваться солитон порядка N_2 :

$$N_2 = \sqrt{\frac{\beta_1'' \gamma_2}{\beta_2'' \gamma_1}} N_1 \quad (3)$$

Относительное изменение коэффициента самосжатия K_s ,

$$\frac{K_{s2}}{K_{s1}} \approx \frac{N_2}{N_1} = \sqrt{\frac{\beta_1'' \gamma_2}{\beta_2'' \gamma_1}} \quad (4)$$

Как показывают численные оценки, при переходе от SSMF световода с дисперсией $\beta_1''=20$ пс²/км к световоду со смещенной ненулевой дисперсией NZDSF $\beta_2''=2$ пс²/км позволяет увеличить степень самосжатия в $10^{1/2}$ раз при незначительном увеличении дальности до точки самосжатия.

Эволюция солитонов фемтосекундной длительности сопровождается также рамановским самосдвигом частоты излучения [6]. На основе этого эффекта могут быть получены перестраиваемые по длине волны измерительные источники излучения. В отличие от источников на базе полупроводниковых кристаллов источники, использующие, нелинейные эффекты в волоконном световоде, позволяют плавно, без “перескоков” перестраивать несущую длину волны. Важным достоинством таких источников является возможность смещения длины волны генерируемого сигнала в область больших длин волн.

Такие источники могут использоваться для формирования символьных импульсов в высокоскоростных волоконно-оптических системах передачи информации, в устройствах ее обработки, системах синхронизации, а также применяться для тестирования компонентов волоконно-оптических систем, в том числе со спектральным уплотнением [7-9].

Список используемых источников:

1. Агравал Г. Нелинейная волоконная оптика. М.: Мир, 1996. 323 с.
2. Кившарь Ю. С., Агравал Г. П. Оптические солитоны. От волоконных световодов до фотонных кристаллов. М.: Физматлит, 2005. 648 с.
3. Ferreira M.: "Nonlinear Effects in Optical Fibers", John Wiley & Sons, Inc., Hoboken, New Jersey, USA. 2011.
4. G. P. Agrawal Nonlinear fiber optics: its history and recent progress. J. Opt. Soc. Am. B. Vol. 28, No. 12. P.A1 – A10.
5. Е. И. Андреева, А. А. Ермолаев, П. А. Хитров. Методы формирования сверхкоротких оптических импульсов высокой мощности с учетом линейных и нелинейных свойств волоконных световодов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. АПИНО 2022. Т. 1. с.86 – 91.
6. Яковлев Н.В. Исследование влияния SRS-эффекта в DWDM-системах. ПКМ-2021, Сборник лучших докладов. с.298 – 302.
7. Шевченко М.А., Андреева Е.И. Особенности построения системы передачи данных с использованием оптических солитонных импульсов. Информационные технологии и

нанотехнологии (ИТНТ-2021). Сборник трудов по материалам VII Международной конференции и молодежной школы. В 3-х томах. Самара, 2021. С. 11162.

8. Ermolaev A.A., Shevchenko M.A., Andreeva E.I. Features of the fiber-optics data system using optical solitons. Journal of Physics: Conference Series. "8th International School and Conference "Saint Petersburg OPEN 2021": Optoelectronics, Photonics, Engineering and Nanostructures, SPbOPEN 2021" 2021. С. 012139.

9. F.Mitschke, C.Mahnke, A.Hause. Soliton Content of Fiber-Optic Light Pulses. Applied science. Vol. 7, p. 635. 2017

Andreeva E., Yakovlev N., Constantinov E.

The Bonch-Bruевич St.Petersburg State University of Telecommunication

The use of optical solitons for creation of measuring light source.

Methods of picosecond and femtosecond pulses creation in optical fiber were researched. Computer simulation of soliton self-compression in optical fiber was carried out. The obtained results are consistent with numerical estimates.

Key words: fiber-optic networks, fiber optic fiber, ultrashort optical pulses, lasers, mode synchronization, optical solitons.

УДК 681.7.068.4
ГРНТИ 49.44.31

МНОГОСЕРДЦЕВИННОЕ ОПТИЧЕСКОЕ ВОЛОКНО С «ТРАНШЕЕЙ» ВОКРУГ КАЖДОЙ СЕРДЦЕВИНЫ

Н. К. Андриевский, М. С. Былина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Многосердцевинное волокно позволяет реализовать технологию пространственного мультиплексирования каналов. Канальные сигналы передаются по отдельным сердцевинам независимо друг от друга. Максимальное число сердцевин, размещаемых в одном волокне ограничено взаимными влияниями между ними. Для уменьшения взаимных влияний между сердцевинами, каждая из них окружается дополнительной оболочкой, которая может иметь различную конструкцию. В данной работе исследуется эффективность применения «траншеи» – кольца с пониженным показателем преломления вокруг сердцевины.

многосердцевинное волокно, одномодовая сердцевина, «траншея», взаимные влияния, перекрестные помехи, затухание перекрестных помех, моделирование

Увеличение объемов трафика является общей тенденцией развития сетей связи, с каждым годом существенно увеличивается объем информации, передаваемой по одному одномодовому оптическому волокну (SMF). В настоящее время пропускная способность существующего стандартного одномодового волокна приближается к своему фундаментальному пределу, несмотря на внедрение новых технологий передачи, которые обеспечивают высокую спектральную эффективность [2].

Мультиплексирование с разделением пространства (SDM) появилось как решение проблемы насыщения пропускной способности оптических систем передачи, примером такой реализации является применение многосердцевинных волокон (МСВ), представляющих собой оптическое волокно (ОВ) с несколькими сердцевинами, заключенными в общую оболочку стандартного диаметра – 125 мкм. Одной из основных проблем МСВ являются взаимные влияния – перекрестные помехи, которые возникают вследствие перехода части оптического сигнала из одной сердцевины в другую. Для уменьшения взаимных влияний каждая сердцевина может окружаться изолирующей оболочкой.

В данной работе рассматривается МСВ, каждая сердцевина которого окружена так называемой «траншеей» – кольцом материала с пониженным по отношению к общей оболочке показателем преломления (ПП).

Конструкция и профиль ПП сердцевины исследуемого МСВ представлены на рис. 1. «Траншея» с ПП n_2 отделена от сердцевины промежуточной оболочкой.

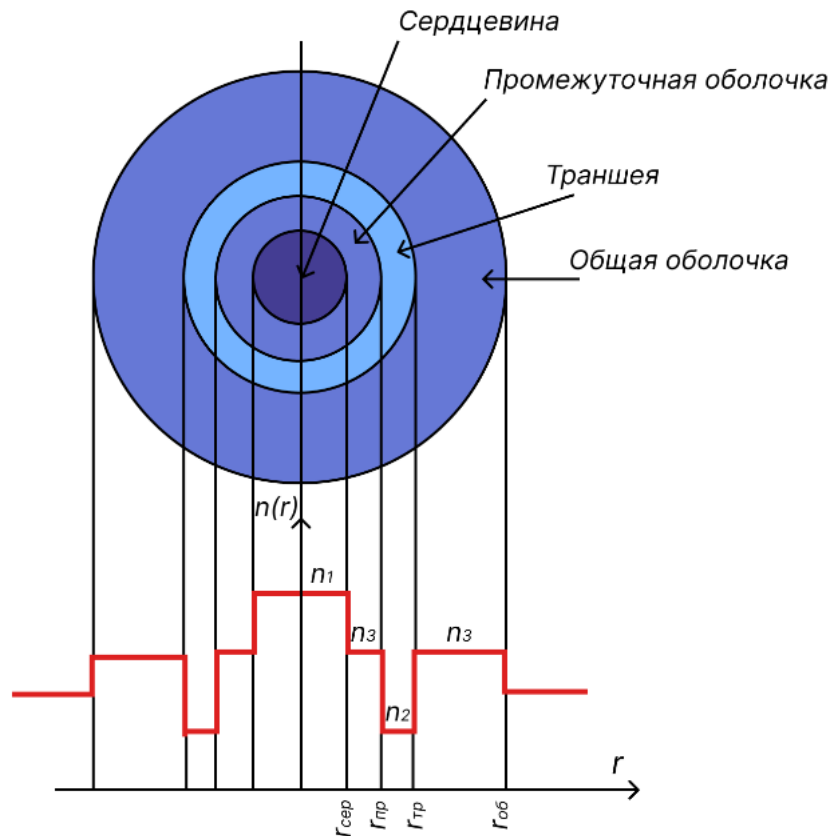


Рис. 1. Сердцевина исследуемого МСВ

Назначением «траншеи» является уменьшение радиуса модового поля, и доли мощности фундаментальной моды, распространяющейся в общей оболочке, что должно снизить взаимные влияния. Для достижения данного эффекта необходимо, чтобы выполнялось следующее соотношение между ПП [1]: $n_1 > n_3 > n_2$.

Целью данной работы является оптимизация конструкции сердцевин (толщины промежуточной оболочки и «траншеи») для достижения минимального расстояния между соседними сердцевинами, обеспечивающего защищенность от взаимных влияний A не менее допустимого уровня. Защищенность A определялась по формуле [1]:

$$A = 10 \cdot P_s P_n \tag{1}$$

где P_s – мощность сигнала (сосредоточенной в сердцевине доли фундаментальной моды), P_n – мощность перекрестных помех.

Для расчета P_s и P_n применялась методика, предложенная в [1]. Для расчета P_s использовалось выражение:

$$P_s = 2 P_{max} \int_0^{r_1} E^2 r dr, \tag{2}$$

где r – полярная координата, отсчитываемая от оптической оси сердцевин радиусом r_1 , E_r – нормированная напряженность электрического поля фундаментальной моды сердцевин, P_{max} – мощность излучения фундаментальной моды на оптической оси.

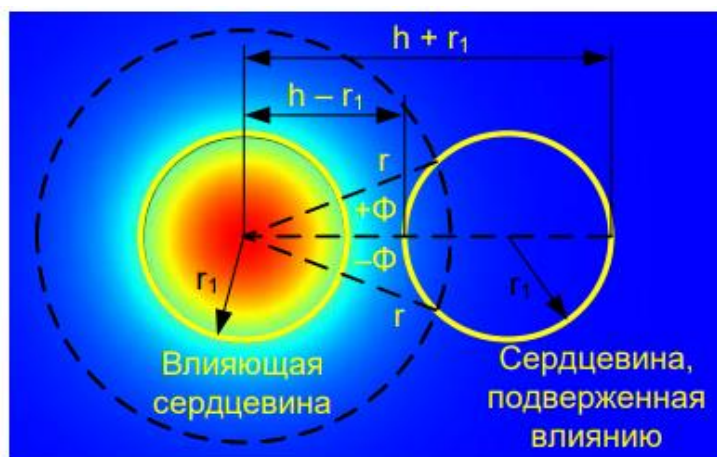


Рис. 2. К методике расчета мощности помехи P_n

Рассмотрим методику расчета мощности P_n , созданной одной влияющей сердцевинной. На рис. 2 представлена часть поперечного сечения МСВ, содержащая влияющую и подверженную влиянию сердцевину. Поле фундаментальной моды влияющей сердцевины не ограничено ее пределами. P_n определяется мощностью поля влияющей сердцевины в той области пространства, где расположена сердцевина, подверженная влиянию:

$$P_n = 2 \cdot P_{max} \int_{h-r_1}^{h+r_1} \frac{r}{E^2} \arccos \frac{r_2 - r_1}{\sqrt{r^2 + h^2}} \cdot h \cdot r \, dr, \quad (3)$$

где h – расстояние между соседними сердцевинами.

В работе было проведено моделирование сердцевин МСВ с «траншеями» и промежуточными оболочками различной толщины. Параметры, при которых проведены расчеты, представлены в таблице 1.

ТАБЛИЦА 1. Параметры сердцевины МСВ с «траншеями»

Параметр	Значение
Материал сердцевины	Кварцевое стекло SiO ₂ , легированное GeO ₂ с концентрацией 4.1 молярных процентов
Показатель преломления n1 сердцевины на длине волны 1550 нм	1.4503
Материал траншеи	Кварцевое стекло SiO ₂ , легированное F с концентрацией 3 молярных процента
Показатель преломления n2 траншеи на длине волны 1550 нм	1.4256
Материал общей и промежуточной оболочек	Кварцевое стекло SiO ₂
Показатель преломления n3 общей оболочки на длине волны 1550 нм	1.4440
Радиус сердцевины r1 мкм	4.1

Для расчета приведенных в табл. 1 показателей преломления и их зависимости от длины волны использовалось известное уравнение Селлмейера [1].

$$n_2 = i = 13Si^2 - i^2 + 1, \quad (4)$$

где i - резонансные длины волн, Si - безразмерные коэффициенты (таблица 2).

ТАБЛИЦА 2. Резонансные длины волн и коэффициенты Селлмейера [1]

Материал	S1	S2	S3	1, мкм	2, мкм	3, мкм
SiO ₂	0.696	0.408	0.897	0.068	0.116	9.896
SiO ₂ + 4.1% GeO ₂	0.687	0.435	0.897	0.073	0.115	10.002

Для расчета показателя преломления «траншеи» n_2 использовалось выражение, описанное в [1].

$$n_2 = n_1 - \Delta n dF, \quad (5)$$

где dF – концентрация F в молярных процентах, $\Delta n = 0.0045992$.

На рис. 3 представлены результаты моделирования распределения полей фундаментальной моды в сердцевинах без «траншеи» и с «траншеей». Разные цвета на рис. соответствуют разным значениям напряженности электрического поля в соответствии с приведенной справа цветовой шкалой.

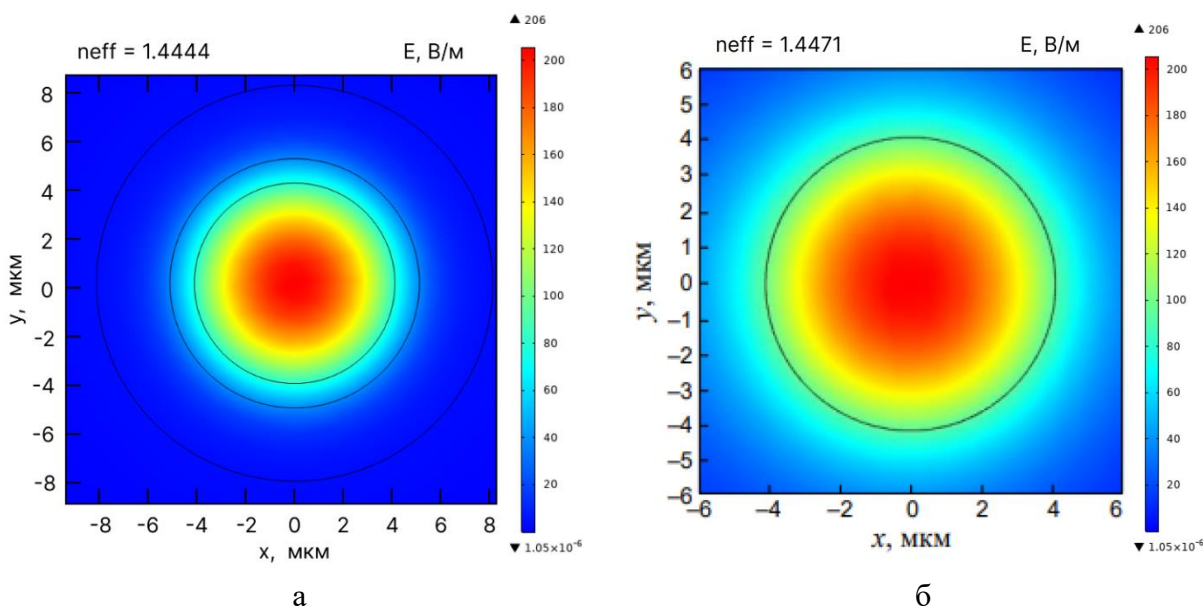


Рис. 3. Распределение поля фундаментальной моды в сердцевине (результат моделирования в COMSOL Multiphysics): а – с «траншеей» толщиной 2 мкм и промежуточной оболочкой толщиной 0.5 мкм, б – без изолирующих элементов

На рис. 4 представлены зависимости затухания перекрестной помехи в сердцевине от расстояния между сердцевинами h в двухсердцевинном МСВ. Расчет проведен по выражениям (1–3) для сердцевин без «траншеи» и с «траншеями» и промежуточными оболочками разной толщины на длине волны 1550 нм.

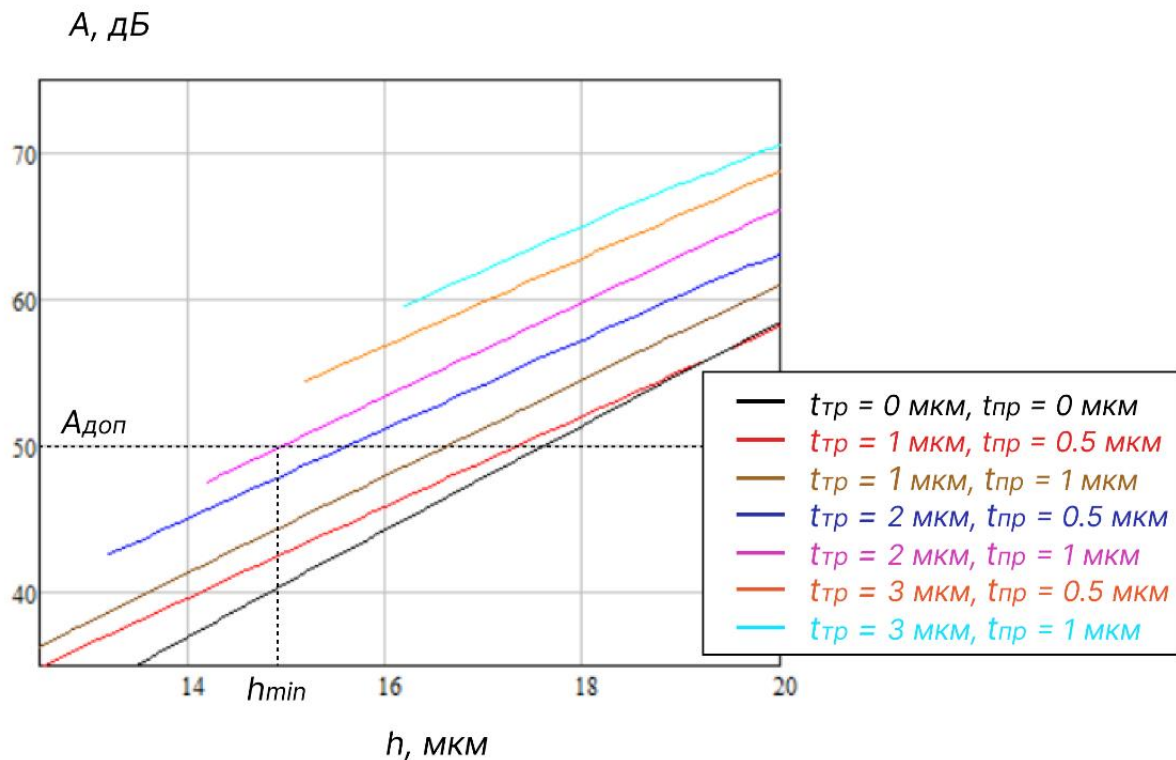


Рис. 4. Затухание перекрестной помехи в МСВ с двумя одинаковыми сердцевинами с «траншеями» и промежуточными оболочками ($t_{тр}$ – толщина траншеи, $t_{пр}$ – толщина промежуточной оболочки)

Из рис. 4 видно, что затухание перекрестной помехи A увеличивается при увеличении расстояния между сердцевинами. Если задаться минимально допустимой величиной $A_{доп}$, по приведенному семейству графиков можно определить наилучшую конструкцию, при которой обеспечивается минимальное расстояние h_{min} между соседними сердцевинами. Например, для $A_{доп} = 50$ дБ наилучшей конструкцией будет сердцевина с «траншеей» толщиной 2 мкм и промежуточной оболочкой толщиной 1 мкм, позволяющая получить $h_{min} = 14.8$ мкм.

Список используемых источников:

1. Былина М. С., Гулятьева Л. А. Многосердцевинное оптическое волокно со ступенчатыми одномодовыми сердцевинами. Часть 1 // Труды учебных заведений связи. Том 8, № 4, 2022.
2. Kunimasa Saito, Shoichiro Matsuo. Multicore fibers for large capacity transmission [Электронный ресурс] // Nanophotonics: electron scientific journal. 2013. Vol. 2. N 5. pp. 441–454. URL: <https://www.degruyter.com/document/doi/10.1515/nanoph-2013-0037/html> (Дата обращения 30.10.2022).
3. Tetsuya Hayashi. Multi-Core Optical Fibers Realizing High-Density/-Capacity Transmissions [Электронный ресурс] // IEEE CPMT Symposium Japan : materials of the VII International Scientific Conference. Japan, 7-9 Nov. 2016, P. 169–172. URL: https://www.researchgate.net/publication/309767726_Multi-Core_Optical_Fibers_Realizing_High-Density-Capacity_Transmissions (Дата обращения 27.10.2022).

Andrievskii N., Bylina M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Multi-core optical fiber with a "trench" around each core.

Multi-core fiber allows to implement the technology of spatial multiplexing of channels. Channel signals are transmitted through separate cores independently of each other. The maximum number of cores placed in one fiber is limited by mutual influences between them. To reduce the mutual influences between the cores, each of them is surrounded by an additional shell, which may have a different design. In this paper, the effectiveness of using a "trench" – a ring with a reduced refractive index around the core is investigated.

Key words: multi-core fiber, single-mode core, "trench", mutual influences, crosstalk, crosstalk attenuation, simulation.

УДК 535.14
ГРНТИ 29.05.15

РАЗРАБОТКА ВИРТУАЛЬНОЙ ЛАБОРАТОРНОЙ РАБОТЫ ПО ИЗУЧЕНИЮ ИНТЕРФЕРОМЕТРА МАХА-ЦЕНДЕРА

А. И. Андрюнин, М. С. Былина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время особое значение приобрели квантовые технологии – технологии, основанные на явлениях квантовой физики. Это одно из наиболее перспективных направлений науки и техники, относящееся к сквозным цифровым технологиям. Выпускники направлений «Инфокоммуникационные технологии и системы связи» и «Фотоника и оптоинформатика» должны получать базовые знания и навыки в этой перспективной области, поэтому в СПбГУТ ведется активная работа по внедрению в учебные планы дисциплин, относящихся к квантовым технологиям. Эти дисциплины предполагают обязательное наличие лабораторного практикума. В данной работе представлена новая виртуальная лабораторная установка с интерферометром Маха-Цендера для изучения квантовых явлений.

фотоника, квантовая механика, интерферометр Маха-Цендера, принцип дополненности, теория скрытых параметров, квантовый ластик, виртуальная лабораторная установка, разработка программного обеспечения

В настоящее время сфера квантовых технологий считается очень перспективной. Квантовые технологии породили одно из важнейших направлений в современной связи – квантовые коммуникации. Заинтересованность квантовыми технологиями рождает спрос у инфокоммуникационных компаний на специалистов в этой области. В связи с этими тенденциями в СПбГУТ внедряются новые направления и дисциплины, которые позволяют готовить таких специалистов. Важной частью учебного процесса являются лабораторные работы по квантовым коммуникациям, позволяющие студентам приобрести необходимые практические умения и навыки.

В 2022 году в нашем университете был создан лабораторный практикум по дисциплине «Квантовые коммуникации» [1], в котором используются виртуальные лабораторные установки, разработанные университетом св. Андрея (Шотландия) [2]. Опыт внедрения данного лабораторного практикума в учебный процесс кафедры Фотоники и линий связи показал, что возможности создания оптических схем в имеющихся виртуальных установках недостаточны для всестороннего изучения квантовомеханических явлений.

Доработка этих установок в принципе невозможна. При модификации схем и изменении параметров их элементов только небольшая часть самых простых расчетов проводится в реальном масштабе времени. Большая часть расчетов произведена заранее и их результаты нельзя изменить. Анимированные картинки также отрисованы заранее в соответствии с результатами предварительных

расчетов. В связи с этим было принято решение разработать собственную виртуальную лабораторную установку с расширенным функционалом.

Средой разработки для новой виртуальной лабораторной установки была выбрана программа Visual Studio – самая популярная IDE (интегрированная среда разработки), которая поддерживает нужный стек протоколов [3]. В качестве основного языка разработки выбран современный язык программирования C#, позволяющий использовать технологии WPF (Windows Presentation Foundation) и .NET. Эти технологии позволяют создавать приложения с удобным интуитивно понятным и красивым интерфейсом.

Отличительной особенностью новой виртуальной установки будет ее математический движок, написанный на C#. Собственный движок позволит внедрить в установку математическую модель, описывающую вектор состояния фотона и его изменение при взаимодействии с оптическими элементами. Это даст возможность в дальнейшем развивать проект, например, добавляя в установку новые оптические элементы.

Внешний вид разрабатываемой установки представлен на рис. 1. Ее центральными компонентами являются однофотонный источник излучения S, интерферометр Маха-Цендера (ИМЦ), состоящий из двух полупрозрачных и двух непрозрачных зеркал, и два детектора. Для создания различных оптических схем на пути фотона можно устанавливать фазовращатели, узкополосные заграждающие фильтры и поляризаторы. Для реализации мысленного эксперимента Элицура-Вайдмана в установке имеются сверхчувствительные бомбы [2, 4].

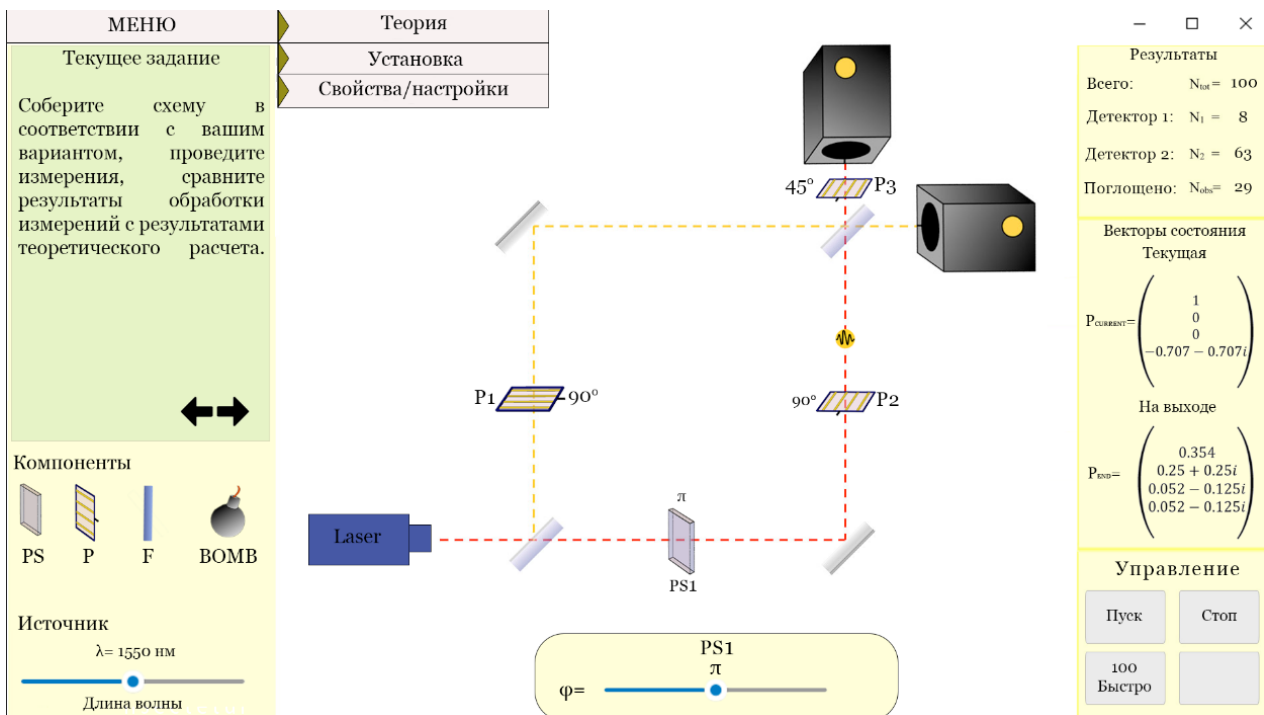


Рис. 1. Внешний вид разрабатываемой установки

На настоящий момент по сравнению с виртуальными установками, разработанными в университете св. Андрея, разрабатываемая установка

полностью русифицирована и содержит больше оптических элементов, параметры которых можно настраивать: сдвиг фазы в фазовращателях может плавно изменяться от 0 до 2π , добавлена возможность изменять частоту (длину волны) источника S и поглощающих фильтров, добавлены поляризаторы с настройкой азимута оси пропускания от 0 до 0.5π .

Разрабатываемая установка допускает размещение оптических элементов на любом из отрезков траектории распространения фотонов в любых сочетаниях, что позволяет создавать новые оптические схемы для исследования.

Основные отличия разрабатываемой версии от имеющейся представлены в таблице 1.

ТАБЛИЦА 1. Основные отличия старой версии ЛР от разрабатываемой.

Оцениваемые характеристики	Комплекс лабораторных установок, разработанных в университете св. Андрея	Разрабатываемая лабораторная установка
Технологии, примененные при разработке	Adobe Animate, HTML, CSS, JavaScript	C#, .NET, ASP.NET, WPF
Среда использования	Веб-браузер	Веб-браузер, Desktop приложение, iOS, Android
Возможность модернизации и расширения функционала	НЕТ	ДА
Продвижение как проекта СПбГУТ	НЕТ	ДА
Максимальное количество компонентов в оптической схеме	от 7 до 11 в зависимости от установки	Ограничено только порогом вычислительной мощности ПК
Возможность изменения параметров компонентов оптической схемы	Ограничено заранее определенными вариантами исследований	ДА

В основу разрабатываемой установки положена математическая модель, в которой квантовомеханический объект (фотон) описывается вектором состояния. В установке учитываются две характеристики фотона – направление его распространения (траектория) и поляризация, поэтому все возможные состояния фотона могут быть описаны векторами в четырехмерном гильбертовом пространстве, образованным четырьмя ортогональными базисными векторами [1, 2, 5]:

$$|UV\rangle = (1\ 0\ 0\ 0), |UH\rangle = (0\ 1\ 0\ 0), |LV\rangle = (0\ 0\ 1\ 0), |LH\rangle = (0\ 0\ 0\ 1). \quad (1)$$

Векторы $|UV\rangle$ и $|UH\rangle$ описывают фотоны, пролетающие по верхнему U плечу ИМЦ и имеющие вертикальную V или горизонтальную H поляризацию. Векторы $|LV\rangle$ и $|LH\rangle$ описывают фотоны, пролетающие по нижнему L плечу ИМЦ и имеющие вертикальную V или горизонтальную H поляризацию.

Любое возможное состояние $|s\rangle$ фотона в лабораторной установке может быть представлено суперпозицией четырех базисных векторов:

$$|s\rangle = A \cdot |UV\rangle + B \cdot |UH\rangle + C \cdot |LV\rangle + D \cdot |LH\rangle \quad (2)$$

где A, B, C, D – амплитуды вероятностей, в общем случае комплексные, удовлетворяющие условию $|A|^2 + |B|^2 + |C|^2 + |D|^2 = 1$ и имеющие следующий физический смысл. Вероятности при измерении фотона во введенном базисе обнаружить его в состояниях $|UV\rangle, |UH\rangle, |LV\rangle$ и $|LH\rangle$ равны $|A|^2, |B|^2, |C|^2$ и $|D|^2$ соответственно.

Взаимодействие фотона с компонентом схемы описывается как изменение его вектора состояния в результате действия матричного оператора P , который для четырехмерного пространства имеет размерность 4×4 :

$$|s_{out}\rangle = P|s_{in}\rangle, \quad (3)$$

где $|s_{in}\rangle$ и $|s_{out}\rangle$ – вектора состояния фотона на входе и выходе компонента. Вид оператора P будет зависеть от вида описываемого компонента и места его установки в оптической схеме. Например, операторы P_{PSU} и P_{PSL} , описывающие фазовращатели в верхнем и нижнем плече ИМЦ, будут иметь вид [1, 2, 5]:

$$P_{PSU} = \begin{pmatrix} e^{i\varphi} & 0 & 0 & 0 & 0 & e^{i\varphi} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, P_{PSL} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & e^{i\varphi} & 0 & 0 & 0 & 0 & e^{i\varphi} \end{pmatrix}, \quad (4)$$

где φ – вносимый сдвиг фазы.

Зная состояние фотона на входах детекторов можно рассчитать вероятность его детектирования в верхнем плече P_1 и в нижнем P_2 :

$$\begin{aligned} P_1 &= |\langle s_{out} | X \rangle|^2 + |\langle s_{out} | Y \rangle|^2, \\ P_2 &= |\langle s_{out} | Z \rangle|^2 + |\langle s_{out} | W \rangle|^2, \end{aligned} \quad (5)$$

где запись вида $\langle s_{out} | X \rangle$ представляет обозначение скалярного произведения эрмитово-сопряженного вектора $|X\rangle$ и вектора состояния $|s_{out}\rangle$.

Разрабатываемая установка обеспечит возможность выполнения целого комплекса лабораторных работ по изучению квантовомеханических явлений. Выполнение каждой работы начинается с изучения теоретических сведений, которые доступны студентам на вкладке «Теория», и предлагаемых для исследования оптических схем. На основе изученной теории студенты проводят расчеты вектора состояния фотона в различных точках исследуемой схемы и определяют теоретические вероятности его регистрации каждым из детекторов.

В практической части студенты последовательно собирают предлагаемые в работе схемы, и проводят исследования в соответствии с полученным заданием. Обработка результатов исследований обязательно включает определение экспериментальных вероятностей регистрации фотона каждым из детекторов, которые нужно сопоставить с теоретически рассчитанными.

Анализируя результаты теоретических расчетов и экспериментальных исследований, студенты должны сделать обоснованные выводы, объяснить полученные результаты и оформить отчет.

На настоящий момент в установке реализованы следующие работы:

- 1) Исследование интерферометра Маха-Цендера;
- 2) Исследование влияния фазовращателей на работу интерферометра Маха-Цендера;
- 3) Исследование влияния поляризаторов на работу интерферометра Маха-Цендера;
- 4) Эксперимент с отложенным выбором, опровергающий теорию скрытых параметров;
- 5) Эксперимент Элицура-Вайдмана, демонстрирующий возможность бесконтактных измерений;
- 6) Исследование эффекта «квантового ластика».

В дальнейшем предполагается расширить возможности установки, реализовав новые режимы работы источника – генерацию электромагнитных волн и генерацию пар запутанных фотонов.

Данная виртуальная лабораторная установка будет внедрена в учебный процесс СПбГУТ в дисциплины «Квантовые коммуникации», «Перспективные оптические технологии и квантовые коммуникации».

Список используемых источников:

1. Былина М. С., Фраз А. В., Андрюнин А. И. Квантовые коммуникации. Часть 1. Изучение квантовых явлений: лабораторный практикум. СПб. : СПбГУТ, 2022. 62 с.
2. Интернет ресурс “The Quantum Mechanics Visualisation Project”: [Электронный ресурс] // URL: <https://www.st-andrews.ac.uk/physics/quvis/> (Дата обращения: 14.11.2022)
3. Microsoft Visual Studio – интегрированная среда разработки: [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Microsoft_Visual_Studio. (Дата обращения: 14.11.2022)
4. Чернов П. С. Квантовая механика : конспект лекций (избранные вопросы). Пенза : Издательство Пензенского университета, 2013. 126 с.
5. Былина М. С., Андрюнин А. И. Виртуальная лабораторная установка для изучения эффекта «квантового ластика» // Ученые Записки Физического Факультета МГУ. 2022г.

Andryunin A., Bylina M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Development of a virtual laboratory work on the study of the Mach-Zehnder interferometer. At present time, quantum technologies have acquired special significance - technologies based on the phenomena of quantum physics. This is one of the most promising areas of science and technology in end-to-end digital technologies. Graduates of the faculty "Infocommunication technologies and communication systems" and "Photonics and optoinformatics" should receive basic knowledge and skills in this promising area, therefore, SPbSUT is actively working to introduce disciplines related to quantum technologies into the curricula. These disciplines require the obligatory presence of a laboratory workshop. This paper presents a new virtual laboratory setup with a Mach-Zehnder interferometer for studying quantum phenomena.

Key words: *photonics, software development, Mach-Center interferometer, quantum states, virtual lab.*

УДК 538.945
ГРНТИ 29.19.22

РАСЧЕТ ПАРАМЕТРОВ БЫСТРОДЕЙСТВУЮЩЕГО СВЕРХПРОВОДЯЩЕГО ФИЛЬТРА

Е. И. Богданова, М. В. Головкина

Поволжский государственный университет телекоммуникаций и информатики

В современном мире важнейшей задачей становится создание материалов с заданными свойствами и обладающими малыми потерями. Для их создания можно использовать высокотемпературные сверхпроводники. Главной целью исследования в области высокотемпературных сверхпроводников можно выделить материалы, работающие как минимум при температурах, распространенных на Земле, максимум – при комнатной температуре и их создание приводит к новому прорыву в электронике.

плазмонный резонанс, сверхпроводимость, двухжидкостная модель, сверхпроводящий фильтр

Использование сверхпроводящих материалов позволяет создавать приборы, обладающими высокими характеристиками при своих малых габаритах, массе и потребляемой мощности [1]. Одна из исследуемых областей считается область применения высокотемпературных сверхпроводников. Высокотемпературные сверхпроводники – это такие структуры, которые при достижении температуры, ниже критической (77 К – температуры кипения жидкого азота), проявляют свойства сверхпроводимости, а также демонстрируют возможность проникновения магнитного поля в толщину сверхпроводника [2]. При этом диэлектрическая проницаемость сверхпроводника может принимать как положительные, так и отрицательные значения. Это означает, что появляется возможность возникновения плазмонного резонанса на границе раздела сверхпроводник – диэлектрик или сверхпроводник – полупроводник [3].

Для создания плазмонного резонанса рассматривается композитная среда, содержащая сверхпроводящие сферические включения из высокотемпературной иттриевой керамики (схожие с YBCO материалы, к примеру высокотемпературный сверхпроводник $YBa_2Cu_3O_{7-x}$) Эффективная диэлектрическая проницаемость композитной среды рассчитывается по формуле Максвелла-Гарнетта [4]:

$$\varepsilon_{eff} = \varepsilon_S + 3 \cdot \varepsilon_S \cdot \frac{f \cdot \frac{\varepsilon_d - \varepsilon_S}{\varepsilon_d + 2 \cdot \varepsilon_h}}{1 - f \cdot \frac{\varepsilon_d - \varepsilon_S}{\varepsilon_d + 2 \cdot \varepsilon_h}},$$

где ε_S – диэлектрическая проницаемость сверхпроводника, зависящая от частоты, ε_d – диэлектрическая проницаемость матрицы, f – концентрация включений.

В качестве сверхпроводящих нановключений можно уменьшить потери и использовать для изменения параметров [5]. Рассмотрим зависимость коэффициента прохождения электромагнитной волны через слой композитной среды от частоты, содержащей сверхпроводящие включения с толщиной d [6]. Пусть I – интенсивность плоской монохроматической световой волны на выходе слоя поглощающего вещества с толщиной d , I_0 – интенсивность плоской монохроматической световой волны на входе слоя поглощающего вещества с толщиной d . Чтобы определить интенсивность волны на выходе из слоя воспользуемся законом Бугера – Ламберта [7]:

$$I = I_0 \cdot e^{-\alpha \cdot d},$$

где d – толщина слоя, α – коэффициент поглощения.

Коэффициент поглощения определяется по формуле [8]:

$$\alpha = \text{Im}(k),$$

где k – волновое число, которое находится по формуле [9]:

$$k = \frac{\omega}{c} \cdot \varepsilon_{eff},$$

где ω – циклическая частота [рад/с], c – скорость света в вакууме, ε_{eff} – эффективная диэлектрическая проницаемость композитной среды.

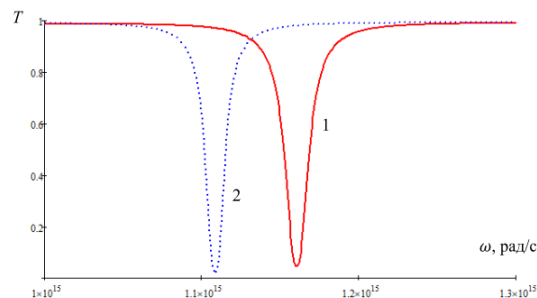


Рис. 1. Зависимость коэффициента прохождения от частоты для нанокompозитной среды со сверхпроводящими включениями. Для различных значений t . Кривая 1: $t=0,85$. Кривая 2: $t=0,98$

На рис. 1 мы видим наличие двух максимумов плазмонного резонанса. Коэффициент прохождения во всем частотном диапазоне, кроме области частот, что соответствуют плазмонному резонансу, равен нулю. Таким образом, сверхпроводящий композит имеет малое затухание во всем частотном диапазоне. А в тех частотах, что соответствуют плазмонному резонансу, наблюдается резкое увеличение коэффициента прохождения T . Из рисунка 1 видно, что при увеличении температуры у нас увеличивается частота, соответствующая плазмонному резонансу.

Таким образом, показано, что можно управлять свойствами композитных сверхпроводников путем изменения температуры. Рассчитаны параметры сверхпроводящего слоистого фильтра на основе нанокompозитных сверхпроводников. Показано, что полосой пропускания сверхпроводящего фильтра можно управлять. Исходя из этого сделан вывод о том, что фильтр пригоден для эксплуатации.

Список используемых источников:

1. Гуревич, А.В. Физика композитных сверхпроводников [Текст] / А.В. Гуревич, Р.Г. Минц, А.Л. Рахманов. – М.: Наука, 1987. - 240 с.
2. Игумнов, В.Н. Основы высокотемпературной криоэлектроники [Текст] / В.Н. Игумнов. – М.: Директ-Медиа, 2014. – 237 с.
3. Головкина М.В., Богданова Е.И. Температурное управление коэффициентом пропускания нанокompозита // XXIX Российская научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов университета с приглашением ведущих ученых и специалистов родственных вузов и организаций, 2022. С. 167.
4. Головкина, М.В. Особенности распространения электромагнитных волн в волноводной структуре со сверхпроводящей пленкой и метаматериалом. [Текст] / М.В. Головкина // Известия Российской академии наук. Серия физическая. - 2010. - Т.74. - № 12. – С.1739-1743.
5. Богданова Е.И. Способы изменения резонансной частоты в наноплазмонной сверхпроводящей среде // Материалы 61 Студенческой научной конференции ПГУТИ, 2022. – С.274 – 275.
6. Богданова Е.И., Головкина М.В. Температурное изменение коэффициента прохождения для нанокompозитной среды // Материалы 25-й Всероссийской молодежной научной конференции г. Ульяновск, 25 – 27 октября 2022 года. – С. 138 – 139
7. Ашкрофт Н. Физика твердого тела [Текст] / Н. Ашкрофт, Н. Мермин. – М.: Мир, 1979. - 458 с.
8. Глущенко, А.Г., Головкина М.В. Распространение электромагнитных волн в периодических структурах со слоями сверхпроводника с электродинамическими параметрами в области нелинейности динамического смешанного состояния [Текст] / Журнал технической физики. - 2007. - Т. 10. - С. 118-120.
9. Golovkina, M. V. The electromagnetic wave amplification in thin superconducting film in non-linear mixed state [Text] / M. V. Golovkina // Journal of Physics: Conference Series. 2020 – V.1679 – P. 022061-1 – 022061-42.

Bogdanova E., Golovkina M.

Povolzhskiy State University of Telecommunications and Informatics

Calculation of the parameters of a fast superconducting filter.

In the modern world, the most important task is to create materials with desired properties and low losses. High-temperature superconductors can be used to create them. The main goal of research in the field of high-temperature superconductors is materials that operate at least at temperatures common on Earth, at most at room temperature, and their creation leads to a new breakthrough in electronics.

Key words: plasmon resonance, superconductivity, two-fluid model, superconducting filter.

УДК 681.7.068.4
ГРНТИ 49.44.31

МНОГОСЕРДЦЕВИННОЕ ОПТИЧЕСКОЕ ВОЛОКНО С ОДНОМОДОВЫМИ СЕРДЦЕВИНАМИ ИЗОЛИРОВАННЫМИ ОБОЛОЧКАМИ ИЗ ВОЗДУШНЫХ КАПИЛЛЯРОВ

М. С. Былина, А. В. Бычков, Л. А. Гультияева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Многосердцевинное оптическое волокно применяется для увеличения пропускной способности линейных трактов систем связи. Количество сердцевин, размещаемых в одном волокне, ограничивается взаимными влияниями между ними. Для уменьшения взаимных влияний между сердцевинами размещают защитные барьеры различной конструкции. В данной работе моделируется многосердцевинное волокно с сердцевинами, окруженными защитными оболочками, каждая из которых представляет собой слой воздушных капилляров. В результате моделирования рассчитаны характеристики фундаментальной моды сердцевин – хроматическая дисперсия и диаметр, проведена оценка взаимных влияний, на основании которой определено максимально возможное число сердцевин, которые можно разместить в общей оболочке стандартного диаметра 125 мкм.

многосердцевинное волокно, одномодовая сердцевина, фундаментальная мода, взаимные влияния, перекрестные помехи, затухание перекрестных помех, моделирование

При построении линейной части оптических трактов систем связи широко используются схемы параллельной передачи с применением пространственного мультиплексирования, одним из вариантов реализации которого является применение многосердцевинных волокон (МСВ) [1, 2].

МСВ представляет собой волокно с несколькими сердцевинами, объединенными общей оболочкой. Диаметр общей оболочки МСВ обычно равен $2r_3 = 125$ мкм – стандартному диаметру кварцевого волокна.

Между сердцевинами в МСВ возникают взаимные влияния, ограничивающие минимальное расстояние между двумя соседними сердцевинами и максимальное количество сердцевин, размещаемых внутри общей оболочки. Для уменьшения взаимных влияний применяются различные конструктивные решения [2].

В данной работе исследуется конструкция МСВ, каждая сердцевина которого окружена защитным барьером из восьми заполненных воздухом капилляров. На рис. 1 показаны две соседние сердцевинки такого МСВ. Параметры сердцевин МСВ, выбранные для моделирования и исследования, приведены в табл. 1. Сердцевинки полагаются одномодовыми со ступенчатым профилем показателя преломления. Моделирование МСВ проводилось в COMSOL Multiphysics [3].

На рис. 2 представлены распределения поля фундаментальной моды в сердцевинах с защитным барьером из воздушных капилляров разного диаметра. Из рис. 2 видно, что защитный барьер эффективно «блокирует» поле внутри ограничиваемой им области.

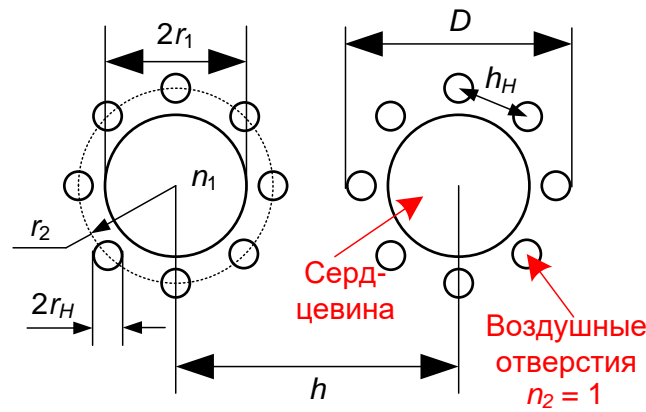


Рис. 1. Конструкция сердцевин с защитными барьерами из воздушных капилляров

ТАБЛИЦА 1. Параметры сердцевин МСВ с защитными барьерами из воздушных капилляров

Параметр	Значение
Материал сердцевины	4.1% GeO ₂ + 95.9% SiO ₂
Материал общей оболочки	100% SiO ₂
Радиус сердцевины r ₁ , мкм	4.1
Радиус защитного барьера r ₂ , мкм	6.0–6.5
Число капилляров	8
Расстояние между соседними капиллярами h _H , мкм	4.24
Радиус капилляра r _H , мкм	0.5–1.75
Длина волны, мкм	1.55

В табл. 2 представлены результаты расчета параметров фундаментальной моды на рабочей длине волны 1550 нм в сердцевинах, окруженных защитным барьером из воздушных капилляров разного диаметра. На рис. 3 представлены зависимости хроматической дисперсии фундаментальной моды от длины волны. Из таблицы и рисунка видно, что при выбранных конструкциях защитного барьера хроматическая дисперсия сердцевин получается несколько выше, чем в стандартном одномодовом волокне G.652, однако характер ее зависимости от длины волны соответствует волокну G.652.

Для оценки взаимных влияний в [4] введено понятие затухания перекрестной помехи, определяемое выражением:

$$A = 10 \lg \left(\frac{P_s}{P_n} \right), \tag{1}$$

где P_s – мощность сигнала в подверженной влиянию сердцевине, P_n – суммарная мощность перекрестных помех, созданных всеми остальными сердцевинами.

На рис. 4 представлены зависимости затухания перекрестной помехи A в сердцевине от расстояния h между сердцевинами в двухсердцевинном ОВ. Расчет мощности перекрестной помехи P_n проведен по методике, предложенной в [4].

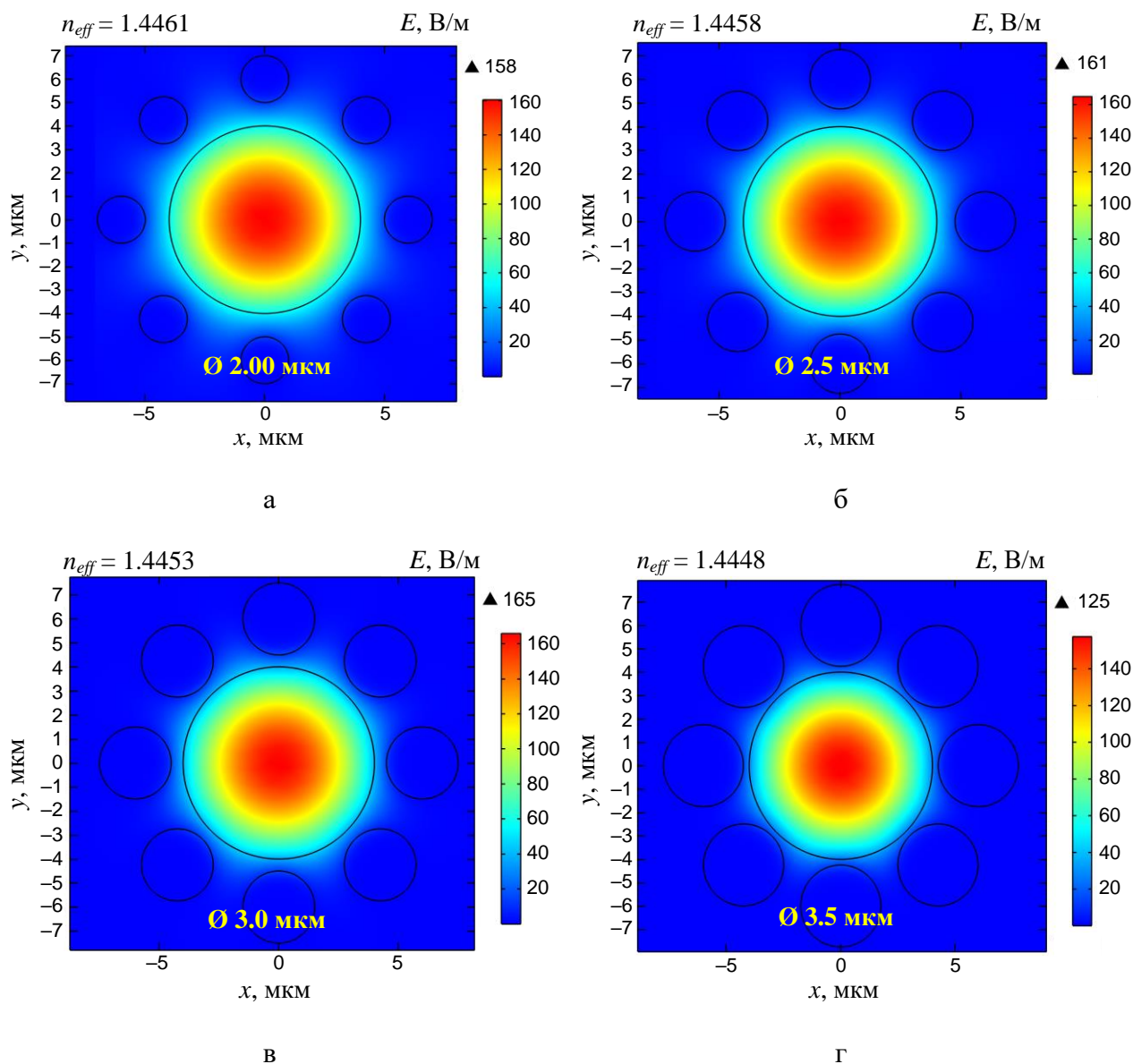


Рис. 2. Распределение поля фундаментальной моды (результат моделирования в COMSOL Multiphysics [3]) в сердцевине с защитным барьером из воздушных капилляров с радиусом: а – 1 мкм, б – 1.25 мкм, в – 1.5 мкм, г – 1.75 мкм

ТАБЛИЦА 2. Параметры фундаментальной моды сердцевины с защитным барьером радиусом из воздушных капилляров на длине волны 1550 нм

Параметр	Радиус капилляра r_H , мкм											
	0.5		0.75		1.00		1.25		1.50		1.75	
Радиус защитного барьера r_2 , мкм	6.0	6.5	6.0	6.5	6.0	6.5	6.0	6.5	6.0	6.5	6.0	6.5
Хроматическая дисперсия, $\text{пс} / (\text{нм} \cdot \text{км})$	26.8	25.3	30.2	28.0	32.8	30.2	35.2	32.2	37.5	34.1	39.8	36.0
Диаметр модового поля, мкм	8.32	8.56	8.05	8.39	7.76	7.76	7.45	7.94	7.12	7.68	6.77	7.40
Полный диаметр сердцевины D , мкм	13.0	14.0	13.5	14.5	14.0	15.0	14.5	15.5	15.0	16.0	15.5	16.5

На рис. 5 показаны зависимости минимально необходимого расстояния h_{\min} между сердцевинами, обеспечивающего определенное заданное значение A , от радиуса капилляра. Из рис. 5 видно, что для $A = 60$ дБ: при $r_2 = 6$ мкм наименьшее достижимое расстояние h_{\min} составляет 15 мкм и достигается при радиусе капилляра 1.5 мкм; при $r_2 = 6.5$ мкм наименьшее достижимое расстояние h_{\min} составляет 15.5 мкм и достигается при радиусе капилляра 1.25 мкм.

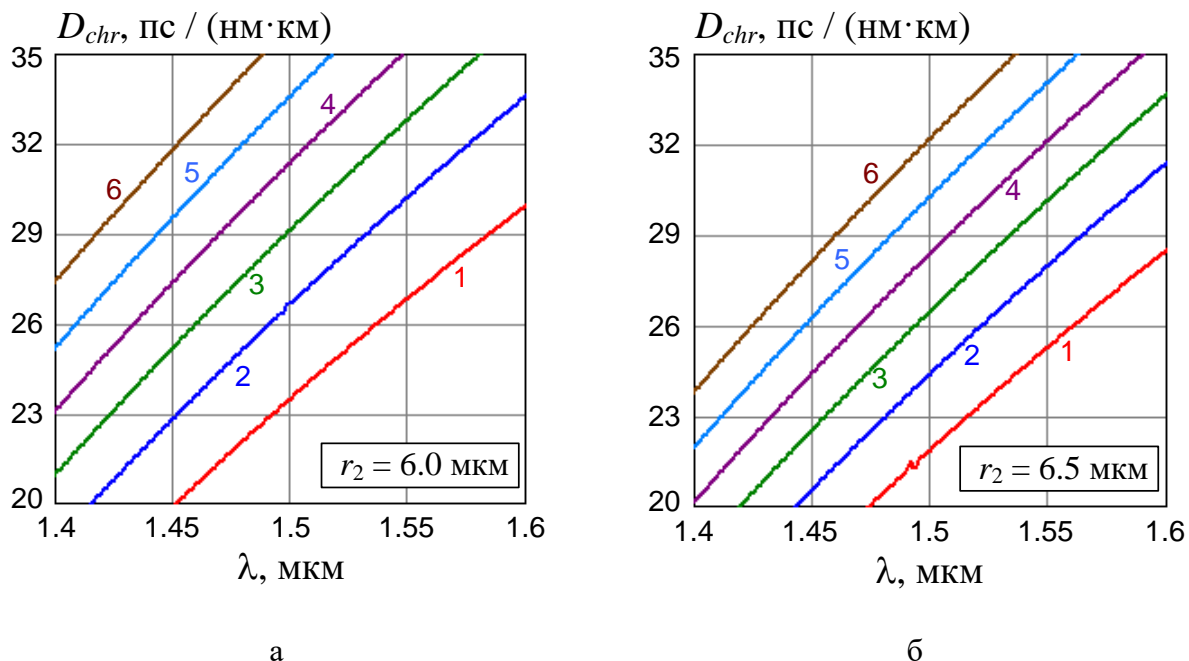


Рис. 3. Зависимость хроматической дисперсии от длины волны для сердцевины с защитным барьером радиусом 6 мкм (а) и 6.5 мкм (б) из воздушных капилляров радиусами: 1 – 0.5 мкм, 2 – 0.75 мкм, 3 – 1.00 мкм, 4 – 1.25 мкм, 5 – 1.5 мкм, 6 – 1.75 мкм

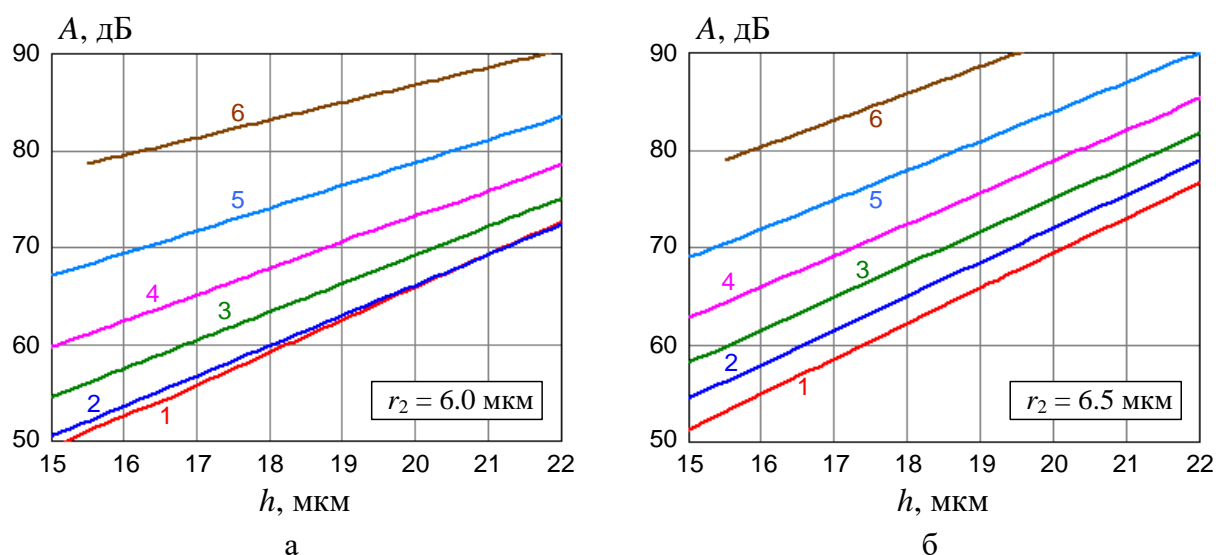


Рис. 4. Затухание перекрестной помехи в МСВ с двумя одинаковыми сердцевинами, окруженными защитными барьерами радиусами 6 мкм (а) и 6.5 мкм (б), состоящими из воздушных капилляров с радиусами: 1 – 0.5 мкм, 2 – 0.75 мкм, 3 – 1.00 мкм, 4 – 1.25 мкм, 5 – 1.5 мкм, 6 – 1.75 мкм

Определенное h_{\min} можно считать эквивалентным диаметром сердцевины МСВ и использовать для определения максимального количества сердцевин N_{\max} , которые можно расположить в общей оболочке МСВ. Для этого нужно решить задачу упаковки кругов с меньшим диаметром $d = h_{\min}$ в круг с большим диаметром $D = 2r_3$ [5].

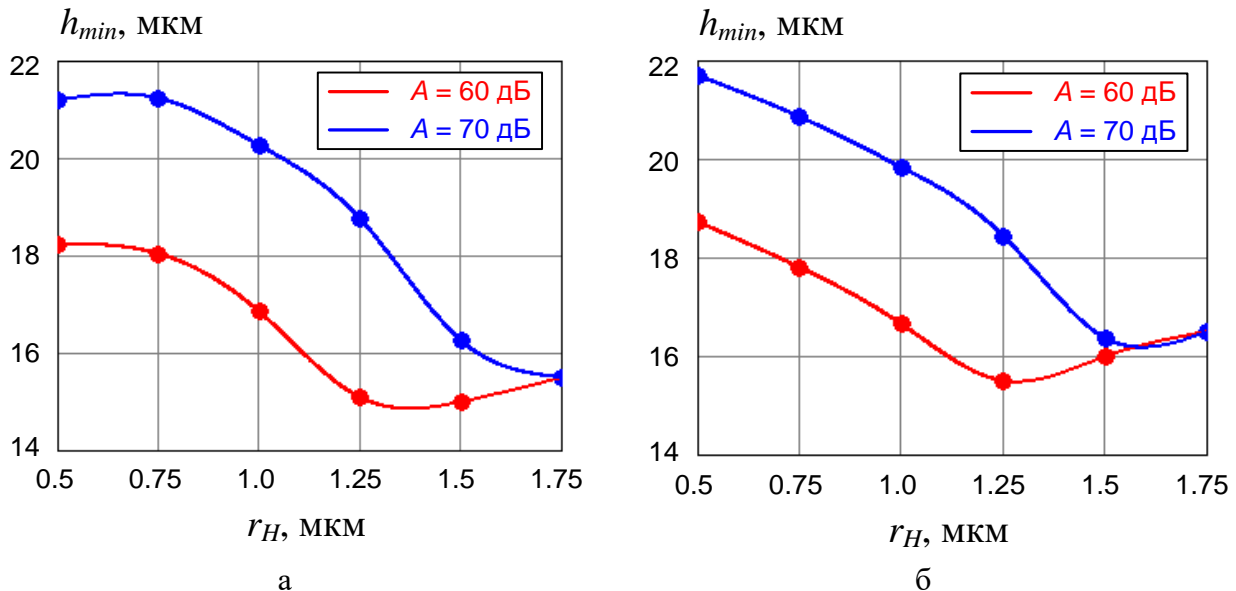


Рис. 5. Минимальное расстояние h_{\min} между сердцевинами в МСВ, при котором обеспечивается затухание перекрестной помехи 60 и 70 дБ. Радиус защитного барьера принят равным: а – 6 мкм, б – 6.5 мкм

Из рассмотренных конструкций наилучшие параметры были достигнуты при $r_2 = 6$ мкм и $r_H = 1.5$ мкм. Для такого ОВ h_{\min} составляет 15 мкм, что позволяет создать МСВ с 54 сердцевинами.

Список используемых источников:

1. Семенов А.Б. Параллельная волоконно-оптическая передача в ЛВС и СКС. Подходы к реализации физического и канального уровней. – М.: Горячая линия – Телеком, 2018. – 272 с.
2. Былина М.С., Гулятьева Л.А. Новые типы многосердцевинных волокон для центров обработки данных. В сборнике: лучших докладов конференции Подготовка профессиональных кадров в магистратуре для цифровой экономики ПКМ – 2021. С. 175-179.
3. Программное обеспечение COMSOL Multiphysics®. Понимание, прогнозирование, оптимизация реалистичных физических процессов и устройств с помощью численного моделирования. URL: <https://www.comsol.ru/comsol-multiphysics> (доступ 13.11.2022).
4. Былина М.С., Гулятьева Л.А. Многосердцевинное оптическое волокно со ступенчатыми одномодовыми сердцевинами. Часть 1. // Труды учебных заведений связи. Том 8, № 4, 2022.
5. G.E. Reis. Dense Packing of Equal Circles within a Circle. Math. Mag. 48 (1975) 1, 33–37.

Bylina M., Bychkov A., Gulyaeva L.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Multi-core optical fiber with single-mode cores insulated with shells of air capillaries. Multi-core optical fiber is used to increase the throughput of linear paths of communication systems. The number of cores placed in one fiber is limited by mutual influences between them. To reduce mutual influences, protective barriers of various designs are placed between the cores. In this paper, a multi-core fiber is modeled with cores surrounded by protective shells, each of which is a layer of air capillaries. As a result of modeling, the characteristics of the fundamental modes of the cores – chromatic dispersion and diameter - were calculated, an assessment of mutual influences was carried out, on the basis of which the maximum possible number of cores that can be placed in a common shell with a standard diameter of 125 microns was determined.

Key words: *multi-core fiber, single-mode core, fundamental mode, mutual influences, crosstalk, crosstalk attenuation, simulation.*

УДК 681.7
ГРНТИ 49.44

ТЕРМИНАЛЬНЫЙ ЧЕТЫРЕХКАНАЛЬНЫЙ МУЛЬТИПЛЕКСОР ДЛЯ СИСТЕМЫ CWDM

М. С. Былина, М. В. Кажаяев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе представлена модель мультиплексора на основе каскадно включенных интерференционных фильтров, предназначенного для системы грубого спектрального уплотнения (CWDM). Рассчитана конструкция каждого фильтра. Разработана схема мультиплексора в среде OptiSystem и проведено его исследование. Определены параметры устройства – вносимые потери, изоляция, спектральные характеристики.

Coarse Wavelength Division Multiplexing, CWDM, интерференционный фильтр, мультиплексор, моделирование

Технология грубого спектрального уплотнения (Coarse Wavelength Division Multiplexing, CWDM) позволяет одновременно передавать по оптическому волокну (ОВ) несколько информационных сигналов, сформированных на разных длинах волн (спектральных каналов). Длины волн каналов CWDM располагаются в диапазоне от 1271 нм до 1611 нм равномерно с шагом 20 нм. Сигнал каждого канала формируется своим передающим устройством, затем все сигналы объединяются в одно ОВ с помощью мультиплексора (MUX).

MUX CWDM традиционно строится на основе каскадно включенных интерференционных фильтров (Thin Film Filter, TFF) [1]. В данной работе исследуется терминальный MUX CWDM, предназначенный для объединения или разделения четырех каналов с длинами волн 1510, 1530, 1550, 1570 нм. Схема моделируемого MUX представлена на рис. 1. Она содержит три отражательных TFF, каждый из которых выделяет из группового сигнала или добавляет в него один спектральный канал.

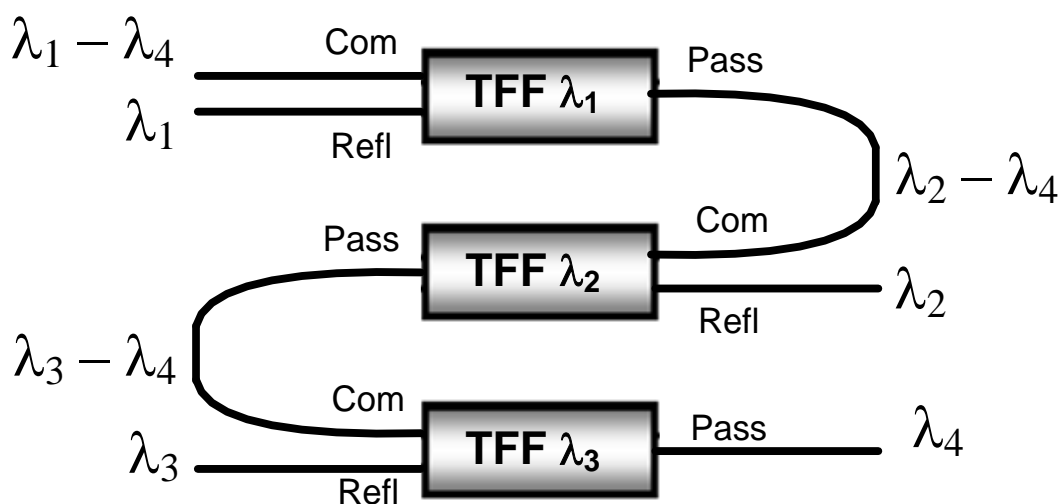


Рис. 1. Схема моделируемого MUX

Синтезируем отражательные фильтры TFF для MUX по следующим требованиям: коэффициент отражения на центральной длине волны не менее $R_{\max} = 0.99$, ширина спектра отражения не более $\Delta\lambda_{\min} = 10$ нм. В табл. 1 представлены параметры синтезированных TFF, рассчитанные по методике, приведенной в [1, 2].

Период интерференционной структуры рассчитывался, исходя из центральной длины волны λ_0 и угла падения излучения θ :

$$\Delta = \frac{\pi}{k(\lambda_0) \cdot \cos(\theta)}, \quad k(\lambda) = \frac{2\pi}{\lambda} \sqrt{\frac{n_2^2 + n_1^2}{2}}, \quad (1)$$

где $k(\lambda)$ – волновое число, n_1 и n_2 – показатели преломления слоев интерференционной структуры.

Необходимое число слоев в интерференционной структуре рассчитывалось, исходя из заданного R_{\max} :

$$N = \frac{\ln\left(\frac{1+R_{\max}}{1-R_{\max}}\right)}{(2 \cdot |K_s(\lambda_0)| \cdot \Delta)}, \quad (2)$$

где K_s – коэффициент связи между противоположно направленными модами:

$$K(\lambda) = \begin{cases} \frac{i}{\lambda \cdot \cos(\theta)} \cdot \sqrt{\frac{2(n_2^2 - n_1^2)}{n_2^2 + n_1^2}} & \text{для } TE \text{ – волны} \\ \frac{i}{\lambda \cdot \cos(\theta)} \cdot \sqrt{\frac{2(n_2^2 - n_1^2)}{n_2^2 + n_1^2}} \cdot \cos(2\theta) & \text{для } TM \text{ – волны,} \end{cases} \quad (3)$$

где i – мнимая единица, λ – длина волны.

ТАБЛИЦА 1. Параметры TFF

Параметр	TFF 1510 нм	TFF 1530 нм	TFF 1550 нм
Угол падения излучения на интерференционную структуру, град.	45	45	45
Показатель преломления одного из слоев n_1	1.52	1.52	1.52
Глубина модуляции показателя преломления $\Delta n = n_2 - n_1$	10^{-5}	10^{-5}	10^{-5}
Период интерференционной структуры Δ , нм	702.5	711.8	721.1
Число периодов в интерференционной структуре	1381	1363	1345
Толщина структуры, мкм	969.8	970.1	970.1
Ширина спектра отражения, нм	2.8	2.8	2.8

На рис. 2 представлены спектральные характеристики синтезированных TFF. Из рис. 2б видно, что ожидаемая изоляция спектральных каналов в MUX на

основе этих фильтров составит не менее 25 дБ, что соответствует параметрам серийно выпускаемых мультиплексоров.

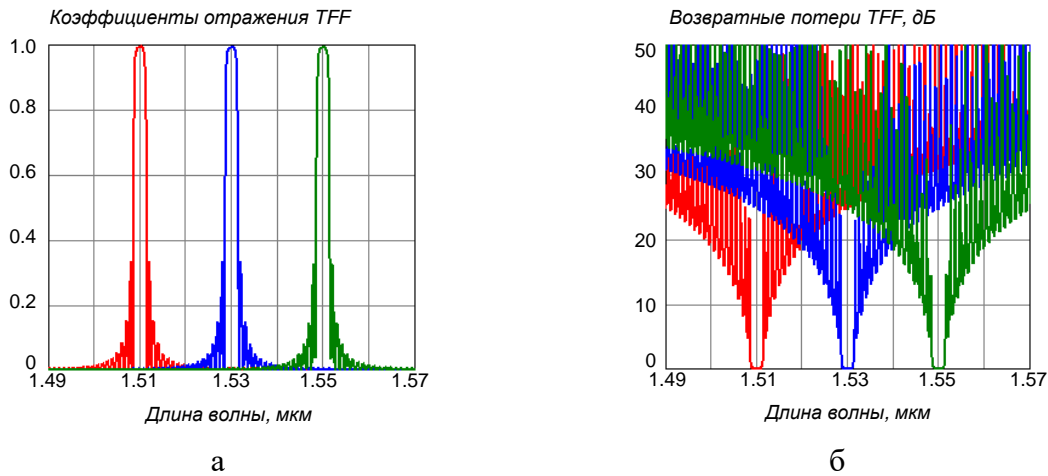


Рис. 2. Спектральные характеристики смоделированных TFF:
 а – коэффициенты отражения, б – возвратные потери

Моделирование MUX было проведено в среде OptiSystem [3]. Схема моделируемого MUX в OptiSystem представлена на рис. 3.

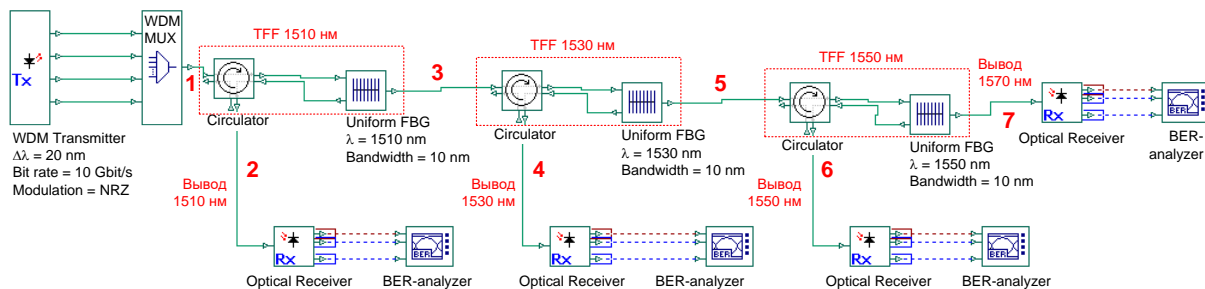


Рис. 3. Модель мультиплексора в Optisystem

Устройство работает в режиме демультиплексирования. В схеме используются 4 передатчика, формирующих цифровые оптические сигналы со скоростью 10 Гбит/с, средней мощностью 10.4 дБм и модуляцией ASK-NRZ на длинах волн 1510, 1530, 1550, 1570 нм. Излучение передатчиков объединяется идеальным мультиплексором WDM MUX в групповой сигнал, который поступает на вход исследуемого устройства – демультиплексора, образованного тремя фильтрами TFF.

Демультиплексированные сигналы принимаются приемными устройствами Optical Receiver. Качество сигналов на выходах приемников контролируется анализаторами цифровой связи BER-analyzer.

На рис. 4 представлена использованная в модели эквивалентная схема трехпортового TFF. В качестве отражательного фильтра использован компонент Uniform FBG (однородная волоконная брэгговская решетка), имеющая спектр отражения, аналогичный спектру отражения TFF [4]. Параметры Uniform FBG выбирались в соответствии с параметрами синтезированных TFF. Для

разделения прямого и отраженного сигналов в эквивалентной схеме используется идеальный циркулятор, вносимые потери которого приняты равными 0.

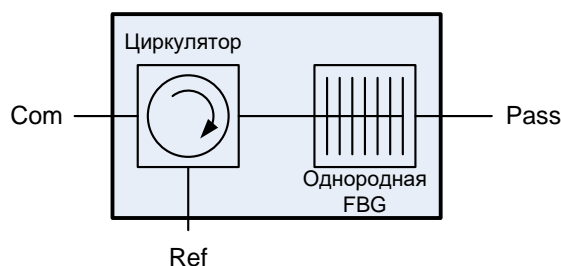


Рис. 4. Схема замещения TFF

Для проведения исследования в разные точки схемы подключались визуализаторы – идеальные измерительные приборы, которые позволяли контролировать уровень мощности и спектр излучения.

Спектр излучения в спектральном канале 1570 нм на выходе передатчика представлен на рис. 5а. На рис. 5б представлен спектр в том же канале после демультиплексирования исследуемым MUX. Видно, что спектры излучения практически одинаковы, то есть MUX практически не внес искажений.

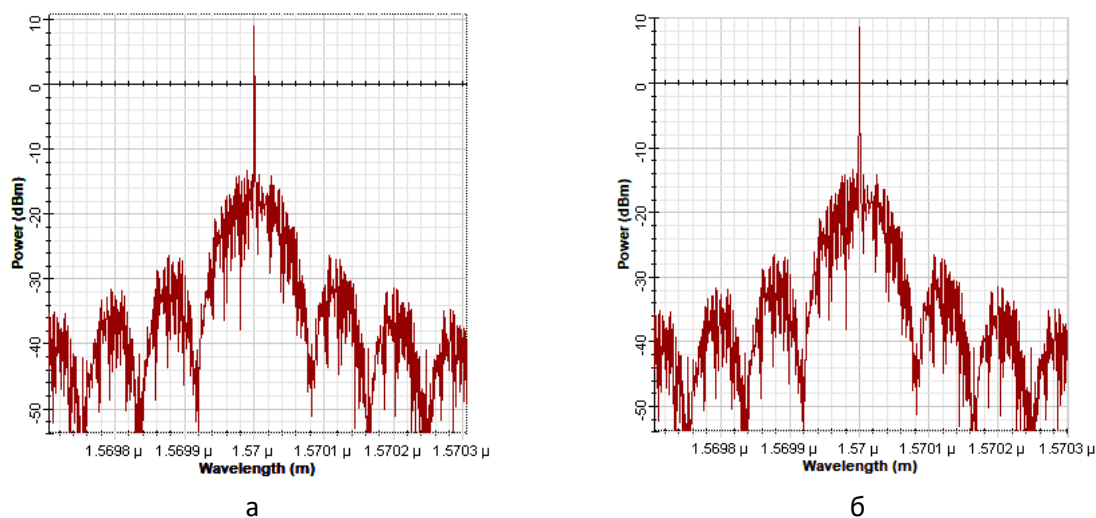


Рис. 5. Спектры излучения в канале 1570 нм:
а – на выходе передатчика, б – на выходе демультиплексора

В табл. 2 представлены результаты измерения уровней сигналов разных спектральных каналов и других параметров в указанных на рис. 2 точках схемы.

ТАБЛИЦА 2. Результаты моделирования

Длина волны, нм	Амплитуда сигнала, измеренная по спектроанализатору (дБм) в точках							Потери в канале, обусловленные неполным отражением от TFF, дБ	Реальные потери в канале, дБ
	1	2	3	4	5	6	7		
1510	8.72	8.70	-5.20	-31.8	-5.20	-35.5	-5.20	0.20	0.72
1530	9.10	-17.4	8.98	8.90	-4.80	-31.0	-4.80	0.20	1.42

Длина волны, нм	Амплитуда сигнала, измеренная по спектроанализатору (дБм) в точках							Потери в канале, обусловленные неполным отражением от TFF, дБ	Реальные потери в канале, дБ
	1	2	3	4	5	6	7		
1550	9.00	-22.1	8.94	-17.6	9.00	8.90	-5.00	0.10	2.11
1570	8.90	-23.5	8.89	-22.2	8.90	-17.0	8.75	0.15	2.25
Общая мощность, дБм	16.4	10.4	15.1	10.2	13.4	10.3	10.5	–	–
Q-фактор	–	1116	–	1296	–	1435	828	–	–

Из табл. 2 следует, что смоделированное устройство имеет малое затухание, так как при расчетах учитывались только потери, обусловленные неполным отражением от TFF. Реальные потери в спектральных каналах будут больше. Приняв средние потери в одном TFF равными 0.7 дБ, что соответствует серийно выпускаемым устройствам, получим полные потери в четырех спектральных каналах – 0.72, 1.42, 2.11 и 2.25 дБ соответственно.

Список используемых источников:

1. Былина М.С., Кажяев М.В. Исследование интерференционного фильтра для мультиплексора CWDM / Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021). Всероссийская научно-методическая конференция магистрантов и их руководителей; материалы конф. – СПб: СПбГУТ, 2022 – С. 487-490.

2. Довольнов, Е.А., Кузнецов В.В., Миргород В.Г., Шарангович С.Н. Мультиплексорное и усилительное оборудование многоволновых оптических систем передачи: учеб. пособие. – Томск: ТУСУР, 2016. – 156 с.

3. Join Optiwave FREE for Academics Program to Support Your Education at Home [Электронный ресурс]. – Режим доступа: [www.url: https://optiwave.com/resources/latest-news/free-for-academics-program-2020/](https://optiwave.com/resources/latest-news/free-for-academics-program-2020/) – 05.11.2022.

4. Варжель С.В. Волоконные брэгговские решетки: учеб. пособие / СПб: ИТМО, 2015. – 65 с.

Bylina M., Kazhaev M.

The Bonch-Bruевич St. Petersburg State University of Telecommunications.

Terminal four-channel multiplexer for CWDM system.

The paper presents a model of a multiplexer based on cascaded interference filters designed for a Coarse Wavelength Division Multiplexing (CWDM) system. The design of each filter is calculated. A multiplexer circuit in the OptiSystem environment has been developed and its research has been carried out. The parameters of the device are determined - insertion loss, isolation, spectral characteristics.

Key word: Coarse Wavelength Division Multiplexing, CWDM, Interference Filter, Multiplexer, Modeling.

УДК 621.39
ГРНТИ 49.44.31

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ФОТОПРИЕМНЫХ УСТРОЙСТВ ДЛЯ ЭНЕРГЕТИЧЕСКОГО ПРИЕМА ЦИФРОВЫХ ОПТИЧЕСКИХ СИГНАЛОВ

Н. С. Васильев, В. П. Клименко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена сравнительному анализу трех типов фотоприемных устройств (ФПУ) для энергетического приема (ЭП) цифровых оптических сигналов с бинарной модуляцией. Рассмотрены ФПУ, использующие лавинные фотодиоды (ЛФД) и *p-i-n* фотодиоды с использованием и без использования предварительных оптических усилителей (ОУ). Исследовались возможности оптимизации ФПУ по величине *Q*-фактора. Проведено имитационное моделирование и сравнение качества связи.

волоконно-оптическая система связи, одномодовое оптическое волокно, фотодиод, лавинный фотодиод, оптический усилитель, Q-фактор

Схемы фотоприемных устройств. Выходные сигналы.

Для сравнительного анализа параметров ФПУ с ЭП будем рассматривать схемы с непосредственной подачей оптического сигнала с изменяющейся мощностью $P(t)$ на фотодиод (ФД) с *p-i-n* структурой или с лавинным умножением (рис. 1а), а также схему с ФД *p-i-n* структуры с предварительным оптическим усилителем ПОУ (рис. 1б) [1, 2].

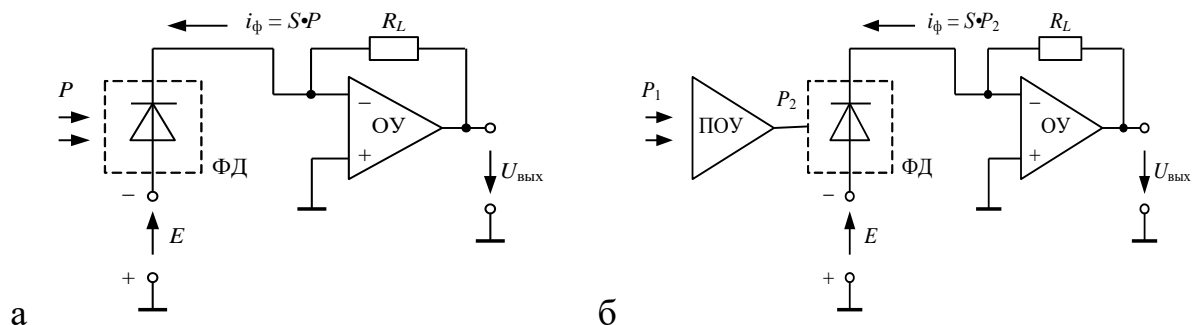


Рис. 1. Схемы аналоговой части ФПУ

ЛФД (рис. 1а) преобразует входную оптическую мощность $P(t)$ в фототок $I_\phi(t) = -S \cdot M \cdot P(t)$, где S – чувствительность ФД без учета лавинного усиления ($M=1$). Для преобразования $I_\phi(t)$ в выходное напряжение $U_{\text{вых}}$ используется трансимпедансный усилитель фототока (УФТ), выполненный на основе операционного усилителя (ОУ), с коэффициентом преобразования равным сопротивлению нагрузки R_L

$$U_{\text{вых_ФД}}(t) = -S \cdot M \cdot P(t) \cdot R_L \quad (1)$$

Выражение (1) пригодно и для ФД р-і-n структуры при $M=1$.

Запишем выражение для выходного напряжения на выходе схемы (рис. 1б) с ПОУ, имеющим коэффициент усиления G .

$$U_{\text{вых}_\text{оу}}(t) = -S \cdot G \cdot P(t) \cdot R_L \quad (2)$$

Далее рассматриваем входной оптический сигнал с бинарной амплитудной модуляцией (АМ), полагая, что при приеме логической «1» мощность составляет P_1 , а при приеме логического «0» P_0 . Выходной сигнал в схеме рис. 1а представляем в виде тока на выходе ЛФД при приеме логической «1» I_1 , а при «0» I_0

$$\begin{aligned} I_1 &= S \cdot M \cdot P_1, \\ I_0 &= S \cdot M \cdot P_0. \end{aligned} \quad (3a)$$

Для схемы рис. 1б с ПОУ получим

$$\begin{aligned} I_1 &= S \cdot G \cdot P_1, \\ I_0 &= S \cdot G \cdot P_0. \end{aligned} \quad (3б)$$

Шумы на выходе ФПУ.

Рассмотрим основные источники шумов ФПУ. Будем их приводить к выходу ФД, и оценивать дисперсией шумового тока при приеме логической «1» σ_1^2 и «0» σ_0^2 , соответственно.

Определим дисперсию дробового шума ЛФД с учетом шума лавины в предположении, что эти шумы имеют распределение Пуассона [2]

$$\sigma_{d1}^2 = \bar{M}^2 \cdot F(\bar{M}) \cdot (S \cdot P_1 + I_T) \cdot \Delta F, \quad \sigma_{d0}^2 = \bar{M}^2 \cdot F(\bar{M}) \cdot (S \cdot P_0 + I_T) \cdot \Delta F, \quad (4)$$

где \bar{M} - средний коэффициент лавинного умножения фототока в ЛФД, I_T - темновой ток, ΔF - полоса пропускания ФПУ, как фильтра нижних частот (ФНЧ), а $F(\bar{M})$ - коэффициент шума лавины, который можно определить по формуле Макинтайра (рис. 2):

$$F(\bar{M}) = \bar{M} \cdot \left[1 - (1 - k_\alpha) \cdot ((\bar{M} - 1) / \bar{M})^2 \right], \quad (5)$$

где $k_\alpha = \alpha_p / \alpha_n$, α_p и α_n - коэффициенты ионизации для дырок и электронов, соответственно, представляющие собой вероятности ионизации атома на единицу длины (1/см). Они зависят от свойств материала полупроводника и составляют: для Si - $k_\alpha = 0.05-0.1$, для Ge - $k_\alpha \approx 1$ и для AsGa - $k_\alpha = 0.4-0.5$. Определим дисперсию приведенного к выходу ФД теплового шума резистора R_L в обратной связи ОУ (рис. 1) с учетом шумов ОУ и последующих схем

$$\sigma_T^2 = 4 \cdot k_b \cdot T_a \cdot \Delta F \cdot k_n / R_L, \quad (6)$$

где $k_b=1.38 \cdot 10^{-23}$ Дж/К постоянная Больцмана, T_a – абсолютная температура, k_n – коэффициент, учитывающий увеличение шума за счет ОУ и последующих схем. Полагаем распределение этих шумов гауссовским с математическим ожиданием равным 0.

Основным источником шумов эрбиевого ПОУ (EDFA) является усиленное спонтанное излучение (УСИ), мощность которого составляет [1, 2]

$$P_{sp} = h \cdot \nu \cdot \Delta \nu \cdot (F_{oy} \cdot G - 1), \quad (7)$$

где F_{oy} - коэффициент шума ПОУ, $h=6.626 \cdot 10^{-34}$ Дж с – постоянная Планка, ν – несущая частота оптического сигнала, $\Delta \nu$ – ширина оптической полосы для сигнала.

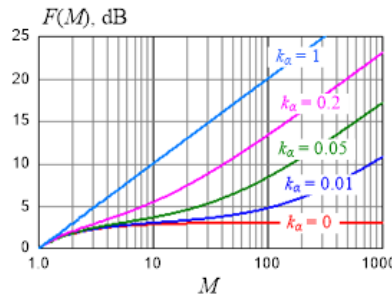


Рис. 2. Зависимость коэффициента шума от коэффициента лавинного умножения

Полагая распределение шумов УСИ пуассоновским, определим обусловленную ими дисперсию шумового тока, приведенного к выходу ФД

$$\sigma_{sp}^2 = S \cdot h \cdot \nu \cdot \Delta \nu \cdot (F_{oy} \cdot (G - 1)) \cdot \Delta F. \quad (8)$$

Источник излучения с мощностью P также обладает своими шумами, которые можно представить дисперсией σ_p^2 в виде некоторой доли от P^2 .

$$\sigma_p^2 = k_{uc} \cdot P^2 \quad (9)$$

Будем полагать, что источники шумов независимы друг от друга и суммарная дисперсия шумового тока будет равна сумме дисперсий отдельных шумовых составляющих. Запишем выражения для суммарной дисперсии шумов при приеме сигналов логической «1» и «0».

$$\text{для рис. 1а: } \sigma_1^2 = \sigma_{d1}^2 + \sigma_T^2 \quad \sigma_0^2 = \sigma_{d0}^2 + \sigma_T^2 \quad (10a)$$

$$\text{для рис. 1б: } \sigma_1^2 = \sigma_{d1}^2 + \sigma_T^2 + \sigma_{oy}^2 + \sigma_{p1}^2 \quad \sigma_0^2 = \sigma_{d0}^2 + \sigma_T^2 + \sigma_{oy}^2 + \sigma_{p0}^2 \quad (10б)$$

Сравнение ФПУ по качеству связи.

Для сравнения различных схем построения ФПУ с ЭП будем оценивать качество связи цифровых ВОСС с бинарной амплитудной модуляцией (АМ) по величине Q – фактора, который однозначно связан с вероятностью битовых ошибок (BER) [1]:

$$Q = (I_1 - I_0) / (\sigma_0 + \sigma_1) \quad (11)$$

Из рис. 3 видно, что качество связи в ФПУ с ЛФД монотонно растет с увеличением входной мощности, а коэффициент лавинного умножения имеет оптимальное значение, примерно равное $M=6$. В ФПУ, использующему р-і-п ФД и ПОУ, качество связи с увеличением коэффициента усиления ПОУ монотонно растет стремясь к насыщению.

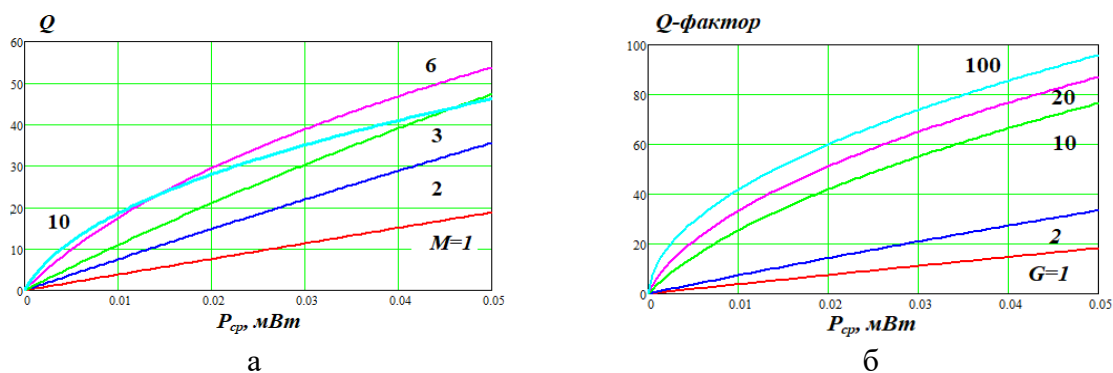


Рис. 3. Результаты расчетов Q -фактора для ФПУ с ЛФД (а) и с ПОУ (б)

Имитационное моделирование рассмотренных ФПУ

Схема моделирования в программе OptiSystem приведена на рис. 4. Она включает: оптический передатчик с длиной волны $\lambda_0=1550$ нм, с бинарной АМ, кодированием NRZ и скоростью передачи $V=10$ Гбит/с; регулируемый аттенюатор; разветвитель 3 дБ; ПОУ, два ФПУ на основе ФД р-і-п структуры и ЛФД. Для измерений использованы приборы: измерители мощности, оптические и электрические осциллографы.

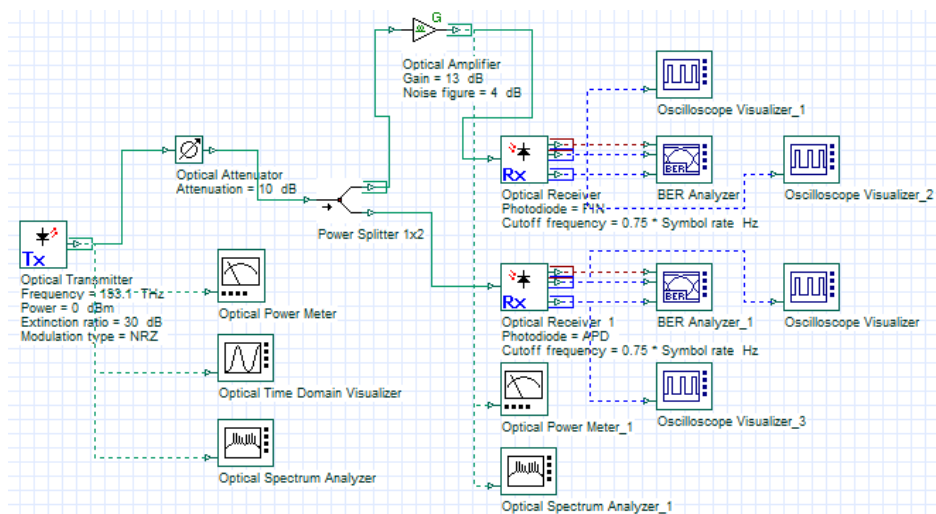


Рис. 4. Схема исследований ФПУ

Исходные данные для исследований: уровень пиковой мощности передатчика $p_m=0$ дБм, затухание в АТТ $a=10$ дБ, коэффициент шума ПОУ $F_{oy}=4$ дБ (2.5), чувствительность ФД $S=1$ А/Вт, темновой ток $I_T=10$ нА.

Первая серия исследований проводилась при постоянном пиковом уровне мощности $p=0$ дБм и постоянном затухании АТТ $a=10$ дБ. Изменялись коэффициент лавинного умножения M для ЛФД и коэффициент усиления ПОУ G . Результаты измерений приведены в таблице 1.

ТАБЛИЦА 1. Результаты исследований ФПУ

№	Исследования ФПУ с ЛФД			Исследования ФПУ с ПОУ		
	M	k_a	Q	G , дБ	F_{oy} , дБ	Q
1	1	0.9	20.3	0	0	19.9
2	2	0.9	36.1	2	4	29
3	3	0.9	44.8	3	4	35.4
4	4	0.9	48.2	4	4	42
5	5	0.9	49	5	4	50
6	6	0.9	48.5	6	4	55
7	8	0.9	46	10	4	75.9
8	10	0.9	43.2	13	4	85
9	15	0.9	37.3	18	4	91.7
10	5	0.7	51.5	16	4	96
11	5	0.5	54.4	20	4	99.7
12	5	0.3	58	26	4	93.6
13	5	0.1	62.6	30	4	93

Выводы. Видно, что результаты теоретических расчетов и имитационного моделирования практически совпадают. Исследования будут продолжены.

Список используемых источников:

1. Листвин В.Н., Трещиков В.Н. DWDM системы. Издание 4-е. – М.: Техносфера, 2021. – 420 с.
2. М.С. Былина, С.Ф. Глаголев, А.С. Дюбов Сравнительный анализ методов энергетического и когерентного приема цифровых информационных оптических сигналов. Часть 1. Энергетический прием. ТУЗС, 2017, т.3, с. 12-20.

Vasiliev N., Klymenko V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Comparative analysis of photodetectors for energy reception of digital optical signals.

The work is devoted to a comparative analysis of three types of photodetectors for energy reception of digital optical signals with binary modulation. Photodetectors using avalanche photodiodes and p-i-n photodiodes with and without pre-amplifiers are considered. The possibilities of optimizing photodetectors in terms of the Q-factor were studied. Simulation modeling and comparison of communication quality were carried out.

Key words: *optical fiber communication system, single-mode optical fiber, photodiode, avalanche photodiode, optical amplifier, Q-factor.*

УДК 535
УДК 535
ГРНТИ 29.31.29

УВЕЛИЧЕНИЕ СООТНОШЕНИЯ СИГНАЛЬНЫХ И ОПОРНЫХ ИМПУЛЬСОВ ДЛЯ ФАЗОВОЙ КОМПЕНСАЦИИ В СИСТЕМАХ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА НА НЕПРЕРЫВНЫХ ПЕРЕМЕННЫХ

Ф. М. Гончаров, Б. А. Наседкин, Б. Е. Первушин

Национальный исследовательский университет ИТМО

Система квантового распределения ключа на непрерывных переменных (КРКНП) является перспективным направлением развития квантовых коммуникаций. Когерентное детектирование, которое лежит в основе работы протоколов КРКНП, влечет за собой необходимость учета и компенсации фазовых искажений. Алгоритмы фазовой компенсации основываются на использовании опорных импульсов, с помощью которых оценивается фазовый шум и производится корректировка измеренных значений квадратур сигнальных импульсов. Соотношение числа опорных импульсов к сигнальным с одной стороны влияет на точность работы алгоритма фазовой компенсации, а с другой стороны на скорость генерации секретного ключа.

квантовое распределение ключа на непрерывных переменных, фазовый шум, фазовая компенсация, скорость генерации секретного ключа

Система квантового распределения ключа на непрерывных переменных (КРК НП) является перспективным направлением развития квантовых коммуникаций [1, 2]. Ключевой особенностью данной системы является когерентное детектирование [3], основанное на интерференции слабого сигнального излучения и сильного локального осциллятора (ЛО), позволяющее измерять квадратурные составляющие электромагнитного поля, с помощью которых производится кодирование информации. Наличие интерференции как основополагающей составляющей обуславливает необходимость учета и компенсации фазовых шумов в системе. Существуют алгоритмы [4, 5], основанные на чередовании сигнальных и опорных импульсов, с помощью которых проводится фазовая компенсация. Однако, использование большого числа опорных импульсов (один опорный к одному сигнальному) снижает скорость генерации секретного ключа. Возможность использования большего числа сигнальных импульсов на один опорный импульс позволяет увеличить скорость генерации ключа.

Для анализа влияния соотношения сигнальных и опорных импульсов используется метод линейной фазовой компенсации, при котором дрейф фазы считается изменяющимся линейно во временном промежутке между двух опорных импульсов. Идея использования двух опорных импульсов для фазовой компенсации одного сигнального между ними с использованием среднего значения дрейфа фазы выдвигалась в [6] для системы с сильными фазовыми

шумами. Исходя из значений квадратур $Q_{BR}^{1st}, P_{BR}^{1st}$ и $Q_{BR}^{2nd}, P_{BR}^{2nd}$ первого и второго опорного импульса, вычисляются значения дрейфа фазы и пропускания для первого и второго опорного импульса по следующим формулам соответственно:

$$\hat{\theta}^{1st} = \arctg\left(\frac{P_{BR}^{1st}}{Q_{BR}^{1st}}\right); T^{1st} = \|(Q_{BR}^{1st}, P_{BR}^{1st})\|^2; \quad (1)$$

$$\hat{\theta}^{2nd} = \arctg\left(\frac{P_{BR}^{2nd}}{Q_{BR}^{2nd}}\right); T^{2nd} = \|(Q_{BR}^{2nd}, P_{BR}^{2nd})\|^2. \quad (2)$$

Далее с помощью полученных по формулам (1,2) значений для каждого сигнального импульса из числа n_s между двумя опорными рассчитываются следующие значения поправки дрейфа фазы и пропускания:

$$\hat{\theta}_m = \frac{m(\theta^{2nd} - \theta^{1st})}{n_s + 1} + \hat{\theta}^{1nd};$$

$$T_m = \frac{m(T^{2nd} - T^{1st})}{n_s + 1} + T^{1nd}.$$

Получатель производит корректировку своих значений Q_{AS}^m и P_{AS}^m (значений сигнальных импульсов, которые отправитель посылал получателю), расположенных между соответствующими опорными импульсами $Q_{AR}^{1st}, P_{AR}^{1st}$ и $Q_{AR}^{2nd}, P_{AR}^{2nd}$ (значения опорных импульсов, которые отправитель посылал получателю) по формуле:

$$(\hat{Q}_{AS}^m \hat{P}_{AS}^m) = \sqrt{T_m} (\cos \hat{\theta}_m - \sin \hat{\theta}_m \sin \hat{\theta}_m \cos \hat{\theta}_m) (Q_{AS}^m P_{AS}^m).$$

Целью увеличения числа сигнальных импульсов в цикле является увеличение скорости генерации секретного ключа (СГСК). Значение СГСК задается в приближении для ключей бесконечной длины выражением [2]:

$$K = f_{sym} \cdot r$$

где f_{sym} – скорость передачи символов (в единицах символов симв^{-1}), а r – скорость генерации ключа в пересчете на посылку. Для упрощения анализа пусть данное выражение уже содержит предельный случай один сигнальный к одному опорному. Тогда можно переписать выражение для скорости генерации секретного ключа таким образом, чтобы учитывалось изменение числа сигнальных импульсов в цикле относительно рассмотренного случая:

$$K' = \varepsilon \cdot K; \varepsilon = 2n_s \cdot (n_s + 1)^{-1},$$

где ε показывает изменение соотношения сигнальных и опорных импульсов в цикле относительно соотношения один к одному.

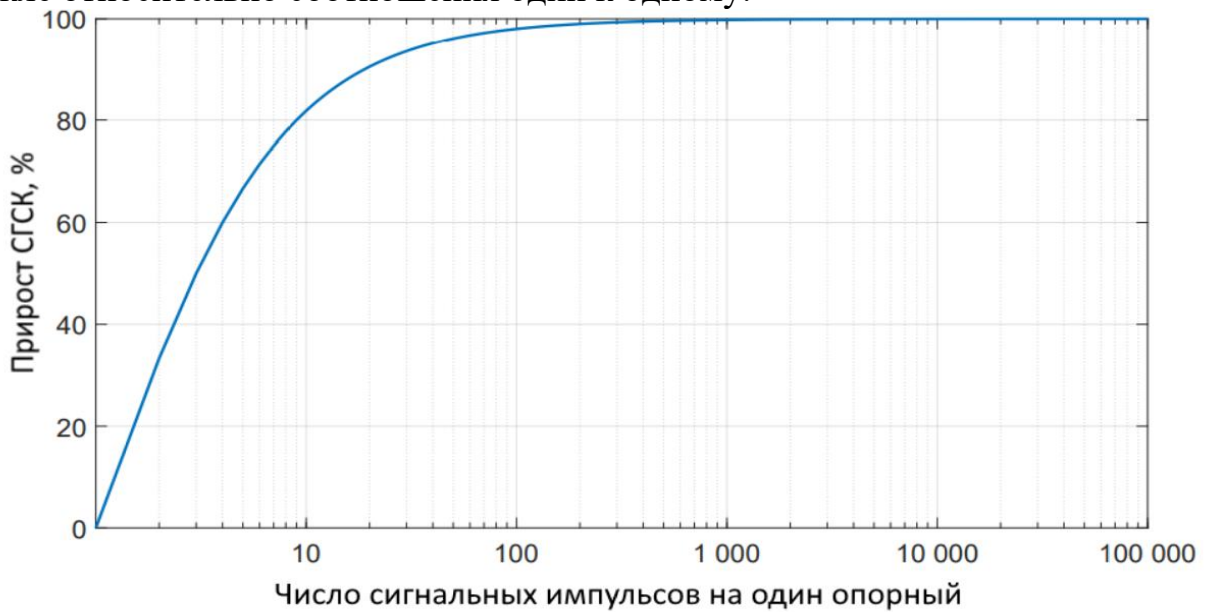


Рис. 1. График зависимости увеличения скорости генерации секретного ключа (относительно одного сигнального импульса в цикле) при изменении числа опорных импульсов в цикле

Схема экспериментальной установки представлена на рис. 2 и по своей сути является интерферометром Маха-Цендера – упрощенным аналогом системы КРК НП. Фазовый шум схемы и его спектр представлены на рис. 3.

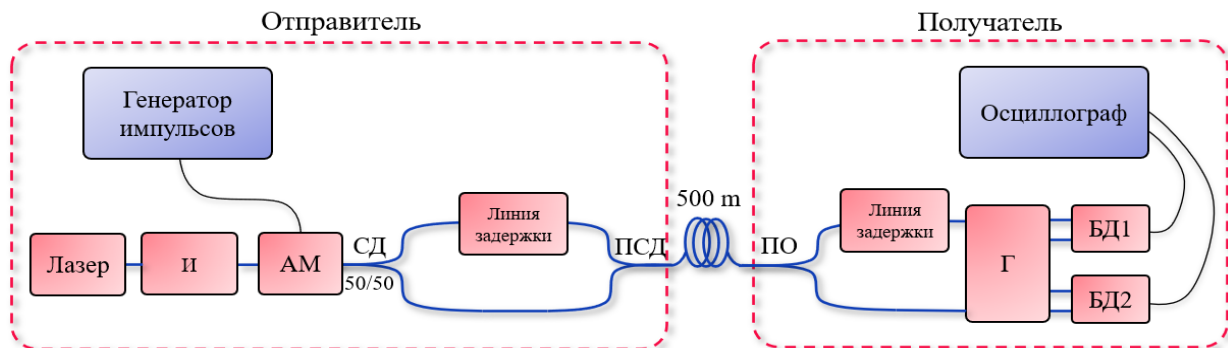


Рис. 2 Схема экспериментальной установки. И – оптический изолятор, АМ – амплитудный модулятор, СД – светоделитель 50/50, ПСД – поляризационный светоделитель, ПО – поляризационный объединитель, Г – 90-градусный гибрид, БД – балансные детекторы.

Проведено моделирование фазовой компенсации для различного числа сигнальных импульсов между двумя опорными импульсами, следовательно, различной частоты опорных импульсов f_R . Для этого некоторые из импульсов считаются опорными, а остальные импульсы между ними – сигнальными. Точность работы фазовой компенсации величиной V_{comp} , определяемой формулой:

$$V_{comp} = var(\theta - \hat{\theta}),$$

где θ – реальный фазовый сдвиг, $\hat{\theta}$ – измеренный фазовый сдвиг.

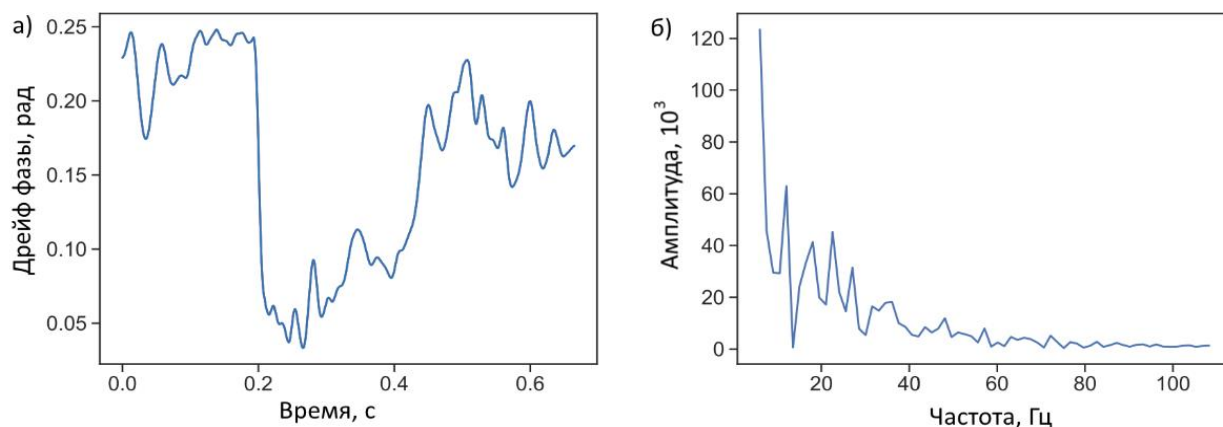


Рис. 3. а) График зависимости фазового шума от времени и б) спектр фазового шума

На рис. 4а представлена зависимость дисперсии ошибки фазовой компенсации V_{comp} для частот опорных импульсов до 150 Гц. Сравнивая данный график со спектром (рис. 3б), можно заметить схожесть данных зависимостей. Для наибольшей характерной частоты фазовых шумов фазовая ошибка уже является достаточно малой (порядка 10^{-5}). Однако, в данном случае и сами фазовые шумы достаточно малы из-за экспериментальных условий. На практике, фазовые шумы могут быть значительно выше, но ограничены $[-\pi/2, \pi/2]$. На рис. 4б можно наблюдать ошибку фазовой компенсации для более высоких частот опорных импульсов, которая стремительно убывает с ее ростом. Для сильных фазовых шумов частоту опорных импульсов можно брать на порядок или два больше, чем характерная максимальная частота фазовых шумов f_{phase} , для слабых фазовых шумов фазовая компенсация будет демонстрировать высокую точность даже при частоте опорных импульсов, сопоставимой характерной частоте фазовых шумов.

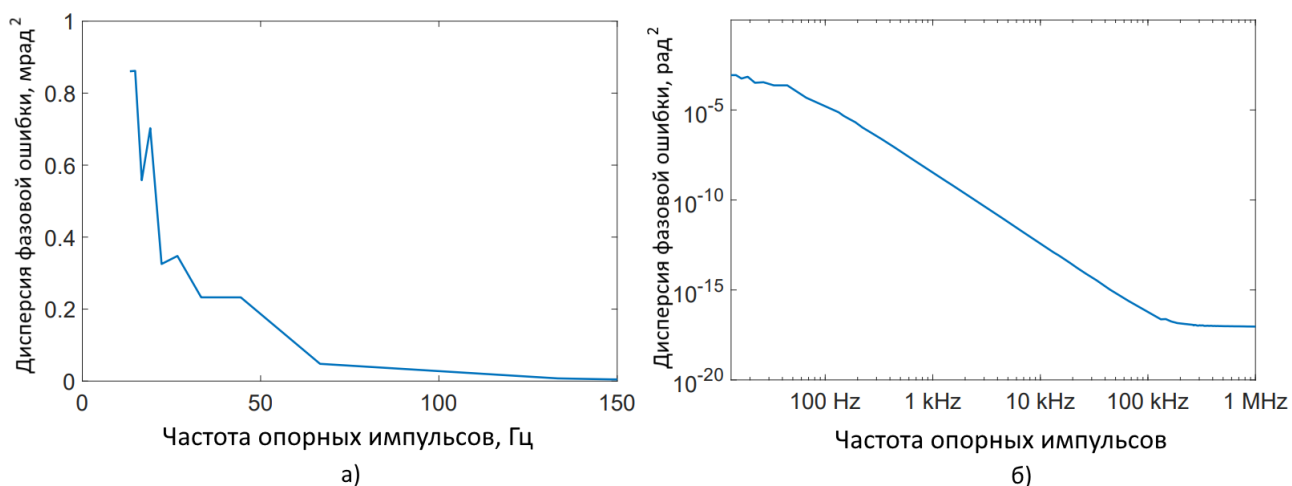


Рис. 4. График зависимости дисперсии ошибки фазовой компенсации V_{comp} от частоты опорных импульсов f_R а) до 150 Гц, б) до 1 МГц

С другой стороны, частота опорных импульсов должна выбираться таким образом, чтобы на один опорный импульс приходилось как можно больше сигнальных вплоть до соотношения 1:100, дальнейшее увеличение соотношения дает крайне малый прирост СГСЧ. Суммируя, для линейного алгоритма фазовой

компенсации оптимальная частота опорных импульсов при низкочастотных фазовых шумах ($f_{phase} \ll f_{rep}$) может быть оценена как

$$10f_{phase} < f_{ref}^{optimal} < 10^{-2}f_{rep}$$

Список используемых источников:

1. Goncharov R. et al. The Rationale for the Optimal Continuous-Variable Quantum Key Distribution Protocol //Optics. – 2022. – Т. 3. – №. 4. – С. 338-351.
2. Laudenbach F. et al. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations //Advanced Quantum Technologies. – 2018. – Т. 1. – №. 1. – С. 1800011
3. Hirano T. et al. Quantum cryptography using pulsed homodyne detection //Physical review A. – 2003. – Т. 68. – №. 4. – С. 042331.
4. Soh D. B. S. et al. Self-referenced continuous-variable quantum key distribution protocol //Physical Review X. – 2015. – Т. 5. – №. 4. – С. 041010.
5. Marie A., Alléaume R. Self-coherent phase reference sharing for continuous-variable quantum key distribution //Physical Review A. – 2017. – Т. 95. – №. 1. – С. 012316.
6. Zou M., Mao Y., Chen T. Y. Phase estimation using homodyne detection for continuous variable quantum key distribution //Journal of Applied Physics. – 2019. – Т. 126. – №. 6. – С. 063105.

Goncharov F., Nasedkin B., Pervushin B.

ITMO University

Increase of signal to reference ratio for phase compensation in continuous-variable quantum key distribution systems.

Continuous variables quantum key distribution (CV-QKD) systems are a promising direction for quantum communications. Coherent detection, which is the basis of CV-QKD protocols requires taking into consideration and compensating phase distortions. Phase compensation algorithms rely on using reference pulses for phase drift estimation and correcting signal pulses quadratures. The ratio of the number of reference pulses to that of the signal ones, affects the accuracy of the phase compensation algorithm. On the other hand, it influences the secure key rate.

Key words: *continuous variables quantum key distribution, phase noise, phase compensation, secure key rate.*

УДК 681.723.4
ГРНТИ 49.46.01

АНАЛИЗ МЕТОДОВ НЕСАНКЦИОНИРОВАННОГО ВОЗДЕЙСТВИЯ В PON

И. К. Григоренко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Высокая скорость передачи и помехоустойчивость делают оптоволокну наиболее оптимальной средой для передачи критически важной и конфиденциальной информации. Однако, существуют технические средства, с помощью которых возможен перехват информации с волоконно-оптических линий связи. Практичная и эффективная система мониторинга позволит защитить волоконно-оптическую линию связи от возможных угроз злоумышленников.

несанкционированный доступ, пассивная оптическая сеть (PON), прослушивание волокна, макроизгибы, микроизгибы

Классификация методов съема информации в ВОЛС

Дадим определение съему информации в ВОЛС. Под съёмом информации с ВОЛС подразумевается процесс выведения части оптического излучения с линии связи.

Методы съема информации с ВОЛС можно условно разделить на несколько категорий:

1. по способу регистрации – пассивные, активные и компенсационные;
2. по способу подсоединения – локальный и протяжённый;
3. по виду воздействия на ОВ – разрывный и безразрывный;
4. по принципу формирования канала утечки – нарушение полного внутреннего отражения, регистрация рассеянного излучения и параметрические методы регистрации проходящего излучения.

Суть пассивных методов основана на регистрации оптического излучения без физического воздействия на волокно. Такой метод трудно обнаружить, но он обладает низкой чувствительностью. К активным методам относятся: механический изгиб ОВ, оптическое туннелирование, подключение к ОВ фотоприемника с помощью направленного ответвителя и др. В активных методах съема информации оптическое волокно подвергается внешнему воздействию для вывода части оптического излучения, создавая тем самым возможность регистрировать выходящее излучение. Активные более чувствительны, однако факт несанкционированного доступа может быть легко установлен путём рефлектометрического контроля. Компенсационные методы, помимо внешнего воздействия, предполагают ввод в ОВ излучения, которое компенсирует потери мощности при выводе информационного сигнала. Они включают в себя преимущества первых двух групп, однако тяжело реализуемы на практике.

Для локального способа характерно подсоединение к ВОЛС в одной точке, в то время как в протяжённом съём информации производится с достаточно протяжённого участка линии связи.

При использовании разрывного способа подключения происходит временный разрыв линии, подсоединение к линии и ее восстановление. Безразрывной метод не подразумевает разрыва основной линии связи. Так как разрывной метод предусматривает временное нарушение работ линии связи, то для маскировки несанкционированного доступа параллельно с подключением злоумышленник может осуществлять дополнительные повреждения кабеля.

Вывод части оптического излучения приводит к нарушению принципа полного внутреннего отражения, что позволяет сформировать канал утечки информации. Чтобы увеличить расстояние между участками ретрансляции, необходимо обеспечить высокую мощность входного сигнала. Высокие мощности входного светового потока создают значительное рассеяние на ближайших к ретрансляторам отрезках сети, что также дает возможность создания каналов утечки информации. Принцип параметрического метода регистрации проходящего излучения заключается в следующем. Оптическое излучение вызывает изменение свойств оптического волокна при прохождении через него. В зависимости от интенсивности световых импульсов модуляцию свойств оптического волокна можно регистрировать специальными высокочувствительными устройствами. В данном методе изменение параметров оптического волокна является основой для создания канала утечки информации. Существующая техника измерений позволяет регистрировать очень малые изменения свойств волокна. Так, использование спектроскопии потерь позволяет фиксировать незначительное изменение показателя поглощения, которое вызвано информационным потоком света [1].

Уязвимости в ВОЛС

В волоконно-оптических линиях связи средой передачи является оптоволокно, где информация распространяется в виде оптического излучения, модулированного информационным электрическим сигналом. Наиболее уязвимыми местами утечки информации являются участки, расположенные за пределами контролируемой зоны, где злоумышленник может применить любые средства съема информации. Необходимым условием для перехвата является прямой доступ к оптическому волокну. Получая доступ к оптическому волокну, нарушитель может выводить часть оптического излучения в зависимости от типа воздействия на ОВ [2].

Волоконно-оптический ответитель-прищепка *FOD-5503* обеспечивает двунаправленное подключение к одномодовому волокну в защитном покрытии диаметром 250 мкм без его разрыва (рис. 1).

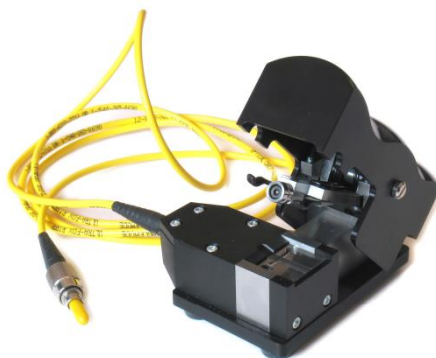


Рис. 1. Внешний вид FOD-5503

При вносимых потерях устройством *FOD-5503* около 2-3 дБ, удается вывести около 1% мощности сигнала, что уже дает возможность регистрировать оптическое излучение.

Макроизгибы и микроизгибы

Основным способом съёма информации с ВОЛС является активный локальный безразрывный метод съёма за счёт нарушения принципа полного внутреннего отражения на изгибе волокна.

Существуют два типа изгибов, вызывающих потери: макроизгибы и микроизгибы. Для макроизгиба волоконно-оптический кабель установлен с изгибом, радиус которого меньше минимально допустимого радиуса изгиба, но значительно больше радиуса одиночного волокна. Свет будет падать на границу раздела «сердцевина–оболочка» под углом меньше критического и пропадать в оболочке (рис. 2).

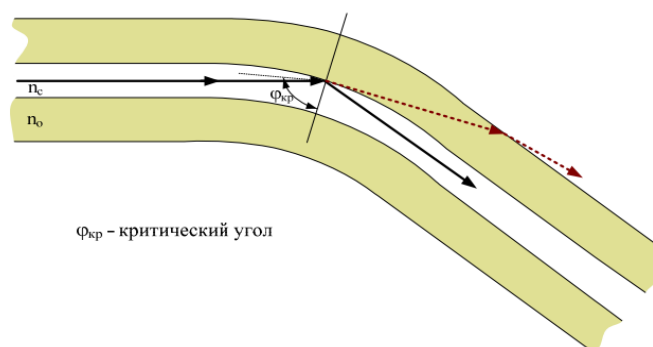


Рис. 2. Макроизгиб

Во втором типе микроизгиб принимает форму очень маленького резкого изгиба (излома) волокна. Для микроизгибов радиус изгиба сопоставим с радиусом одиночного волокна. Подобно случаю с макроизгибами, световой луч будет падать под углом меньше критического и попадать в оболочку (рис. 3).

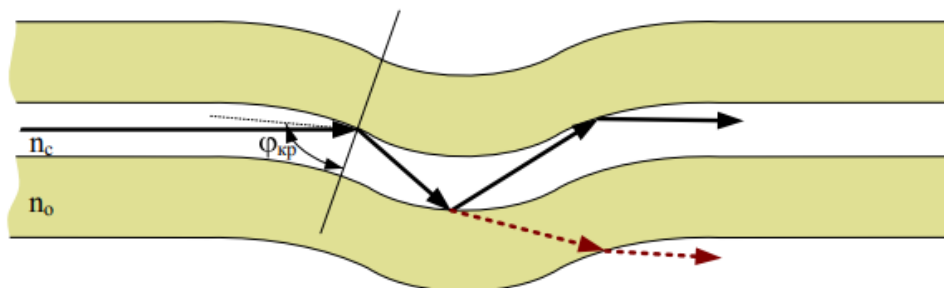


Рис. 3. Микроизгиб

Эксперимент

Эксперимент включает в себя съем оптического излучения при передаче потокового видео через оптический *Ethernet* с одного компьютера на другой (рис. 4).

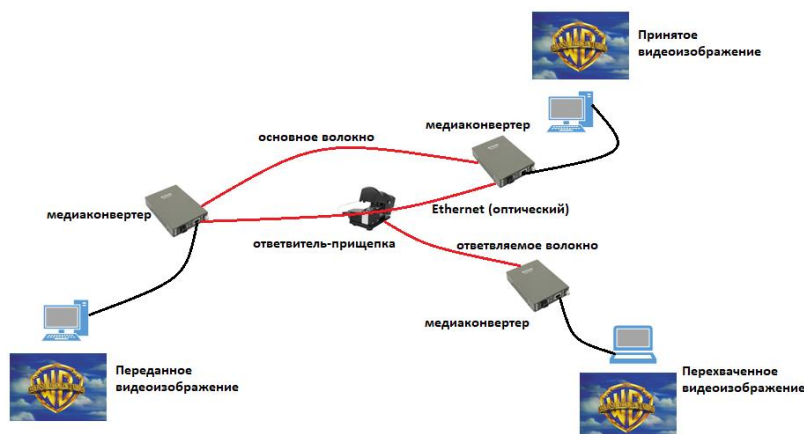


Рис. 4. Экспериментальная схема установки

Для потоковой передачи и воспроизведения видео было использовано программное обеспечение *VLC*, анализатор протоколов *Wireshark* для захвата пакетов и *Chaosreader* для восстановления видеоклипов из захваченных пакетов. В качестве устройства перехватчика использовался ответвитель-прищепка *FOD-5503*. С помощью этого устройства создается макроизгиб и ответвляется сигнал на однонаправленный медиаконвертер *Ethernet*, после чего кадры *Ethernet* обрабатываются на третьем ПК для восстановления копии исходных видеокадров. *Wireshark* преобразует кадры *Ethernet* и предоставляет такую информацию, как *MAC*-адреса отправителя и получателя. Он также обрабатывает полезную нагрузку кадра *Ethernet* и получает от него *IP*-пакеты. Информация, полученная из пакетов, включает *IP*-адреса, сообщения протокола сигнализации и биты полезной нагрузки. Захваченные таким образом пакеты сохраняются в файле формата **.pcap* (формат пакета перехваченных данных). Затем обрабатываем файл программным обеспечением *Chaosreader*, которое восстанавливает исходные файлы и создает индекс восстановленных файлов. При открытии этого файла в программном обеспечении *VLC* воспроизводится захваченная часть видеопотока [3].

Помимо воспроизведения видео, данная экспериментальная установка может использоваться для выполнения ряда операций по подслушиванию, таких как атака на IP-адреса, кража пароля, прослушивание VoIP-вызовов и восстановление электронной почты с использованием различных программ.

Заключение

В статье была приведена классификация методов съема информации с ВОЛС, а также продемонстрирован эксперимент, позволяющий захватить часть оптического излучения для восстановления информации злоумышленником.

Список используемых источников:

1. А.В. Горбунов. Волоконно-оптический ответвитель-прищепка для съема информации в волоконно-оптических линиях связи: учеб. пособие. Таганрог: ТТИ ЮФУ, 2009. 54 с.
2. В.В. Шубин. Информационная безопасность волоконно-оптических систем: монография: Саров РФЯЦ-ВНИИЭФ, 2015. 43 с.
3. Zafar M. Iqbal, H. Fathallah, Nasser-Eddine Rikli. Optical fiber tapping: Methods and precautions [Paper]. – Pakistan: PSATRI Communication and Networks Research Lab, 2011.

Grigorenko I.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of unauthorized exposure methods in PON.

High transmission speed and noise immunity make fiber the most optimal medium for the transmission of critical and confidential information. However, there are technical means by which it is possible to intercept information from fiber-optic communication lines. A practical and effective monitoring system will protect the fiber-optic communication line from possible threats from intruders.

Key words: *unauthorized access, passive optical network (PON), fiber eavesdropping, macrobends, microbends.*

УДК 621.39
ГРНТИ 49.27.31

ЛАБОРАТОРНАЯ РАБОТА «ИССЛЕДОВАНИЕ СПЕКТРАЛЬНЫХ ХАРАКТЕРИСТИК ОПТИЧЕСКОГО ИЗЛУЧЕНИЯ ИСТОЧНИКОВ И ПЕРЕДАЮЩИХ ОПТИЧЕСКИХ МОДУЛЕЙ»

Д. В. Дмитриева, А. Э. Цыганок

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С каждым годом растет потребление интернет трафика - требуются большие скорости, объемы, и оптические линии связи перекрывают данную потребность, однако повышаются требования к передающему и принимающему оборудованию, в особенности к качеству самого оптического сигнала. Важной характеристикой оптического сигнала является его спектр. Данная лабораторная работа посвящена исследованию спектральных характеристик источников излучения и передатчиков.

волоконно-оптические линии связи, источники излучения, передающие оптические модули, анализатор спектра, спектрограмма, измерение спектральных характеристик излучения

Современный этап развития систем связи характеризуется постоянным ростом объемов и скорости передаваемой информации, что предъявляет повышенные требования к широкополосности среды передачи. Наибольшей широкополосностью среди всех направляющих систем обладают оптические волокна (ОВ), достоинства которых в наибольшей степени проявляются в системах со спектральным уплотнением, использующих технологию OTN. Поэтому в учебном процессе СПбГУТ изучению этих систем уделяется повышенное внимание.

Основными компонентами волоконно-оптической системы связи с OTN являются: приёмопередающее, каналообразующее и усилительное оборудование, которое осваивается студентами в рамках лабораторного практикума. В данном докладе представлена новая лабораторная работа, посвященная исследованию спектральных характеристик источников излучения (ИИ) и передающих устройств.

Лабораторная установка, которая изображена на рис. 1, включает следующее оборудование:

1. Набор ИИ – светоизлучающие диоды, многомодовые лазеры Фабри-Перо, одномодовые лазеры с распределенной обратной связью (DFB)
2. Набор трансиверов SFP и SFP+ с модуляциями ASK и PSK (рис. 2)
3. DWDM транспондер TT-10EP из состава платформы «Волга» (рис. 3).
4. Измерительные приборы – анализатор оптического спектра AQ6370D YOKOGAWA (рис. 4) и измеритель оптической мощности (рис. 5).

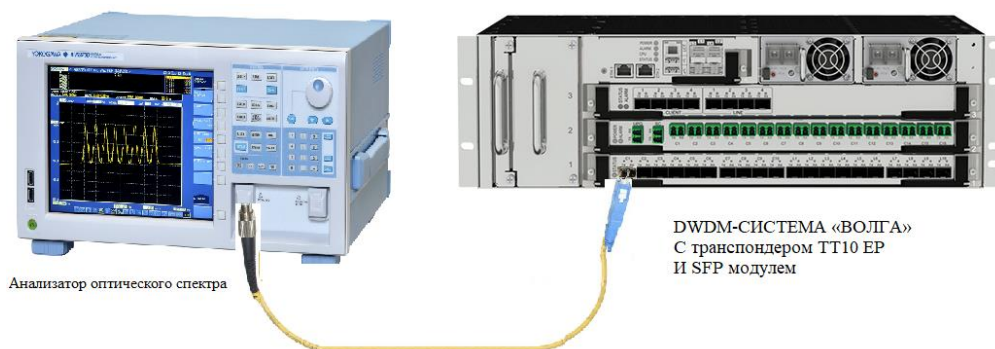


Рис. 1. Схема лабораторной установки



Рис. 2. SFP модуль. Вид внешний



Рис. 3. Транспондер ТТ-10EP. Вид внешний



Рис. 4. Анализатор оптического спектра AQ6370D YOKOGAWA. Вид внешний



Рис. 5. Измеритель оптической мощности. Вид внешний

В первой части лабораторной работы студенты исследуют спектральные характеристики светодиодных и лазерных ИИ. Выполнение работы начинается с ознакомления с принципами работы и конструкциями источников. На рис. 6 представлена конструкция стабилизированного по мощности лазерного диода (LD). Диод имеет две системы стабилизации мощности: схему управления температурой с основным измерительным элементом термистором и схему управления средней мощностью с основным измерительным элементом фотодиодом (PD). Для защиты от обратных отражений на выходе лазерного диода установлен изолятор.

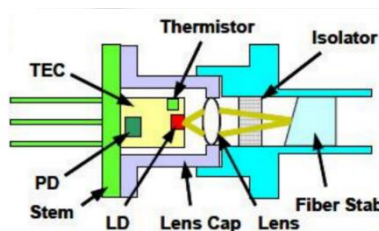


Рис. 6. Конструкция стабилизированного по мощности лазерного диода

На рис. 7 представлен спектр перестраиваемого DFB лазера и в таблице 1 приведены его измеренные параметры на длине волны 1551,7, что соответствует 32 каналу. Модуль может работать во всём DWDM диапазоне.

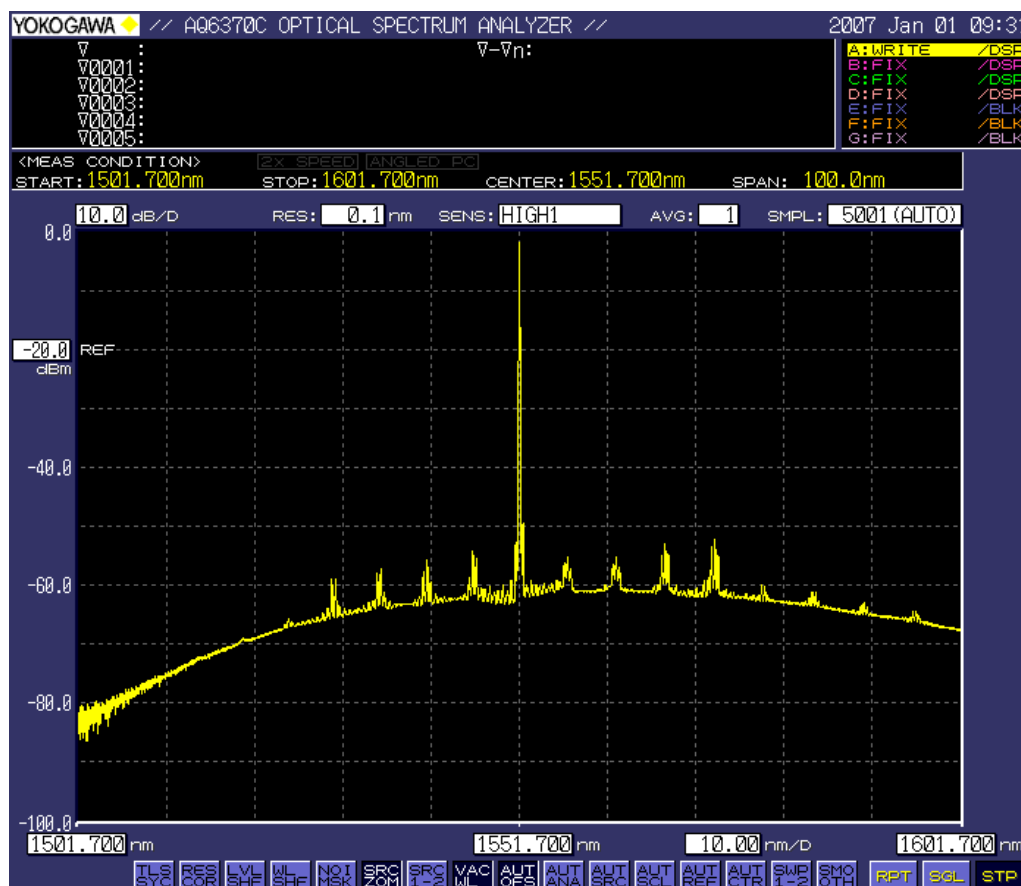


Рис. 7. Спектрограмма перестраиваемого модуля

ТАБЛИЦА 1. Измеренные параметры модуля

Мощность, дБм	Спектральный интервал между перестраиваемыми каналами, нм	Пиковая мощность в канале, дБм	Ширина спектра излучения канала, нм	Коэффициент подавления боковых мод, дБ	Центральная длина волны канала, нм
2,25	5,5	-0,2	0,23	-55	1551,7

Из рис. 7 видно, что при перестроении по каналам данный трансивер не полностью подавляет излучение на соседних 8 каналах, однако остальные каналы подавлены достаточно сильно.

Вторая часть работы посвящена исследованию передающих устройств. На рис. 8 представлен спектр излучения передающего оптического модуля, входящего в состав трансивера производителя Ne.Photonics модели PT7420-62-2W+, а в табл. 2 приведены его измеренные параметры. Трансивер работает на длине волны 1310 нм со скоростью 2.5 Гбит/с, используется модуляция ASK NRZ. Данный модуль предназначен для CWDM сетей.

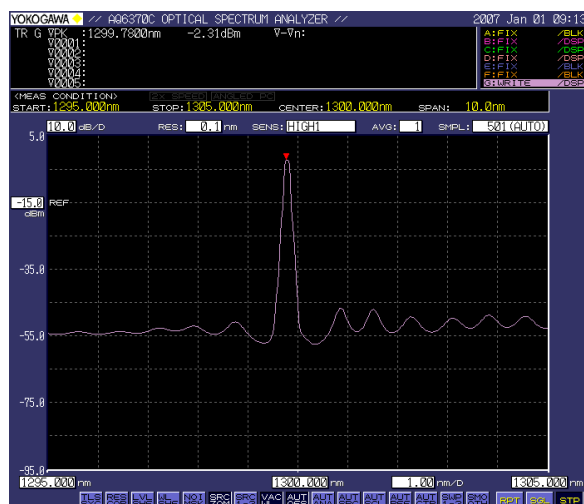


Рис. 8. Спектрограмма трансивера PT7420-62-2W+

ТАБЛИЦА 2. Измеренные параметры модуля

Мощность, дБм	Пиковая мощность в канале, дБм	Ширина спектра излучения канала, нм	Центральная длина волны канала, нм
-0,505	-2,307	0,44	1295,78

На рис. 9 представлена спектрограмма передающего оптического модуля, входящего в состав трансивера модели SFPD+MR-80-F, а в таблице 2 приведены его измеренные параметры. Трансивер работает на длине волны 1551.7 нм, что соответствует 32 каналу DWDM. Скорость данного трансивера составляет 10 Гбит/с, используется модуляция ASK NRZ. Данный модуль предназначен для DWDM сетей.

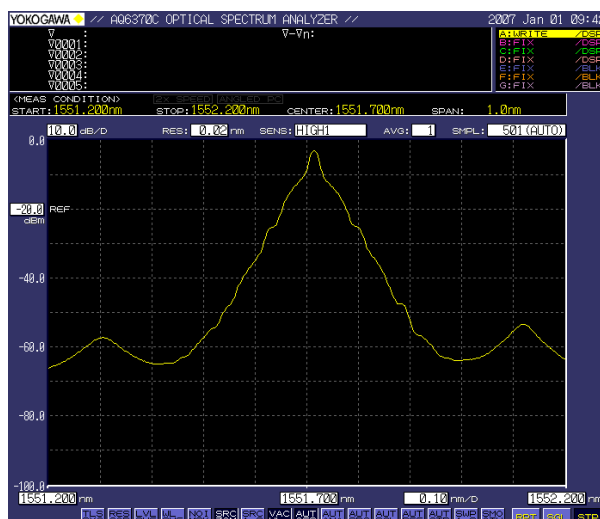


Рис. 9. Спектрограмма трансивера SFPD+MR-80-F

ТАБЛИЦА 3. Измеренные параметры модуля

Мощность, дБм	Пиковая мощность в канале, дБм	Ширина спектра излучения канала, нм	Центральная длина волны канала, нм
-0,326	-2,964	0,464	1551,7

К предложенной лабораторной работе были подготовлены методические указания, включающие теоретические сведения, описания экспериментально-измерительного оборудования, задания для выполнения, пример оформления отчета и контрольные вопросы для самопроверки.

Лабораторная работа будет внедрена в учебный процесс базовой кафедры ВТС DWDM и кафедры Фотоники и линии связи СПбГУТ.

Список используемых источников:

1. Трешиков В. Н., Листвин В. Н. DWDM системы. М.: Техносфера, 2021. 420 с.
2. Былина М. С., Глаголев С. Ф. Методы и приборы для оптических измерений в инфокоммуникациях. Часть 2. Спектральные измерения. Измерения параметров волоконно-оптических линейных трактов: учебное пособие. СПб.: СПбГУТ, 2021. 78 с.

Dmitrieva D., Tsyganok A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Laboratory work "Investigation of the spectral characteristics of optical radiation sources and transmitting optical modules".

Every year the consumption of Internet traffic is growing - high speeds, volumes are required, and optical communication lines cover this need, however, the requirements for transmitting and receiving equipment, especially for the quality of the optical signal itself, are increasing. An important characteristic of an optical signal is its spectrum. This laboratory work is devoted to the study of the spectral characteristics of radiation sources and transmitters.

Key words: fiber-optic communication lines, radiation sources, transmitting optical modules, spectrum analyzer, spectrogram, measurement of spectral characteristics of radiation.

УДК 535.015
ГРНТИ 49.46.33

РАЗРАБОТКА СИСТЕМЫ КОНТРОЛЯ РАДИОАКТИВНОЙ ОБСТАНОВКИ НА ОСНОВЕ ВОЛОКОННО-ОПТИЧЕСКИХ ДАТЧИКОВ ДЛЯ ВОДНЫХ БАССЕЙНОВ АТОМНЫХ ЭЛЕКТРИЧЕСКИХ СТАНЦИЙ

Д. С. Дмитриева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обоснована необходимость разработки системы дистанционного контроля радиоактивной обстановки на основе волоконно-оптических датчиков для водных бассейнов АЭС. Предложена новая конструкция волоконно-оптического датчика, определены его функциональные возможности. Представлены результаты экспериментальных исследований.

волоконно-оптический датчик, экспозиционная доза, волоконно-оптическая линия связи, лазерное излучение, гамма-излучение, брызгальные бассейны

На сегодняшний день количество использования радиоактивных материалов в различных областях промышленности только возрастает, увеличивается число атомных электрических станций [1]. Несмотря на большое количество защитных экранов и перекрытий, нередко случаи радиоактивных выбросов, последствия от которых невозможно устранить еще долгое время. Помимо самих реакторов, опасность представляют брызгальные бассейны, применяемые для непрерывного охлаждения оборудования АЭС. В случае утечки так же нередко становятся источниками выбросов в атмосферу из-за попадания в воду жидких радиоактивных отходов. Из-за наличия системы сопел, часть капель, содержащих в себе радионуклиды, разносятся ветром за пределы брызгальных бассейнов. Кроме того, естественное испарение воды с поверхности бассейна также приводит к изменению радиационной обстановки в атмосфере. Именно поэтому возможности контроля уровня радиации в водных бассейнах атомных электрических станций уделяется большое внимание.

Наибольший интерес уделяется возможности дистанционного контроля радиационной обстановки в водных бассейнах АЭС. Проведение контроля мощности радиоактивного излучения связано с рядом сложностей. Такой контроль должен проводиться непрерывно в режиме реального времени. Более того, в ряде случаев необходимо организовать контроль в автоматическом режиме на расстоянии в несколько километров от центра мониторинга. С подобной задачей не справляется большинство дозиметрических приборов. Приборы часто зашкаливают из-за накопления радиации, а системы связи, которые используются для передачи информации об уровне радиации в центр мониторинга, выходят из строя [2]. Обслуживание таких систем контроля является достаточно трудным так как радиация накапливается на корпусах приборов и их функциональных узлах, что представляет большую опасность для человека.

Одним из способов реализации непрерывного контроля уровня радиации является применение волоконно-оптических датчиков. Однако датчики, разработанные на данный момент, не способны проводить измерения при больших значениях экспозиционной дозы облучения из-за длительной естественной релаксации оптического волокна. Так как экспозиционная доза облучения в зоне контроля может изменяться на несколько порядков за достаточно короткий промежуток времени, естественная релаксация оптического волокна, применяемого в датчиках, может составить порядка 10^6 с и более. Более того, в существующих на данный момент волоконно-оптических датчиках невозможно использовать более мощные источники излучения (датчики на основе поляризации лазерного излучения под воздействием γ -излучения проводят измерения на небольших мощностях – порядка 5 мВт). Применение более мощного излучения не представляется возможным, так как есть риск повреждения фоточувствительного слоя фотоприемного модуля. Таким образом, разработка системы контроля радиационной обстановки на основе волоконно-оптических датчиков, способной выдерживать высокие уровни экспозиционной дозы, крайне актуальна.

Полученные ранее результаты [3] позволяют предложить в качестве основы системы контроля радиоактивной обстановки для водных бассейнов атомных электрических станций использовать следующую конструкцию волоконно-оптического датчика. Оптическое волокно длиной в 200 м с сердцевиной из $SiO_2 - GeO_2$ с процентом легирования 20%, которое подключается к оптическому волокну из чистого кварца через оптические разъемы. Для ускорения процесса естественной релаксации волокна в данной конструкции применяется разработанный ранее метод по контролю образования E' -центров для магистральных ВОЛС. Для проверки работоспособности предложенной конструкции было проведено исследование скорости восстановления свойств оптического волокна при воздействии γ -излучения мощностью 100 Гр. В данном исследовании применялось импульсное лазерное излучения с длиной волны $\lambda=1310$ нм, длительностью 0.1 в течение 10 с. Измерения проводились при различных мощностях лазерного излучения. Результаты исследований представлены на рис. 1 и рис. 2.

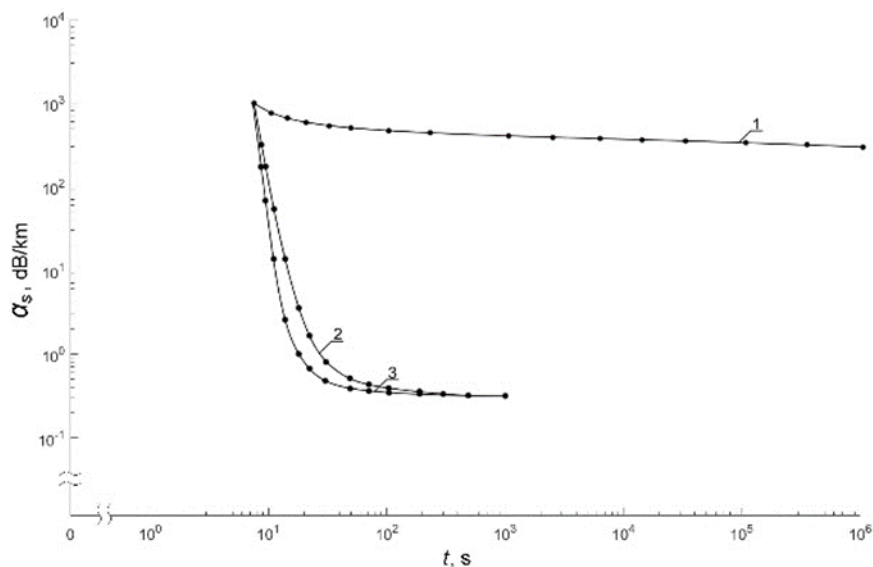


Рис. 1. Зависимость изменения потерь α_s от времени t на длине волны $\lambda = 1550$ нм для одномодового волокна сердцевина $SiO_2 - GeO_2$ (концентрация легирования 10.0 %) с полимерной оболочкой при $T = 294.3$ К. Графикам 1, 2 и 3 соответствует различная мощность импульсного лазерного излучения в мВт: 0; 40; 80.

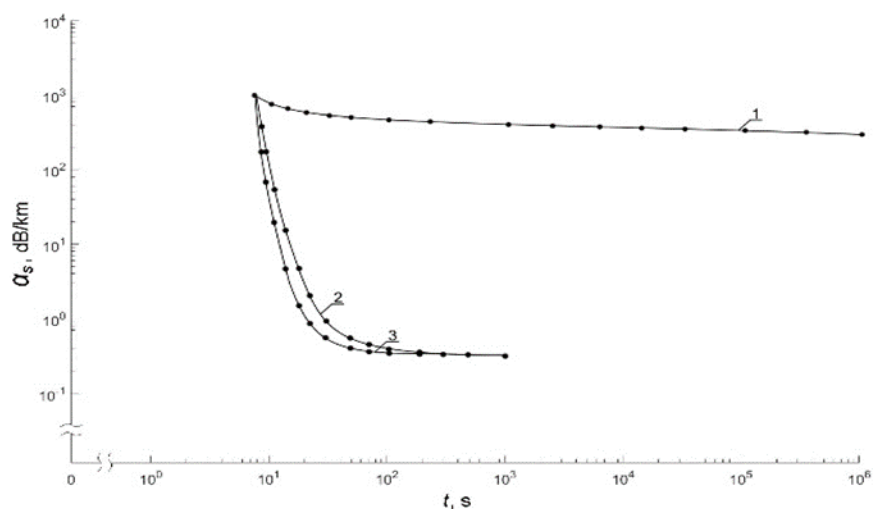


Рис. 2. Зависимость изменения потерь α_s от времени t на длине волны $\lambda = 1550$ нм для одномодового волокна сердцевина $SiO_2 - GeO_2$ (концентрация легирования 10.0 %) с полимерной оболочкой при $T = 21.3$ °С. Графикам 1, 2 и 3 соответствует различная мощность непрерывного лазерного излучения в мВт: 0; 20; 40.

Анализ полученных результатов подтвердил возможность увеличения скорости релаксации при использовании дополнительного лазерного излучения. Оптические свойства волокна восстанавливаются за время порядка 10с. Более того, в результате проведения исследования было установлено, что восстановление оптического волокна быстрее протекает при использовании импульсного лазерного излучения, а не непрерывного.

Полученные результаты показали надежную работу разработанного датчика в непрерывном режиме. Его использование позволит осуществлять

контроль дозы облучения от 0,1 до 1000 Гр в реальном времени в водных бассейнах АЭС.

Кроме того, у разработанного волоконно-оптического датчика для дистанционного контроля радиационной обстановки присутствует одна особенность, отличающая его от ранее применяемых. При определенном значении экспозиционной дозы облучения и мощности дополнительного лазерного излучения наблюдается равновесие между двумя процессами: образованием центров окраски и их релаксацией. Значение потерь a_s за определенный промежуток времени увеличивается менее чем на 1% от своего исходного значения. В таком случае волоконно-оптический датчик для контроля радиационной обстановки будет находиться в режиме ожидания радиоактивного выброса. При этом влияние фонового γ -излучения, наличие которого характерно для бассейнов атомных электрических станций, компенсируется.

Список используемых источников:

1. Davydov V.V., Myazin N.S. and Kiryukhin A.V. Nuclear-Magnetic Flowmeter-Relaxometers for Monitoring Coolant and Feedwater Flow and Status in Npp // Atomic Energy. 2020. Vol 127(5). P. 274–279.
2. Khan P.W., Abbas K., Shaiba H., Abuarqoub A. and Khayyat M. Energy efficient computation offloading mechanism in multi-server mobile edge computing—An integer linear optimization approach // Electronics. 2020. Vol. 9(6). P. 1–20.
3. Dmitrieva, D., Pilipova, V., Andreeva, E., Dudkin, V., Davydov, V. Method for determination of negative influence to γ - radiation on fiber optic information transmission systems // Proceedings of ITNT 2020 - 6th IEEE International Conference on Information Technology and Nanotechnology. 2020. Vol. 9253348. P. 13-17.

Dmitrieva D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Development of the radiation situation monitoring system based on fiber-optic sensors for pools of nuclear power plants.

The necessity of development of the remote monitoring system of the radiation situation based on fiber-optic sensors for pools of nuclear power plants is substantiated. New method of building of communication line with fiber-optic sensor for controlling exposure dose of radioactive radiation in the large range of changes (several orders of magnitude) in remote mode is suggested. The design of sensor to provide measurements for long distance (more than 10 km from the location of the monitoring center) is developed. Functional capabilities of the fiber-optic sensor are identified. Experimental results are presented.

Key words: *γ -radiation, radiation exposure dose, fiber-optic sensor, laser radiation.*

УДК 621.39
ГРНТИ 49.44.33

ОПТИЧЕСКИЕ ПОЛЯРИЗАЦИОННО-НЕЗАВИСИМЫЕ ИЗОЛЯТОРЫ ДЛЯ СПЕЦИАЛЬНЫХ ПРИМЕНЕНИЙ

А. С. Дюбов, Л. И. Калашникова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа оптических изоляторов основана на магнитооптическом эффекте Фарадея. Изоляторы обеспечивают одностороннее прохождение оптического излучения. Изоляторы применяются для защиты лазерных источников от отраженных сигналов, встречаются в конструкциях оптических волоконных и полупроводниковых усилителей, а так же в измерительных приборах. В докладе рассмотрены специальные типы объемных изоляторов выполненных на дискретных элементах и обеспечивающих поляризационную независимость для проходящих через них сигналов. Особенностью рассматриваемых изоляторов является возможность работы с излучениями высокой интенсивности, при обеспечении высокой изоляции и низких потерь в прямом направлении. Приводятся схемы прохождения лучей, наиболее распространенных конструкция, даются характеристики применяемых материалов в зависимости от диапазона рабочих длин волн.

оптический изолятор, двулучепреломляющий кристалл, полуволновая пластина, фарадеевский ротор, линза, поляризация, вносимые потери, изоляция, коэффициент отражения

Оптические изоляторы используются для защиты от воздействия случайных внешних отражений. Источниками отражений могут являться места соединения оптических волокон или поверхности объемных дискретных элементов оптических приборов. Нежелательные отражения, попавшие в резонатор лазерных диодов, могут нарушить их работу, привести к расширению спектра излучения, нарушению когерентности и нестабильности уровня излучаемого сигнала.

Различают несколько типов изоляторов: полностью волоконно-оптические, интегрально-оптические, гибридного типа. В данном докладе внимание уделено поляризационно-независимым объемным изоляторам, выполненным на дискретных элементах. Такие изоляторы предназначены для работы со значительными уровнями оптической мощности. К ним предъявляются требования минимального вносимого затухания и высокой степени изоляции [1–3].

В основе работы изоляторов данного типа лежат эффекты двойного лучепреломления в кристаллах и магнитооптического эффекта Фарадея.

Конструкция, схемы прохождения лучей и принцип работы поляризационно-независимого изолятора приведены на рис. 1 и 2.

Оптическая схема состоит из двух коллимирующих линз, двулучепреломляющих элементов и ячейки Фарадея.

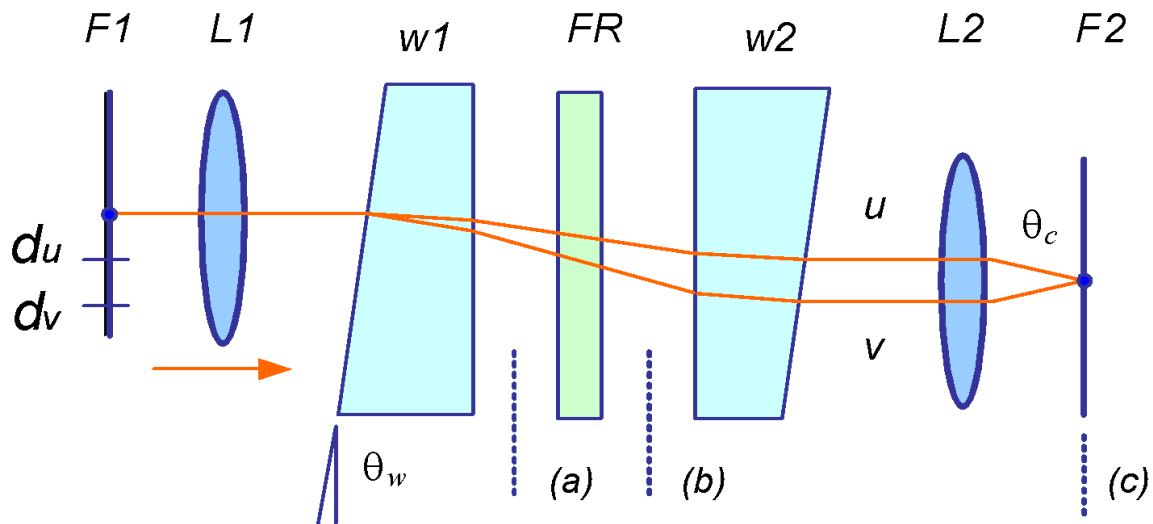


Рис. 1. Схема прохождения лучей в прямом направлении в поляризации-независимом изоляторе

Двулучепреломляющие элементы выполняются из анизотропных одноосных кристаллов. При распространении световой волны под углом к оптической оси кристалла происходит раздвоение входного излучения на ортогонально поляризованные компоненты (обыкновенный и необыкновенный световой луч), происходит пространственное смещение лучей (рис. 1).

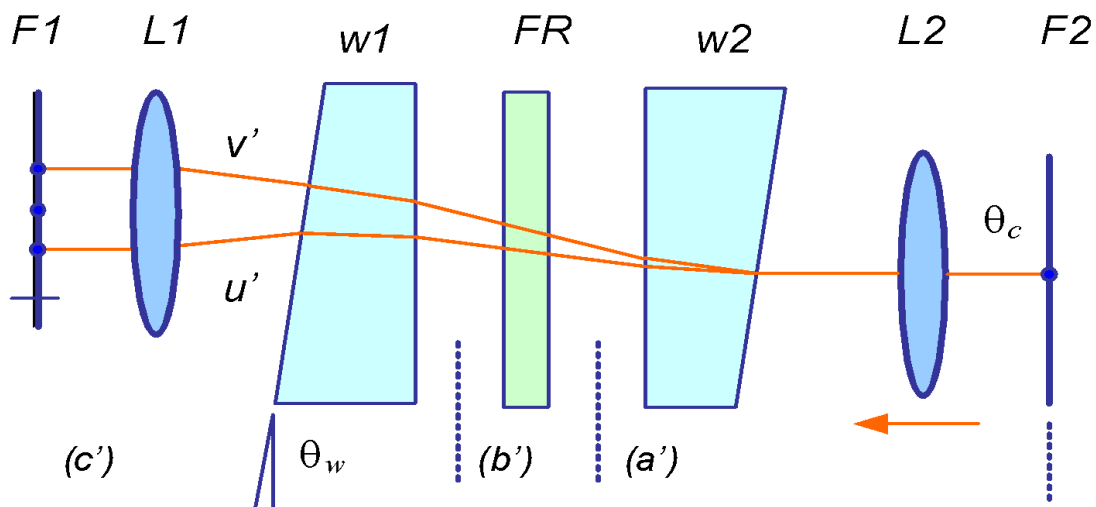


Рис. 2. Схема прохождения лучей в обратном направлении в поляризации-независимом изоляторе

Невзаимный поворот плоскости поляризации в ячейке Фарадея используется для возникновения изоляции при обратном распространении отраженного сигнала (рис. 2) [4].

Характеристик оптического изолятора во многом определяются выбором оптических материалов, на котором и основана работа этого устройства. Распространенными анизотропными кристаллами являются: ванадата иттрия (YVO_4), рутил (TiO_2), исландский шпат ($CaCO_3$), ниобат лития ($LiNbO_3$). Из

перечисленных кристаллов, самым большим двулучепреломлением обладает кристалл рутила. Ванадат иттрия обладает широким диапазоном прозрачности, хорошей температурной стабильностью, а также физическими и механическими свойствами.

Для выполнения ячейки Фарадея могут быть применены боро-германатное стекла с высоким содержанием оксида тербия или оптические керамики, совмещающие достоинства стекол и кристаллов и обладающие большой постоянной Верде [5].

Для специальные применения с целью увеличения степени изоляции в широком диапазоне рабочих длин волн и температур могут потребоваться две или более ступеней. На рис. 3 и 4 приведены схемы прямого и обратного хода лучей двухкаскадного изолятора отклоняющего типа.

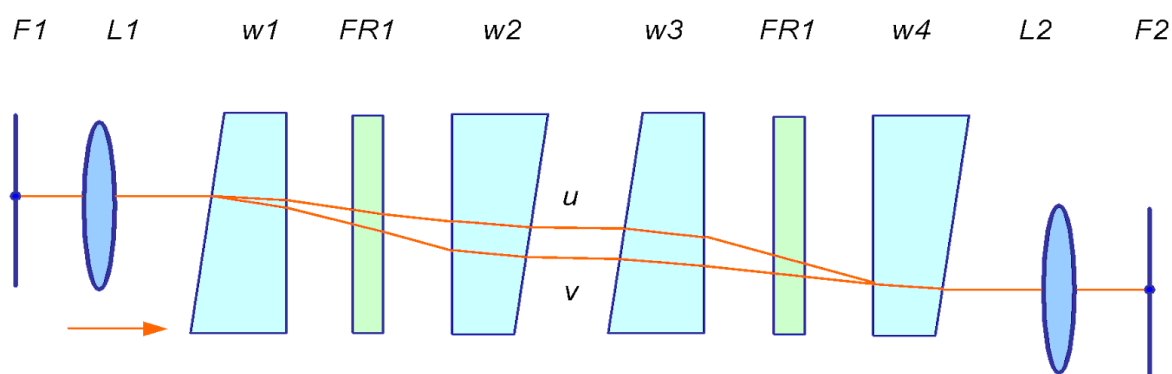


Рис. 3. Схема прохождения лучей в прямом направлении в двухступенчатом изоляторе

Сведение лучей при распространении излучения в прямом направлении выполняется второй парой клиньев ($w3$ и $w4$) повернутой на 90 градусов относительно первой пары ($w1$ и $w2$). Такое решение снижает поляризационную чувствительность изолятора и снижает дифференциальную групповую задержку.

По сравнению с одноступенчатым изолятором, двухступенчатый обеспечивает большее разведение лучей при распространении излучения в обратном направлении (рис. 4) [4].

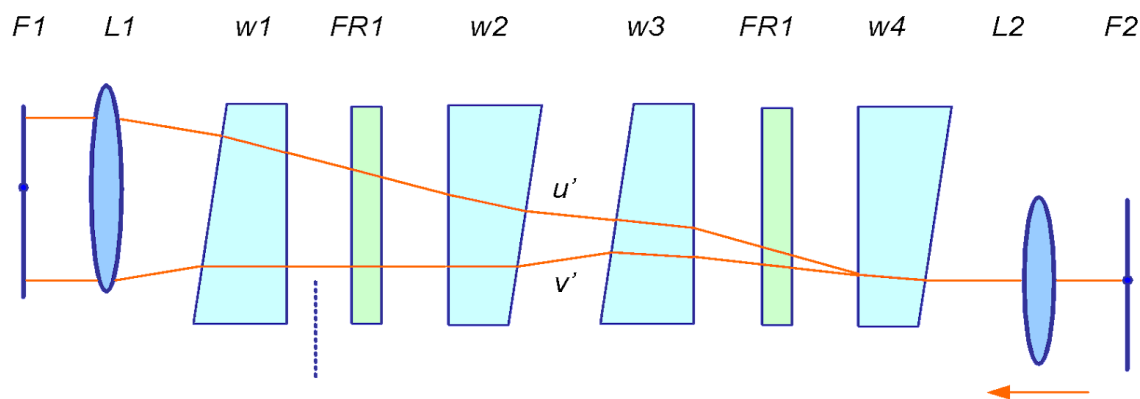


Рис. 4. Схема прохождения лучей в обратном направлении в двухступенчатом изоляторе

Выбор схемы построения изолятора и размеры объемных элементов конструкции определяется областью применения изолятора, спектру рабочих длин волн, требованиями к степени изоляции, диапазону рабочих температурам и прочим.

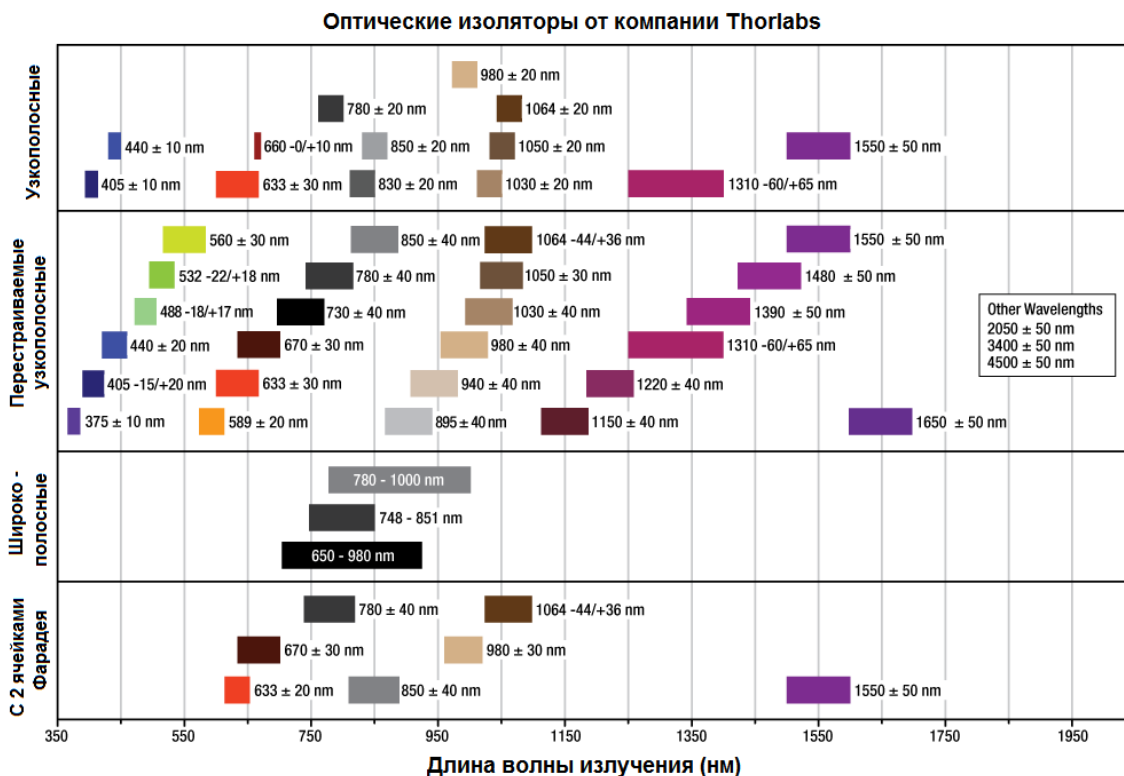


Рис. 5 Разнообразие оптических изоляторов, представленных на рынке

Развитие сфер применения оптических технологий, достижения в области оптических материалов и методов производства привели к появлению оптических изоляторов различных типов. Примером разнообразия коммерчески доступных исполнений может служить график из каталога компании «Thorlabs», приведенный на рис. 5.

В настоящий момент коммерчески доступны фиксированные и перестраиваемые изоляторы, узкополосные и широкополосные поляризационно-независимые и поляризационно-зависимые оптические изоляторы, выполненные на основе ячейки Фарадея, для работы в спектральном диапазоне от 400 до 4500 нм. Проведенный в ходе работы анализ публикаций свидетельствует о продолжающемся совершенствовании конструкций и технологий изготовления оптических изоляторов. [6]

Список используемых источников:

1. Chang K.W., Sorin W.V. Polarization independent isolator using spatial walkoff polarizers. // IEEE Photonics Technology Letters. 1989. V. 1. P. 68–70.
2. Shiraishi K., Kawakami S. Cascaded optical isolator configuration having high-isolation characteristics over a wide temperature and wavelength range // Optics Letters. 1987. V. 12. № 7. P. 462–464.

3. Миронов С. А. Расчет характеристик поляризационно-независимого оптического изолятора для волоконно-оптических линий связи. // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. № 5(63). 2009 С. 21 – 29.

4. Damask J. N. Polarization Optics in Telecommunications. New York. : Springer, 2005.

5. Ярив А., Юх П. Оптические волны в кристаллах: Пер. с англ. – М.: Мир, 1987.

6. Оптические изоляторы от Thorlabs / Азимут фотоник [Электронный ресурс] URL: <https://azimp.ru/articles/tech/38763/> (дата обращения 10.11.2022).

Diubov A., Kalashnikova L.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Optical polarization-insensitive isolators for special purposes.

The operation of optical isolators is based on the magneto-optical Faraday effect. Isolators provide one-way passage of optical radiation. Isolators are used to protect laser sources from reflected signals; they are found in the designs of optical fiber and semiconductor amplifiers, as well as in measuring instruments. The report discusses special types of bulk isolators made on discrete elements and providing polarization independence for signals passing through them. A feature of the considered isolators is the ability to operate with high-intensity radiation, while providing high insulation and low losses in the forward direction. Schematic layouts of the passage of rays, most common designs are given, the characteristics of the materials used are given depending on the range of operating wavelengths.

Key words: optical isolator, birefringent crystal, half-wave plate, Faraday rotor, lens, polarization, insertion loss, isolation, reflection coefficient.

УДК 621.39
ГРНТИ 49.44.33

МОДЕЛИРОВАНИЕ РАБОТЫ ПЕРЕДАТЧИКА ОПТИЧЕСКОЙ СИСТЕМЫ СВЯЗИ

А. С. Дюбов, В. Э. Кузьмина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В докладе рассмотрена работа передатчиков волоконно-оптических систем связи, построенных на основе светоизлучающих и лазерных диодов с прямой и внешней модуляцией. Результаты моделирования показывают эффекты, связанные с ограниченным быстродействием полупроводниковых излучателей, и преимущества применения внешних модуляторов на основе интерферометра Маха–Цандера.

светоизлучающий диод, лазерный диод, модулятор, оптический передатчик, формат модуляции, глаз диаграмма, волоконно-оптическая система связи

Источником оптического сигнала в передатчиках большинства современных оптоволоконных систем связи служит лазерный диод. Структуры светоизлучающего и лазерного диодов, представляют собой р-п переход (рис. 1) и поэтому их электрические характеристики описываются аналогично р-п переходу [1-3].

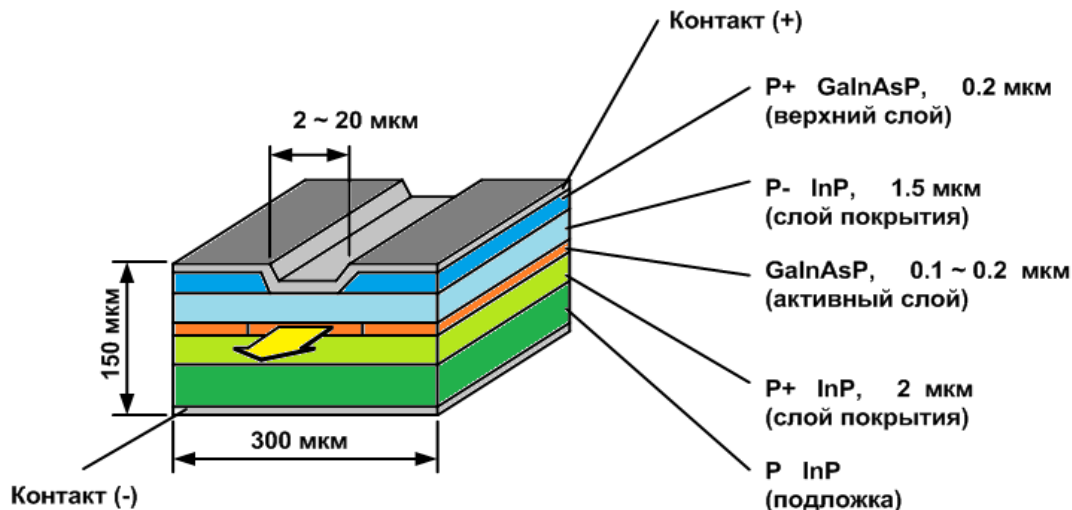


Рис. 1. Структура лазерного диода

На рис. 2 приведена схема моделирования передатчика на основе светоизлучающего диода с прямой модуляцией. Схема состоит из генератора битовой последовательности, формирователя кода (NRZ), исследуемого светоизлучающего диода, идеального фотоприемника, полосового фильтра. В схему включены измерительные приборы: осциллографы, спектроанализаторы, прибор для наблюдения глаз диаграмм.

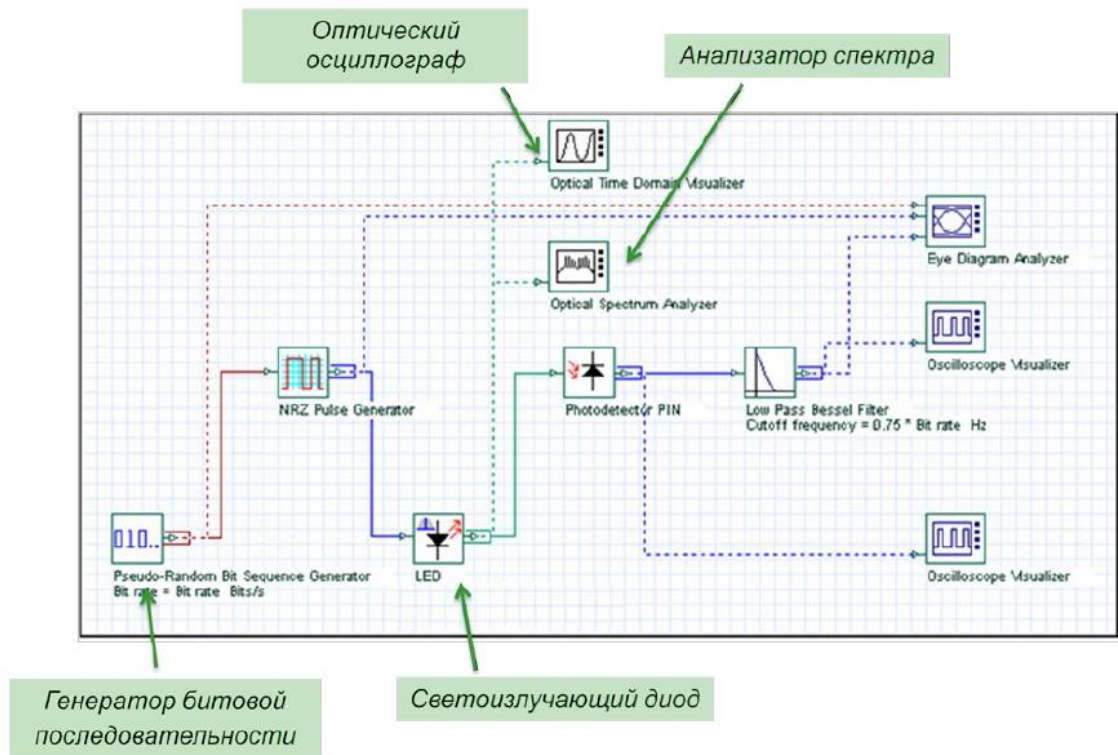


Рис. 2. Схема моделирования передатчика на основе светоизлучающего диода с прямой модуляцией

Битовая скорость, с которой может работать передатчик на основе светоизлучающего диода, в основном определяется динамикой носителей заряда (характеризуемой временем жизни носителей) и паразитной ёмкостью светодиода (характеризуется постоянной времени RC-цепи).

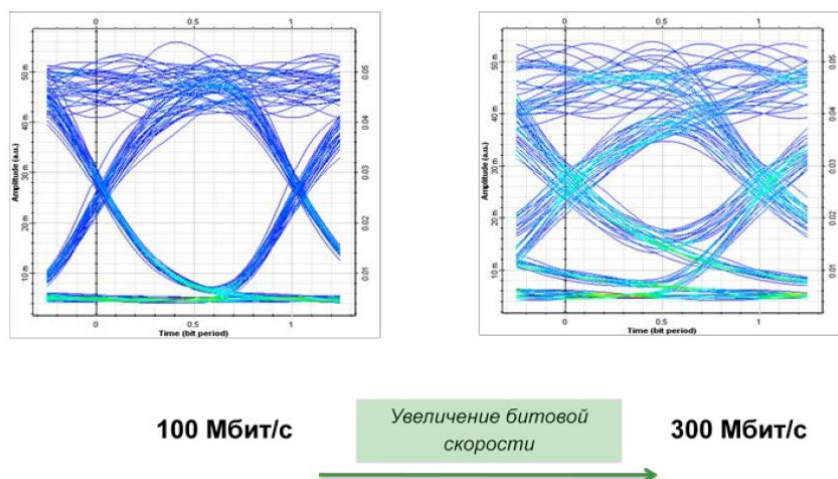


Рис. 3. Глаз-диаграммы для передатчика на основе светоизлучающего диода

Глаз диаграммы, приведенные на рис. 3 показывают, что производительность системы передачи значительно ухудшается с увеличением скорости передачи.

Лучшими характеристиками обладают передатчики на основе лазерных диодов. Особенностью работы лазерных диодов является появление релаксационных колебаний на фронтах оптических импульсов, рис. 4. При этом глаз-диаграмма не показывает признаков ухудшения сигнала даже при значительных скоростях передачи [4].

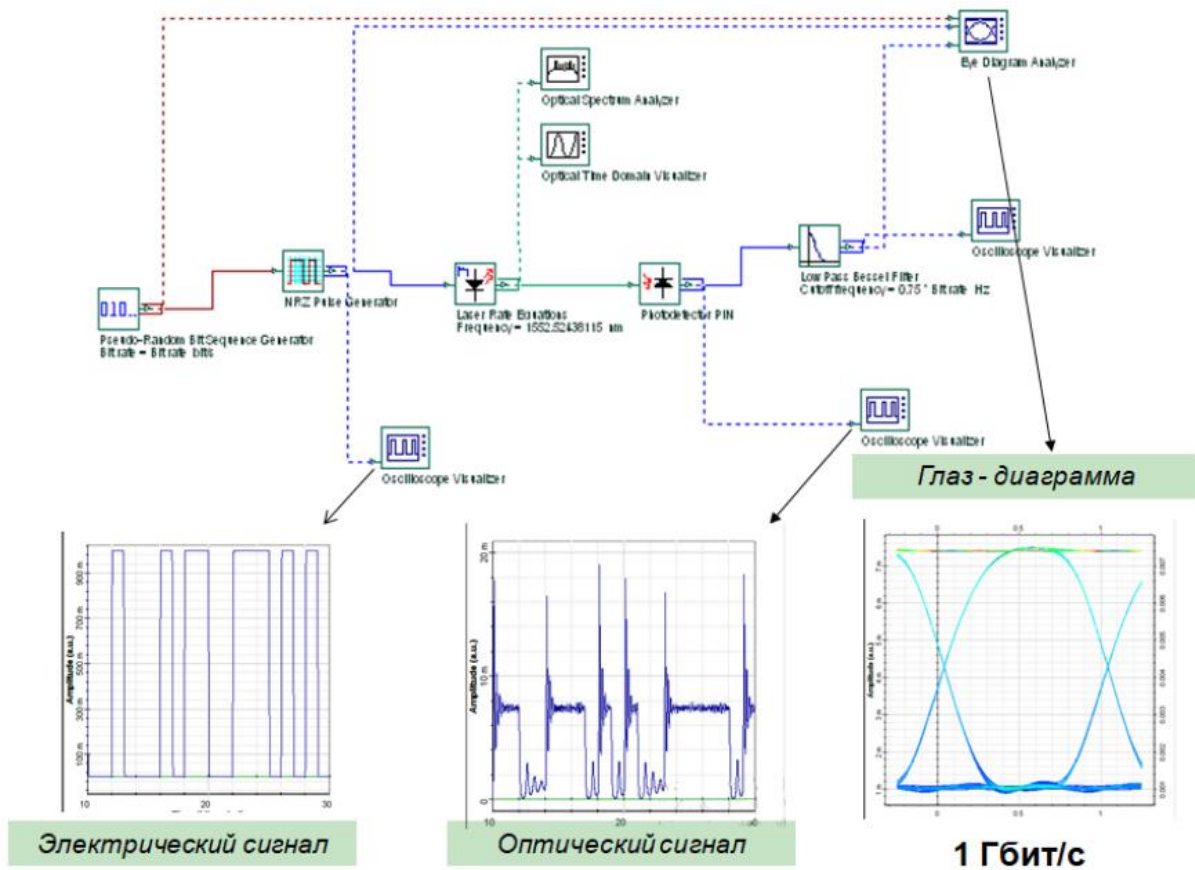


Рис. 4. Схема моделирования работа передатчика на основе лазерного диода и сигналы в различных точках схемы

Помимо схем с прямой модуляцией в аналоговых и цифровых волоконно-оптических системах связи большее распространение получили схемы с амплитудными электрооптическими модуляторами. На рис. 5 приведено схематичное представление конструкции модулятора интенсивности интерферометрического типа на основе ниобата лития. Интегрально-оптическая схема модулятора строится по принципу интерферометра Маха–Цандера и состоит из системы канальных оптических волноводов сформированных на подложке ниобата лития. Лазерное излучение входного волновода разделяется на два пути, которые затем объединяются в выходном волноводе. Вдоль волноводов сформированы электроды [5].

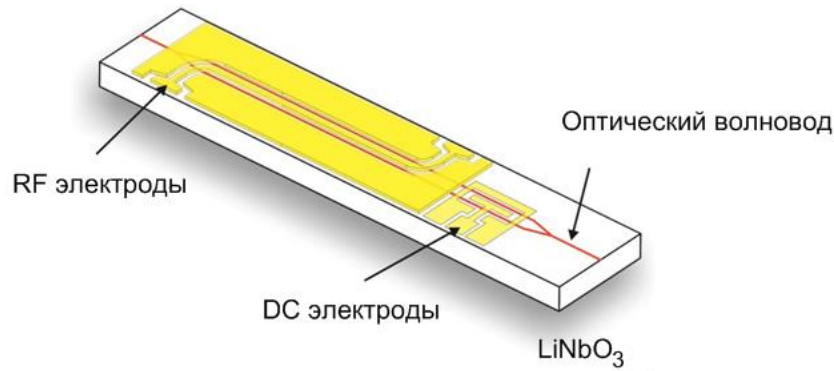


Рис. 5. Схема модулятора интенсивности на основе ниобата лития

Применяя модуляторы Маха-Цендера можно формировать сигналы амплитудной модуляции, квадратурной фазовой манипуляции, квадратурной амплитудной модуляции.

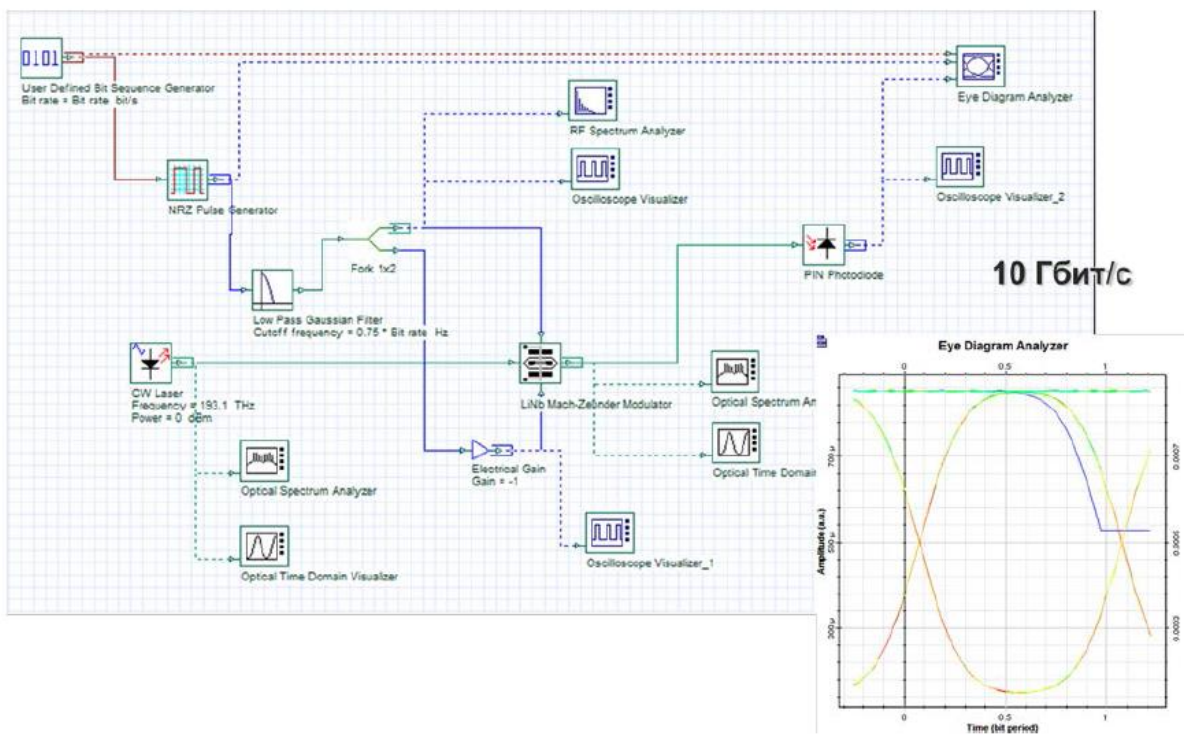


Рис. 6. Схема моделирования передатчика с внешней модуляцией и полученная глаз-диаграмма

На рис. 6 приведена схема моделирования работы передатчика с внешней модуляцией. Схемы с внешними модуляторами на электрооптических эффектах позволяют получить наилучшие характеристики быстродействия.

Список используемых источников:

1. Иванов, А. Б. Волоконная оптика: компоненты, системы передачи, измерения. / А. Б. Иванов. – Москва : Сайрус-систем, 1999.
2. Суэмацу Я. Основы оптоэлектроники. М. Мир, 1988.
3. Тугов, Н. М. Полупроводниковые приборы: учебник для ВУЗов / Н. М. Тугов, Б.А. Глебов, Н. А. Чарыков – М.: Энергоатомиздат, 1990.
4. OptiSystem Optical Communication System Design Software, version 13 // Tutorial, Volume 2, 2014.
5. Афанасьев В.М. Электрооптические амплитудные модуляторы маха–цендера на основе ниобата лития, их модификации и форматы модуляции / В.М. Афанасьев, Р.С. Пономарев // Прикладная фотоника. – 2018. – 04 – С. 336–360.

Diubov A., Kuzmina V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Modeling the operation of a transmitter of the optical communication system.

The report considers the operation of transmitters of fiber-optic communication systems based on light-emitting and laser diodes with direct and external modulation. The simulation results show the effects associated with the limited speed of semiconductor emitters and the advantages of using external modulators based on the Mach–Zehnder interferometer.

Key words: light emitting diode, laser diode, modulator, optical transmitter, modulation format, eye diagram, fiber optic communication system.

УДК 621.39
ГРНТИ 49.44.33

АКТИВНЫЕ И ПАССИВНЫЕ КОМПОНЕНТЫ ПЕРСПЕКТИВНЫХ ВОЛОКОННО-ОПТИЧЕСКИХ СЕТЕЙ СВЯЗИ

А. С. Дюбов, Е. В. Николаев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В докладе рассмотрено существующее положение и перспективы развития оптических сетей доступа и транспортных сетей. Показано, что перспективными являются технологии спектрального мультиплексирования с гибкой сеткой частот. Разветвленные сетевые топологии требуют применения компонентов и устройств для маршрутизации и управления спектральными каналами. Особое внимание уделено источникам оптического излучения, мультиплексорам длин волн, полупроводниковым оптическим усилителям и устройствам на их основе. Показана тенденция к интеграции оптических компонентов и внедрению фотонных интегральных схем.

волоконно-оптическая сеть связи, полупроводниковый оптический усилитель, мультиплексор длин волн, оптический коммутатор, нелинейный эффект, кросс-модуляция, конвертер длин волн

Развитие волоконно-оптической связи движется к созданию полностью оптических «фотонных» сетей, в которых все процессы передачи, приема, обработки и коммутации сигналов осуществляются на чисто фотонном уровне, без участия электронных процессов и электронных устройств. Для этого уже разработаны такие фотонные устройства, как оптические усилители с удаленной накачкой, оптические коммутаторы с оптическим управлением. Очевидна тенденция к интеграции оптических компонентов и внедрению фотонных интегральных схем. Важными фотонно-электронными компонентами и устройствами современных оптических сетей (рис. 1) являются оптические приемопередатчики (O-E-O, транспондеры), мультиплексоры/демультиплексоры (Mux, Demux), усилители (OA, EDFA), управляемые мультиплексоры ввода/вывода (ADM, FOADM, ROADM) [1].

Одним из основных компонентов волоконно-оптической системы связи является приемопередающий модуль, включающий в себя источник и приемник излучения. От параметров этих элементов во многом зависит качество и надежность работы системы передачи. Наиболее распространение получили: лазеры Фабри-Перо (Fabry-Perot, FP), вертикально-излучающие лазеры (Vertical-Cavity Surface-Emitting Lasers, VCSEL) и лазеры с распределенной обратной связью (Distributed Feedback, DFB) [2-4].

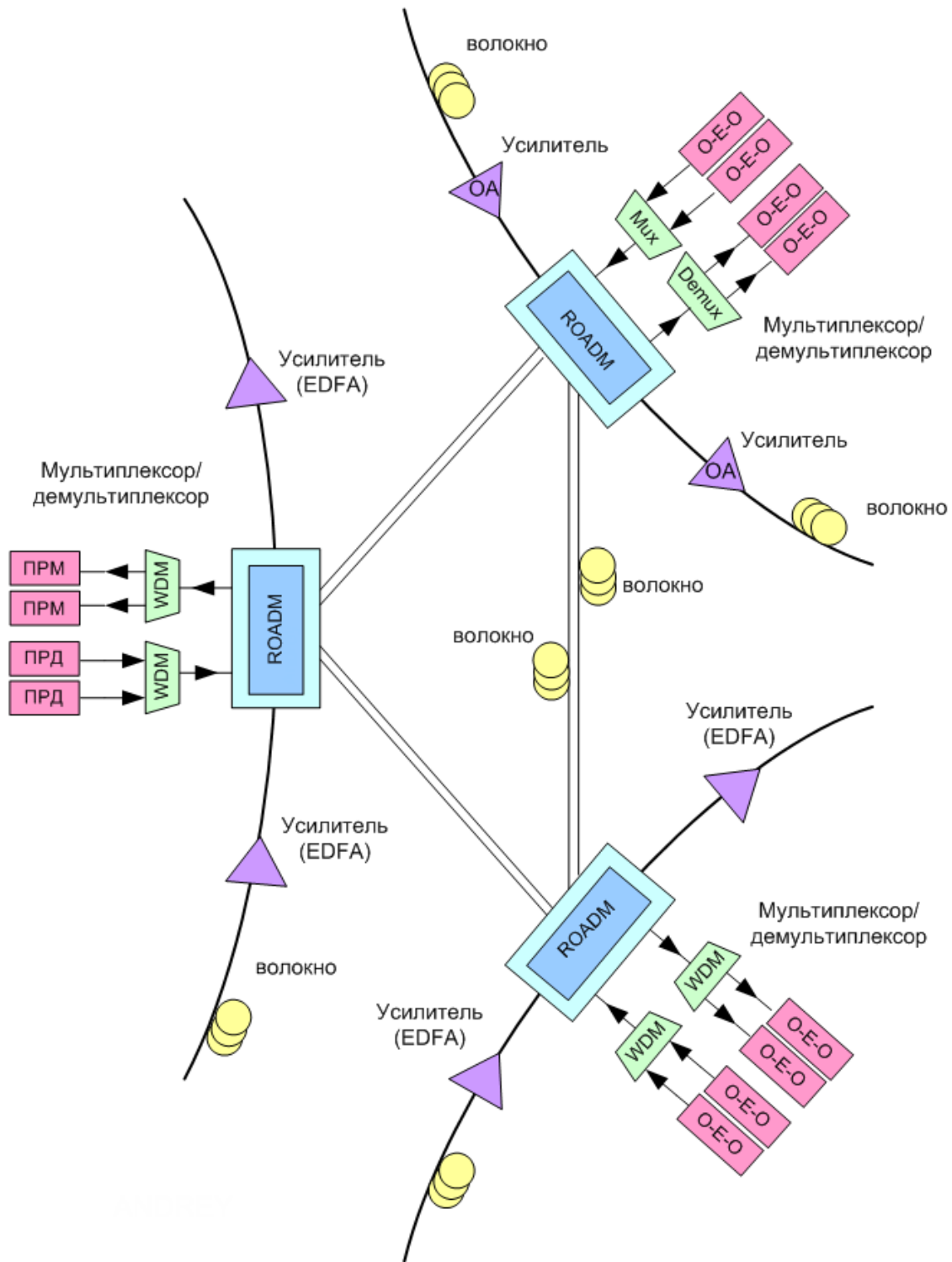


Рис. 1. Схема сети связи со спектральным уплотнением и ROADM

Когда лазер образован при помощи EAM и DFB-лазера на одном кристалле, его обычно называют электроабсорбционным модулированным лазером (Electroabsorptive Modulated Laser, EML).

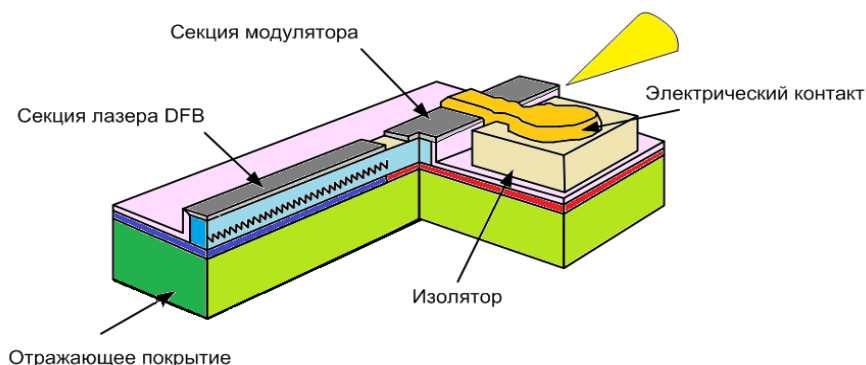


Рис. 2. EML-источник

Именно эта связка позволяет генерировать световые пучки с высокой стабильностью длины волны и достаточно высокой мощностью. Многие устройства со скоростью 10G-25G, предназначенные для передачи на дальности порядка 80-100 километров основываются на EML лазерах. EAM построены из полупроводниковых материалов, таких как фосфид индия (InP). Главное преимущество EAM заключается в способности интегрироваться с DFB-лазерами на одном кристалле.

Для выполнения коммутации одного или нескольких оптических сигналов, переходящих из одних волокон в другие на сетях используются оптические переключатели. Переключатели становятся важным элементом оптических сетей. На рынке представлены оптические переключатели, реализованные на разных принципах и по различным схемам. От технологии, на которой основан коммутационный элемент, зависит его возможности, характеристики и стоимость.

На рис. 3 приведена схема 2D коммутатора и конструкция микрозеркала, выполненного по технологии MEMS (Micro Electro Mechanical Systems). На основе зеркал MEMS могут быть построены аттенюаторы, 2D и 3D коммутаторы и аттенюаторы. Конструкция таких устройств представляет массив подвижных микрозеркал и оптических волокон. Управляемым поворотом зеркала осуществляется перенаправление светового пучка из входного волновода в выходной.

Однако коммутаторы на основе MEM-устройств ограничены в том, что они реализуют фиксированную ширину канала. Более перспективной технологией для построения сетевых устройств можно считать Liquid Crystal on Silicon (LCoS, жидкий кристалл на кремнии) поддерживающую Flexgrid, которая обеспечивает динамическое управление шириной канала. [5, 6]

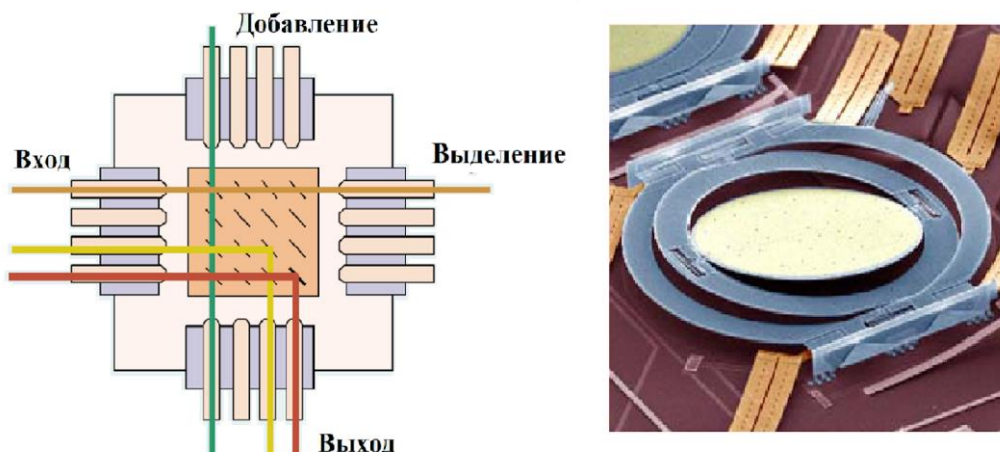


Рис. 3. Коммутатор 2D и микрозеркало MEMS

Следующим рассматриваемым устройством является полупроводниковый оптический усилитель. Работа полупроводниковых оптических усилителей (SOA, semiconductor optical amplifier) основана на использовании возбуждаемой эмиссии, возникающей благодаря взаимодействию фотонов входного возбуждающего излучения с электронами на возбужденном уровне в зоне проводимости. Конструкция полупроводникового усилителя представляет собой две металлические подложки, между которыми располагаются слои вещества с р- и n-типом проводимости, а так же слой активного вещества, рис. 4.

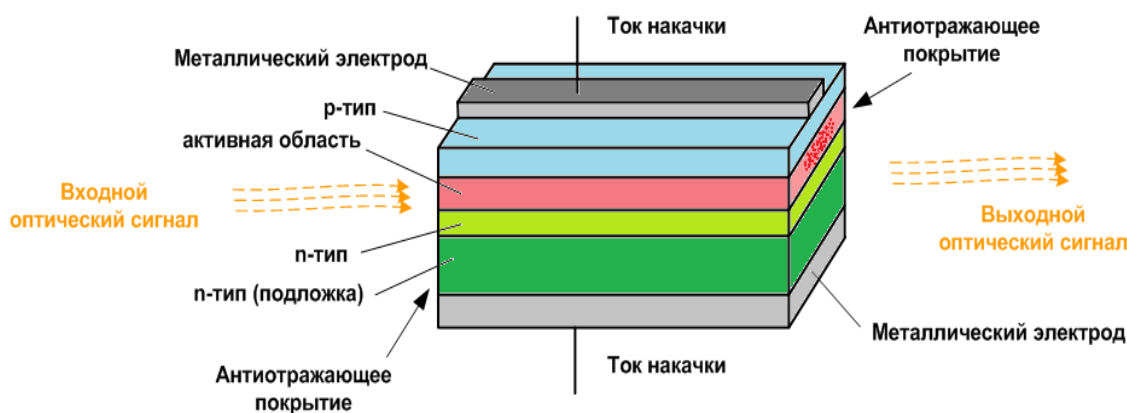


Рис. 4. Структура оптического полупроводникового усилителя

Полупроводниковые оптические усилители до недавнего времени не получили столь широкого распространения, как усилители на примесном волокне (волоконные усилители). Дело в том, что они обладают рядом существенных недостатков: неравномерный и достаточно узкий спектр усиления, зависимость коэффициента усиления от направления поляризации, малая площадь поперечного сечения активной области (что снижает эффективность сопряжения SOA с одномодовыми волокнами).

Однако полупроводниковые оптические усилители компактны, относительно дешевы и являются универсальными устройствами. Они сильнее подвержены нелинейным искажениям, таким как кроссмодуляция усиления,

фазовая кроссмодуляция, фазовая самомодуляция и четырехволновое смешение (ЧВС). Эти, казалось бы, нежелательные явления открывают возможности для использования SOA в устройствах обработки оптических сигналов. Благодаря этим свойствам, на основе полупроводниковых усилителей создаются устройства, служащие для регенерации сигнала и преобразования длины волны [3, 4].

Список используемых источников:

1. Le Nguyen Binh Advanced Digital Optical Communications Second edition : CRC Press-Taylor & Francis Group, 2015 – p. 926
2. M. Jamal Deen, P. K. Basu, Silicon Photonics Fundamentals and Devices // John Wiley & Sons Ltd 2012.
3. Дураев В. П. Полупроводниковые оптические усилители в диапазоне длин волн 840-1550 нм / В. П. Дураев, С. В. Медведев // Научное приборостроение. – 2012. – Т. 22. – № 3. – С. 53-57
4. Ghafouri-Shiraz H. The principles of semiconductor laser diodes and amplifiers. Analysis and Transmission Line Laser Modeling / H. Ghafouri-Shiraz. – London : Imperial College Press, 2004
5. MEMS Matrix Optical Switches / DiCon Fiberoptics, Inc. [Сайт]. – URL : https://www.diconfiberoptics.com/products/mems_matrix_optical_switches.php (дата обращения: 14.06.2020).
6. Fixed Grid and Flexible Grid. — Текст : электронный // Huawei : [Сайт]. — URL: https://info.support.huawei.com/onlinetoolweb/resources/en/23_grid.html (дата обращения: 24.06.2020).

Diubov A., Nikolaev E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Active and passive components for perspective fiber-optical communication networks.

The report considers the current situation and prospects for the development of optical access networks and transport networks. It is shown that the technologies of spectral multiplexing with a flexible frequency grid are promising. Branched network topologies require the use of components and devices for routing and managing spectral channels. Particular attention is paid to sources of optical radiation, wavelength multiplexers, semiconductor optical amplifiers and devices based on them. A trend towards the integration of optical components and the introduction of photonic integrated circuits is shown.

Key words: *fiber optic communication network, semiconductor optical amplifier, wavelength multiplexer, optical switch, non-linear effect, cross modulation, wavelength converter.*

УДК 681.7
ГРНТИ 49.44

АНАЛИЗ ОБЛАСТЕЙ ПРИМЕНЕНИЯ CWDM И DWDM ТЕХНОЛОГИЙ

А. И. Исупов, В. А. Кравцова, М. А. Орлов, Д. И. Сухомлинов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Для передачи больших объемов данных между узлами, необходима технология WDM. Она разделяется на грубое мультиплексирование с разделением по длине волны, CWDM, и плотное мультиплексирование с разделением по длине волны, DWDM.

WDM, CWDM, DWDM, мультиплексоры, усилители, спектр

Объемы трафика растут с каждым днём. Для того, чтобы передавать их максимально быстро и качественно, а также не прокладывать новые волокна, необходимы технологии спектрального уплотнения. Технология WDM позволяет организовать передачу нескольких оптических сигналов на одном волокне с использованием разных длин волн. Благодаря этой технологии мы можем добиться увеличения емкости уже имеющихся у нас волокон. Различают грубое и плотное спектральное уплотнение, которые мы будем рассматривать и сравнивать по критериям.

CWDM – грубое спектральное мультиплексирование - способ объединенной передачи разнородных независимых потоков данных в одном волокне, с дальнейшим разделением на выходе (рис. 1). Диапазон рабочих частот технологии CWDM лежит в пределах от 1270 до 1610 нм, можно организовать до 18 каналов, разнесенных по длине волны на 20 нм[1], скорость передачи данных каждого канала от 10 Мбит/с до 10 Гбит/с. В системе CWDM наиболее востребованы мультиплексоры, основанные на интерференционных фильтрах.

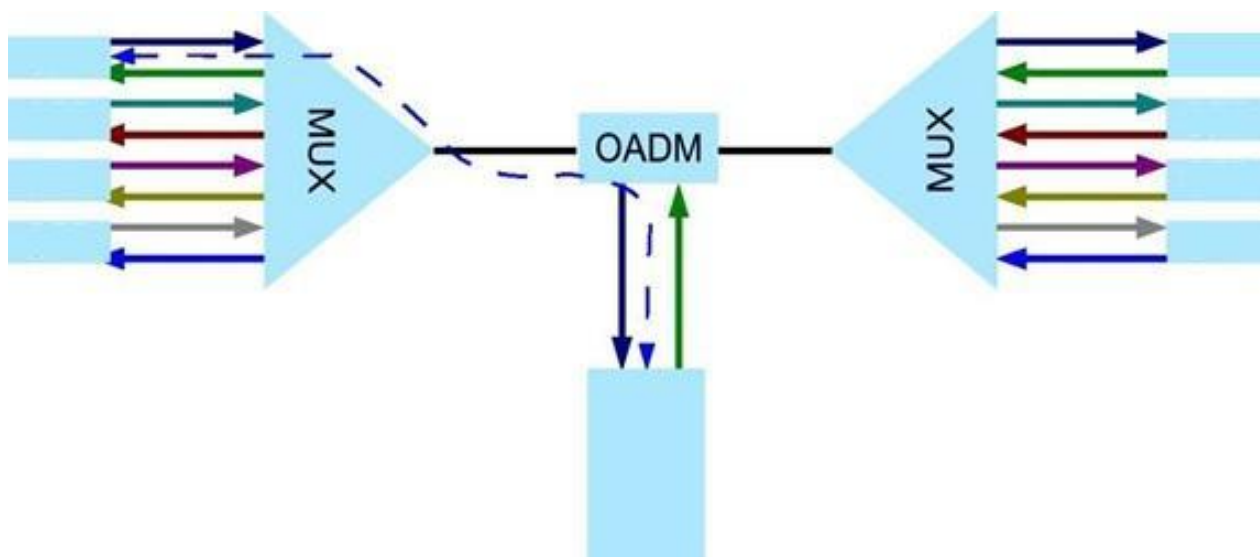


Рис. 1. CWDM система

Область применения данной технологии – построение технологических и производственных сетей, а также участков небольшой протяженности, на окончательных участках зонных сетей для подключения малых населенных пунктов. Также система может использоваться как межблочное соединение в стойках, скорость достигает 100 Гбит/с. Преимуществом является относительно небольшая цена, по сравнению с DWDM, так как требования к оптическим фильтрам и стабильности источников излучения не столь велики.

DWDM – Плотное спектральное мультиплексирование. Диапазон рабочих частот технологии DWDM лежит в пределах от 1525 до 1565 нм и от 1570 до 1610 нм (рис. 2.). В каждый диапазон попадают по 40 каналов с шагом по 0,8 нм [3].

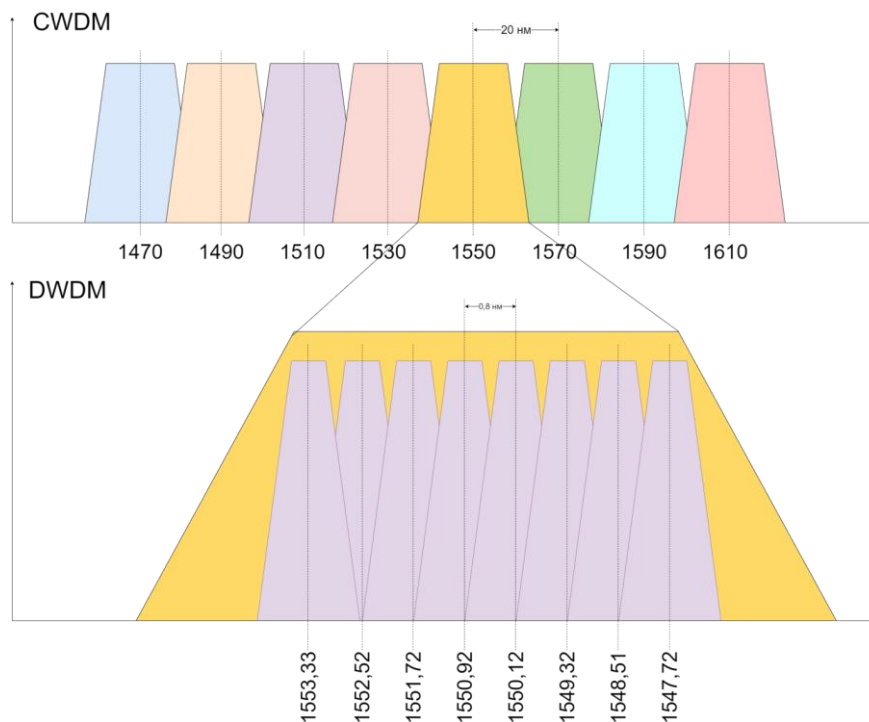


Рис. 2. Спектры технологий CWDM и DWDM

DWDM система состоит из транспондера, усилителей, мультиплексора и демультиплексора (рис. 3).

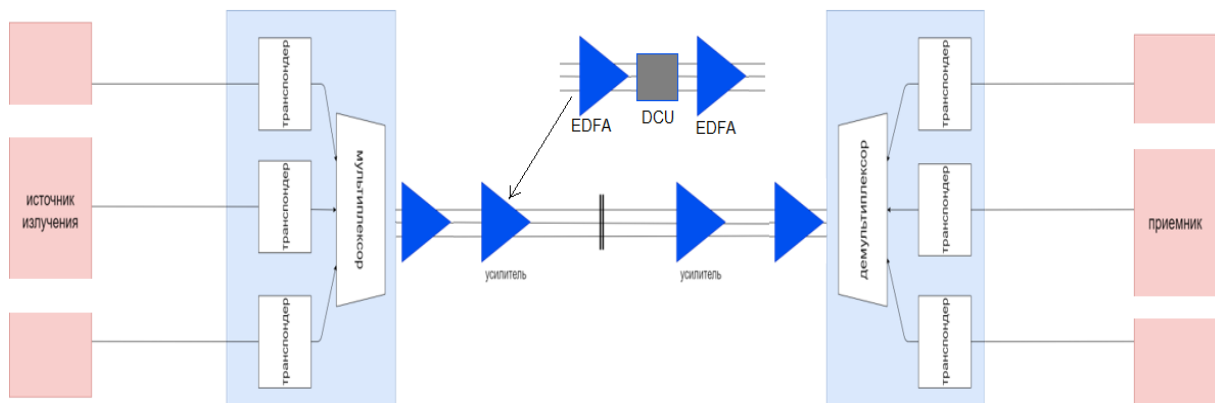


Рис. 3. DWDM система

Преобразование входящей длины волны в необходимую исходящую выполняет транспондер, после которого сигналы смешиваются на мультиплексоре и передаются в оптическую линию. Так как сигнал, в процессе прохождения по линии, имеет свойство затухать, необходимо устанавливать усилители, которые будут выравнивать сигнал до необходимого уровня. В конце линии происходит обратное преобразование на демультиплексоре, который выделяет из группового сигнала один сигнал и передает его на транспондер, который меняет приходящие длины волн и передает их на оборудование клиента [4]. В DWDM системах используются интегрально-оптические мультиплексоры на основе фазосогласованных волноводных решеток – AWG (Arrayed Waveguide Grating).

Стоимость DWDM системы в несколько раз выше CWDM, так как лазер, необходимый для её реализации, будет стоить выше, в связи с меньшим порядком допуска при изготовлении (+0,1 нм, у CWDM +2...3 нм).

Главная область применения DWDM технологии – магистральные сети, так как системы DWDM могут использовать EDFA для усиления всех длин волн в DWDM окне и увеличения длины передачи до 500 км.

Для получения решения о выборе конкретной системы (CWDM, DWDM) был разработан короткий классификатор. Он основывается на результате ответов на следующие вопросы: Какая скорость должна поддерживаться, сколько каналов должно быть организовано, на какое расстояние необходимо передать сигнал, и, при выборе системы DWDM: подвержен ли участок, на котором будет проложена система, грозам (рис. 4.).

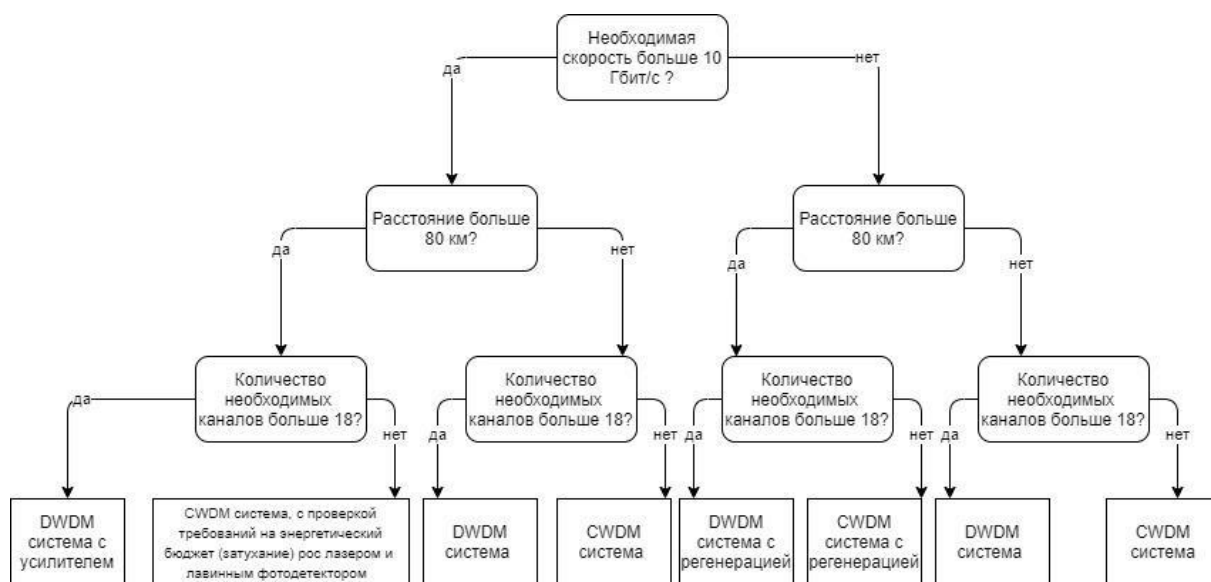


Рис. 4. Алгоритм выбора WDM системы

При выборе DWDM системы, необходимо уточнить, насколько активны молнии в месте прокладки трассы (вопрос к элементной базе транспондера).

Для этого, сначала необходимо определить, как будет проложен ОК (в грунт или методом воздушной прокладки). Если по условиям прокладки и эксплуатации ОК выбирается прокладка в грунт, то влияние гроз не учитывается.

Если выбирается воздушная прокладка, необходимо понять, в какой части полушария будет проходить трасса, так как грозы на экваторе сильнее. При ударе молнии, вектор поляризации начинает вращаться. Молния на северо-западе вызывает вращение вектора 500 рад/с. Большинство транспондеров могут это компенсировать, но в южных регионах понадобится другое оборудование, так как скорость вращения может достигать до 25 Мрад /с. В этом случае, сигнал обрабатывается более сложными алгоритмами, поэтому будет необходим грозоустойчивый транспондер.

Ниже разобраны некоторые результаты алгоритма:

Вариант 2: скорость больше 10 Гбит/с, расстояние больше 80 км, количество необходимых каналов меньше 18. Результат: CWDM система, с проверкой требований на энергетический бюджет (затухание) рос лазером и лавинным фотодетектором. При использовании CWDM системы можно добавить SFP модули, для увеличения протяженности канала связи до 160-180 км, оптический бюджет таких модулей составляет 41 дБ.

Вариант 3: скорость больше 10 Гбит/с, расстояние меньше 80 км, количество необходимых каналов больше 18. Результат: DWDM система, так как при длине волны излучения больше 1650 нм километровое затухание волокна резко возрастает и в добавленном канале будут неприемлемо высокие потери.

Вариант 6: скорость меньше 10 Гбит/с, расстояние больше 80 км, количество необходимых каналов меньше 18. Результат: CWDM система с регенерацией, так как количество каналов, достаточное для размещения их в сетке CWDM, но для преодоления большого расстояния, необходим регенератор, так как в системах CWDM не используются усилители.

В результате рассмотрения технологий CWDM и DWDM были получены главные факторы, определяющие выбор оптимальной системы, такие как протяженность линии, количество каналов и их скорость, бюджет организации.

Список используемых источников:

1. Кусен, К. Е. Анализ транспортных сетей на основе CWDM и DWDM / К. Е. Кусен, У. С. Есенжолов // Вестник Казахской академии транспорта и коммуникаций им. М. Тынышпаева. – 2013. – № 4(83). – С. 91-96. – EDN YRVUIT.
2. Имамова, Д. А. Исследование технологий спектрального уплотнения для увеличения пропускной способности магистральной сети / Д. А. Имамова, Е. А. Барабанова, В. М. Дорохов // Наука, образование, инновации: пути развития : Материалы Восьмой всероссийской научно-практической конференции, Петропавловск-Камчатский, 23–25 мая 2017 года. – Петропавловск-Камчатский: Камчатский государственный технический университет, 2017. – С. 76-79. – EDN YRKXTM.
3. ITU-T G.694.1 Spectral grids for WDM applications: DWDM frequency grid. / Recommendation ITU-T G.694.1 (10/2020)
4. ITU-T G.694.2. Spectral grids for WDM applications: CWDM wavelength grid. / Recommendation ITU-T G.694.2 (12/2003)
5. Трещиков В. Н. DWDM системы. / Трещиков В. Н. Листвин В. Н. – Москва : ТЕХНОСФЕРА, 2021. – 420 с. – ISBN 978-5-94836-634-0

Isupov A., Kravtsova V., Orlov M., Sukhomlinov D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of application areas of CWDM and DWDM technologies.

To transfer large amounts of data between nodes, WDM technology is required. It is divided into coarse wavelength division multiplexing, CWDM, and dense wavelength division multiplexing, DWDM.

Key words: WDM, CWDM, DWDM, multiplexers, amplifiers, spectrum.

УДК 621.396.99
ГРНТИ 49.33.29

ВОЛОКОННО-ОПТИЧЕСКИЕ ДАТЧИКИ НА ПРИНЦИПЕ РАССЕЯНИЯ МАНДЕЛЬШТАМА-БРИЛЛЮЭНА

В. Э. Карлин

Сибирский Государственный университет телекоммуникаций и информатики

В представленной работе рассматривается рассеяние Мандельштама-Бриллюэна и различные типы волоконно-оптических датчиков, построенных на его основе. Анализируется спектр рассеяния Мандельштама-Бриллюэна и приводится формула для расчета среднего значения частоты рассеянного сигнала. Предлагается классификация различных типов бриллюэновских датчиков и приводится их сравнение.

оптическое волокно, датчики распределенного типа, волоконно-оптические датчики, рассеяние Мандельштама-Бриллюэна, Бриллюэновский сдвиг частоты

Волоконно-оптические датчики (ВОД) на основе рассеяния Мандельштама-Бриллюэна (РМБ) относятся к группе датчиков распределенного типа. ВОД распределенного типа состоят из двух компонент – подводящего волоконно-оптического кабеля и опросного устройства. Опросное устройство посылает лазерные импульсы, которые приводят к возникновению РМБ в оптическом волокне (ОВ). ОВ используется одновременно в качестве чувствительного элемента и линии передачи данных. Опросное устройство детектирует рассеянные сигналы и получает промежуточную измерительную информацию. Принцип функционирования ВОД на основе РМБ заключается в анализе спектров и амплитуды детектированных сигналов. Спектры различных компонент рассеяния света в ОВ показаны на рис. 1. Датчики, построенные на РМБ, фильтруют спектр РМБ от других компонент рассеяния света и по заданному алгоритму производят компьютерный анализ полученных данных.

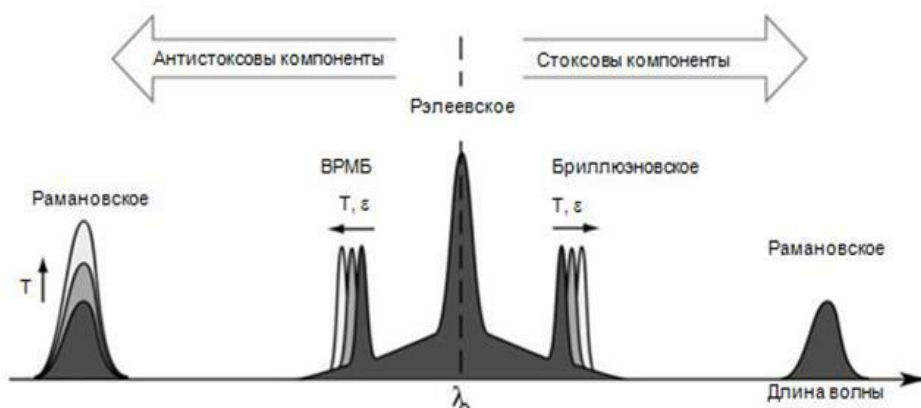


Рис. 1. Спектр различных компонент рассеяния, возникающих при распространении по ОВ импульса накачки с длиной волны λ_0 (T – температура, ε – деформации)

Из закона сохранения импульса и энергии можно найти величину сдвига центральной частоты ν_B спектра рассеяния по Бриллюэну [1]:

$$\nu_B = \frac{2n_1 V_A}{\lambda_0} \sin(\theta/2), \quad (1)$$

где n_1 – коэффициент преломления материала сердцевины ОВ; λ_0 – длина волны тестового импульса; V_A – скорость акустической волны; θ – угол между падающим и рассеянным светом.

Из рисунка 1 видно, что сдвиг центральной частоты спектра РМБ относительно частоты накачки значительно меньше, чем аналогичная величина для комбинационного рассеяния (~10 ГГц для РМБ против ~13 ТГц для комбинационного рассеяния). Естественная ширина линии РМБ также намного меньше ширины спектра комбинационного рассеяния (~30 МГц против ~6 ТГц). Это делает РМБ гораздо более универсальным эффектом для построения датчиков распределенного типа, чем комбинационное рассеяние. Перечислим основные причины такого различия:

1. Спектр РМБ в ОВ более чувствителен к деформации и температуре ОВ. Измеряемым параметром в ВОД на РМБ является спектральный сдвиг рассеянного света. Величина спектрального сдвига определяется как разница центральных частот, точность определения которых выше для более узких спектральных распределений. Ширина рамановской линии значительно больше ширины линии РМБ (рис. 1) и она не используется для измерения частотного сдвига. Возможность точного измерения сдвига частоты РМБ позволяет с помощью ВОД на РМБ получать данные о деформации и температуре по всей длине ОВ.

2. Узкая спектральная ширина линии РМБ позволяет повысить качество принимаемого сигнала с помощью оптического усиления и гетеродинных методов. Поэтому ВОД на РМБ позволяют увеличить длину контролируемых участков ОВ до десятков километров. Напротив, методы оптического усиления неэффективны для очень широких сигналов, таких как комбинационное рассеяние, а обнаружение гетеродина полностью исключено, учитывая, что приемнику потребуется полоса пропускания в несколько ТГц для захвата сигнала.

3. Вынужденное рассеяние Манделъштама-Бриллюэна (Stimulated Brillouin scattering – SBS) возникает, когда мощность тестового импульса накачки превышает пороговое значение [1]. Это позволяет использовать вынужденное РМБ при конструировании ВОД распределенного типа. Первые опубликованные подходы к зондированию Бриллюэна были основаны на вынужденном РМБ. Сигнал, полученный в этом случае, является мерой усиления (или потери) при взаимодействии двух встречно распространяющихся волн. Это привело к некоторым очень интересным конфигурациям, в которых сигналы сконструированы таким образом, что они могут взаимодействовать только на очень коротких расстояниях, и, как результат, были продемонстрированы

пространственные разрешения в миллиметровом диапазоне. Эти конфигурации не имеют аналогов в рамановском распределенном датчике температуры (DTS).

4. Сигнал спонтанного обратного рассеяния Бриллюэна существенно сильнее (примерно на порядок величины), чем сигнал антистоксовой компоненты обратного рассеяния комбинационного рассеяния, хотя это преимущество смягчается более слабой чувствительностью его интенсивности к температуре.

5. Хотя физика в этих двух случаях различна, существует много общего между спонтанным рассеянием Бриллюэна (Spontaneous Brillouin scattering – SpBS) и спонтанным комбинационным рассеянием. Сдвига частоты, чувствительность и ширины линии используются в рамановских распределенных датчиках деформации и температуры (Distributed strain and temperature sensor – DTSS).

6. SBS привносит совершенно разные концепции в том смысле, что в стимулированном случае измеряется профиль усиления, а не спектр интенсивности обратного рассеяния, хотя эти два параметра тесно связаны. В процессе измерения спектра усиления существует большая гибкость в реализации. Это привело ко многим схемам использования SBS, включая оптический анализ Бриллюэна во временной области (BOTDA), оптический анализ Бриллюэна в частотной области (BOFDA), анализ области оптической когерентности Бриллюэна (BOCDA) и рефлектометрию области оптической когерентности Бриллюэна (BOCDR) и методы, основанные на динамических брэгговских решетках (Dynamic bragg gratings – DBGs).

В настоящее время появилось большое число различных типов ВОД на РМБ. ВОД можно классифицировать по принципу функционирования [2] и по способу ввода зондирующего сигнала [3-6] (таблица 1).

ТАБЛИЦА 1. Классификация ВОД

<i>По принципу функционирования</i>	функционирующие во временной области
	с частотно модулированным зондирующим сигналом
<i>По способу ввода зондирующего сигнала</i>	ввод зондирующего сигнала с одного конца оптического волокна (Brillouin Optical Time-Domain Reflectometry - BOTDR) [3, 4]
	ввод зондирующего сигнала с обоих концов (BOTDA- Brillouin optical time-domain analysis) [5, 6]

Бриллюэновские оптические рефлектометры (BOTDR) различаются по методам спектральной обработки:

- *Brillouin optical coherence domain reflectometry (BOCDR)*. Использование узкополосного источника позволяет применять когерентные методы обнаружения. Существуют две основные реализации концепции BOCDR, а именно гетеродинное и гомодинное обнаружение.

- *Brillouin Optical Time-Domain Reflectometry with wavelength division multiplexing (WDM-BOTDR)*. Мультиплексирование с разделением длин волн позволяет улучшить отношение сигнал/шум распределенных сенсорных систем, которое определяет динамический диапазон и точность измерений.

- *Synthetic BOTDR (S-BOTDR)*. В этом методе выполняется объединение спектров Бриллюэна четырех измерений BOTDR с определенными весами. Получаемый спектр близок к спектру Лоренца. При этом становится возможным увеличить пространственную разрешающую способность до 10 см, которая значительно превышает предел разрешения обычного BOTDR.

Бриллюэновские оптические анализаторы во временной области (Brillouin optical time-domain analysis) классифицируются следующим образом [7]:

- *Brillouin Dynamic Gratings – Brillouin Optical Time-Domain Analysis (BDGs-BOTDA)*. В приборах этого типа сочетаются измерения фазового сдвига Бриллюэна с рефлектометрией динамических решеток Бриллюэна (BDGs) в волокнах с поддержанием поляризации. Способ выгодно сочетает в себе рефлектометрию BDGs с высоким пространственным разрешением с повышенной устойчивостью к флуктуациям оптической мощности при фазовых измерениях для повышения производительности волоконно-оптических тензодатчиков.

- *Brillouin Optical Time Domain Analysis with fiber Bragg grating (FBG-BOTDA)*. В этих системах используется сдвиг длины волны Брэгга, который пропорционален изменениям температуры, деформации и давления. Волоконная решетка является чувствительным оптическим устройством, где показатель преломления сердцевины волокна изменяется вдоль оси, что приводит к изменению его спектральных характеристик.

- *Phase-Shift Pulse Brillouin Optical Time Domain Analysis (PSP-BOTDA)*. Для расширения функциональных возможностей в датчиках этого используется одновременно пара кодированных импульсных последовательностей. В результате получается более длинный код, обеспечивающий улучшение отношения сигнал/шум.

- *Differential Pulse-width Pair Brillouin Optical Time Domain Analysis (DPP-BOTDA)*. Этот тип модифицированного BOTDA с более высоким пространственным разрешением менее 1 метра основан на группе импульсов, называемых дифференциальной широтно-импульсной парой. Импульсы незначительно отличаются по длительности. Спектр взаимодействия Бриллюэна регистрируется дважды. Тем самым обеспечивается высокое пространственное разрешение, определяемое малой разностью длительности импульсов.

Заключение

ВОД на эффекте РМБ обладают достаточно высокой точностью и пространственной разрешающей способностью для измерения температурных и механических параметров ОВ. При выборе ВОД на эффекте РМБ следует учитывать, как требования к разрешающей способности ВОД, так и требования к диапазону измеряемых величин. Так, системы ВОТДА имеют более высокое пространственное разрешение и меньшие погрешности измерений, но диапазон измерений их ниже, чем у систем ВОТДР. Но ВОД на методе ВОТДА позволяют гибко настраивать производительность. Например, для улучшения пространственного разрешения можно использовать метод композитного импульса. Рост числа публикаций по ВОД РМБ характеризует об увеличении их функциональных возможностей и расширении сферы их применения.

Список используемых источников:

1. Heiman, D., D. S. Hamilton, and R. W. Hellwarth. 1979. Brillouin scattering measurements on optical glasses. *Phys. Rev. B* 19: 12: 6583.
2. Zhang H., Zhou D., Wang B., Pang Chao, Xu P., Jiang T, Ba D., Li H., Dong Y., “Recent Progress in Fast Distributed Brillouin Optical Fiber Sensing”, *Appl. Sci.* 2018, 8, 1820; doi:10.3390/app8101820.
3. Zhou D., Dong Y., Wang B., Pang C., Ba D., Zhang H., Lu Z., Li H., Bao X., “Single-shot BOTDA based on an optical chirp chain probe wave for distributed ultrafast measurement”, *Light Sci. Appl.* 2018, 7, 32.
4. Chow D. M., Yang Z., Soto M.A., Thévenaz L., “Distributed forward Brillouin sensor based on local light phase recovery”, *Nat. Commun.* 2018, 9, 2990.
5. Bao X., Chen L., “Recent Progress in Brillouin Scattering Based Fiber Sensors”, *Sensors* 2011, 11.
6. Hotate K., “Recent achievements in BOCDA/BOCDR” In Proceedings of the IEEE SENSORS 2014, Valencia, Spain, 2–5 November 2014; pp. 142–145.
7. Bogachkov I.V., Gorlov N.I. Joint testing of optical pulse reflectometers of various types for early diagnostics and detection of "problem" sections in optical fibers// 13th international scientifictechnical conference on actual problems of electronic instrument engineering (APEIE - 2016). Proceedings: in 12 volumes. 2016. pp. 152-156.

Karlin V.

The Siberian State University of Telecommunications and Information Science

Current status of measurement systems based on Mandelstam-Brillouin scattering.

In the presented work the Mandelstam-Brillouin scattering and different types of fiber-optic sensors built on its basis are considered. The Mandelstam-Brillouin scattering spectrum is analyzed and a formula for calculating the average value of the scattered signal frequency is given. A classification of different types of Brillouin sensors is proposed and their comparison is given.

Keywords: *optical fiber, sensors distributed type, optical fiber sensors, Mandelstam-Brillouin scattering, Brillouin frequency shift.*

УДК 621.391.63
ГРНТИ 49.44.31

ИССЛЕДОВАНИЕ ПРОЦЕССА ПОДДЕРЖАНИЯ КВАЗИСОЛИТОННОГО РЕЖИМА РАСПРОСТРАНЕНИЯ ИМПУЛЬСОВ В ОДНОМОДОВОМ ВОЛОКНЕ С АНОМАЛЬНОЙ ДИСПЕРСИЕЙ

Г. Р. Лыков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Доклад посвящен исследованиям процессов поддержания квазисолитонного режима распространения секансных импульсов в одномодовом волокне (ОМОВ) с аномальной дисперсией и потерями. Рассмотрены процессы поддержания квазисолитонного режима с помощью дискретных оптических усилителей (ОУ) и с использованием ОУ на основе вынужденного комбинационного рассеяния (ВКР) со встречной накачкой. Сопоставлены результаты теоретических расчетов с результатами имитационного моделирования в программе OPTISYSTEM.

одномодовые волокна, солитоны, хроматическая дисперсия (ХД), нелинейная длина, фазовая самомодуляция (ФСМ), квазисолитонный режим, рамановский усилитель

1. Исследование квазисолитонного режима в ОВ с потерями

В ОМОВ с потерями фундаментальные солитоны существовать не могут, т.к. пиковая мощность секансных оптических импульсов с увеличением расстояния уменьшается и мощности для поддержания солитонного режима становится недостаточно. Можно говорить только о квазисолитонном (близком к солитонному) режиме распространения секансных импульсов с использованием оптического усиления. Этот метод называют «управление затуханием». Он состоит в том, чтобы на каждом усилительном участке (УУ) сохранять среднюю величину пиковой мощности равную пиковой мощности фундаментального солитона. Усиление может осуществляться дискретным ОУ типа EDFA или распределенным рамановским ОУ [1, 4].

2. Поддержание квазисолитонного режима за счет применения дискретных усилителей EDFA

Схема исследования квазисолитонной ВОСС с дискретными ОУ типа EDFA приведена на рис. 1. Схема содержит источник бинарной псевдослучайной последовательности (ПСП), формирователь оптических секансных импульсов, многопролетный волоконно-оптический линейный тракт (ВОЛТ), включающий ОМОВ и ОУ, полосовой фильтр и фотоприемное устройство (ФПУ). В схеме присутствуют оптические и электрические приборы контроля параметров сигнала.

Исходные данные для расчетов параметров и моделирования ВОСС: скорость передачи $B=10$ Гбит/с, длина волны $\lambda=1550$ нм, длительность секансного импульса $t_u=0.2$ бит, ОМОВ типа DSF, с параметрами: коэффициент

затухания $\alpha=0.2$ дБ/км, коэффициент ХД $D_x=1$ пс/(км·нм), дисперсия групповых скоростей (ДГС) $\beta_2=-1.27$ пс/нм², крутизна дисперсионной характеристики $S_x=0.085$ пс/нм²/км, эффективная площадь модового поля $A_{ef}=41$ мкм², нелинейный показатель преломления $n_2=26 \cdot 10^{-21}$ м²/Вт, коэффициент нелинейности $\gamma=2.571$ 1/(Вт·км). Длина волны накачки ОУ Рамана $\lambda_p=1450$ нм.

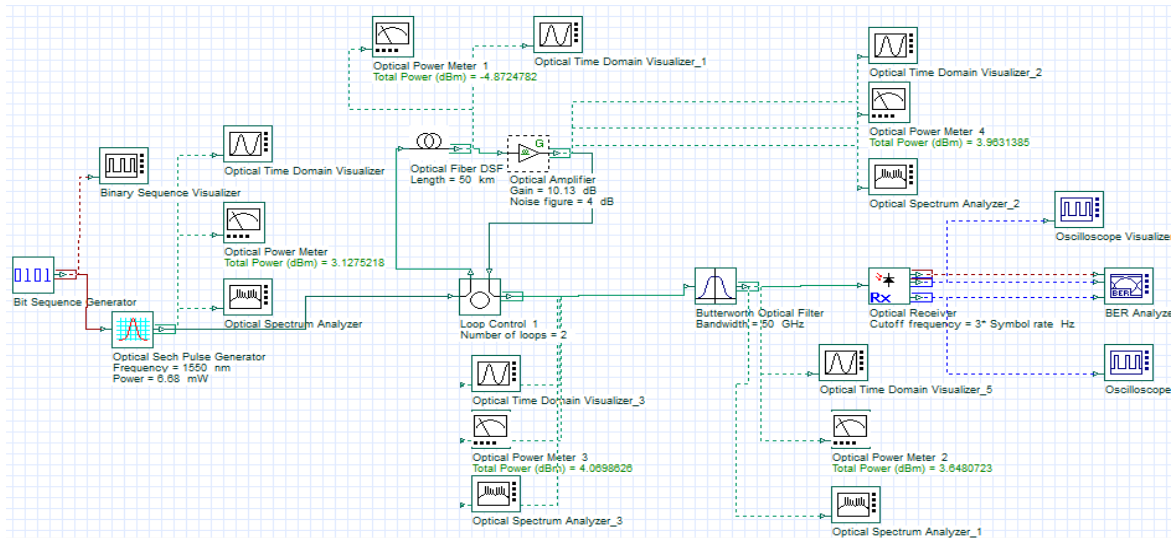


Рис. 1. Схема многопролетной ВОСС с дискретными ОУ EDFA

3. Предварительные расчеты

Длительность секансного импульса $t_u = t_{u0}/B = 20$ пс, (1)

Каноническая полуширина секансного импульса $T_0 = t_u/1.763 = 11.34$ пс, (2)

Пиковая мощность фундаментального солитона $P_0 = |\beta_2|/(\gamma \cdot T_0^2) = 3.85$ мВт, (3)

Дисперсионная длина ОМОВ $L_D = (T_0)^2/|\beta| = 101.3$ км, (4)

Нелинейная длина ОМОВ $L_{nl} = 1/(\gamma \cdot P_0) = 101.3$ км, (5)

Коэффициент ОМОВ $\alpha=0.2$ дБ/км или 0.046 Нп/км.

Для поддержания квазисолитонного режима на УУ длиной L_A с помощью дискретных ОУ необходимо на вход УУ подавать импульс с пиковой мощностью $P_{m\phi\alpha}$ большей, чем мощность, требуемая для фундаментального солитона $P_{m\phi}$.

$$P_{m\phi\alpha} = P_{m\phi} \cdot L_A/L_{ef} = 10 \text{ мВт} \quad (6)$$

где $L_{ef} = (1 - \exp(-\alpha \cdot L_A))/\alpha = 19.9$ км эффективная длина ОМОВ.

В качестве начального значения длины УУ примем: $L_A = L_D/2 = 50.7$ км. Необходимый коэффициент усиления дискретного ОУ:

$$G = \alpha L_A = 10.13 \text{ дБ} \quad (7)$$

Из табл. 1 видно, что для одного УУ теоретические расчеты подтвердились и совпали с экспериментом. При увеличении количества УУ до 8 пришлось корректировать мощность входного импульса в пределах 1-0,7 мВт.

4. Квазисолитонная ВОСС с ОУ Рамана и встречной накачкой

Схема двухпролетной ВОСС с ОУ Рамана показана на рис. 2. Она содержит два УУ, Для поддержания квазисолитонного режима УУ представляют собой распределенные усилители Рамана со встречной накачкой. Излучение накачки с

частотой сдвинутой вверх на 13 ТГц относительно несущей частоты сигнала вводится в ОМ ОВ с помощью WDM направленного ответвителя (НО) и отдает свою энергию излучению сигнала [3].

ТАБЛИЦА 1. Результаты измерений при коэффициенте усиления $G=10.13$ дБ

Устанавливаемые параметры				Измеренные величины		
Кол-во участков, n	Длина ВОТ, l_T км	Вх. пик. мощн. на входе, мВт	Длит. имп. на входе в ОВ t_{uo} , бит	Вых. пик. мощн. на выходе, мВт	Длит. имп. на выходе из ОВ, бит	Q
1	50.7	10	0.2	10.05	0.2	218
2	50.7	10	0.2	10.1	0.202	178
5	50.7	9.3	0.2	9.3	0.2	102
8	50.7	9	0.2	10	0.199	75

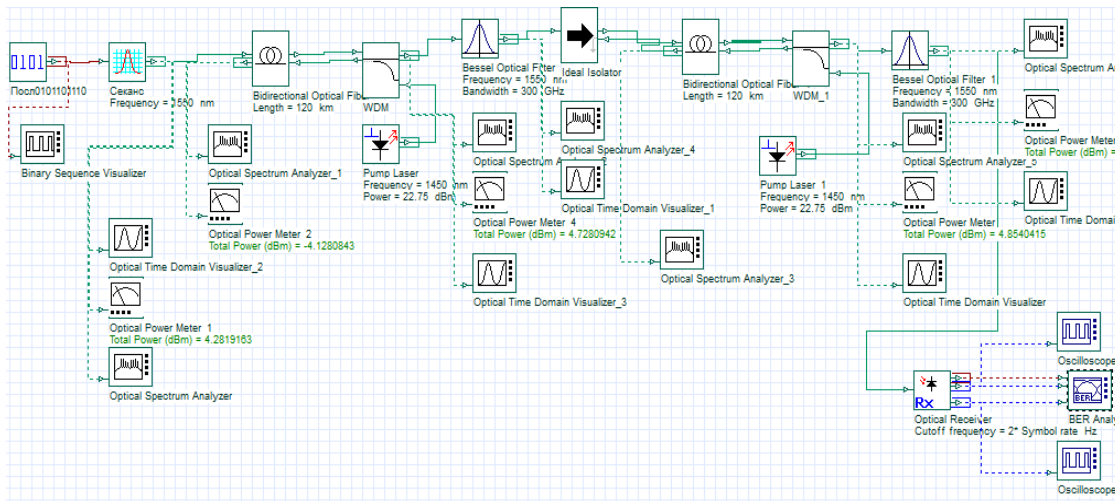


Рис. 2. Схема двухпролетной ВОСС с ОУ Рамана

Изменения пиковой мощности сигнала $P_m(z)$ на участке dz ОМОВ с коэффициентом затухания α описываются дифференциальным уравнением

$$\frac{dP_m(z)}{dz} = [g(z) - \alpha] \cdot P_m(z), \quad (8)$$

где $g(z)$ - усилительная способность ОМОВ, которая зависит от z и определяется уровнем накачки в этой точке.

В конце УУ при $z=L_A$ усилительная способность и уровень накачки максимальны. При $g(z) < \alpha$ пиковая мощность на участке dz уменьшается, а при $g(z) > \alpha$ возрастает.

Вначале УУ мощность накачки минимальна и преобладает затухание, уровень сигнала с увеличением расстояния убывает до некоторого уровня. С увеличением расстояния мощность накачки возрастает, и сигнал усиливается до первоначального уровня в конце УУ. Средний уровень сигнала на УУ должен быть равен уровню фундаментального солитона. В каждой точке линии невозможно компенсировать потери, но может быть скомпенсировано общее затухание на расстояние L_A между ОУ при условии

$$\int_0^{L_A} g(z) \cdot dz = \alpha \cdot L_A \quad (9)$$

Экспериментально определенная пиковая мощность фундаментального солитона в ОМОВ без потерь составила $P_{m\phi}=4,74$ мВт (теоретически рассчитанная $P_{m\phi}=3,9$ мВт). Пренебрегая истощением накачки, запишем упрощенное выражение для усилительной способности на УУ

$$g(z) = g_0 \cdot \exp[-\alpha_p \cdot (L_A - z)] \quad (10)$$

где α_p – коэффициент затухания ОМОВ для накачки, $g_0=g(L_A)$ – максимальная усилительная способность ВКР ОУ.

Запишем выражение для мощности сигнала, решив уравнение (8) с учетом (9), при котором пиковая мощность на выходе УУ равна входной $P_{0m}=P_m(L_A)$.

$$P_m(z) = P_{0m} \cdot \exp\left\{\alpha \cdot \left[L_A \cdot \left[\frac{\exp(\alpha_p \cdot z)-1}{\exp(\alpha_p \cdot L_A)-1}\right] - z\right]\right\} = P_{0m} \cdot p(z). \quad (11)$$

При встречной накачке, пиковая мощность входных импульсов P_{0m} должна быть больше или равна мощности солитона $P_{m\phi}$ в ОМ ОВ без потерь [1]

$$P_{0m} = P_{m\phi}/p_0, \quad p_0 = (1/L_A) \cdot \int_0^{L_A} p(z) \cdot dz \quad (12)$$

где p_0 – среднее значение нормализованной пиковой мощности излучения на УУ. Рассчитанные значения p_0 и P_{0m} приведены в таблице 2. Зависимости нормализованной пиковой мощности $p(z)$ от относительного расстояния z/L_A в пределах одного УУ рассчитанные по (13) показаны на рис. 3.

ТАБЛИЦА 2. Среднее значение p_0 и P_{0m} для на УУ с различными длинами L_A

L_A , км	40	60	80	100	120
p_0	0.737	0.544	0.390	0.291	0.228
P_{0m} , мВт	6.384	8.676	12.01	16.188	20.812

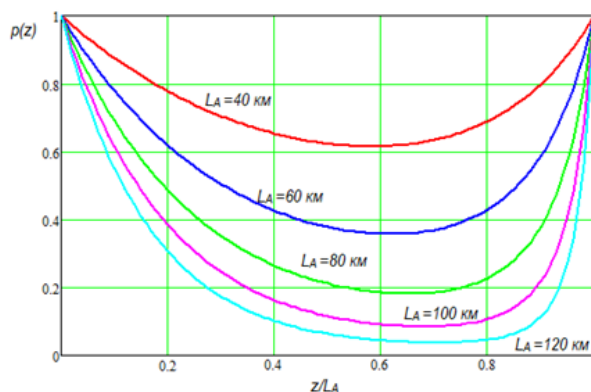


Рис. 3. Зависимости нормализованной пиковой мощности $p(z)$ от относительного расстояния z/L_A в пределах одного УУ

Результаты экспериментального исследования ВОСС с одним пролетом (УУ) приведены в табл. 3, а с большим количеством пролетов в табл. 4. Они подтвердили возможность поддержания квазисолитонного режима в ВОСС.

ТАБЛИЦА 3. Результаты исследований ВОСС с одним УУ

L_A , км	40	60	80	100	120
P_{0m} , мВт	6.4	8.7	12.0	16.2	20.8
P_{lm} , мВт	6.3-6.4	8.6-8.8	12.0-12.3	15.9-16.3	20-21
t_{ul} , бит	0.201	0.208	0.215	0.225	0.25

P_p , дБм	18.50	19.90	21.05	21.97	22.77
Q	294	241	197	164	139

ТАБЛИЦА 4. Результаты исследований ВОСС с несколькими пролетами

Кол-во УУ ($L_{общ}$, км)	L , км	60	80	100	120
	P_{0m} , мВт	8.7	12	16.2	20.8
	P_p , дБм	19.9	21.07	22.0	22.75
2 УУ	P_{lm} , мВт	8.6	8.4	13	17.4
	t_{ul} , бит	0.21	0.21	0.21	0.22
	Q	171	162	122	79
4 УУ	P_{lm} , мВт	8.2	13.8-14.1	18.4-19.4	19.8-20.8
	t_{ul} , бит	0.21	0.20	0.23	0.24
	Q	125.8	82.5	61.6	45
8 УУ (480- 960 км)	P_{lm} , мВт	7.8-8.3	17.6-19.6	24.5-27	20.2-24.7
	t_{ul} , бит	0.22	0.18	0.19	0.22
	Q	74	62	51	30

Предложенные схемы моделирования и результаты исследований могут быть использованы в лабораторном практикуме кафедры ФилС.

Список используемых источников:

1. Глаголев С. Ф., Горсков В. С., Доценко С. Э. Использование оптических усилителей EDFA для поддержания квазисолитонного режима распространения сигналов по одномодовым волокнам со смещенной дисперсией // АПИНО-21, Т. 1. С. 228-234.
2. Глаголев С. Ф., Горсков В. С., Доценко С. Э. Использование ВКР усилителей для поддержания квазисолитонного режима в одномодовых волокнах со смещенной дисперсией // АПИНО-21: СПбГУТ, Т. 1. С. 234-239.
3. Андреева Е.И., Былина М.С., Глаголев С.Ф. и др. Свойства временных оптических солитонов в оптических волокнах и возможность их использования в телекоммуникациях. Части 1-4 // ТУЗС, 2018-2019. Т. 4, № 1-3. Т. 5, № 1.
4. Агравал Г. Нелинейная волоконная оптика. М.: Мир, 1996. 323 с.

Likov G.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Investigation of the process of maintaining a quasi-soliton mode of pulse propagation in a single-mode fiber with anomalous dispersion.

Report is devoted to the research of the processes of maintaining the quasi-soliton mode of propagation of secant pulses in a single-mode fiber (SMF) with anomalous dispersion and losses. The processes of maintaining the quasi-soliton regime with the help of discrete optical amplifiers (OA) and with the use of an OA based on stimulated Raman scattering (SRS) with counterpumping are considered. The results of theoretical calculations are compared with the results of simulation modeling in the OPTISYSTEM program.

Key words: *single-mode fibers, solitons, chromatic dispersion (CD), nonlinear length, phase modulation (FSM), quasi-soliton mode, Raman amplifier.*

УДК 681.7
ГРНТИ 49.44

ИССЛЕДОВАНИЕ И МОДЕЛИРОВАНИЕ ВОЛОКОННО-ОПТИЧЕСКОГО ДАТЧИКА ТЕМПЕРАТУРЫ И ДЕФОРМАЦИИ НА ОСНОВЕ ВОЛОКОННЫХ РЕШЕТОК БРЭГГА

М. С. Матющенко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе представлена методика расчета спектра отражения волоконной брэгговской решетки с учетом ее зависимости от температуры и деформации. С использованием представленной методики проведено моделирование волоконно-оптических датчиков температуры и деформации. В качестве волокна для записи решетки выбрано стандартное одномодовое волокно. Определена чувствительность датчиков к изменению внешних воздействий.

волоконная брэгговская решетка, брэгговская длина волны, спектр коэффициента отражения, датчик температуры, датчик деформации, моделирование

Для мониторинга технического состояния различных объектов широко применяются волоконно-оптические датчики (ВОД). Наиболее подходящим ВОД для одновременной регистрации изменений температуры и деформации является датчик на основе волоконной брэгговской решетки (ВБР). ВБР записывается в оптическом волокне (ОВ) и представляет собой изменение показателя преломления (ПП) вдоль сердцевины ОВ с некоторым периодом Λ [2]. Принцип действия ВБР объясняется теорией связанных мод.

Центральная длина волны в спектре отражения такой ВБР λ_B определяется условием Брэгга:

$$\lambda_B = 2n_{eff}\Lambda \quad (1)$$

где n_{eff} – эффективный показатель преломления сердцевины ОВ. На длине волны λ_B коэффициент отражения ВБР максимален.

Спектр коэффициента отражения R ВБР зависит от ее длины l и амплитуды модуляции ПП Δn и имеет вид [3]:

$$R(\lambda, l, \Delta n) = \frac{\Omega^2 \cdot \sinh^2(sl)}{\Delta k^2 \cdot \sinh^2(sl) + s^2 \cdot \cosh^2(sl)}, \quad (2)$$

где λ – длина волны, $s^2 = \Omega^2 - \Delta k^2$, Δk – волновой вектор расстройки, Ω – коэффициент связи мод:

$$\Delta k = k - \frac{\pi}{\Lambda} = \frac{2n_{eff}}{\lambda} - \frac{\pi}{\Lambda}, \quad \Omega = \frac{\pi \cdot \Delta n \cdot \eta(V)}{\lambda}. \quad (3)$$

В (2) и (3) k – волновое число, $\eta(V)$ – функция, определяющая процент интенсивности основной моды в сердцевине ОВ, V – нормированная частота.

Для моделирования ВОД было выбрано стандартное одномодовое волокно SMF-28, параметры которого приведены в табл. 1.

Результаты расчета спектров коэффициента отражения представлены на рис. 1 и 2. Из рис. 1 видно, что увеличение длины ВБР приводит к увеличению максимального коэффициента отражения R_{\max} на длине волны λ_B . Из рис. 2 видно, что при уменьшении Δn спектр отражения ВБР той же длины l сужается. Также видно, что при этом уменьшается R_{\max} и для сохранения его величины необходимо увеличивать длину ВБР.

ТАБЛИЦА 1. Параметры SMF-28 и записанной в нем ВБР на длине волны 1550 нм

Эффективный ПП основной моды сердцевины	Радиус сердцевины волокна, мкм	Числовая апертура волокна	Нормированная частота	Период ВБР, нм
1.4682	4.1	0.12	1.994	528

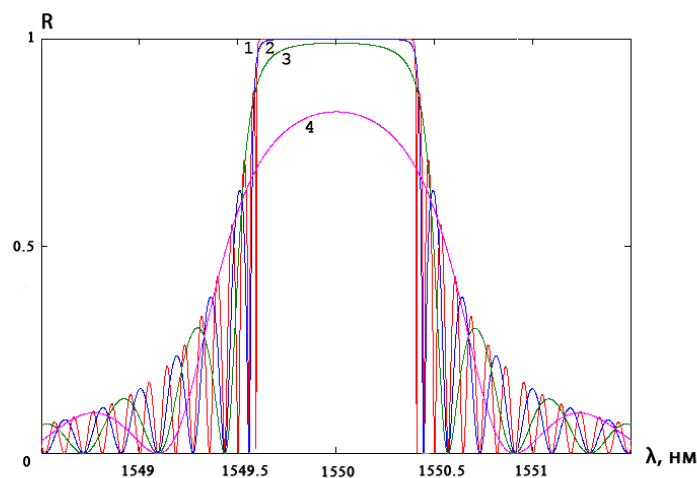


Рис. 1. Спектры отражения ВБР разной длины с одинаковой глубиной модуляции ПП $n=10-3$ (1 – $l=8$ мм, 2 – $l=4$ мм, 3 – $l=2$ мм, 4 – $l=1$ мм)

Таким образом, исходными данными для определения конструкции ВБР можно считать центральную длину волны λ_B в спектре отражения, ширину спектра отражения $\Delta\lambda$ и максимального коэффициент отражения R_{\max} . Можно рекомендовать следующую последовательность выбора параметров ВБР: 1) выбор периода Λ по (1), исходя из заданной λ_B ; 2) Выбор амплитуды модуляции ПП Δn , исходя из заданной $\Delta\lambda$; 3) Выбор длины ВБР, исходя из заданного R_{\max} .

Работа ВБР в качестве ВОД основана на том, что температурные и механические воздействия приводят к изменению Λ и n_{eff} , то есть в соответствии с (1), приводят к смещению центральной длины волны λ_B в спектре отражения. Для сдвига λ_B из-за изменения температуры ΔT и удлинения Δl справедливо выражение, следующее из (1) [3]:

$$\Delta\lambda_B = 2 \left(\Lambda \cdot \frac{\partial n_{eff}}{\partial l} + n_{eff} \cdot \frac{\partial \Lambda}{\partial l} \right) \Delta l + 2 \left(\Lambda \cdot \frac{\partial n_{eff}}{\partial T} + n_{eff} \cdot \frac{\partial \Lambda}{\partial T} \right) \Delta T. \quad (4)$$

Таким образом, отслеживая длину волны брэгговского отражения λ_B , можно измерять параметры внешнего воздействия.

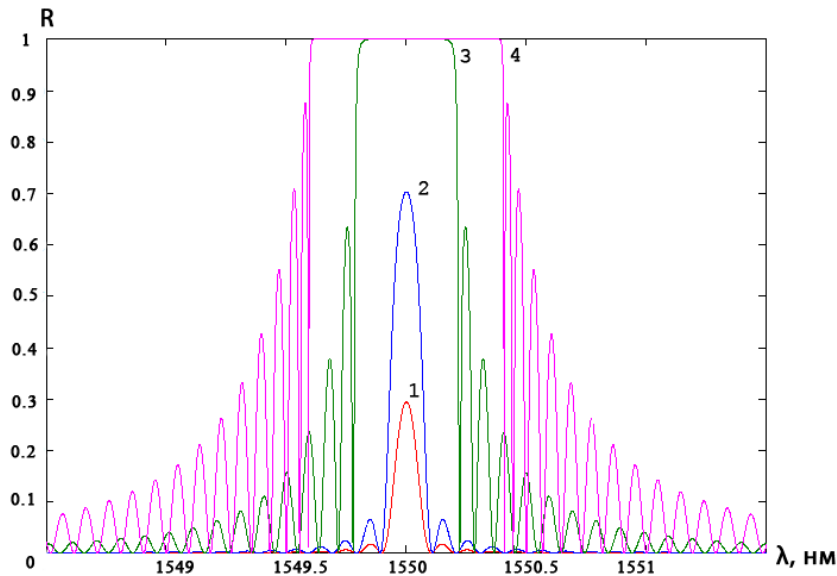


Рис. 2. Спектры отражения ВБР длиной $l = 8$ мм с разной глубиной модуляции ПП (1 – $\Delta n = 0.5 \cdot 10^{-4}$, 2 – $\Delta n = 10^{-4}$, 3 – $\Delta n = 0.5 \cdot 10^{-3}$, 4 – $\Delta n = 10^{-3}$)

Первый член в (4) учитывает изменение Λ и n_{eff} вследствие упрягооптического эффекта [3]:

$$\Delta\lambda_B = \lambda_{B0}(1 - p_e)\varepsilon(z) = \lambda_{B0} \left(1 - \frac{n_{eff}^2}{2} [p_{12} - \nu(p_{11} + p_{12})] \right) \varepsilon(z) \quad (5)$$

где p_e – эффективная упрягооптическая составляющая, p_{11} и p_{12} – компоненты тензора, ν – коэффициент Пуассона для кварцевого стекла, $\varepsilon(z) = \frac{\Delta l}{l}$ – относительное удлинение ОВ. Из (5) можно получить механическую чувствительность ВБР:

$$\frac{\partial\Delta\lambda_B}{\partial\varepsilon(z)} = \lambda_B(1 - p_e), \quad (6)$$

Для стандартного одномодового ОВ с параметрами $p_{11} = 0,113$, $p_{12} = 0,252$, $\nu = 0,17$, $n_{eff} = 1,4826$ на длине волны $\lambda_B = 1550$ нм при $\varepsilon(z) = 10^{-6}$ получаем: $\frac{\partial\Delta\lambda_B}{\partial\varepsilon(z)} = \lambda_B(1 - p_e) = 1.33$ пм. На рис. 3 представлена зависимость λ_B от деформации.

Сравнивая рассчитанную зависимость с экспериментальными данными, приведенными в [3, 5], можно сделать вывод, что и на практике механическая чувствительность ВБР имеет линейную зависимость от удлинения. Однако качество ВБР как датчика деформации определяется не только ее параметрами, но в большей степени физическими свойствами ОВ, в котором она записана.

На рис. 4 представлены спектры отражения ВБР, рассчитанные при разных значениях деформации. Видно, что смещение λ_B достаточно для измерения величины удлинения ОВ.

Второй член в (4) описывает влияние температурного расширения кварцевого стекла. Смещение $\Delta\lambda_B$ при изменении температуры [3]:

$$\Delta\lambda_B = \lambda_{B0} \left(\frac{\partial\lambda}{\partial T \cdot \lambda} + \frac{\partial n}{\partial T \cdot n} \right) \Delta T = \lambda_{B0} (\alpha + \xi) \Delta T. \quad (7)$$

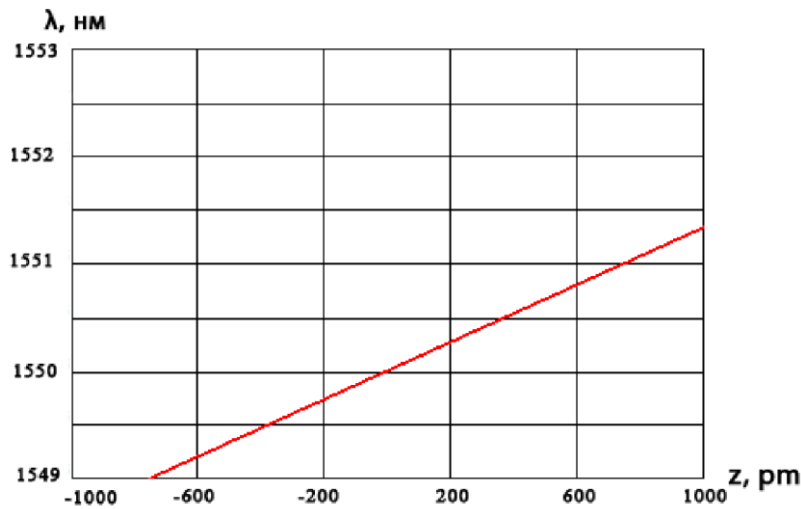


Рис. 3. Зависимость длины волны резонанса решетки от деформации

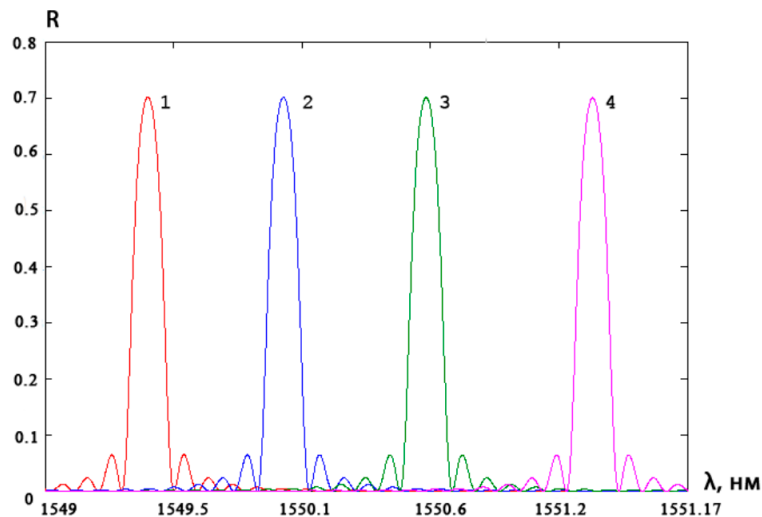


Рис. 4. Семейство спектров отражения для разных значений деформации (1 – $z = -500$ пм, 2 – $z = 0$, 3 – $z = 500$ пм, 4 – $z = 1000$ пм)

где α – температурный коэффициент расширения сердцевины волокна, ξ – термооптический коэффициент. Из (7) можно получить температурную чувствительность решетки:

$$\frac{\partial\Delta\lambda_B}{\partial T} = \lambda_B (\alpha + \xi), \quad (8)$$

Согласно справочной литературе для кварца $\alpha = 0,55 \cdot 10^{-6}$, а термооптический коэффициент для ОВ с добавками германия $\xi = 8,6 \cdot 10^{-6}$. Таким образом, из (8) при $\lambda_B = 1550$ нм получаем $\frac{\partial\lambda_B}{\partial T} = 14,2$ пм/°С.

Сравнивая рассчитанную зависимость с экспериментальными данными, приведенными в [1, 3], можно сделать вывод, что на практике температурная

зависимость также имеет линейный характер в пределах погрешности до определенных высоких температур [4], индивидуальных для каждого волокна и типа записанной в нем ВБР.

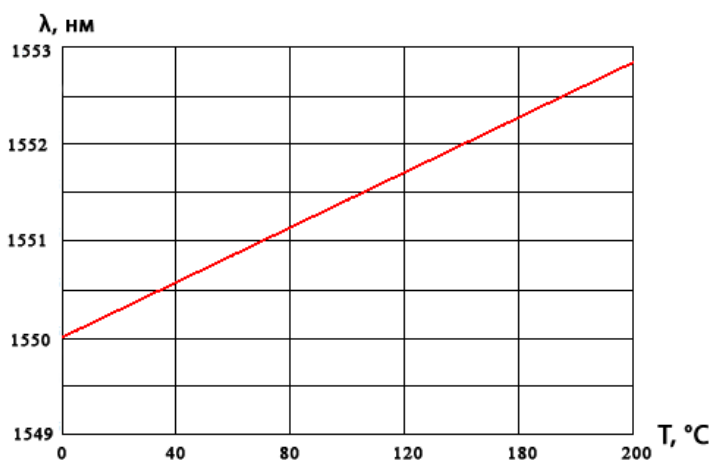


Рис. 5. Зависимость длины волны резонанса ВБР от температуры

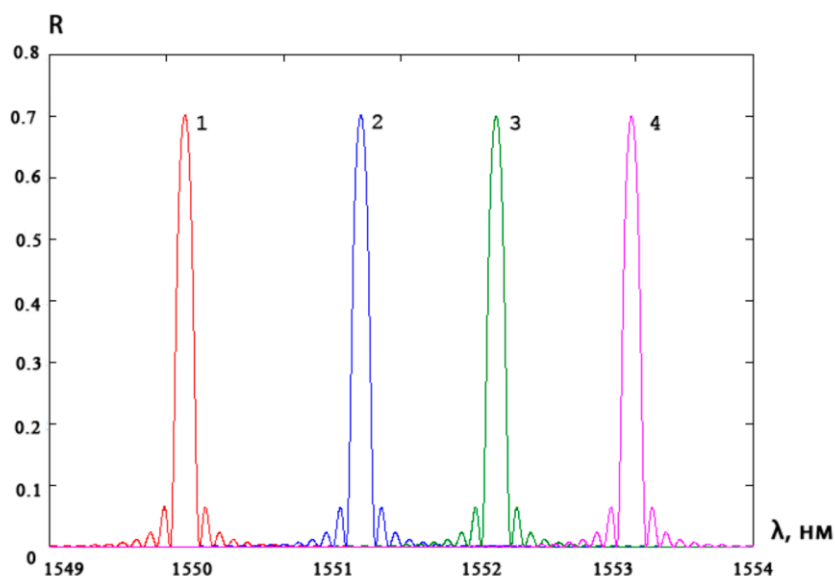


Рис. 6. Семейство спектров отражения для разных значений температуры (1 – $T = 0\text{ }^{\circ}\text{C}$, 2 – $T = 80\text{ }^{\circ}\text{C}$, 3 – $T = 150\text{ }^{\circ}\text{C}$, 4 – $T = 240\text{ }^{\circ}\text{C}$)

Проведенные расчеты показали, что ВОД на основе ВБР в SMF-28 могут использоваться в качестве датчиков температуры и деформации с чувствительностью 1.33 пм и 14.2 пм/°C.

Список используемых источников:

1. Беспрозванных В.Г., Зырянов С.В. Влияние корпусировки волоконной брэгговской решетки на температурную стабильность широкополосного источника излучения // Инновационная наука. 2015. – №11. – С. 24-27.
2. С.А. Васильев, И.О. Медведков, И.Г. Королев, А.С. Божков, А.С. Курков, Е.М. Дианов. Волоконные решетки показателя преломления и их применение // Квантовая электроника. – 2005. – Т. 35, № 12. – С. 1085–1103.
3. С.В. Варжель, Волоконные брэгговские решетки. – СПб: Университет ИТМО, 2015. – 65 с.

4. Леко В. К., Мазурин О. В. Свойства кварцевого стекла. — Л.: Наука, 1985. — 166 с.

5. В.В. Махсидов, Л.А. Кашарина, А.А. Евдокимов, А.Е. Раскутин. Применение волоконных брэгговских решеток для определения деформации авиационных и строительных конструкций из полимерных композиционных материалов // Прикладная фотоника. – 2017. – Т. 4, № 4. – С. 263-268.

Matyushchenko M.

The Bonch-Bruевич St. Petersburg State University of Telecommunications

Investigation and modeling of a fiber-optic temperature and strain sensor based on fiber Bragg gratings.

The paper presents a method for calculating the reflection spectrum of a fiber Bragg grating, taking into account its dependence on temperature and strain. Using the presented technique, modeling of fiber-optic temperature and strain sensors was carried out. A standard single-mode fiber was chosen as the grating recording fiber. The sensitivity of sensors to changes in external influences is determined.

Key words: *fiber Bragg grating, Bragg wavelength, reflectance spectrum, temperature sensor, strain sensor, modeling.*

УДК 681.335
ГРНТИ 47.35.41

ИССЛЕДОВАНИЕ РАЗЛИЧНЫХ СТАНДАРТОВ ОПТИЧЕСКИХ 100G ТРАНСИВЕРОВ

И. Н. Медведев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В связи со значительным увеличением объема передаваемой информации, в последние годы все чаще встает проблема экономически выгодной передачи данных со скоростями 100 Гбит/с и выше. На сегодняшний день разработаны и применяются различные варианты организации высокоскоростных сетей, при этом каждый вариант имеет как свои преимущества, так и недостатки. В данной статье рассмотрены основные технологии 100G приемопередатчиков, их сравнительные характеристики и сферы применения.

трансивер, 100G, Ethernet, ВОЛС, xWDM

Прародителем 100-Гигабитных приемопередатчиков можно назвать модуль CFP SR10/LR10 (Short Range и Long Range, соответственно). Это приемопередатчик формата CFP, передача информации в котором осуществлялась с помощью 10 независимых каналов. Одним из недостатков такого модуля являлся его размер, который ограничивал возможность более плотной установки модулей в шасси, и соответственно ограничивал ресурс сети. Также, одним из недостатков было большое энергопотребление. В следующих поколениях 100-Гигабитных приемопередатчиков использовались более компактные форм-факторы, такие как CFP2 и CFP4. На сегодняшний день, самым популярным и массово производимым форм-фактором является QSFP28. На рис. 1 показано наглядное сравнение вышеуказанных форм-факторов.



Рис. 1. Форм-факторы современных оптических трансиверов

Наиболее популярным стандартом, описывающим взаимодействие на скоростях 100 Гбит/с, является 100G Ethernet. Семейство стандартов 100G Ethernet описывается следующим образом: для примера можно взять 100GBASE-SR4, где 100GBASE описывает скорость 100Гбит/с, SR является условным обозначением дальности передачи, «4» означает передачу и прием по четырем независимым линиям.

Одним из самых популярных и экономически выгодных решений для обеспечения связи между оборудованием в пределах ЦОД или Дата-центра являются модули стандарта 100GBASE-SR4. Как можно понять из описания

стандарта (Short Reach), данный тип модулей применяется для работы на коротких расстояниях, порядка 150 метров. Длина волны лазера, как и у менее скоростных многомодовых модулей: 850нм. Особенностью данных модулей является коннектор, который представлен не стандартным двухволоконным интерфейсом, а интерфейсом MPO, в котором расположен массив отдельных волокон. Схема коннектора MPO представлена на рис. 2. Таким образом, в модулях 100GBASE-SR4 передача осуществляется по 8 независимым волокнам, что позволяет соединять один 100G модуль с четырьмя 25G, при помощи специальной MPO-кассеты.

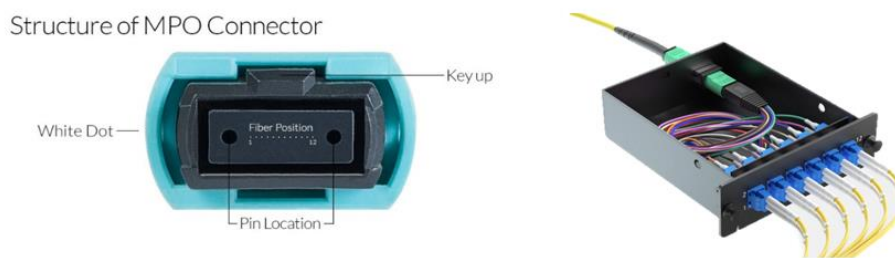


Рис. 2. MPO коннектор (слева) и MPO кассета (справа)

Следующий тип приемопередатчиков – это 100GBASE-LR4. Стандарт LR (Long Reach) означает возможность передачи данных на расстояние порядка 10 - 20км. Данные приемопередатчики имеют стандартный оптический duplex LC интерфейс, однако, поскольку номенклатура все еще содержит в себе «4», можно понять, что в данных модулях также используется 4 независимых канала передачи. Добиться передачи по двум волокнам вместо восьми позволило применение мультиплексора и демультиплексора в конструкции модуля, как показано на схеме на рис. 3. Длины волн стандарта 100GBASE-LR4 находятся во втором окне прозрачности (O-диапазоне). Этот диапазон был выбран как основной для передачи на скоростях 100Гбит/с, поскольку хроматическая дисперсия для сигналов 1300 в стандартном волокне G.652D равна нулю [1]. Длины волн стандарта LR4, на которых ведется передача и прием: 1295.56нм, 1300.05нм, 1304.58нм, 1309.14нм.

Схожим принципом работы обладают приемопередатчики стандарта 100G-CWDM4. Отличие состоит в том, что длины волн, используемые в данном стандарте, соответствуют волновому плану CWDM (1270 нм, 1290 нм, 1310 нм, 1330 нм).

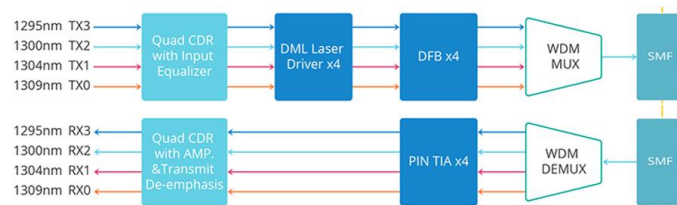


Рис. 3. Структурная схема приемопередатчика с четырьмя каналами

Продолжением развития стандарта 100GBASE-LR являются стандарты 100GBASE-ER/ZR. Волновой план остался таким же, как и в стандарте LR. Отличие от стандарта LR кроется в компонентной базе этих устройств.

Приемопередатчики типа ER оснащены охлаждаемыми EML лазерами, а также более чувствительными фотоприемниками, что позволяет увеличить оптический бюджет и, соответственно, дальность передачи. Приемопередатчики стандарта 100GBASE-ZR предназначены для передачи данных по одномодовому оптическому волокну на расстояние до 80км. Данные модули помимо прочего оснащаются функцией FEC, которая позволяет исправлять ошибки, чтобы достичь нужного значения BER при передаче на большие расстояния.

Совершенно другим подходом к высокоскоростным приемопередатчикам является использование стандарта PAM4. Цифра «4» в названии стандарта указывает не на количество каналов передачи, а на количество уровней при модуляции. PAM4 – это технология, кодирующая два бита данных четырьмя различными уровнями сигнала, как показано на рис. 4. Это удваивает полосу пропускания, каждый уровень сигнала представляет 2 бита логической информации.

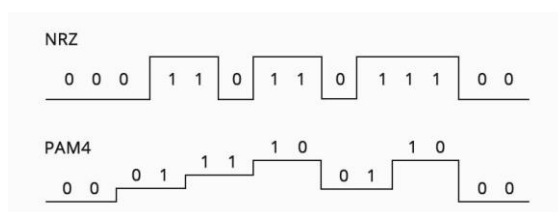


Рис. 4. Модуляция NRZ и PAM4

Методы модуляции PAM4 применяются в 100G-DWDM приемопередатчиках. Оптические модули PAM4 могут использоваться непосредственно в коммутаторах DWDM, что является простым решением для создания сетей высокой емкости. Однако недостатком этого решения является то, что 100G DWDM QSFP28 PAM4 требует использования усилителей и компенсаторов дисперсии, когда расстояние передачи превышает 5 км, что приводит к высоким затратам на построение линии. Более того, показатель dispersion tolerance у этих модулей крайне низок, поэтому не во всех случаях можно использовать стандартные модули компенсации с эквивалентной длиной 20 – 120 км [3]. Во многих проектах будут необходимы DCM с нестандартной эквивалентной длиной, например 42 км или 58 км, следовательно, при построении такой сети нужно использовать либо перестраиваемые DCM, либо делать DCM нестандартной длины.

Подводя итоги, можно сказать, что найти универсальный оптический приемопередатчик невозможно. Каждая технология была создана, чтобы закрыть определенные потребности в определенной области телекоммуникаций. Так, например, для коротких расстояний от 5 до 100 метров наилучшим решением будут модули стандарта SR4. Для соединений среднего радиуса действия, от 100 до 2 км, модули PSM4 и CWDM4 могут предложить экономически эффективные решения. Они могут поддерживать до 500 метров по одномодовому оптоволоконному кабелю MTP с 12 волокнами и до 2 км по одномодовому оптоволоконному кабелю LC соответственно. Для передачи до

10, 40 и 80 километров в одном пролете без усилителей идеально подойдут модули 100GBASE-LR4/ER4/ZR4 соответственно. Для организации 100-Гигабитной сети DWDM можно использовать приемопередатчик стандарта RAM4 или же системы с когерентным приемом.

Список используемых источников:

1. IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force. official web site. IEEE. June 19, 2010. Retrieved June 24, 2011
2. А.Н. Gnauck, et al., High-capacity optical transmission systems, J. Lightw. Technol., vol. 26, no. 9
3. Overview of Requirements and Applications for 40 Gigabit and 100 Gigabit Ethernet <http://www.ethernetalliance.org>
4. Родина, О.В. Волоконно-оптические линии связи. Практическое руководство / О.В. Родина. - М.: Горячая линия - Телеком, 2012

Medvedev I.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Different standards of 100G optical transceivers.

In connection with a significant increase in the amount of transmitted information, in recent years, the problem of cost-effective data transmission at speeds of 100 Gbps and higher has become more and more frequent. To date, various options for organizing high-speed networks have been developed and are being used, and each option has both its advantages and disadvantages. This article discusses the main technologies of 100G transceivers, their comparative characteristics and applications.

Key words: *transceiver, 100G, Ethernet, FOCL, xWDM.*

УДК 535.015
ГРНТИ 29.31.15

РАЗРАБОТКА МИКРОСТРУКТУРИРОВАННОГО ОПТИЧЕСКОГО ВОЛОКНА С ЗАДАНЫМ МОДАЛЬНЫМ СОСТАВОМ

В. М. Пилипова, В. В. Давыдов, Д. С. Дмитриева, Г. А. Пчелкин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Экспериментально обоснована необходимость использования маломодовых микроструктурированных оптических волокон с наведенной продольной скруткой. Изготовлены и исследованы опытные образцы микроструктурированных оптических волокон для изучения квази-кольцевого распределения оптического поля в поперечном сечении. Представлены результаты экспериментальных исследований оптического элемента с 6 сердцевинами, дана оценка зависимости базовых характеристик от параметров технологического цикла его производства.

микроструктурированное оптическое волокно, сердцевина, лазерное излучение, киральность

В настоящее время потребность в передаче больших объемов информации постоянно возрастает [1]. Это необходимо как при проведении экспериментов, так и в различных системах навигации и связи. Возрастают требования к скорости передачи и качеству обработки информации. Волоконно-оптические линии связи являются одним из наиболее надежных способов реализации этих задач, особенно в сложных условиях [2]. В современных конструкциях одномодовых оптических волокон для магистральных линий связи практически достигнут предел возможностей передачи больших объемов информации с использованием различных уплотнений и компрессий, поэтому в данном направлении ведутся работы по поиску новых решений [3-4].

В настоящее время скрученные микроструктурированные оптические волокна (МОВ) рассматриваются как новые волоконно-оптические элементы с большим потенциалом для различных применений как в волоконно-оптических датчиках/сенсорных сетях, так и в телекоммуникациях [4].

В этой работе представлены изготовленные МОВ из скрученного кварца со специальной геометрией ядра, легированными GeO_2 , ступенчатым профилем показателя преломления, внешним диаметром 125 мкм, работающим в маломодовом режиме и индуцированной киральностью с закручиванием 1000 оборотов в минуту (или, например, при скорости волочения ~ 2 м в минуту ~ 500 оборотов на 1 м).

Для регистрации вихревых распределений оптического поля в маломодовых микроструктурированных оптических волокнах с 6 сердцевинами из высоколегированного кварцевого стекла GeO_2 был модифицирован измерительный стенд. Используемая ранее оптическая схема имела большие габариты, чрезмерные потери при пропускании излучения и повышенные требования к температурной стабилизации.

На рис. 1 представлены топологии маломодовых микроструктурированных оптических волокон, для которых исследовано распределение оптического излучения на выходе при различных частотах скрутки и других параметрах технологического цикла.

Конструкция изготовленного микроструктурированного оптического волокна с 6 ядрами показана на рис. 1. Ожидается, что эта геометрия в сочетании с индуцированной киральностью, улучшит модальную стабильность. Была изготовлена заготовка со ступенчатым профилем показателя преломления, отношение диаметров сердцевин и самой заготовки составляло 0,4 (рис. 2). Геометрия изготовленного МОВ уменьшена до внешнего диаметра 125 мкм, что является типичным диаметром оболочки для обычных имеющихся в продаже телекоммуникационных оптических волокон, чтобы упростить последующее подключение к измерительному оборудованию.

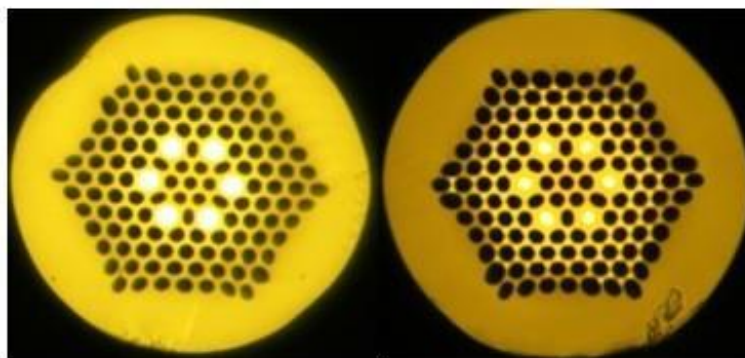


Рис. 1. Изображения поперечных сечений микроструктурированных волокон с 6 сердцевинами.

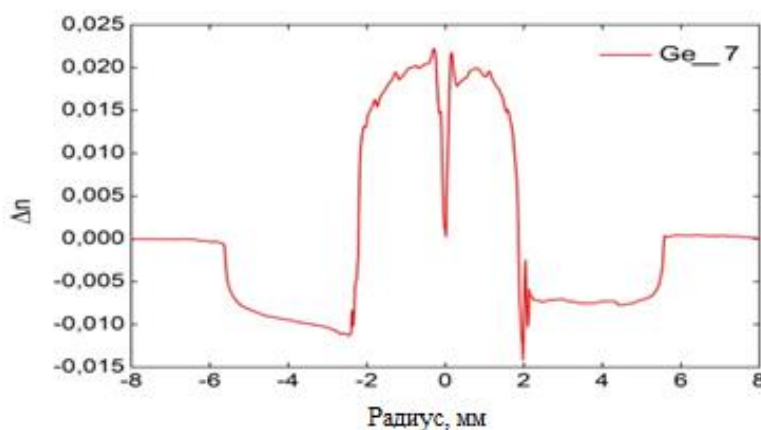


Рис. 2. Заготовки для капиллярных сердечников с радиальным распределением профиля показателя преломления стержневой заготовки со ступенчатым профилем показателя преломления.

На рис. 3 в качестве примера представлено продольное сечения киральных микроструктурированных волокон с 6 сердцевинами. Для них были проведены исследования модового распределения оптического излучения при различной частоте скручивания ω_c и других параметрах технологического цикла.



Рис. 3. Изображение продольного сечения микроструктурированного волокна с 6 сердцевинами.

На рис. 4 в качестве примера представлены распределения оптического излучения на выходе из микроструктурированного волокна исследуемой топологии.

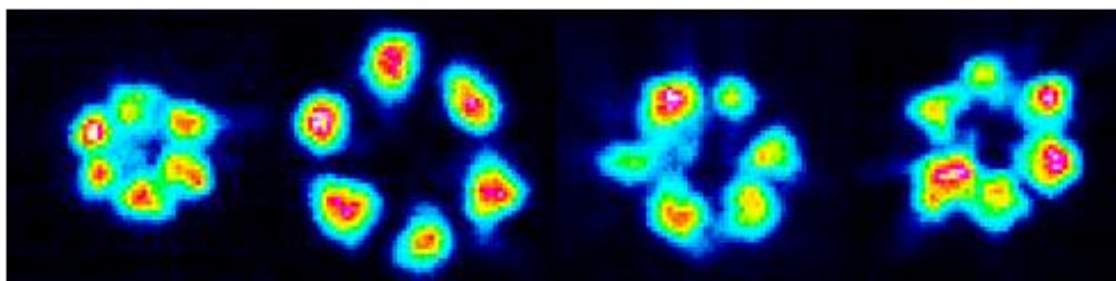


Рис. 3. Изображения поперечных сечений модового распределения в микроструктурированных волокнах с 6 сердцевинами.
(а - 50 об/мин, б - 100 об/мин, с - 400 об/мин, д - 500 об/ мин)

Анализ представленных данных показывает, что распределение оптического излучения носит квази-кольцевой и неравномерный характер. Это распределение можно контролировать.

Таким образом, были приведены некоторые результаты испытаний опытных образцов спроектированных и изготовленных микроструктурированных оптических волокон, в том числе их геометрические параметры, основные характеристики передачи, а также измерения профилей лазерного луча в дальней зоне. Детальное исследование свойств МОВ в различных измерениях/датчиках и/или лазерных системах, телекоммуникациях и т.д. требует проведения дополнительной серии тестов и экспериментов в будущих работах.

Список используемых источников:

1. Myazin N. S., Dudkin V. I., Grebenikova N. M., Davydov R. V., Podstrigaev A. S. Fiber - optical system for governance and control of work for nuclear power stations of low power // Lecture Notes in Computer Science. - 2019. - №11660. - С. 744-756.
2. Semenov V. V., Nikiforov N. F., Ermak S. V Calculation of stationary magnetic resonance signal in optically oriented atoms induced by a sequence of radio pulses // Soviet journal of Communications Technology and Electronics. - 1991. – Vol.36(4). - P. 59-63.

3. Grevtseva A. S., Dmitriev R. A The use of digital data processing to improve the metrological characteristics of the rubidium frequency standa // Conference Series. - 2021. – Vol.2086(1) – 012070
4. Dudkin V.I., Velichko E.N., Karseev A.Yu Fiber-optic system for simulating accidents in the cooling circuits of a nuclear power plant // Journal of Optical Technology. - 2015. – Vol.82(3). - P. 132-135.
5. Burdin V.A., Dashkov M.V., Demidov V.V., Zhukov A.E., Bourdine A.V. New silica laser-optimized multimode optical fibers with extremely enlarged 100- μm core diameter for gigabit onboard and industrial networks // Fibers. - 2020. – Vol.8(3). - P. 18.

Pilipova V., Davydov V., Dmitrieva D., Pchelkin G.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development of a microstructured optical fiber with a given modal composition. The necessity of using low-mode microstructured optical fibers with induced longitudinal twisting is experimentally substantiated. Prototypes of microstructured optical fibers were fabricated and studied to study the quasi-annular distribution of the optical field in the cross section. The results of experimental studies of an optical element with 6 cores are presented, an assessment is made of the dependence of the basic characteristics on the parameters of the technological cycle of its production.

Key words: microstructured optical fiber, core, laser radiation, chirality.

УДК 535.015
ГРНТИ 47.13.07

ПРИМЕНЕНИЕ КИРАЛЬНЫХ МИКРОСТРУКТУРИРОВАННЫХ ОПТИЧЕСКИХ ВОЛОКОН В СЕНСОРНЫХ ПРИЛОЖЕНИЯХ

А. Н. Подопригора

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Разнообразные датчики измерения физических возмущений являются важнейшими компонентами промышленности и не только. Их работа основана на различных явлениях, технологиях и предназначаются они для множества применений в человеческой жизнедеятельности. За последние несколько десятилетий волоконно-оптические датчики получили широкое распространение из-за их выдающихся преимуществ. В работе представлены результаты экспериментальных исследований характеристик изготовленных опытных образцов длин кварцевых киральных микроструктурированных оптических волокон с шестью германатными стержнями.

спектр потерь, киральные микроструктурированные оптические волокна, сенсорные устройства, метод термической постобработки, формование преформы

Поведение света в киральных структурах продолжает вызывать большой интерес, и в различных разделах фотоники появляется множество приложений. Примеры включают оптическую активность в биологических молекулах, генерацию в холестерических жидких кристаллах, киральные метаматериалы, скрученные микроструктурированные (фотонно-кристаллические) волокна.

Киральное микроструктурированное волокно состоит из единственной одноосной хиральной единицы, содержащей одно или несколько светопроводящих ядер, бесконечно протяженных в третьем измерении в направлении крутки – распространения оптического излучения. В своей наиболее распространенной форме данный тип волокна состоит из гексагональной матрицы полых или заполненных определенным материалом микроканалов, капилляров, проходящих по длине стеклянной нити. При непрерывном закручивании по всей длине он принимает вид так называемой «мультиспирали».

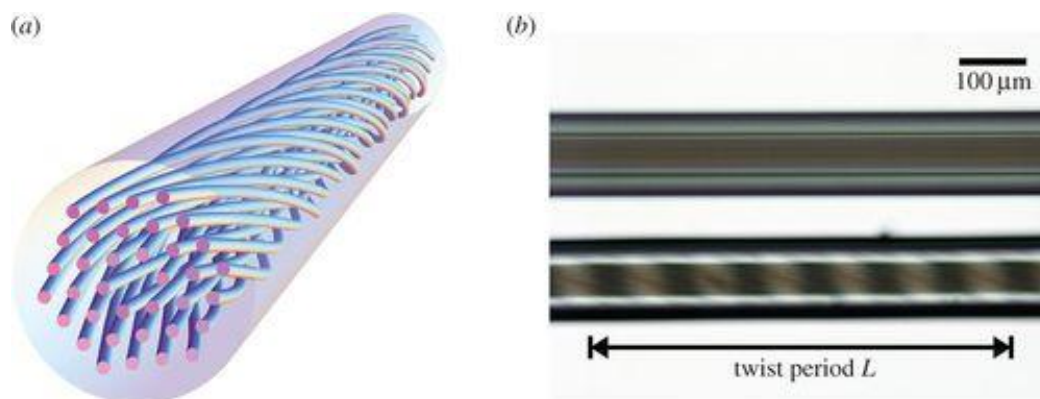


Рис. 1. а) эскиз кирального микроструктурированного волокна б) вид с боку

Для изготовления скрученных киральных волокон используются два основных метода: термическая постобработка нескрученного волокна и формование преформы во время вытягивания волокна.

Метод термической постобработки впервые была предложена в 1998 году и после многократно модернизирована. Он заключается в том чтобы CO₂-лазер нагревает волокно до размягченного состояния, в то время как два моторизованных прецизионных вращающихся держателя волокна могут вращаться в противоположных направлениях, таким образом изготавливая структурно-индуцированный HLPG. Эта решетка образуется путем скручивания волокна по спиральной траектории.

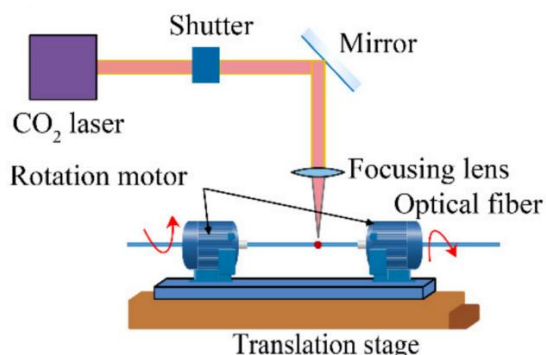


Рис. 2. Экспериментальная установка для закрутки волокон

Более длинные отрезки непрерывно скрученных волокон также могут быть изготовлены путем вращения преформы во время вытягивания волокна. Это влечет за собой использование двигателя, вращающегося со скоростью несколько тысяч оборотов в минуту, и вращающегося соединения с несколькими впускными отверстиями для регулирования давления внутри полых каналов. Тогда период скручивания вытянутого волокна равен скорости вытягивания волокна, деленной на скорость вращения преформы. Микроструктуру можно точно оптимизировать за счет активной регулировки давления во время вытяжки.

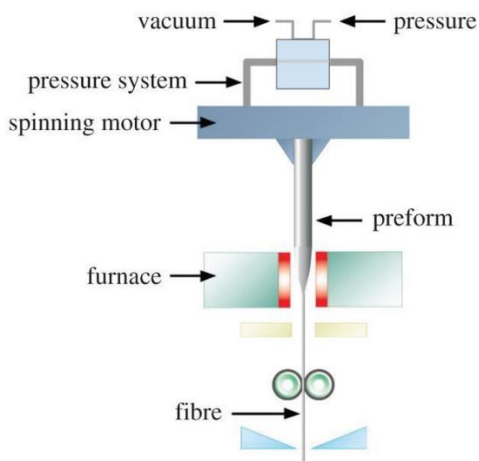


Рис. 3. Эскиз вращения волокнистой заготовки в процессе вытяжки в башне для вытягивания волокна

В структуре киральных волокон существует периодичность в стекловолокне, это позволяет расширить их функциональные возможности, а, именно, представляется полезным в различных фильтрах, поляризаторах, сенсорных и лазерных приложениях. Был проведен эксперимент на определение потенциальной возможности применения опытного образца в датчике кручения. Он заключался в нахождении спектра пропускания оптического волокна в момент его поворота на ± 90 градусов, то есть оптическое волокно закреплялось на входе неподвижно (входные условия для каждого случая оставались постоянными) и вращалось оно в круг своей оси на выходе. В данном опыте использовались киральные микроструктурированные оптические волокна с шесть германатными стержнями изготовленные в государственном оптическом институте (ГОИ).

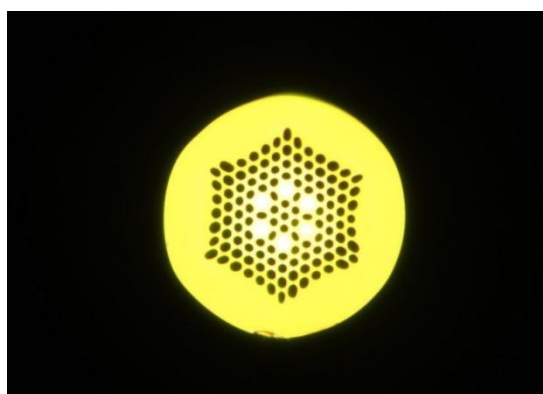


Рис. 4. Скол используемого волокна

В результате эксперимента было получено, что при повороте оптического волокна вокруг своей оси его спектр смещался.

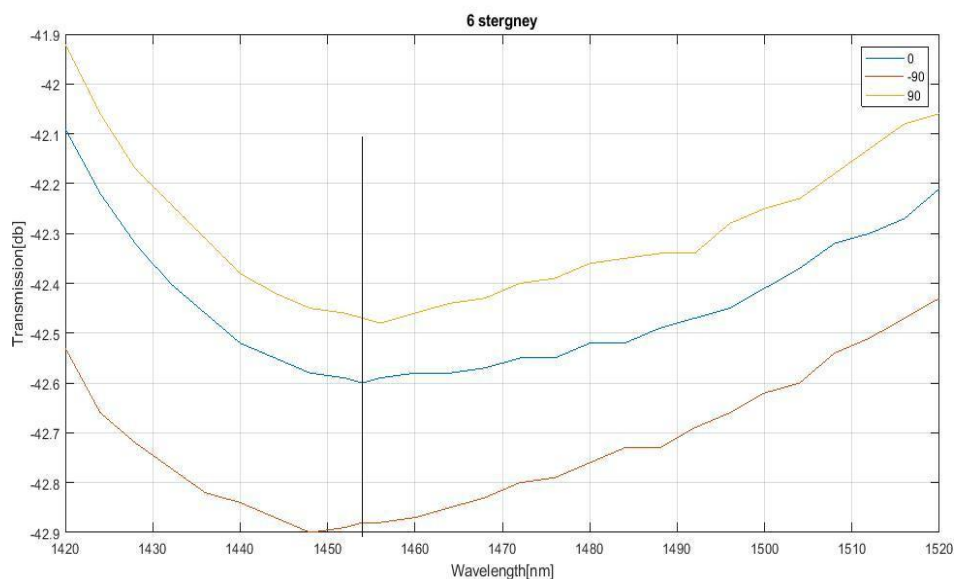


Рис. 5. Картина спектров потер полученных в результате эксперимента

Полученные результаты проведённой серии экспериментальных исследований пилотных образцов световодов демонстрируют принципиальную

возможность практической реализации применения киральных микроструктурированных волокон в датчиках кручения.

Список используемых источников:

Study of the characteristics of few-mode microstructured optical fibers with 6 cores made of highly doped GeO₂ silica and induced chirality / G. A. Pchelkin, V. I. Demidov¹, A. V. Bourdine [и др.].

1. Chao, Ma Review of Helical Long-Period Fiber Gratings / Ma Chao, Wang Jian, Yuan Libo. // Photonics . — 2021. — № 8. — С. 193.

2. Hua, Zhao Advances on Mode-Coupling Theories, Fabrication Techniques, and Applications of the Helical Long-Period Fiber Gratings: A Review / Zhao Hua, Li Hongpu. // Photonics . — 2021. — № 8(4). — С. 106.

3. P, St,J Helically twisted photonic crystal fibres / St,J P, Beravat,and,G,K,L R. // Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. — 2017. — № 2087. — Том. 375.

Podoprigora A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Application of chiral microstructured optical fibers in sensor applications.

A variety of sensors measuring physical disturbances are essential components of industry and beyond. Their work is based on various phenomena, technologies and they are intended for many applications in human life. Over the past few decades, fiber optic sensors have been widely used due to their outstanding advantages. The paper presents the results of experimental studies of the characteristics of the manufactured prototype lengths of quartz chiral microstructured optical fibers with six germanate rods.

Key words: *loss spectrum, chiral microstructured optical fibers, sensor devices, thermal post-processing method, preform molding.*

УДК 681.7.08
ГРНТИ 49.29.14

ПРОЕКТИРОВАНИЕ, СБОРКА, НАСТРОЙКА И ПРИЕМОСДАТОЧНЫЕ ИСПЫТАНИЯ МОДЕЛИ DWDM ЛИНИИ

А. А. Поздняков, О. О. Шоргин, П. В. Свинтуховский

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье в соответствии с техническим заданием спроектирована волоконно-оптическая сеть связи между Шлиссельбургом и Санкт-Петербургом. Рассмотрены структурная ситуационная и канальная схемы проектируемой линии. Приведен расчет энергетического бюджета линии, проведены приемо-сдаточные испытания.

ВОЛС, волоконно-оптические линии связи, DWDM, техническое задание, OSNR, BER, энергетический бюджет

Введение. В проектировании крайне важно правильно подобрать параметры и характеристики волоконно-оптической линии для ее надежной и продолжительной работы.

Поэтапное выполнение задач проектирования, сборки, настройки будет рассмотрено в данной рукописи.

Техническое задание. Требуется организовать связь типа точка-точка, между Шлиссельбургом и Санкт-Петербургом, длина линии 80 км, требуется реализовать:

3 канала 10 Гбит/с: 1552.52 нм (N31), 1537.4 (N50), 1546.92 nm (N38)

1 канал 2.5 Гбит/с 1550.92 (N33) 1557.36 (N25) с резервированием

Служебный канал 1510 нм(без усиления)

Требуемый эксплуатационный запас 3дБ, и BER на стороне клиента равный 10^{-12} . Используемое волокно G.652.

Разработка структурной, ситуационной и канальной схем.

Ситуационная схема - схема, которая показывает примерную трассу прокладки кабеля. Для разработки структурной схемы исходными данными служит онлайн-сервис карт OpenStreetMap [1]. Разработанная ситуационная схема представлена на рис. 1.

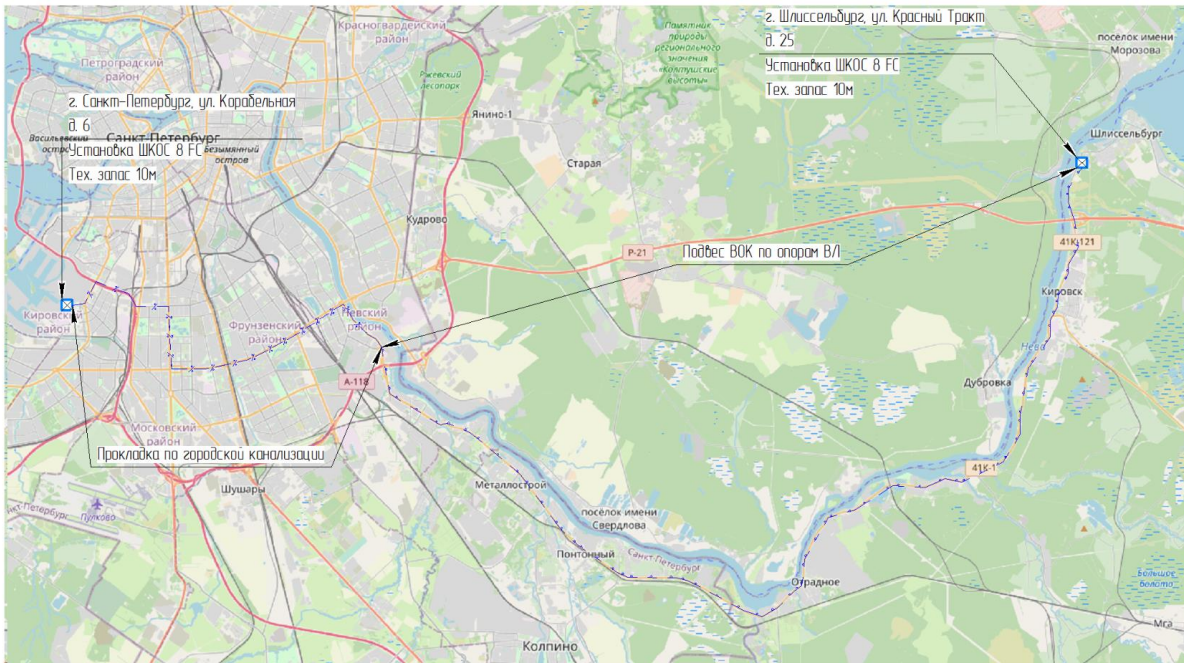
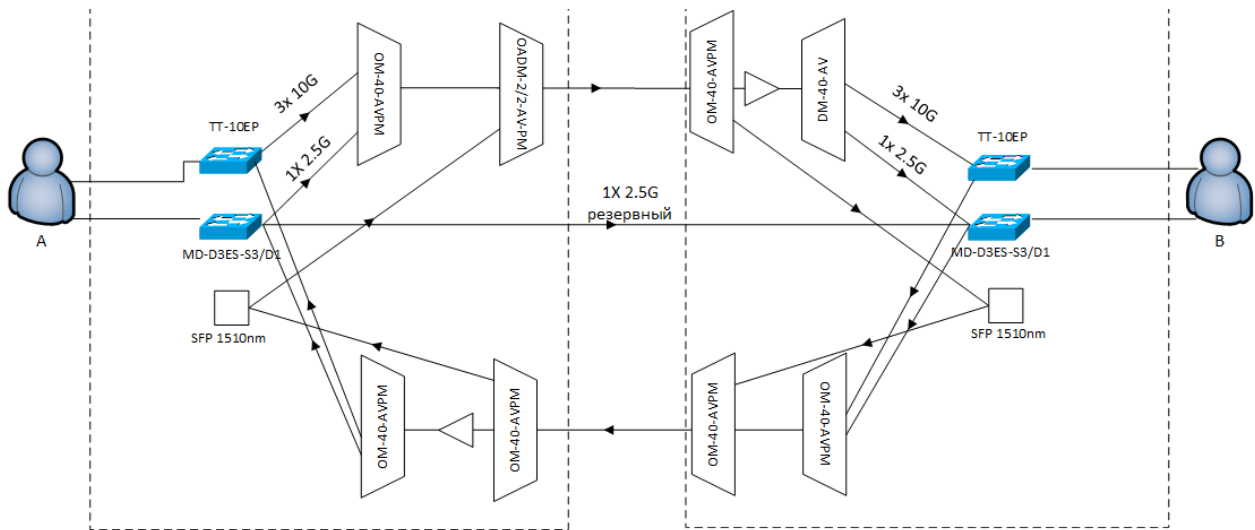


Рис. 1. Ситуационная схема

Структурная схема - схема которая показывает структуру DWDM линии. Исходные данные для разработки схемы содержатся в ТЗ. Схема показана на рис. 2.



Проектная длина
линейного участка: 80 км

Рис. 2. Структурная схема

Канальная схема - показывает соединение каналов в линии DWDM. Исходные данные для разработки схемы содержатся в ТЗ. Схема показана на рис. 3.

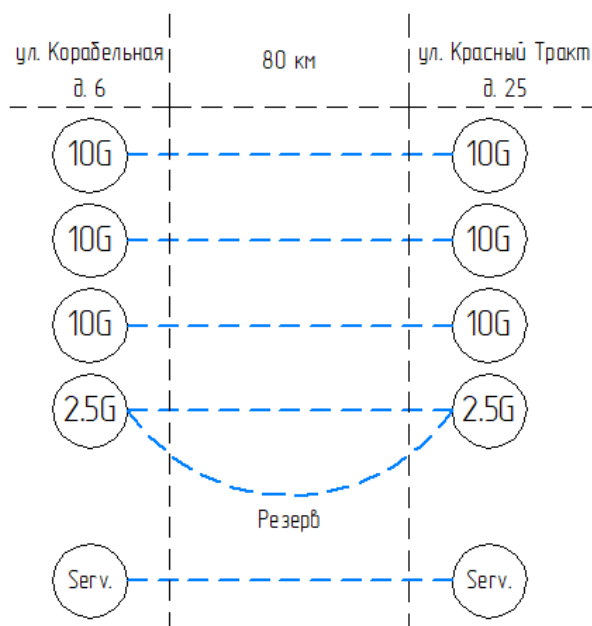


Рис. 3. Канальная схема

Расчет энергетического бюджета, регенерационного участка по дисперсии. Расчеты параметров системы сделаны в соответствии с [2]. Исходные данные для расчетов приведены в таблице.

ТАБЛИЦА 1. Спецификация используемого оборудования

№	Модель оборудования	Спецификация	Количество
1	Транспондер ТТ-10ЕР	Блок 10 транспондеров для передачи 10 независимых 10G сигналов	2
2	Мультиплексор MD-D3ES-S3/D1	Блок двух независимых агрегаторов. В каждом: агрегация до двух низкоскоростных клиентов в один из линейных интерфейсов до 2.5G (резервирование 1+1)	2
3	Мультиплексор OM-40-AVPM	Мультиплексирование 40 каналов, возможность подстройки каждого канала, затухание на канал 6дБ	2
4	Демультимплексор DM-40-AV	Демультимплексирование 40 каналов, затухание на канал 6дБ	2
5	Мультиплексор ввода/вывода OADM-2/2-AV/PM	Возможность подстройки каналов, затухание на канал 2дБ	2
6	Усилитель EDFA	Перестраиваемый коэффициент усиления в диапазоне 14-24дБ, шум фактор 6дБ	2

Энергетический бюджет. Для расчета энергетического бюджета используется “классический” метод [4]. В соответствии со спецификацией на оборудование:

$$P_{in\ line} = 0 - 6 - 2 = -8\text{дБм};$$

где $P_{in\ line}$ - мощность на входе в линию, после прохождения мультиплексоров.

$$P_{outline} = P_{in\ line} - \alpha L = -8 - 0.2 * 80 = -24\text{дБм};$$

где $P_{outline}$ - мощность на выходе из волокна.

$$P_{in} = -24 - 2 = -26\text{дБм};$$

где P_{in} - мощность на входе усилителя, после прохождения только OADM мультиплексора.

$$P_{in} + g - A_{TT_{DM}} - A_{\text{экспл}} \geq P_{min};$$

где g - усиление мощности на усилителе в децибелах, $A_{TT_{DM}}$ - затухание на демультиплексоре равно: 6дБ

$$-26 + g - 6 - 3 \geq -15,$$

следовательно $g \geq 20\text{дБ}$.

Таким образом требуемый коэффициент усиления усилителя EDFA лежит в диапазоне от 20 дБ до 24 дБ, что с учетом эксплуатационного запаса является оптимальным значением усиления.

Дисперсия. Компенсация дисперсии в данной линии не требуется, так как длина линии меньше 100 км [2].

Расчёт OSNR в линии. ; $OSNR_{R_{TP}}$ - требуемый на транспондере OSNR с учётом компенсации дисперсии, $OSNR_{R_{TP}} = 13\text{дБ}$. Для работы при BER_R (отношение количества ошибок к количеству переданных бит);

$$OSNR_{Line} = 58 + p_{in} - \alpha * L - nf - A_{\text{экспл}} \text{ (реальный OSNR линии);}$$

$$OSNR_{Line} = 56 - 8 - 16 - 6 - 3 = 23\text{дБ}$$

$$OSNR_M = OSNR_{R,Line} - OSNR_{Line} = 13 - 23 = -10\text{дБ (запас по OSNR).}$$

Приемо-сдаточные испытания. Способ проведения приемо-сдаточных испытаний соответствовал программе локальных и секционных испытаний оборудования DWDM«Волга» производства ООО «Т8» [3]. Тестирование BER производилось в соответствии со схемой на рис. 4. Для работы линии количество

ошибочных битов не должно превышать $BER_{cl} = 10^{-12}$. Для исследования эксплуатационного запаса в макет линии вносилось затухание до превышения запаса $OSNR_M$, для этого добавлялся аттенюатор.

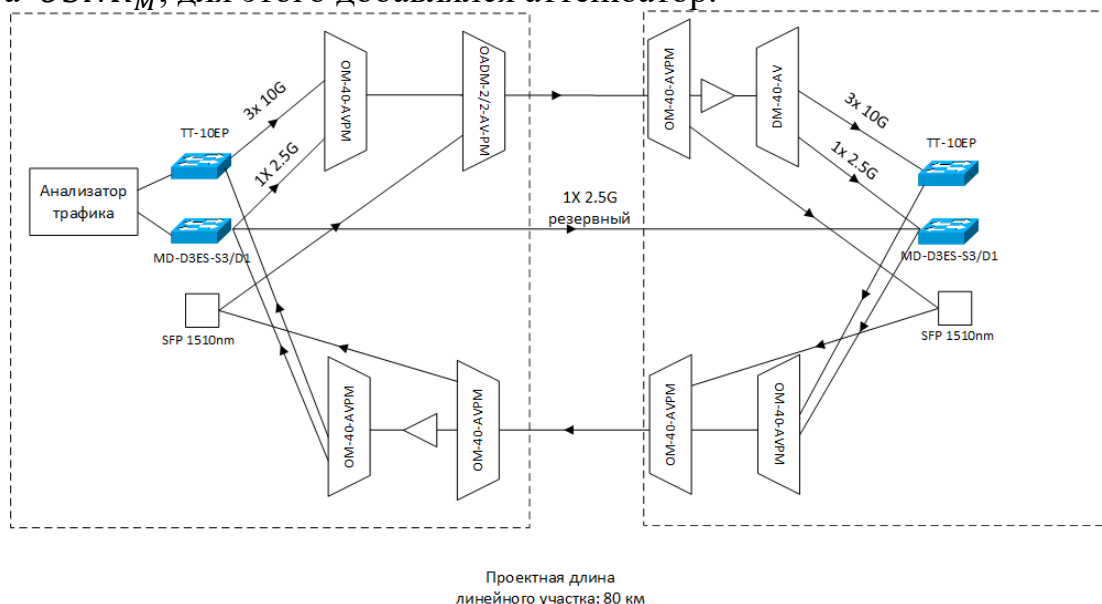


Рис. 4. Схема подключения для проведения тестирования организованных каналов

Заключение.

Была спроектирована DWDM линия связи, проведена сборка модели линии и проведено её тестирование.

Список используемых источников:

1. Онлайн сервис карт Open Street Map URL: <https://www.openstreetmap.org/#map=3/69.62/-74.90>
2. Листвин В.Н ; Трешиков В Н DWDM-СИСТЕМЫ М.: Техносфера, 2021 , 420с.
3. Программа локальных и секционных испытаний оборудования DWDM«Волга» производства ООО «Т8».
4. Дмитриев С.А., Слепов Н.Н. Волоконно-оптическая техника: Современное состояние и перспективы. 2-е изд., Москва, 2005, 576 с.

Pozdnyakov A., Shorgin O., Svintukhovskii P.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Design, assembly, adjustment and acceptance testing of the DWDM line model.

In this article, in accordance with the specification, a fiber-optic communication network between Shlisselburg and St. Petersburg is designed. Structural, situational and channel schemes of the designed line are considered. The calculation of the energy budget of the line is given, acceptance tests are carried out.

Keywords: *FOCS, Fiber optic communication system, DWDM, specification, OSNR, BER, energy budget.*

УДК 621.396.99
ГРНТИ 49.33.29

ОБЛАСТЬ ПРИМЕНЕНИЯ ДАТЧИКОВ НА ПРИНЦИПЕ РАССЕЙЯНИЯ МАНДЕЛЬШТАМА-БРИЛЛЮЭНА

А. А. Ступникова

Сибирский Государственный Университет Телекоммуникаций и Информатики

В распределенных тензодатчиках преобладает технология Бриллюэна, особенно на больших расстояниях. На более коротких расстояниях очевидное преимущество имеет оптическая рефлектометрия Рэля в частотной области (OFDR). Однако обе технологии страдают от присущей им неспособности отличить влияние температуры от воздействия деформации. В связи с этим имеет смысл обсуждения доступных методов распознавания температуры/деформации, за которыми следует описание основных применений распределенного тензодатчика.

тензодатчики, волоконно-оптические датчики, Бриллюэновское рассеяние, рефлектометрия Рэля, BOTDR, OTDR

Основным недостатком распределенных датчиков Бриллюэна, особенно тех, которые ориентированы на сдвиг частоты Бриллюэна, является их неспособность отличить изменения частоты Бриллюэна, вызванные деформацией, от изменений, вызванных температурой.

Концептуально относительно простой подход включает в себя специальную конструкцию кабеля. Она должна гарантировать независимость оптических волокон, используемые для определения температуры, от механического воздействия на оптический кабель. Другие волокна плотно соединены со структурой кабеля, таким образом, напряжение на кабеле передается на последние волокна с хорошо откалиброванной передаточной функцией. Волокна, не связанные с деформацией, упакованы в свободные трубки. Таким образом, сдвиг Бриллюэна, измеренный на этих волокнах, надежно отражает их температуру. Результаты измерений могут быть использованы для температурной компенсации волокон, связанных с деформацией. Волокна, связанные с деформацией, были прикреплены силиконовой смолой к элементу натяжения кабеля. Альтернативой является разработка кабеля с двумя или более волокнами, которые по своей природе по-разному реагируют на изменение частоты в зависимости от температуры и напряжения.

Определенные типы когерентных рефлектометров Рэля могут измерять статическое распределение температуры и деформации. Измерение Рэля является гораздо более чувствительным (на три порядка величины) измерением этих величин, чем сдвиг частоты Бриллюэна, и матрица коэффициентов чувствительности 2×2 для двух измерений хорошо обусловлена. Два измерения могут быть объединены для получения независимых распределений температуры и деформации.

Заманчивым является использование для разделения температуры и деформации двух ортогональных состояний поляризации в волокне,

поддерживающем поляризацию, которые, по сути, можно рассматривать как два независимых волновода в одной сердцевине. Однако измерения температурной чувствительности сдвига Бриллюэна в волокнах с высоким напряжением и двулучепреломлением показали лишь незначительную разницу (несколько МГц) в этом параметре между главными осями и вообще никакой разницы в их чувствительности.

Применение распределённых измерений деформации

ВОТDR был предложен для мониторинга воздушных линий электропередачи. Измеряемыми параметрами в них являются температура конструктивных элементов в результате ударов молнии, а также напряжение вследствие гололедной нагрузки. Подводные энергетические кабели, используемые для соединения сетей из разных стран, в настоящее время обычно оснащаются оптическими волокнами, которые обычно имеют одномодовую конструкцию. Расстояния, на которые приходится зондировать, благоприятствуют технологии Бриллюэна. В мелководных морях тросы иногда зацепляются траулерами или корабельными якорями. Для обнаружения поврежденного участка и ускорения восстановления троса использование распределенных данных о деформации в реальном времени позволяет определить точное время и место происшествя и может помочь назначить ответственность за него.

Распределенные датчики Бриллюэна нашли применение в крупных телекоммуникационных компаниях. Одним из первых применений распределенного тензодатчика был мониторинг установки многоволоконных кабелей в каналах [1], где часть усилий, передаваемых кабелю, передается волокнам.

Еще одной темой, представляющей интерес для телекоммуникационных компаний, является мониторинг разветвленных сетей, т.е. конфигурации, в которых одно волокно передает данные на несколько отдельных волокон. Первоначально это было выполнено с помощью систем Рэлеевского **OTDR**, работающих вне диапазона около 1650 нм. Разветвленная сеть запрашивается с общего конца, так что сигналы обратного рассеяния от всех волокон перекрываются на **OTDR**. Однако этот подход не обеспечивает идентификацию того, какое волокно в сети вышло из строя или понесло повышенные потери, и поэтому для этой цели был использован **ВОТDR**, поскольку сдвиги Бриллюэна в волокнах, установленных в относительно ранних сетях, немного отличались. Вместо того, чтобы полагаться на случайность, более поздняя реализация этой идеи была сосредоточена на использовании **ВОТDA** для измерения разницы в длине между каждой ветвью. Это позволяет определять уровень обратного рассеяния в каждом месте индивидуально по отношению к концу волокна.

В гражданском строительстве мониторинг изменений размеров конструкции может обеспечить раннее предупреждение о начинающемся разрушении. До настоящего времени использовались тензодатчики и хрупкие контрольные пластины. Однако в крупномасштабных конструкциях установка достаточного количества точечных датчиков является дорогостоящей и подверженной поломке. Кроме этого, датчики могут быть недоступны для

осмотра. Распределенное тензометрическое зондирование может восполнить этот пробел.

Крупнейшая телекоммуникационная компания Японии Nippon Telegraph and Telephone (NTT) использовала BOTDR для мониторинга деформации туннелей, используемых для прокладки телекоммуникационных кабелей [2]. Обычно они не обслуживаются, и поэтому автоматизированная система, способная контролировать большие сооружения, идеально подходит для обеспечения раннего обнаружения деформации оптического кабеля. Чувствительное волокно было натянуто и прикреплено к конструкции туннеля. Изменения в напряжении волокна можно было интерпретировать как смещения в относительном положении точек крепления. Система была способна разрешать удлинение или сжатие на 0,1 мм при длине волокна 2 м.

Французское агентство по обращению с радиоактивными отходами ANDRA провела детальное исследование и долгосрочные полевые испытания [3] изменений размеров в бетонных контейнерах, предназначенных для использования в хранилищах ядерных отходов. При этом были произведены оценки производительности и долговечности волоконно-оптических датчиков наряду с обычными экстензометрами и термометрами. Были проверены методы установки и процедуры эксплуатации волоконных датчиков.

Одна из возникших проблем заключалась в том, что при разрыве волокна терялись все возможности мониторинга. В этом случае имелось достаточное количество дополнительных волокон для обеспечения непрерывного покрытия.

Эффективное обнаружение трещин требует очень высокого пространственного разрешения. ВОСДА, который может достигать миллиметрового разрешения, использовался для демонстрации обнаружения трещин в бетоне [4]. Наименьшая ширина трещины, которая была обнаружена в этом исследовании, составляла 0,08 мм, по сути, волосная трещина. Изменение деформации было очевидным на протяжении примерно 10 см, что является отражением длины волокна, на которую передается деформация от одноточечного удлинения.

Пригодность распределенных датчиков Бриллюэна для условий ионизирующего излучения включает мониторинг мест хранения ядерных отходов. Помимо увеличения ослабления, вызванного ионизирующим излучением, обнаружено, что сдвиги частоты Бриллюэна изменяются в результате радиационно-индуцированного повреждения. Это согласуется с более ранними наблюдениями на одномодовых волокнах, легированных оксидом германия GeO_2 . Вредное воздействие ионизирующего излучения (в частности, γ -лучей) может быть частично уменьшено за счет использования волокон с сердцевиной из чистого кремнезема. В них было обнаружено, что сдвиг частоты Бриллюэна, вызванный радиационным повреждением, ограничен примерно 2 МГц. При этом также уменьшено радиационно-индуцированное затухание чем в обычном одномодовом волокне. Напротив, более высокие уровни концентрации GeO_2 приводят к дальнейшему радиационно-индуцированному сдвигу пика Бриллюэна [5].

Прогнозирование и предотвращение оползней, защита подземных трубопроводов и обнаружение эрозии на берегах рек — это лишь несколько примеров необходимости мониторинга потенциально нестабильного грунта. Эта проблема мониторинга, естественно, подходит для распределенных датчиков из-за больших расстояний, которые необходимо преодолеть. Раннее прогнозирование оползней имеет важные преимущества, поскольку позволяет своевременно проводить эвакуацию и, возможно, принимать меры по исправлению положения. Оползни часто вызываются проливными дождями, которые проникают в неустойчивую почву и размягчают ее, вызывая ее разрушение под действием напряжения сдвига.

BOTDR — это один из методов мониторинга, который используется для обнаружения ранних признаков движения. Когда склон проваливается, однородный участок отделяется от соседних участков и перемещается как единое целое. При этом представляет интерес определить границы провала, а также степень перемещения. Волоконно-оптические измерения деформации, используемые для мониторинга движения грунта, включают в себя не только распределенные датчики Бриллюэна (в основном BOTDR), но и массивы FBG, а также интерферометрические методы [6].

Системы защиты рек предназначены для предотвращения попадания необычно высоких уровней воды в охраняемые зоны со стороны суши. Современные дамбы состоят из внутреннего непроницаемого слоя, предназначенного для блокирования прохода воды, поддерживаемого несущей массой для обеспечения устойчивости, в первую очередь, за счет силы тяжести, и, наконец, со стороны суши, дренажной массы из проницаемого материала, позволяющей выходить высокой воде внутри сооружения. Поскольку современные технологии строительства дамб часто включают геотекстиль, встраивание чувствительного волокна в сетку является привлекательным вариантом.

Рассмотренные выше приложения и многие другие, о которых сообщалось в литературе, показали, что распределенное зондирование, в первую очередь с использованием методов Бриллюэна, является надежным и ценным методом мониторинга защиты водных путей от наводнений. Их дальнобойность, чувствительность и инертный характер делают их идеальными кандидатами для выполнения этой важной задачи.

Список используемых источников:

1. Downes, J., and H. Y. Leung. 2004 год. Распределенное температурное зондирование во всем мире применение мониторинга силовых цепей, Международная конференция по системным технологиям электроснабжения, Сингапур 2: 1804-1809, том 1802.
2. Нарусэ, Х., К. Комацу, К. Фудзихаси и М. Окуцу. 2005. Система мониторинга телекоммуникационных туннелей, основанная на измерении деформации распределенного оптического волокна, 17-я Международная конференция по волоконно-оптическим датчикам, Брюгге, Бельгия-Post Deadline Paper, SPIE: 168-171.
3. Фархунд, Р., С. Делепин-Лесойль, С. Бусшердт и К. Ригини - Was. 2015. Проектирование системы мониторинга подземного хранилища радиоактивных отходов — демонстратор на месте. IACSIT Int. J. Англ. Технол. 7: 6: 484–489.

4. Онг, С., Х. Кумагаи, Х. Иваки и К. Горячая вода. 2003. Обнаружение трещин в бетоне с использованием волоконно-оптического распределенного тензодатчика на основе анализа области оптической корреляции Бриллюэна. На 16-й Международной конференции по оптоволоконным датчикам, Нара, Япония We3-3 (октябрь 2003).
5. Делепин-Лесойль, С., Х. Ферон, Ж. Бертран и др. 2012. Промышленный процесс квалификации оптических волокон для измерения распределенной деформации и температуры в хранилищах ядерных отходов. J. Sensors 2012: 369375.
6. Богачков И.В., Горлов Н.И. Новые задачи технической эксплуатации разветвленных волоконно-оптических сетей. // Омский научный вестник. 2009. № 1 (77). с. 195-198.

Stupnikova A.

Siberian State University of Telecommunications and Informatics

Application of distributed load cells.

In distributed load cells, Brillouin technology prevails, especially at long distances. At shorter distances, Rayleigh optical reflectometry in the frequency domain (OFDR) has an obvious advantage. However, both technologies suffer from their inherent inability to distinguish the effects of temperature from the effects of deformation. In this regard, it makes sense to discuss the available methods of temperature/strain recognition, followed by a description of the main applications of a distributed load cell.

Key words: *Strain gauges, fiber-optic sensors, Brillouin scattering, Rayleigh reflectometry, BOTDR, OTDR.*

УДК 621.396.99
ГРНТИ 49.33.29

ПРАКТИЧЕСКИЕ ПРИЛОЖЕНИЯ РАСПРЕДЕЛЕННЫХ ТЕНЗОДАТЧИКОВ

Т. Н. Шайгараева

Сибирский государственный университет телекоммуникаций и информатики

Работа посвящена анализу области применения волоконно-оптических датчиков на принципе рассеяния Мандельштама-Бриллюэна. Наиболее важный интерес представляют волоконно-оптические датчики, которые позволяют контролировать состояние трубопровода по периметру охраны. Важным аспектом является усовершенствование алгоритмов автоматической обработки спектров с дальнейшим увеличением функциональных возможностей датчиков.

волоконно-оптический датчик, рассеяния Бриллюэна, чувствительное оптическое волокно, сдвиг частоты Бриллюэна

В настоящее время волоконно-оптические датчики представляют наибольший интерес ученых, так как с помощью этих средств информация о реальном мире поступает в электронные системы, позволяющие обрабатывать и хранить данные, которые были собраны в процессе мониторинга. Эти системы могут самостоятельно принимать решение на основе полученной информации. Датчики позволяют преобразовывать измеряемые величины, например, деформацию, температуру, давление в сигналы, которые могут быть прочитаны в электронном формате. Данная волоконно-оптическая система представлена на рис. 1 [1].

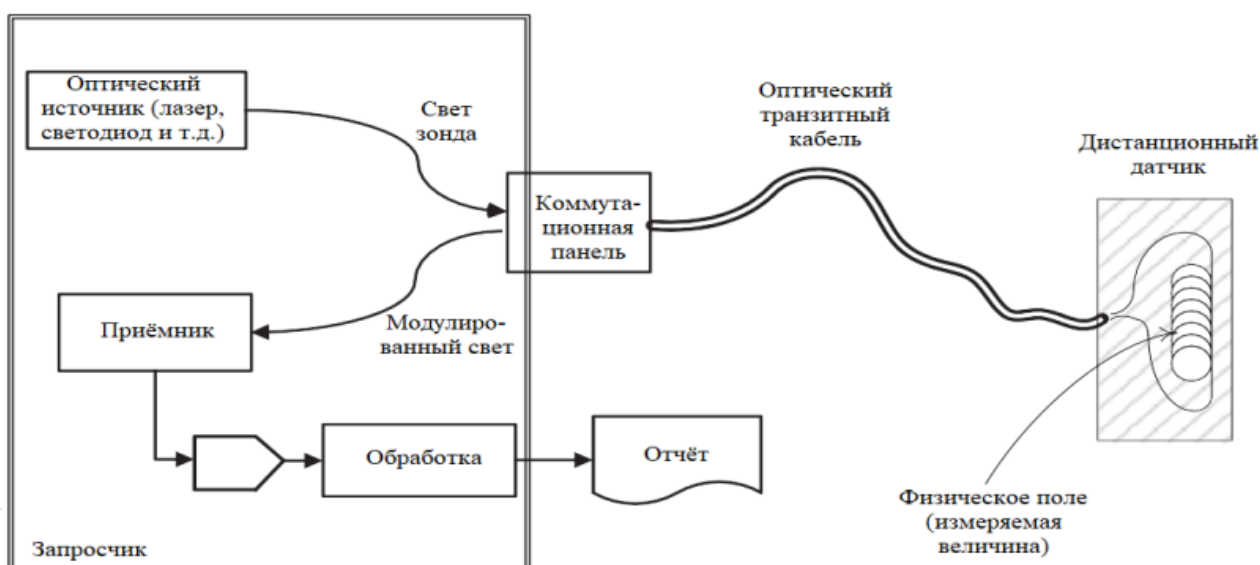


Рис. 1. Простая схема волоконно-оптической системы

Схема представляет собой оптическое волокно в транзитном кабеле, которое передает зондирующий свет на датчик и возвращает модулированный со

значением измеряемой величины свет на устройство приема через коммутационную панель.

Устройство опроса – представляет собой оптико-электронную систему, которая излучает зондирующий свет и преобразует отраженный свет в электрический сигнал, для дальнейшей обработки на выход сигнала системы для создания выходного сигнала системы.

Датчик представляет собой конструкцию, которая реагирует на измеряемую величину и не подвержена помехам. Работа основана на функционирование классифицируемых волоконно-оптических датчиков и представляет собой анализ спектров сигналов обратного рассеяния Мандельштама-Бриллюэна. Сдвиг частоты и интенсивность обратного рассеяния Бриллюэна чувствительны к температуре и деформации. Эти отношения можно описать с помощью матрицы 2×2 [2]

$$[\Delta u_B \Delta I_B] = [C_{uBE} C_{uBT} C_{IBE} C_{IBT}],$$

где C_{uBE} , C_{uBT} , C_{IBT} , C_{IBE} - коэффициенты сдвига частоты и интенсивность, из-за изменений деформации $\Delta \varepsilon$ и температуры ΔT могут быть определены экспериментально для волокна и длины волны измерения.

Значения коэффициентов чувствительности для типичных одномодовых волокон представлены ниже

$$[C_{uBE} C_{uBT} C_{IBE} C_{IBT}] = [0,046 \text{ МГц/мк}\varepsilon \quad 1,07 \text{ МГц/К} \quad - 8 \cdot 10^{-4} \% / \text{мк}\varepsilon \quad 0,36 \% / \text{К}].$$

Таким образом, область применения волоконно-оптических датчиков на принципе рассеяния Мандельштама-Бриллюэна достаточно большая, а именно:

1. Обнаружение трещин в бетоне, чтобы точно обнаружить трещины требуется очень высокого пространственного разрешения для отсутствия потерь небольшого изменения размеров при большой длине калибра [3];

2. Повреждения в морских сооружениях. Перфторированные полимерные волокна были протестированы в качестве детекторов трещин для морских стальных конструкций. При опросе с помощью обычного, но с высоким пространственным разрешением, эти волокна реагируют всплеском усиленного сигнала при приложении локализованной осевой деформации, как в случае образования трещины. Пластичная природа материала позволяет волокну непрерывно прикрепляться к конструкции и в то же время выдерживать локальное увеличение размеров, которое могло бы привести к разрушению стекловолокна [4].

Датчики включают в себя мониторинг мест хранения ядерных отходов, которые являются не безопасными для окружающей среды. Увеличение ослабления, которое вызвано ионизирующим излучением, обнаруживается сдвиг частоты Бриллюэна в результате радиационно-индуцированного повреждения [5].

Данное воздействие очень вредное, но может быть уменьшено за счет использования волокон с сердцевиной из чистого диоксида кремния, в которых обнаружено, что сдвиг частоты Бриллюэна, вызванный радиационным повреждением, ограничен примерно 2 МГц. При чем, уменьшается радиационно-индуцированное затухание, чем в обычном одномодовом волокне [6]. Применение волоконно-оптических датчиков следующее:

1. Определение формы. Область применения датчиков разнообразна, например, в медицине для измерения движения руки хирурга при управлении удаленным вмешательством, можно также воспользоваться для оценки трехмерного перемещения длинных объектов: канатов или гибких труб. Форма определяется путем измерения деформации в нескольких местоположениях в поперечном сечении тела, которое измеряется так, чтобы имелась возможность определить изгиб по меньшей мере в двух осях. Это возможно, когда тело не скручивается [7];

2. Мониторинг состояния составных конструкций. Деформация конструкций рассматривается с использованием волокон, встроенных в материал, например, в беспилотных летательных аппаратах. Волокно в достаточной степени совместимо с производственным процессом;

3. Деформация в скважинах. Строительство скважин несет угрозу по поводу механической целостности и деформации обсадной колонны, а также песчаного грунта, который возникают в нестабильных пластах. Данные изменения могут быть сняты с помощью опроса Бриллюэна с высоким пространственным разрешением;

4. Контроль целостности трубопровода. Данная задача актуальна при транспортировке жидкости по трубопроводам. Трещины, сколы труб может быть опасным как для людей, так и для окружающей среды, что ведет за собой огромные материальные убытки, гибель людей и животных.

Исследовать нарушение целостности трубопровода для персона достаточно сложно, так как протяжённость труб достаточно большая, а многие газопроводы высокого давления покрыты полимерным материалом для ограничения коррозии. Производители часто не разрешают дополнять трубы каким-либо материалом. Это связано с тем, что в поверенное изделие необходимо вносить изменения с связанные с установкой тензодатчиков, что необходимо отражать в технической документации.

Однако, установка волокна в траншее может вызвать оползни, которые приводят к неисправности трубопровода, и как следствие утеки жидкости;

5. Уплотнение и оседание в подземных пластах. Стабильность окружающих подземных пластов заключается в целостности окружающих их геологических формаций. Добыча полезных ископаемых и обрушение породы создают напряжение, которое может привести к уплотнению и оседанию грунта. Нагнетание пара также приводит к тепловому расширению. Другие проблемы такие как грунтовые воды или снижение давления за счет добычи углеводородов. С данными вопросами отлично справятся оптоволоконные датчики;

6. Движение грунта. В настоящее время есть необходимость в контроле потенциально опасного грунта для предотвращения и прогнозирования оползней, защиты подземных трубопроводов и т.п. С этой проблемой отлично

справляются распределенные датчики, которые работают на большие расстояния. Вовремя обнаруженный оползень позволяет провести раннюю эвакуацию людей из опасных мест и принять меры по предотвращению оползня, которые чаще всего вызванные проливными дождями. Вода, попадая в почву, разрушает ее под воздействием напряжения сдвига.

Волоконно-оптический датчик - это один из методов, который можно использовать для обнаружения ранних признаков движения почвы;

7. Берега рек и дамбы. Защита рек необходима для предотвращения увеличения уровня воды в водоемах в охраняемых зонах. Дамбы производятся из внутреннего слоя, который обладает свойством непроницаемости, предназначенный для недопущения прохода воды. Обеспечивается устойчивость, за счет силы тяжести, со стороны суши, дренажной массы из проницаемого материала, позволяющего выходить большой воде внутри сооружения. Распределенное зондирование методом Бриллюэна надежно и существенным методом мониторинга защиты водных сооружений от надвигающихся наводнений.

Датчики обладают дальностью, чувствительностью, а также имеют инертный характер, что делает их идеальными для выполнения поставленной задачи;

8. Охрана по периметру. Большая часть волоконно-оптических систем обнаружения проникновения основаны на акустических сигналах. Например, квазистатического напряжения, создаваемого волокном в результате присутствия постороннего, позволяет обнаруживать вторжение для этого необходимо использование распределенного датчика с чувствительным волокном [8]. Требуется быстрое обнаружение, и измерение обновлялось с интервалом в 1,5 секунды для предполагаемого уровня деформации.

В этом случае для поддержания надежности системы необходима низкая частота ложных срабатываний в сочетании с высокой вероятностью обнаружения, так как кабель очень чувствительный и устанавливается на двух разных уровнях ограждения, когда происходит одновременное обнаружение на обоих оптоволоконных кабелях, то это может использоваться для перекрестной проверки сигналов тревоги. Метод Бриллюэна, квазистатический, способен отклонять переходные эффекты, вызываемые ветром вибрации, но они зависят от высокой силы, для преодоления порога чувствительности [9].

Таким образом, волоконно-оптические датчики на принципе рассеяния Мандельштама-Бриллюэна достаточно успешны в различных областях деятельности. Они применяются для обнаружения трещин в бетоне, помогают определить повреждения морских сооружений, в местах хранения ядерных отходов, а также позволяют успешно наблюдать состояние составных конструкций. Большой интерес вызывают волоконно-оптические датчики для контроля целостности трубопровода по периметру охраны.

Список используемых источников:

1. Bosselmann, T., and R. Ulrich. 1984. High-accuracy position-sensing with fiber-coupled white-light interferometers, 2nd International Conference on Optical Fibre Sensors, Stuttgart, Germany, VDE Verlag: 361–364.

2. Davey, S. T., D. L. Williams, B. J. Ainslie, W. J. M. Rothwell, and B. Wakefield. 1989. Optical gain spectrum of GeO₂–SiO₂ Raman fibre amplifiers. IEE Proc. J. 136: 6: 301–306.
3. Ong, S., H. Kumagai, H. Iwaki, and K. Hotate. 2003. Crack detection in concrete using a Brillouin optical correlation domain analysis based fiber optic distributed strain sensor. In 16th International Conference on Optical Fiber Sensors, Nara, Japan We3-3 (Oct. 2003).
4. Kuang, K. 2015. Distributed damage detection of offshore steel structures using plastic optical fibre sensors. Sensor. Actuat. A-Phys. 229: 59–67.
5. Phйron, X., J. Bertrand, S. Girard et al. 2012. Brillouin scattering based sensor in high gamma dose environment: Design and optimization of optical fiber for long-term distributed measurement, 22nd International Conference on Optical Fibre Sensors, SPIE, 8421: A4.
6. Delepine-Lesoille, S., X. Phйron, J. Bertrand et al. 2012. Industrial qualification process for optical fibers distributed strain and temperature sensing in nuclear waste repositories. J. Sensors 2012: 369375.
7. Moore, J. P., and M. D. Rogge. 2012. Shape sensing using multi-core fiber optic cable and parametric curve solutions. Opt. Expr. 20: 3: 2967–2973.
8. Фердинанд П., С. Ружо, Н. Руссель и др. 2012. Датчик Бриллюэна для периметрического обнаружения: Проект SMARTFENCE, 22-я Международная конференция по оптоволоконным датчикам, Пекин, Китай, SPIE, 8421: 9X.
9. Богачков И.В., Горлов Н.И. Экспериментальные исследования влияния температуры на спектр бриллюэновского рассеяния и характеристики оптических волокон. // Вестник СибГУТИ. 2015. № 4 (32). с. 3-12.

Shaigarayeva T.

Siberian State University of Telecommunications and Informatics

Practical applications of distributed load cells.

The work is devoted to the analysis of the field of application of fiber-optic sensors based on the Mandelstam-Brillouin scattering principle. The most important interest is represented by fiber-optic sensors that allow monitoring the condition of the pipeline along the perimeter of the guard. An important aspect is the improvement of algorithms for automatic processing of spectra with a further increase in the functionality of sensors.

Key words: *fiber-optic sensor, Brillouin scattering, sensitive optical fiber, Brillouin frequency shift.*

**Секция 3.5.
Программная инженерия**

УДК 004.42
ГРНТИ 50.41.25

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЯЗЫКОВ JAVA И KOTLIN С ПОЗИЦИИ НАПИСАНИЯ БЕЗОПАСНЫХ ПРОГРАММ

К. М. Богомедова, К. Е. Израйлов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе решается актуальная задача разработки программного кода без уязвимостей. Для этого предлагается делать обоснованный выбор среди таких популярных и относительно близких языков программирования, как Java и Kotlin. С этой позиции производится сравнительный анализ языков программирования по следующим критериям: конструкции для безопасного программирования, распространенность, размер получаемого кода, скорость компиляции, мощность синтаксиса, поддержка современных тенденций программирования, поддержка умной трансляции. По данным критериям и делается вывод об условном равенстве языков для безопасной программной инженерии.

программная инженерия, язык программирования, сравнительный анализ, Kotlin, Java

Введение

Программная инженерия является неотъемлемой частью обеспечения функционирования большинства современных информационных процессов [1]. В результате, встает вопрос выбора соответствующего программного обеспечения, которое бы позволяло разработчику создавать безопасный программный код, то есть разрабатывать программы без уязвимостей или же способствовать их снижению [2, 3, 4]. Одной из наиболее востребованных процессорных платформ, выполняемых на практически любом аппаратном обеспечении, является Java Virtual Machine (далее – JVM) [5]. В интересах вышесказанного, в статье будет произведен сравнительный анализ двух языков программирования, код которых выполняется на JVM, а именно – Java и Kotlin. И если первый является достаточно старым, уже ставшим классическим языком разработки полноценных программных продуктов, то второй по праву можно назвать новым и достаточно перспективным.

Java

Компания Sun Microsystems простояла на плаву 28 лет. В 80-х данная компания была одной из самых быстрорастущих компаний в США. Она разработала процессорную архитектуру SPARC и язык программирования Java (который изначально именовался, как Oak). В последние годы появилась потребность в новых языках, которые компилируются в переносимый байт-код для основной части исполняющей системы Java – так называемой Java Runtime Environment (далее – JRE). История разработки языков на данной платформе

имеет довольно длительное время и разработчики уже более десяти лет создают новые языки программирования на Java Virtual Machine (далее – JVM), однако популярность такие языки получили относительно недавно. На данный момент довольно частое использование получили динамически типизированные языки, такие как JRuby, Groovy и Clojure, а среди статически типизированных языков свою популярность получили Scala, Fantom и Gosu.

К одной из главных особенностей Java можно отнести то, что приложение написанное на Java без всяких проблем запускается на платформе со средой исполнения JRE. Это обеспечивается благодаря компиляции написанного на Java кода в байт-код, не привязанный к конкретной аппаратной платформе; а JVM же является частью JRE.

Также стоит отметить, что в Java реализован механизм управления памятью – Garbage Collector с помощью которого очищается память, когда объекты перестают использоваться.

Kotlin

Создатели языка Kotlin хорошо «прочувствовали» потребности разработчиков и, как результат, создали удобный современный инструмент для разработки. Под современностью подразумевается не только компилятор, но и поддержка языка в Integrated Device Electronic (далее – IDE) – без нее деятельность разработчика является совершенно невозможной [6].

В качестве двух главных особенностей Kotlin можно выделить простоту и полную совместимость с Java. Последнее обосновывается тем, что Kotlin создавался компанией, которая делает много продуктов на Java и хорошо разбирается в современных инструментах разработки. Запрос на новый язык был актуален уже давно, однако сделать язык, который бы позволил взять большую готовую кодовую базу Java, обычных Java-разработчиков, дать им новый инструмент и более эффективно продолжать разработку – такого инструмента до появления языка Kotlin не существовало.

Также немаловажную роль в особенностях языка играет безопасность языка Kotlin. В начальное смысловое значение операторов, основных конструкций (семантика) языка заложены принципы, предотвращающие разные ошибки, проявляющиеся во время исполнения программы. Это очень помогает разработчикам снизить затраты на тестировании кода.

Kotlin в последнее время очень востребован и популярен, хотя это и не означает, что он не имеет конкуренции среди других «молодых» языков, поскольку он, как и любые другие, имеет свои плюсы и минусы.

Kotlin поддерживается всеми крупными IDE для Java, включая IntelliJ IDEA, Android Studio, Eclipse и NetBeans; хотя при этом замечается некоторая нестабильность в его работе.

Сравнительный анализ

Осуществим сравнительный анализ представленных языков с позиции использования их особенностей и возможностей программистами для написания безопасных программ, используя следующие логичные критерии:

1. *Конструкции для безопасного программирования* – наличие в языке конструкций, предназначенных для создания безопасного кода (сборщик мусора и т.п.) [7];
2. *Распространенность* – то, насколько язык программирования популярен и используется при разработке продуктов, поскольку широкое распространение автоматически ведет к вниманию общественности, наличию документации, примеров и обсуждений (например, на сайте StackOverflow и т.п.);
3. *Размер получаемого кода* – то, насколько код получается компактным по содержанию, поскольку большое число строк автоматически увеличивает шанс как допустить ошибку, так и ее не выявить при отладке;
4. *Скорость компиляции* – то, насколько код быстро преобразуется в выполняемый, что хотя напрямую и не влияет на безопасность, но тем не менее увеличение сборки кода уменьшает время на его отладку и поиск уязвимостей [8];
5. *Мощность синтаксиса* – размер набора ключевых слов, операций, их комбинаций и т.п., увеличение чего очевидно ухудшает как написание кода, так и поиск в нем уязвимостей;
6. *Поддержка современных тенденций программирования* – возможность использования новых и перспективных концепций программирования, такие как делегаты, расширения, функции высшего порядка и т.п. [9];
7. *Поддержка умной трансляции* – что означает дополнительные интеллектуальные проверки кода на предмет ошибок и/или безопасности.

Сравнение языков по критериям представлено в табл. 1, в которой для каждого из языков указано его соответствие критерию, для которых также проставлены баллы следующим образом: 0 – не соответствует, 0.5 – частично соответствует, 1 – полностью соответствует. Затем, баллы суммируются, что позволяет оценить интегральное соответствие Java и Kotlin всем критериям.

ТАБЛИЦА 1. Сравнительный анализ Kotlin и Java

Критерий	Java	Kotlin
Конструкции для безопасного программирования	1	0
Распространенность	1	0.5
Размер получаемого кода	0	1
Скорость компиляции	0	1
Мощность синтаксиса	1	0
Поддержка современных тенденций программирования	1	1
Поддержка умной трансляции	0.5	1
Сумма баллов	4.5	4.5

Сравнительный анализ (см. табл. 1) позволяет сделать вывод о том, что языки похожи между собой, поскольку оба набрали одинаковое количество баллов – 4.5. Таким образом, разработчик может обоснованно выбирать любой из языков, естественно, при учете того, что будет пользоваться всеми возможностями обоих (в т.ч. согласно критериям).

Выводы

В работе был проведен сравнительный анализ языков программирования Java и Kotlin с позиции их использования разработчиком для написания кода без уязвимостей [10]. Для этого использовались следующие критерии: конструкции для безопасного программирования, распространенность, размер получаемого кода, скорость компиляции, мощность синтаксиса, поддержка современных тенденций программирования, поддержка умной трансляции. Результаты анализа позволили сделать вывод, что согласно выбранным критериями оба языка могут считаться безопасными для разработки программ в одинаковой степени. Продолжением исследования должна стать проверка данного вывода на практике.

Список используемых источников:

1. Романов Н.Е., Израилов К.Е., Покусов В.В. Система поддержки интеллектуального программирования: машинное обучение feat. быстрая разработка безопасных программ // Информатизация и связь. 2021. № 5. С. 7-17. DOI: 10.34219/2078-8320-2021-12-5-7-16.
2. Израилов К.Е. Система критериев оценки способов поиска уязвимостей и метрика понятности представления программного кода // Информатизация и связь. 2017. № 3. С. 111-118.
3. Буйневич М.В., Израилов К.Е., Мостович Д.И., Ярошенко А.Ю. Проблемные вопросы нейтрализации уязвимостей программного кода телекоммуникационных устройств // Проблемы управления рисками в техносфере. 2016. № 3(39). С. 81-89.
4. Израилов К.Е., Кузнецов С.А. Применение искусственного интеллекта и методов машинного обучения для поиска уязвимостей исходного кода // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2020): сборник научных статей IX Международной научно-технической и научно-методической конференции (Санкт-Петербург, 26-27 февраля 2020 г.). 2020. С. 361-366.
5. Алиевский Д. Java: магия отражений. часть III. компиляция Java средствами Java // Системный администратор. 2003. № 2 (3). С. 64-72.
6. Emomaliyev M.R., Popov A.A. Kotlin and Android development // Modern Science. 2019. № 1. С. 58-61.
7. Гуров Д.В., Гуров В.В., Иванов М.А., Шустова Л.И. Технология безопасного программирования и особенности ее преподавания в вузе // Дистанционное и виртуальное обучение. 2010. № 9. С. 35-44.
8. Пилипенко А.В. Обзор интерпретации и компиляции в виртуальных машинах // Компьютерные инструменты в образовании. 2012. № 3. С. 3-15.

9. Немченко Е. Поддержка функций высших порядков в языке КРНР // Студенческий вестник. 2019. № 17-4 (67). С. 30-32.
10. Izrailov K.E., Buinevich M.V., Kotenko I.V., Yaroshenko A.Y. Identifying characteristics of software vulnerabilities by their textual description using machine learning // World Automation Congress (Taipei, Taiwan, 1-5 august 2021). 2021. PP. 186-192. DOI: 10.23919/WAC50355.2021.9559470.

Bogomedova K., Izrailov K.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Comparative analysis of Java and Kotlin languages from the point of view of writing secure programs.

The paper solves the actual problem of developing program code without vulnerabilities. To do this, it is proposed to make an informed choice among such popular and relatively close programming languages as Java and Kotlin. From this position, a comparative analysis of programming languages is carried out according to the following criteria: constructions for secure programming, prevalence, size of the resulting code, compilation speed, syntax power, support for modern programming trends, support for smart translation. Based on these criteria, a conclusion is made about the conditional equality of languages for safe software engineering.

Key words: software engineering, programming language, benchmarking, Kotlin, Java.

УДК 519.876.5
ГРНТИ 49.33.29

ПРОБЛЕМЫ СОЗДАНИЯ И ЭКСПЛУАТАЦИИ УМНЫХ ЗДАНИЙ

Н. А. Ерохова, А. В. Пачин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Технология «умного здания» включает в себя эффективные автоматизированные средства управления и приложения, которые используют интеллектуальные энергетические продукты, сетевые датчики и программное обеспечение для мониторинга данных об окружающей среде и привычках жителей к потреблению энергии для улучшения эксплуатации зданий и энергоэффективности.

В данной статье рассматриваются основные проблемы «умных зданий», их последствия и возможные решения.

умное здание, искусственный интеллект, интернет-соединение, IoT-устройства

«Умное здание» — это здание, в котором используются технологии, позволяющие эффективно и экономно использовать ресурсы, создавая при этом безопасную и комфортную среду для жильцов [1]. В «умных» зданиях может использоваться широкий спектр существующих технологий, и они проектируются или модернизируются таким образом, чтобы обеспечить интеграцию будущих технологических разработок. Датчики Интернета вещей (IoT), системы управления зданием, искусственный интеллект (ИИ) и дополненная реальность являются одними из механизмов, которые могут использоваться в умном здании для управления и оптимизации его производительности [2].

Концепция «умного здания» состоит из физических ресурсов внутри здания, цифровых ресурсов, которые создают структуру во всем подключенном пространстве, и, наконец, вариантов использования, которые становятся возможными благодаря сочетанию физических и цифровых ресурсов (рис. 1) [3]:

1. Физические ресурсы

- A. Система отопления, вентиляции и кондиционирования воздуха
- B. Система освещения
- C. Датчики
- D. Контроль физического доступа
- E. Шлюзы
- F. Счетчики энергии

2. Цифровые ресурсы

- G. Цифровая автоматизация
 - Распознавание лиц
 - Биометрический доступ
 - Дополненная/виртуальная реальность
- H. Облачное хранилище
 - Управляющее программное обеспечение

- Кибербезопасность
- Многофакторная аутентификация
- I. Платформа интернета вещей
 - Искусственный интеллект
 - Wi-Fi
 - Сбор и анализ данных
- 3. Варианты использования
 - J. Виртуальный ассистент
 - K. Бронирование помещения
 - L. Обслуживание, основанное на использовании
 - M. Осведомленность о местоположении
 - N. Умная парковка

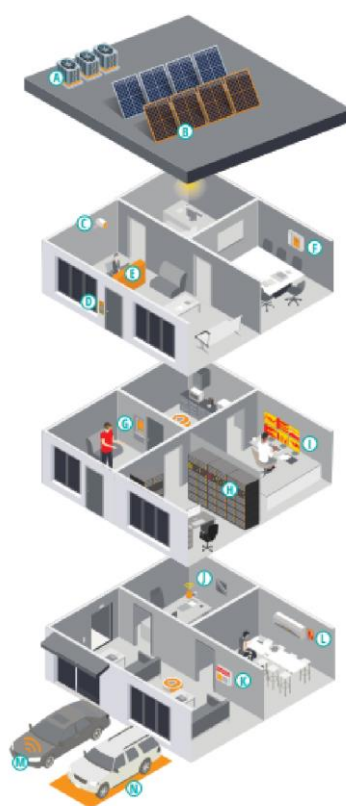


Рис. 1. Концепция «умного здания»

«Умные здания» могут помочь снизить затраты на электроэнергию и оптимизировать использование ресурсов, однако, как и многое вокруг нас, умные здания имеют свои недостатки [4]. Вот некоторые из них:

1. Их строительство, модернизация и эксплуатация являются дорогостоящими.

«Умные здания» дорого строить, потому что они состоят из следующих элементов, которых нет в традиционных зданиях:

- IoT-устройства
- Возможность подключения устройств
- Интуитивно понятное программное обеспечение

Но помимо этого есть также много скрытых затрат, связанных с «умными зданиями», в том числе:

- Стоимость внешней поддержки
- Обслуживание и замена IoT-устройств
- Модернизация интернет-соединения
- Стратегия кибербезопасности
- Замена несовместимых устройств
- Решение для резервного питания
- Программные обновления и т. д.

2. Реализация «умного здания» может не всегда соответствовать требованиям заказчика на этапе эксплуатации.

Технология «умного здания» разумно использует данные, чтобы помочь создать комфортное рабочее и жилое пространство с точки зрения температуры и освещения. К сожалению, это не всегда так, так как технология может быть не точной или вообще работать со сбоями.

Например, в жаркий летний день технология «умного здания» может установить слишком низкую температуру климат-контроля, в результате чего в здании будет холодно, что неудобно для сотрудников.

3. Для бесперебойной работы «умного здания» требуется надежное и быстрое подключение к интернету.

«Умные здания» предлагают фантастическое удобство, поскольку они автоматизируют раннее ручные аспекты управления. Тем не менее, они хороши настолько, насколько хорошо их интернет-соединение. Если здание расположено в районе с прерывистым или слабым интернет-сигналом, оно не будет работать должным образом и может стать пустой тратой инвестиций.

4. «Умные здания» не могут работать во время отключения электроэнергии.

Некоторые экстремальные погодные явления могут привести к обрыву линий электропередач, что приведет к отключению электроэнергии на несколько дней, а возможно и недель.

5. Умные строительные устройства имеют ограниченный срок службы.

В зависимости от размера умного здания в нем могут быть от десятков до сотен IoT-устройств, таких как беспроводные датчики. Эти устройства рассчитаны на несколько лет службы и в зависимости от того сколько их, стоимость замены датчиков может быть существенной.

Последствиями некоторых проблем является угроза жизни и здоровью человека. Например, при отсутствии электроэнергии система пожаротушения не сработает или люди, застрявшие в лифте могут остаться без кислорода. Чтобы избежать такого рода последствий, в здании необходимо установить резервный источник питания.

В дальнейшей работе предполагается создание программного обеспечения для решения критических ситуаций при помощи онтологических моделей.

Список используемых источников:

1. Muhammad Saidu Aliero, Muhammad Asif, Imran Ghani, Muhammad Fermi Pasha, Seung Ryul Jeong. Systematic Review Analysis on Smart Building: Challenges and Opportunities // sustainability. 2022.
2. Gomasa Ramesh. National Conference on Innovations & Recent Trends in Civil Engineering (NCIRCE-2021) 9th and 10th June 2021, Sri Venkateshwara College of Engineering, Bengaluru, India. С. 206-208.
3. Smart Building Technology: Concept, Features, and Application.[Электронный ресурс]. URL: <https://www.scnsoft.com/blog/smart-buildings>.
4. Advantages and Disadvantages of Smart Buildings in 2021.[Электронный ресурс]. URL: <https://smart-cre.com/advantages-and-disadvantages-of-smart-buildings-in-2021/>.

Erokhova N, Pachin A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Problems of creation and operation of smart buildings.

Smart building technology incorporates efficient automated controls and applications that use smart energy products, networked sensors and software to monitor data on the environment and occupants' energy consumption habits to improve buildings operation and energy performance.

This article discusses the main problems of smart buildings, their consequences and possible solutions.

Key words: smart building, artificial intelligence, internet connection, IOT devices.

УДК 004.891.3
ГРНТИ 50.41.25

СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ В ПОДХОДАХ К ФОРМИРОВАНИЮ СИСТЕМ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ НА БАЗЕ КЛАВИАТУРНОГО ПОЧЕРКА

А. А. Завацкая

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Учитывая стремительные темпы развития информационных технологий, увеличение количества информационных угроз, а также степень неопределенности их происхождения и реализации, задача построения системы информационной безопасности становится все более актуальной в наше время. Одним из способов минимизировать угрозы вредоносных атак, а также риски кражи конфиденциальной информации является идентификация пользователей по клавиатурному почерку. Данная работа посвящена рассмотрению существующих проблем в подходах к формированию систем идентификации пользователя на базе клавиатурного почерка.

клавиатурный почерк, идентификация, психофизиологическое состояние

Идея использования клавиатурного почерка для идентификации личности не нова. Еще в годы Второй мировой войны спецслужбы разных стран учитывали, так называемый, “почерк радиста” для более точной оценки достоверности источника полученных разведданных. В 1979 году специалисты SRI International (Stanford Research Institute) представили чип со встроенным алгоритмом распознавания клавиатурного почерка. В 1984 году Национальное бюро стандартов США признало технологию эффективной на 98%. А уже в начале 80-ых Национальный научный фонд и Национальное Бюро Стандартов в Соединенных Штатах провели исследования, устанавливающие, что образцы клавиатурного почерка содержат уникальные особенности, которые могут быть идентифицированы. На первый взгляд рассматриваемый метод идентификации кажется достаточно убедительным, но если немного покопаться в данной теме, то всплывают весьма существенные недостатки, которые не могут давать 100%-ой гарантии правильной идентификации человека. Сразу же возникает вопрос, какие проблемы существуют в настоящее время, насколько они немаловажны и возможно ли уменьшить вероятность их возникновения?

Идентификация - это установление тождественности неизвестного объекта известному на основании совпадения признаков, другими словами - опознание. Именно от этого зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. Традиционные методы идентификации и аутентификации, основанные на использовании смарт-карт, USB-ключей, электронных ключей или других портативных идентификаторов, а также паролей и кодов доступа, имеют существенные недостатки, такие как: возможность кражи предмета у пользователя; необходимость специального оборудования для работы с магнитными картами, смарт-картами и другими; возможность сделать копию уникального предмета. В целом, основным недостатком таких методов является

не всегда надежная аутентификация. Этот недостаток может быть устранен с помощью методов биометрической идентификации.

Биометрические методы основаны на определении личности человека по присущим только ему признакам, которые намного сложнее потерять или подделать, в отличие от паролей и носителей информации для систем контроля доступа. Биометрические характеристики делятся на физиологические и поведенческие. К физиологическим относится сканирование отпечатков пальца, радужной оболочки глаза, формы лица и т.д. Поведенческие - предполагают анализ речи, рукописного и клавиатурного почерка, походки. Поведенческие характеристики сложнее распознать с высокой точностью, но вместе с тем, сложнее и подделать. Также, для их снятия редко требуется специальное оборудование. Поведенческую биометрическую информацию можно изменить по воле человека. Поведенческие образцы обладают меньшей надежностью и стабильностью по сравнению с физиологическими биометрическими образцами, но являются высоко информативными и адаптируемыми, поэтому сегодня ведутся активные исследования в области их применения.

Как уже было описано ранее, клавиатурный почерк - это поведенческая биометрическая характеристика, состоящая из паттернов ритма и динамики, характерных для данного оператора при наборе текста. Характерными особенностями для клавиатурного почерка могут стать:

- скорость ввода – количество введенных символов, деленное на время печати;
- динамика ввода – время между нажатиями клавиш и время их удержания;
- частота возникновения ошибок при вводе и их род;
- использование функциональных клавиш;
- сила нажатия на клавиши [1].

Эффективность аутентификации по клавиатурному почерку, как и любого другого биометрического метода, определяется с помощью трех основных критериев:

- FRR (False Reject Rate) или ошибка первого рода – вероятность ошибочных отказов авторизованному пользователю (ошибочный отказ «своему»);
- FAR (False Accept Rate) или ошибка второго рода – это вероятность допуска незарегистрированного пользователя (ошибочный пропуск «чужого»);
- EER (Equal Error Rates) – равная вероятность ошибок первого и второго рода.

Также необходимо отметить, что между коэффициентами FAR и FRR существует функциональная связь. Чем больше FAR, тем меньше FRR и наоборот, чем меньше FAR, тем больше FRR.

В процедуре аутентификации пользователя по клавиатурному почерку основным этапом является обработка первичной информации. На основании этой информации происходит разделение входных потоков данных на ряд признаков, характеризующих уникальные параметры идентифицируемой личности. Эти данные подвергаются статистическому исследованию и в результате выводится ряд эталонных значений биометрической характеристики пользователя. Чем больше производится сбор данных на этапе обучения

(возможно повторное обучение системы), тем точнее определяются эталонные характеристики пользователя. Существует несколько этапов обработки данных. Первый из них – это фильтрация. На этом этапе удаляется лишняя информация о функциональных, служебных клавишах, а также клавишах управления курсором. Следующий этап, это увеличение числа эталонных биометрических характеристик. Данный этап позволяет увеличить надежность системы, за счет разделения входных потоков на данные, которые относятся к левой и правой руке соответственно. Это возможно сделать, учитывая статистику набора таких клавиш как SHIFT, которая нажимается мизинцем либо с правой стороны клавиатуры, либо с левой; тоже самое можно выявить, акцентируя внимание на такие клавиши как CTRL и ALT/Command.

Данные полученные на этапе обучения системы, которые становятся эталонными для данного пользователя позволяют сделать заключение о степени устойчивости клавиатурного почерка и установить доверительный интервал по разбросу параметров для последующей аутентификации пользователя. На данный момент произведена оценка стабильности клавиатурного почерка пользователя [2]:

ТАБЛИЦА 1. Характеристики стабильности клавиатурного почерка пользователей

Ошибки, %	Аритмичность, %	Скорость, знак/мин	Характеристики перекрытий		Оценка
			Число перекрытий, %	Используемое число пальцев	
> 2	> 10	< 200	< 50	Все	5
> 4	> 15	< 150	< 30	Большинство	4
> 8	> 20	< 100	< 10	Несколько	3
< 8	< 20	> 100	> 10	По одному	2

Использование клавиатурного почерка для идентификации личности имеет ряд несомненных преимуществ:

- алгоритмы относительно просты и могут быть реализованы как в виде ПО, так и прошиты в чипе;
- относительная дешевизна (реализация алгоритма не требует больших вложений, из «железа» фактически используется только клавиатура);
- скрытость использования, например, злоумышленник может и не подозревать о такой возможности;
- относительно высокая степень эффективности.

Но нельзя забывать и о недостатках данного метода идентификации. Первая проблема - это необходимость долгого обучения системы, так как практически все известные методы идентификации и аутентификации пользователей по клавиатурному почерку основаны на анализе полученных входных данных.

Следующая проблема заключается в изменении клавиатурного почерка пользователя из-за его психофизического состояния. Небезызвестно, что именно

оно влияет на особенность и стабильность воспроизведения подсознательных движений человека. В данной работе можно представить модель пяти психофизиологических состояний, потенциально влияющих на вероятность изменения клавиатурного почерка человека [3].

1. Адекватное (или нормальное) состояние, при котором субъект не подвергался каким-либо воздействиям.

2. Возбуждение – характерно для человека, сконцентрированного на решении ответственной задачи.

3. Усталость (после нагрузки) – возникает в период после выполнения ответственного задания, характеризуется угнетенностью, утомлением.

4. Расслабленное состояние, характеризующееся легкой сонливостью, низкой продуктивностью.

5. Опьянение.

Исследования в этой сфере позволили вычислить биометрические признаки – параметры, характеризующие субъекты и их психофизиологические состояния. Рассматриваемая проблема является весьма существенной, но, предположительно, ее можно разрешить нейросетевым методом идентификации пользователя по клавиатурному почерку за счет увеличения размерности вектора, который в свою очередь содержит эталонные характеристики пользователя. Также ранне проведенные исследования могут помочь в выявлении каких-либо зависимостей изменения клавиатурного почерка от психофизиологического состояния человека.

Следующим немаловажным фактом, относящимся к недостаткам идентификации на базе клавиатурного почерка, является пользователь, не имеющий длительного опыта работы с клавиатурой. Как показывают данные из таблицы 1, чем опытнее пользователь, тем стабильнее его почерк и проще его идентификация. Данная проблема не считается слишком существенной, так как в современном мире распространение компьютеров с каждым годом набирает обороты, и большинство людей уже имеют сформировавшийся клавиатурный почерк.

Последний недостаток, на который необходимо обратить внимание - это замена клавиатуры. Из-за другого расстояния между клавишами, их размера и т.п. возникает большая вероятность изменения почти всех характерных особенностей клавиатурного почерка. При таких существенных изменениях необходимо переобучение, что, как мы уже выяснили, занимает достаточно длительное время.

Таким образом, можно сделать вывод о том, что идентификация пользователя на базе клавиатурного почерка имеет как положительные аспекты, отличающиеся от остальных методов идентификации своей эффективностью и простотой внедрения, так и существенные проблемы, которые нуждаются в дальнейшем исследовании и их возможном решении.

Список используемых источников:

1. Яндиев, И. Б. Исследование временных характеристик клавиатурного почерка для быстрой аутентификации личности / И. Б. Яндиев. — Текст : непосредственный // Молодой ученый. — 2017. — № 14 (148). — С. 154-158.

2. Ермошин, Р.В., Кузнецов, М.В. Комбинированный метод аутентификации пользователя на основе клавиатурного почерка [Текст]/ Р.В. Ермошин, М.В. Кузнецов// Работа поддержана грантом фонда содействия развитию малых форм предприятий. - Самара, 2014.

3. Машин В.А., Машина М.Н. Классификация функциональных состояний и диагностика психоэмоциональной устойчивости на основе факторной структуры показателей variability сердечного ритма// Российский физиологический журнал им. И.М. Сеченова, 2004. Т. 90(12). С. 1508-1521.

Zavatskaya A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Existing problems in approaches to the formation of user identification systems based on handwriting.

Taking into account the rapid pace of the development of information technologies, the increase in the number of informational threats, as well as the degree of uncertainty of their origin and implementation, the task of building an information security system is becoming increasingly more relevant in our time. One of the ways to minimize the threat of malicious attacks, as well as the risks of theft of confidential information, is to identify users by keyboard handwriting. This work is devoted to the review of the existing problems in approaches to the formation of user identification systems based on keyboard handwriting.

Key words: *keyboard handwriting, identification, psychophysiological state.*

УДК 654.024
ГРНТИ 49.34.06

ДЕЦЕНТРАЛИЗОВАННЫЙ МЕССЕНДЖЕР НА БАЗЕ ОТКРЫТОГО ПРОТОКОЛА МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ФЕДЕРАТИВНОЙ СЕТИ И МОСТОВ

И. И. Искра, С. С. Новиков, А. В. Помогалова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире пользуются популярностью различные системы мгновенного обмена сообщениями. В большинстве своём такие системы состоят из различных клиентов и одной общей сети. Такие сети никак не связаны между собой и поддерживать коммуникацию для клиентов разных сетей попросту невозможно. Протокол Matrix предоставляет способы объединить подобные сети через технологию мостов. Так же этот протокол позволяет создавать независимые экземпляры коммуникационных сервисов через возможности федераций.

Matrix, Synapse, Element, федерация, мосты, децентрализованные платформы

В настоящее время глобальную сеть Интернет невозможно представить в отрыве от систем мгновенного обмена сообщениями. Общение является одним из основных условий существования человеческого общества и личности. Именно поэтому возможность коммуницировать в реальном времени является одной из основных целей современных сетей.

Для подобного рода коммуникации необходима клиентская программа, так называемый мессенджер. В ранних версиях программ всё, что печатал пользователь, тут же передавалось. Если он делал ошибку и исправлял её, это также было видно. В таком режиме общение напоминало телефонный разговор. В современных программах сообщения появляются на мониторе собеседника уже после окончания редактирования и отправки сообщения. Как правило, мессенджеры не работают самостоятельно, а подключаются к центральному компьютеру сети обмена сообщениями, называемому сервером. Поэтому мессенджеры и называют клиентами (клиентскими программами). Термин является понятием из клиент-серверных технологий.

На данный момент существует огромное количество реализаций сетей и работающих с ними клиентских программ. Клиенты могут быть реализованы для разных платформ, иметь уникальный дизайн и функционал. Причём существуют такие, которые объединяют в себе возможности для работы с несколькими различными сетями.

Каждая из этих сетей разработана отдельной группой разработчиков, имеет отдельные серверы и протоколы, отличается своими правилами и особенностями. Между различными сетями обычно нет прямой связи (только в XMPP существует понятие межсетевое транспорта), таким образом, пользователь сети *Telegram* не может связаться с пользователем сети *Discord*.

А это значит, что для общения с пользователями из другой сети для начала нужно создать аккаунт в этой самой сети. Исходя из этого была обозначена ключевая цель *Matrix* [1] — стать основной системой для отправки сообщений и синхронизации данных по всей сети, позволяя людям, сервисам и устройствам легко общаться друг с другом, давая пользователям контроль над своими данными и выбор между сервисами и вендорами, которые они захотят использовать.

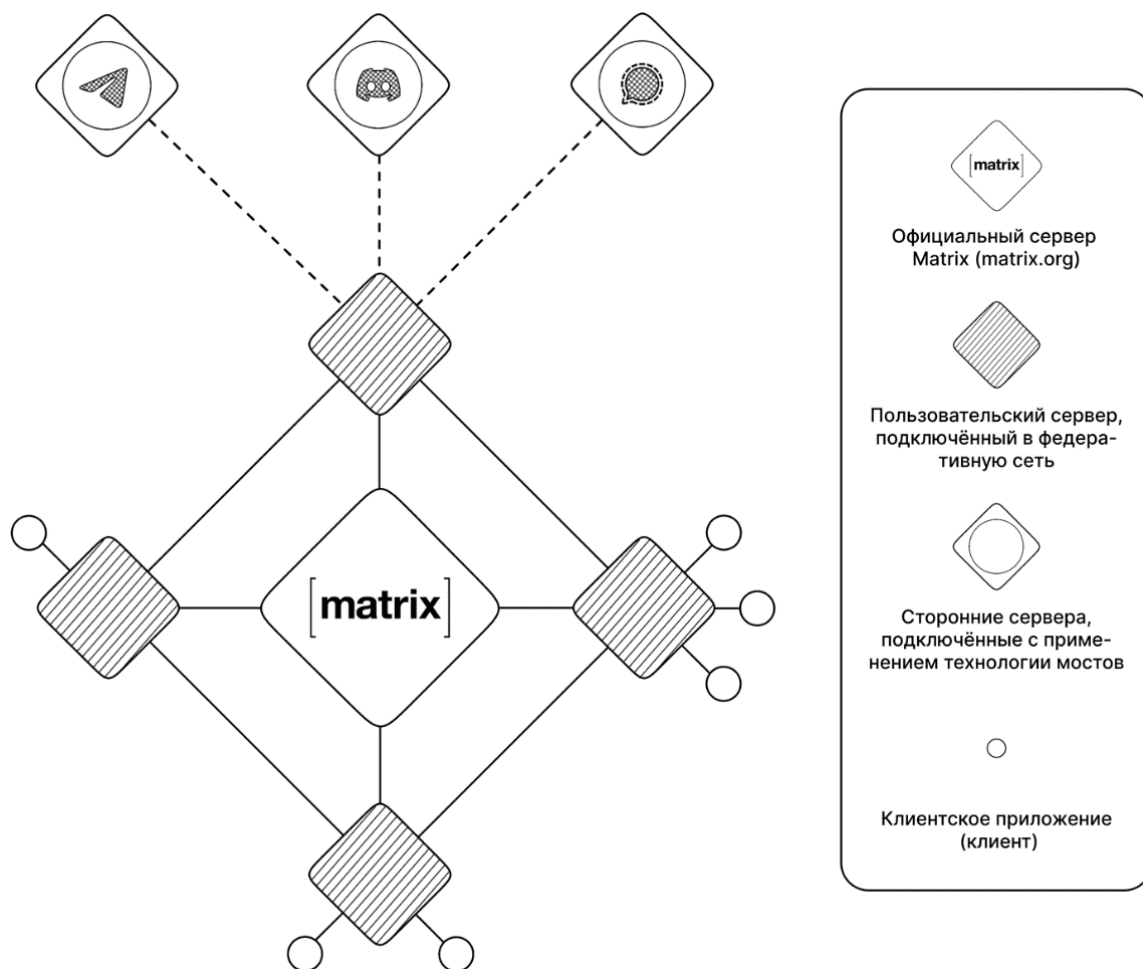
Matrix — это открытый и свободный протокол для децентрализованного и федеративного общения в реальном времени. Он может быть использован для мгновенных сообщений, аудио- и видеосвязи с помощью *WebRTC*, интернета вещей и чего угодно, где может понадобиться стандартный *HTTP API*.

Федерация позволяет независимым экземплярам коммуникационных сервисов общаться между собой - например, как почтовый сервер *Gmail* взаимодействует с почтовым сервером *Microsoft*, когда отправляется письмо с *@gmail.com* на *@hotmail.com*. В федерации сами сервера обмениваются данными между собой, понимая друг друга, схематичное изображение процесса приводится на рис. 1. *Matrix* обеспечивает открытую федерацию — это означает, что любой в интернете может присоединиться к экосистеме *Matrix*, развернув свой сервер.

Каждый сервер хранит историю и данные аккаунта всех его клиентов, а также обменивается данными со всей многочисленной *Matrix* экосистемой, синхронизируя историю бесед с другими серверами и их клиентами. Клиенты как правило общаются между собой обмениваясь событиями в контексте виртуальных комнат. Данные комнаты дублируются на все сервера, чьи клиенты принимают участие в данной комнате.

Также *Matrix* поддерживает передачу сообщений из разных чат-приложений в комнаты *Matrix*. Такая технология называется мостами, схематично изображена на рис. 1. Эти мосты представляют собой программы, которые работают на сервере и взаимодействуют с серверами, не относящимися к *Matrix*. Мосты могут действовать как марионетки или ретрансляторы, где в первом случае учетная запись отдельного пользователя явно публикует сообщения, а во втором бот публикует сообщения для учетных записей пользователей.

На данный момент официально поддерживаются [2] мосты для следующих сервисов: *Gitter*, *IRC*, *Slack/Mattermost* и *XMPP*. Мосты для большинства других приложения поддерживаются сообществом, в их числе: *iMessage*, *Discord*, *Telegram*, *Signal* и многие другие.


 Рис. 1. Архитектура сети *Matrix*

Matrix определяет стандарт и предоставляет *open-source* реализации серверов, клиентов, инструментов для разработки (*SDK*) и сервисов приложений, чтобы помочь в создании новых или в расширении существующих решений для коммуникации.

Подводя итог, система *Matrix* относительно молодая и только набирает свою популярность, но уже можно заметить хорошую поддержку со стороны команды разработчиков и сформировавшегося сообщества. Технология мостов позволит связать уже сформированные группы и чаты в других сетях. А возможности федеративной архитектуры — поддерживать связь с пользователями за пределами домашнего сервера. Таким образом, основные идеи, которые заложены в философию этого продукта хорошо резонируют с потребностями современных компаний, любых других групп и объединений. Поэтому можно с уверенностью назвать *Matrix* перспективным и многообещающим проектом в области мгновенного обмена сообщениями.

Список используемых источников:

1. Matrix: An open network for secure, decentralized communication [Электронный ресурс]. URL: <https://matrix.org/> (дата обращения 11.11.2022).
2. Matrix specification [Электронный ресурс]. URL: <https://spec.matrix.org/v1.3/> (дата обращения 11.11.2022).

Iskra I., Novikov S., Pomogalova A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

A decentralized messenger based on an open instant messaging protocol using federated network and bridge technologies.

In the modern world, various instant messaging systems are popular. For the most part, such systems consist of different clients and one common network. Such networks are not interconnected in any way and it is simply impossible to maintain communication for clients of different networks. The Matrix protocol provides ways to combine similar networks through bridge technology. Also, this protocol allows you to create independent instances of communication services through the capabilities of federations.

Key words: Matrix, Synapse, Element, Federation, Bridges, Decentralized Platforms.

УДК 004.9
ГРНТИ 20.53

АНАЛИЗ ПРОБЛЕМАТИКИ ЭКСПЛУАТАЦИИ СИСТЕМ ОБЕСПЕЧЕНИЯ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

С. А. Клабуков, А. А. Федоров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Проведен анализ проблематики эксплуатации систем обеспечения центров обработки данных. Рассмотрены уровни сертификации Uptime Institute. Выявлены компоненты системы обеспечения, которым не уделяется должное внимание при техническом обслуживании. Описаны способы обнаружения проблем с перегревом устройств в дата-центрах. Приведены тенденции в области эксплуатации. Заявлено перспективное направление развития систем обслуживания центров обработки данных по фактическому состоянию.

Uptime Institute, центр обработки данных, отказоустойчивость, обслуживание, охлаждение, звуковые сигнатуры

Центры обработки данных безусловно являются сложными инженерными системами, которые нуждаются в постоянном техническом обслуживании и контроле. Логично что, как и у любых других сложных инженерных систем у центров обработки данных есть свои требования к эксплуатации, однако из-за того, что на разных объектах используются разные внутренние элементы, у этих систем отсутствует единая программа эксплуатации. Из-за этого при прохождении сертификации Uptime Institute на операционную устойчивость, каждый объект рассматривается индивидуально. Известны четыре уровня стандарта Uptime Institute, что предоставлен на рис. 1.

	Tier I	Tier II	Tier III	Tier IV
Минимальное кол-во активных компонентов, поддерживающих ИТ-нагрузку	N	N+1	N+1	N после любого отказа
Каналы распределения — входной участок системы энергоснабжения	1	1	1 активный и 1 запасной	2 активных одновременно
Распределение бесперебойного энергоснабжения	1	1	2 активных одновременно	2 активных одновременно
Concurrently Maintainable (возможно обслуживание без остановки)	Нет	Нет	Да	Да
Fault Tolerance (отказоустойчивость)	Нет	Нет	Нет	Да
Compartmentalization (секционирование).	Нет	Нет	Нет	Да
Непрерывное охлаждение	Нет	Нет	Нет	Да

Рис. 1. Четыре уровня стандарта Uptime Institute

При этом каждый следующий уровень сертификации включает в себя требования для всех предыдущих уровней.

Кроме того, данные уровни показывают ожидаемый уровень безотказной работы дата-центра. Для Tier I – это 99,671% (1729 минут годового простоя), для Tier II – это 99,741% (1361 минут годового простоя), для Tier III – это 99,982% (95 минут годового простоя), и для Tier IV – это 99,995% (26 минут годового простоя) [1]. Если использовать случай среднего простоя длительностью 90 минут, средняя стоимость одного простоя обходится приблизительно в 505500 долларов США.

Основой для обеспечения непрерывного охлаждения и высоких показателей отказоустойчивости является своевременное техническое обслуживание. Бен Киссел, директор отдела сервисных решений компании Emerson Network Power в подразделении Liebert Services уверен в том, что должным образом организованное техническое обслуживание позволяет избегать около трети простоев: “По нашим оценкам, 30-40% отключений систем, обусловленных отказами оборудования, можно предупредить с помощью соответствующего профилактического обслуживания” [2].

В технической документации компании APC “Preventive Maintenance Strategy for Data Centers” (“Стратегия профилактического обслуживания дата-центров”), говорится, что, как правило, трансформаторы, распределительные блоки питания (PDU) и системы распределения воздуха и воды требуют мало обслуживания, тогда как такое оборудование как модули CRAC, системы пожаротушения, чиллеры и генераторы требуют высокого уровня обслуживания. Другое оборудование, типа систем бесперебойного питания, следующего поколения источником бесперебойного питания (ИБП), могут требовать всего лишь среднего уровня обслуживания.

В ряде дата-центров некоторые области, обычно, страдают от недостаточного внимания к техническому обслуживанию. Бен Киссел выделяет несколько таких областей, включая коммутационное оборудование, автоматические выключатели, ATS (автоматический ввод резерва) и PDU, а также критические системы, например, ИБП, аккумуляторы и оборудования системы охлаждения, кондиционирования и вентиляции. Однако некоторые не столь очевидные тактические приемы позволяют быстро и легко обнаруживать проблемы в системах до того, как они станут причиной простоя. Например, можно использовать термографию, основанную на методах инфракрасного сканирования, которая позволяет локализовать источники целого ряда проблем. Также для технического обслуживания можно использовать такой инструмент, как вычислительная гидродинамика. Данный инструмент позволяет администратору центра обработки данных с помощью соответствующего программного обеспечения или с помощью стороннего провайдера сервиса моделировать воздушные потоки и распределение тела в центре обработки данных [3], представленных на рис. 2.

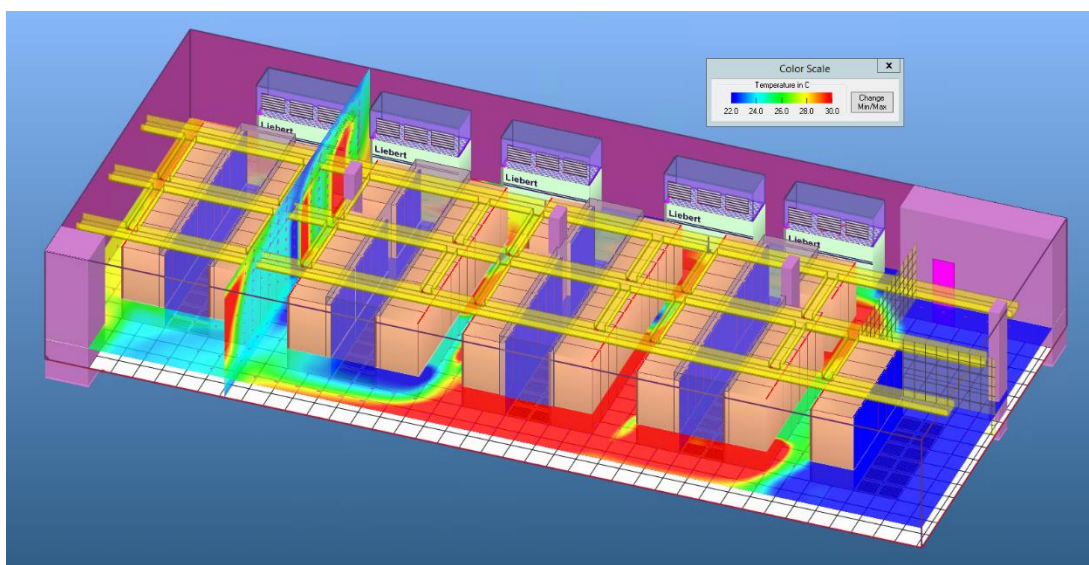


Рис. 2. Распределение воздушных потоков и их температура.

Одна из наиболее интересных тенденций сегодняшнего времени в области эксплуатации дата-центров — использование системы прогнозирования состояния [4]. Связано это с тем, что традиционные системы обслуживания производственных объектов по плановым показателям становятся весьма неэффективны из-за своей дороговизны. Поэтому в последнее время наметилась тенденция к управлению надежностью и обслуживанию по фактическому состоянию, когда все работы по ремонту и техническому обслуживанию производятся в зависимости от состояния системы. Система контроля за эксплуатацией по фактическому состоянию подразумевает большое количество систем мониторинга. Необходимость планового ремонта по фактическому состоянию позволяет сократить количество ремонтов в несколько раз. Это огромный потенциал для экономии, особенно в крупных центрах обработки данных.

Перспективным направлением развития систем обслуживания центров обработки данных по фактическому состоянию является разработка аппаратно-программного комплекса построения звуковых сигнатур технических систем в реальном времени. Данная система позволит своевременно обслуживать системы обеспечения температурно-влажностного режима центров обработки данных. В дальнейшем мы планируем разработать вышеописанный аппаратно-программный комплекс.

Список используемых источников:

1. Классификация ЦОД Tier. [Электронный ресурс]. URL: https://habr.com/ru/company/cloud_mts/blog/332864/.
2. Инженерная структура центров обработки данных. [Электронный ресурс]. URL: <http://dcnt.ru/?p=9443/>.
3. CFD моделирование. [Электронный ресурс]. URL: <https://www.dataspace.ru/services/colocation/cfd-modelirovanie-potokovykh-protsessov-v-tsode/>
4. Жизнь ЦОДа после сдачи в эксплуатацию. [Электронный ресурс]. URL: <https://habr.com/ru/company/datapro/blog/231751/>

Klabukov S., Fedorov A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of the problems of operation of data center security systems.

The problems of data center support systems operation are analyzed. Levels of Uptime Institute certification are considered. The components of the provisioning system that are not given proper attention during maintenance are identified. Ways to detect problems with overheating devices in data centers are described. Maintenance trends are given. The future direction of data center maintenance systems by actual state is stated.

Key words: *Uptime Institute, data center, fault tolerance, maintenance, cooling, sound signature.*

УДК 004.457
ГРНТИ 20.53.23

СИСТЕМА ОБМЕНА СООБЩЕНИЯМИ ПО ШАБЛОНУ ПРОЕКТИРОВАНИЯ «ИЗДАТЕЛЬ - ПОДПИСЧИК»

П. С. Кукушкин, Е. Э. Кулигина, Г. В. Степаненков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Согласно отчету "DIGITAL 2022: THE RUSSIAN FEDERATION" в России насчитывается 129,8 миллионов интернет-пользователями. Таким образом, уровень проникновения интернета в России на начало года достиг 89,0% от общей численности населения, что на 4,7% выше прошлого года. Каждый месяц на домене .ru регистрируют больше чем по 100 тысяч новых доменов. Это постоянное увеличение числа новых сайтов и интернет-пользователей требует более оптимальных способов разработки систем распределенного обмена сообщениями, для связи между приложениями, а также между приложениями и пользователями. Одним из вариантов решения этой проблемы может стать разработка системы по шаблону проектирования «издатель – подписчик». Подобная система значительно облегчить и ускорить разработку новых сервисов и систем.

шаблон проектирования «Издатель – подписчик»

Введение

Вследствие возросшего уровня информатизации современного общества, так же появилась необходимость сокращать время разработки различных сервисов и систем. Для большинства интернет-ресурсов критически важно сохранять связь со своими клиентами. Распределенная система доставки сообщений спроектированная по шаблону «издатель – подписчик», развернутая на облачной инфраструктуре, и предоставляемая сторонним разработчикам в качестве услуги может значительно упростить и ускорить разработку.

Шаблон проектирования

«Издатель – подписчик» (так же известный как Pub/Sub) - это шаблон обмена сообщениями, при котором отправители сообщений, называемые издателями, напрямую не привязаны программным кодом отправки сообщений к получателям, называемым подписчиками, а вместо этого классифицируют опубликованные сообщения по топикам и не содержат сведений, какие подписчики, если таковые имеются, могут быть у этого топика. Аналогичным образом, подписчики обращаются к одному или нескольким классам и получают только сообщения, представляющие интерес, не зная, какие издатели, если таковые имеются, есть. Шаблон «Издатель – подписчик» концептуально очень близок к парадигме очереди сообщений [1] и обычно является частью более крупной системы промежуточного программного обеспечения, ориентированной на сообщения.

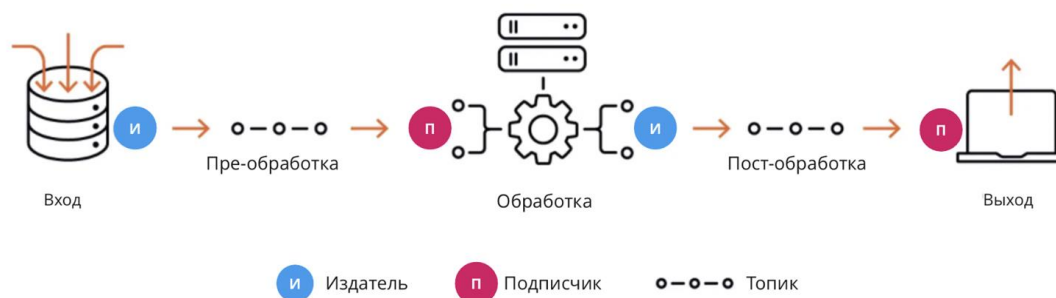


Рис. 1. Пример системы проектированной по шаблону «издатель – подписчик»

Хотя этот шаблон основан на более ранних шаблонах проектирования, таких как очередь сообщений и брокеры событий, он более гибкий и масштабируемый. Ключевой фактор этого способа в том, что Pub/Sub позволяет перемещать сообщения между разными компонентами системы, при этом компоненты ничего не знают об идентичности друг друга. Пример схемы шаблона приведен на рис. 1.

Шаблон «Издатель – подписчик» развился из-за необходимости расширения масштабов информационных систем. В эпоху до Интернета и даже в первые дни Интернета системы в основном масштабировались статически. Однако с расширением Интернета и веб-приложений, вызванного массовым внедрением мобильных устройств и устройств IoT, системы должны были динамически масштабироваться.

С помощью этой архитектуры разработчик может программировать модули на изолированные и четко определенные обязанности, поэтому модулям больше не нужно хранить информацию о местонахождении других модулей. Модули ввода принимают только пользовательский ввод, модули обработки обрабатывают только данные, а модули вывода отображают только выходные данные.

Данная архитектура может применяться в большом количестве сервисов и веб-приложений. Приложение чата является классическим примером использования этого шаблона [2]. В приложении чата участники могут подписаться на чаты, которые являются отдельными топиками сообщений в шаблоне «издатель – подписчик». Когда пользователь отправляет сообщение в чат, его экземпляр приложения чата публикует сообщение в топике, а подписчики топика получают сообщение.

Преимущества использования шаблона «издатель – подписчик»

Создание масштабной информационной системы с использованием шаблона Pub/Sub приносит пользу всем заинтересованным сторонам, разработчикам, архитекторам, тестировщикам. Процесс разработки

программного обеспечения выигрывает от простоты шаблона Pub/Sub. Из основных преимуществ для разработчиков можно выделить следующие:

Системы, построенные на Pub/Sub, позволяют разработчикам разделять систему на модули на основе бизнес-логики системы. Модульзация и разделение проблем приводят к улучшению качества кода.

Разработка программного обеспечения, независимого от языка - приложение разбито на более мелкие логические части. Эти части разрабатываются с использованием подходящего языка программирования. Взаимосвязь между частями происходит через Pub/Sub. Фактически, Pub/Sub сшивает компоненты в одно рабочее программное обеспечение.

Ясность в бизнес-логике - брокер сообщений берет на себя ответственность за надежную доставку сообщения, тем самым освобождая разработчика от написания дополнительного кода. Вследствие чего кодовая база становится проще и удобнее для чтения.

Повышение отзывчивости - в программном шаблоне Pub/Sub связь асинхронна. Это позволяет разрабатывать отдельные модули также асинхронно. Доставка сообщений не блокирует издателя. Издатель возвращается к своей задаче сразу же после публикации сообщения. Аналогично, подписчик прерывается только при появлении сообщения на подписанную тему.

Недостатки использования шаблона «издатель – подписчик»

Но каждый шаблон проектирования имеет свои ограничения и компромиссы. И есть сценарии использования, когда шаблон «издатель – подписчик» будет плохим выбором:

Издатель – подписчик - будет избыточным для простой системы, которые вряд ли будут масштабироваться. В системах, где динамическое масштабирование не требуется и где будет достаточно статического масштабирования, использовать эту архитектуру будет не оптимальным выбором.

Потоковое аудио и видео имеют нюансы требования к плавному рендерингу со стороны пользователя. Синхронная связь "точка-точка" между двумя конечными точками является лучшим решением для потоковой передачи мультимедиа. Pub/Sub не подходит для переноса трафика VoIP или видеотелефонии через Интернет.

Несмотря на многочисленные достоинства Pub/Sub, крайне важно выбрать правильную инфраструктуру для внедрения этого шаблона проектирования. В противном случае это может помешать масштабируемости системы и создать проблемы с надежностью.

Система обмен сообщениями по шаблону проектирования «издатель – подписчик» может быть развернута самостоятельно или развернута в предварительно настроенной облачной инфраструктуре и предоставляться разработчикам как услуга.

Предложенная система

Вся система состоит из нескольких асинхронных микросервисов (Рис. 2.). Вся система постоянная по шаблону проектирования издатель-подписчик. Роль

издателя может выполнят сторонний сервис с которым настроенная интеграция, например частный сервер Gitlab. Так же у пользователей будет возможность интегрировать собственный продукт при помощи API которая будет

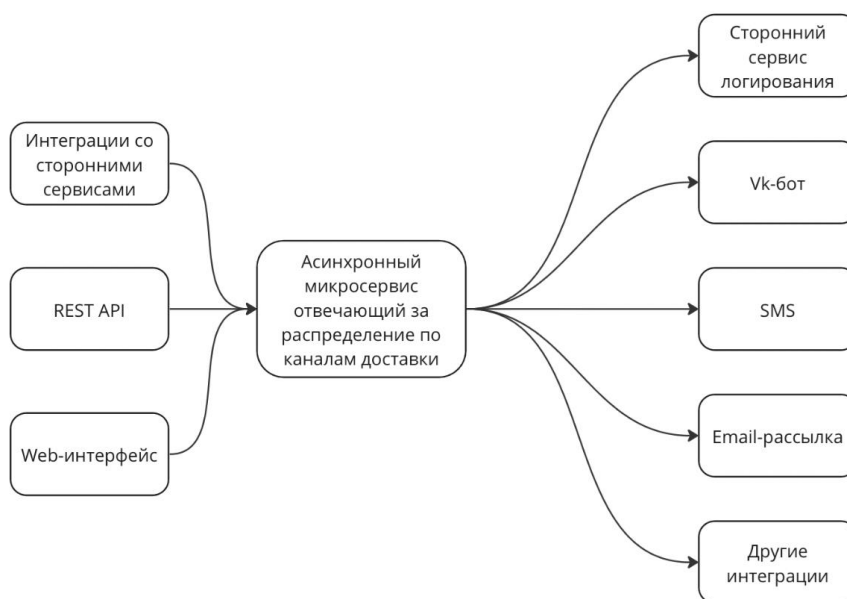


Рис. 2. Примерная структурная схема предлагаемой системы

представленная сервисом.

И помимо программных интеграция у пользователя будет возможность добавить сообщение в топик через веб веб интерфейс. Через этот веб интерфейс у пользователя будут и другие возможности. Так же через этот веб интерфейс у пользователя будет возможность создавать и настраивать топики сообщений. В качестве настройки у пользователя будет возможность подключать каналы рассылки сообщений, указывать срок хранения сообщений, которые публикуются в созданных им топиках. Также в системе есть асинхронный микросервис, который будет отвечать за обработку сообщений которые были опубликованы в топиках.

Последней составляющей системы является набор микросервисов, которые отвечают за постобработку сообщений. Пост-обработка делится на два типа, в зависимости от "подписчиков" которые подписаны на топик. Первый тип это доставка сообщений в другой сервис, через заранее настроенную интеграцию - например в сервис для логирования. Второй вариант, это доставка сообщения до конкретного клиента пользователя, который пользуется сервисом для интеграции его в бизнес-процессы своих систем.

Каналы доставки сообщений до клиента могут быть следующими:

SMS

Доставка каких либо сообщений до клиента через смс. Перед подключением этого канала доставки сообщений пользователю будет предоставленная тестовая среда. У тестовой среды будет ограничения на количество номеров телефонов,

на которые можно будет отправлять сообщения. Для добавления номера телефона в тестовую среду необходимо будет подтвердить что номер телефона действительно принадлежит пользователю. Процесс верификации будет проходить по средствам отправки верификационного кода на номер который пользователь хочет добавить.

Email-рассылка

Доставка сообщений через этот канал распространения будет отправлять письма клиентам пользователя через почтовые сервера. у пользователя будет возможность указать данные конкретного почтового сервера через который он хочет рассылать письма. по умолчанию письма будут рассылаться через собственный почтовый сервер системы.

Интеграция с социальной сетью Вконтакте

Эта интеграция позволит пользователю подключить свое сообщество в социальной сети Вконтакте. Для этого необходимо будет создать ключ доступа в настройках сообщества, и добавить его в систему. при добавлении этого способа доставки сообщений, будет возможность рассылки сообщений либо всем пользователям, которые дали разрешение на отправку им сообщений от имени сообщества. либо конкретным клиентам, которых пользователь подписал на топик.

Так же архитектура сервиса позволяет добавлять и другие способы доставки сообщений клиентам пользователя.

Заключение

Подобный сервис может быть развернут на облачной инфраструктуре и предоставляется как услуга. Набор уже готовых интеграций и простота в подключении новых каналов распространения сообщений значительно упростит и ускорит разработку сервисов и систем, в которых необходимо постоянно поддерживать связь с пользователями системы. Помимо массовых рассылок в сервисе может быть реализована доставка одиночных сообщений через SMS или почтовые сервисы. Подобный функционал можно будет использовать для доставки одноразовых паролей или для верификации контактных данных клиента.

Список используемых источников:

1. Microsoft. Message Queuing. 2022. - [Электронный ресурс]. URL: [https://learn.microsoft.com/en-us/previous-versions/windows/desktop/legacy/ms711472\(v=vs.85\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/desktop/legacy/ms711472(v=vs.85)?redirectedfrom=MSDN) (дата обращения: 28.10.2022)
2. Aply. Pub/Sub Examples: 5 Use Cases to Understand the Pattern and its Benefits. 2022. - [Электронный ресурс]. URL: <https://ably.com/blog/pub-sub-pattern-examples> (дата обращения: 14.11.2022)

Kukushkin P., Kuligina E., Stepanenkov S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Messaging system based on the "Publisher/Subscriber" design pattern.

According to the report "DIGITAL 2022: THE RUSSIAN FEDERATION" there are 129.8 million Internet users in Russia. Thus, the level of Internet penetration in Russia at the beginning of the year reached 89.0% of the total population, which is 4.7% higher than last year. Every month, more than 100 thousand new domains are registered on the .ru domain. This constant increase in the number of new sites and Internet users requires more optimal ways to develop distributed messaging systems for communication between applications, as well as between applications and users. One of the solutions to this problem may be the development of a system based on the "publisher – subscriber" design pattern. Such a system will greatly facilitate and accelerate the development of new services and systems.

Key words: Publish/Subscribe pattern, sms, web application.

УДК 004.75
ГРНТИ 49.34.01

DDNS КАК НОВЫЙ ЭТАП РАЗВИТИЯ СЕРВИСОВ КОНТРОЛЯ И ПРИСВОЕНИЯ ДОМЕННЫХ ИМЕН

В. А. Мишаков, А. В. Помогалова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. Бонч-Бруевича

В данной статье разбираются общие принципы технологий, лежащих в основе современной системы доменных имён, производится выявление их недостатков, а также анализ также анализ современных подходов контроля присвоения доменных имен. На основании полученных данных делаются предложения по основным требованиям к DDNS.

блокчейн, система доменных имён, сертификация, сети, децентрализация, обратная совместимость

На сегодняшний день, почти невозможно представить сеть интернет без этих двух основополагающих технологий: dns и ssl/tls. Так, с 2016 года, количество активных доменов выросло с 906 миллионов, до более чем 1 миллиарда 167 тысяч [1], а количество пользовательских запросов, использующих защищённое соединение превысило 86% [2]. В связи со столь широкой распространённостью, возникает вопрос о том, насколько хороши эти технологии, и имеют ли они какие-то недостатки. Рассмотрим основные из основные особенности и недостатки, из-за которых они смогли занять столь значимое место в устройстве современной сети интернет.

DNS (Domain Name System) – это распределённая система, созданная для получения информации о доменах; чаще всего используется для получения ip-адреса из доменного имени. Отличительной особенностью DNS является иерархичность: каждый сервер может передать ответственность за часть домена другому серверу (рис. 1).

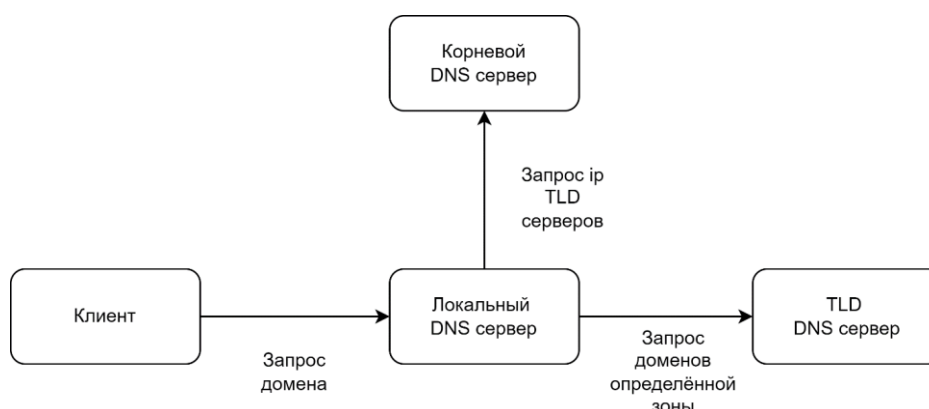


Рис. 1. Схема разрешения имени при помощи DNS

Несмотря на то, что DNS сумел стать всемирным стандартом, он всё ещё имеет много недостатков:

- Централизация.

Несмотря на то, что DNS сервера развернуты по всему миру, реестр может контролироваться только одной некоммерческой организацией - ICANN, находящейся в США.

- Уязвимости незашифрованного DNS.

По причине того, что даже сегодня, процент незашифрованных DNS запросов остаётся достаточно высок [3], пользователи остаются уязвимы к атакам типа “Человек посередине” (что может привести не только к утечке информации о посещаемых сайтах, но и подмены искомого ресурса злоумышленником), а также к слежке со стороны провайдера.

- Сложность входа.

Рынок DNS становится всё более недоступным для новых игроков. Так, 98% умных ассистентов и 72% умных тв используют Google DNS без возможности его сменить [4]. В следствии этого, отказ от обслуживания таким DNS провайдером отдельного ресурса может нанести этому ресурсу непоправимый вред.

- Скорость актуализации данных.

В случае внесения изменений в DNS запись, публикация изменений на все DNS сервера может занять до 72 часов [5].

- Зависимость от организаций, выпускающих домены.

Пользователь не имеет прямого управления над доменом, что оставляет простор для обмана со стороны регистратора.

SSL(Secure Sockets Layer)/TLS(Transport Level Security) — это протоколы, обеспечивающие защищенную передачу данных в сети. Они широко используются во всех сферах связи, начиная с веб-браузеров, а также при работе с электронной почтой и заканчивая обменом мгновенными сообщениями и IP-телефонией. После своего широкого распространения, значительно повысили безопасность пользования интернетом, позволив перевести в онлайн даже такие чувствительные к безопасности сервисы, как банкинг. При этом, они также имеют ряд недостатков:

- Уязвимости.

Несмотря на то, что SSL/TLS делает сайты значительно более безопасными, это совершенно не значит, что у него нет уязвимостей, например, уязвимость POODLE [6], подставившая в своё время значительное количество пользователей под удар.

- Использование устаревших версий.

Способы обхода защиты развиваются почти с той же скоростью, что и сама защита. Именно поэтому стоит использовать как можно более современные версии протоколов. При этом, 68% сайтов всё ещё поддерживают TLS 1.0, а почти 7% из 100 000 самых популярных веб ресурсов всё ещё разрешают подключаться к ним с использованием SSL 2.0 и SSL 3.0 [7]

- Централизованный выпуск сертификатов.

Несмотря на успехи Let's Encrypt, предложивших в своё время выпуск бесплатных сертификатов и на порядки увеличившую долю защищённого трафика [8], сильная централизация отрасли и высокая плата за выпуск сертификата всё ещё являются большими проблемами, требующими решения.

- Замедление скорости и рост потребления памяти.

Хоть и на персональных компьютерах и современных смартфонах проблема может не стоять так резко, однако, носимая электроника и устройства интернета вещей могут столкнуться с проблемой нехватки производительности. [9].

В рамках данной работы предлагается альтернативное решение, которое позволит избежать обозначенных ранее недостатков.

Блокчейн — это частный случай технологии распределенного реестра (DLT), который состоит из растущего списка записей, называемых блоками, которые надежно связаны друг с другом с помощью криптографии. Каждый блок содержит криптографический хэш предыдущего блока, метку времени и данные транзакции (обычно представляемые в виде дерева Меркла, где узлы данных представлены листьями). Временная метка доказывает, что данные транзакции существовали на момент создания блока. Поскольку каждый блок содержит информацию о предыдущем блоке, они фактически образуют цепочку (сравните структуру данных связанного списка), где каждый дополнительный блок связан с предыдущими блоками. Следовательно, транзакции блокчейна необратимы в том смысле, что после их записи данные в любом данном блоке не могут быть изменены задним числом без изменения всех последующих блоков.

Именно благодаря этим свойствам блокчейна стало возможно избежать проблем с централизацией процессов выдачи доменов и сертификатов в руках крупных институтов, а также предоставить прозрачный инструментарий по управлению доменами конечному пользователю.

Система DDNS (Distributed DNS) должна будет предоставлять возможность ведения децентрализованного регистра доменных имён на базе уже существующего блокчейна. DDNS будет гарантировать право конкретного пользователя на домен, а также предоставлять ему возможность подписания трафика приватным ключом по схожему с TLS алгоритму (рис. 2).

Одной из важнейших особенностей DDNS должна стать возможность обеспечения максимально возможной совместимости с существующими решениями. Так, например, система доменных имён должна быть доступна не только через API блокчейна, но и через открытый API, совместимый с DNS.

К системе должны быть выдвинуты следующие требования:

- Домен и сертификат должны представлять собой единую сущность.
- Домены должны приобретаться через аукцион.
- Покупка доменов должна осуществляться за токены в сети ethereum, выпущенные специально для DDNS.
- Время владения доменом должно быть ограничено. За некоторое время до его истечения пользователь будет иметь возможность продления без участия в аукционе. В случае непродления, домен будет возвращаться в общий список доменов, доступных для покупки.
- Должна присутствовать возможность передачи доменов между участниками сети.
- Должна присутствовать система перевода доменов из существующих доменных зон.

- Оптимальным решением по реализации клиентской стороны будет расширение для браузера, предоставляющее доступ к DDNS по префиксу “dw.”, вместо www.

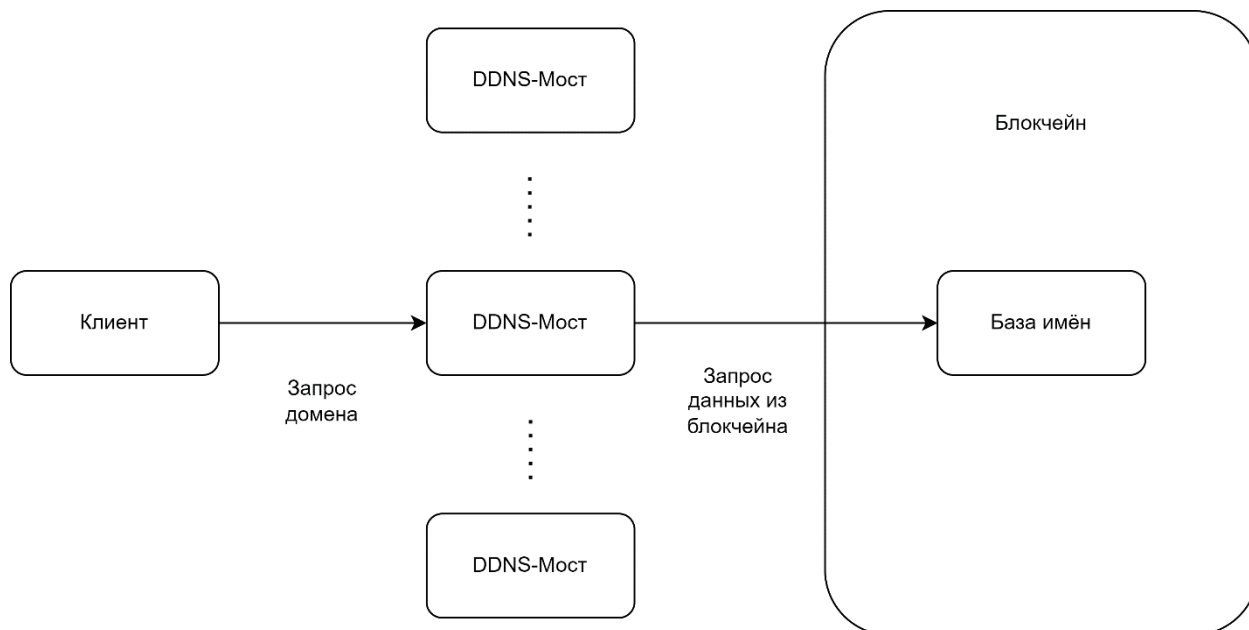


Рис. 2. Схема разрешения имени при помощи DDNS

Заключение

В данной работе были проанализированы современные технологии, используемые в системе доменных имён, выделены и проанализированы их недостатки и перспективы, а также выдвинуты некоторые предложения по разработке системы, решающей многие проблемы текущей связки DNS плюс SSL/TLS.

Список используемых источников:

1. Nick, Huss How Many Websites Are There in the World? / Huss Nick. — Текст : электронный // siteefy.com : [сайт]. — URL: <https://siteefy.com/how-many-websites-are-there/#The-Reasons-for-the-Growth> (дата обращения: 31.10.2022).
2. David, Warburton 2019 TLS TELEMETRY REPORT / Warburton David. — Текст : электронный // f5.com : [сайт]. — URL: <https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/F5Labs-2019-TLS-Telemetry-Report-Summary.pdf> (дата обращения: 31.10.2022).
3. Sebastián, García Large Scale Measurement on the Adoption of Encrypted DNS / García Sebastián. — Текст : электронный // arxiv.org : [сайт]. — URL: <https://arxiv.org/pdf/2107.04436.pdf> (дата обращения: 31.10.2022).
4. Hammad, M. M. Characterizing Smart Home IoT Traffic in the Wild / M. M. Hammad. — Текст : электронный // arxiv.org : [сайт]. — URL: <https://arxiv.org/pdf/2001.08288.pdf> (дата обращения: 31.10.2022).
5. DNS Propagation: A Necessary Evil?. — Текст : электронный // ns1.com : [сайт]. — URL: <https://ns1.com/resources/dns-propagation> (дата обращения: 31.10.2022).
6. Alert (TA14-290A) SSL 3.0 Protocol Vulnerability and POODLE Attack. — Текст : электронный // Cybersecurity and Infrastructure Security Agency : [сайт]. — URL: <https://www.cisa.gov/uscert/ncas/alerts/TA14-290A> (дата обращения: 31.10.2022).

7. Nick, Galov 21 SSL Statistics that Show Why Security Matters so Much / Galov Nick. — Текст : электронный // webtribunal.net : [сайт]. — URL: <https://webtribunal.net/blog/ssl-stats/> (дата обращения: 31.10.2022).
8. Let's Encrypt Stats. — Текст : электронный // letsencrypt.org : [сайт]. — URL: <https://letsencrypt.org/stats/> (дата обращения: 31.10.2022).
9. John, W. P. SSL Performance Problems / W. P. John. — Текст : электронный // bemonitor.com.mx : [сайт]. — URL: <http://bemonitor.com.mx/docs/competitive/SSL%20Performance%20Problems.pdf> (дата обращения: 31.10.2022).

Mishakov V., Pomogalova A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

DDNS as a new stage of domain name control and assignment services development.

The following article examines the general principles of the technologies that underlie the modern domain name system, identifies their shortcomings, as well as analyzes and analyzes modern approaches to control the assignment of domain names. Based on the data obtained, proposals are made on the basic requirements for DDNS.

Key words: blockchain, domain name system, certification, networks, decentralization, backward compatibility.

УДК 004.75
ГРНТИ 49.33.29

АНАЛИЗ P2P-СЕТЕЙ НА ОСНОВЕ СУЩЕСТВУЮЩИХ РЕШЕНИЙ

Н. А. Мурашкин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современное общество невозможно представить без связи. Интернет, мобильная связь, спутниковые коммуникации, распределенные сети – всё это есть у человечества благодаря технологическому прогрессу, а он в свою очередь раскрывается в новых технологиях. В начале 21 века был представлен первый концепт распределенной системы файлообмена, построенной на протоколе Napster для передачи музыки через центральный сервер другим пользователям. В данный момент наиболее популярным применением P2P-сети становится блокчейн, технология которого имеет огромные перспективы. В данной статье будет представлен анализ наиболее популярных существующих P2P-сетей, начиная с истоков.

P2P, Blockchain, одноранговая сеть, Napster, Gnutella, BitTorrent, распределенные сети

Протокол файлообмена Peer-to-Peer (P2P) — важнейшая часть технологии блокчейн, осуществляющая создание мощной и надежной сети. В отличие от централизованных систем передачи информации, P2P не могут быть выведены из строя единственной DDOS-атакой на центральный сервер, что является огромным преимуществом в хранении и передаче информации между пользователями сети.

Принцип работы P2P сети заключается в следующем: пользователь одновременно использует сеть и обеспечивает её существование благодаря предоставлению вычислительной мощности своего устройства. Такая сеть содержит неопределенное количество одноранговых узлов (или нод), которые имеют равные права по сравнению с другими. Нода предоставляет часть вычислительных ресурсов напрямую другим участникам без необходимости управления центральным сервером или хостом. Под вычислительными ресурсами понимаются: дисковое хранилище, мощность процессора или пропускная способность сети. Равноправие узлов ограничено соответствующими ролями в рамках схемы экосистемы. Таким образом, сеть блокчейна может существовать благодаря нескольким видам ролей: майнерам (устройствам, добывающим блоки), легким узлам (нодам, хранящим неполную информацию о блоках транзакций) и полным узлам (нодам, хранящим полную информацию о блоках транзакций, начиная с genesis-блока). Информация, хранящаяся в блокчейне, не может быть потеряна, изменена или уничтожена, поскольку, чтобы это сделать нужно уничтожить все полные узел в этой сети. Отсюда следует, если существует единственный узел с полной копией блокчейна, то все записи остаются нетронутыми. [1]

Родоначальником архитектуры P2P было приложение Napster, выпущенное в 1999 году, где технология была внедрена для обмена файлами. Пользователи данного приложения обращались к системе из нескольких компьютеров, на

которых хранились музыка или фильмы. Фундаментом данной системы являлись центральные сервера, имеющие список файлов и адреса пиров. Пир(клиент) подключался к серверу, а тот, в свою очередь, посылал ему адреса пиров, имеющих необходимый файл. Затем, через этот же сервер клиент устанавливал соединение с пиром, обладающим файлом для передачи, и производил передачу файла. Прямое соединение между пирами было невозможно из-за фаерволов и NAT. Таким образом, у центральных серверов была информация обо всех пирах с IP, обо всех файлах и обо всех передачах между пирами.[2]

К сожалению, дистрибуция информации таким образом была незаконной, поскольку приложение позволяло распространять пиратские копии защищенного авторским правом контента. Однако несмотря на незаконность сервис стал очень популярен из-за своей уникальности и эффективности, хотя и имел недостаток в виде центрального сервера, хранящего абсолютное большинство данных.

В начале 2000 года был создан полностью децентрализованный (в отличие от Napster) протокол P2P обмена данными Gnutella. Сеть Gnutella состояла из обычных пользователей, каждый из которых назван листом(leaf) и ультрапиром, к которым подключены листья и другие ультрапиры. Из-за децентрализации каждый пользователь может объявить себя ультрапиром, если удовлетворяет требованиям по пропускной способности, конфигурации системы и отсутствию фаервола, а также новый ультрапир должен быть подтвержден другими ультрапирами. Пользователь, использующий сеть впервые, получает доступ к сети, подключившись к существующему ультрапиру. Адрес последнего пользователь может получить простыми ring сообщениями. Следующее взаимодействие с сетью происходит благодаря протоколу маршрутизации запросов (QRP- Query Routing Protocol).

Пользователи обмениваются таблицей маршрутизации запросов (QRT), имена файлов пользователей обрезаются и хэшируются SHA-1. Далее в таблицу заносится булева переменная, подтверждающая существование данного файла с хэшем у пользователя. После этого таблица отправляется ближайшему ультрапиру, который агрегирует таблицы своих листьев и обменивается ей между ультрапирами. Чтобы найти конкретный файл, отправляется запрос имени файла ультрапиру, который хэширует его по уже известному алгоритму, сверяет его с QRT и при совпадении отправляет запрос либо соответствующему листу, либо соседнему ультрапиру. Так запрос доходит до нужного пользователя, который уже напрямую связывается с запросившим пользователем.

Для обмена файлами создается прямое соединение между пользователями и происходит обмен посредством HTTP. Если лист расположен за фаерволом или NAT, то соединение происходит посредством push проху, где ультрапиры выступают в качестве прокси-сервера.[3]

В данный момент существует уже более продвинутая версия Gnutella под номером 2, которая сохранила идею децентрализации сети и разбиение на обычных и ультра-пользователей, но имеет более проработанные алгоритмы их

коммуникации, а также алгоритмы поддержания и управления сетью, защищающие от DDoS-атак. Тем не менее оригинальная Gnutella сохраняет лидирующие позиции по количеству пользователей, исчисляемом в миллионах.

Однако наиболее используемым и популярным на нынешний момент протоколом P2P соединения является не Napster и не Gnutella. Лидер популярности - BitTorrent, являющийся основой всех нынешних торрент-клиентов. Изначально он был создан для ускорения централизованных HTTP-раздач, поскольку в концепции клиент-сервер при подключении многих клиентов к серверу, тот вынужден ограничивать исходящий трафик, значительно замедляя загрузку.

BitTorrent-сеть состоит из веб-сервера, хранящего метаинформацию о файлах, трекера, что содержит информацию о пользователях, хранящих файлы, оригинального распространителя(дистрибьютора) файла (пользователя или пира сети), и других пиров, запустивших торрент-клиент (приложение, использующее протокол). В первых версиях пиры взаимодействуют между собой по протоколу TCP, в дальнейших версиях их заменили на разработанный специально для этого соединения - протокол uTP. Примечательно, что пиры одновременно раздают и загружают имеющиеся файлы, что позволяет строить наиболее эффективные обменные взаимодействия между пользователями сети. Для появления файла в раздаче пиру необходимо запустить приложение, в котором будет трекер, создать файл с расширением .torrent, который будет хранить метаинформацию об оригинальном файле вместе с URL-ссылкой на свой трекер, и загрузить его на сервер. Метаинформационный файл .torrent состоит из ссылки на трекер раздающих пользователей и словаря, хранящего данные об определенных частях файла на раздаче, а именно их размер, имя и хэш-суммы всех частей файла. Разбитые на небольшие части файлы (около 5MB) передаются по отдельности, и не от одного дистрибьютора. Оригинальный протокол использует SHA-1, что стало проблемой и одни из дальнейших поводов для дальнейшей модификации протокола. Все сообщения между пирами начинаются со специального идентификатора, который принимает значения от 0 до 8, и, в зависимости от этого, пиры понимают в каком состоянии их соединение. К примеру, после получения идентификатора с номером 2, пир, желающий скачать конкретный файл, будет знать, что у пира, отправившего идентификатор 2, существует часть этого файла, поскольку 2 означает, что пользователь может раздавать данную информацию (состояние interested). В свою очередь идентификатор под номером 8 будет указывать, на то, что наступает конец раздачи – состояние, когда остаются всего несколько частей (“endgame mode”). В этом режиме принимающая сторона запрашивает оставшиеся части у всех возможных клиентов-пиров, поскольку последние части обычно загружаются с единственного пира и это занимает много времени. В таком случае при загрузке каждой части принимающая сторона посылает cancel-сообщение с информацией об этой части и уведомляет о том, что данная часть уже была получена.[4]

Инновационным подходом в данном протоколе было разбиение файла на небольшие части, которые можно было получить от нескольких раздающих.

Такое распределение информации значительно снизило нагрузку на одного пользователя и повысило безопасность протокола, поскольку серверы не имеют доступа к содержимому файлов. Однако анонимность протокола всё ещё осталась под вопросом, в основном из-за надёжности хэш-функции SHA-1.

К 2005 году специалистами была создана модификация протокола - BitTorrent protocol encryption, использующая шифр RC4 (из-за большей скорости шифрования) для шифрования заголовков сообщений и передаваемых частей. Во второй версии протокола (BitTorrent v2) также изменили хэш-функцию на SHA-256 для более надёжного хэширования файлов, хотя она также на сегодняшний день считается уязвимой. Протокол BitTorrent всё ещё находится в разработке, а вторую версию пока поддерживают очень немногие клиенты, как и в случае с Gnutella.

Использование протоколов на основе технологии P2P, в частности BitTorrent, для обмена файлами, защищёнными авторским правом, породило множество юридических и законодательных вопросов. В некоторых случаях, использование протоколов Torrent может повлечь юридическую ответственность как для первоначального распространителя файла, так и для скачавших его пользователей в качестве соучастников дела.

В 2005 году автор протокола BitTorrent Брэм Коэн - CEO BitTorrent, Inc, которая занималась развитием протокола и разработкой новых приложений P2P сетей, заключил соглашение с Американской ассоциацией кинокомпаний об удалении ссылок на авторский контент с официального сайта BitTorrent, сейчас BitTorrent куплен криптовалютным стартапом TRON

Вкупе с протоколами VPN с недавнего времени в России начались попытки заблокировать функциональность протокола BitTorrent по требованию Роскомнадзора, из-за чего произошли сбои в работе серверов Google и Amazon, выведших из строя целые экосистемы Google, VK и сервисы Яндекс.

Опираясь на данные события, с полной уверенностью можно сказать, что система централизованных сетей показывает себя не с лучшей стороны: стабильность сервисов слишком важна для пользователя, поэтому, на данный момент, децентрализованные сети, где вычислительная мощность распределена между участниками сети, являются выгоднейшим из решений для поддержания стабильности сервисов.

Список используемых источников:

1. Bitcoin White Paper: [Электронный ресурс]. URL: <https://bitcoin.org/ru/bitcoin-paper> (дата обращения 12.11.2022).
2. Napster API Version 2.2 Overview [Электронный ресурс] URL: <https://developer.prod.napster.com/api> (дата обращения: 12.11.2022).
3. The Gnutella Protocol Specification v0.4: [Электронный ресурс]. URL: https://courses.cs.washington.edu/courses/cse522/05au/gnutella_protocol_0.4.pdf (дата обращения 12.11.2022).
4. BitTorrent (BTT) White Paper: [Электронный ресурс]. URL: [https://www.bittorrent.com/btt/btt-docs/BitTorrent_\(BTT\)_White_Paper_v0.8.7_Feb_2019.pdf](https://www.bittorrent.com/btt/btt-docs/BitTorrent_(BTT)_White_Paper_v0.8.7_Feb_2019.pdf) (дата обращения: 12.11.2022).

Murashkin N.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunications

Analysis of P2P network solutions.

Modern society is impossible to imagine without communications. Internet, mobile and satellite communications, distributed networks – humanity has all that, because of technological progress, which is unfolding in new technologies. In the beginning of 21 century there was presented the first concept of file-exchange distributed system built on Napster protocol for transferring music files through mainframe to other users. Currently Blockchain technology is becoming the most popular application of P2P-network due to its large perspectives. This article presents analysis of the most popular P2P networks from the beginning of its development.

Key words: P2P, Blockchain, peer-to-peer network, Napster, Gnutella, BitTorrent, distributed networks.

УДК 004.422.8
ГРНТИ 50.05.19

БАЗОВЫЙ ПАЙПЛАЙН ИДЕНТИФИКАЦИИ ЛИЦ В СИСТЕМАХ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ

Л. А. Николаева, А. А. Березкин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматриваются особенности работы пайплайна по распознаванию лиц, разработанного группой компаний “Омега” на базе одноплатного компьютера “Нейробокс”. В статье представлена общая схема работы пайплайна и детально описана схема основного элемента - модуля распознавания лиц. Указаны проблемы представленного решения и обозначены возможные способы их решения.

распознавание лиц, детекция лиц, вектор биометрии, dlib, HOG + Linear SVM

Группой компаний “Омега” на базе одноплатного компьютера “Нейробокс” [1] был разработан пайплайн для распознавания лиц. Пайплайн разрабатывался в рамках реализации проекта Алкозамок для контроля состояния водителей большегрузных автомобилей.

В основу пайплайна легли решения, реализуемые в библиотеке dlib [2]. Dlib осуществляет распознавание лиц с помощью сопоставления полученного изображения лица со 128-мерным векторным пространством, где изображения одного и того же человека расположены близко друг к другу, а изображения разных людей — далеко друг от друга [3].

Общая схема работы базового пайплайна содержит следующие шаги (рис. 1):

1. Детектирование лица с установленной в автомобиле камеры;
2. Определение ключевых точек;
3. Выравнивание лица на кадре;
4. Получение вектора биометрии;
5. Сравнение полученного вектора по базе данных лиц, допущенных к управлению транспортным средством.

Изображение, полученное с камеры, сначала попадает в детектор, далее - в модуль определения ключевых точек, нормализатор и, наконец, в matching модуль, результатом которого является определение вектора биометрии. На основе полученного вектора биометрии идет сравнение изображения со всеми имеющимися в базе лицами и делается вывод о наличии или отсутствии снятого камерой человека в базе.



Рис. 1. Общая схема работы модуля распознавания лиц

Рассмотрим реализацию каждого из описанных шагов подробнее:

1. Детектирование лиц (детектор)

В пайплайне применяется стандартный детектор библиотеки `dlib` - *HOG* (histogram-of-oriented-gradients) + *Linear SVM* (support vector machines) [4].

В `dlib` детектор реализован с помощью функции `dlib.get_frontal_face_detector()`. Функция `get_frontal_face_detector` не принимает никаких параметров. Вызов данной функции позволяет получить объект детектора лиц *HOG* + *Linear SVM*, включенный в библиотеку `dlib`. Детектор обнаружит на изображении лицо.

2. Получение набора биометрических точек (модуль определения ключевых точек)

Получение биометрических точек осуществляется с помощью модели `shape_predictor_68_face_landmarks_GTX.dat`. Модель обучена на наборе данных `ibug300-W` [5].

Результат работы модели - 68 ключевых точек лица (контур вокруг лица, глаз, носа, бровей, рта человека).

3. Выравнивание (нормализатор)

Для выравнивания лица на изображении используется функция `get_face_chip` из состава библиотеки `dlib`. Итог работы функции - вертикально расположенное на изображении лицо с масштабом до 150x150 пикселей (либо с тем размером, который был указан при вызове функции).

4. Получение вектора биометрии (matching модуль)

Для получения вектора биометрии в пайплайне применяется нейросетевая модель `dlib_face_recognition_resnet_model_v1`. Данная модель представляет собой сеть ResNet с 29 слоями. Сеть ResNet была обучена на наборе данных, состоящим из приблизительно 3 миллионов лиц.

5. Поиск по базе лиц (модуль по поиску лиц в базе данных)

На этом этапе для полученного вектора биометрии осуществляется вычисление евклидова расстояния для каждого фото из имеющейся базы данных. Если евклидово расстояние меньше 0.6, то делается вывод, что на фото лицо, которое есть в базе данных (то есть происходит распознавание лица).

Требуемая точность модели - 95 %. Это говорит о том, что при предъявлении пары изображений с лицами, инструмент должен правильно определить, принадлежат изображения одному и тому же человеку или разным

людям в 95% случаев, однако в настоящий момент точность распознавания ниже требуемой.

По итогам работы с пайплайном были выявлены несколько проблем:

1. Если лицо не смотрит прямо в камеру и/или частично перекрыто, то детектор может работать некорректно;
2. Проблема с точностью в определении ключевых точек лица - например, когда на человеке очки;
3. Точность распознавания ниже требуемой (0.95).

В дальнейшей работе предполагается усовершенствовать базовый пайплайн с целью повышения точности идентификации лиц.

Решением проблемы с детекцией нефронтально расположенных или частично перекрытых лиц может стать замена детектора на более современное решение. Возможные варианты детекторов для замены - RetinaFace, SCRFD, Yolo5_face.

Замена детектора, вероятно, поможет и в работе над проблемой с корректным получением набора биометрических точек: в детекторах RetinaFace и SCRFD выделение точек происходит одновременно с детекцией лица.

Для повышения точности распознавания также можно рассмотреть замену модели `dlib_face_recognition_resnet_model_v1.dat` на более современную модель, обученную с использованием лосс функций ArcFace или CosFace [6]. Однако, чтобы оценить точность работы каждой из моделей в рамках пайплайна необходимо провести тестирование на собственных данных.

Список используемых источников:

1. Нейробокс. Российский одноплатный компьютер: [Электронный ресурс]. URL: <https://omegafuture.ru/resheniya/neuroboks-rossiyskiy-odnoplatnyy-kompyuter/> (Дата обращения 07.10.2022).
2. Официальный сайт библиотеки dlib: [Электронный ресурс]. URL: <http://dlib.net/> (Дата обращения 05.10.2022).
3. Инструкция по использованию инструмента распознавания лиц dlib: [Электронный ресурс]. URL: http://dlib.net/face_recognition.py.html (Дата обращения 05.10.2022).
4. H. Bristow, S. Lucey, Why do linear svms trained on hog features perform so well?, arXiv preprint arXiv:1406.2419
5. C. Sagonas, E. Antonakos, G. Tzimiropoulos, S. Zafeiriou, M. Pantic. 300 faces In-the-wild challenge: Database and results. Image and Vision Computing (IMAVIS), Special Issue on Facial Landmark Localisation "In-The-Wild". 2016.
6. J. Deng, J. Guo, and S. Zafeiriou, "ArcFace: AdditiveAngular Margin Loss for Deep Face Recognition," CoRR, vol. abs/1801.07698, 2018.

Nikolaeva L, Berezkin A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Basic pipeline for face recognition - general algorithm of working and identified problems. This article discusses the features of the face recognition pipeline developed by the Omega group of companies based on the Neurobox single-board computer. The article presents the general scheme of the pipeline and describes in detail the scheme of the main element - the face recognition module. The problems of the presented solution were indicated and possible ways to solve them proposed.

Key words: *face recognition, face detection, biometrics vector, dlib, HOG + Linear SVM.*

УДК 004.415.2
ГРНТИ 50.41.25

АВТОМАТИЗИРОВАННЫЕ АЛГОРИТМЫ ДЛЯ ОПТИМИЗАЦИИ ПРОЦЕССА КОНТРОЛЯ ОБРАЗОВАТЕЛЬНЫХ ПРОЦЕССОВ

Н. Э. Самохина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматривается один из возможных вариантов автоматизации систем для контроля образования, предоставления доступа к учебным материалам, а также учета выполнения заданий с доступом к части функционала сервиса с помощью ботов. Рассмотрена работа ботов и их особенности. Описано взаимодействие сервиса с ботами и архитектура сервиса. Рассмотрены преимущества монолитной архитектуры. Описан и показан частичный функционал пользователей сервиса, как на сайте, так и при использовании ботов.

системы контроля образования, бот, дистанционное образование

В процессе обучения студенты получают и выполняют задания преподавателей по различным дисциплинам. Чаще всего преподаватели выдают и оценивают задания в разных местах и различными способами. Из-за этого нередко возникают ситуации, когда студенты путаются и забывают, где и как отправлять результаты своих работ и отслеживать прогресс выполнения заданий. Решением данной проблемы может стать сервис хранения и учета выполнения учебных заданий с возможностью доступа к его функционалу через Telegram бота или чат-бота ВКонтакте. Бот – это скрипт, который получает уведомления о действиях пользователей и обрабатывает их, автоматически выполняя заранее настроенные задачи. Также благодаря данному сервису преподаватели смогут один раз загрузить задания и лекции, после чего давать доступ к ним различным группам, что позволит избавиться от необходимости повторной отправки группам одних и тех же документов.

Большинство студентов регулярно пользуются социальной сетью ВКонтакте или мессенджером Telegram, поэтому они смогут легко и быстро находить там с помощью бота предстоящие задания, отправлять отчеты преподавателям, а также просматривать оценки за них. Цель ботов – ускорить и упростить процесс отправки студентами результатов выполнения заданий преподавателям. Главное преимущество ботов – возможность их использования практически с любого устройства: с компьютера, телефона, планшета или умных часов. При этом на устройстве должен быть лишь доступ к сети Интернет, а также браузер или установленное приложение ВКонтакте или Telegram. Таким образом, бот в удобном студенту сервисе поможет иметь быстрый доступ к самому часто используемому функционалу сервиса.

Для создания чат-бота ВКонтакте используются:

- сообщество ВКонтакте, от имени которого бот общается с пользователями;

- сервер, который принимает уведомления о событиях;
- скрипт с логикой бота, который определяет, как бот реагирует на происходящие события;
- ключ доступа, для получения обновлений в Long Poll и для работы с программным интерфейсом приложения (API).

Существуют два способ получения обновлений: Callback API [1] и Bots Long Poll API [2]. Callback API присылает на сервер запрос с данными в формате JSON, содержащими основную информацию об объекте, вызвавшем событие. В ответ скрипт подтверждает получение каждого запроса, отправляя в ответ строку с текстом «ok». Bots Long Poll API возвращает ответ в формате JSON, когда происходит новое событие или истекает время ожидания. При использовании CallBack API, сервер ВКонтакте сам отправляет информацию о произошедшем событии на сервер, а при использовании Long Poll API ВКонтакте ничего не отправляет и хранит все события у себя на серверах, поэтому необходимо постоянно посылать запросы для получения информации. Также недостатком Long Poll API является зависимость скорости работы бота от пропускной способности хостинга, на котором развернут сервер сервиса учёта выполнения учебных заданий. Поэтому при больших нагрузках бот может пропустить чье-либо сообщение, так как не успеет послать запрос в это время. По этим причинам, был выбран Callback API как оптимальный способ получения обновлений.

При создании Telegram бота используется Telegram Bot API, который предоставляет фреймворк и необходимые инструменты разработки. В Telegram боте @BotFather разрабатываемый бот регистрируется и для него выдается уникальный токен аутентификации, который необходим для авторизации бота и отправки запросов к Bot API [3].

Для взаимодействия с сервисом с помощью бота студенту необходимо иметь аккаунт в социальной сети ВКонтакте или в мессенджере Telegram. Для того, чтобы начать использовать бот, необходимо перейти по ссылке на один из ботов с главной страницы сервиса. При выборе бота ВКонтакте откроется страница сообщества, где для активации бота необходимо нажать кнопку «Написать сообщение» и в открывшемся диалоге нажать кнопку «Начать». При выборе Telegram бота откроется диалог, где для активации бота необходимо нажать кнопку «Старт».

Используя ботов, студент может совершать следующие действия:

- загружать файлы отчетов, выбрав предмет и задание;
- получать напоминания о крайних сроках сдачи заданий за заданный период времени;
- получать уведомления об оценивании заданий преподавателем (с оценкой и комментарием).

При проектировании сервиса учёта выполнения учебных заданий используются принципы монолитной архитектуры, то есть сайт и боты представляет собой единый программный модуль [4]. Архитектура сервиса

представлена на рис. 1. К преимуществам монолитной архитектуры можно отнести следующие особенности:

1. При правильной сборке монолитные сервисы обычно более производительны, чем сервисы на основе микросервисной архитектуры. Микросервисная архитектура – это метод организации архитектуры проекта, основанный на ряде независимо развертываемых служб [4]. К примеру, сервис с микросервисной архитектурой должен выполнить 40 запросов для 40 различных микросервисов для того, чтобы загрузить каждую страницу веб-приложения, что, очевидно, приводит к снижению производительности. Монолитные же решения, в свою очередь, обеспечивают более быструю связь между программными компонентами благодаря общему коду и памяти [5].

2. Так как все действия выполняются с одним каталогом, упрощается процесс развертывания. Благодаря монолитному ядру разработчикам не нужно развертывать изменения или обновления по отдельности, поскольку они могут сделать это сразу и сэкономить много времени [5].

3. Практически полное отсутствие сквозных проблем. Большое количество сервисов имеют зависимость от задач, которые совершаются между компонентами программы, например, ведение контрольных журналов, логирования, ограничения скорости. При монолитной архитектуре данные проблемы сводятся к минимуму, так как все сконцентрировано в одном коде и все работает в одном приложении [6].

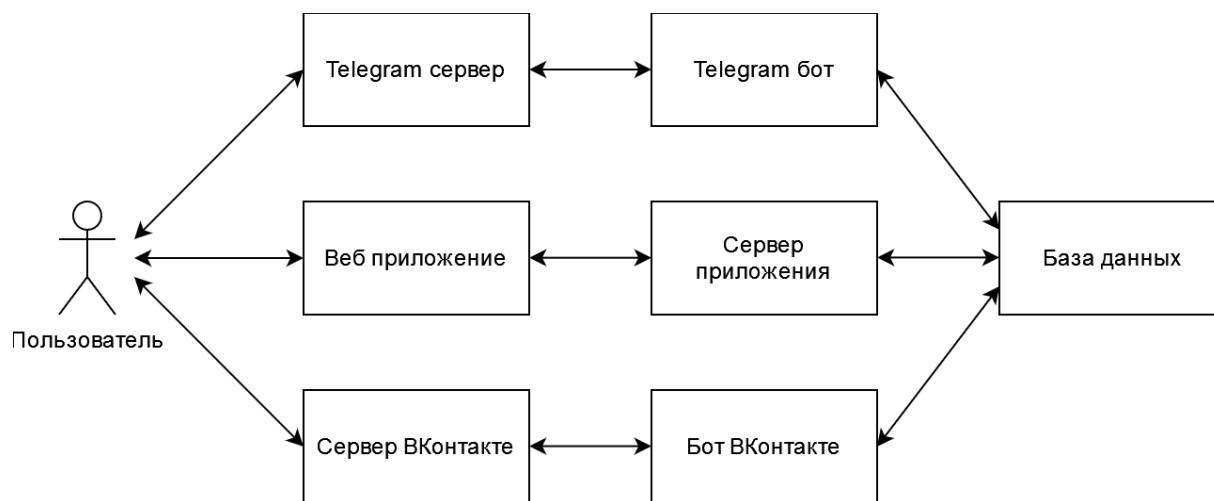


Рис. 1. Архитектура сервиса



На сайте сервиса студент может совершать следующие действия:

- просматривать список предметов;
- просматривать информацию по предметам (преподаватели: лектор, преподаватель по практическим работам, преподаватель по лабораторным работам, форма зачета: зачет, зачет с оценкой, экзамен, курсовая работа);
- просматривать список лекций с описанием и скачивать прикрепленные файлы с лекций;
- просматривать список заданий по учебным дисциплинам;

- просматривать задания, крайние сроки сдачи и скачивать прикрепленные документы;
- писать и отлаживать программный код в интегрированной среде разработки на страницах задания;
- загружать файлы отчетов по заданиям и комментарии к ним;
- просматривать оценки за задания и комментарии к ним;
- просматривать таблицу с оценками по всем предметам;
- получать напоминания о крайних сроках сдачи заданий за заданный период времени;
- получать уведомления об оценивании заданий преподавателем (с оценкой и комментарием).

Часть функционала для студента представлена на рис. 2 в виде макета страницы одной из учебных дисциплин.

Учебные дисциплины
Оценки

Теория автоматов и формальных языков

Лектор: Выборнова Анастасия Игоревна
Преподаватель по практическим работам: Выборнова Анастасия Игоревна
Преподаватель по лабораторным работам: Марочкина Анастасия Вячеславовна

Форма зачета: зачет с оценкой

Лекции ▾

Лекция 1. Формальные языки 📎 TA_1.pptx

Данная лекция посвящена изучению определений естественного, искусственного и формального языков, алфавита и цепочек слов.

Практические работы ▾

Практическая работа 1. Порождающие грамматики Крайний срок сдачи: 12.04.2023	<div style="background-color: #28a745; color: white; padding: 5px; border-radius: 5px; display: inline-block;">Оценка</div> <div style="background-color: #28a745; color: white; padding: 5px; border-radius: 5px; display: inline-block;">Принято, 5</div>
Практическая работа 2. Преобразование НКА в ДКА Крайний срок сдачи: 26.04.2023	<div style="background-color: #ffc107; color: white; padding: 5px; border-radius: 5px; display: inline-block;">Оценка</div> <div style="background-color: #ffc107; color: white; padding: 5px; border-radius: 5px; display: inline-block;">Доработать</div>

Лабораторные работы ▾

Лабораторная работа 1. Порождающие и перечисляющие грамматики Крайний срок сдачи: 19.04.2023	<div style="background-color: #28a745; color: white; padding: 5px; border-radius: 5px; display: inline-block;">Оценка</div> <div style="background-color: #28a745; color: white; padding: 5px; border-radius: 5px; display: inline-block;">Принято, 5</div>
Практическая работа 2. Конечные автоматы Крайний срок сдачи: 2.05.2023	<div style="background-color: #fff3cd; color: #6c757d; padding: 5px; border-radius: 5px; display: inline-block;">Оценка</div> <div style="background-color: #fff3cd; color: #6c757d; padding: 5px; border-radius: 5px; display: inline-block;">Не сдано</div>

Рис. 2. Макет страницы учебной дисциплины

Список используемых источников:

1. Документация Callback API социальной сети «ВКонтакте» [Электронный ресурс]. // vk.com. 2022. URL: https://vk.com/dev/callback_api (дата обращения: 14.11.2022).
2. Документация Bots Long Poll API социальной сети «ВКонтакте» [Электронный ресурс]. // vk.com. 2022. URL: https://vk.com/dev/bots_longpoll (дата обращения: 14.11.2022).
3. Bots: An introduction for developers [Электронный ресурс]. // telegram.org. 2022. URL: <https://core.telegram.org/bots> (дата обращения: 14.11.2022).
4. Харрис Ч. Сравнение микросервисной и монолитной архитектур [Электронный ресурс]. // atlassian.com. 2022. URL: <https://www.atlassian.com/ru/microservices/microservices-architecture/microservices-vs-monolith> (дата обращения: 14.11.2022).
5. Лучшая архитектура для MVP: монолит, SOA, микросервисы или бессерверная?.. Часть 1 [Электронный ресурс]. // Блог компании OTUS, Программирование. 15.11.2019. URL: <https://habr.com/ru/company/otus/blog/476024/> (дата обращения: 14.11.2022).
6. Монолитная архитектура. Традиционный метод разработки приложений [Электронный ресурс]. // codernet.ru. 09.06.2021. URL: https://codernet.ru/articles/drugoe/monolitnaya_arxitektura_tradicionnyij_metod_razrabotki_prilozhenij/ (дата обращения: 14.11.2022).

Samokhina N.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Automated algorithms for optimizing the process of monitoring educational processes.

This article describes one of the possible options for automated systems for monitoring education, providing access to educational materials, and accounting of assignments with access to part of the functionality of the service using bots. The work of bots, their specificities, service's interaction with bots, architecture of the service and benefits of the monolithic architecture are described. The partial functionality of the service's users, both on the site and bots, is described and shown.

Key words: *education control systems, bot, distance education.*

УДК 004.415.538

ГРНТИ 81.81.26

АРХИТЕКТУРА ПРОГРАММНО-АППАРАТНОГО СТЕНДА ДИСТАНЦИОННОГО ТЕСТИРОВАНИЯ КИБЕР-ФИЗИЧЕСКИХ СИСТЕМ

А. Г. Серегин, Р. В. Киричек

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящий момент умные устройства активно проникают в жизни людей, но слишком мало внимания уделяется безопасности этих умных устройств. Поэтому и встаёт проблема массовой проверки не похожих друг на друга приборов на самые разные проблемы в рамках информационной безопасности. В статье рассматривается создание программно-аппаратного комплекса для осуществления массового тестирования, а так же дальнейшее его развитие.

безопасность, интернет вещей, тестирование

Введение

Существующие исследования в области безопасности производимых устройств интернета вещей сигнализируют о большом количестве проблем связанных с безопасностью. Устройства зачастую производятся уже с устаревшими версиями программного обеспечения и после выпуска производители не обеспечивают, своевременное обновление программного обеспечения их продуктов. Большинство устройств так никогда и не получают обновлений.

Развитие кибер-физических систем предполагает существование и создание устройств с разным набором функционала, тестирование которого уже само по себе крайне трудоёмко, а проверка безопасности всей общности часто уходит из поля зрения производителей.[1]

Исходя из этого назревает проблема массового тестирования гетерогенных устройств на самое базовое соответствие стандартам безопасности. Для осуществления массовой проверки гетерогенного набора устройств необходима готовая программно-аппаратная среда в которую будут помещаться тестируемые устройства. Уже сейчас ведутся работы для создания такой среды[2], но на данный момент им не хватает единства подхода, который позволит не только легко воспроизводить подобную среду, но и совместно расширять функционал, разрабатывая дополнения и расширения.

Основная часть

Предлагается архитектура стенда для тестирования устройств интернета вещей на уязвимости. Чётко построенная архитектура до создания реализации позволит создать не просто программно-аппаратное решение, а полноценный программно-аппаратный продукт, который будет интересен для использования как исследователям, так и компаниям производящем оборудование. Так же

откроется возможность лёгкой адаптации и доработок под узкоспециализированные задачи.

Аппаратная часть стенда состоит из сетевого оборудования – отвечающего за сетевое взаимодействие устройств, сервера – где располагается программная часть стенда и непосредственно тестируемых устройств.

Программную часть стенда можно разделить на: часть сбора данных, часть обработки собранных данных, часть анализа данных и часть управления средой представлено на рис 1.

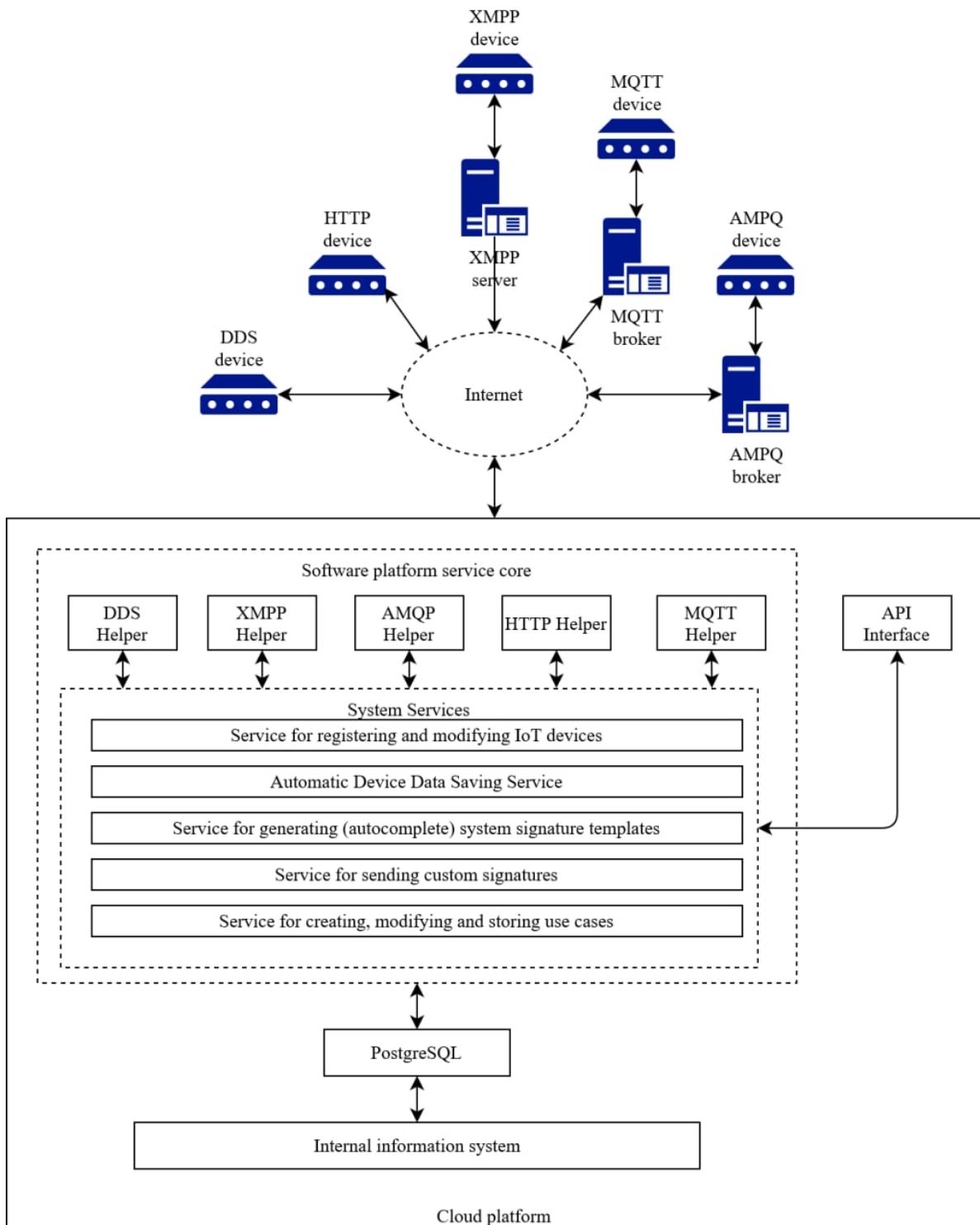


Рис. 1. Схема архитектуры стенда

Часть сбора данных непосредственно обращается к устройствам, по поддерживаемым ими протоколам, запрашивая данные, необходимые для ведения статистики. Главной проблемой является широкое разнообразие устройств с необходимостью разработки под каждый тип своего набора запросов.

Система тестирования выступает как в роли системы с правами администратора, так и в роли клиента, то есть собирает внутренние данные доступные только для администраторов устройств и общается с устройством как базовая станция или клиент, для этого реализуется поддержка широкого набора протоколов: MQTT, CoAP, XMPP, DDS, AMQP, HTTP.

Наличие большого разнообразия вариантов взаимодействия с устройствами позволяет формировать автоматически проводимые тестовые сценарии включающие в себя как тестирование одного устройства, так и тестирование взаимодействия группы устройств.

Часть обработки данных переводит все полученные данные в единый формат и сохраняет в базу данных.

Часть анализа информации работает с уже записанными данными из базы данных – проводит анализ, поиск закономерностей и явных проблем в безопасности.

Часть управления средой способна изменять сетевые настройки, настройки самих устройств и способов взаимодействия с ними.

В части программного обеспечения будут использоваться уже существующие свободные программы для хранения записей, передачи сообщений с использованием протоколов связи, мониторинга сетевого трафика.

Часть программного обеспечения для анализа данных, для сбора данных и для синхронизации настроек с проводимым тестированием – будет создана.

Создание единого API взаимодействия с системой позволит легко интегрировать её с другими решениями и разрабатывать расширения основной системы.

Заключение

Создание такого стенда позволит в сжатые сроки проводить анализ подверженности сетевым атакам большого количества приборов.

Так же стенд позволит выполнять сложное кросс-тестирование сети устройств устройств при нештатных ситуациях, что будет полезно при производстве.

В будущем возможно вырастить из тестового стенда в полноценную эмуляционную среду использования устройств, для этого будут созданы эмуляторы изменения физических состояний и расширен спектр поддерживаемых устройств и протоколов.

Список используемых источников:

1. Наралиев Нишонали Анорматович, Самаль Дмитрий Иванович Обзор и анализ стандартов и протоколов в области интернет вещей. Современные методы тестирования и проблемы информационной безопасности IoT // International Journal of Open Information

Technologies. 2019. №8. URL: <https://cyberleninka.ru/article/n/obzor-i-analiz-standartov-i-protokolov-v-oblasti-internet-veschey-sovremennye-metody-testirovaniya-i-problemy-informatsionnoy> (дата обращения: 11.11.2022).

2. Папуловская Наталья Владимировна, Изотов Илья Николаевич, Блиничкин Денис Юрьевич, Катаев Андрей Юрьевич РАЗРАБОТКА ЯДРА ПЛАТФОРМЫ АВТОМАТИЗИРОВАННОГО ТЕСТИРОВАНИЯ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ // International Journal of Open Information Technologies. 2021. №6. URL: <https://cyberleninka.ru/article/n/razrabotka-yadra-platformy-avtomatizirovannogo-testirovaniya-ustroystv-interneta-veschey> (дата обращения: 11.11.2022).

Seregin A., Kirichek R.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Architecture of the software and hardware stand for remote testing of cyber-physical systems. At the moment, smart devices are actively penetrating people's lives, but too little attention is paid to the security of these smart devices. That is why the problem of mass testing of dissimilar devices for a variety of problems in the framework of information security arises. This article discusses the creation of a hardware-software complex for mass testing, as well as its further development.

Key words: *Internet of things, security, testing.*

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

Секция 4.1.

Интеллектуальные коммуникационные технологии

УДК 004.75
ГРНТИ 20.53.17

ОБЗОР МЕТОДОВ ПОСТРОЕНИЯ НАДЕЖНОЙ СТРУКТУРЫ СЕТЕЙ ХРАНЕНИЯ ДАННЫХ

М. А. Ананьев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе приведены общие сведения о методах построения сетей хранения данных (SAN). Приведен сравнительный анализ надежности существующих топологий построения SAN. Автором предложен один из вариантов построения SAN, основанный на расчётах показателей надежности и стоимости. В текущих реалиях в связи с уменьшением стоимости комплектующих необходимых для построения данных сетей сети хранения данных широко распространены в средних бизнес-категориях. В статье рассматриваются практические реализации данных методов.

SAN, структура, отказоустойчивость, надежность, FibreChannel

На текущий момент объем информации, хранящийся в сетях хранения данных, неуклонно растет согласно годовому отчету Cisco за 2020 год [1]. Соответственно растет и потребность в хранении и управлении данным объемом информации. В связи с этим перед «Инженерами сетей» и «DevOps инженерами» среднего бизнеса стоит задача обеспечения высокоэффективной и отказоустойчивой сети хранения данных, решение которой приведет к снижению стоимости на развертку и поддержание подобной сети. В работе предложен вариант по построению сети хранения данных, позволяющий повысить надежность с помощью изменения конфигурации сети при уменьшении накладных расходов на развертку.

Сеть хранения данных (Storage Area Network, SAN) – высокоскоростная специализированная выделенная сеть, предназначенная для соединения серверов и систем хранения. Одним из главных свойств сети SAN является надежность [2].

Инфраструктура сетей хранения данных чаще всего основывается на технологии Fibre Channel (FC) – Fibre Channel SAN или FC SAN. Fibre Channel является высокоскоростной сетевой технологией передачи данных, основанной на применении оптоволоконных соединений с высокой пропускной способностью и последовательной передачей данных. Одной из причин частого выбора инженерами протокола Fibre Channel для сетей хранения данных является то, что архитектура Fibre Channel легко масштабируется и при этом является надежной [3].

У любой проектируемой сети имеется модель построения, которая характеризуется топологией. Топология предполагает собой схему расположения коммутаторов, маршрутизаторов и другого сетевого оборудования. Каждая топология во многом определяет, насколько будущая сеть хранения данных масштабируема, производительна или надежна.

Основные топологии, применяемые при построении SAN, характеризуются ниже представленными особенностями.

Каскад. Является базовой топологией. Практически нигде не применяется, поскольку производительность по мере роста коммутаторов сильно уменьшается, а каждый коммутатор является потенциальной точкой отказа сети.

Кольцо. Является базовой топологией. Применяется на малых сетях. Рекомендуемое число коммутаторов не более четырех. Представляет собой каскадное подключение только с подключенными между собой оконечными устройствами. Подобное решение позволяет повысить производительность по сравнению с каскадной топологией, но при добавлении устройств внутрь звеньев кольца производительность сети, также продолжает падать.

Полный граф или mesh сеть. Предусматривает подключение каждого коммутатора с каждым в сети. Решает проблемы колец и каскадов. Расстояние до любого из коммутаторов минимально. Существенный недостаток – ограничения по масштабированию из-за того, что количество портов на коммутаторах ограничено. Например, если коммутатор имеет 8 портов, то получаемая сеть будет состоять из восьми доменов. Применяется на средних бизнес предприятиях.

Топология центр/периферия или ядро/периферия, Core Edge. Является основной при построении. Улучшенная версии топологии «Звезда». В ней единственный центральный коммутатор обеспечивает связь до периферийных коммутаторов, а периферийные в свою очередь осуществляют доступ к серверам. Имеет хорошую сбалансированность и экономичность вкуче с простотой масштабируемости и легкой модификацией.

Основой для реализуемой конфигурации сети хранения данных является топология Core Edge. Для решения проблем надёжности стоит рассматривать количество серверов в конфигурации именно в количестве не менее двух штук, так как при отказе одного из работающих серверов второй сможет выполнять вычисления за двоих, а отказ одного из серверов не отразится негативно на свойстве доступности. Главным недостатком данного выбора является стоимость, которая увеличивается пропорционально производительности [4].

Рассматриваемая конфигурация Core Edge имеет две фабрики с двумя центральными коммутаторами, которые впоследствии подключаются к периферийным коммутаторам, с одной стороны, и СХД, с другой. Количество фабрик аналогично с серверами обеспечивает надёжность и доступность данной сети хранения данных.

Периферийные коммутаторы, подключаемые к серверам с помощью FC, должны подключаться напрямую к серверам, с одной стороны, а, с другой, к центральным коммутаторам.

Схема рассматриваемой топологии Core Edge SAN представлена на рис. 1.

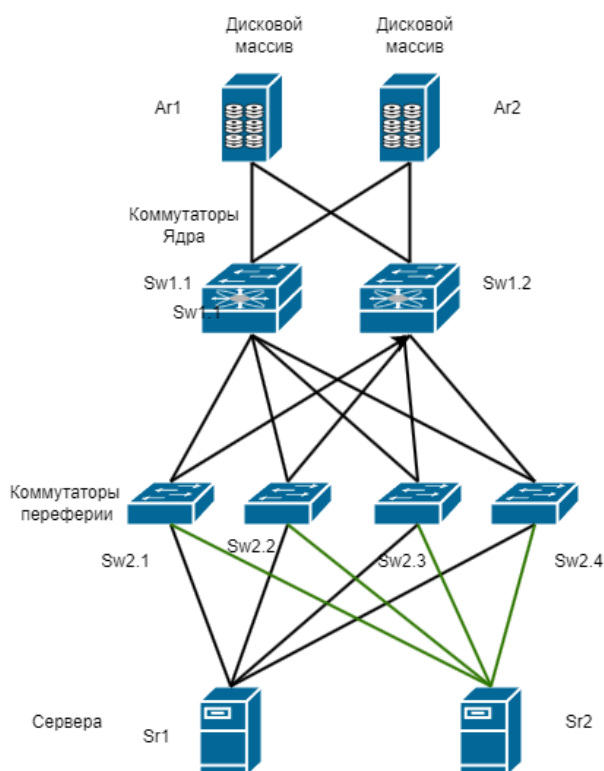


Рис. 1. Структурная схема рассматриваемой топологии SAN

Рассматриваемая сеть анализируется по профилю отказоустойчивости в соответствии с методом, представленным в [5].

Анализ выполняется только с учетом отказоустойчивости оборудования, не включая возможности сбоя в передачах между соединениями.

Учитываемые сбои в сети представлены на рис. 2.

В данной топологии вероятности для каждого из событий будут одинаковы, поэтому достаточно оценить вероятность для одного любого события.

В процессе анализа выведено выражение для определения вероятности сбоя между Сервером 1 (Sr1) и Дисковым массивом (Ar1). При выводе использована теорема умножения вероятностей для независимых событий. В таком случае получено ниже приведённое представление.

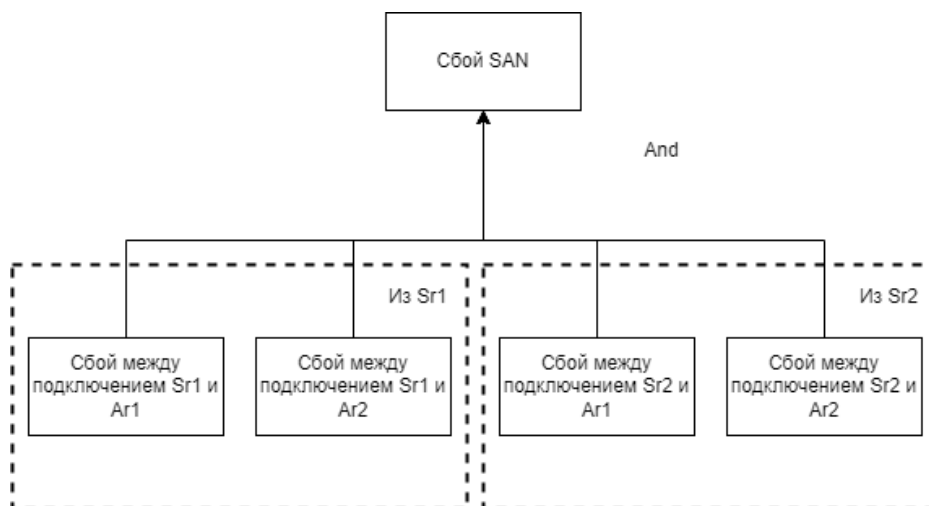


Рис. 2. Схема вероятности отказа SAN

$$\begin{aligned}
 P_{Sr1 \rightarrow Ar1} = & \\
 = & P(Sr_1) + \\
 & P(\overline{Sr_1} \cdot Ar_1) + \\
 & P(\overline{Sr_1} \cdot \overline{Ar_1} \cdot Sw_{1.1} \cdot Sw_{1.2}) \\
 & P(\overline{Sr_1} \cdot \overline{Ar_1} \cdot \overline{Sw_{1.1}} \cdot \overline{Sw_{1.2}} \cdot Sw_{2.1}) + \\
 & P(\overline{Sr_1} \cdot \overline{Ar_1} \cdot \overline{Sw_{1.1}} \cdot \overline{Sw_{1.2}} \cdot Sw_{2.1}) + \\
 & P(\overline{Sr_1} \cdot \overline{Ar_1} \cdot \overline{Sw_{1.1}} \cdot \overline{Sw_{1.2}} \cdot Sw_{2.2}) + \\
 & P(\overline{Sr_1} \cdot \overline{Ar_1} \cdot \overline{Sw_{1.1}} \cdot \overline{Sw_{1.2}} \cdot Sw_{2.3}) + \\
 & P(\overline{Sr_1} \cdot \overline{Ar_1} \cdot \overline{Sw_{1.1}} \cdot \overline{Sw_{1.2}} \cdot Sw_{2.4}) + \\
 & P(\overline{Sr_1} \cdot \overline{Ar_1} \cdot \overline{Sw_{1.2}} \cdot Sw_{1.2} \cdot Sw_{2.2}) + \\
 & P(\overline{Sr_1} \cdot \overline{Ar_1} \cdot \overline{Sw_{1.2}} \cdot Sw_{1.2} \cdot Sw_{2.3}) + \\
 & P(\overline{Sr_1} \cdot \overline{Ar_1} \cdot \overline{Sw_{1.2}} \cdot Sw_{1.2} \cdot Sw_{2.4}) + \\
 & P(\overline{Sr_1} \cdot \overline{Ar_1} \cdot \overline{Sw_{1.2}} \cdot Sw_{1.2} \cdot \overline{Sw_{2.1}} \cdot \overline{Sw_{2.2}} \cdot \overline{Sw_{2.3}} \cdot \overline{Sw_{2.4}}).
 \end{aligned}$$

Далее оценки вероятности задействованы данные из открытых источников [5], приведённые в таблице 1.

ТАБЛИЦА 1. Спецификации компонентов

Компонент	Доступность	Вероятность отказа
Коммутаторы	99,9999%	0,00001
Дисковые массивы	99,9999%	0,00001
Серверы	99,81%	0,0219

Таким образом, оцениваемая вероятность для одного пути принимает следующее значение:

$$\begin{aligned}
 P_{Sr1 \rightarrow Ar1} = & 0,0219 + 9,7 \cdot 10^{-11} + (9,8 \cdot 10^{-11} \cdot 8) + \\
 + & (9,7805 \cdot 10^{-11}) = 0,0219097874356.
 \end{aligned}$$

В схеме таких путей четыре – значит общий отказ сети хранения данных характеризуется вероятностью, принимающей вычисленное значение:

$$P_{\text{общ}} = (0,0219097874356)^4 = 2,30437 \cdot 10^{-7}.$$

Следовательно, отказоустойчивость системы равна:

$$P_0 = 1 - 2,30437 \cdot 10^{-7} = 0,99999976.$$

Далее выполнено оценивание среднего простоя за год (MDT):

$$MDT = P_{\text{общ}} \cdot 365 \text{ дней} \cdot 24 \text{ часа} = 4,2 \text{ часа}$$

ТАБЛИЦА 2. Показатели надежности

	Каскад	Core Edge	Mesh
Состав	Два коммутатора последовательно, 2 сервера, 2 дисковых массива	Шесть коммутаторов, 2 сервера, 2 дисковых массива	Восемь коммутаторов, 2 сервера, 2 дисковых массива
Надежность	0,9780804	0,99999976	0,99999977
Среднее время простоя	192 часа	4,2 часа	4,2 часа

Анализ отказоустойчивости для полного графа представлен в статье [5]. Анализ надежности для каскадной модели с учетом сбоя хотя бы в одном из четырех коммутаторов раскрыт в [6].

Таким образом, при сравнительно недорогой конфигурации получается отказоустойчивая сеть, обеспечивающая выполнение критерия надежности.

Список используемых источников:

1. Cisco Annual Internet Report (2018–2023) [Электронный ресурс] White Paper URL: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html>
2. Josh J. Brocade SAN, Basic of SAN, Brocade, Brocade Communications Systems, Inc. 2009, 175 с.
3. Fibre Channel Solution Guide By Marc Angelinovich [Электронный ресурс] <https://fibrechannel.org/fibre-channel-delivers-so-much-more-than-speed/>
4. Fausto V, Datacenter Technologies, Design a Reliable and Highly Available Fibre Channel SAN, Cisco, 2017. 42с.
5. Liudong X., Massarah T., Vinod M. Reliability Modeling of Mesh Storage Area Networks for Internet of Things // IEEE Journal, 2015, 11 с.
6. Simache, C., & Kaaniche, M. (2005). Availability assessment of SunOS/Solaris Unix systems based on syslogd and wtmpx log files: A case study. Proceedings of 11th Pacific Rim International Symposium on Dependable Computing, 8 с.

Ananiev M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Review of methods for building a reliable structure of storage area Networks.

This paper provides general information about the methods of building storage networks (SANs). A comparative analysis of the reliability of existing topologies for constructing a SAN is given. The author proposed a variant of constructing a SAN based on calculations of reliability and cost indicators. In the current realities, due to the decrease in the cost of components necessary for building data networks, storage networks are widespread in medium business categories. The article discusses the practical implementation of these methods.

Key words: *SAN, structure, failure probability, reliability, Fibre Channel.*

УДК 004.8
ГРНТИ 28.23.15

АНАЛИЗ МАТЕМАТИЧЕСКИХ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ В ЗАДАЧАХ РАСПОЗНАВАНИЯ ОБЪЕКТОВ НА ИЗОБРАЖЕНИИ

П. П. Бовшик, В. Л. Литвинов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире нашли широкое применение модели глубокого обучения по распознаванию объектов на изображении, например, в системах дорожного видеонаблюдения, биометрической идентификации и т.д. В работе приведен обзор математических методов глубокого обучения в задачах распознавания объектов на изображении. В качестве результата научного исследования приведен сравнительный анализ рассмотренных методов.

глубокое машинное обучение, математические методы, распознавание образов

Компьютерное зрение – одно из основных направлений применения глубокого машинного обучения. Технологии компьютерного зрения применяются для интеллектуальной обработки изображений в промышленности [1, 2, 3], сферах здравоохранения [4, 5], образования [6, 7] и многих других.

Глубокое обучение характеризуется как класс алгоритмов машинного обучения, который [8]:

- использует многослойную систему нелинейных фильтров для извлечения признаков с преобразованиями. Каждый последующий слой получает на входе выходные данные предыдущего слоя;
- обладает несколькими слоями выявления признаков или параметров представления данных (обучение без учителя). При этом признаки организованы иерархически, признаки более высокого уровня являются производными от признаков более низкого уровня;
- формирует в процессе обучения слои на нескольких уровнях представлений, которые соответствуют различным уровням абстракции. При этом слои образуют иерархию понятий.

По данным опроса Ipsos для Всемирного экономического форума в среднем в 28 странах, участвующих в исследовании, 64% опрошенных утверждают, что хорошо понимают, что такое искусственный интеллект, но только 50% знают, где или как он используется. В рамках данной статьи будут рассмотрены и проанализированы такие базовые математические методы, как метод дискриминантного анализа и таксономии [9, 10, 11].

Цель работы – проанализировать математические методы глубокого обучения в задачах распознавания объектов на изображении для правильного применения с учетом их особенностей при обучении моделей.
Распознавание образов.

Задачи распознавания образов основаны на классификации объектов. Существуют различные способы их решения, но в рамках данной статьи будут рассмотрены методы решения систем линейных неравенств.

Основываясь на том, что задача распознавания образов есть задача классификации, можно сказать, что образ есть множество всех объектов, сходных друг с другом в некотором фиксированном отношении, а распознать образ объекта – значит указать, к какому классу он относится.

Классификацию можно охарактеризовать как простейшую логическую операцию, являющуюся формой систематизации.

Необходимость математических методов классификации обуславливается неэффективностью обычных интуитивных методов в вопросах типологии сложных систем, например, при работе с большим количеством числового материала, особенно, учитывая непрерывное возрастание сложности изучаемых систем в современной науке. Примерами таких систем может послужить система анализа сущности природных, технических и экономических явлений или различные системы прогнозирования.

Вектор состояния.

Вектор состояния считается простейшей моделью, применяемой в распознавании образов, на основе которой строятся более сложные. Вектор состояния имеет вид [12]:

$$x = (\xi_1, \dots, \xi_n),$$

где ξ_n – вещественные числа, интерпретируемые как значения параметров или признаков объекта.

Предполагается, что $x = (\xi_1, \dots, \xi_n)$ есть вектор пространства R^n . Скалярное произведение векторов $x, y \in R^n$ будет записываться как $\langle x, y \rangle$.

Модель дискриминантного анализа.

Математической моделью образа как некоторого множества всех объектов, сходных друг с другом в каком-то фиксированном отношении, является подмножество в пространстве R^n : $M \subset R^n$.

Модель таксономии.

Пусть задано конечное множество

$$X = (x_1, \dots, x_r) \subset R^n,$$

и пусть k – число классов (таксонов), на которое необходимо разбить представленное множество:

$$X = X_1 \cup \dots \cup X_k, \quad X_i \cap X_j = \emptyset \ (i \neq j); \#(1),$$

где X_i – i -й таксон, k задается заранее, либо определяется в результате решения задачи таксономии.

Существует большое количество способов разбиения (1), но если имеется функционал φ , оценивающий качество разбиения:

$$\varphi(X_1, \dots, X_k),$$

причем с увеличением значения φ улучшается и качество, то задача таксономии имеет вид:

$$\max \{ \varphi(X_1, \dots, X_k) : X = X_1 \cup \dots \cup X_k, X_i \cap X_j = \emptyset (i \neq j) \}.$$

Функционал φ может учитывать качество строения таксона $X_i(\forall_i)$, то есть его однородность, достаточную близость друг к другу его элементов, и достаточную степень различия между таксонами с различными номерами, и какие-либо другие критерии.

Методы дискриминантного анализа.

На данный момент существует большое количество методов дискриминантного анализа, хотя их формализация и обоснования находятся на самых различных уровнях, некоторые из них имеют только эвристическое основание, но являются полезными при решении некоторых практических задач. Рассмотрим классические и в большей степени изученные с математической точки зрения методы статистических решений [12].

Образы будут рассматриваться как некоторые бесконечные множества в пространстве R^n . Основываясь на образах, могут быть известны различные вероятностные параметры, или же эти параметры могут быть оценены по конечным выборкам из образов.

Параметрические методы обеспечивают:

- определение зависимости дискриминантных функций от параметров;
- оценку параметров, основываясь на материале обучения;
- подстановку оценок вместо параметров в дискриминантные функции.

Методы таксономии.

Методов таксономии достаточно много, и большая часть из них связана с весьма сложными критериями оценки качества разбиения на таксоны. Рассмотрим два метода, описанных Н. В. Загоруйко [13]: метод сфер и метод «масок».

Метод сфер.

Заданы: конечное множество $|X| \subset R^n$ и радиус r гиперсферы. Необходимо построить шар $B(x, r)$, где x – любая точка из X , затем множество $X \cap B(x, r)$. Пусть z_1 – центр тяжести множества $X \cap B(x, r)$. Затем необходимо построить

$X \cap B(z_1, r)$, определить z_2 как центр тяжести этого множества. Затем необходимо построить $X \cap B(z_2, r)$, найти центр тяжести z_3 этого множества и так далее.

Этот процесс закончится, когда $z_{i+1} = z_i$. В качестве первого таксона пусть предполагается $X_1 = X \cap B(z_1, r)$, затем необходимо повторить все изложенное для множества X/X_1 , получить таксон X_2 и так далее.

Метод «масок».

Пусть задано конечное множество X векторов $x = (\xi_1, \dots, \xi_n) \in R^n$ с координатами $\xi_1 \in \{0,1\}$. Необходимо разбить множество X на таксоны X_1 опираясь на «сходство» элементов, иными словами, по числу совпадающих координат. Порог есть некоторое число $\alpha > 0$. Далее выбирается элемент $x_1 \in X$ в качестве элемента таксона X_1 . Затем необходимо произвольно выбрать элемент x из X и сравнить его с x_1 .

Если число $r = r(x, x_1)$ совпадающих координат не меньше, чем α , то векторы считаются «похожими» и выбранный элемент x отбрасывается. Но если же $r < \alpha$, то считается, что элемент $x = x_2$, и вектор x_2 становится элементом таксона X_2 и так далее.

Таким образом выделяются «маски» x_1, \dots, x_k . Далее для всех элементов множества X формируются «знаки». «Знак» вектора x есть k -мерный вектор, j -я координата которого равна 1, если $r(x, x_j) \geq \alpha$, и равна 0 в противном случае. Все векторы с одним знаком попадают в один таксон X_j , этот знак – «имя» таксона.

Несмотря на успехи использования глубокого обучения, у него всё же есть фундаментальное ограничение: модели глубокого обучения ограничены в том, что они могут представлять, и большинство программ нельзя выразить в виде непрерывного геометрического морфинга многообразия данных.

Список используемых источников:

1. Лопатин А.К. О распознавании габаритов объектов в деревообрабатывающей промышленности. – Актуальные направления научных исследований XXI века: теория и практика. Том 3, №5-4, 2015, с. 369-371.

2. Ятматова А.А. «Компьютерное зрение» как контроль за качеством пищевой промышленности. – Информационные технологии в современном мире – 2016, 2016, с 178-181.

3. Загоруйко Н.Г. Методы распознавания и их применение. – М., 1972.

4. Наркевич А.Н., Виноградов К.А. Распознавание объектов на цифровых изображениях микроскопических препаратов с использованием искусственных нейронных сетей. – Вестник новых медицинских технологий. – 2018, №4 – с. 235-241.

5. Бузанов Н.А. Применение свёрточных нейронных сетей в задаче распознавания объектов из видеоряда в сфере горнодобывающей промышленности. – Заметки по информатике и математике. – Сборник научных статей. Том Выпуск 12. Ярославль, 2020, с 24-28.

6. Онокой Л.С., Морев У.А. Применение технологий компьютерного зрения в экономике и образовании. – Дискуссия. – 2021. – с. 24-30.

7. Баранова Е.В., Солодкая М.А. Методика обучения бакалавров педагогического образования технологиям компьютерного зрения. – Новые образовательные стратегии в

современном информационном пространстве. Сборник научных статей по материалам международной научно-практической конференции. Санкт-Петербург, 2022, с 172-180.

8. Гудфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение = Deep Learning. – М.: ДМК Пресс, 2017. – 652 с.

9. Азарченков А.А., Любимов М.С., Лушков В.И. Распознавание объектов дорожной инфраструктуры с помощью полносверточной нейронной сети. – Автоматизация и моделирование в проектировании и управлении №4 (06), 2019, с 38-43.

10. Местецкий Л. М. Математические методы распознавания образов. – Москва, МГУ, ВМиК, кафедра «Математические методы прогнозирования», 2002-2004.

11. Чабан Л. Н. Теория и алгоритмы распознавания образов. – Москва, 2004.

12. Дороничева А.В., Савин С.З. Методы распознавания медицинских изображений для задач компьютерной автоматизированной диагностики. – Современные проблемы науки и образования. – 2014. – № 4.

13. Мазуров В. Д. Математические методы распознавания образов. – Екатеринбург: Изд-во Уральский государственный университет им. А.М.Горького, 2010.

Bovshik P., Litvinov V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of mathematical methods of deep learning for the tasks of object recognition in an image.

In the modern world, deep learning models for recognizing objects in an image are widely used, for example, in traffic video surveillance systems, biometric identification, etc. The paper provides an overview of the mathematical methods of deep learning in the tasks of recognizing objects in an image. As a result of a scientific study, a comparative analysis of the considered methods is given.

Key words: deep machine learning, mathematical methods, pattern recognition.

УДК 681.3
ГРНТИ 27.41.17

РАЗРАБОТКА МНОГОАГЕНТНОГО ПОДХОДА ДЛЯ ОПТИМАЛЬНОЙ ЗАЩИТЫ МНОГОУРОВНЕВОЙ ПРОМЫШЛЕННОЙ СИСТЕМЫ

И. Б. Бондаренко, Д. А. Крылов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье разработан подход для защиты многоуровневой иерархической системы с помощью многоагентного подхода. Для увязки локальных генераторов решений агентами на отдельных уровнях предложено использовать метод анализа иерархий. Актуальность темы работы обосновывается малой проработанностью вопросов многомерной оптимизации в сложных иерархических системах. Результаты работы могут быть использованы при разработке систем безопасности для многоуровневых промышленных систем, в том числе относящихся к критически важным.

информационная система, многоагентный подход, агент, защита, угроза, уязвимость, многоуровневая система, промышленная система, метод анализа иерархий

Для современного этапа развития сетей промышленной автоматизации характерно повышение их функциональной насыщенности и направленность на создание единой информационной инфраструктуры предприятий. Защита информации в таких промышленных системах усложняется из-за большой номенклатуры оборудования, разноплановых бизнес-процессов и многоуровневой структуры систем, применяемых на предприятиях. Современные промышленные системы – это самый сложный комплекс, состоящий из персональных и панельных компьютеров, активного и пассивного оборудования. Такая сложная система не может обходиться без автоматизированного управления на всех уровнях. Решение задачи управления сложными объектами возможно с развитием и внедрением информационных и коммуникационных технологий в сферу управления промышленными предприятиями, а именно автоматизированных систем. В свою очередь, внедрение таких систем невозможно без использования надежных систем сбора первичной технологической информации и ее передачи на вышестоящие уровни управления для принятия решений. Поэтому задача сбора технологических данных и оперативного управления производством на их основе обычно решается с использованием автоматизированных систем управления технологическими процессами (АСУ ТП) [1].

Задачи многоуровневой оптимизации возникают при выработке оптимальных решений в иерархических сложных системах, которые представляют собой множество взаимоподчиненных уровней [2]. Сложность процесса принятия решений заключается в том, что оптимальное решение, достигнутое на нижних уровнях системы, – локальное и не означает получение оптимального – глобального решения для системы в целом. При этом процесс выработки решения носит лавинообразный характер, а результаты, полученные на промежуточных уровнях, взаимосвязаны. Поэтому исследования в данной

области направлены на выделение координирующих переменных, определяющих взаимосвязь нижних и верхних уровней, а также декомпозицию системы на подсистемы меньшей размерности с последующим решением локальных задач оптимизации [3].

Крайне важно понимать, что многоуровневые промышленные системы (МПС) уязвимы в большей степени. Они могут быть подвержены различного рода внешним или внутренним угрозам, могут стать целью злоумышленников, и риски при этом очень высоки, вплоть до нарушения работоспособности системы и остановки производства в целом. Причем атакам могут подвергаться как отдельные подсистемы, так и вся система в целом.

Еще более опасным случаем является перехват контроля над устройством или подсистемой, при котором элемент начинает выполнять команды извне, становясь "на сторону" злоумышленника.

Исходя из этого, необходимо разрабатывать комплексную защиту МПС, уделяя внимание всем без исключения подуровням.

Архитектура МПС характеризуется количеством уровней, которое зависит от масштабов анализируемого предприятия (рис. 1).

Низший уровень – это датчики и исполнительные механизмы, которые могут иметь встроенный микроконтроллер и цифровой интерфейс.

Первый уровень составляют программируемые логические контроллеры и устройства ввода-вывода.

На втором уровне располагаются рабочие станции с установленными системами диспетчерского управления, которые осуществляют мониторинг и анализ действий оператора, аварийных ситуаций и запуск управляющих процедур.

На третьем уровне объединяются автоматизированные системы управления и автоматизированные системы управления процессами.

В зависимости от масштабов предприятия определенное количество уровней интегрируется с четвертым уровнем – высшего руководства, которое может функционировать удаленно.



Рис. 1. Архитектура многоуровневых промышленных систем

Среди угроз обеспечения информационной безопасности, свойственных МПС, можно выделить три класса.

1. Угрозы техногенного характера, обусловленные физическим воздействием на компоненты МПС. Для защиты от данного класса угроз применяются меры и средства обеспечения безопасности от несанкционированного физического доступа и обеспечивают технический контроль доступа к ключевым компонентам МПС.

2. Угрозы антропогенного характера – угрозы преднамеренного и непреднамеренного действия персонала, занятого обслуживанием МПС, в том числе ошибки в организации работ с компонентами системы.

3. Угрозы несанкционированного доступа. Поскольку компоненты МПС взаимодействуют с локальной вычислительной сетью предприятия для передачи информации о состоянии технологической среды, а также для формирования управляющих воздействий на технологические объекты, необходимы меры по формированию выделенных технологических сетей передачи данных и использованию средств защиты периметра (средства межсетевое экранирования, обнаружения вторжений, криптографической защиты каналов связи).

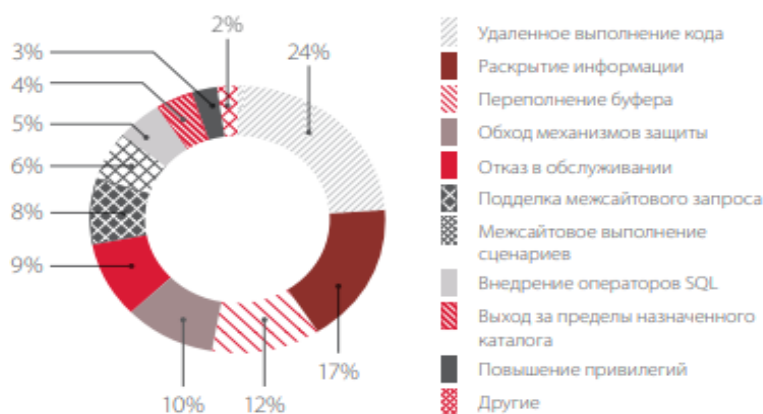
В качестве основных угроз в области информационной безопасности, реализация которых может вызвать аварию, выделим следующие (рис. 2) [4]:

– активное создание вредоносного программного обеспечения и коммерциализация этого процесса, приводящие к созданию вредоносных программных комплексов, снабженных различными инструментами взлома систем защиты информации, а также встраивание средств технической поддержки (например, для обновления вредоносного кода);

– утечки информации, связанные как с проникновением злоумышленников извне, так и со сбором и передачей инсайдерской информации;

– проблемы, связанные с квалификацией работников компаний в области информационной безопасности;

– несогласованность действий сторон в процессе передачи и использования информации, в том числе составляющей коммерческую тайну.



Распространенные типы уязвимостей компонентов АСУ ТП

Рис. 2. Распространенные виды уязвимостей компонентов промышленных систем

По данным исследований компаний [5] долю уязвимостей АСУ ТП отражает диаграмма (рис. 3). Наиболее уязвимыми техническими компонентами являются каналы передачи данных, устройства и система в целом.

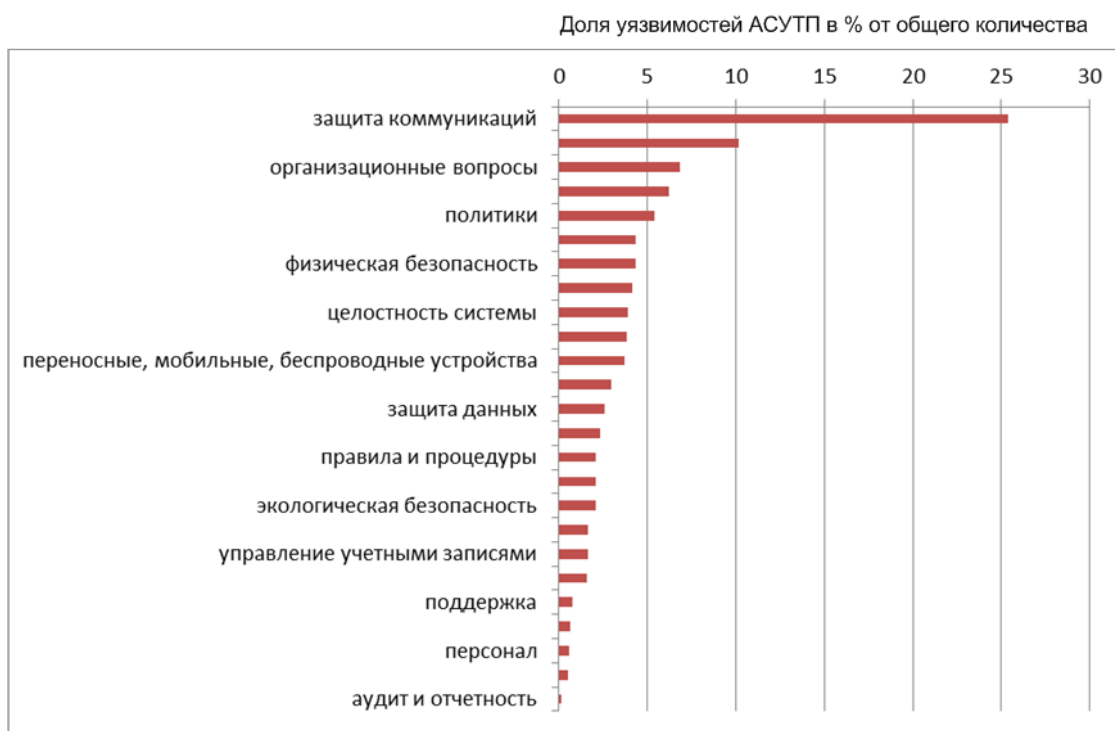


Рис. 3. Доля уязвимостей АСУ ТП

Для оптимизации системы защиты МПС может использоваться многоагентный подход, при котором глобальную функцию цели G оптимизирует агент-координатор, а каждая из j -х подсистем описывается на i -м уровне наборами, являющимися параметрами локальных функций целей G_{ij} :

$$G_{\text{опт}} = \text{extr} (f(G_{ij})), G_{ij} = f(C, S, R, Y, F(S,Y)),$$

причем:

$$F(S,Y) \rightarrow R, F(X,Y),$$

где: S – множество средств для достижения целей C алгоритма подсистемы МПС; R – множество полученных результатов на подсистеме; Y – множество состояний внешней среды; X – множество внутренних параметров системы защиты; $F(S,Y)$ – оператор связи средств и состояний внешней среды.

Локальные цели достигаются в результате обработки процедур, составляющих основу работы агентов-исполнителей.

Для поддержки принятия решений всей мультиагентной системой может использоваться метод анализа иерархий. Основными процедурами метода являются: формулировка цели в аналитическом виде и построение иерархии, начиная с вершины (глобальной цели G), через промежуточные уровни – к

самому нижнему уровню. Промежуточные уровни будут содержать критерии, а последний – набор альтернатив.

Подход, описанный в статье, не является конечным вариантом и нуждается еще в дополнительном анализе, проработке отдельных подсистем и апробации на конкретном примере, что будет сделано в последующих работах.

Список используемых источников:

1. Бондаренко И. Б., Шиманчук С. Н. Защита информации конфиденциального характера в многоуровневых автоматизированных системах // Информационная безопасность регионов России : материалы . Юбилейной X Санкт-Петербургской межрегион. конф. Санкт-Петербург, 1-3 нояб. 2017 г. СПб. : СПОИСУ, 2017. С. 440-442.

2. Бондаренко И. Б., Мишина Н. С., Мишин Я. Д. Методы формализации модели многоагентной иерархической системы // Сборник тезисов докладов VIII конгресса молодых ученых. Электронное издание. [Электронный ресурс]. URL: <https://kmu.itmo.ru/digests/article/646> (дата обращения 06.11.2022).

3. Якимов А. И. Технология имитационного моделирования систем управления промышленных предприятий: монография / А. И. Якимов. – Могилев: Белорус.-Рос. ун-т, 2010. – 304 с.

4. Безопасность АСУ ТП: итоги 2017 года [Электронный ресурс]. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/ics-security-2017/> (дата обращения 09.11.2022).

5. Оценка уровня защищенности технологической системы и КВО [Электронный ресурс]. URL: www.elvis.ru/services/asutp/audit_asutp/ (дата обращения 07.11.2022).

Bondarenko I., Krylov D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Developing a multi-agent approach for optimal protection of a multilevel industrial system. In this paper a multi-agent approach is developed to protect multilevel hierarchical system. The method of hierarchy analysis is proposed for linking local decision generators by agents on individual levels. The relevance of the topic is justified by the low elaboration of the issues of multidimensional optimization in complex hierarchical systems. The results of the work can be used in the development of security systems for multilevel industrial systems, including those related to the critical.

Key words: information system, multi-agent approach, agent, protection, threat, vulnerability, multilevel system, industrial system, hierarchy analysis method.

УДК 614.84
ГРНТИ 28.27.19

РАЗРАБОТКА ПОДХОДА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ АНАЛИЗА ЖИВУЧЕСТИ

И. Б. Бондаренко, П. В. Миронов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Несмотря на то, что показателям надежности уделяется много внимания, методы анализа живучести стремительно развиваются, образуя подраздел теории надежности. Одной из областей применения таких методов является защита информационных систем. В статье освещены такие понятия, как отказоустойчивость, живучесть, выживаемость, безопасность, и показана их взаимосвязь. Предложены три компонента подхода для защиты информационной системы на основе анализа живучести. Описан универсальный сценарий нагрузочного тестирования медиа-сервера при отсутствии и наличии системы анализа трафика и выявления запросов, которые ухудшают стабильность работы системы.

информационные технологии, информационные системы, живучесть, системы мониторинга, сервер, безопасность, методы, нагрузочное тестирование

Современное общество характеризуется широким использованием и непрерывным совершенствованием ИТ-систем, которые в большинстве своем имеют развитую структуру и обеспечивают эффективное принятие решений в различных сферах деятельности. Такими системами являются, например, информационные системы, обеспечивающие поддержку принятия управленческих решений, мониторинга, прогнозирования в сферах жилищно-коммунального хозяйства, транспорта, муниципального управления, связи и др. Совершенствование ИТ-систем приводит к усложнению их топологической структуры и в большинстве случаев она является комбинаторной т.е. состоит из множества узлов связанных между собой информационными потоками и характеризуется экстремальностью нагрузок и влиянием негативных внешних воздействий. Это приводит к изменению или уничтожению информационных потоков, которые характеризуются соответствующими наборами параметров.

Информационная структура может не выполнять возложенные на нее функции или может быть разрушена вследствие сбоя, разрывов информационных потоков, перегрузок, выхода из строя ее элементов и возникновения дефектов, имеющих место, как в процессе эксплуатации, так и вследствие воздействий.

Отказ информационных систем часто приводит к серьезной потере в предоставляемых услугах. Таким образом, их надежность стала важным аспектом. Показатели надежности ИТ-систем, такие как устойчивость, доступность, безопасность, защищенность, конфиденциальность, целостность и ремонтпригодность, не полностью отвечают потребностям потребителей, поскольку они не учитывают частичной потери качества при выполнении основной задачи. Определение живучести [1, 2] позволяет в данном случае иметь

точное представление о формах услуг, которые приемлемы в системе и обстоятельствах, при которых каждая форма наиболее полезна, а так же, определение интервала времени, в течение которого сервис может оказывать услуги не в полном объеме [3]. В настоящей работе живучесть рассматривается как новая характеристика в дополнение к надежности.

В работе был рассмотрен стандарт DLNA (DigitalLivingNetworkAlliance), который был создан некоммерческой ассоциацией производителей электроники и компьютеров под руководством фирмы Sony в 2003 году для организации обмена файлами между устройствами домашней сети (передаваемых через Ethernet или WiFi).

Необходимо отметить, что не все устройства поддерживают эту технологию, и такие устройства уже нельзя адаптировать. Стандарт DLNA базируется на клиент-серверном взаимодействии. И некоторые компании, такие как Apple и Samsung, предоставляют свои собственные сертификаты DLNA, гарантирующие возможность обмена мультимедийными файлами между их устройствами с помощью платформ AirPlay и SamsungLink. Другие, такие как LG и Philips, также присоединились к альянсу DigitalLivingNetworkAlliance со своими платформами обмена SmartShare и SimpleShare, соответственно.

В качестве сервера DLNA для хранения и передачи мультимедийных файлов могут выступать устройства хранения данных, ноутбуки или мультимедийные серверы для дома, такие как Serviio, Orb, TVersity или TwonkyMedia. ПК с операционной системой Windows уже имеют встроенный DLNA, а проигрыватель WindowsMedia может выступать в качестве медиа-сервера.

Клиентами могут быть, например, телевизоры с технологией SmartTV, стереосистемы или принтеры.

При использовании обмена контентом между домашними устройствами возможна ситуация, когда авторские права ограничены и не позволяют его воспроизвести на устройствах с DLNA-сертификатом.

Еще одной проблемой является возможная несовместимость аппаратуры с различными форматами файлов, таких как MP4, или DivX, хотя некоторые мультимедийные серверы, такие как TVersity, позволяют декодировать контент "на лету".

Определение и анализ требований к живучести является важнейшим первым шагом в достижении живучести системы [4]. Живучесть должна учитывать не только требования к функциональности программного обеспечения, но и требования к использованию программного обеспечения, его разработке, эксплуатации и развитию. Есть пять типов требований, предъявляемых к живучим системам:

- требования к системе/живучести;
- требования к использованию/вторжению;
- требования к разработке;
- требования к эксплуатации;
- требования к эволюции.

Отказоустойчивость позволяет системам продолжать функционировать, несмотря на наличие неисправностей [5]. Отказоустойчивость состоит из четырех этапов:

- обнаружение ошибок;
- оценка повреждений;
- восстановление состояния;
- продолжение обслуживания.

Кроме взаимосвязи между живучестью и отказоустойчивостью можно также констатировать связь живучести и безопасности. Действительно, приложение может использовать механизмы безопасности, такие как пароли и шифрование, и все равно может перейти в неработоспособное состояние, когда сервер или сетевое соединение обрываются. С другой стороны, "жизнеспособное" приложение должно выдержать некоторые из вредоносных атак. Следовательно, живучесть включает в себя информационную безопасность.

Существует два аспекта выживаемости:

- выживание за счет защиты;
- выживание за счет адаптации.

Например, контроль доступа и шифрование, пытаются обеспечить высокий уровень живучести, защищая приложения от вредных, случайных или злонамеренных изменений в среде. А для выживания за счет адаптации, в приложение может быть встроен механизм, использующий контроль доступа или увеличивающий длину ключа при обнаружении угрозы вторжения.

Большинство современных приложений не способны к адаптации, так как механизмы повышения живучести сложны. А разработчики больше внимания уделяют функциональности программ, поэтому инструментарий поддержки живучести оказывается ограниченным.

Еще необходимо отметить, что не все сценарии адаптивного поведения приводят к повышению выживаемости. Например, завершение работы приложения при возникновении исключения, указывающего на изменение среды, никак не влияет на выживаемость приложения. Фактически, такая адаптация облегчает целый класс атак типа "отказ в обслуживании", в то время как живучесть заключается в продолжении выполнения целевой функции, несмотря на изменения окружающей среды.

В работе предложены три компоненты подхода для защиты информационной системы на основе анализа живучести [6].

Во-первых, необходимо предусмотреть возможность самообслуживания (SelfMaintenance), которое входит в более широкое понятие (SelfRecovery) – самовосстановление. Самовосстановление является комбинацией самостоятельного обслуживания и саморемонта.

Самообслуживание состоит из таких технологий, как перекомпозиция, динамическая реконфигурация, резервное копирование и реконструкция, то есть технологий, которые позволяют изменять или даже восстанавливать состояние системы при выполнении обслуживания для некоторых уровней.

Самовосстановление – это функция, которая позволяет системе реагировать на любые изменения, происходящие в ее среде. Самовосстановление состоит из возможностей реагирования, мониторинга и корректировки внутренней структуры системы, а также компенсации неисправностей во время эксплуатации, где это применимо.

Во-вторых, необходима подсистема мониторинга – периодической проверки, которая выполняется для компонентов сервиса и для самого сервиса. Мониторинг можно классифицировать по двум основным подходам: активный, который основан на отправке запросов системному компоненту, и пассивный, основанный на оценке выходных данных системы или одного из конкретных компонентов и определению по ним состояния системы или компонента. Из-за распределенного характера сервисных компонентов для обнаружения и идентификации неисправностей требуется опрос множества датчиков, что замедляет работу подсистемы мониторинга.

В-третьих, взятая из области искусственного интеллекта концепция мобильных агентов, используется для решения проблем, связанных с моделью клиент/сервер, таких как масштабируемость и распределенная обработка разреженных данных.

В качестве системы мониторинга выбран бесплатный продукт с открытым исходным кодом Zabbix.

Zabbix имеет средства для интеллектуального автоматизированного сбора метрик с гибко настраиваемыми: граничными значениями, уровнями безопасности и обнаружением аномалий. В работе подробно освещена установка и настройка данного программного продукта в связке с репозиторием Grafana.

Для мониторинга медиа-сервера была выполнена установка и настройка серверного программного обеспечения: системы управления базой данных MariaDB; веб-сервера NGINX, включающего HTTP-сервер и обратный прокси-сервер, почтовый прокси-сервер, а также TCP/UDP прокси-сервер общего назначения; системы мониторинга Zabbix 6.2; дополнительного сервиса Grafana.

Нагрузочное тестирование было выполнено с помощью виртуальной машины на базе дистрибутива LinuxCentos 7. С помощью утилиты Python была запущена программа GoldenEye, загруженная с ресурса GitHub.

Сервер при этом легко подвергнулся DoS-атаке, при этом нагружая полностью процессор, и, выводя из строя веб-сервис.

Используя утилиту Cgn и скрипт, который с помощью утилиты собирал данные о подключениях, были выявлены те из них, которые ухудшали стабильность работы системы. При новом запуске нагрузочного тестирования скрипт перекрывал брешь в защите веб-сервера путем ограничения доступа по порту запросов, поступающих с одного из IP-адресов виртуальной машины.

В результате был разработан сценарий работы системы защиты медиа-сервера, который можно внедрять на различные сервера предприятий, а так же подход, являющийся универсальным.

Список используемых источников:

1. Черкесов Г. Н. Методы и модели оценки живучести сложных систем. М. : Знание, 1987. 55 с.
2. Стекольников Ю. И. Живучесть систем. СПб. : Политехника, 2002. 155 с.
3. Громов Ю. Ю., Долгов А. А., Хорохорин М. А., Минин Ю. В. Использование теории возможностей при оценке живучести сетевых информационных структур // Информация и безопасность. 2014. Т. 17. № 1. С. 62-67.
4. Елисеев А. И., Долгов А. А., Хорохорин М. А., Аль Балуши М. К вопросу исследования живучести информационных систем в рамках механики катастроф // Прикладная математика, управление и информатика : сб. науч. тр. Белгород: БелГУ, 2012. Т.1. С. 122 - 125.
5. Бондаренко И. Б., Карманов А. Г., Чжао Лэй, Ткачев К. О. Оценивание живучести систем связи линейного типа с наземными подвижными объектами // Известия вузов. Приборостроение. 2016. Т.59. №3. С. 173-180.
6. Долгов А. А., Хорохорин М. А., Елисеев А. И., Минин Ю. В. Решение задачи оценки живучести локальных вычислительных сетей с целью повышения устойчивости их функционирования // Информатика: проблемы, методология, технологии : материалы XIII Междунар. науч.-метод. конф., Воронеж, 7-8 фев. 2013 г. Воронеж : Изд-во ВГУ, 2013. Т.1. С. 387-390.

Bondarenko I., Mironov P.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Development of an approach for the protection of information systems based on survivability analysis.

Despite the fact that a lot of attention is paid to reliability indicators, methods for analyzing survivability are rapidly developing, forming a subsection of reliability theory. One of the applications of such methods is the protection of information systems. The article highlights such concepts as resiliency, survivability, survival, safety, and shows their relationship. Three components of the approach for the protection of the information system based on survivability analysis are proposed. Described is a universal scenario of load testing of a media server in the absence and presence of a traffic analysis system and the detection of requests that impair the stability of the system.

Key words: information technology, information systems, survivability, monitoring systems, server, security, methods, load testing.

УДК 004.415.2
ГРНТИ 20.23.25

КРАТКИЙ ОБЗОР ПЛАТФОРМ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Р. Г. Григорьева, О. В. Раковский

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире часто возникает потребность организовывать образовательный процесс дистанционно. В этом случае появляется возможность расширить аудиторию обучающихся, избежать дополнительных транспортных и организационных расходов, а также проводить обучение независимо от мобильности обучающихся и карантинных ограничений. Для этого существуют системы дистанционного и удаленного образования.

СДО, образование, дистанционное обучение, информационные технологии

В настоящее время потребность людей в обучении достаточно высока. Школьное образование является обязательным, многие люди выбирают получение высшего образования, а также многие работники обязаны повышать квалификацию и подтверждать свои знания. Традиционно, обучение и прохождение контроля знаний выполняется в очной форме. Однако с появлением информационных технологий появилась возможность перенести обучение в дистанционный формат. Многие люди по тем или иным причинам не всегда имеют возможность присутствовать очно на занятиях или проходить контроль знаний в очной форме. Многим компаниям слишком невыгодно выделять время и персонал для обучения своих рабочих очно. Гораздо более удобна автоматизированная система контроля знаний, которая позволяет систематизировать данные о прохождении тестов и помогает распространить информацию. Для таких целей разработаны системы дистанционного обучения, помогающие получать учебную информацию дистанционно.

Система дистанционного обучения (СДО) – платформа для автоматизации и организации процессов обучения и получения информации студентами [1]. Данные платформы используются в случае необходимости донести учебный материал до студентов удаленно, а также для организации образовательного процесса в случае невозможности проведения его очно, к примеру, при различных эпидемиях. СДО позволяет систематизировать учебный материал, обеспечить к нему более широкий доступ, а также облегчает отслеживание успеваемости, как на уровне индивидуального пользователя, так и на уровне группы. На сегодняшний день существует множество разных платформ для организации дистанционного обучения.

Одной из таких систем обучения является платформа Moodle, используемая многими вузами, в том числе СПбГУТ. Платформа Moodle имеет открытый исходный код и позволяет создавать настраиваемые веб-сайты. Платформа Moodle бесплатна [2] и адаптируется под мобильные телефоны, однако считается сложной из-за необходимости установки. Рассмотрим подробнее достоинства и недостатки данной платформы на примере СДО СПбГУТ, построенной на платформе Moodle.

У каждого пользователя в системе есть свой профиль, позволяющий обеспечить приватность данных и надежность хранения личной информации. После входа в систему под индивидуальным логином и паролем обучающийся в системе имеет возможность записаться на какой-либо учебный курс. Для удобства и безопасности каждый курс защищен кодовым словом, которое руководитель курса назначает сам. При вводе кодового слова обучающийся получает доступ к учебным материалам, тестам и видеоконференциям по курсу. Преподаватель имеет возможность создавать различные темы для обсуждения и размещать объявления.

Обучающийся имеет возможность отправить работы дистанционно через СДО и просмотреть информацию о дате сдачи и оценке. Удобным является возможность загрузки файлов простым перетаскиванием из программы “Проводник”. Однако недостатком является загрузка файлов только до 20 Мбайт. В настоящее время работы студентов зачастую превышают данный объем из-за улучшения производительности персональных компьютеров. Зачастую презентации, программы и курсовые с большим количеством страниц превышают данный вес и возникает необходимость создания архива для уменьшения веса файлов. Учебные материалы загружаются преподавателем в СДО, после чего обучающийся имеет возможность их скачать на персональный компьютер. К сожалению, не все форматы файлов поддерживаются в СДО, а также скачивание может работать некорректно на мобильных устройствах.

Преподаватель имеет возможность настроить количество попыток, время прохождения и время доступности теста. После прохождения теста обучающийся может посмотреть время прохождения и дату завершения теста, оценку, а также выбранные варианты ответов теста.

В каждом курсе информация структурирована в отдельные темы, в которых можно проходить тесты и просматривать материал. Данные темы отображаются в боковом меню сайта. В боковом меню можно просмотреть участников курса, компетентности и оценки за различные задания. Во вкладке “Оценки” отображается информация об оценке, диапазоне, проценте выполнения, отзыве преподавателя, а также о вкладе теста в итог курса. Во вкладке “Студенты” отображаются все студенты в алфавитном порядке, группа студента и последнее время доступа к курсу.

У каждого обучающегося существует личный кабинет. Личный кабинет отображает информацию обо всех курсах студента, календарь, и хранилище личных файлов. В сводке по курсам присутствует фильтрация по названию и посещению курса. Можно настроить разные виды отображения курсов. Есть возможность просмотреть подробную информацию о пользователе. При этом отображается номер группы, форма обучения, номер зачетной книжки и ФИО, а также последнее посещение сайта. Есть доступ к мобильному приложению через QR.

Из недостатков СДО можно отметить отсутствие информации о зачетах и экзаменах, отсутствие расписания, а также отсутствие мобильной версии. Платформа Moodle оказывает большую нагрузку на сервер, поэтому финансовые

затраты на обеспечение работоспособности сайта СДО могут оказаться выше, чем у аналогичных платформ, требующих установки. Одной из причин нагрузки является наличие в Moodle большого количества инструментов, часть из которых не является необходимой для функционирования сайта. Для настройки Moodle необходимо хорошо знать систему. Самостоятельная установка затруднена.

Существует большое количество платформ СДО, в которых исправлены многие недостатки, присутствующие на платформе Moodle, однако присутствуют другие минусы. Среди таких платформ можно отметить Google Classroom. Данная платформа не требует установки, более простая и удобная в администрировании. Однако данная платформа обладает гораздо меньшим набором функций и подходит в основном для школ. Её интерфейс схож с интерфейсом стандартных приложений от компании “Google”, однако зачастую данная платформа не может обеспечить полностью комфортное дистанционное образование из-за отсутствия многих необходимых инструментов.

Из популярных платформ для СДО также можно отметить “iSpring Learn”. Данный сервис тоже является простым в регистрации. Данное СДО является более простым в установке, так как является интернет-сервисом и не требует отдельного сервера для комфортного использования. Из плюсов платформы можно отметить наличие мобильной версии и мобильного приложения. В этой системе есть возможность собрать статистику и выгрузить ее в различных форматах. В техподдержку iSpring Learn можно обратиться по телефону, через чат или отправив сообщение на почту. В отличие от Moodle, есть возможность сохранять записи вебинаров. Из минусов можно отметить платность системы. Цена формируется из времени аренды сервиса и количества активных пользователей на платформе.

Из бесплатных российских разработок можно отметить платформу Ё-Стади. Система Ё-Стади менее ориентирована на теоретический материал, однако дает больше возможностей при создании тестов и проверочных работ. При авторизации на СДО Ё-Стади можно увидеть область, в которой находятся тесты, учебные материалы и информация, размещенная преподавателем. Преподаватели имеют возможность объединить разные области, а также предоставить или запретить доступ конкретным обучающимся. Имеется возможность загрузки файлов и добавления к ним комментариев, а также журнала успеваемости. Журнал успеваемости содержит в себе информацию о пройденных тестах. Тесты можно импортировать из файлов, ограничивать срок проведения и количество попыток, а также запретить переключение между окнами браузера. В рассматриваемой системе существует форум, на который преподаватели могут писать необходимую информацию и создавать темы для обсуждения, и поддерживается возможность настройки e-mail рассылки.

Из плюсов можно отметить что Ё-Стади является более простой в установке и менее затратной, чем другие похожие системы. Однако существенным минусом является отсутствие широкого количества инструментов для проведения дистанционного обучения и ограниченность системы.

Таким образом, на данный момент есть несколько конкурентоспособных систем СДО. Каждая из них имеет свои недостатки и преимущества. Большинство систем являются либо недостаточно функциональными, либо чересчур перегруженными и тяжелыми. Отмечается, что основной функционал систем СДО в основном схож. В данный момент во многих системах не хватает оптимизации под мобильные устройства, а также во многих системах СДО присутствует ограничение по объему загруженного файла, что значительно затрудняет предоставление более объемных работ на проверку.

Список используемых источников:

1. Что такое Learning Management System (LMS) и как с ее помощью управлять обучением [Электронный ресурс]. URL: <https://www.ispring.ru/elearning-insights/chto-takoe-lms> (дата обращения 07.11.2022).

2. Обзор популярных СДО [Электронный ресурс]. URL: <https://ediscus.ru/blog/articles/obzor-populyarnyh-sdo-kakuyu-sistemu-vybrat> (дата обращения 07.11.2022).

Grigoreva R., Rakovskii O.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Brief overview of Learning Management Systems.

In the modern world, there is often a need to organize the educational process remotely. Thus, it becomes possible to expand the audience of students, avoid additional transportation and organizational costs, as well as conduct training regardless of student mobility and quarantine restrictions. For this purpose, there are systems of distance and remote education.

Key words: *LMS, education, remote learning, information technologies.*

УДК 519.6
ГРНТИ 27.03.66

ИССЛЕДОВАНИЕ ИНФОРМАЦИОННОЙ МОДЕЛИ ОЦЕНКИ УРОВНЯ ПОДГОТОВКИ СТУДЕНТОВ ПРИ ТЕСТИРОВАНИИ

А. Н. Губин, Е. А. Михайлова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В процессе обучения важным составляющим звеном является результат освоения программы. Уровень освоения программы у студентов определяется при помощи проведения самостоятельных, контрольных и итоговых экзаменационных работ. Помимо этого, для выявления уровня подготовки студентов проводится тестирование. В данной работе рассмотрены модели оценивания знаний студентов при тестировании.

тестирование, классическая модель, модель с учетом времени выполнения заданий, модель на основе уровней, модель Раша, модель Бирнбаума

По мере развития информационных технологий обычная форма контроля освоения учебного материала частично заменяется проведением тестирования. Особенно, проведение тестовых заданий широко распространено в формате дистанционного обучения.

Для того чтобы наиболее объективно оценить качество уровня подготовки студентов посредством тестирования, разработаны различные модели оценки знаний. В работе будут рассмотрены наиболее распространенные модели оценки знаний при тестировании.

Классическая модель является самой простой моделью оценивания знаний. В данной модели ответы оцениваются по двухбалльной (правильно или неправильно) или многобалльной (например, пятибалльной) шкале. Результат тестирования определяется по формуле:

$$R = \frac{\sum_{i=1}^k R_i}{n},$$

где R_i – правильный ответ обучаемого на i -е задание; k – количество правильных ответов из n предложенных ($k \leq n$), которое обычно округляется по правилам математики.

К достоинствам модели относится простота реализации. К недостатку данной модели следует отнести зависимость только от количества правильных ответов (не учитываются частично правильные выполненные задания).

В моделях, учитывающей время выполнения задания при определении результата учитывается время ответа на каждое задание или на весь тест. Этот метод позволяет определить насколько самостоятельно выполняется тестирование. В случае, если студент не обладает достаточными знаниями для успешного прохождения теста, он потратит много времени на поиск ответов в

сторонних источниках и не успеет ответить на все вопросы. Для правильных ответов рассчитывается значение R_i по формуле:

$$R_i = \begin{cases} 1, & t \leq t_{\max} \\ 0, & t > t_{\max} \end{cases},$$

где t – время выполнения задания; t_{\max} – время, отведенное для выполнения задания.

Затем итоговая оценка вычисляется так же, как и в простой модели [1].

Модели с учетом времени выполнения задания позволяют повысить надежность результатов тестирования.

В модели на основе уровней усвоения характеристикой усвоения учебного материала является уровень. Уровни разделяются на следующие группы: понимание, опознание, воспроизведение, применение и творческая деятельность.

Задания составляются для каждого из пяти уровней, при этом переход на следующий уровень возможен только в случае успешного освоения предыдущего.

Для измерения степени владения учебным материалом на каждом уровне используется коэффициент:

$$K_\alpha = \frac{P_1}{P_2}, \quad 0 \leq K_\alpha \leq 1$$

где P_1 – количество правильно выполненных существенных операций в процессе тестирования; P_2 – общее количество существенных операций в тесте; $\alpha=0, 1, 2, 3, 4$ – соответствует уровню освоения.

Существенные операции – это операции, которые выполняются на проверяемом уровне. Считается, что при $K < 0,7$ учебный материал не освоен [2].

Современная теория тестирования или Item Response Theory (IRT) использует математико-статистический анализ для оценки качества тестов. Данная теория позволяет отобразить, как в рамках всего теста функционирует каждое задание.

В рамках современной теории тестов разработаны три логистические модели, которые различаются числом задействованных параметров: однопараметрическая модель Раша, двухпараметрическая и трехпараметрическая модели Бирнбаума. Дополнительные параметры каждой модели влияют на применимость и получаемую по итогам анализа информацию. В рамках данных моделей параметры – это переменные, не подлежащие непосредственному измерению (латентные переменные). Все параметры измеряются через испытуемых на тестовые задания.

Однопараметрическая модель Раша представляет процесс выполнения теста, как взаимодействие множества испытуемых с множеством заданий. В основу теории положено утверждение о том, что трудность задания для каждого

испытуемого влияет на вероятность правильного ответа [3]. Математическая форма модели:

$$P(x) = \frac{e^{(\theta_i - \beta_j)}}{1 + e^{(\theta_i - \beta_j)}},$$

где $P(x)$ – вероятность правильного ответа; i – уровень подготовки i -го студента; j – сложность j -го тестового задания [4].

В двухпараметрической модели Бирнбаума вводится новый параметр – дискриминация, который показывает, насколько эффективно тестовое задание различает испытуемых с относительно высокими достижениями по критерию и тех, чьи достижения относительно низкие [3].

$$P(x) = \frac{e^{a_j(\theta_i - \beta_j)}}{1 + e^{a_j(\theta_i - \beta_j)}},$$

где a_j – дифференцирующая способность j -го тестового задания [4].

В трехпараметрической модели Бирнбаума появляется параметр угадывания, который отражает способность испытуемых дать правильный ответ наугад [3].

$$P(x) = c_j + (1 - c_j) \frac{e^{a_j(\theta_i - \beta_j)}}{1 + e^{a_j(\theta_i - \beta_j)}},$$

где c_j – вероятность угадывания правильного ответа для j -го задания [4].

Все три модели отличаются друг от друга добавлением нового параметра. Выбор модели для оценивания уровня подготовки студента в каждом случае должен рассматриваться отдельно. При выборе модели, необходимо учитывать необходимость дополнительных параметров, поскольку в некоторых случаях такие параметры как дифференцирующая способность и вероятность угадывания правильного ответа могут оказаться излишними во время процедуры оценки качества теста.

К наиболее эффективным следует отнести модели современной теории тестов. Благодаря параметрам, используемых в моделях, можно более точно определить уровень подготовки студента. Например, при известных значениях функции успеха $P_{xi=1}=0,9$ и сложности теста $i=1$ [5], становится возможным определить уровень подготовки студента по конкретному материалу, отраженному в тесте, используя модель Раша, согласно которой

$$0,9 = \frac{e^{\theta_i - 1}}{1 + e^{\theta_i - 1}}$$

откуда $i=1,197$.

Список используемых источников:

1. Зайцева Л.В., Прокофьева Н.О. Модели и методы адаптивного контроля знаний // Образовательные технологии и общество. – 2004. – Т. 7. - № 4. – С. 265-277.
2. Соловов, А. В. Проектирование компьютерных систем учебного назначения / А. В. Соловов. – Самара : Самарский национальный исследовательский университет имени академика С.П. Королева, 1995. – 138 с.
3. Бутина, Т. Д. Модели оценки качества тестов в современной теории тестирования / Т. Д. Бутина // Наука настоящего и будущего. – 2020. – Т. 2. – С. 184-186.
4. Маслак, А. А. Теория и практика измерения латентных переменных в образовании : монография / А. А. Маслак. – Москва : Издательство Юрайт, 2022. – 255 с.
5. Губин, А. Н. Методы анализа и оценки сложности тестовых заданий фондов оценочных средств дисциплины / А. Н. Губин, Ф. В. Филиппов, В. Л. Литвинов // Проектирование и обеспечение качества информационных процессов и систем : Сборник докладов Международной конференции, Санкт-Петербург, 15–17 марта 2022 года. – Санкт-Петербург: Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина), 2022. – С. 149-151.

Gubin A., Mikhailova E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Research of the information model for assessing the level of students' training in testing.

In the learning process, an important component is the result of mastering the program. The level of development of the program for students is determined by conducting independent, control and final examination papers. In addition, testing is conducted to identify the level of training of students. In this paper, models for assessing students' knowledge during testing are considered.

Key words: *testing, classic model, task time-based model, level-based model, rush model, Birnbaum model.*

УДК 004.7:004.422.8
ГРНТИ 20.01.07

ФОРМИРОВАНИЕ РАСШИРЕНИЙ МАТЕМАТИЧЕСКИХ ФОРМАЛИЗАЦИЙ ДЛЯ ИССЛЕДОВАНИЯ МЕТОДОВ И СРЕДСТВ УПРАВЛЕНИЯ КРУПНО-ГРАНУЛЯРНЫМИ ПРОЦЕССАМИ

Б. Б. Дамдинов, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрены сферы деятельности и артефакты с крупно-гранулярными процессами. Описаны основные цели управления крупно-гранулярными процессами. Представлены технологические компоненты жизненного цикла крупно-гранулярных процессов. Выявлены проблемные ситуации в жизненном цикле. Выделено ядро математических формализаций для анализа крупно-гранулярных процессов. Предложены новые приёмы для формирования расширений выделенного ядра.

процесс, управление, качество, расширение, формализация, модель, объектно-ориентированное моделирование

Масштабная цифровизация всевозможных видов жизнедеятельности характеризуется ускорением ключевых этапов жизненных циклов любых артефактов. В профессиональной деятельности наблюдается возрастающая степень концентрации коллективных работ, сочетающих знания специалистов различных отраслевых сфер.

Современные достижения в развитии инфотелекоммуникационных технологий определяют представительное многообразие решений, обеспечивающих достижения одних и тех же целей. Благодаря подобному многообразию порождаются вариации в организации сопутствующих крупно-гранулярных процессов, описывающих выполняемую деятельность и функционирование создаваемых и сопровождаемых артефактов.

В подавляющем большинстве современных артефактов, создаваемых в эпоху цифровой экономики, крупно-гранулярные процессы характеризуются семантической неоднородностью, обусловленной широким использованием представительного разнообразия физических и виртуальных ресурсов.

Решающую роль в ускорении жизненных циклов любых артефактов играют обширные исследования, опирающиеся на моделирование крупно-гранулярных процессов [1, 2]. При этом крупно-гранулярные процессы представляются в парадигме объектно-ориентированного подхода к проектированию артефактов.

С позиций системного подхода к научным исследованиям в методологических разработках формализаций анализа крупно-гранулярных процессов требуется объединить и согласовать:

- 1) методики выбора показателей и критериев качества крупно-гранулярных процессов;
- 2) методики представления гарантий;
- 3) методики построения моделей крупно-гранулярных процессов;
- 4) методики построения моделей окружающей среды;
- 5) методики разработки методов анализа моделей крупно-гранулярных процессов в благоприятных условиях;

б) методики разработки методов анализа крупно-гранулярных процессов в неблагоприятных (критических) условиях;

7) методики преодоления априорной неопределённости в знаниях о взаимодействиях составляющих подпроцессов в различных ситуациях;

8) методики подтверждения результатов анализа моделей крупно-гранулярных процессов;

9) методики управления крупно-гранулярными процессами с гарантиями качества.

В рамках объектно-ориентированного подхода к проектированию артефактов предпочтение отдаётся объектно-ориентированным моделям. Подобное предпочтение обеспечивает концептуальную связность указанных компонентов методологии жизненных циклов артефактов.

В опорную методологию объектно-ориентированного проектирования артефактов включаются концептуальные основы; объектно-ориентированные модели, разделяемые по классам; нотации моделей по выделенным классам и способы автоматизации разработки многокомпонентного программного обеспечения артефактов.

В опорной методологии остаются открытыми вопросы качества и, тем более, гарантий качества. Однако нарастающая востребованность в артефактах, характеризующихся различными профилями качества, является основной движущей силой для развития опорной методологии объектно-ориентированного проектирования. Основным звеном развития опорной методологии объектно-ориентированного проектирования являются объектно-ориентированные модели, расширяемые с сохранением преемственности в разделении на классы. Расширяемость достигается посредством введения новых элементов их описаний.

Новые элементы описания распространяются на стохастические свойства отражаемых характеристик элементов моделей и функциональных особенностей связи задействованных элементов. Позиционирование преемственности обеспечивает ещё один вид дополнительной связности указанных компонентов методологии жизненных циклов артефактов.

Расширение методологии объектно-ориентированного проектирования артефактов, в первую очередь, осуществляется применительно к прикладным сферам. К примеру, расширение проводится в жизненном цикле интеллектуальных сервис-ориентированных систем, биометрических систем, интеллектуальных комплексных систем защиты информации [4, 5, 6].

В методиках, относящихся к пятой группе, при работе с расширенными объектно-ориентированными моделями предусматривается учет топологической вариативности в организации крупно-гранулярных процессов. Однако на топологии, в которых наблюдаются циклы, не распространяются методики пятой группы. В связи с этим требуется их расширение, позволяющее выполнить аналитическое моделирование.

Наряду с этим, в работе [7] отслеживается характер связности подпроцессов в циклах. Выявленная особенность обуславливает определение теоретической основы для формирования нововведений в управлении крупно-гранулярными процессами.

Предлагаемые методические материалы определяют порядок и содержание работ по формированию расширений математических формализаций для исследования методов и средств управления крупно-гранулярными процессами.

Список используемых источников:

1. Птицына Л. К., Дамдинов Б. Б. Исследование методов управления крупно-гранулярными процессами // Региональная информатика : материалы Юбилейной XVIII Санкт-Петербургской междунар. конф., Санкт-Петербург, 26-28 окт. 2022 г. СПб. : СПОИСУ, 2022. С. 575-576.
2. Птицына Л. К. Программное обеспечение компьютерных сетей. Управление крупно-гранулярными процессами на основе языка BPEL : учебное пособие. СПб. : Издательство Политехнического университета, 2011. 105 с.
3. Баринов В. А., Болотова Л. С., Волкова В. Н., Денисов А. А., Дуболазов В. А., Емельянов А. А., Катаев А. В., Кузин Б. И., Кузьменков В. А., Ланкин В. Е., Лышарь Ю. И., Ногин В. Д., Птицына Л. К., Старовойтова М. И., Ступак В. Б., Татарова А. В., Федотов А. В., Ходырев В. В., Чудесова Г. П., Широкова С. В. и др. Теория систем и системный анализ в управлении организациями : справочник / под ред. В. Н. Волковой, А. А. Емельянова. М. : Инфра-М, 2021. 847 с.
4. Птицына Л. К., Эль Сабаяр Шевченко Н., Белов М.П., Птицын А.В. Математическое обеспечение мягких архитектур сервис-ориентированных систем в условиях неопределённости // Сборник докладов : материалы XXIV Междунар. конф. по мягким вычислениям и измерениям, Санкт-Петербург, 26 – 28 мая 2021 г. СПб. : СПбГЭТУ «ЛЭТИ», С. 121-124.
5. Птицына Л. К., Жаранова А. О., Птицын Н. А., Белов М. П. Расширение интеллектуальных технологий мягких архитектур интегрированных биометрических систем // Сборник докладов Международной конференции : материалы Междунар. конф. «Проектирование и обеспечение качества информационных процессов и систем», Санкт-Петербург, 15-17 марта 2022 г. СПб. : СПбГЭТУ «ЛЭТИ», 2022. С. 104-107.
6. Птицына Л. К., Дымченко А. В. Аналитическое моделирование мультиагентных систем принятия решений по обнаружению угроз информационной безопасности // Информационная безопасность регионов России : материалы XI Санкт-Петербургской межрегион. конф., Санкт-Петербург, 23-25 октября 2019 г. СПб. : СПОИСУ, 2019. С. 138 – 140.
7. Птицына Л. К., Эль Сабаяр Шевченко Н., Птицын А. В. Моделирование коммуникационно-вычислительных процессов систем телекоммуникаций при сквозном объединении диаграмм состояний и диаграмм деятельности // Телекоммуникации. 2022. № 4. С. 32-40.

Damdinov B., Ptitsyna L.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Formation of extensions of mathematical formalizations for the study of methods and means of controlling large-granular processes.

The spheres of activity and artifacts with large-granular processes are considered. The main objectives of the control of large-granular processes are described. The technological components of the life cycle of large-granular processes are presented. Identified problem situations in the life cycle. The core of mathematical formalizations for the analysis of large-granular processes is singled out. New techniques are proposed for the formation of extensions of the selected kernel.

Key words: *process, control, quality, extension, formalization, model, object-oriented modeling.*

УДК 004.658.3
ГРНТИ 77.01.85

PLANNING OF RESEARCH OF SERVICE-ORIENTED SYSTEMS WITH SOFT ARCHITECTURE

D. A. Ermolaev, V. A. Ivanova, A.V. Kovalchuk, L. K. Ptitsyna

St. Petersburg State University of Telecommunications named after Prof. M. A. Bonch-Bruевич

The key aspects of the prevalence of service-oriented systems are considered. The advantages of service-oriented systems are described. The results of the analysis of the service-oriented systems functioning quality are investigated. New topical areas of research of the systems under consideration have been identified. Studies of service-oriented systems with soft architecture in conditions of situational uncertainty in their functioning are planned.

concept, system, service, soft architecture, priori uncertainty, modeling

Currently, the integration of various kinds of data cannot solve all the problems associated with enterprise management, since the most important thing is not the data themselves, but their use in various business processes of the company. In modern information systems, it is not information that is considered an atomic unit, but a certain service that corresponds to a business process. At the present stage of the development of the information society, there are many applications that are created using various technologies, used on different computers and run under heterogeneous operating systems. In this regard, there is a need to combine a set of heterogeneous loosely coupled components into a single system. In this situation, one of the few solutions to this problem is the creation of multicomponent products according to the paradigm of service-oriented architectures (SOA – Service-Oriented Architecture). SOA is intended for the organization and use of a distributed set of functions that can be controlled by different owners [1].

Thanks to SOA existing facilities are reused, where new services are created for the deployed infrastructure. When focusing on a service-oriented architecture, the enterprise uses previously used assets and existing applications that guarantee compatibility between heterogeneous applications and technologies.

The main advantage of using service-oriented systems is that they provide a previously unattainable level of flexibility in the sense that:

- interfaces of software components are separated from their implementation;
- services are loosely coupled and are performed by services in accordance with the tasks;
- composite applications are built from aggregates of other services.

The "find-link-execute" paradigm is embedded in the service-oriented system. In this paradigm, suppliers register their services in a public registry. The specified register is used by consumers to search for services that meet certain criteria. If the desired service is located in the registry, then the consumer is provided with a contract and an endpoint address for the found service.

SOA-based systems are referred to as distributed multi-level applications that have layers of presentation, business logic and persistence [2]. Applications are the building blocks of SOA systems. Although any functionality can turn into a system, the challenge is to define the application interface at the right level of abstraction.

Key performance indicators of service-oriented systems are focused on organizations engaged in software development. They are analyzed in order to understand how resources should be used to ensure optimal business value and coordinate business projects for software development and investments in the IT sector, taking into account changes in the market. Key performance indicators are based on specialized practices to measure and improve the overall SOA approach.

Evaluating the effectiveness of service-oriented systems requires evaluating the enterprise service bus (ESB) in the system. When comparing an open source ESB, different factors are taken into account. As a rule, when determining productivity and efficiency, [3] the following indicators are evaluated:

- Average response time: The average response time is calculated as the amount of time elapsed from the moment the request was sent to the moment the response was received.
- Throughput: Throughput measured in transactions per second. A transaction is considered successful if it matches the expected response to this request.

After receiving test data for performance comparison, the results and achievements are analyzed.

Following the development of the concept of service-oriented systems, much attention is paid to methodological aspects.

In methodological aspects, the knowledge-intensive core is formalizations, including basic topologies of service-oriented systems, methods for constructing models of service-oriented systems, basic models of services, basic models of typical topological fragments of service-oriented systems, methods for displaying logic for integrating services in systems, methods for analyzing service integration, methods for developing techniques for analyzing innovative integration of services in systems and methods for confirming the correctness of the analysis results [4].

Based on the accumulated groundwork in the development of methodological aspects of the life cycle of service-oriented systems, various approaches to the design and creation of their soft architectures are being developed.

The main reasons for the transition to soft architectures of service-oriented systems lie in partial or complete priori uncertainty of the conditions for the performance of activities and a high degree of variability in the volumes and states of resources of those environments in which service-oriented systems are implemented.

The published materials devoted to soft architectures of service-oriented systems remain open in relation to the study of the influence of these reasons on their quality of functioning [5, 6, 7, 8, 9, 10, 11].

To eliminate the identified gap in knowledge, it is proposed to formalize research to determine the degree of influence of situational uncertainty on the quality of functioning of service-oriented systems with a soft architecture.

When conducting research, it is planned to distinguish three groups of experiments:

- study of the influence of partial or complete priori uncertainty of the performance activities conditions on the quality of service-oriented systems functioning;

- study of the influence of variability in the volumes and states of resources of environments in which service-oriented systems are implemented on the quality of their service-oriented systems functioning;

- study of the influence of partial or complete priori uncertainty of the activities performance conditions and variability of the volumes and states of the resources of the environments in which service-oriented systems are implemented on the quality of their service-oriented systems functioning.

For each group of studies, quality indicators of service-oriented systems with a soft architecture functioning are selected, mechanisms for displaying situational uncertainty on the formalization of the service-oriented systems life cycle are proposed, bases of extended object-oriented models are formed, techniques for modifying methods for identifying performance quality indicators are determined and possible quality profiles are evaluated in case of situational uncertainty.

The proposed research plan for intelligent service-oriented systems with a soft architecture will provide end-to-end connectivity in their mapping to the environments in which their functional specifications are implemented.

References:

1. KNOW INTUIT: [electronic resource]. November, 2022. URL: <https://intuit.ru/studies/courses/1055/271/lecture/6878?page=2> (accessed: 01.11.2022).

2. Service-Oriented Architecture (SOA) and Web Services: The Road to Enterprise Application Integration (EAI) [electronic resource] // oracle. November, 2022. URL: <https://www.oracle.com/technical-resources/articles/javase/soa.html> . (Accessed 01.11.2022).

3. O'Brien, (2009). A Framework for Scope, Cost and Effort Estimation for Service Oriented Architecture (SOA) Projects, Proc. 20th Australian Software Engineering Conference (ASWEC'09), IEEE Press, pp. 101-110.

4. Ptitsyna L. K., El Sabayar Shevchenko N., Belov M. P., Ptitsyn A.V. Mathematical support of soft architectures of service-oriented systems in conditions of uncertainty // XXIV International Conference on Soft Computing and Measurements (SCM-2021). Collection of reports. Saint-Petersburg. May 26 – 28, 2021 St. Petersburg: SPbSETU "LETI". pp. 121-124.

5. Ptitsyna L. K. Computer network software. Management of large-granular processes based on the BPEL language : textbook / L. K. Ptitsyna, N. G. Smirnov; rec. V. G. Orekhov. St. Petersburg : Polytechnic University Publishing House, 2011. 105 p.

6. Ptitsyna L. K., Ptitsyn A.V. Intelligent configuration of service-oriented systems // Information systems and technologies in modeling and management : collection of materials of the IV All-Russian scientific and practical conference with international participation (May 21-23, 2019) / editor K.A. Makoveychuk. – Simferopol : IT "ARIAL", 2019. pp. 48-51.

7. Zolotov O. I., Ptitsyna L. K., Temnikova M. V. Organization of intellectual content search for distance education systems // Actual problems of infotelecommunications in science and education. IX–th International scientific-technical and scientific-methodical conference: collection of scientific articles. St. Petersburg : SPbSUT, 2020. pp. 351-356.

8. Ptitsyna L. K., Karachinskaya E. A., Margaritova Ya. S. Extended object-oriented models of service-oriented systems for the organization of communication processes of counterparties //

Information security of the regions of Russia (IBRD-2019). XI St. Petersburg Interregional Conference. St. Petersburg, October 23-25, 2019: Conference proceedings. / SPOISU. – St. Petersburg, 2019. pp. 142-144.

9. Ptitsyna L. K., Dymchenko A.V. Modeling of multi-agent decision-making systems for detecting information security threats // Regional informatics and information security. Collection of works. Issue 7 / SPOISU. – St. Petersburg, 2019. pp. 115- 118.

10. Ptitsyna L. K., Zharanova A. O., Belov M. P., Ptitsyn A.V. CONTROL OF SOFT ARCHITECTURE OF DISTRIBUTED COMPLEX INFORMATION SECURITY SYSTEMS. In the collection: Proceedings of 2021 IV International Conference on Control in Technical Systems (CTS). IEEE, 2021. C. 103-106.

11. Ptitsyna L. K., El Sabayar Shevchenko N., Ptitsyn A.V. Modeling of communication and computing processes of telecommunication systems with end-to-end integration of state diagrams and activity diagrams // Telecommunications. № 4. 2022. C. 32-40.

Ermolaev D., Ivanova V., Kovalchuk A., Ptitsyna L.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunications

Planning for Service-Oriented Systems Research with a Soft Architecture.

The key aspects of the prevalence of service-oriented systems are considered. The advantages of service-oriented systems are described. The results of the analysis of the service-oriented systems functioning quality are investigated. New topical areas of research of the systems under consideration have been identified. Studies of service-oriented systems with soft architecture in conditions of situational uncertainty in their functioning are planned.

Key words: concept, system, service, soft architecture, priori uncertainty, modeling.

УДК 004.052.32
ГРНТИ 49.01.81

ОСНОВНЫЕ ПРИЧИНЫ СНИЖЕНИЯ ЭФФЕКТИВНОСТИ ЭКСПЛУАТАЦИИ МАГИСТРАЛЬНЫХ СЕТЕЙ СВЯЗИ

Д. И. Исаенко¹, Б. К. Резников¹, Д. Р. Романюк², Е. Е. Карпов²

¹ Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

² Национальный исследовательский университет ИТМО

Современная промышленность, системы обеспечения безопасности, научные и исследовательские центры не могут эффективно функционировать без постоянного обмена данными. Объемы передаваемого трафика постоянно увеличиваются, при этом также ужесточаются требования к надежности магистральных сетей передачи данных, как критических компонент государственной и корпоративной инфраструктуры. При этом, несмотря на целый спектр мер, направленных на сокращение количества отказов и снижение потерь, полностью решить проблему невозможно. При этом постоянное развитие технологий позволяет применять для повышения надежности магистральных сетей новые подходы, основанные на применении технологий искусственного интеллекта.

телекоммуникации, сети передачи данных, надежность, bit error rate, рефлектометрия

Магистральные сети - совокупность кабельных линий, усилителей, регенераторов и станционного оборудования, предназначенных для соединения крупных узлов (населенных пунктов и регионов) между собой. Иначе говоря, магистральные сети служат чем-то вроде артерий в теле человека - широкие каналы, способные на передачу большого объема данных.

Магистральные сети связи являются критически важной инфраструктурой государственного уровня. От качества их работы и надежности зависят такие важные сферы, как здравоохранение, государственная безопасность, экономические структуры. Поэтому возникает задача обеспечения максимальной эффективности работы магистральных сетей связи, для чего необходимо не только определить основные причины снижения эффективности эксплуатации подобных сетей, но и проводить их непрерывный контроль. Мониторинг основных параметров позволяет своевременно реагировать на возникшие неполадки внутри магистральных сетей, тем самым снизить финансовые и репутационные потери оператора связи. Стоит отметить, что в настоящее время, практически все магистральные сети связи представляют собой оптические линии связи, обладающие своей индивидуальной спецификой, в сравнении с металлическими магистральными линиями.

Все возможные отказы магистральных сетей связи можно разделить на:

1. физический отказ линейных сооружений и станционного оборудования;
2. отказ в обслуживании (перегрузка).

Основным параметром эффективности магистральных сетей связи является количество ошибок BER (bit error rate), так как связан со всеми остальными возможными параметрами. BER представляет собой достаточно эффективную меру оценки состояния сети, рассчитывается как отношение ошибочных битов к общему количеству битов.

Под физическим отказом подразумевается переход всей сети или ее элементов из работоспособного состояния в неработоспособное [1], причиной которого могут быть как полная или частичная потеря целостности как линейных сооружений (оптических кабелей, муфт и т. п.), так и физические повреждения станционного оборудования по причине нарушения условий эксплуатации или истощения ресурса (деградации компонентов). Физический отказ приведет к резкому увеличению показателя BER выше критических значений, при которых магистральная сеть будет непригодна для использования.

Частой причиной физического отказа является обрыв оптического кабеля по различным непрогнозируемым причинам (строительные работы, природные явления) и аварии на станционном оборудовании. Например, часто из строя выходят приемопередающие модули. В таком случае достаточно их заменить.

К отказу в обслуживании может привести некорректная настройка оборудования, ввиду ошибок обслуживающего персонала или ошибок проектирования, а также проникновения во внутреннюю сеть (предназначенную для управления оборудованием) злоумышленников с целью нарушения ее работоспособности.

В настоящее время для контроля основных параметров, влияющих на отказ магистральных сетей используются следующие методы:

1. рефлектометрия - позволяет получить достаточно удобный и понятный график (рефлектограмму) (рис. 1) зависимости оптической мощности сигнала от расстояния, а также видеть на ней изменения, вызванные различными неоднородностями, которые могут привести к ухудшению эффективности работы сети связи. Существенным недостатком является предельная дальность работы рефлектометров, проводящих эти измерения, ограниченная 100-150 км [3, 4].

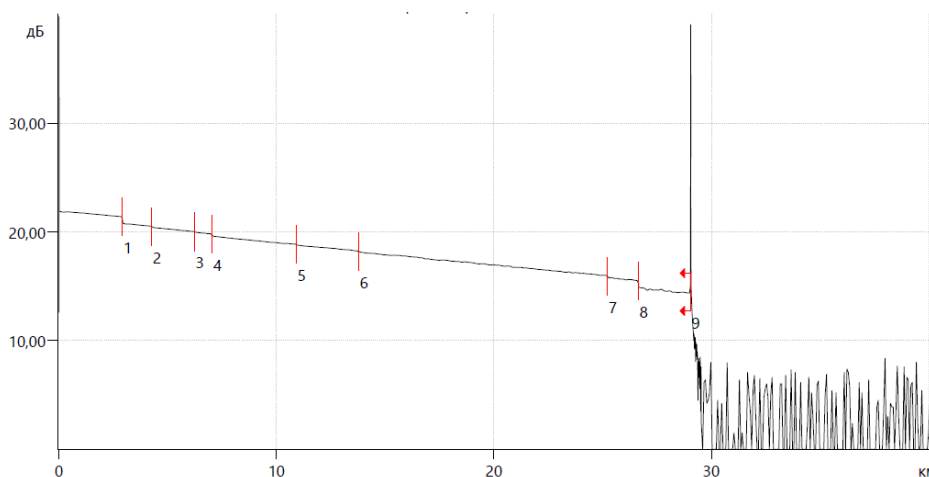


Рис. 1. Пример рефлектограммы

2. BER-тестирование обычно применяется на протяженных и высокоскоростных сетях, к которым относятся магистральные. С помощью BER-анализаторов генерируется псевдослучайная последовательность, имитирующая пользовательский трафик, которая вводится в магистральную сеть. BER-тестирование обычно проводится на этапе приемосдаточных работ. Тестирование считается успешным, при значении BER не выше 10^{-12} .

Однако, рефлектометрия и BER-тестирование не проводится постоянно, а значит не позволяет проводить непрерывный мониторинг магистральных сетей связи, что может привести к несвоевременному реагированию на аварию. Для организации непрерывного мониторинга или мониторинга по расписанию, возможно дополнительно устанавливать в стойки рефлектометр и BER-анализатор с удаленным управлением. При этом, контроль можно проводить на пользовательском трафике без ущерба для него. Таким образом можно не только быстро обнаружить проблемы на линии, но и спрогнозировать возможную аварию, вызванную различными причинами, при помощи инструментов искусственного интеллекта и нейросетевых модулей, что впоследствии может значительно повысить эффективность эксплуатации магистральных сетей связи, с точки зрения их надежности.

Для повышения надежности магистральных сетей связи применяются существующие решения:

1. резервирование оборудования и линейных сооружений. Дорогостоящий способ, при котором конечная стоимость проекта может вырасти в несколько раз, но при этом самый простой и надежный. Например, при резервировании оптического кабеля, проложенного другим путем до одной точки, становится возможна одновременная передача сразу по двум линиям. В таком случае на приемной стороне будет выбран тот канал, который обладает лучшим качеством. Однако данный подход требует использования дополнительного оборудования, что может существенно увеличить затраты на создание и эксплуатацию системы.

2. Прямая коррекция ошибок (FEC) позволяет существенно повысить BER, при этом сохраняя устойчивую связь. На данный момент, все сетевое каналобразующее оборудование имеет достаточно мощный алгоритм коррекции ошибок, благодаря чему BER имеет значение близкое к нулю. Однако, при превышении максимальной возможности работы алгоритма FEC связь резко обрывается.

3. Приоритизация трафика метод, пришедший из программно-конфигурируемых сетей. Применение данного метода весьма ограничено и может использоваться в случае перегрузки оборудования, где предпочтение будет отдаваться более значимому трафику. Вопрос приоритизации трафика в магистральных сетях связи с применением искусственных нейронных сетей требует дополнительных исследований.

4. Предсказание трафика с помощью нейросетевых модулей тоже является перспективной идеей, однако на данный момент действующих разработок представлено не было. Для подтверждения состоятельности данного решения необходимо также проведение дополнительных исследований.

Список используемых источников:

1. ГОСТ 27.002-2015. Надежность в технике. Термины и определения. МКС 21.020. Дата введения 2017-03-01.
2. ГОСТ 27.310-95. Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения. МКС 21.020. ОКСТУ 0027. Дата введения 1997-01-01.
3. Бурдин А. В., Пашин С.С. Оценка коэффициента отражения на разъемном соединении одномодовых оптических волокон по результатам анализа изображений торцевых

поверхностей феррул коннекторов. Труды учебных заведений связи. 2020;6(4):16-27.
<https://doi.org/10.31854/1813-324X-2020-6-4-16-27>

4. Ращупкин Е. О. Исследование принципов ранней диагностики повреждений в волоконно-оптических линиях передач. Евразийский союз ученых ЕСУ 2015.

Isaenko D., Reznikov B., Romanyuk D., Karpov E.

*The Bonch-Bruевич Saint-Petersburg State University of Telecommunication
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics*

*The Main Reasons For The Decrease In The Efficiency Of Backbone Network Operation.
Modern industry, security systems, scientific and research centers cannot function effectively without constant data exchange. The volume of transmitted traffic is constantly increasing, while the requirements for the reliability of backbone data networks, as critical components of government and corporate infrastructure, are also becoming stricter. At the same time, despite a range of measures aimed at reducing the number of failures and losses, it is impossible to completely solve the problem. At the same time, the constant development of technologies makes it possible to apply new approaches based on the application of artificial intelligence technologies to improve the reliability of backbone networks.*

Key words: telecommunications, data networks, reliability, bit error rate, OTDR.

УДК 004.415.2
ГРНТИ 50.41.29

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ИНТЕЛЛЕКТУАЛЬНОГО МОНИТОРИНГА МИКРОКЛИМАТА

К. А. Красавцева, О. В. Раковский

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе представлен результат проектирования и разработки информационной системы для мониторинга микроклимата. Описаны основные функции системы, выбор методов и технологий проектирования, а также результаты проектирования. Система мониторинга и анализа микроклимата может быть применена при проведении исследований по влиянию изменения микроклимата на состояние растений.

микроклимат, мониторинг микроклимата, обработка данных, отчет, датчик, разработка, анализ, выращивание растений

Изучение растений и способов их адаптации является актуальной задачей. Это обусловлено повышенным социальным интересом, а следовательно, и финансированием, т. к. затрагивает важнейшие сферы человеческой жизни, в первую очередь медицину и сельское хозяйство.

Так, например, согласно докладу «Селекция 2.0» высшей школы экономики и федеральной антимонопольной службы, в нашей стране очень высока доля импорта в посадочном материале. На момент исследования у подсолнечника она составляет 73%, картофеля - 90% и сахарной свеклы - 98%. Тогда как, согласно недавно утвержденной доктрине продовольственной безопасности, доля отечественных посадочных материалов должна составлять не менее 75% [1].

Состояние микроклимата оказывает значительное влияние на растения и является одним из необходимых условий их нормальной жизнедеятельности. На данный момент большинство исследований в сфере жизнеспособности различных биологических видов осуществляется в специальных помещениях, которые в той или иной степени изолированы от воздействия внешней среды и при этом должны ее имитировать.

С задачей поддержания заданных параметров микроклимата успешно справляются программы, предназначенные для этого, однако особенность специализации подобных систем не позволяет проводить более детальные исследования и, соответственно, применять их в научной сфере. Изучение и сравнение существующих систем позволяет выделить следующие особенности:

- всем системам доступно масштабирование (увеличение числа датчиков), однако оно ограничено доступным для подключения оборудованием;
- визуализация информации предусмотрена во многих системах, однако она не всегда является удобной и наглядной;
- в большинстве систем отсутствует возможность внесения изменений в настройки визуализации, а также нет возможности составления настраиваемых отчетов.

Выявленные особенности существующих систем, их достоинства и недостатки позволили сформулировать требования к разрабатываемой системе. Таким образом, она должна обеспечивать возможность:

- подключения различных датчиков и редактирование информации о них (в том числе внесение дополнительной информации и параметров);
- мониторинг и представление параметров микроклимата в доступном для анализа виде;
- создание и редактирование отчетов, шаблонов отчетов.

Для понимания модели функционирования системы построена диаграмма прецедентов, представленная на рис. 1. С информационной системой мониторинга микроклимата взаимодействуют следующие актеры типа «пользователь» – администратор, сотрудник.

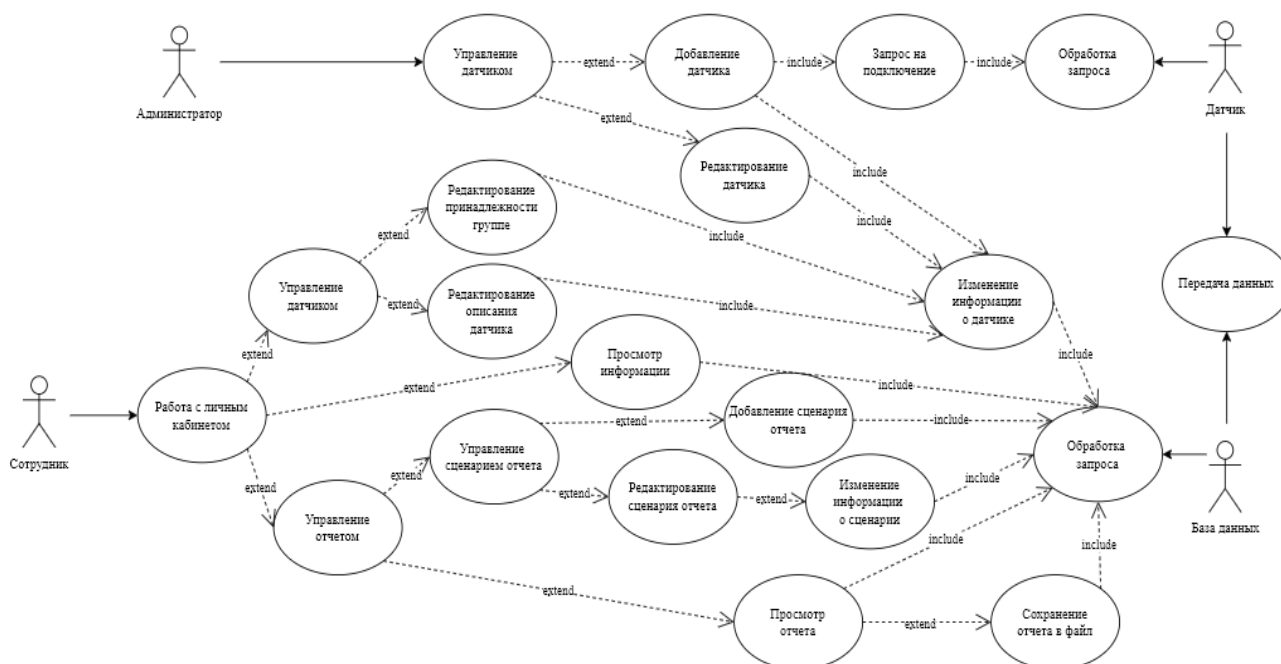


Рис. 1. Диаграмма прецедентов

Поскольку микроклимат – это динамическое явление, он определяется как совокупность физических процессов, которые включают перенос энергии (излучение и тепло) и массоперенос (потoki водяного пара и CO₂).

Проведение анализа с точки зрения микроклимата требует больших вычислительных затрат из-за внутренней сложности системы и связанных с ней явлений. Предлагаемые программные средства должны быть пригодны для работы с большими объемами разнородных данных для мониторинга и прогнозирования микроклимата.

Для проектирования базы данных системы разработана реляционная модель, представленная на рис. 2. Она определяет совокупность информационных объектов, их атрибуты и отношения.

Исходя из требований к системе выделены следующие сущности — сотрудник, датчик, значение показателя, отчет, шаблон и группа датчиков. В процессе проектирования добавлены сущности «датчик в отчете» и «датчик в группе».

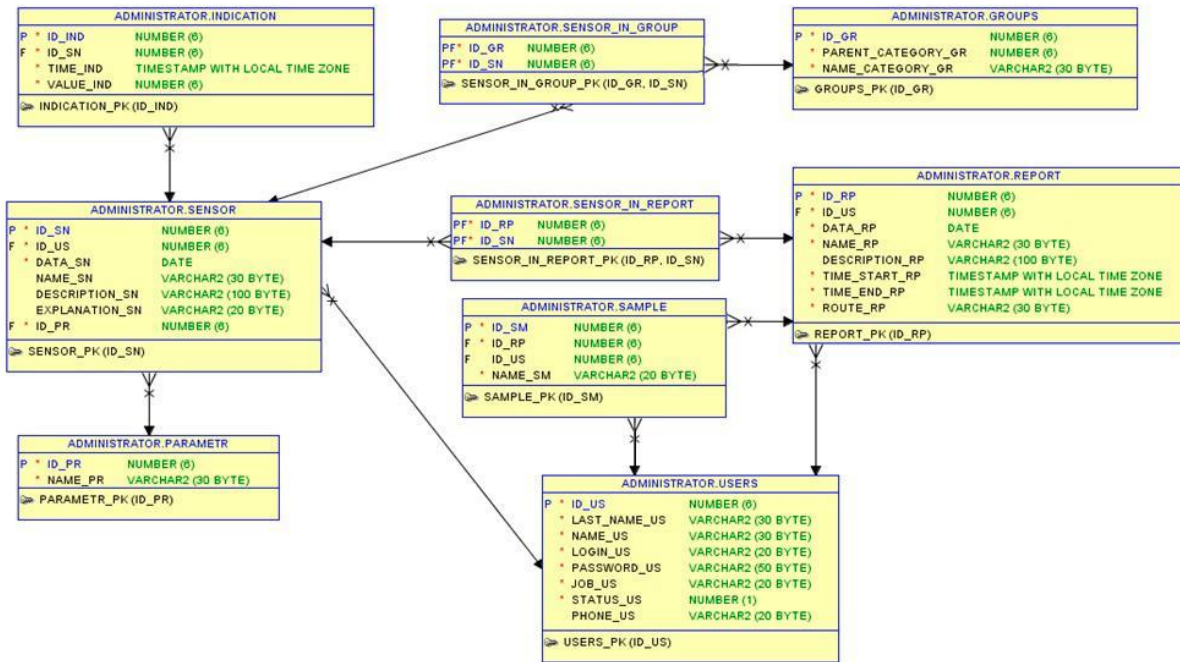


Рис. 2. Реляционная модель базы данных

После успешной авторизации пользователь, в зависимости от своей должности, получит доступ к одному из двух модулей программы: «Сотрудник» или «Администратор».

На рис. 3 представлена общая структура интерфейса. Белым цветом выделены общие модули, зеленым – доступные только администратору, синим — доступные только сотруднику.

Данная структура позволяет научному сотруднику просматривать данные от датчиков, создавать и редактировать отчеты, отслеживать параметры микроклимата.

Администратор, в свою очередь, может подключать датчики, просматривать и редактировать информацию о них, а также осуществлять работу с сотрудниками.

Разметка страниц системы выполнена по классической схеме для удобства ориентации пользователя. Визуализация интерфейса выполнена на базе библиотеки React.

Задействованный подход избавляет пользователя от необходимости дополнительного просмотра страницы для отображения изменений.

К стандартным операциям сотрудника можно отнести составление и просмотр отчета. Этот набор операций наиболее часто будет задействован при эксплуатации системы.

После внесения всех данных в форму отчета пользователь нажимает кнопку «Создать отчет». В результате этого действия на экране появляется запрошенная информация, представленная на рис. 4.

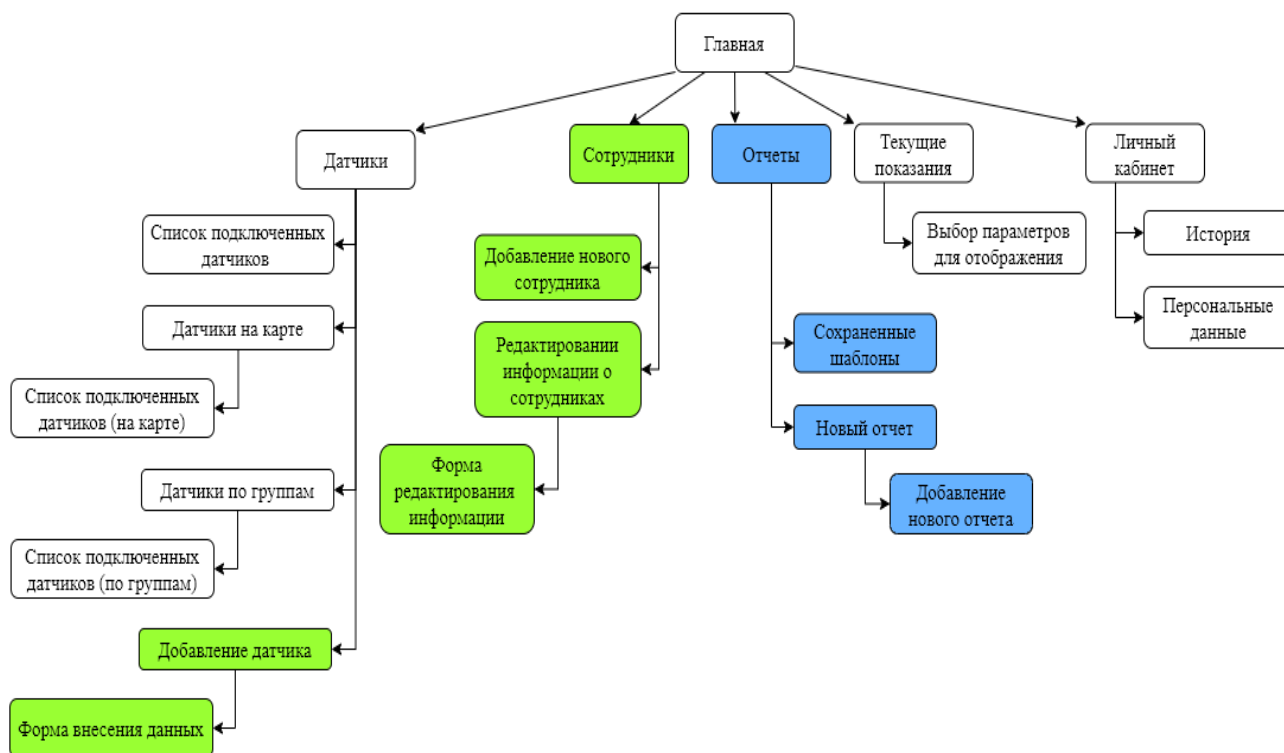


Рис. 3. Структура интерфейса

В рамках данной работы используются показания микроклимата из научных статей [2] и [3].

Разработанная система является самостоятельным модулем мониторинга микроклимата. Она может быть использована и в качестве части системы всестороннего мониторинга факторов, влияющих на состояние растения.

Дальнейшее развитие системы предполагает внедрение функций мониторинга состояния самого растения и происходящих в нем химико-биологических процессов, а также функций мониторинга состояния почвы и биоразнообразия окружающей среды.

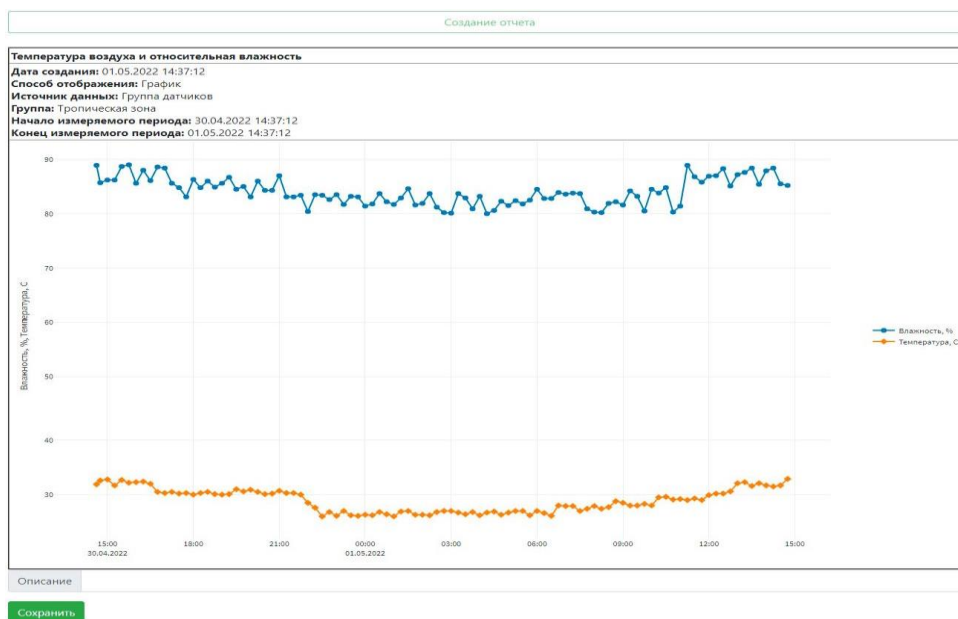


Рис. 4. Сформированный отчет

Список используемых источников:

1. Структура российского селекционного рынка / В.С. Волощенко, О.А. Гаврилова, С.В. Гончаров [и др.] // «Селекция 2.0». – Москва: Национальный исследовательский университет "Высшая школа экономики", 2020. – С. 17-112.
2. An Innovative Adaptive Control System to Regulate Microclimatic Conditions in a Greenhouse // MDPI.
3. Захлебин А.С. Моделирование тепловых режимов теплиц / А.С. Захлебин, А. М. Мукашев, И.С. Терновая // Science time. – Томск, 2016. – С. 370-375.

Krasavtseva K., Rakovskii O.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Development of an information system for intelligent microclimate monitoring.

The paper presents the result of designing and developing an information system for monitoring the microclimate. The main functions of the system, the choice of design methods and technologies, as well as design results are described. The microclimate monitoring and analysis system can be applied when conducting research on the effect of microclimate changes on the condition of plants.

Key words: microclimate, microclimate monitoring, data processing, report, sensor, development, analysis, growing plants.

УДК 004.7:004.422.8

ГРНТИ 20.01.07

АНАЛИЗ ВЛИЯНИЯ КОММУНИКАЦИОННОГО ВЗАИМОДЕЙСТВИЯ НА КАЧЕСТВО ФУНКЦИОНИРОВАНИЯ МУЛЬТИАГЕНТНЫХ СИСТЕМ УМНОГО ДОМА

К. С. Кусиков, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Актуализировано развитие систем умного дома. Рассмотрены различные подходы к повышению степени интеллектуализации систем умного дома. Выделены перспективные технологии архитектур систем умного дома. Представлены методы исследования качества функционирования систем умного дома с различными технологическими базисами. Предложен подход к формированию базиса формализаций для анализа влияния коммуникационного взаимодействия на качество функционирования мультиагентных систем умного дома.

умный дом, агентные технологии, мультиагентная система, распределённость, качество

В условиях развития цифровой экономики рационализация использования ресурсов в жизнедеятельности социума и повышение качества жизни ассоциируется с расширением масштабов применения и совершенствованием систем умного дома. По своему назначению и основополагающим принципам организации системы умного дома относятся к разряду распределённых систем [1].

Совершенствование систем умного дома, в первую очередь, базируется на интеграции и интеллектуализации [1, 2].

Определяющая роль в совершенствовании рассматриваемых систем отводится технологиям интеллектуализации с их современным арсеналом богатейших возможностей. При этом интеллектуализируется как отдельное оборудование, интегрируемое в систему, так и система в целом.

Перспективный тренд технологического базиса интеллектуализации на системном уровне ориентируется на использование агентных технологий, технологий интеллектуальных сервис-ориентированных систем и смешанных агентно-сервисных технологий.

Проводимая интеллектуализация предваряется анализом предлагаемых нововведений. Благодаря предварительности анализа удастся избежать реализации неконструктивных решений организации интеллектуальных систем умного дома.

В [3] раскрываются разработанные модели и методы анализа мультиагентной системы мониторинга оборудования электросетей, газового оборудования и средств водоснабжения сферы жилищно-коммунального хозяйства, предусматривающие последующее управление качеством их функционирования.

В [2] представляются методы анализа систем умного дома, организованных на основе сервисных технологий. В таком случае модели и методы анализа при

исследованиях систем умного дома разрабатываются на основе принципов и формализаций, приведённых в [4, 5, 6].

Неотъемлемой составляющей архитектур мультиагентных систем являются технические решения по интеграции субагентов. При описании альтернатив этих решений могут проводиться контекстные аналогии, позволяющие применять формализации, предлагаемые в [7].

Анонсированные методы исследования интеллектуальных систем умного дома не касаются учета влияния коммуникационного взаимодействия на качество их функционирования.

В целях детальной проработки деталей организации и функционирования мультиагентных систем умного дома проводится расширение формализаций их исследования посредством моделирования коммуникационных процессов субагентов, являющихся системообразующими составляющими общей работы интегрируемого оборудования. Расширение осуществляется на основе приёмов, представленных в [8, 9].

При моделировании коммуникационных процессов субагентов выделяются два типа их взаимодействия.

Первый тип взаимодействия ориентируется на отображение ключевых особенностей организации подсистем планирования действий мультиагентных систем. В этом случае ранжируются частные планировщики действий субагентов, согласованное функционирование которых координируется генеральным планировщиком мультиагентной системы. При отображении взаимодействия предусматривается моделирование подпроцессов планирования, присущих подсистеме планирования действий мультиагентной системы [10, 11].

Второй тип взаимодействия касается информационного обмена между агентами.

Каждый тип взаимодействия планируется исследовать посредством расширенного объектно-ориентированного моделирования.

Предлагаемая постановка задач анализа коммуникационного взаимодействия на качество функционирования мультиагентных систем умного дома характеризуется научной новизной на уровне модельного ряда и методов их исследования.

Список используемых источников:

1. Долгун В. О., Птицына Л. К. Архитектура распределённых интеллектуальных систем управления умным домом // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VIII Междунар. научно-технич. и научно-методич. конф., Санкт-петербург, 27-28 февр. 2019 г. СПб. : СПбГУТ, 2019. Т. 2. С. 264 – 268.
2. Птицына Л. К., Кусиков К. С. Методы исследования интегрированных систем умного дома // Региональная информатика : материалы XVIII Санкт-Петербургской междунар. конф., Санкт-Петербург, 26-28 октября 2022 г. СПб. : СПОИСУ, 2022. С. 577.
3. Кадынцева Д. В., Птицына Л. К. Моделирование мультиагентной системы мониторинга оборудования электросетей, газового оборудования и средств водоснабжения сферы жилищно-коммунального хозяйства // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы IX Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 26-27 февр. 2020 г. СПб. : СПбГУТ, 2020. С. 375-379.

4. Птицына Л. К., Смирнова П. В. Методика формирования модели сервис-ориентированных систем с темпоральной логикой синхронизации сервисов // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VI Междунар. научно-технич.я и научно-методич. конф., Санкт-Петербург, 1-2 марта 2017 г. СПб. : СПбГУТ, 2017. Т. 3. С. 355 – 360.

5. Птицына Л. К., Эль Сабаяр Шевченко Н. Н., Белов М. П., Птицын А. В. Моделирование сервис-ориентированных систем в условиях неопределённости // Сборник докладов : материалы Междунар. конф. по мягким вычислениям и измерениям, Санкт-Петербург, 23-25 мая 2018 г. СПб. : СПбГЭТУ «ЛЭТИ», 2018. С. 291-294.

6. Птицына Л. К., Эль Сабаяр Шевченко Н., Белов М. П., Птицын А. В. Математическое обеспечение мягких архитектур сервис-ориентированных систем в условиях неопределённости // Сборник докладов : материалы XXIV Междунар. конф. по мягким вычислениям и измерениям, Санкт-Петербург, 26 – 28 мая 2021 г. СПб. : СПбГЭТУ «ЛЭТИ». С. 121-124.

7. Птицына Л. К., Жаранова А. О., Птицын Н. А., Белов М. П. Расширение интеллектуальных технологий мягких архитектур интегрированных биометрических систем // Проектирование и обеспечение качества информационных процессов и систем : материалы Междунар. конф., Санкт-Петербург, 15-17 марта 2022 г. СПб. : СПбГЭТУ «ЛЭТИ», 2022. С. 104-107.

8. Птицына Л. К., Карачинская Е. А., Маргаритова Я. С. Расширенные объектно-ориентированные модели сервис-ориентированных систем для организации коммуникативных процессов контрагентов // Информационная безопасность регионов России : XI Санкт-Петербургская межрегион. конф., Санкт-Петербург, 23-25 октября 2019 г. СПб. : СПОИСУ, 2019. С. 142-144.

9. Птицына Л. К., Лебедева А. А. Методика формирования динамических характеристик интеллектуальных информационных агентов в условиях активной инфокоммуникационной среды // Информация и космос. 2017. № 1. С. 105-111.

10. Птицына Л. К., Жаранова А. О., Птицын Н. А., Белов М. П. Расширенное объектно-ориентированное моделирование планировщиков интеллектуальных информационных агентов // Список докладов : материалы XXV Междунар. конф. по мягким вычислениям и измерениям, Санкт-Петербург, 25 – 27 мая 2022 г. СПб. : СПбГЭТУ «ЛЭТИ», С. 87-90.

11. Ptitsyna L. K., Zharanov A. O., Ptitsyn N. A., Belov M. P. Extended Object-Oriented Modeling of Intelligent Information Agent Planners // XXV International Conference on Soft Computing and Measurements, Saint Petersburg, 25 - 27 May 2022. IEEE, 2022. С. 60-63.

Kusikov K., Ptitsyna L.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of the impact of communication interaction on the quality of functioning of multi-agent smart home systems.

The development of smart home systems has been updated. Various approaches to increasing the degree of intellectualization of smart home systems are considered. Promising technologies of architectures of smart home systems are highlighted. Methods for studying the quality of functioning of smart home systems with various technological bases are presented. An approach to the formation of the basis of formalizations for analyzing the influence of communication interaction on the quality of functioning of multi-agent smart home systems is proposed.

Key words: *smart house, agent technology, multi-agent system, distribution, quality.*

УДК 004.7:004.422.8

ГРНТИ 20.01.07

КОНЦЕПТУАЛЬНОЕ МОДЕЛИРОВАНИЕ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ С МЯГКОЙ АРХИТЕКТУРОЙ

Е. А. Лакомкина, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Описаны ключевые факторы востребованности комплексных систем защиты информации. Рассмотрены цели интеллектуализации комплексных систем защиты информации. Проведен анализ основных подходов к интеллектуализации рассматриваемого класса систем. Выделены отличительные особенности технологий интеллектуализации комплексных систем защиты информации. Предложены альтернативные среды для концептуального моделирования комплексных систем защиты информации с мягкой архитектурой.

защита, интеллектуализация, технологический базис, знание, моделирование, модельно-аналитический интеллект

При масштабном погружении различных аспектов жизнедеятельности в современном социуме проявляется объективная потребность в обеспечении должного уровня информационной безопасности.

При непрерывном разрастании поля угроз, присущих информационному пространству, информационная безопасность обеспечивается комплексными системами защиты информации.

В условиях развития цифровой экономики комплексные системы защиты информации активно совершенствуются. При этом одно из приоритетных направлений совершенствования комплексных систем защиты информации ассоциируется с разработкой и внедрением технологий интеллектуализации, пронизывающих насквозь из жизненный цикл.

Любая из технологий интеллектуализации ориентируется не только на повышение степени автоматизации базовых функциональных процессов и степени защищённости информационных инфраструктур и их ключевых ресурсов, но и на снижение влияния человеческого фактора на эффективность функционирования комплексных систем защиты информации. В связи с этим агентные технологии вводятся в качестве системообразующих компонентов в технологический базис интеллектуальных комплексных систем защиты информации [1, 2, 3].

Благодаря распределённости комплексных систем защиты информации их соответствующее многокомпонентное программное обеспечение может проектироваться, создаваться и сопровождаться в соответствии с парадигмой сервис-ориентированных систем. В таком случае арсенал технологий интеллектуальных сервис-ориентированных систем может включаться в технологический базис жизненного цикла комплексных систем защиты информации [4].

В рассматриваемом арсенале выделяются не только гомогенные технологии интеллектуализации, но и гетерогенные, определяющие сквозную связность агентных технологий и нейросетевых технологий.

В последующем расширении арсенала технологий интеллектуализации комплексных систем защиты информации предусматривается переход на их мягкую архитектуру, при которой управление конфигурацией и процессом функционирования комплексной системой защитой информации осуществляется модельно-аналитическим интеллектом [5, 6, 7, 8].

Модельно-аналитический интеллект формируется посредством аналитического моделирования процессов функционирования комплексных систем защиты информации, соответствующих требуемым классам защищенности в поле угроз окружающей среды.

Формирование модельно-аналитического интеллекта базируется на основе генерации системно-аналитического ядра безопасных информационных технологий [9, 10, 11].

В зависимости от типа класса защищённости в комплексные системы интегрируются средства защиты различного назначения, профилированные на определённые виды угроз. Характер интеграции может варьироваться в зависимости от задействованных технологий обработки информации в комплексных системах.

В задействованных технологиях обработки информации в комплексных системах различаются: последовательная, параллельная и распределённая обработка.

Каждый вид обработки данных требует применения соответствующих методов анализа построенных моделей комплексных систем защиты информации.

В каждом из выделенных направлений интеллектуализации комплексных систем защиты информации сформировался представительный арсенал формализаций, обеспечивающих сквозную связность гомогенных технологий и выбор приоритетных технологических сочетаний при различных ситуациях поведения окружающей среды. В целях накопления и расширения знаний о технологиях интеллектуализации комплексных систем защиты информации предлагается концептуальное моделирование их мягких архитектур, которое может осуществляться в различных средах, автоматизирующих построение и анализ моделей. Для каждого типа сред выделяются как преимущества, так и недостатки, обеспечивая приоритетный выбор в зависимости от целеполагания при приобретении знаний о технологическом базисе комплексных систем защиты информации с мягкой архитектурой.

Представляемые исследования обеспечивают формирование средств для хранилища знаний, необходимого для создания банка технологий, начатого в Российской Федерации.

Список используемых источников:

1. Птицына Л. К., Лебедева А. А. Методика формирования динамических характеристик интеллектуальных информационных агентов в условиях активной инфокоммуникационной среды // Информация и космос. 2017. № 1. С. 105-111.
2. Птицына Л. К., Птицын А. В. Обеспечение информационной безопасности на основе методологического базиса агентных технологий // Вестник Брянского государственного технического университета. 2017. № 2 (55). С. 146 -154.
3. Птицына Л. К., Дымченко А. В. Моделирование мультиагентных систем принятия решений по обнаружению угроз информационной безопасности // Региональная информатика и информационная безопасность: сб. тр. / СПб. : СПОИСУ, 2019. Вып. 7. С. 115- 118.
4. Птицына Л. К., Эль Сабаяр Шевченко Н. Н., Белов М. П., Птицын А. В. Нейросетевой подход к преодолению априорной неопределённости при оптимальном планировании действий интеллектуальных информационных агентов для мягких архитектур сервис-ориентированных систем // NeuroNT'2021 : материалы II Междунар. конф. по нейронным сетям и нейротехнологиям, Санкт-Петербург, 16 июня. 2021 г. СПб. : СПбГЭТУ «ЛЭТИ», 2021. С 36-39
5. Ptitsyna L. K., El. Sabayar Shevchenko N., Belov M. P., Ptitsyn A. V. A NEURAL NETWORK APPROACH TO OVERCOMING A PRIORI UNCERTAINTY IN OPTIMAL ACTION PLANNING OF INTELLIGENT INFORMATION AGENTS FOR SOFT ARCHITECTURES OF SERVICE-ORIENTED SYSTEMS // NeuroNT 2021 : 2nd International Conference on Neural Networks and Neurotechnologies, SPb, 2021. С. 31-34.
6. Птицына Л. К., Жаранова А. О., Белов М. П., Птицын А. В. Управление мягкой архитектурой распределенных комплексных систем защиты информации // ПУТС-2021 : материалы IV Междунар. науч. конф. по проблемам управления в технических системах, Санкт-Петербург, 21-23 сент. 2021 г. СПб. : СПбГЭТУ «ЛЭТИ», 2021 г. Т.1. С. 138-142.
7. Птицына Л. К., Жаранова А. О. Вычислительный интеллект мониторинга информационной защищенности распределенных систем учета // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы X Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 24-25 февр. 2021 г. СПб. : СПбГУТ, 2021. С. 235-239.
8. Ptitsyna L. K., Zharanova A. O., Belov M. P., Ptitsyn A. V. CONTROL OF SOFT ARCHITECTURE OF DISTRIBUTED COMPLEX INFORMATION SECURITY SYSTEMS // CTS : IV International Conference on Control in Technical Systems, Saint Petersburg, 21-23 Sept.. 2021. С. 103-106.
9. Птицын А. В. Генерация системно-аналитического ядра безопасных информационных технологий / А. В. Птицын, Л. К. Птицына. СПб.: Изд-во Политехн ун-та, 2011. 263 с.
10. Птицын А. В. Аналитическое моделирование комплексных систем защиты информации. Новые формализации аналитического исследования комплексных систем защиты информации / А. В. Птицын, Л. К. Птицына. Гамбург. Saarbrucken: LAP LAMBERT Academic Publishing. 2012. 293 с.
11. Птицын А. В. Методологический базис агентных технологий для обеспечения информационной защищённости // Научные технологии в космических исследованиях Земли. 2015. Т.7. № 1. С. 50-55.

Lakomkina E., Ptitsyna L.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Conceptual modeling of complex information security systems with soft architecture.

The key factors of demand for complex information security systems are described. The goals of intellectualization of complex information security systems are considered. The analysis of the main approaches to the intellectualization of the considered class of systems is carried out. Distinguishing features of technologies of intellectualization of complex information security systems are highlighted. Alternative environments for conceptual modeling of complex information security systems with soft architecture are proposed.

Key words: protection, intellectualization, technological basis, knowledge, modeling, model-analytical intelligence.

УДК 004.853
ГРНТИ 20.53.19

ОБЗОР МЕТОДОВ СЕГМЕНТАЦИИ ИЗОБРАЖЕНИЙ

Е. А. Леонова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье раскрывается понятие сегментации изображения. Рассмотрены области, в которых применяется компьютерное зрение, и, сегментация, в частности. Приведены методы сегментации изображения, а также описаны подходы для каждого из методов.

компьютерное зрение, сегментация, поиск объекта, распознавание объекта, изображение

Сегментация изображений относится к области цифровой обработки изображений, которая фокусируется на разделении изображения на различные части в соответствии с их особенностями и свойствами. Основной целью является упрощение изображения для более простого анализа. При сегментации изображения происходит его разделение на различные части, которые имеют схожие атрибуты. Части, на которые делится изображение, называются объектами изображения [1].

Сегментация изображений является важным аспектом компьютерного зрения и активно применяется в различных отраслях. К числу областей, где сегментация изображений находит широкое применение, относятся [2]:

1. Распознавание лиц. Технология распознавания лиц, присутствующая, например, в современных системах безопасности, использует сегментацию изображения для идентификации лица человека. Благодаря возможности определения уникальных черт лица, нежелательные лица не могут получать доступ к охраняемой системе.

2. Идентификация номерных знаков. Многие светофоры и камеры используют идентификацию номерных знаков для начисления штрафов и помощи в поиске нарушителя. Технология идентификации номерных знаков позволяет дорожной системе распознать автомобиль и получить информацию о его владельце. Она использует сегментацию изображения, чтобы отделить номерной знак от остальных объектов, присутствующих в поле зрения.

3. Поиск на основе изображений. *Google* и другие поисковые системы, предлагающие поиск по картинкам, используют методы сегментации для идентификации объектов, присутствующих на заданном изображении.

4. Медицинская визуализация. В медицинской сфере используется сегментация изображений для обнаружения и идентификации раковых клеток, измерения объема тканей, виртуального моделирования операций.

Помимо вышеперечисленных областей применения, сегментация изображений используется в производстве, сельском хозяйстве, безопасности и многих других отраслях. По мере того, как технологии компьютерного зрения становятся все более совершенными, применение методов сегментации изображений будет расширяться [3].

Например, некоторые производители начали использовать методы сегментации изображений для поиска бракованной продукции. Здесь алгоритм

захватывает только необходимые компоненты с изображения объекта и классифицирует их как неисправные. Такая система снижает риск человеческих ошибок и делает процесс тестирования более эффективным для организации.

Методы сегментации изображений служат для решения широкого круга задач и у этого процесса есть разные способы выполнения. Принято классифицировать сегментацию изображений по следующим критериям:

1. Классификация на основе используемого подхода.

В самом базовом смысле сегментация изображения – это идентификация объекта. Алгоритм не может классифицировать различные компоненты, не идентифицировав сначала объект. От простых до сложных реализаций, все сегментации изображений работают на основе идентификации объекта [4]. Таким образом, можно классифицировать методы сегментации изображений на основе того, как алгоритмы идентифицируют объекты, то есть собирают похожие пиксели и отделяют их от непохожих. Существует два подхода к выполнению этой задачи:

- Подход на основе области (обнаружение сходства). В этом методе происходит обнаружение похожих пикселей изображения в соответствии с выбранным порогом, объединение, распространение и рост областей. Кластеризация и подобные алгоритмы машинного обучения используют этот метод для обнаружения неизвестных характеристик. Алгоритмы классификации используют этот подход для обнаружения признаков и разделения сегментов изображения в соответствии с ними.

- Подход на основе границ (обнаружение разрывов). Подход на основе границ является противоположностью подхода на основе областей для идентификации объектов. В отличие от обнаружения на основе региона, где происходит поиск пикселей с похожими характеристиками, при подходе на основе границ происходит поиск пикселей, непохожие друг на друга. Алгоритмы обнаружения точек, краев, линий и аналогичные алгоритмы используют этот метод, определяя границы несхожих пикселей и отделяя их от остальной части изображения.

2. Классификация на основе используемых данных.

Эти методы используются в зависимости от типа заданного изображения, а также от желаемых целей и результатов [5]. На основании этих параметров происходит деление алгоритмов сегментации изображений на следующие категории:

- Структурные методы. Эти алгоритмы требуют наличия структурных данных используемого изображения. Сюда входят пиксели, распределения, гистограммы, плотность пикселей, распределение цветов и другая соответствующая информация. Затем необходимо получить структурные данные об области, которую нужно выделить из изображения.

Эта информация необходима для того, чтобы алгоритм мог идентифицировать область. Алгоритмы, используемые в этом случае, следуют подходу, основанному на обнаружении сходства.

- Стохастические методы. Эти алгоритмы требуют информацию о дискретных значениях пикселей изображения, а не о структуре требуемого участка изображения. Благодаря этому они полезны, когда приходится работать с несколькими изображениями. Алгоритмы машинного обучения, такие как кластеризация *K-means* и технологии нейронных сетей, относятся к этой категории.

- Гибридные методы. Как можно догадаться из названия, эти алгоритмы используют как стохастические, так и структурные методы. Это означает, что для сегментации изображения они используют структурную информацию требуемой области и дискретную информацию о пикселях всего изображения.

Технологии глубокого обучения существенно улучшили и упростили алгоритмы семантической сегментации, проложив путь для более широкого применения в реальной жизни. Концепты методов, показанных в статье, не являются исчерпывающими, так как сообщество исследователей постоянно стремится улучшить точность и производительность этих алгоритмов в реальном мире.

Список используемых источников:

1. Sharipov D., Mukhiddinov D., Ruziqulova N. Segmentation in an ancient Document Imaging and Characters // Проблемы вычислительной и прикладной математики. 2022. N 2/1(40). – С. 272-279.

2. Wang S. Image segmentation: Generic modeling, detection, and estimation of discontinuities in image surfaces: Thesis (Ph. D.) / Wang Sheng-Jyh. Stanford University/ 1994. 220 p.

3. Митропольский Н. Н. Агломеративная сегментация и поиск однородных объектов на растровых изображениях: диссертация на соискание ученой степени канд. техн. наук: 05.13.17 / Митропольский Николай Николаевич. Москва, 2010. 137 с.

4. Khanykov I. G., Tolstoj I. M., Levonevskiy D. K. The classification of the image segmentation algorithms // International Journal of Intelligent Unmanned Systems. 2020. Vol. 8. N 2. p. 115-127.

5. Wang B., Jia Q., Zhao B., Luo X. Image interference elimination method based on image segmentation in a multi-CCD measurement system // Qinghua Daxue Xuebao/ Journal of Tsinghua University. 2010. Vol. 50. N 2. p. 208-223.

Leonova E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Review of image segmentation methods.

The article reveals the concept of image segmentation. The fields in which computer vision is applied, and segmentation in particular, are considered. The methods of image segmentation are given, and the approaches for each of the methods are described.

Key words: *computer vision, segmentation, object search, object recognition, image.*

УДК 65.011.56
ГРНТИ 71.01.85

ИССЛЕДОВАНИЕ МЕТОДОВ АВТОМАТИЗАЦИИ ЛОГИСТИЧЕСКИХ ЦЕНТРОВ

В. Л. Литвинов, А. В. Яшин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Актуальность статьи обусловлена развитием логистических технологий и стремлением сократить трудозатраты за счет внедрения средств автоматизации. Создание новых бизнес-моделей подтолкнули компании к поиску инновационных технологических решений для поддержания конкурентоспособности. Это приводит к появлению автономных и мобильных роботов на логистических центрах.

автоматизация, логистика, склады, высокие технологии, роботизация

В современном мире процесс автоматизации является неотъемлемым этапом развития производства промышленных компаний. Этот процесс также затронул и логистическое складирование. Тенденция автоматизации склада является важной частью развития предприятий для поддержания конкурентоспособности [1].

Автоматизация склада – это внедрение передового программного обеспечения и современного оборудования в логистические процессы. Такие технологии ускоряют бизнес-операции складской деятельности и оптимизируют их, позволяя сократить цикл товарооборота на складе. Это во многом оптимизирует и временные ресурсы компании [2].

Существует два типа автоматизации склада:

- Цифровая автоматизация;
- Физическая автоматизация.

Для визуального представления процесса автоматизации разработана концептуальная модель, которая показана на рис. 1.

Цифровая автоматизация использует данные и программное обеспечение для сокращения ручных процессов. Например, все активнее используются технологии автоматической идентификации и сбора данных (AIDC): штрих-кодирование, радиочастотные RFID-метки, биометрия и т.д.

К преимуществам цифровой автоматизации процессов относится возможность интеграции с системами планирования ресурсов (ERP), высокая эффективность управления данными, снижение операционных и юридических рисков, снижение ручных процессов и ошибок из-за «человеческого фактора». Такие технологии, как радиочастотная идентификация (RFID) и мобильное штрих-кодирование, могут повысить результативность сотрудников, уменьшить трудозатраты и снизить эксплуатационные расходы.

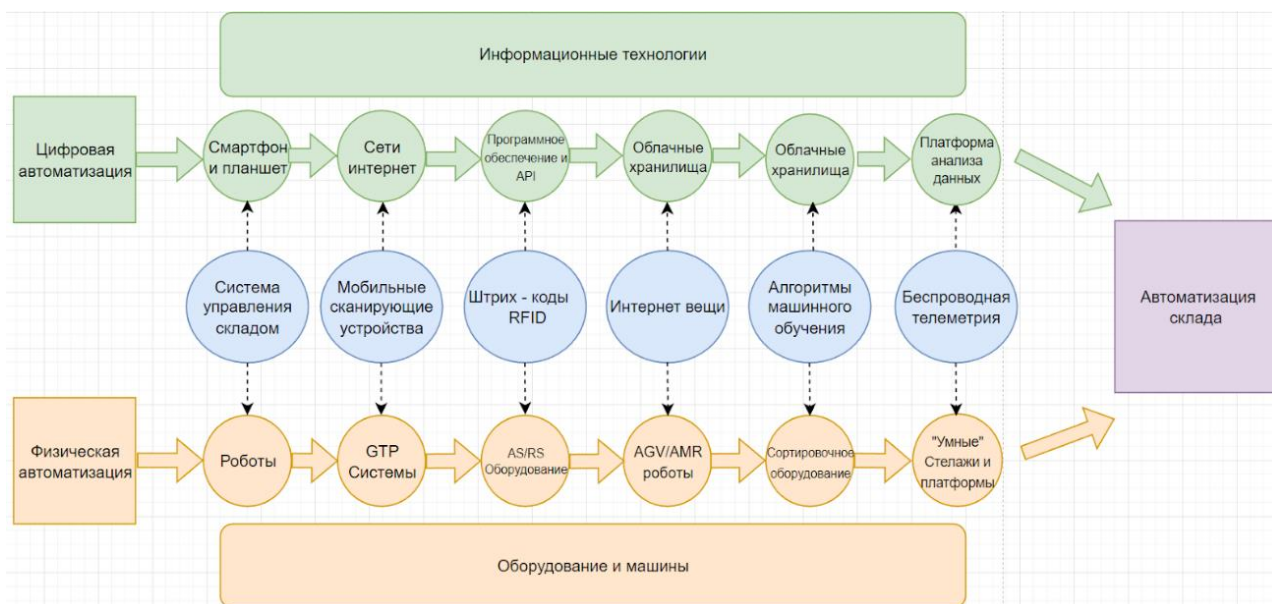


Рис. 1. Процессы автоматизации склада

Для внедрения технологии цифровой автоматизации требуются значительные предварительные инвестиции.

Физическая автоматизация – это способ использования технологий для минимизации трудозатрат сотрудников. К преимуществам физической автоматизации относятся повышение эффективности склада, надежность, масштабируемость и повышение производства.

Технологии автоматизации склада можно классифицировать на несколько категорий:

1. Базовая автоматизация склада: этот тип автоматизации относится к простой технологии, которая помогает людям с задачами, которые в противном случае потребовали бы больше ручного труда. Например, конвейер или карусель перемещает запасы из точки А в точку Б.

2. Автоматизация складской системы: этот тип системы использует программное обеспечение, машинное обучение, робототехнику и анализ данных для автоматизации задач и процедур. Например, система управления складом просматривает все заказы, которые необходимо выполнить в течение дня, и предлагает пользователям выбирать одинаковые товары для выполнения всех этих заказов одновременно, чтобы им не приходилось несколько раз перемещаться по складу туда и обратно.

3. Автоматизация механизированного склада: в этом виде автоматизации склада используется роботизированное оборудование и системы, помогающие людям выполнять складские задачи и процедуры. Одним из примеров являются автономные мобильные роботы-загрузчики полок, которые поднимают стеллажи с продуктами и доставляют их сборщикам для извлечения и сортировки.

4. Усовершенствованная автоматизация склада. Усовершенствованная автоматизация склада сочетает в себе механизированную складскую робототехнику и системы автоматизации, которые могут заменить трудоемкие рабочие процессы, выполняемые человеком. Например, парк роботизированных

вилочных погрузчиков, который использует передовой искусственный интеллект, камеры и датчики для навигации по складу и передачи местоположения каждого вилочного погрузчика на онлайн-портал отслеживания.

Рассмотрим один из способов физической автоматизации – внедрение роботизации в логистические маршруты склада. Внедрение на склад роботов дает такие преимущества как [3]:

- Повышение производительности работы склада.
- Экономия площади склада за счет размеров современных роботов.
- Снижение количества ошибок из-за человеческого фактора.
- Быстрая реализация, введение роботов в рабочий процесс длится примерно от 5 до 7 недель в зависимости от специфики операций.
 - Существует несколько видов роботов:
 - Autonomous Mobile Robot (AMR);
 - Automated Guided Vehicle (AGV);
 - Automated Storage/Retrieval System (AS/RS).

AMR – это робот с естественной навигацией, способный изменять свой маршрут при возникновении препятствий. Естественная навигация означает, что робот наносит на карту окружающий его ландшафт, позволяющий при перемещении локализовать себя, сканируя окружающую среду. Это технология называется SLAM (Simultaneous Localization and Mapping), когда с помощью датчиков LIDAR сканируется окружающая среда и заносится в карту робота [4].

AGV – робот, который перемещается по заданным путям. Это могут быть физические или виртуальные маршруты движения, внесенные в базу робота, магнитные ленты и отражатели. Эти роботы двигаются только по заданным маршрутам. Когда на пути робота датчики безопасности обнаруживают препятствие, AGV робот останавливается и ждет, пока препятствие не будет убрано. В таблице 1 приведены достоинства и недостатки двух таких систем [4].

AS/RS состоит из множества персональных компьютеров – контроллеров для автоматической загрузки и разгрузки грузов из определенных зон на складе. Система будет особенно полезна при повышенном грузопотоке или для хранения габаритных товаров. AS/RS использует максимум пространства для складирования различных товаров путем увеличения стеллажной площади и уменьшения внутрискладских проходов. Похожая система в логистике грузов используется в Московском аэропорту «Шереметьево».

По данным статистического агентства «Statista» количество роботизированных складов с каждым годом только увеличивается. Лидерами в этой области являются Япония (17%), Южная Корея (15%) и Китай (14%).

ТАБЛИЦА 1. Достоинства и недостатки систем автоматизации

Критерии сравнения	AGV	AMR
Навигация	Движение по проводам, светоотражающие маркеры, радиочастотная идентификация, магнитная лента, лазерное наведение	Естественная навигация, все измерения выполняются внутри робота
Препятствия	Останавливает до удаления препятствия	Выстраивает новый маршрут в объезд препятствия
Гибкость	Трудности в добавлении новых меток маршрута	Быстрое перепрограммирования на новые цели и задачи
Стоимость	20 000 долларов США (с магнитной навигацией)	40 000 долларов США (с навигацией SLAM)
Стоимость установки и ввода в эксплуатацию	Требует больше времени для создания инфраструктуры (магнитные ленты)	Быстрый ввод в эксплуатацию
Надежность	Следуют по заранее заданным путям движения	Более чувствительны к изменениям окружающей среды. Потеря позиции в пространстве
Стандарты	B56.5-2019 in US / ISO 3691-4:2020 in UE	ANSI/RIA R15.08-1-2020

К сожалению, в России показатель роботизации по всей стране всего 4%. Это связано с тем, что в передовых в области автоматизации странах экономическая эффективность подобных вложений обеспечивается льготами в налогообложении и экономией на оплате труда. В России оба параметра существенно ниже, что делает автоматизацию значительной части складских процессов пока экономически невыгодной [5].

Таким образом, в работе проведена классификация систем автоматизации логистических центров, дан сравнительный анализ систем роботизации складов, а также прогноз направлений развития складских систем роботизации.

Список используемых источников:

1. Федорян. А. В. Категорирование складских и производственных объектов, требования к объемно-планировочным и конструктивным решениям объектов: учебное пособие / А. В. Федорян, - издательство «Директ – медиа», 2020. – 222с.
2. Волгин В.В Склад: логистика, управление, анализ / В. В. Волгин, - издательство «Дашков и К», 2012 – 880 с.
3. Интегрированные логистические системы доставки ресурсов: (теория, методология, организация) / И. А. Еловой, И. А. Лебедева. – Минск: Право и экономика, 2011. –460 с.
4. Дом роботов AGV и AMR – Технология [Электронный ресурс]. URL: <https://www.agvnetwork.com/what-is-automated-guided-vehicle-agv-robot>
5. Камазинская Е. Время роботов еще нее пришло / Е. Камазинская // Склады и логистика. – 2018 – №12. – С. 37-41.

Litvinov V., Yashin A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunications

Research of methods for logistics centers automation.

The relevance of the article is due to the development of logistics technologies and the desire to reduce labor costs through the introduction of automation tools. The creation of new business models has pushed companies to search for innovative technological solutions to maintain competitiveness. This leads to the emergence of autonomous and mobile robots at logistics centers.

Key words: automation, logistics, warehouses, high technology, robotics.

УДК 004.087.2
ГРНТИ 20.53.17

СРАВНЕНИЕ СТРУКТУР СИСТЕМ ХРАНЕНИЯ ДАННЫХ, ИСПОЛЬЗУЮЩИХ ТВЕРДОТЕЛЬНЫЕ НАКОПИТЕЛИ

Р. Д. Мендус

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассмотрены структуры построения систем хранения данных с использованием твердотельных накопителей, а также различия между этими структурами. Из таких структур построения выделяется несколько, а именно: all-flash и гибридные. На основе данного выбора происходит сравнительный анализ этих структур, а также сравнение накопителей, используемых в этих структурах для построения систем хранения данных.

СХД, all-flash СХД, гибридные СХД, твердотельные накопители, Системы Хранения Данных

Развитие IT сферы в последние десять лет привело к тому, что все большее и большее значение в системах хранения данных приобретает такой показатель, как скорость работы с данными. За это время параметры доступности и надежности, накопителей, использующих флеш память, увеличилась, а затраты на их покупку снизились [1]. Это позволило данным накопителям найти свое место в системах хранения данных. Выделяют два типа систем хранения данных с использованием накопителей на флеш памяти:

All-flash – это системы хранения данных, построенные полностью на флеш памяти.

Гибридные – это системы хранения данных, совмещающие как накопители с флеш памятью, так и накопители, основанные на принципе магнитной записи.

Все это приводит к тому, что перед инженерами и разработчиками систем хранения данных стоят не простые задачи по выбору структуры построения таких систем, а, следовательно, и по выбору накопителей для этих систем. В статье проведен анализ накопителей и структуры построения систем хранения данных с целью выявления наилучшего решения.

Прежде чем выбрать перейти к анализу структур построения систем хранения данных, необходимо провести сравнение накопителей, используемых в all-flash и гибридных системах. В подобных системах могут использоваться накопители [2], представленные в таблице 1.

ТАБЛИЦА 1. Описание накопителей

Тип накопителя	Интерфейсы	Тип памяти	СХД
HDD	SATA, SAS	жесткий магнитный диск	гибридные
SSHD	SATA	гибридный	гибридные
SSD	SATA, PCIe	флеш память	all-flash, гибридные

Так как одной из важных характеристик для систем хранения данных является скорость работы с данными, то для сравнения накопителей воспользуемся показателем IOPS (Input/Output Operations Per Second), представленным в таблице 2 [3]. IOPS это количество блоков, которое успевает считаться или записаться на носитель в секунду. Чем выше данный параметр, тем с большим количеством блок может работать накопитель.

ТАБЛИЦА 2. Сравнение накопителей по IOPS

Устройство	Тип	IOPS	Интерфейс
7,200 об/мин SATA-диски	HDD	~75-100 IOPS	SATA 3 Гбит/с
10,000 об/мин SATA-диски	HDD	~125-150 IOPS	SATA 3 Гбит/с
10,000 об/мин SAS-диски	HDD	~140 IOPS	SAS
15,000 об/мин SAS-диски	HDD	~175-210 IOPS	SAS
SSHD	SSHD	~330-350 IOPS	SATA 3 Гбит/с
SSD SATA	SSD	~8 600 IOPS	SATA 3 Гбит/с
SSD SATA	SSD	~60 000 IOPS	SATA 6 Гбит/с
SSD NVMe	SSD	~200 000 IOPS	M2
SSD PCIe	SSD	~1 400 000 IOPS	PCIe

Как видно из таблицы 2, наибольшими показателями обладают SSD накопители. Также следует отметить, что использование данных накопителей снижает потребление электроэнергии на 60 % по сравнению с накопителями, использующими принцип магнитной записи [4].

Преимуществами SSD является скорость работы с данными и энергоэффективность. Однако существуют и другие характеристики систем хранения данных. Одной из таких следует выделить показатель доступности. Чтобы сравнить показатели доступности различных структур построения систем хранения данных, необходимо воспользоваться показателем A_{op} (operational availability of the system), представленным в формуле 1 [5]. Данный показатель отражает бесперебойность работы системы.

$$A_{op} = \frac{MTBF}{MTBF+MTTR}, \quad (1)$$

где MTBF (Mean Time Between Failure) – среднее время наработки между отказами системы, MTTR (Mean Time To Repair) – среднее время на восстановление работоспособности системы.

Как видно из формулы 1, для оценки показателя доступности необходимо определить характеристики MTBF и MTTR. Оценивание хаактеристики MTBF произведено в [6] и спецификации «NVMe Cloud SSD Specification» [7]. Для оценивания характеристики MTTR необходимо воспользоваться формулой 2 [8].

$$MTTR_{disk} = T_{DIAG} + T_{REP} + T_{RBLD}, \quad (2)$$

где T_{DIAG} – время, необходимое для обнаружения неисправного диска; T_{REP} – время затраченное на ремонт/замену неисправного диска; T_{RBLD} – время, необходимое для восстановления потерянных данных на замененном диске.

Если взять в расчет наличие диска, используемого в «горячем» резерве, то характеристики T_{DIAG} и T_{REP} можно не учитывать в формуле 2, то есть приравнять их величину равной 0. Следовательно, формула измениться и будет иметь следующий вид:

$$MTTR_{disk} = T_{RBLD} = \frac{C_{vol}}{P_{disc}}, \quad (3)$$

где C_{vol} – размер тома, P_{disc} – скорость чтения данных с диска.

Для вычислений характеристик примем размер тома за 500гб. Данные о скорости чтения, представленные в таблице 3, берутся из спецификации оборудования.

ТАБЛИЦА 3. Показатели различных накопителей

Тип накопителя	Скорость чтения
SSHД	156 Мбайт/сек
HDD	125 Мбайт/сек
SSD	500 Мбайт/сек

Таким образом, получается определение времени восстановления для разных типов накопителей согласно формулам 4-6. Для вычисления характеристики MTTR для гибридной СХД на SSD и HDD накопителей находится среднее время.

$$MTTR_{SSD} = \frac{500 \cdot 1024}{500} = 1024 \text{ сек}, \quad (4)$$

$$MTTR_{SSHД} = \frac{500 \cdot 1024}{156} = 3282,1 \text{ сек}, \quad (5)$$

$$MTTR_{SSD+HDD} = \frac{\left(\frac{500 \cdot 1024}{500} + \frac{500 \cdot 1024}{125}\right)}{2} = \frac{(1024 + 4096)}{2} = 2560 \text{ сек}. \quad (6)$$

Данные для оценивания показателя доступности приведены в таблице 4, а само вычисление проводится по формулам 7-9.

ТАБЛИЦА 4. Показатели доступности для разных СХД

Тип СХД	Типы накопителей	MTBF	MTTR
Гибридная	SSHД	1500000 сек	3282,1 сек
Гибридная	SSD, HDD	2000000 сек	2560 сек
All-flash	SSD	2500000 сек	1024 сек

$$A_{op(SSHD)} = \frac{1500000\text{сек}}{1500000\text{сек}+3282,1\text{сек}} = 0,997817 \quad , \quad (7)$$

$$A_{op(SSD+HDD)} = \frac{2000000\text{сек}}{2000000\text{сек}+2560\text{сек}} = 0,998716 \quad , \quad (8)$$

$$A_{op(SSD)} = \frac{2500000\text{сек}}{2500000\text{сек}+1024\text{сек}} = 0,999591 \quad . \quad (9)$$

Таким образом видно, что наибольший параметр доступности у систем хранения данных, построенных по структуре all-flash. Следовательно, данная структура предпочтительна при построении систем хранения данных.

Список используемых источников:

1. Белова Елена Юрьевна. Обзор систем хранения данных на флеш-накопителях // Известия СПбГЭТУ «ЛЭТИ» 2017 N 9. С. 27–28.
2. Шарапов Руслан Владимирович. Аппаратные средства хранения больших объемов данных. // Инженерный вестник Дона. 2012. N 4-2. С. 67.
3. IOPS — что это такое, и как его считать. [Электронный ресурс]. URL: <https://habr.com/ru/post/164325/>.
4. Intel and KIO Networks Case Study. С. 3. [Электронный ресурс] URL: https://www.intel.com/content/dam/www/public/us/en/documents/case-studies/intel-and-kio-networks-case-study.pdf?roistat_visit=72733.
5. Fausto Vaninetti, EMEAR Consultant Systems Engineer, Datacenter Technologies. Design a Reliable and Highly Available Fibre Channel SAN // Cisco 2017. С. 42 -49.
6. Bianca Schroeder Garth A. Gibson. Disk failures in the real world: What does an MTTF of 1,000,000 hours mean to you? // Conference on File and Storage Technologies, San Jose, CA, Feb. 14-16 2007. С. 1.
7. Ross Stenfort, Ta-Yu Wu, Lee Prewitt .NVMe Cloud SSD Specification С. 39-40
8. Игорь Афонин. Надёжность избыточных дисковых массивов. [Электронный ресурс] URL: <https://www.cta.ru/articles/spravochnik/v-zapisnuyu-knizhku-inzhenera/124353/>.

Mendus R.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Structure comparison of data storage systems using solid state drives.

This article discusses methods for building storage systems using solid state drives, as well as distinguishing between these methods. Several of these construction methods stand out, namely: all-flash and hybrid. Based on this choice, a comparative analysis of these methods is carried out as well as a comparison of the drives used in these methods to build data storage systems.

Key words: *data storage systems, all-flash storage, hybrid storage, solid-state drives.*

УДК 004.42
ГРНТИ 50.41.17

ОПТИМИЗАЦИЯ ЖИЗНЕННОГО ЦИКЛА РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПУТЁМ ВНЕДРЕНИЯ GITOPS ПРАКТИК

Г. А. Михаль, Г. Н. Смородин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Внедрение современных практик непрерывного развёртывания является одним из актуальных направлений оптимизации жизненного цикла программных систем. Технологический подход «инфраструктура как код» стал одним из самых значимых открытий в развитии данного направления, который привел к появлению методологии DevOps. Однако обновление динамической системы в соответствии с изменившимся состоянием статического репозитория оставалось «узким местом», требовавшим «ручного» воздействия. Технология GitOps позволила внести элементы автоматизации в процесс изменения состояния динамической системы и способствовать повышению объективности в реализации одной из важнейших составляющих жизненного цикла программных систем.

жизненный цикл, программное обеспечение, gitops, devops, git, web приложения

GitOps - это набор практик, которые используются для непрерывного развертывания программного обеспечения. Эти практики ориентированы на разработчиков, и для управления инфраструктурой используется удобный для разработчиков инструмент, такой как Git. Git - это единственный источник истины для всей автоматизации развертывания инфраструктуры и приложений.

GitOps состоит из трех основных компонентов [1]. Это комбинация инфраструктуры как кода (IaC), запросов на слияние и автоматизации CI/CD.

Для минимальной реализации непрерывной доставки программного обеспечения необходимы следующие технологии:

1. Git - Распределённая система управления версиями;
2. Docker - Программное обеспечение для автоматизации развёртывания и управления приложениями в средах с поддержкой контейнеризации;
3. Docker Registry – Хранилище Docker образов;
4. Kubernetes - Открытое программное обеспечение для оркестровки контейнеризированных приложений - автоматизации их развёртывания, масштабирования и координации в условиях кластера.
5. Werf (GitOps оператор) - это CLI-утилита, организующая полный цикл доставки приложения в Kubernetes.

В GitOps все начинается с Git-репозитория. В нем есть YAML-файлы, описывающие желаемое состояние Kubernetes. Вместе они формируют некоторое простое приложение, которое располагается в кластере Kubernetes.

Также важной частью системы является GitOps-оператор, отвечающий за синхронизацию состояния из Git в Kubernetes. Для этого он периодически (или по событию, которое может быть запущено, например, через webhook):

- считывает состояние из Git,
- считывает состояние из Kubernetes,
- сравнивает их,
- меняет состояние Kubernetes (если это необходимо).

Схема GitOps отображена на рис. 1.

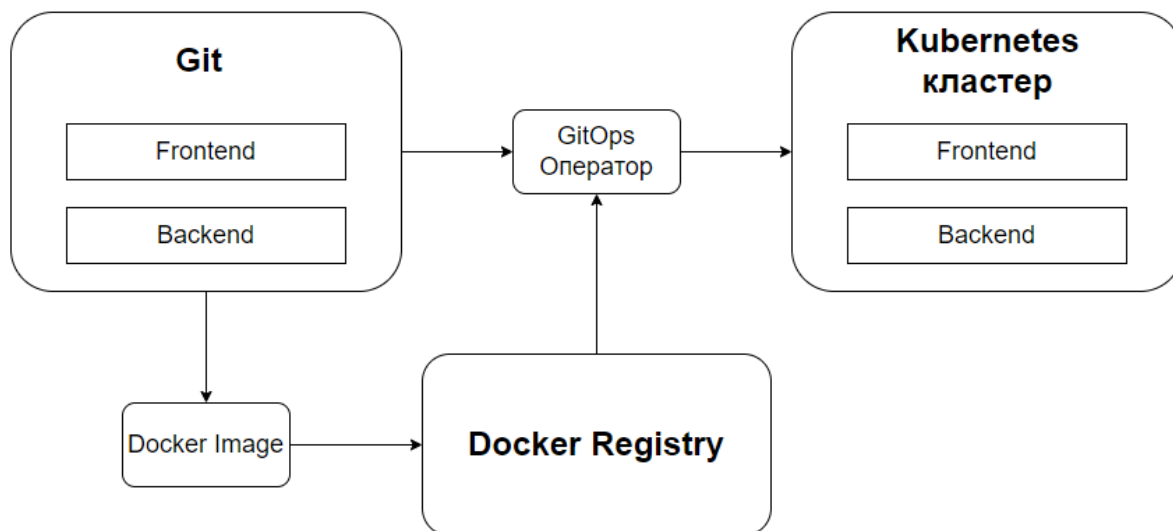


Рис. 1. Схема GitOps

Процесс работы в GitOps выглядит следующим образом [2]:

1. Разработчик делает запрос на слияние с новой функцией;
2. Код проверяется и одобряется, сливается с кодовой базой;
3. Слияние активирует конвейер CI/CD, автоматически собирающий, тестирующий и выкатывающий код в registry;
4. Программный агент получает уведомление об обновлении, скачивает новый код из registry и обновляет файл настроек (написанный на YAML) в репозитории настроек;
5. Программный агент в кластере Kubernetes определяет, основываясь на файле настроек, что его настройки устарели, скачивает изменения и выкатывает новую функцию.

Детализированная схема данного процесса изображена на рис. 2.



Рис. 2. Процесс работы в GitOps

GitOps предоставляет только одну точку для изменений, которой является сам Git. Данная особенность отображена на рис. 3.

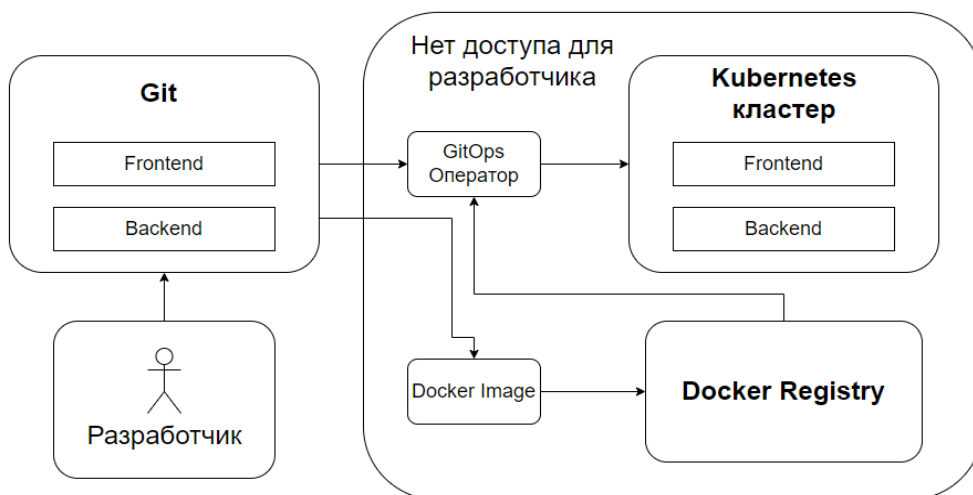


Рис. 3. Область доступа разработчика в GitOps

GitOps имеет следующие преимущества [3]:

1. Автоматизация - Разработчик не производит вручную ни какие-либо правки в Kubernetes, ни синхронизацию состояния из Git. Для последнего есть GitOps-оператор, который отвечает за синхронизацию, выполняя ее полностью автоматически;

2. Конвергентность - Система стремится прийти в желаемое состояние и, даже если время от времени происходит рассинхронизация, сама возвращается обратно в требуемое, синхронизированное состояние;

3. Идемпотентность - Если мы повторим синхронизацию несколько раз, результат первой синхронизации не повлияет на результат второй, они оба не повлияют на третью, и так далее;

4. Детерминизм - Состояние в Kubernetes целиком и полностью определяется тем, что написано в Git;

5. Наблюдаемость - В любой момент времени производится мониторинг состояния системы;

6. Безопасность – Рядовой разработчик не имеет доступа к кластеру Kubernetes. Есть возможность ограничить доступ к слиянию с основными ветками определённым разработчикам.

Таким образом можно считать, что применение современных практик непрерывного развёртывания, в том числе GitOps является одним из актуальных направлений оптимизации жизненного цикла программных систем. Технология GitOps привносит элементы автоматизации в процесс изменения состояния динамической системы и способствует повышению объективности в реализации одной из важнейших составляющих жизненного цикла программных систем.

Список используемых источников:

1. Что такое GitOps? Расширяем Devops на Kubernetes и далее [Электронный ресурс] – URL: <https://itnan.ru/post.php?c=1&p=525462> (дата обращения 08.11.2022).
2. Мартин Р. Чистый Agile — Питер, 2022 – 270 с.: ил.
3. Джин К. Проект "Феникс". Как DevOps устраняет хаос и ускоряет развитие компании — Бомбора, 2022 – 384 с.: ил.

Mikhail G., Smorodin G.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Optimization of the software development life cycle through the implementation of GitOps practices.

The introduction of modern practices of continuous deployment is one of the relevant areas of optimization of the life cycle of software systems. The technological approach "infrastructure as code" has become one of the most significant discoveries in the development of this direction, which led to the emergence of the DevOps methodology. However, updating the dynamic system to reflect the changed state of the static repository remained a bottleneck that required "manual" action. GitOps technology made it possible to introduce elements of automation into the process of changing the state of a dynamic system and contribute to increasing objectivity in the implementation of one of the most important components of the life cycle of software systems.

Key words: *lifecycle, software, gitops, devops, git, web applications.*

УДК 004.832.22
ГРНТИ 20.53.19

РАЗРАБОТКА СИСТЕМЫ НОРМАЛИЗАЦИИ ДАННЫХ ДЛЯ ОБУЧЕНИЯ АЛГОРИТМОВ КОМПЬЮТЕРНОГО ЗРЕНИЯ

А. А. Панченко, А. С. Попонин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В повседневной жизни людям приходится оцифровывать документы путем фотографирования их на камеры мобильных устройств. Однако такие изображения чаще всего страдают плохим качеством читабельности из-за перспективных, геометрических искажений изображения. Такой недостаток в дальнейшем негативно сказывается на работу алгоритмов распознавания текста и объектов документа.

компьютерное зрение, обработка данных, нормализация данных, нейронная сеть

В настоящее время с развитием технологий машинного обучения задачи компьютерного зрения становятся особенно актуальными. Данная технология уже применяется в таких областях как видеонаблюдение, медицина, беспилотное управление, производство.

В повседневной жизни людям приходится оцифровывать документы путем фотографирования их на камеры мобильных устройств. Однако такие изображения чаще всего страдают плохим качеством читабельности из-за перспективных, геометрических искажений изображения. Такой недостаток в дальнейшем негативно сказывается на работу алгоритмов распознавания текста и объектов документа. В данной статье описана методика, которая позволяет нормализовать фотографии документов для дальнейшего обучения алгоритмов компьютерного зрения.

Для начала необходимо определить местоположение документа на фотографии. Существует метод определения контура объекта, который основан на получении двухуровневого изображения в градациях серого. На таком изображении более точно можно определить контуры объектов. Однако если фотография сделана при плохом освещении или на заднем фоне есть много сторонних объектов, то данный метод работает некорректно. Поэтому было принято решение обучить модель COCO Instance Segmentation Baselines / Mask R-CNN R50-FPN 3X [1] определять документ на фотографии.

Для того, чтобы получить модель, способную правильно детектировать документ, необходимо внимательно подойти к данным. Важнейшим критерием качественных данных в данном случае являются большое разнообразие вариаций перспективных искажений документов на плоскости и широкий выбор заднего фона. С этой целью был разработан генератор случайных искажений, основанный на изменении координат угловых точек листа. Были также учтены возможности того, что некоторые углы документа могут быть обрезаны границами всего изображения.

Для обучения модели сгенерированные данные необходимо было правильно разметить. В данном случае самой главной информацией об объекте является его сегментация. Под сегментацией подразумевается разбиение изображения на области, соответствующие различным объектам. Так как детектировать необходимо всего лишь один документ, то задача разметки сводится к определению сегментации одного объекта, как показано на рис. 1.

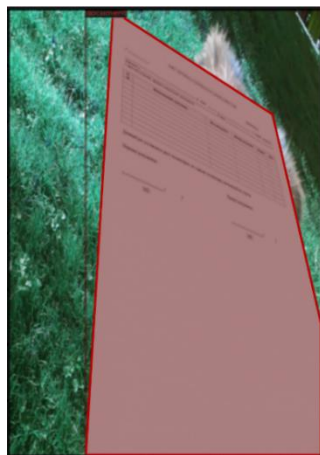


Рис. 1. Демонстрация работы алгоритма определения сегментации

В сегментации не должно быть точек, выходящих за пределы всего изображения. По этой причине некоторые координаты необходимо преобразовывать в набор точек, идущих по границе изображения как показано на рис. 2. Данный алгоритм был реализован на основе нахождения точек пересечения границ документа с границами изображения.

После обучения модели тестирование проводилось на реальных данных. Был собран небольшой набор тестовых документов, сфотографированных на камеру смартфона под разными углами.

Модель корректно срабатывает на геометрически искаженные документы. Согласно результатам, представленным на рис. 2 и 3, можно сделать вывод о том, что модель не реагирует на задний фон и определяет сегментацию объекта по границам изображения в случае, если углы документа выходят за пределы.

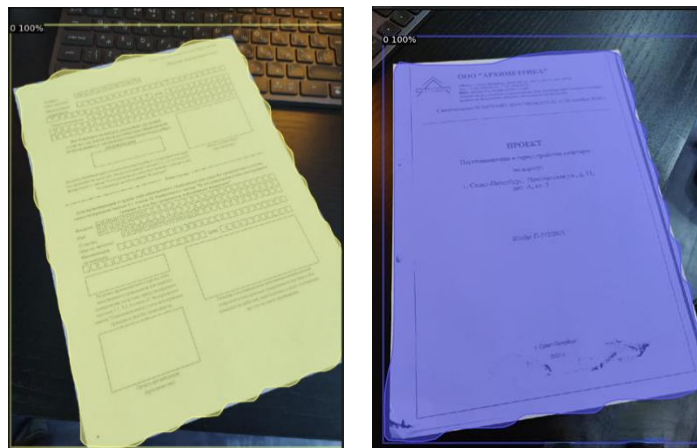


Рис. 2, 3. Демонстрация работы обученной модели на реальных данных

После того как модель определила местоположение документа, необходимо выпрямить границы сегментации с целью определения 4 угловых точек листа. Контурная аппроксимация, использующая алгоритм Рамера-Дугласа-Пекера, направлена на упрощение кривой линии за счет уменьшения количества ее вершин при заданном пороговом значении [2]. По алгоритму, учитывающему начальную и конечную точку кривой, определяется вершина на максимальном расстоянии от линии, соединяющая две опорные точки. Если точка максимума находится на расстоянии меньше порогового значения, алгоритм пренебрегает всеми вершинами между начальной и конечной точками и делает кривую прямой. Пример работы алгоритма РДП приведен на рис. 4.



Рис. 4. Пример работы алгоритма РДП

В результате работы алгоритма аппроксимации были получены ровные границы сегментации. Рис. 5 показывает, что некоторые углы документа обрезаны границами изображения. Необходимо достроить сегментацию в этих углах с целью получения 4 угловых точек контура для дальнейшей трансформации документа. Алгоритм преобразования контура так же, как и при генерации, основан на нахождении точек пересечения, только в этом случае ищутся точки пересечения граней контура.

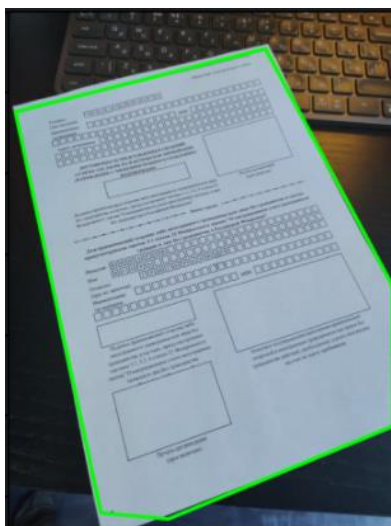


Рис. 5. Демонстрация работы алгоритма РДП

Если есть плоскость Π , которая проецируется из центра S на плоскость Π , то коллинеарным (перспективным) соответствием плоских полей называют

случай, когда каждой точке первой плоскости соответствует точка второй плоскости и наоборот [3]. Такое соответствие обладает следующими свойствами:

1. Соответствие взаимно однозначно;
2. Сохраняются свойства взаимной принадлежности точек и прямых;
3. Прямым линиям соответствуют прямые.

Перспективное преобразование не сохраняет параллельность, длину прямых и углы между ними, но сохраняет коллинеарность, то есть прямые линии останутся прямыми даже после преобразования.

Перспективное преобразование задается формулой 1:

$$x' \ y' \ w' = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} * \begin{bmatrix} x \\ y \\ w \end{bmatrix} \quad (1)$$

где (x', y') – преобразованные точки, (x, y) – входные точки, а $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$ является матрице перспективного преобразования. Разработанная методика и основана на расчете данной матрицы A .

Матрица преобразования определяется 8 константами. Чтобы найти эту матрицу необходимо определить 4 точки во входном изображении и сопоставить эти точки с желаемым местоположением в выходном изображении. Таким образом получается 8 уравнений с 8 неизвестными, которые возможно решить. После вычисления матрицы применяется перспективное преобразование ко всему входному изображению.

Для получения окончательного преобразованного изображения необходимо выровнять документ. Благодаря алгоритму преобразования Хафа можно найти прямые линии на изображении, чтобы высчитать угол наклона каждой из них относительно системы координат. На документе есть большое множество параллельных линий, поэтому если взять среднее значение элементов массива углов, то это значение и будет углом наклона всего документа.

В результате работы всего алгоритма нормализации изображения получается документ, готовый к дальнейшему анализу. Демонстрация результата работы алгоритма приведена на рис. 6 и 7.

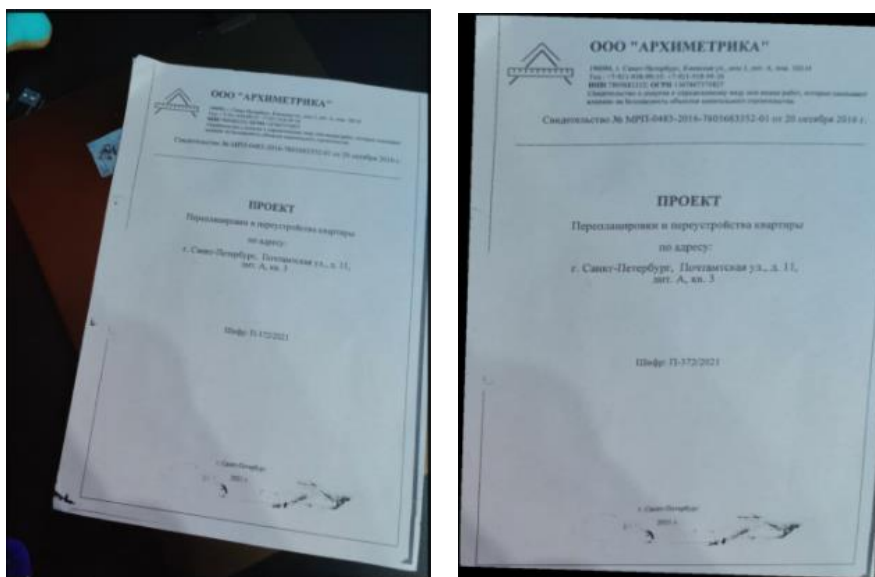


Рис. 6,7. Демонстрация работы алгоритма нормализации

Список используемых источников:

1. Mask R-CNN. [Электронный ресурс]. URL:<https://arxiv.org/pdf/1703.06870.pdf> (дата обращения 20.09.2022)
2. Ramer–Douglas–Peucker algorithm. [Электронный ресурс]. URL: <https://en.wikipedia.org/wiki/Ramer>
3. Галай В.А. Начертательная геометрия. Методология и методика. 2014. 224 с.

Panchenko A., Poponin A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Development of a data normalization system for training computer vision algorithms.

In everyday life, people must digitize documents by photographing them on mobile devices. However, such images most often suffer from poor readability due to perspective, geometric distortions of the image. Such a defect further negatively affects the performance of the algorithms for recognizing the test and the document objects.

Key words: computer vision, data processing, data normalization, neural network.

УДК 004.832.22
ГРНТИ 20.53.19

ПОВЫШЕНИЕ УПРАВЛЯЕМОСТИ ГЕНЕРАЦИИ РЕЧИ В АЛГОРИТМАХ ГЛУБОКОГО МАШИННОГО ОБУЧЕНИЯ В ОБЛАСТИ СИНТЕЗА РЕЧИ

А. С. Попонин, И. И. Триандафилиди,

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Последние достижения в области синтеза речи позволяют синтезировать в реальном времени все более естественно звучащую человеческую речь. Однако для достижения высокого уровня схожести, помимо инновационных нейронных архитектур, немаловажным аспектом является качественная предобработка обучающих данных. В данной работе описано, как с помощью детализации обобщений в данных добиться более качественного результата.

синтез речи, нейронные сети, TTS, обработка данных

В настоящее время стремительно растут и набирают популярность голосовые ассистенты. На рынке представлено много подобных систем. Самыми популярными решениями являются «Алиса» от *Yandex*, «Олег» от *Tinkoff*, «Маруся» от *Mail*, голосового телефонного ответчика от *Sber*.

Одним из необходимых элементов таких ассистентов является система синтеза речи, которая позволяет преобразовывать текст в речь (*Text to Speech, TTS*). Последние достижения в области синтеза речи позволяют синтезировать естественно звучащую человеческую речь в реальном времени. Вкупе с другими элементами, такими как *Automatic Speech Recognition, Dialogue system, Voice Active Detection* и др., которые так же способны отдавать ответы в режиме реального времени, голосовые ассистенты могут без особой задержки генерировать ответ на полученный запрос от пользователя.

Разработчики всех голосовых систем стремятся к максимальной схожести синтетической речи с речью человека. В данной статье описана методика, которая позволит повысить управляемость генерации речи на примере обучения модели *FastPitch* [1].

Для того чтобы получить качественную модель, способную генерировать схожую с человеческой речь, нужно внимательно подойти к данным. Самым важным критерием качественных данных служит полное соответствие текстовой транскрипции аудиофайла с фактическим текстом, произносимым в аудиофайле. Также стоит обратить внимание на качество самих аудиофайлов. В лучшем случае это должны быть аудиофайлы, записанные на профессиональной записывающей музыкальной студии. Если не удастся записать данные в профессиональной студии, то нужно обратить внимание на звучание голоса - он должен звучать одинаково на всех аудио образцах. Следует позаботиться и о текстовой транскрипции - в ней не должно быть лишних символов, числа должны быть прописаны текстом, так же рекомендуется ставить точку в конец. Пример данных представлен в таблице 1.

ТАБЛИЦА 1. Пример данных-1

<i>audio_file_with_text_1.wav</i>	<i>Hello world.</i>
<i>audio_file_with_text_2.wav</i>	<i>I am medical robot</i>
<i>audio_file_with_text_3.wav</i>	<i>My name is Alexa</i>

Одним из критериев схожести синтезированной речи с человеческой являются паузы. В обучающей выборке можно оставить литературные запятые, но они не всегда означают фактическую паузу в речи. Соответственно для усвоения паузы просто запятой или точки, если в образце два и более предложений, не хватит. Наша идея заключается в том, что мы должны проанализировать каждый аудиофайл на наличие фактических пауз.

После проведенного анализа аудиофайлов мы обнаружили, что фактические паузы в нашем аудио датасете варьируются по длительности. Разделив паузы по диапазонам:

- Короткая пауза - от 0 до 0.2 секунд
- Средняя пауза - от 0.2 од 0.4 секунд
- Длинная пауза - больше 0.4с

Мы получили следующее распределение (рис. 1):

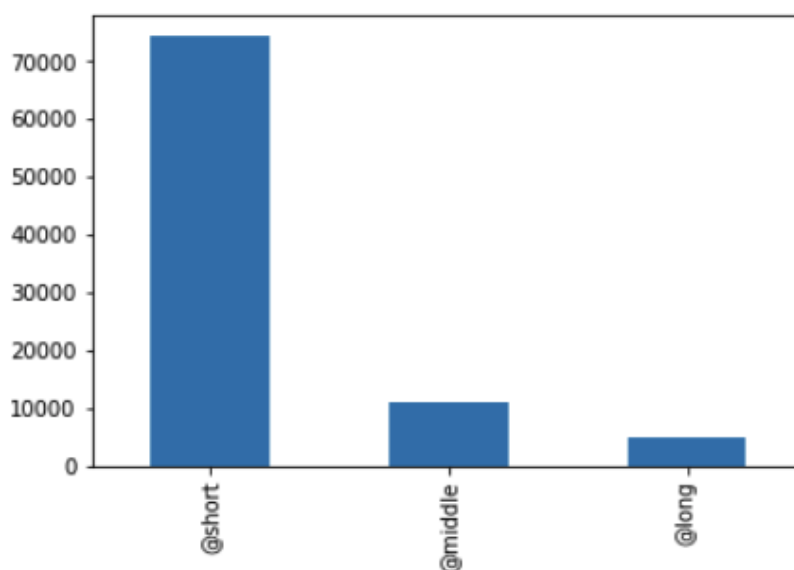


Рис 1. Распределение полученных длительностей пауз

Из распределения следует, что коротких пауз много больше, чем средних и длинных, соответственно было принято решение объединить все паузы в один токен-паузу и поставить этот токен в текст там, где фактически присутствует пауза в аудиофайле. Пример данных представлен в таблице 2.

ТАБЛИЦА 2. Пример данных-2

<i>audio_file_with_text_1.wav</i>	<i>{token-pause} Hello world {token-pause}</i>
<i>audio_file_with_text_2.wav</i>	<i>I am {token-pause} medical robot</i>
<i>audio_file_with_text_3.wav</i>	<i>My name is Alexa {token-pause}</i>

Для сравнения мы так же произвели обучения на чистом литературном тексте с запятыми. На рис. 2,3,4 и 5 представлены графики синтезированных аудиофайлов с текстом, который представлен в таблице 3.

ТАБЛИЦА 3. Текст к аудиофайлам

Рисунок 2	<i>But, what I want to talk to you, about now is a different information network</i>
Рисунок 3	<i>But {token-pause} what I want to talk to you {token-pause} about now is different information network</i>
Рисунок 4	<i>Hello friend, I am medical robot, I can help you</i>
Рисунок 5	<i>Hello friend {token-pause} I am medical robot {token-pause} I can help you</i>

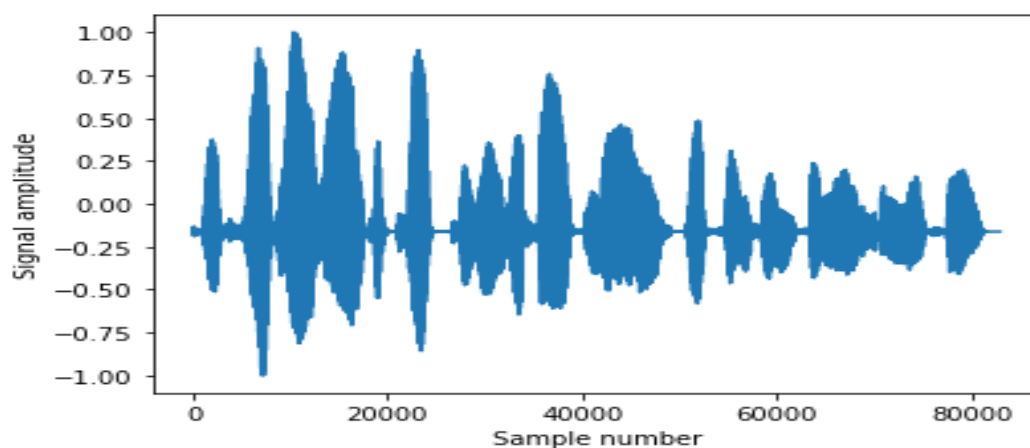


Рис. 2. Отображение амплитуд звука в аудио при использовании запятых.

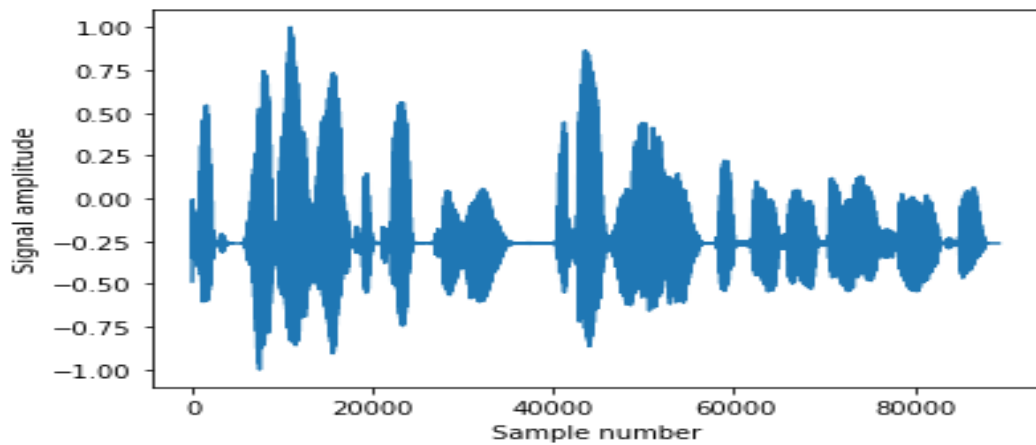


Рис. 3. Отображение амплитуд звука в аудио при использовании токена-пауз.

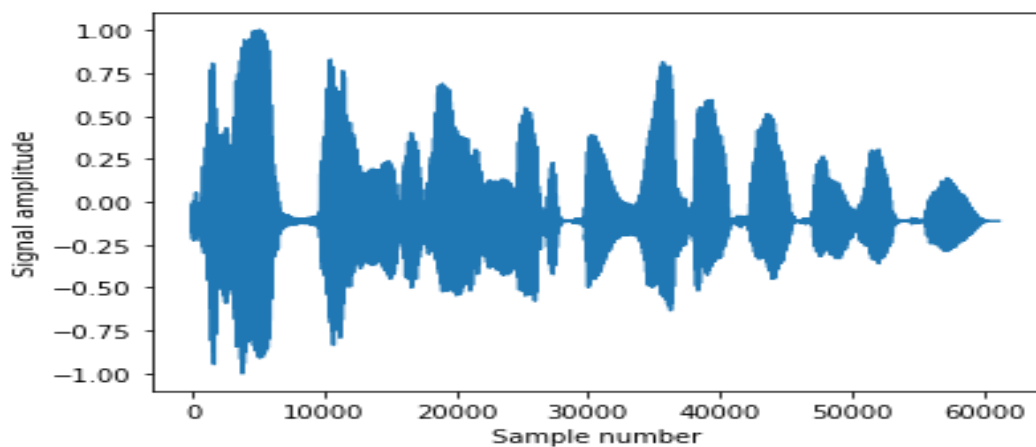


Рис. 4. Отображение амплитуд звука в аудио при использовании запятой.

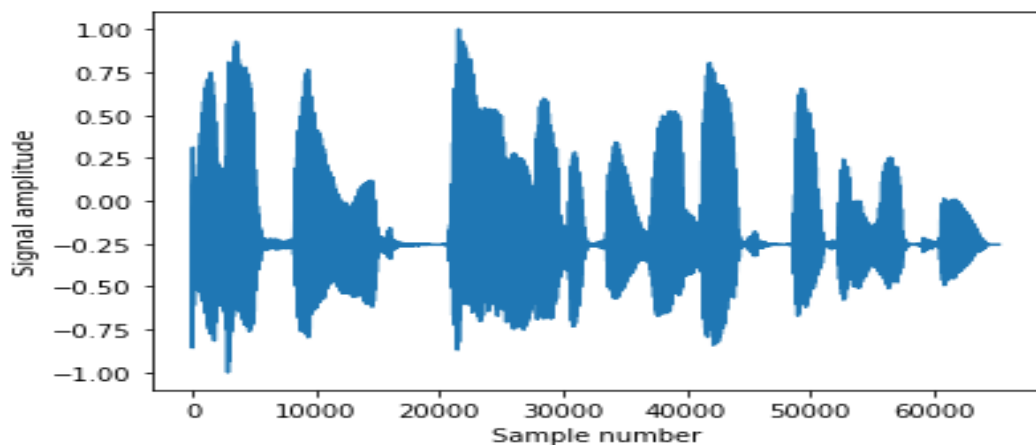


Рис. 5. Отображение амплитуд звука в аудио при использовании токена-пауз.

Посмотрев на графики, можно убедиться в том, что при использовании токена-паузы в сгенерированных аудиофайлах можно наблюдать более качественную паузу, имеющую большую длительность и меньшую

зашумленность, в то время, как в некоторых моментах запятые в целом не дают никакой паузы. Вследствие чего мы предлагаем использовать наш метод обработки входных аудиоданных, так как он позволяет нейронным моделям усвоить признаки пауз более точно, что позволит генерировать более естественно звучащую речь.

Список используемых источников:

1. FASTPITCH: PARALLEL TEXT-TO-SPEECH WITH PITCH PREDICTION [Электронный ресурс]. URL: <https://arxiv.org/pdf/2006.06873.pdf>.

Poponin A., Triandafilidi I.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Increasing the control of speech generation in deep machine learning algorithms in the field of speech synthesis.

Recent advances in the field of speech synthesis make it possible to synthesize in real time increasingly natural human speech. However, in order to achieve a high level of similarity, in addition to innovative neural architectures, an important aspect is the qualitative pre-processing of educational data. This paper describes how to achieve a better result by detailing generalizations in data.

Key words: speech synthesis, neural networks, TTS, data processing.

УДК 004.9
ГРНТИ 20.53.19

МЕТОД ФОРМАЛИЗАЦИИ ВИДЕОКОНТЕНТА В СРЕДЕ PYTHON

А. А. Складов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается метод формализации видеоконтента в среде Python при помощи библиотеки OpenCV на основе алгоритмов преобразования в пространстве представления видеоконтента в массив координат пикселей с цифровой обработкой данных.

искусственный интеллект, нейронные сети, медиазадачи, библиотеки Python

На сегодняшний день существует различное множество медиазадач. Одно из направлений – это проблемы моделирования и технологии макетирования в киноиндустрии. Например, кинооператор снимает сцену взрыва моста на модели в одну десятую натуральной величины. Как следует изменить частоту кадров при съемке, чтобы в кинофильме сцена выглядела правдоподобно? [1] Для решения данной проблемы, разработаны формулы и методы, но все они не автоматизированы должным образом, поэтому необходим метод вычисления автоматическим путем. Для этого предлагается использовать нейронные сети.

Нейронные сети – одна из популярнейших моделей машинного обучения. Направление в разработке систем искусственного интеллекта, заключающейся в воспроизведении работы человеческого мозга с помощью математических моделей. Нейронные сети получили свое название благодаря принципам работы математической модели, которая схожа с функционированием нервной системы человека. Каждый нейрон представляет собой ячейку, которая получает на вход определенное количество первоначальных данных и отдает на выход уже обработанные данные, а соединены эти ячейки так называемыми синопсисами. За формирование входящих сигналов в выходящий отвечает определенный алгоритм вычисления.

В данной статье рассматривается способ преобразования видеоконтента в массив координат пикселей, для дальнейшего решения необходимой медиазадачи. В качестве языка программирования выбран скриптовый язык Python по причине наличия большого количества библиотек при работе с машинным обучением и работы с изображениями [2]. В качестве основной библиотеки используется OpenCV. Также применяются некоторые возможности библиотек MoviePy, Pillow.

OpenCV – это набор типов данных, функций и классов для обработки изображений алгоритмами компьютерного зрения [4]. В основные модули библиотеки входит: `sxcore` — ядро, содержащее базовые структуры данных и алгоритмов; `CV` — модуль обработки изображений и компьютерного зрения; `Highgui` — модуль для ввода/вывода изображений и видео, создания пользовательского интерфейса, а также еще несколько модулей, которые в данной статье не будут задействованы.

Pillow это форк PIL (Python Image Library), которая появилась благодаря поддержке Алекса Кларка и других участников. Основана на коде PIL, а затем преобразилась в улучшенную, современную версию. Предоставляет поддержку при открытии, управлении и сохранении многих форматов изображения. Многие работает так же, как и в оригинальной PIL [5].

MoviePy – это библиотека Python для редактирования видео: нарезка, конкатенация, вставка заголовков, композитинг видео (он же нелинейный монтаж), обработка видео и создание пользовательских эффектов. Смотрите [галерею](#) для некоторых примеров использования. MoviePy может читать и записывать все наиболее распространенные аудио- и видеоформаты, включая GIF, и работает на Windows/Mac/Linux с Python 2.7+ и 3 (или только Python 3.4+ из версии 1.0). MoviePy зависит от модулей Python [Numpy](#), [imageio](#), [Decorator](#) и [tqdm](#) [6].

Важной деталью, для данного метода, является компьютерное зрение для обнаружения объектов. Обнаружение объектов с использованием каскадных классификаторов на основе признаков Хаара — это эффективный метод обнаружения объектов, предложенный Полом Виолой и Майклом Джонсом в их статье «Быстрое обнаружение объектов с использованием усиленного каскада простых признаков» в 2001 году. Это подход, основанный на машинном обучении, при котором каскадная функция обучается на множестве положительных и отрицательных изображений. Затем он используется для обнаружения объектов на других изображениях [7].

Обнаружение объектов в статье представлено в двух форматах: с помощью установки цветового порога и использовании каскадного классификатора. Для использования каскадного классификатора, необходимо перейти на официальный репозиторий [github OpenCV](#) и скачать классификатор, необходимый для условий интересующей задачи.

Видео состоят из огромного количества изображений, которые быстро переключаются между собой. По этой причине работа будет происходить с изображениями.

Первым шагом станет получение отдельных кадров из видео. Большинство видео записывается с частотой кадров равной 24 кадра в секунду [3]. Учитывая это, библиотека Python MoviePy или OpenCV позволяет установить количество сохраняемых кадров в секунду 10. Для примера, если видео, длительностью 30 секунд, преобразовать таким образом, то получим 300 кадров, для баланса точности и производительности. Важно отметить, если важна скорость выполнения, для данного шага следует использовать библиотеку OpenCV, но сохраняемые кадры будут большего размера. В свою очередь, библиотека MoviePy позволяет сохранять кадры в меньшем размере, но длительность выполнения в разы больше, чем при использовании OpenCV. Исходя из этого, использование библиотеки зависит от поставленных приоритетов.

Далее, с помощью библиотек OpenCV, Pillow или подобных, представляется возможным найти координаты каждого пикселя и записать его данные в массив. Для этого необходимо знать ширину и высоту изображения. Эту задачу

предлагается решить с помощью двух циклов `for` и функции `pixels()`, либо подобных в названных выше библиотеках.

В заключительном этапе предстоит при помощи компьютерного зрения отделить необходимые элементы ранее полученного массива. Процесс выглядит следующим образом. Изначально необходимо обнаружить цель. Для этого необходимо подготовить каскадный классификатор, либо установить цветовой порог. Далее следует создать пустую очередь, в которую центральная точка цели добавляется в очередь при обнаружении цели или сопровождении.

Обработывая каждый кадр и обнаруживая необходимый объект на предоставленном материале, необходимо выполнить следующие операции. В случае, если был выбран способ обнаружения через установку цветowego порога: перейти в пространство HSV; создать маску на основе порога; обработать эффект коррозии, а затем расширения, суть которых заключается в открытии операции расширения и устранении шума; обнаружить контур и инициализировать центр тяжести контура объекта; найти контур и определить описанную окружность контура с наибольшей площадью; вычислить центроид, и, заключительный этап, прослеживать точки слежения, записывая в массив координаты центральной точки обнаруженной цели.

Совместив полученные данные, другими словами, сравнивая последовательно изначальный массив пикселей целого изображения с массивами, полученные при обработке с помощью обнаружения, представляется возможным определить изменение местоположения объекта на видеоконтенте и использовать эти данные для последующего решения медиазадачи, требующей отслеживание одного объекта в пространстве представления.

В заключение можно сказать, что эффективность данного метода формализации видеоконтента на прямую зависит от уровня развития компьютерного зрения. Возможно, есть более рациональный метод решения данной задачи, так как на данный момент основным недостатком является то, что представленный метод работает только со статичным расположением камеры.

Также стоит отметить, если определение изменения местоположения объекта на видеоконтенте не достигло ожидаемого результата, следует вернуться к первому шагу и увеличивать количество сохраняемых кадров до того количества, пока не будет достигнута ожидаемая точность.

Список используемых источников:

1. Ходанович А.И. Методы математической физики.- СПб.: СПбГИКиТ, 2021, С 22.
2. Питон и машинное обучение: что поможет разработчику: [Электронный ресурс]. 2022. URL: <https://otus.ru/journal/piton-i-mashinnoe-obuchenie-cto-pomozhet-razrabotchiku/> (Дата обращения: 12.11.2022).
3. Научное объяснение — почему кино выглядит фальшиво с частотой 60 fps, но в играх чем выше частота, тем лучше: [Электронный ресурс]. 2020. URL: <https://shazoo.ru/2020/08/12/98030/nauchnoe-obyasnenie-pochemu-kino-vyglyadit-falshivo-s-chastotoj-60-fps-no-v-igrah-chem-vyshe-chastota-tem-luchshe/> (Дата обращения: 12.11.2022).
4. OpenCV шаг за шагом. Введение: [Электронный ресурс]. 2010. URL: <https://robocraft.ru/computervision/264>. (Дата обращения: 15.11.2022).

5. Основные возможности библиотеки Python Imaging Library / Pillow / PIL Classifier: [Электронный ресурс]. 2020. URL: <https://pythonru.com/biblioteki/osnovnye-vozmozhnosti-biblioteki-python-imaging-library-pillow-pil>. (Дата обращения: 15.11.2022).
6. Video editing with Python: [Электронный ресурс]. 2020. URL: <https://pyri.org/project/moviepy/>. (Дата обращения: 15.11.2022).
7. Cascade Classifier: [Электронный ресурс]. 2022. URL: https://docs.opencv.org/3.4/db/d28/tutorial_cascade_classifier.html. (Дата обращения: 15.11.2022).

Sklyarov A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Method for formalizing video content in the python environment.

The article discusses a method for formalizing video content in the Python environment using the OpenCV library based on algorithms for converting video content in the representation space into an array of pixel coordinates with digital data processing.

Key words: *artificial intelligence, neural networks, media tasks, Python libraries.*

УДК 004.7:004.422.8
ГРНТИ 20.01.07

ПРОГНОЗИРОВАНИЕ ДОСТИЖИМОСТИ ЦЕЛИ ПРИ ИСПОЛЬЗОВАНИИ КРУПНО-МАСШТАБНЫХ СЕРВИС- ОРИЕНТИРОВАННЫХ СИСТЕМ

А. С. Соловьев, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Показана объективная востребованность крупно-масштабных сервис-ориентированных систем. Рассмотрены ключевые принципы организации крупно-масштабных сервис-ориентированных систем. Выбраны показатели достижимости цели деятельности при использовании крупно-масштабных сервис-ориентированных систем. Выделены альтернативные подходы к прогнозированию достижимости цели. Предложено инновационное прогнозирование достижимости цели с помощью модельно-аналитического интеллекта. Представлены формализации для формирования подобного модельно-аналитического интеллекта.

прогнозирование, достижимость цели, сервис-ориентированная система, крупно-масштабность, модельно-аналитический интеллект

Интенсивным совершенствованием технологических платформ информационных инфраструктур в условиях развития цифровой экономики, высокой значимостью техногенных объектов в изменяющихся условиях жизнедеятельности и обусловленной ею расширяемостью их функциональных возможностей обуславливается востребованность крупно-масштабных сервис-ориентированных систем с контролируемой достижимостью цели.

Основа выделенной востребованности заключается в парадигме сервис-ориентированных архитектур, обеспечивающей высокую степень гибкости соответствующих сервис-ориентированных систем в сочетании с возможной автономностью выполняемых сервисов.

Процесс функционирования крупно-масштабных сервис-ориентированных систем классифицируется как одна из разновидностей крупно-гранулярных процессов [1].

Одной из многочисленных сфер, где предусматривается применение интеллектуальных крупно-масштабных сервис-ориентированных систем является транспортная отрасль [2].

При обеспечении информационной защищённости крупно-масштабных сервис-ориентированных систем появляются еще новые основания для возрастающей потребности в прогнозировании их достижимости цели [3].

Выделенное подобие процессов позволяет ориентироваться на профилирование достижимости цели через временные профили крупно-масштабных сервис-ориентированных систем, в основе которых фигурируют их динамические характеристики. Вариации в представлении динамических характеристик раскрываются в [1].

Благодаря предлагаемым приёмам проведения аналогий открываются обширные возможности подключения базовых компонентов методологии профилирования качества сервис-ориентированных систем, раскрываемых в [4,

5, 6, 7, 8], к прогнозированию достижимости цели при использовании крупномасштабных сервис-ориентированных систем.

При сочетании методов планирования действий и нейросетевых формализаций, раскрытым в [9], становится возможным преодолеть априорную неопределённость в знаниях относительно факторов, влияющих на достижимость цели.

В организации возможных подходов к прогнозированию достижимости цели при использовании крупномасштабных сервис-ориентированных систем цели могут различаться два варианта.

При первом варианте прогнозирование осуществляется лишь на этапе проектирования для выбора наилучшей архитектуры крупномасштабной сервис-ориентированной системы.

При втором варианте прогнозирование проводится при функционировании крупномасштабной сервис-ориентированной системы. В изменяющихся условиях жизнедеятельности становится очевидным предпочтительность второго функционального варианта.

В представляемом подходе к функциональному прогнозированию достижимости цели при использовании крупномасштабных сервис-ориентированных систем задача прогнозирования возлагается на распределённый модельно-аналитический интеллект, объединяющий модельно-аналитические интеллекты выполняемых и интегрируемых в систему сервисов и интегральный модельно-аналитический интеллект.

Для формирования распределённого модельно-аналитического интеллекта для прогнозирования достижимости цели при использовании крупномасштабных сервис-ориентированных систем разрабатывается методика построения их расширенных объектно-ориентированных моделей.

Вслед за построением новых расширенных объектно-ориентированных моделей предусматривается выбор базовых методов их анализа и вывод аналитических зависимостей для прогнозирования достижимости цели.

Предлагаемый подход к прогнозированию достижимости цели при использовании крупномасштабных сервис-ориентированных систем с модельно-аналитическим интеллектом и соответствующие методологические приемы его формирования расширяют методологический базис жизненного цикла крупномасштабных сервис-ориентированных систем для техногенных объектов.

Список используемых источников:

1. Птицына Л. К. Программное обеспечение компьютерных сетей. Управление крупно-гранулярными процессами на основе языка ВРЕL : учебное пособие / Л. К. Птицына, Н. Г. Смирнов. СПб. : Издательство Политехнического университета, 2011. 105 с.
2. Птицына Л. К., Медведев И. В., Нежинский В. В. Инновационные профили интеллектуальной мультимодальной транспортной системы // Информационные системы и технологии в моделировании и управлении : материалы II всерос. науч.-практ. конф., Ялта, 5 – 7 июня 2017 г. Ялта : ООО «Издательство Типография «Ариал», 2017. С. 69-73.
3. Птицына Л. К., Нежинский В. В. Инновации жизненного цикла защищённых сервис-ориентированных систем для цифровой экономики // Информационная безопасность регионов России-2017 : материалы X Санкт-Петербургской межрегион. конф., Санкт-Петербург, 1-3 нояб. 2017 г. СПб. : СПОИСУ, СПИИРАН, 2017. С. 526 – 528.
4. Птицына Л. К. Методология генерации модельно-аналитического интеллекта сервис-ориентированных систем с гарантиями качества // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VI Междунар. научно-технич. и

научно-методич. конф., Санкт-Петербург, 1-2 марта 2017 г. СПб. : СПбГУТ, 2017. Т. 3. С. 351 – 354.

5. Птицына Л. К., Птицын А. В. Интеллектуальное конфигурирование сервис-ориентированных систем // Информационные системы и технологии в моделировании и управлении : материалы IV Всерос. научно-практич. конф. с международным участием, Ялта, 21-23 мая 2019 г. Симферополь : ИТ «АРИАЛ», 2019. С. 48-51.

6. Птицына Л. К., Карачинская Е. А., Маргаритова Я. С. Расширенные объектно-ориентированные модели сервис-ориентированных систем для организации коммуникативных процессов контрагентов // Информационная безопасность регионов России : материалы XI Санкт-Петербургской межрегион. конф., Санкт-Петербург, 23-25 октября 2019 г. СПб. : СПОИСУ, 2019. С. 142-144.

7. Птицына Л. К., Эль Сабаяр Шевченко Н., Белов М. П., Птицын А. В. Математическое обеспечение мягких архитектур сервис-ориентированных систем в условиях неопределённости // Сборник докладов : материалы XXIV Междунар. конф. по мягким вычислениям и измерениям, Санкт-Петербург, 26 – 28 мая 2021 г. СПб. : СПбГЭТУ «ЛЭТИ». С. 121-124.

8. Птицына Л. К., Эль Сабаяр Шевченко Н., Птицын А.В. Моделирование коммуникационно-вычислительных процессов систем телекоммуникаций при сквозном объединении диаграмм состояний и диаграмм деятельности // Телекоммуникации. 2022. № 4. С. 32-40.

Solovyov A., Ptitsyna L.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Prognostication achievability of the goal when using large-scale service-oriented systems.

The objective demand for large-scale service-oriented systems is shown. The key principles of organizing large-scale service-oriented systems are considered. The indicators of the achievability of the goal of the activity when using large-scale service-oriented systems are selected. Alternative approaches to prognostication the attainability of the goal are highlighted. An innovative forecasting of the attainability of the goal with the help of model-analytical intelligence is proposed. Formalizations for the formation of such a model-analytical intelligence are presented.

Key words: *prognostication, goal attainability, service-oriented system, large scale, model-analytical intelligence.*

УДК 004.9
ГРНТИ 50.41.25

АНАЛИЗ ПОДХОДОВ К СОЗДАНИЮ РЕКОМЕНДАТЕЛЬНЫХ СИСТЕМ

П. А. Ягунов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Интернет — это цифровой рынок, который предоставляет множество вариантов, иногда слишком ошеломляющих, чтобы выбрать из них. Сегодня все может быть легко доступно благодаря этому цифровому рынку. От контента в сфере развлечений до продуктов и одежды — все предметы первой необходимости или предметы роскоши доступны в сети. В условиях множества доступных вариантов, всегда существовала серьезная потребность фильтровать, расставлять приоритеты и эффективно доставлять соответствующую информацию, чтобы преодолеть потенциальную проблему информационной перегрузки, создающую путаницу для многих пользователей Интернета. Рекомендательные системы могут помочь решить эту проблему, обрабатывая большой объем динамически генерируемой информации, чтобы предоставить пользователям персонализированный контент и услуги.

рекомендательные системы, нейронные сети, collaborative filtering, content based filtering

Широкое распространение для бизнеса в последнее десятилетие получили рекомендательные системы, основанные на машинном обучении [1]. Рекомендательные системы — это системы фильтрации информации, которые помогают решить проблему информационной перегрузки путем фильтрации и выделения фрагментов из больших объемов динамически генерируемой информации, в соответствии с предпочтениями, интересами или наблюдаемым поведением пользователя в отношении определенного элемента или элементов. Система рекомендаций имеет возможность предсказать, предпочтет ли конкретный пользователь какой-либо товар или нет, на основе профиля пользователя и его истории. Системы рекомендаций также доказали свою эффективность в улучшении процессов и качества принятия решений. В условиях электронной коммерции рекомендательные системы увеличивают доходы от маркетинга, поскольку они являются эффективным средством продажи большего количества продуктов. Следовательно, нельзя пренебрегать необходимостью использования эффективных и точных методов рекомендаций в системе, которая предоставляет релевантные и надежные рекомендации для пользователей.

Такие сервисы, как *Netflix*, используют механизм рекомендаций, чтобы предлагать своим зрителям фильмы и шоу, а *Amazon* использует свой механизм рекомендаций, чтобы предлагать клиентам рекомендации по продуктам. Хотя каждый из них использует эти алгоритмы для немного разных целей, оба в целом преследуют одну и ту же цель: стимулировать продажи, повышать вовлеченность и удержание клиентов, а также предоставлять более

персонализированный клиентский опыт. Рекомендации обычно ускоряют поиск и облегчают пользователям доступ к контенту, который им всегда был интересен, и удивляют их предложениями, которые они никогда бы сами не искали. Ведущие компании могут привлекать новых клиентов, рассылая персонализированные электронные письма со ссылками на новые предложения, отвечающие интересам получателей, или предложениями фильмов и телешоу, которые соответствуют их конкретным профилям.

В течение ряда лет рекомендательные системы больше фокусировались на пользователе, чем на товаре. Идея заключалась в том, что следует относиться к каждому пользователю как к уникальному, и не пытаться использовать историю одного пользователя для создания рекомендаций другому пользователю. Однако на данный момент наиболее популярными алгоритмами являются совместная (коллаборативная) фильтрация (*collaborative filtering*) и фильтрация на основе контента (*content based filtering*).

Метод совместной фильтрации — это метод, основанный исключительно на прошлых взаимодействиях, которые были записаны между пользователями и элементами, для создания новых рекомендаций. Совместная фильтрация находит то, что понравилось похожим пользователям. Она классифицирует пользователей по кластерам схожих типов и выдает рекомендации пользователям в соответствии с предпочтениями их кластеров. Основная идея, которая лежит в основе метода совместной фильтрации, заключается в том, что благодаря прошлым взаимодействиям пользователя с элементом при обработке в системе становится достаточно обнаружить похожих пользователей или аналогичные элементы, чтобы делать прогнозы на основе этих фактов. Фильтрация на основе содержимого обычно моделируется как взаимодействие пользователя со сложным объектом. Используемая модель предпочтений аналогична, но вместо того, чтобы рассматривать элементы как цельные объекты, она использует дополнительную информацию об объектах и пользователях.

Сравнение между возможными моделями напоминает сравнение яблок с апельсинами, потому что рекомендуемые объекты могут быть абсолютно различны. Если разрабатываемая система будет предлагать клиенту такие предметы как фрукты или столовые приборы, то имеет смысл смоделировать их как цельные объекты.

Если же система должна рекомендовать такие вещи, как видеоигры или фильмы, то имеет смысл моделировать их с уточнением их компонентов. Например, у фильма есть название, актерский состав, жанр, режиссер, оператор, сценарист, пользовательский рейтинг и так далее. Если пользователь выбирает фильм, то ему, вероятно, стоит узнать о киноленте всё и решить, насколько она ему интересна, прежде чем принимать решение о просмотре.

Контент-ориентированный подход использует дополнительную информацию о пользователях и/или элементах. Этот метод фильтрации использует характеристики элемента, чтобы рекомендовать другие элементы, похожие на то, что нравится пользователю, а также на основе его предыдущих

действий или явных отзывов. Если мы рассмотрим пример для системы рекомендаций фильмов, дополнительной информацией может быть возраст, пол, работа или любая другая личная информация для пользователей, а также категория, главные действующие лица, продолжительность или другие характеристики фильмов.

Контент-ориентированный подход гораздо меньше страдает от проблемы холодного старта, чем метод совместной фильтрации, потому что новые пользователи или элементы могут быть описаны по их характеристикам, то есть по содержанию, и поэтому для этих новых объектов могут быть сделаны соответствующие предложения. Только новые пользователи или элементы с ранее неизвестными функциями будут очевидно страдать от этого недостатка, но как только система будет достаточно обучена, вероятность этого будет стремиться к нулю. По сути, он предполагает, что если пользователь интересовался каким-либо элементом в прошлом, он снова будет заинтересован в том же самом в будущем. Подобные предметы обычно группируются на основе их характеристик. Профили пользователей создаются с использованием исторических взаимодействий или путем явного опроса пользователей об их интересах. Существуют и другие системы, не считающиеся чисто контентными, которые используют личные и социальные данные пользователей.

Проблемы могут возникнуть в тех случаях, когда в системе мало рецензий на конкретную книгу или фильм. Тогда возникнет риск, что фильм будет незаслуженно редко рекомендоваться пользователям. Это называется предвзятостью контента (*content bias*).

Если взять популярный фильм, то очевидно, что у него будет много отзывов. Когда у нас много отзывов, среди них будут как положительные, так и отрицательные отзывы. В худшем случае, когда у малоизвестного фильма очень мало отзывов, тогда все они могут быть отрицательными.

Для решения этой проблемы, возможно просто удалять или игнорировать негативные оценки и использовать только позитивные оценки. Проблема в том, что негативные оценки могут говорить о предпочтениях человека лучше, чем позитивные оценки. Также в некоторых отраслях (например, если речь идет о магазине электроники) пользователи значительно активнее ставят отрицательные оценки, исходя из того, что о ненадлежащем качестве товара следует сообщить, а если товар устраивает — то не стоит и тратить времени на его оценку.

Для создания хорошей рекомендательной системы необходимы хорошие обучающие данные. В противном случае работает принцип *GIGO* (*garbage in — garbage out*). Если необходимо построить модель, которая производит рекомендации фильмов, потребуется набор данных с большим количеством фильмов, их рейтингов, а также других данных. Если обучающий датасет слишком маленький, невозможно получить достаточно точную модель, чтобы давать хорошие рекомендации [2].

Список используемых источников:

1. Кежватова А.Т., Суслина А.А., Громов А.Ю. Анализ средств реализации рекомендательных систем. // Методы и средства обработки и хранения информации: Межвузовский сборник научных трудов / Под ред. Б.В. Кострова; - Рязань: ИП Коняхин А.В. (Book Jet), 2019, Выпуск 2. – 188 с.
2. Ricci F., Rokach L., Shapira B., Kantor P.B. (Eds.) Recommender System Handbook vol. 3. - Springer, 2022. 1053 с.

Yagunov P.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of Approaches to Creation of Recommender Systems.

The Internet is a digital marketplace that provides many options, sometimes too overwhelming to choose from. Today, everything can be easily accessible thanks to this digital market. From entertainment content to products and clothing, all essentials or luxury items are available online. With many options available, there has always been a serious need to filter, prioritize and efficiently deliver relevant information in order to overcome the potential problem of information overload, creating confusion for many Internet users. Recommendation systems can help solve this problem by processing a large amount of dynamically generated information to provide users with personalized content and services.

Key words: *recommender systems, neural networks, collaborative filtering, content based filtering.*

**Секция 4.2.
Интеллектуальные технологии в автоматизации и цифровых системах
управления**

УДК 004.35
ГРНТИ 20.53.23

УПРАВЛЕНИЕ СИСТЕМОЙ УМНЫЙ ДОМ С ИСПОЛЬЗОВАНИЕМ DTMF

К. В. Белоус, А. К. Кириллова, М. К. Кириллова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время активно развиваются технологии интеллектуального управления устройствами, обеспечивающими комфортные условия пребывания в жилище – все они объединены под общим названием «Умный дом». Важной процедурой в процессе взаимодействия пользователя с системой является процедура ввода и получения информации. В статье рассматривается возможность использования для этого технологии DTMF.

DTMF, умный дом, Arduino, автоматизация

В современном мире активно развивается технология интеллектуального управления зданиями, сооружениями и инженерными объектами, получившая общее название «умный дом», при этом, чаще всего под данным термином понимают:

- системы, обеспечивающие безопасность, ресурсосбережение и комфорт в здании для всех пользователей. Она должна уметь распознавать различные ситуации, происходящие в здании, и реагировать на них, при этом одна из систем может управлять поведением других по заранее выработанным алгоритмам. Умный дом подразумевает слаженную работу системы отопления и кондиционирования, контроль факторов, влияющих на необходимость их включения или отключения. Система работает в автоматизированном режиме в соответствии с внешними и внутренними условиями задаются и отслеживаются режимы работы всех инженерных систем и электроприборов. В данном случае сокращается количество средств управления оборудованием и приборами.

- системы домашней автоматизации, способных выполнять действия и решать определённые повседневные задачи без участия человека. Домашняя автоматизация в современных условиях — чрезвычайно гибкая система, которую пользователь конструирует и настраивает самостоятельно в зависимости от собственных потребностей. Это предполагает, что каждый владелец умного дома самостоятельно определяет, какие устройства куда установить и какие задачи они будут исполнять. Наиболее распространенные примеры автоматических действий в «умном доме» — автоматическое включение и выключение света, автоматическая коррекция работы отопительной системы или кондиционера и автоматическое уведомление о вторжении, возгорании или протечке воды. Домашняя автоматизация рассматривается как частный случай интернета вещей, она включает доступные через интернет домашние устройства, в то время как интернет вещей включает любые связанные через интернет устройства.

Одной из задач, которые необходимо решать в процессе создания системы «умный дом» является задача удалённого контроля и управления компонентами системы. Наиболее распространённым решением в настоящее время является управление через интернет с использованием web-сервера умного дома или с использованием бота, разработанного в мессенджере Telegram. Несмотря на очевидные преимущества, данные способы интерактивного взаимодействия с компонентами системы имеют свои недостатки – необходимо постоянно, или, по крайней мере, большую часть времени находится в зоне доступа к сети Интернет.

В данной статье рассматривается возможность управления устройствами с помощью DTMF — двухтонального многочастотного аналогового сигнала, используемого при вводе команд интерактивных сервисов, например, IVR. Для кодирования символа в DTMF сигнал необходимо сложить два синусоидальных сигнала. Частоты выбираются из таблицы по соответствующему столбцу и строке, соответствующих передаваемому символу (таблица 1). Например, для передачи символа «*» необходимо передавать сигналы с частотами 941 Гц и 1209 Гц (рис. 1) [1, 2].

ТАБЛИЦА 1. Частоты для формирования DTMF-сигнала

1	2	3	A	697 Гц
4	5	6	B	770 Гц
7	8	9	C	852 Гц
*	0	#	D	941 Гц
1209 Гц	1336 Гц	1477 Гц	1633 Гц	

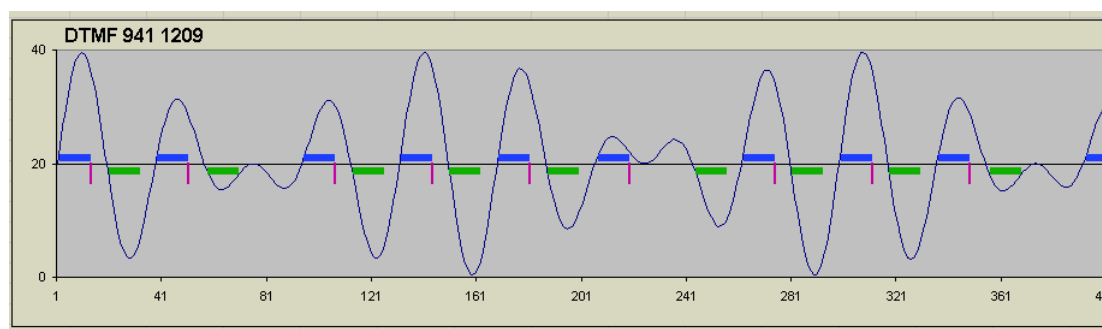


Рис. 1. Осциллограмма DTMF-сигнала при передаче символа «*»

Для проведения эксперимента по кодированию и декодированию DTMF-сигнала была собрана экспериментальная установка на базе микроконтроллерной платы Arduino Nano, которая находит широкое применение в системах малой автоматизации.

За основу генератора была взята схема, описанная в [3], в которую была добавлена матричная клавиатура 4*4 (рис. 2). Так же был модифицирован скетч – добавлена возможность постоянного звучания тонального сигнала, пока нажата соответствующая клавиша.

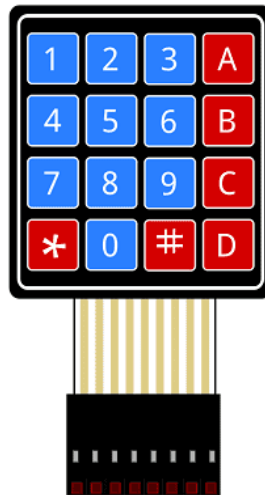


Рис. 2. Матричная клавиатура 4*4

Декодирование сигнала DTMF может быть выполнено с использованием алгоритма Гёрцеля.

Для декодирования сигнала использовалась схема [4], с незначительными доработками – вместо светодиодов был добавлен ЖК-экран для большей эффективности процедуры контроля.

Система управления на базе DTMF требует наличия GSM-модуля, наиболее распространёнными из которых являются платы на базе SIM800 или SIM900, обладающие приблизительно схожими функциональными возможностями.

Список используемых источников:

1. Black DTMF Decoding Algorithm [Электронный ресурс] https://www.romanblack.com/DTMF/DTMF_alg.htm (дата обращения 30.09.2022).
2. Пономарев В.А., Пономарева О.В., Пономарев А.В., Пономарева Н.В. Обобщение алгоритмов Герцеля и скользящего параметрического дискретного преобразования Фурье. Журнал Цифровая обработка сигналов № 1/2014, с. 3–11.
3. Генерация тонов DTMF только с помощью Arduino [Электронный ресурс] <https://arduinoplus.ru/generacia-dtfm-arduino/> (дата обращения 06.10.2022).
4. DTMF Decoder Using Only Arduino [Электронный ресурс] https://create.arduino.cc/projecthub/MM_Shoaib/dtmf-decoder-using-only-arduino-872502 (Дата обращения 20.10.2022).

Belous K, Kirillova A, Kirillova M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Smart home system control using DTMF.

Currently, technologies for intelligent control of devices that provide comfortable conditions for staying in a home are being actively developed - all of them are united under the common name "Smart Home". An important procedure in the process of user interaction with the system is the procedure for entering and receiving information. The article discusses the possibility of using DTMF technology for this.

Key words: *DTMF, Smart home, Arduino, automation.*

УДК 004.946
ГРНТИ 28.17.33

АГЕНТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД К ФОРМИРОВАНИЮ ДЕЦЕНТРАЛИЗОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

А. К. Выжлова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В представленном докладе рассматривается формирование агентно-ориентированной системы управления, построенной на базе микросервисной архитектуры. Проведен сравнительный анализ централизованной и децентрализованной систем управления. Показаны перспективы агентно-ориентированных децентрализованных систем управления.

микросервис, децентрализованная система, централизованная система, киберсреда, агенты

В данный момент времени централизованные системы управления теряют свою актуальность в связи с громоздкостью, сложностью модификации и проблемам с масштабируемостью. В таких системах может проявляться существенная задержка при выработке решения из-за длинного маршрута передачи информации в силу иерархичности таких систем. Для решения поставленной задачи в рамках централизованной системы необходимо послать запрос на главный узел с целью получения ответа (рис. 1) [1-2].

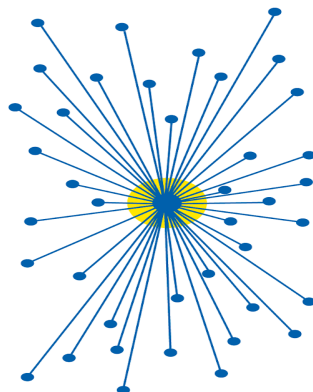


Рис. 1. Топология централизованной системы управление

Децентрализованная архитектура системы управления обладает возможностью распределять задачи между отдельными элементами системы, частным случаем, которых являются агенты. Данная архитектура набирает популярность за счёт своей универсальности и гибкости, что обеспечивает более рациональную организацию решения задач (рис. 2) [3].

Одним из перспективных видов децентрализованных систем управления являются агентно-ориентированные системы, функционирующие в рамках киберсреды. Основными принципами создания киберсред являются: агентность, информационное самообслуживание и управляемая информационная открытость, а именно непрерывная информационная поддержка поставок и

жизненного цикла изделий. Микросервис обладает всеми необходимыми свойствами для реализации отдельных агентов. Каждый микросервис в системе фактически является агентом, который выполняет присвоенные ему задачи и в сотрудничестве с другими агентами предоставляет конечному пользователю полностью функциональный сервис [4-6].

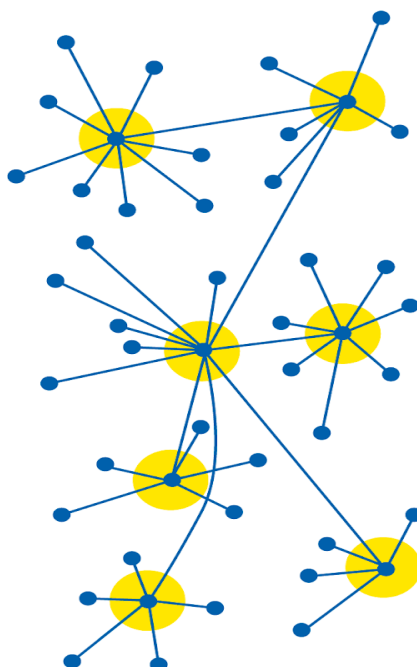


Рис. 2. Модель децентрализованной системы управления

Автономность каждого микросервиса позволяет выполнять свою задачу без вмешательства человека и независимо от других микросервисов. На рис. 3 три микросервиса фактически могут функционировать автономно. Микросервис 2 имеет роль шлюза, отвечает за пересылку сообщений, работая в автономном режиме. Микросервис 1 выполняет сохранение данных в хранилище, а Микросервис 3 извлекает из информационного хранилища информацию.

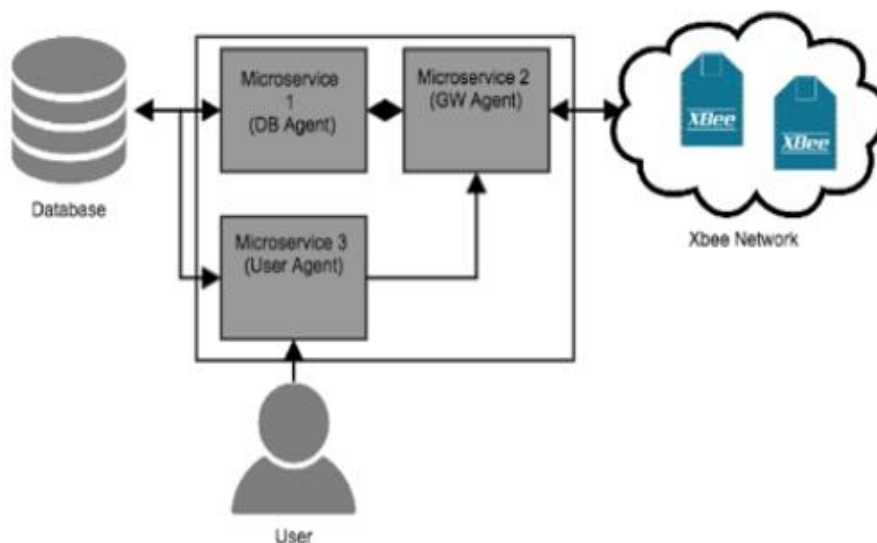


Рис. 3. Архитектура взаимодействия микросервисов с базами данных

Взаимодействие, сотрудничество и координация – это три основных свойства микросервисов. Модульная система, состоящая из нескольких микросервисов, должна иметь четко определенный интерфейс между ними, чтобы работать правильно и эффективно. Каждый микросервис на рис. 3 сам по себе не имеет цели, однако вместе они образуют полноценную функционирующую систему.

Агентно-ориентированные децентрализованные системы обеспечивают формирование защищенного киберпространства, которое необходимо для решения конкретных бизнес-задач цифровой экономики, и в частности, Индустрии 4.0. Особенности агентно-ориентированных децентрализованных систем управления делает их хорошим кандидатом для формирования единого киберпространства постиндустриального общества [7].

Список используемых источников:

1. Павлов И.Ю., Колосков В.Л., Иванов Е.Б. Анализ централизованных и децентрализованных систем автоматизированного управления «Интеллектуальным» домом. // Москва. 2016 .
2. Хорсдал К. Микросервисы на платформе .NET. // Питер. 2018г.
3. Ричардсон К. Микросервисы. Паттерны разработки и рефакторинга // Питер. 2019 г.
4. Кэм Дж. Микро-фронтенды [Электронный ресурс]. URL: <https://martinfowler.com/articles/micro-frontends.html> (дата обращения 19.11.2021)
5. Акимов С.В., Верхова Г.В., Меткин Н.П. Теоретические основы CALS. // СПб. 2018.
6. Микросервисный подход в веб-разработке: micro frontends [Электронный ресурс]. URL: <https://dou.ua/lenta/articles/micro-frontend/> (дата обращения 21.11.2021)
7. Верхова Г.В., Акимов С.В. Интеграция локальных интероперабельных киберсред виртуальных организаций в единую киберсреду постиндустриального общества. // СПб. 2018.

Vyzhlova A.K.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Agent-based approach to the formation of decentralized management systems.

The presented report discusses the formation of an agent-oriented management system built on a microservice management architecture. The question of the relevance of a centralized management system is raised. The analogy of a decentralized management system with a micro-service architecture is drawn.

Key words: *microservice, decentralized system, centralized system, cyber environment, agents.*

УДК 004.051
ГРНТИ 50.49.37

РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ПО УПРАВЛЕНИЮ НАУЧНЫМИ КОНСОРЦИУМАМИ

А. Ю. Гребешков, Ю. Е. Пенькова

Самарский государственный технический университет

Цифровые решения в настоящее время являются ядром трансформационных процессов, протекающих во всех сферах деятельности. Перспективная практика объединения субъектов научно-исследовательского пространства в научные консорциумы включает в себе колоссальный задел и предполагает решение глобальных вызовов путем реализации инновационных проектов. Разработка методики оценки эффективности деятельности в рамках данных мероприятий на основе цифровой платформы позволит использовать сквозные информационные технологии при принятии управленческих решений и будет способствовать повышению эффективности, а значит и конкурентоспособности научных консорциумов и российской экономики в целом.

научный консорциум, оценка эффективности, деятельность в рамках консорциума, разработка методики, работа с данными, цифровая платформа

Основополагающую роль в прогрессивном становлении и развитии научных консорциумов играет эффективно-прогрессивная модель управления, включающая в себя инновационные средства и методы, ориентированные на длительный горизонт планирования и постоянно развивающиеся в зависимости от условий внешней и внутренней среды. С учетом современных реалий симбиоз разноплановых организационных структур в области научных исследований направлен, с одной стороны, на сохранение существующих традиций участников научного консорциума, с другой – на выполнение новых задач по ускоренному развитию новых решений и стимулированию инноваций. Именно поэтому модель управления и оценки эффективности управления таким объединением может быть основана на цифровой платформе упорядоченной обработки и предоставления результатов научной деятельности посредством витрины данных, использовании мастер-данных и корпоративного хранилища данных.

Для оценки эффективности деятельности по управлению научными консорциумами следует рассматривать проводимые мероприятия и проекты по различным метрикам. Эффективность в данном случае определяется как степень достижения показателей деятельности и в более широком смысле – как удовлетворенность процессом реализации проекта или деятельности как участников, по-другому – концепция множественности заинтересованных сторон. Такая интегральная оценка призвана учитывать интересы различных сторон стейкхолдеров научных проектов и степень их удовлетворения. На начальном этапе формирования системы оценки эффективности управления целесообразно использовать идеализированную модель оценки результатов управления научного консорциума, включая работу с данными.

Для этого экспертным способом задаются метрики оценки и проводится комплексный системный анализ результатов работы условного консорциума на предмет соответствия заданным условиям и показателям. В случае удовлетворительной оценки можно обоснованно полагать, что работа с данными ведётся также удовлетворительно. Для общей оценки состояния управления деятельностью консорциумов предлагается использовать метрики, относящиеся к следующим областям и их примерные значения, представленные на рис. 1.

Наименование групп метрик и отдельных метрик	Возможные значения метрик
1. Научно-исследовательская и инновационная деятельность	
1.1 Количество статей в областях, определяемых приоритетами научно-технологического развития Российской Федерации, в научных изданиях, индексируемых в международных базах данных РИНЦ/ВАК, приравненных к Scopus (Q1-Q4) или к Web of Science (Q1-Q4), ед.	от 1000 до 5000 целевое значение – 4000
1.2 Количество патентов на изобретения по областям, определяемым приоритетами научно-технологического развития Российской Федерации, зарегистрированных в Российской Федерации и (или) имеющих правовую охрану за рубежом, ед.	от 100 до 800 целевое значение – 500
1.3 Участие в выполнении финансируемых НИОКР и проектах, млн. руб.	от 5 до 100 целевое значение – 50
1.4 Количество разработанных и переданных для внедрения в производство в организациях, действующих в реальном секторе экономики, конкурентоспособных технологий и высокотехнологичной продукции, ед.	от 100 до 500 целевое значение – 250
2. Кадровый потенциал	
2.1 Доля работников организаций, участвующих в создании центра, прошедших обучение по дополнительным профессиональным программам в соответствии с приоритетными направлениями, %	от 20 до 40 целевое значение – 30
2.2 Количество иногородних обучающихся по ОП высшего образования, прибывших из субъектов Российской Федерации, участвующих в создании центра, а также иностранных обучающихся, чел.	от 20000 до 70000 целевое значение – 65000
2.3 Количество лиц, завершивших обучение в центрах развития компетенций в интересах развития региона, чел.	от 100 до 500 целевое значение – 300
2.4 Реализация академической мобильности научно-педагогических работников между участниками консорциума, чел.	от 10 до 100 целевое значение – 50
3. Инфраструктурное обеспечение	
3.1 Совместное использование оборудования и инфраструктуры участниками консорциума, установок, ед.	от 10 до 50 целевое значение – 40
3.2 Доля новой и усовершенствованной высокотехнологичной продукции в общем объеме отгруженной продукции, %	от 15 до 80 целевое значение – 60
3.3 Количество новых высокотехнологических рабочих мест в результате реализации проекта, ед.	от 500 до 1000 целевое значение – 850
3.4 Наличие в субъекте инструментов развития (ТОР, ОЭЗ, промышленных технопарков, индустриальных парков, промышленных, инновационных кластеров, инновационных научно-технологических центров), используемых консорциумом, ед.	от 10 до 50 целевое значение – 40
4. Вовлеченность инициативной молодежи	
4.1 Реализация индивидуальных образовательных траекторий под конкретные потребности организаций-участников консорциума, чел.	от 50 до 150 целевое значение – 120
4.2 Доля исследователей в возрасте до 39 лет в общей численности исследователей, %	от 30 до 65 целевое значение – 50
4.3 Количество проведенных проектных хакатонов и других обучающих мероприятий, развивающих навыки в разных областях разработки в процессе командной работы над проектами, на базе центра развития современных компетенций в рамках консорциума, ед.	от 20 до 100 целевое значение – 50
4.4 Количество обучающихся, вовлеченных в проект консорциума, чел.	от 500 чел. до 1000 целевое значение – 850

Рис. 1. Показатели для оценки эффективности деятельности консорциума, включая работу с данными

Данные, приведенные в таблице 1, являются ориентировочными, в рассматриваемом контексте предполагается, что метрические величины определяются на основе данных из публичных источников [1].

На следующем этапе эксперты выражают оценки предпочтений в отношении значимости метрик с помощью шкалы предпочтений, где 1 - равная значимость метрик для эксперта, 9 - очень сильное превосходство значимости метрики [2]. Далее эксперты выставляют балльные оценки о деятельности в рамках консорциума согласно методу анализа иерархий, который позволяет в формализованном виде оценить степень соответствия собранной информации по целевым или граничным значениям метрик оценки качества деятельности консорциума с учетом механизма оценки противоречивости суждений экспертов [3]. Эксперты оценивают значимость групп метрик из таблицы 1 по шкале следующим образом: $a_{1-2}=2$, $a_{1-3}=1$, $a_{1-4}=3$, $a_{2-1}=0,5$, $a_{2-3}=2$, $a_{2-4}=3$, $a_{3-1}=1$, $a_{3-2}=0,5$, $a_{3-4}=2$, $a_{4-1}=0,33$, $a_{4-2}=0,33$, $a_{4-3}=0,5$. Согласно замечанию, $a_{1-1}=a_{2-2}=a_{3-3}=a_{4-4}=1$ [4]. Эти оценки свидетельствуют о том, что для экспертов вопросы научно-исследовательской и инновационной деятельности находятся в приоритете по отношению к другим областям управления. Принимая базу проекта равной 1000, рассчитаем максимальную сумму баллов по отдельным группам метрик по формуле (1):

$$\text{БГМ}_k = \text{БП} \times C_k^{\text{ГМВП}} \quad (1)$$

где $C_k^{\text{ГМВП}}$ – значение вектора приоритетов для k-ой группы метрик, рассчитываемое по формуле (2):

$$C_k^{\text{ГМВП}} = \frac{c_k^M}{\sum_{i=1}^K c_i^M}, \quad (2)$$

где c_k^M – значение элемента вектора приоритетов для k-ой группы метрик;
 K – общее количество групп метрик.

Для расчёта c_k^M применяется формула (3):

$$c_k^M = \left(\prod_{i=1}^K a_{ki} \right)^{1/K}, \quad (3)$$

где a_{ki} – мера относительной важности или значимости k-й группы метрик относительно i-й группы метрик с использованием шкалы. Получаем $C_1^{\text{ГМВП}} = 0,358$; $C_2^{\text{ГМВП}} = 0,301$; $C_3^{\text{ГМВП}} = 0,229$; $C_4^{\text{ГМВП}} = 0,111$. Тогда распределение базы проекта по отдельным группам метрик, согласно формуле (1), будет равно: БГМ1= 358 баллов, БГМ2=301 баллов, БГМ3=229 балл, БГМ4= 111 баллов, контрольная сумма 358+301+229+111=1000. Это максимальное количество баллов, которые могут быть получены по группам метрик, если текущие значения превосходят граничные или целевые показатели.

Далее эксперты проводят оценки значимости отдельных метрик в рамках группы метрик. Пусть для метрик 1-й группы получены следующие значения: $a_{1.1-1.2}=0,5$, $a_{1.1-1.3}=0,5$, $a_{1.1-1.4}=0,5$, $a_{1.2-1.1}=2$, $a_{1.2-1.3}=2$, $a_{1.2-1.4}=1$, $a_{1.3-1.1}=2$, $a_{1.3-1.2}=0,5$; $a_{1.3-1.4}=3$, $a_{1.4-1.1}=2$, $a_{1.4-1.2}=0,5$; $a_{1.4-1.3}=3$, $a_{1.1-1.1}=a_{1.2-1.2}=a_{1.3-1.3}=1$. Применяя к указанным оценкам последовательно формулы вида (3), получаем следующие значения элементов вектора приоритетов для метрик: $C_1^{\text{МВП1}} = 0,11$; $C_2^{\text{МВП1}} = 0,36$; $C_3^{\text{МВП1}} = 0,33$, $C_4^{\text{МВП1}} = 0,20$. Аналогичным способом проводятся оценки для остальных трех групп метрик, в результате чего получены следующие итоговые значения:

- для метрик 2-й группы значения элементов вектора приоритетов составляет $C_1^{\text{МВП2}}=0,24$; $C_2^{\text{МВП2}}=0,32$; $C_3^{\text{МВП2}}=0,27$, $C_4^{\text{МВП2}}=0,17$;
- для метрик 3-й группы значения элементов вектора приоритетов составляет $C_1^{\text{МВП3}}=0,02$; $C_2^{\text{МВП3}}=0,38$; $C_3^{\text{МВП3}}=0,22$, $C_4^{\text{МВП3}}=0,20$;
- для метрик 4-й группы значение элементов вектора приоритетов составляет $C_1^{\text{МВП4}}=0,49$; $C_2^{\text{МВП4}}=0,24$; $C_3^{\text{МВП4}}=0,15$, $C_4^{\text{МВП4}}=0,12$.

Для оценки отношения согласованности (ОС) балльных оценок экспертов применяется параметр случайной согласованности $CC^M \delta 0,9$ (для четырёх метрик или четырёх групп метрик) и рассчитывается по формуле (4);

$$OC_m^M = \frac{IC_m^M}{CC^M}. \quad (4)$$

где IC_m^M – индекс/мера согласованности максимального приоритета, $МП_m^M$, для метрик заданной k-й группы, как показано в формуле (5):

$$IC_m^M = \frac{МП_m^M - M}{M - 1}, \quad (5)$$

Значение $МП_m^M$ определяется по формуле (6):

$$МП_m^M = \sum_{m=1}^M \left(\left(\sum_{i=1}^M a_{im} \right) \times C_m^{MBПk} \right). \quad (6)$$

Как правило, величину ОС берут менее 10% ($\delta 0,1$). Изучив реальные значения по каждой метрике, полученные в результате наблюдений или изучения документации, эксперты выставляют относительные оценки, позволяющие охарактеризовать степень приближения к целевым или граничным значениям метрик, а не натуральное значение. Полученные значения $ОЭ_m$ суммируются в рамках каждой группы метрик, в результате чего получаем суммарную балльную оценку экспертов для k-й группы, которая будет меньше или равна $БГМ_k$. Окончательно для формирования общей оценки эффективности деятельности консорциума используется следующая формула (7):

$$C_{БП}^{ОЭ} = \frac{\sum_{k=1}^K \left(\sum_{m=1}^M OЭ_m \right)_k}{БП}, \quad (7)$$

В итоге получаем оценку эффективности деятельности в рамках консорциума $(227+174+170+77)/(358+301+229+111)=0,633$ или 633 балла.

Интерпретация полученных результатов предполагает:

- 0,00...0,4 - качество выполнения консорциумом показателей эффективности не соответствуют целевым значениям по большинству метрик, то есть эффективность управления деятельностью консорциума неудовлетворительна, требуется системный реинжиниринг деятельности;
- 0,41...0,7 - качество выполнения консорциумом показателей эффективности соответствует целевым значениям по некоторым метрикам, то есть управление деятельностью консорциума требует улучшения;
- 0,71...1,00 - качество выполнения консорциумом показателей эффективности соответствует целевым значениям по большинству метрик, то есть эффективность управления деятельностью консорциума удовлетворительна, необходим только постоянный самоконтроль качества и реализация деятельности по улучшению процессов.

В контексте предлагаемой методики открывается перспективная возможность учета не только количественных, но и качественных показателей эффективности - таких как: совместное использование оборудования и инфраструктуры участниками консорциума; реализация индивидуальных образовательных траекторий под конкретные потребности организаций-участников консорциума; реализация академической мобильности научно-педагогических работников между участниками консорциума и т.д. В современных реалиях возможно формирование институтов экспертных советов, в состав которых могут войти представители органов государственной власти, научно-образовательного сообщества, институтов развития региона и организаций реального сектора для оценки перспектив развития и результатов реализации проектов консорциумов.

Таким образом, в фокусе применения предлагаемой методики оценки эффективности управления можно обеспечить унификацию и приведение к единому стандарту способов оценки параметров эффективности основных направлений совместной деятельности в рамках консорциума. Основным инструментом системы управления станет единая автоматизированная информационная платформа, оптимизирующая основные бизнес-процессы и работу по сопровождению и контролю реализации проектов, что позволит на выходе выделить центры принятия решений, определяющих стратегию развития участников консорциума.

Список используемых источников:

1. Ежегодный отчет о результатах программы деятельности научно-образовательного центра мирового уровня «Инженерия будущего» за 2020 г.
2. Быкова Т.В. Метод анализа иерархий как инструмент решения практических задач многокритериальной оптимизации // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2019. №1. С. 1-10
3. Саати, Т. Принятие решений. Метод анализа иерархий: Пер. с англ. – М.: Радио и связь, 1993. – 320 с.
4. Гребешков А. Ю. Метод анализа состояния системы эксплуатационной поддержки OSS оператора связи // Инфокоммуникационные технологии. – 2008. – Т.6, №2. – С. 82–87

Penkova J., Grebeshkov A.

Samara State Technical University

Development of Methodology of Efficiency Evaluation of Scientific Consortia Management. Digital solutions are currently the core of transformational processes in all spheres of activity. The promising practice of uniting the subjects of the research space in consortia contains a huge reserve and involves the solution of global challenges through the implementation of innovative projects. Development of the methodology for assessing the effectiveness of these activities on the basis of a digital platform will allow the use of end-to-end information technology in making management decisions and will contribute to improving the efficiency and thus the competitiveness of consortia and the Russian economy as a whole.

Key words: scientific consortium, performance evaluation, activities within the consortium, development of methodologies, work with data, digital platform.

УДК 004.457
ГРНТИ 50.41.23

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИНФРАСТРУКТУРНЫХ ИНСТРУМЕНТОВ INFRASTRUCTURE AS CODE

А. В. Елфимов, В. В. Косенков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Облачные вычисления с каждым годом становятся все более популярными. Навыки создания устойчивой инфраструктуры никогда не были так востребованы, как сейчас. Инструменты IaC создают файлы конфигурации, содержащие спецификации инфраструктуры, что упрощает редактирование и распространение конфигураций. Это также гарантирует, что каждый раз создаются идентичная среда и идентичные ресурсы. В области DevOps крупнейшими конкурентами являются Terraform и Pulumi.

инфраструктура, облако, IaC, Terraform, Pulumi

1. Введение

Для того чтобы иметь возможность автоматизировать и стандартизировать процесс создания инфраструктуры, появились инструменты IaC. Инфраструктура как код (IaC) — это управление инфраструктурой и ее предоставление с помощью кода, а не ручных процессов. Облачные вычисления это модель, позволяющая использовать ресурсы, отсутствующие локально, такие как: серверы, сети, хранилища данных, службы и приложения. Существует три способа создания инфраструктуры. Первый способ — через веб-интерфейс. Другой способ — использование команд CLI. Третий и наиболее предпочтительный способ — использование инструментов IaC, основанных на вызовах API.

Проблемы, которые решают инструменты IaC: проблемы согласованности инфраструктуры, проблемы скорости развития инфраструктуры, проблемы создания повторно используемой инфраструктуры и минимизация человеческих ошибок. [1]

2. Уровни облачных вычислений

Инфраструктура как услуга (IaaS) - она представляет собой самый нижний слой пирамиды и служит основой облачных вычислений. IaaS - это наиболее полный и гибкий тип доступных услуг. По сути, он предоставляет полностью виртуализированную вычислительную инфраструктуру, управляемую через Интернет. [3]

Платформа как услуга (PaaS) - он расположен на уровне выше уровня IaaS. PaaS является более специализированным. Вместо чистой инфраструктуры PaaS предоставляет структуру, необходимую для создания, тестирования, поставки, управления и обновления программных продуктов. Программное обеспечение как услуга (SaaS) - для большинства людей SaaS является наиболее знакомой основой облачных вычислений. Находится на уровне пирамиды над уровнем PaaS. SaaS — это полностью разработанное программное решение, готовое к

использованию через Интернет по подписке. Функция как услуга (FaaS) - этот слой находится на самом вершину пирамиды. FaaS делит вершину пирамиды с технологией SaaS. FaaS позволяет своим пользователям выполнять логику, упакованную в функции, без предварительной подготовки инфраструктуры и серверов. Контейнер как услуга (CaaS) - Технология, позволяющая создавать приложения и управлять ими с помощью абстракции на основе контейнеров. Он работает по другому принципу, чем FaaS. Пользователя просят написать функцию, затем эта функция упаковывается в контейнер и размещается на сервере. [1]

3. Terraform и Pulumi

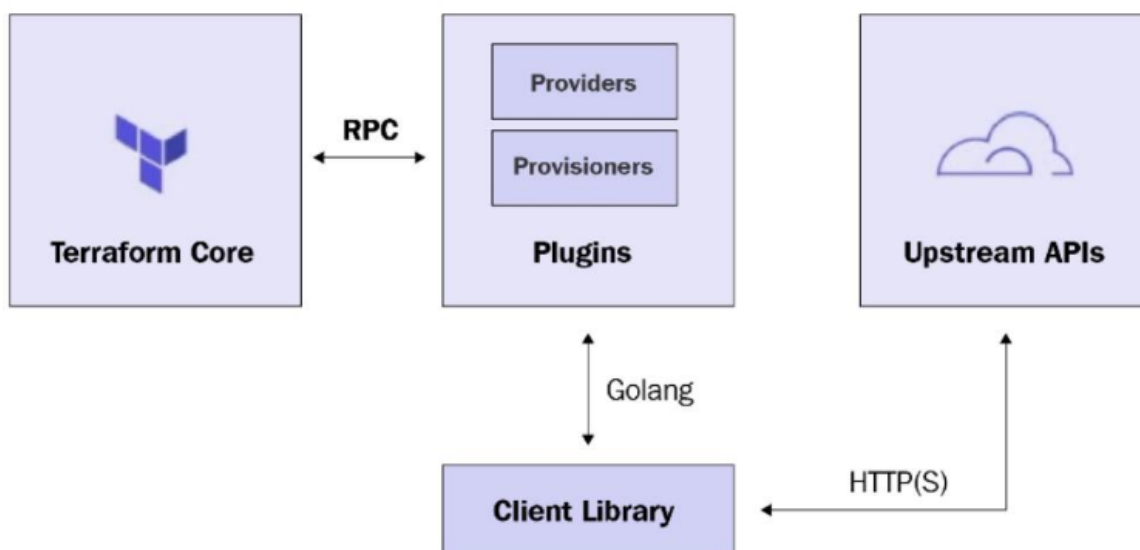


Рис. 1. Архитектура Terraform.

Terraform — это технология для тех, кто хочет настраивать и управлять некоторой инфраструктурой в виде простого кода. Инфраструктура в первую очередь относится к облаку на основе инфраструктуры, хотя технически инфраструктура — это все, чем можно управлять через API. Основной принцип технологии Terraform заключается в том, чтобы дать возможность писать удобочитаемый код конфигурации для определения IaC. Язык, используемый Terraform, называется языком конфигурации HashiCorp (HCL). Он предназначен для достижения баланса между читаемым программным кодом и удобством для машин. Благодаря удобству работы с машинами Terraform также может считывать конфигурации JSON. [4]

Pulumi использует модель «желаемое состояние» для управления инфраструктурой. [2] Механизм развертывания сравнивает желаемое состояние с текущим состоянием стека и определяет, какие ресурсы следует создать, обновить или удалить. Механизм развертывания инфраструктуры использует набор поставщиков ресурсов, например AWS, Azure или Kubernetes, для управления отдельными ресурсами. Во время работы механизм развертывания обновляет состояние инфраструктуры, добавляя информацию обо всех подготовленных ресурсах, а также обо всех незавершенных операциях.

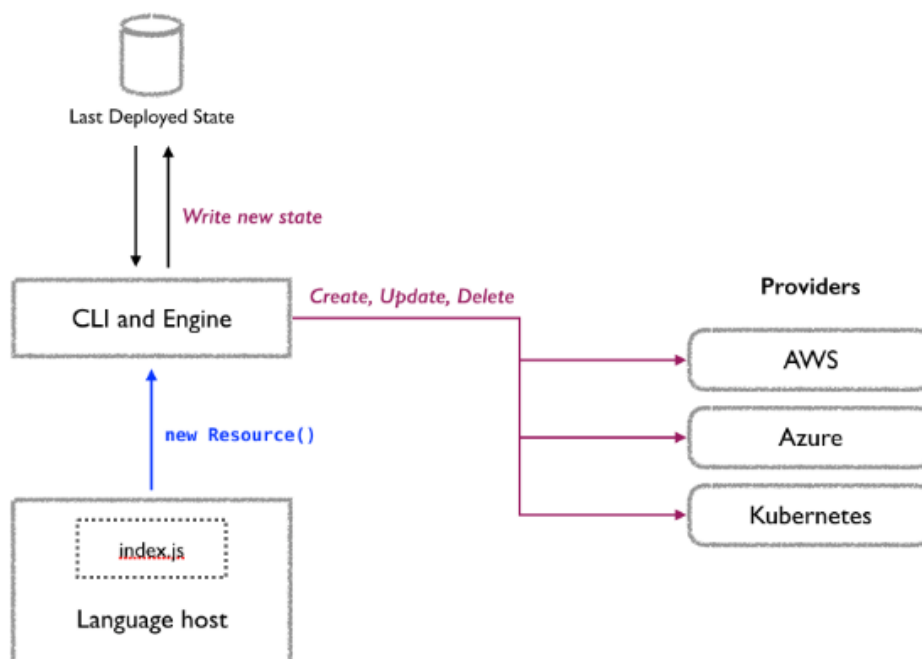


Рис. 2. Архитектура Pulumi.

4. Сравнение

Нелегко установить критерии сравнения. То, что кто-то считает недостатком, не обязательно означает, что это недостаток. Сравнение технологий Terraform и Pulumi производилось по нескольким объективным категориям:

- Простота использования
- Сообщество
- Предложения Enterprise для компаний и команд

Возможность и простота тестирования кода инфраструктуры

1. Предположим, инженеру нужно написать инфраструктуру для AWS. Также предположим, что у него нет опыта работы с инструментами IaC или некоторыми другими языками общего назначения (Python, JavaScript, Golang и т. д.). Terraform использует язык конфигурации Hashicorp. Это описательный язык, который имеет узкую цель. Эта цель состоит в том, чтобы написать файлы конфигурации. HCL предназначен для чтения теми, кто его пишет, и он очень прост. Он состоит из блоков и аргументов. Инженеру не потребуется много времени, чтобы полностью освоить HCL и научиться писать модульный и многократно используемый код Terraform.

С технологией Pulumi дело обстоит иначе. Он опирается на языки общего назначения. Это предлагает гораздо больше гибкости и возможностей, если это необходимо. Можно моделировать гораздо более сложные связи между создаваемыми ресурсами. Инженеру не обязательно знать язык программирования, чтобы написать простую инфраструктуру. Когда проект становится более сложным, возможность хорошего моделирования связей, отношений между ресурсами, а также управления ресурсами становится решающей. Имея это в виду, для хорошо написанной сложной инфраструктуры

необходимо знать язык, на котором эта инфраструктура написана. Это влечет за собой большое количество времени, затрачиваемого на изучение принципов и работы языка общего назначения. Эти накладные расходы отсутствуют в случае использования технологии Terraform.

2. Почему сообщество является одним из критериев сравнения? При работе с инструментами IaC, как и со всеми другими технологиями, ошибки и проблемы неизбежны. Лучше всего, если это возможно, учиться на чужих ошибках. Если сообщество большое, есть большая вероятность, что вы не первый, кто столкнулся с ошибкой, и вы можете использовать известный способ решения этой ошибки.

Состояние официального проекта Terraform на платформе Github очень динамично. В настоящее время ~1700 человек вносят вклад в развитие своей работой. На момент написания статьи насчитывается около 34 000 звезд. Звезды имеют двойное назначение. Некоторые люди используют звездочки, чтобы указать, что им нравится проект, другие используют их в качестве закладок, чтобы позже следить за тем, что происходит в репозитории.

Pulumi добилась значительного прогресса в последние годы с точки зрения количества поддерживаемых провайдеров и людей, вносящих свой вклад в это. На момент написания статьи в разработке Pulumi участвовало около 180 человек. Судя по проектам Github, Pulumi не пользуется такой популярностью, как его конкурент. На данный момент имеет: ~15000 звезд. Где Pulumi сияет, так это в общедоступном канале Slack, где вы можете спросить, есть ли проблема.

3. Оба инструмента имеют предприятие версию, которая не является бесплатной и позволяет использовать облачное управление версиями этих инструментов. Начнем с Terraform. Зачем кому-то использовать корпоративную версию Terraform?

Экономия времени на стандартизацию-развертывание. С помощью частных реестров можно легко создавать и распространять модули и провайдеры внутри организации.

Простая интеграция CI/CD. Просто подключить VCS к облаку Terraform и добавить шаг, на котором необходимо вручную подтвердить инфраструктуру развертывания.

Оценщик стоимости. Для каждого изменения в инфраструктуре можно получить точную информацию об изменении затрат, которое произойдет при изменении инфраструктуры.

Поддержка, предоставляемая Terraform своим клиентам, возможна через веб-портал или по электронной почте. Для большинства технических проблем служба поддержки HashiCorp запросит диагностическую информацию, включенную в запрос на поддержку. Чтобы убедиться, что необходимая информация включена, Terraform Cloud

У Pulumi тоже есть предприятие версия. Некоторые преимущества, которые предприятие включает:

- Защита политиками.
- Федеративное управление идентификацией и группами.

- Надзор. Pulumi будет записывать все действия, которые выполняли пользователи, с возможностью экспорта записей и интеграции с другими инструментами безопасности.

- Хостинг у клиента.

4. Оба инструмента поддерживают тестирование инфраструктуры. Terraform поддерживает: модульные, контрактные, интеграционные и сквозные тесты. Pulumi поддерживает: модульное, интеграционное и имущественное тестирование. Поскольку Pulumi использует языки общего назначения, тестирование зависит от сред тестирования для этих языков. Это означает, что тестирование кажется очень естественным, тогда как в случае с Terraform это не так.

Заключение

В конечном счете, выбор лучшего инструмента зависит от ваших потребностей. Из личного опыта могу сказать, что Terraform гораздо больше используется на коммерческих, клиентских проектах. Terraform больше нравится DevOps, даже программистами, которые уже знают Python или другой язык общего назначения. Существует несколько причин, которые приводят к этому. Когда дело доходит до обслуживания инфраструктуры, Terraform является явным победителем. Не существует единого способа или стандарта написания инфраструктуры с использованием Pulumi и языка общего назначения. Это связано с большой гибкостью, предлагаемой языками общего назначения.

Список используемых источников:

1. Kief Morris. Infrastructure as Code: Managing Servers in the Cloud. O'Reilly Media, Inc., 2016. 336 p.
2. What is Pulumi? Introduction to Infrastructure as Code [<https://phoenixnap.com/blog/what-is-pulumi>]
3. IaaS (Infrastructure-as-a-Service) [<https://www.ibm.com/cloud/learn/iaas>]
4. Mikael Krief, Mitchell Hashimoto. Terraform Cookbook. Packt Publishing, 2021. 366 p.

Kosenkov V., Elfimov A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Comparative analysis of infrastructure tools infrastructure as code.

Cloud computing is becoming more and more popular every year. The skills of creating a sustainable infrastructure have never been in such demand as they are now. IaC tools create configuration files containing infrastructure specifications, which makes it easier to edit and distribute configurations. It also ensures that an identical environment and identical resources are created each time. In DevOps, Terraform and Pulumi are the biggest competitors.

Key words: IPTV, caching, TV, time-shifted, the proxy.

УДК 004.415.2
ГРНТИ 50.41.29

ОЦЕНКА РЕЛЕВАНТНОСТИ ССЫЛОК В ПОИСКОВОЙ СИСТЕМЕ “ЯНДЕКС”

В. Д. Изряднов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрены особенности работы механизма поисковой системы "Яндекс", приводящие к появлению нерелевантных ссылок в поисковой выдаче и пути оптимизации поиска с использованием программного обеспечения, основанного на библиотеке "Selenium".

релевантность, поисковая система, ссылки

Постоянное совершенствование поисковых алгоритмов и последующая SEO-оптимизация сайтов под них привели к возникновению паразитной обратной связи, которая в настоящее время характеризуется нарастающей изоляцией пользователя от релевантного контента. Это явление так называемого "информационного пузыря", при котором пользователь не может найти через поисковую систему ту информацию, которая ему нужна, хотя эта информация объективно в интернете присутствует и доступна для индексации поисковыми системами [1].

Почти на каждый пользовательский запрос общего или познавательного характера найдется некоторое количество конкретных коммерческих предложений продажи какого-либо товара и владельцы таких ресурсов используют SEO-технологии для повышения релевантности своих страниц и уменьшения стоимости рекламных компаний [2]. Со своей стороны, поисковые системы оптимизируют алгоритмы поиска с целью понизить релевантность страниц с коммерческими предложениями и повысить релевантность страниц с информационным содержанием, если запрос пользователя содержит поиск именно содержимого информационного характера, а не коммерческих предложений. Объективно существующая проблема неоднозначности лингвистических конструкций и трудности распознавания искусственным интеллектом контекста языкового сообщения приводит к тому, что поисковые системы при оценке релевантности выдаваемых страниц вынуждены опираться как на историю поисковых запросов самого конкретного пользователя, так и на собственную оценку релевантности страниц [3].

Все это, вкуче с постоянно проводимой владельцами сайтов SEO - оптимизацией приводит к перемешиванию в поисковой выдаче релевантных и нерелевантных ссылок с тенденцией к уменьшению релевантности ссылок, располагаемых на первых страницах поисковой выдачи [2].

В результате пользователи вынуждены тратить дополнительное время на поиск релевантных ссылок, а в некоторых случаях релевантные ссылки исчезают из поисковой выдачи вовсе, поскольку по техническим причинам поисковые системы ограничивают общее количество единовременно выдаваемых пользователям страниц.

Для оптимизации процесса поиска и исследования соотношения степени релевантности ссылок и общего количества выдаваемых поисковыми системами страниц, было разработано программное обеспечение на языке Python и библиотеке Selenium, которое позволило в автоматизированном режиме делать запрос к поисковым системам и сортировать ссылки в порядке уменьшения релевантности. Степень релевантности оценивалась с использованием алгоритма, основанного на нечеткой логике. Для контроля релевантности ссылок, собранных автоматически, использовался упрощенный метод экспертных оценок. В общем случае причинами уменьшения релевантности ссылок в поисковой выдаче являются:

- пузырь фильтров;
- темная seo-оптимизация;

Все исследование можно условно разделить на три этапа:

- оценка экспертом первой и последующих страниц поисковой выдачи системы “Яндекс”;
- автоматизированная оценка программной системой ссылок, выдаваемых системой Яндекс при увеличении просмотренного числа страниц;
- сравнение результатов.

ТАБЛИЦА 1. Экспертный расчет процента релевантных ссылок на первых 10 страницах поисковой выдачи.

Поисковый запрос	Всего страниц (Яндекс)	Процент релевантных ссылок (Яндекс)	Всего страниц (Google)	Процент релевантных ссылок (Google)
копирование ключа windows с одного ноутбука на другой	10	30%	10	40%
почему поисковые системы выдают нерелевантные страницы	10	20%	10	20%
работа js программистом спб	10	50%	10	70%
Среднее значение	10	33,333 %	10	43,33 %

Рассматривая таблицу, можно сказать, что релевантность ссылок, представленных на первых 10 страницах не слишком высока и в среднем не превышает 44%.

В таблице 2 представлено изменение количества релевантных ссылок с увеличением количества анализируемых страниц поисковой выдачи и использованием дополнительного программного обеспечения на стороне пользователя.

ТАБЛИЦА 2. Оценка количества релевантных ссылок в поисковой выдаче Яндекса в сравнении с результатами работы разработанного программного обеспечения.

	Количество релевантных ссылок в Яндексе на страницу (n) по экспертной оценке				Количество релевантных ссылок в ИС “Оптимизации интернет-поиска” на страницу (n)				Коэффициент отношения релевантности			
	1	2	5	10	1	2	5	10	1	2	5	10
Количество страниц (n)												
Причины нерелевантных результатов в выдаче	4	6	1	1	3	4	6	8	0.75	0.67	6.0	8.0
Проекты для портфолио React	12	2	1	2	2	3	3	5	0.17	1.5	3.0	2.5
Госты для ВКР	9	10	5	3	3	5	7	7	0.33	0.5	1.4	2.33

График изменения коэффициента отношения релевантности представлен на рис. 1.

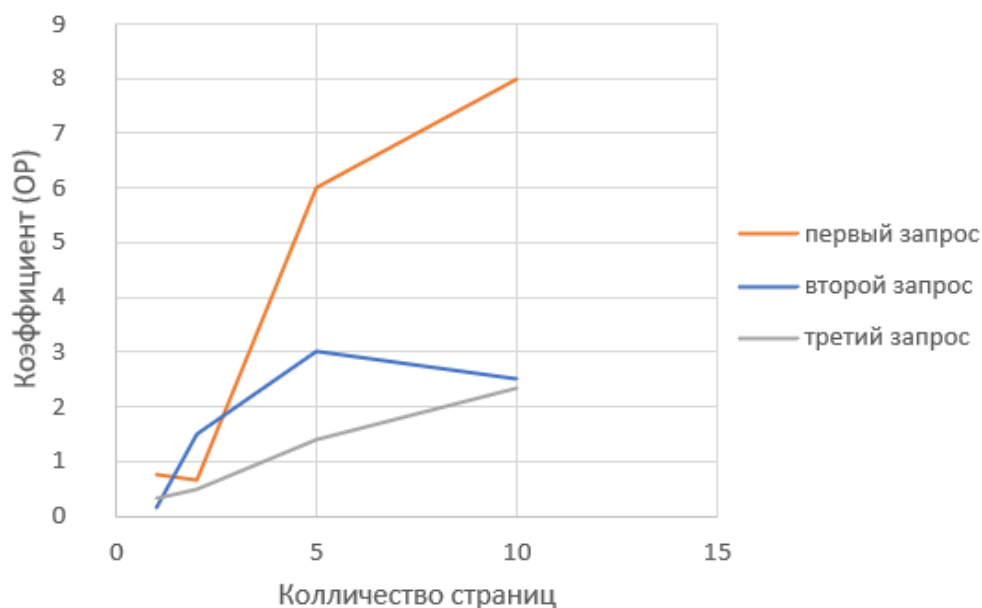


Рис. 1. График изменения коэффициента отношения релевантности

Из данных, представленных в таблице 2 можно сделать вывод, что процент релевантных ссылок на страницу в поисковой системе значительно варьирует от запроса к запросу. В среднем максимальное количество релевантных ссылок в поисковой системе Яндекса содержится на первых двух страницах, затем резко падает и пользователю требуется просматривать все большее количество страниц, чтобы получить релевантный контент.

Использование разработанного программного обеспечения позволяет получать меньшее количество релевантных ссылок на первых страницах выдачи,

однако для последующих страниц коэффициент, отражающий процентное содержание релевантных ссылок стабильно растет по всем трем запросам. Следовательно, можно прогнозировать, что дальнейшее развитие и использование средств интеллектуальной автоматизации на стороне пользователя в перспективе позволит разгрузить пользователя от просмотра большого количества нерелевантного контента и при этом увеличить общий объем обрабатываемой информации.

Список используемых источников:

1. 4brain.ru [Электронный ресурс] // Что такое информационный пузырь и как из него выйти (статья). – 2020 – Режим доступа: <https://4brain.ru/blog/information-bubble/>, свободный – Загл. с экрана. – Яз.рус.
2. habr.com [Электронный ресурс] // Как черные SEO-оптимизаторы собирают миллионы посетителей по высоко-актуальным запросам в Яндексе (статья). – 2020. – Режим доступа: <https://habr.com/ru/post/342026/>, свободный – Загл. с экрана. – Яз.рус.
3. систематикус.рф [Электронный ресурс] // Google, Facebook и другие гиганты увеличивают Информационный Пузырь. Как с этим бороться? (статья). – 2020. – Режим доступа: <https://систематикус.рф/2019/08/29/информационный-пузырь-увеличивается/>, свободный – Загл. с экрана. – Яз.рус.

Izryadnov V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Evaluation of the relevance of links in the yandex search engine.

The article discusses the features of the Yandex search engine, which lead to the appearance of irrelevant links in the search results, and ways to optimize the search using software based on the Selenium library.

Key words: *relevance, search engine, links.*

УДК 004.891.2
ГРНТИ 20.53.19

ОБНАРУЖЕНИЕ АНОМАЛИЙ С ПОМОЩЬЮ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Ю. О. Качуровский, Е. Ю. Рузманов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обнаружение аномалий — один из наиболее распространенных вариантов использования машинного обучения. Поиск и идентификация выбросов помогает предотвратить мошенничество, атаки со стороны злоумышленников и вторжения в сеть, которые могут поставить под угрозу будущее компаний. В статье рассмотрены принципы работы обнаружения аномалий и методы машинного обучения.

машинное обучение, аномалии, классификация, метод

Аномалия — это то, что отличается от нормы: отклонение, исключение. В программной инженерии под аномалией подразумевается редкое явление или событие, которое не укладывается в шаблон, поэтому кажется подозрительным [1]. Примеры:

- внезапный всплеск или снижение активности;
- ошибка в тексте;
- внезапное резкое падение или повышение температуры.

Распространенными причинами выбросов являются:

- ошибки предварительной обработки данных;
- шум;
- мошенничество;
- атаки.

Программа должна работать бесперебойно и быть предсказуемой, поэтому каждый выброс представляет собой потенциальную угрозу ее надежности и безопасности. Выявление и идентификация аномалий — это обнаружение аномалий или выбросов.

Существуют следующие типы выбросов:

1. Глобальные выбросы

Когда точка данных принимает значение, выходящее далеко за пределы всех других диапазонов значений точек данных в наборе данных, это можно рассматривать как глобальную аномалию [2]. Другими словами, это редкое событие.

Например, если вы ежемесячно получаете на свой банковский счет среднюю американскую зарплату, но однажды получаете миллион долларов, это будет выглядеть глобальной аномалией для аналитической группы банка, что представлено на рис. 1.



Рис. 1. Пример глобального выброса

2. Контекстные выбросы

Когда выброс называется контекстным, это означает, что его значение не соответствует тому, что мы ожидаем наблюдать для аналогичной точки данных в том же контексте [3]. Контексты обычно временны, и одна и та же ситуация, наблюдаемая в разное время, не может быть исключением.

Например, для магазинов вполне нормально наблюдать увеличение числа покупателей в праздничный сезон. Однако, если внезапный рост происходит вне праздников или распродаж, его можно считать контекстуальным выбросом. Пример представлен на рис. 2.



Рис. 2. Пример контекстных выбросов

3. Коллективные выбросы

Коллективные выбросы представлены подмножеством точек данных, которые отклоняются от нормального поведения.

В целом, технологические компании, как правило, становятся все больше и больше. Некоторые компании могут приходить в упадок, но это не общая тенденция. Однако, если сразу несколько компаний показывают снижение выручки за один и тот же период времени, мы можем выявить коллективный выброс. Пример представлен на рис. 3.

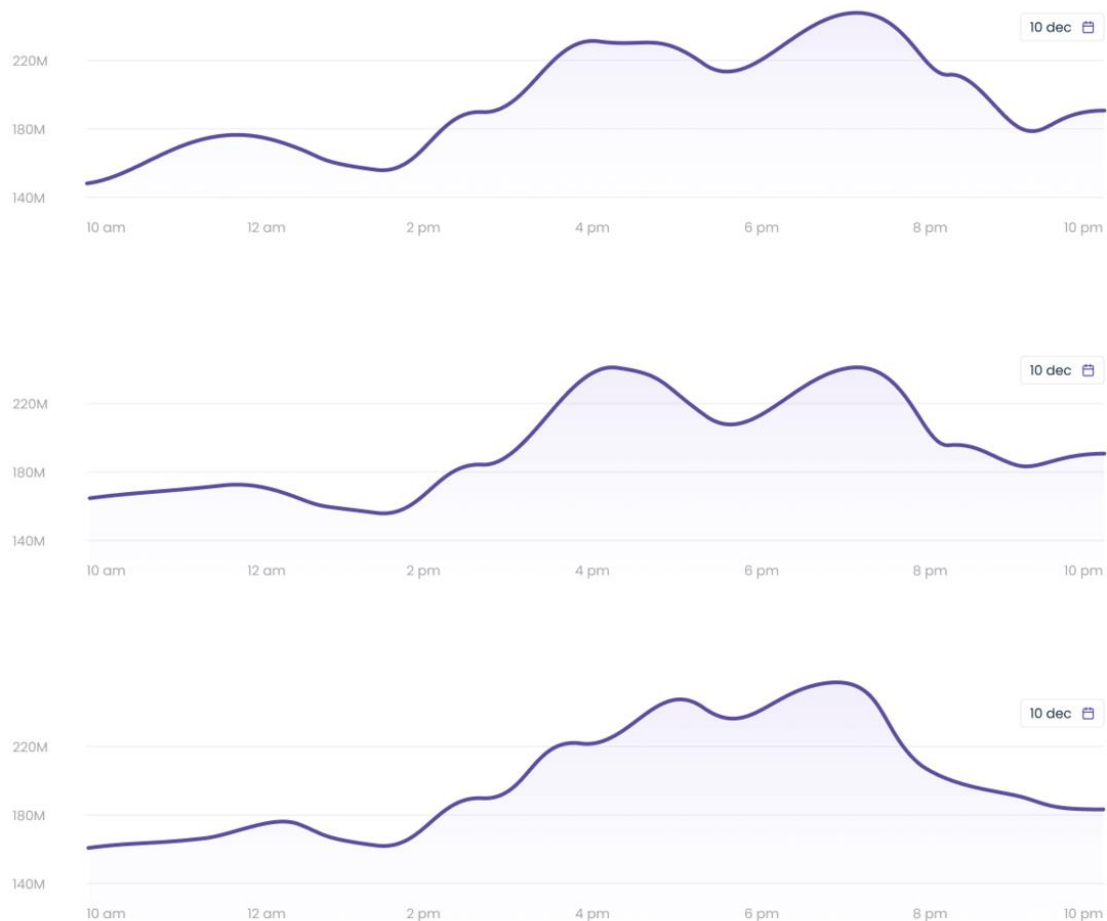


Рис. 3. Пример коллективных выбросов

Существуют следующие методы обнаружения аномалий:

1. Под наблюдением

При контролируемом обнаружении аномалий инженеру машинного обучения нужен обучающий набор данных. Элементы в наборе данных разбиты на две категории: нормальные и ненормальные. Модель будет использовать эти примеры для извлечения закономерностей и сможет обнаруживать аномальные закономерности в ранее невидимых данных.

2. Без присмотра

Этот тип обнаружения аномалий является наиболее распространенным типом, и наиболее известным представителем неконтролируемых алгоритмов являются нейронные сети.

Искусственные нейронные сети позволяют уменьшить объем ручной работы, необходимой для предварительной обработки примеров: не требуется ручная маркировка. Нейронные сети можно применять даже к неструктурированным данным. *NN* могут обнаруживать аномалии в неразмеченных данных и использовать полученные знания при работе с новыми данными.

3. Полуконтролируемый

Методы полуконтролируемого обнаружения аномалий сочетают в себе преимущества предыдущих двух методов. Инженеры могут применять

неконтролируемые методы обучения для автоматизации изучения функций и работы с неструктурированными данными [4]. Однако, сочетая это с человеческим наблюдением, у них есть возможность отслеживать и контролировать, какие шаблоны изучает модель. Обычно это помогает сделать предсказания модели более точными.

Алгоритмы машинного обучения для обнаружения аномалий:

- Фактор локального выброса (*LOF*)
- К-ближайшие соседи
- Машины опорных векторов
- ДБСКАН
- Автоэнкодеры
- Байесовские сети

Обнаружение аномалий — это идентификация точек данных в данных, которые не соответствуют обычным шаблонам. Это может быть полезно для решения многих задач, включая обнаружение мошенничества, медицинскую диагностику и т. д. Методы машинного обучения позволяют автоматизировать обнаружение аномалий и сделать его более эффективным, особенно при работе с большими наборами данных. Некоторые из распространенных методов машинного обучения, используемых для обнаружения аномалий, включают *LOF*, автоэнкодеры и байесовские сети.

Список используемых источников:

1. What is Anomaly Detection in Machine Learning? [Электронный ресурс]. URL: <https://serokell.io/blog/anomaly-detection-in-machine-learning> (дата обращения 22.01.2022).
2. Coluccia, A., D'Alconzo, A., & Ricciato, F. (2013). Distribution-Based Anomaly Detection in Network Traffic. Lecture Notes in Computer Science, 202-2016
3. Stijn Luca, Peter Karsmakers Anomaly Detection Using the Poisson Process Limit for Extremes // Conference: IEEE International Conference on Data Mining At: Shenzhen, China Volume: 14
4. Wagner, Cynthia & Engel, Thomas. (2012). Detecting Anomalies in Netflow Record Time Series by Using a Kernel Function. 7279. 10.1007/978-3-642-30633-4_16.

Kachurovskii I., Ruzman ov E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Anomaly detection using machine learning methods.

Anomaly detection is one of the most common use cases for machine learning. Finding and identifying outliers helps prevent fraud, malicious attacks, and network intrusions that can compromise the future of companies. The article discusses the principles of anomaly detection and machine learning methods.

Key words: machine learning, anomalies, classification, method.

УДК 681.5
ГРНТИ 71.01.85

РАСПРЕДЕЛЕННАЯ СИСТЕМА УПРАВЛЕНИЯ И ЗАЩИТЫ ОТ ВНЕШТАТНЫХ СИТУАЦИЙ

Д. А. Корнюшкин, А. А. Крылов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире крупнейшие производители уже не могут успешно функционировать и развиваться без современных систем управления. Так же в особое внимание следует уделять системам противоаварийной защиты для минимизации рисков на производстве. Внедрение высокотехнологичных решений приводит к увеличению капитализации предприятия и служит залогом успешного развития и роста компании.

АСУ ТП, контроллеры, распределённая система управления, DCS-системы, алгоритмов противоаварийной защиты

Цель исследования:

В 2018 году было запущено производство хлористого калия на Усольском калийном комбинате в Пермском крае. К концу 2021 года в эксплуатацию был введен 31 комбайновый комплекс. АО «МХК «ЕвроХим» является крупнейшим в России производителем минеральных удобрений и хлористого калия.

Производство хлористого калия осуществляется двумя методами флотационным и галургическим.

Технологический процесс переработки руды флотационным способом основывается на особенности поверхности сильвина и галита смачиваться водой, данный эффект достигается при помощи обработки реагентами.

Флотационный метод включает в себя:

- Дробление руды;
- Сушка концентрата;
- Приготовление реагентов;
- Облагораживание гранул;
- Погрузка готовой продукции;
- Размещение производственных отходов в специализированных помещениях;

Технологический процесс переработки руды галургическим методом напрямую зависит от растворимости составляющих.

Галургический метод включает в себя:

- Дробление руды;
- Сушка калия хлористого;
- Перемещение готовой продукции в отсеки для хранения для дальнейшей погрузки;
- Снижение температуры оборотной воды;
- Изготовление реагентов;

• Размещение производственных отходов в специализированных помещениях;

На производстве были выполнены работы по внедрению систем автоматизации:

- проектирование;
- разработка прикладного программного обеспечения АСУ ТП;
- монтажные и пусконаладочные работы;
- предварительные испытания;
- проверка алгоритмов противоаварийных защит (ПАЗ);
- обучение операторов и инженеров АСУ ТП;
- сдача системы в опытную эксплуатацию;
- коррекция программного обеспечения по результатам опытной эксплуатации;
- сборка и отладка шкафов автоматизации;

Назначение и цели создания АСУ ТП:

Автоматизированная система управления технологическим процессом (АСУ ТП) предназначена для контроля, управления технологическим процессом и противоаварийной защиты установки производства хлористого калия (рис. 1).

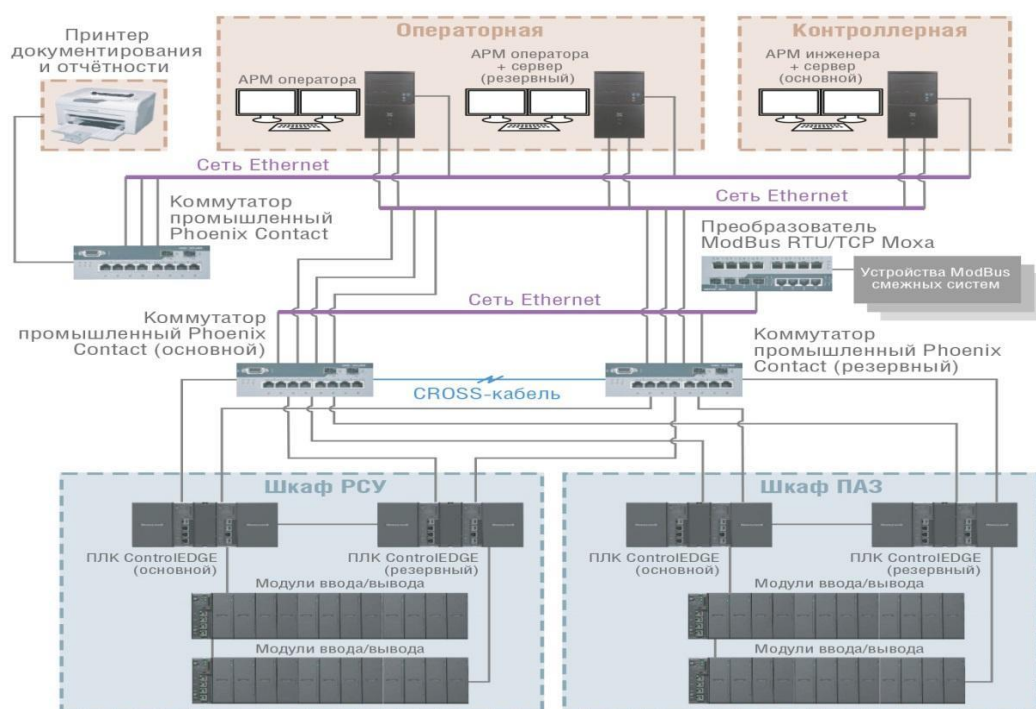


Рис. 1. Структурная схема РСУ и ПАЗ установки производства хлористого калия

Данные о функциональных способностях объекта от дублированных датчиков поступают на систему ПАЗ, при срабатывании любых 2 из 3 датчиков, которые установлены на любой из контрольных точек, является необходимым условием для срабатывания защитной блокировки и применения резервных исполнительных механизмов. У системы ПАЗ есть мобильная инженерная станция, с помощью которой выполняется конфигурирование ПЛК

системы ПАЗ. Со станции оператора РСУ, соединенной с системой ПАЗ через сетевой экран, можно контролировать процесс работы системы ПАЗ, но нельзя ей управлять [1].

РСУ предоставляет возможность связать воедино большое количество оборудования при помощи современных сетей и шин передачи данных. Цифровая сеть позволяет объединить разрозненные компоненты системы в единый программно-аппаратный комплекс. РСУ применяется для управления процессами, приостановка которых не допустима даже на короткое время. Остановка таких процессов неизбежно приведет к остановке добычи руды, приведению в неисправное положение производственного оборудования, а также к возможному возникновению чрезвычайных ситуаций на производстве [2].

АСУ ТП спроектирована на базе контроллеров компании Honeywell для DCS-систем (Distributed Control System – распределённая система управления) и обеспечивает:

- автоматизированный контроль
- управление основными и вспомогательными технологическими процессами установки в режиме реального времени;
- автоматическую защиту оборудования объекта;
- выполнение контроля в соответствии с заданными параметрами производства
- целесообразное управления режимами работы оборудования.

Архитектуру подобной информационной системы управления предприятием, можно представить, как совокупность взаимодействующих друг с другом открытых подсистем, каждая из которых реализована в виде стандартной коробочной или самостоятельно разработанной информационной подсистемы определенного вида [1,2].

В случае если у оператора возникает потребность произвести корректировочные действия, система автоматически запросит подтверждение действия, для исключения не вынужденных ошибок и человеческого фактора. В случае принятия оператором ошибочного решения будет произведена диагностика, которая в свою очередь будет сопровождена оповещением.

Описание технического решения:

Данная система разработана как распределённая информационно-управляющая система, использующая симбиоз человека и машины, таким образом, нивелируя недостатки гибкости работы автоматического комплекса и потенциальных ошибок оператора [3].

В качестве компонентной базы унифицированных комплексов технических средств контроля, управления и противоаварийной защиты использованы гибридные резервируемые ПЛК нового поколения семейства Control-EDGE компании Honeywell в варианте РСУ.

Принцип работы:

Верхний уровень АСУ ТП

Выполняет следующие функции:

- сервер базы данных конфигурации обеспечивает централизованное хранение конфигурации программно-технического комплекса (ПТК) АСУ ТП;
- обмен информации между контроллерами и АРМ ПТК происходит через сервер связи, используется для снижения нагрузки на контроллеры путём перераспределения коммуникационных функций;
- сервер ОРС обеспечивает обмен данными с внешними системами по протоколам ОРС;
- сервер истории обеспечивает долгосрочное хранение информации об изменении параметров технологического процесса, информация сохраняется в виде кольцевого буфера.

Рабочая станция оператора (АРМ оператора) представляет собой интерфейс операторов-технологов, реализованный на базе ПО Honeywell PlantCruise.

Инженерная станция АСУ ТП (АРМ РСУ, ПА3) выполняет функции рабочего места инженера АСУ ТП и при необходимости АРМ оператора или инженера КИП. Все данные конфигурации, наладки и эксплуатации хранятся централизованно на сервере базы данных, а создаются и редактируются на рабочих местах инженера (АРМ РСУ).

Сеть управления – двухсторонняя высокоскоростная выделенная локальная сеть данных Ethernet, которая работает со скоростью передачи данных 1 Гб/с по протоколу TCP/IP. Она обеспечивает связь серверов, АРМ, контроллеров [4].

Средний уровень АСУ ТП

Состоит из контроллеров, коммуникационных интерфейсов полевых сетей, модулей ввода/вывода, реле, клемм. Основной блок ЦПУ реализует функции исполнения кода приложений, резервный блок ЦПУ постоянно обновляется, так что он всегда готов взять на себя исполнение кода в случае отказа основного блока.

Аппаратная часть контроллера состоит из

- Два устройства ЦПУ
- Устройства расширения для коммуникационных интерфейсов.

Питание контроллеров и системы ввода/вывода осуществляется от резервированных источников питания. Для сигналов, подключённых непосредственно на модуль ввода/вывода, защита от короткого замыкания обеспечивается самим модулем [5]. Для сигналов, подключённых через промежуточные реле, защита обеспечивается предохранителями, установленными в промежуточных клеммах.

Шкафы АСУ ТП поставлены в сборе и полностью укомплектованы (компоненты системы управления, конструктив шкафа, кабели питания и заземления, автоматические выключатели, предохранители, клеммы, блоки питания, осветительная арматура, маркировка).

Заключение:

Показателем преобразования и применения современной системы управления базирующейся на контроллерном оборудовании стал рост производительности, снижение количества аварийных ситуаций, повышение качества выпускаемой продукции. Грамотно выстроенная компонентная база

системы АСУ ТП даёт возможность лёгкой интеграции высокотехнологичных MES-систем.

Средством достижения лидирующего положения в отрасли является координация сложных взаимосвязей, определяющих предложение, спрос и реализацию намеченных планов.

Необходимо отметить, что процесс внедрения распределительных систем управления и защиты от внештатных ситуаций на производстве должен осуществляться в соответствии с утвержденным планом, в комплексе и на всех уровнях.

В результате исследования установлено, что для получения максимального эффекта от системы управления и защиты от внештатных ситуаций необходима информационно-управляющая система, нивелирующая недостатки гибкости работы автоматического комплекса и потенциальных ошибок человека. Это позволит уменьшить финансовые потери на всех этапах производства и минимизирует финансовые издержки, затрачиваемые на устранение внештатных ситуаций, а также позволит избежать простоя производственной линии. Устойчивое функционирование всех перечисленных процессов является главной задачей представленной ранее системы.

Список используемых источников:

1. Клепиков В. И., Калинин С. В., Захаров Н. А., Подхватилин Д. С. Архитектура распределенных систем управления жесткого реального времени // Радиоэлектронные и компьютерные системы. 2008. №5. С. 57–61.
2. Перухин М. Ю., Ягьяева Л. Т., Обади Абдулфаттах. Высокоскоростные распределенные сети // Вестник Казанского технологического университета. 2013. №6. С. 240-241.
3. Швецов А. Н., Яковлев С. А. Распределенные интеллектуальные информационные системы. СПб. : Изд-во СПбГЭТУ «ЛЭТИ», 2003. 318 с.
4. Ожерельева Т. А. Структурный анализ систем управления // Государственный советник. 2015. №1. С. 40-44.
5. Воронин А. А., Мишин С. П. Модель оптимального управления структурными изменениями организационной системы // Автоматика и телемеханика. 2002. №. 8. С. 136-150.

Kornyushkin D., Krylov A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Distributed control and emergency protection system.

In the modern world the largest manufacturers cannot function and develop successfully without up-to-date control systems. In the same way, special attention has to be paid to safety systems in order to minimise risks in production. The implementation of high-tech solutions leads to an increase in the capitalisation of the company and serves as a guarantee for the successful development and growth of the company.

Key words: process control systems, controllers, distributed control system, DCS systems, emergency protection algorithms.

УДК 378.147
ГРНТИ 50.41.29

СЕМАНТИЧЕСКИЙ РАЗБОР ТЕКСТОВ С ПОМОЩЬЮ ИСКУССТВЕННЫХ НЕЙРОСЕТЕЙ

Е. В. Кривоногова, Г. А. Рябов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время увеличивается объем сведений, хранимых в современных информационных системах, что приводит к созданию эффективных методов обработки текстов на естественном языке, а также системы автоматизированного анализа и поиска информации. В связи с этим в статье рассматриваются современные методы семантического разбора текстов с использованием искусственных нейронных сетей.

семантический разбор, нейронная сеть, векторное представление, алгоритм CBOW, алгоритм skip-gram.

Быстрый рост объемов и разнообразия сведений, хранимых в современных информационных системах (ИС), расширение функциональных возможностей этих систем привели к тому, что среди их пользователей появляются все новые категории, не связанные ни с вычислительной техникой, ни с информационными технологиями. Поэтому дальнейшее развитие ИС требует создания эффективных методов общения с пользователем (пользовательского интерфейса) человеко-ориентированным образом, в частности, обработки текстов на естественном языке, а также системы автоматизированного анализа и поиска информации. Сегодня на смену статистическим алгоритмам приходят алгоритмы семантического индексирования [1], в которых важная роль отводится непосредственно семантическому разбору текста.

Семантический разбор – это этап в последовательности действий алгоритма автоматического понимания текстов, заключающийся в выделении семантических отношений между словами или фрагментами текста, формировании семантического описания и представления текстов.

Использование нейросетевых методов при работе с лексическими единицами напрямую пока не видится возможным, поэтому возникает необходимость каждому используемому в тексте слову сопоставить число – т.е. закодировать слово [2, 3].

Использование целочисленного кодирования (например, порядковый номер слова в словаре) может:

- создавать ложные корреляции, т.к. такая кодировка упорядочена;
- затруднить анализ результатов, когда нейросеть, например, предсказывает на выходе с примерно одинаковой вероятностью слово A с индексом $N1$ или слово B с индексом $N2$ – в данном случае ложным результатом будет не имеющее с ними ничего общего слово B со «средним» индексом $(N1+N2)/2$.

Поэтому вместо целочисленного кодирования лучше применять так называемое «быстрое кодирование» (англ. *one-hot encoding*) – представление слова в виде битового вектора. Длина вектора (число бит) равна числу слов в словаре. Все биты, кроме одного, имеют значение 0. У первого слова первый бит равен 1, у второго слова второй бит равен 1 и т.д. Для практической реализации быстрого кодирования существуют различные алгоритмы, встроенные в библиотеки для машинного обучения и обработки естественного языка. Такие алгоритмы есть, например, в библиотеках *pandas* и *sklearn*.

Недостатками такого метода кодировки являются большие затраты памяти для объемных словарей и изменение кодировки всех слов при добавлении новых слов в словарь [2,3,4,5].

Их можно устранить с помощью векторного представления слов. Векторное представление – общее название для различных подходов к моделированию и обработке естественного языка, направленных на сопоставление словам из некоторого словаря векторов из условного пространства R^n (словесного векторного пространства) для определенного числа n , значительно меньшего, чем количество слов в словаре [6]. Теоретической базой для векторных представлений является дистрибутивная семантика – область лингвистики, которая занимается вычислением степени семантической близости между лингвистическими единицами на основании их распределения (дистрибуции) в больших массивах лингвистических данных (текстовых корпусах).

В рамках метода дистрибутивной семантики к текстам изучаемого языка применяется упорядоченный набор универсальных процедур, что позволяет выделить основные единицы языка (фонемы, морфемы, слова, словосочетания), провести их классификацию и установить отношения сочетаемости между ними. Классификация при этом основывается на принципе замещения: языковые единицы относятся к одному и тому же классу, если они могут выступать в одних и тех же контекстах (т.н. дистрибутивная гипотеза). При построении словесного векторного пространства векторы соответствуют лингвистическим единицам (словам или словосочетаниям), а измерения соответствуют контекстам. Выбор пространства контекстных признаков определяется поставленной задачей [7].

Одним из наиболее распространенных методов получения векторного представления слова (*word embedding*) на естественном языке является *Word2Vec*. Идея метода заключается в следующем:

1. на основе корпуса текстов строится словарь, для каждого слова в словаре определяется встречаемость;
2. редкие слова удаляются из словаря;
3. из корпуса вычленяется так называемое субпредложение – некий базовый элемент корпуса, которым может быть как предложение, так и абзац или целая новостная статья. На основе субпредложения проводится субсэмплирование – изъятие наиболее частотных слов. Это позволяет исключить из рассмотрения предлоги, союзы, служебные глаголы и т.п., не несущие самостоятельной смысловой нагрузки, и тем самым улучшить качество получающейся модели;

4. субпредложение анализируется с помощью одного из двух алгоритмов – *CBOW* или *skip-gram*. Алгоритм *CBOW* (англ. *Continuos Bag Of Words*, непрерывный мешок слов) основан на предсказании слова из контекста. Обучение нейросети строится на предсказании пропущенного слова в предложении. Алгоритм *skip-gram* строится на предсказании контекста по слову, а обучение нейросети строится на поиске слов, которые чаще всего встречаются в одном предложении рядом с выбранным [6, 7].

Выбор алгоритма (*CBOW* или *skip-gram*) определяет структуру нейросети.

При использовании алгоритма *CBOW* у нейросети есть N входов, на которые подаются слова суб-предложения, формирующие контекст. На выходе нейросеть предсказывает слово, которое с наибольшей вероятностью должно появиться в данном контексте.

При использовании алгоритма *skip-gram* (сокращенное от *k-skip n-gram*, последовательность длиной n элементов, n -грамма, где элементы находятся на расстоянии не более, чем k друг от друга) у нейросети есть один вход, на который последовательно подаются слова субпредложения. На выходе нейронная сеть предсказывает n -граммы, в которые с наибольшей вероятностью будет входить слово.

Алгоритм *CBOW* позволяет обучать нейросеть быстрее, но алгоритм *skip-gram* обеспечивает высокую точность предсказания связи слова с контекстом независимо от частоты появления слова в корпусе.

Кроме алгоритма, в методе *Word2Vec* есть еще один гиперпараметр – функция активации нейросети. Как правило, это либо *negative sampling*, либо *hierarchical softmax* (в редких случаях они могут использоваться совместно).

При использовании *negative sampling* каждому возможному прогнозу соответствует один выходной узел сети. Чтобы улучшить то предсказание, которое создает определенный входной контекст, проверяются выходные узлы для «правильного» слова (текущего фрагмента учебного примера) и для N других «неправильных» слов (которые не соответствуют текущему учебному примеру). Затем корректируются внутренние весовые коэффициенты сети и входные векторы, чтобы сделать «правильную» активацию выходного узла слова немного более сильной, а N «неправильных» активаций выходных узлов слова немного более слабыми. При этом рассматриваются не все возможные «неправильные» варианты, а относительно небольшое их число.

При использовании *hierarchical softmax* вместо рассмотрения отдельных выходных узлов, каждому из которых соответствует свое предсказываемое слово, некоторое шаблонное значение множественных активаций выходных узлов интерпретируется как конкретное слово. Это позволяет довольно точно определить прогнозируемое слово, но замедляет время обучения при работе с большими словарями, потому что среднее число узлов, участвующих в каждом примере обучения, растет.

При применении *negative sampling* всегда используется $N + 1$ узлов (один «правильный» и N «неправильных»), поэтому при работе с большим корпусом текстов его использование предпочтительнее [7, 8].

Резюмируя, можно отметить, что для первоначальной задачи классификации текстов вполне достаточно быстрого кодирования (*one-hot encoding*). Например, текст имеет тему XI , если в нем присутствуют слова $A1, A2, \dots, AM$. Сумма битовых векторов отдельных слов-признаков дает уникальный битовый вектор темы. Хотя на практике такой подход далеко не всегда работает корректно из-за наличия слов-синонимов.

А для обучения искусственных нейронных сетей задачам семантического разбора, помимо быстрого кодирования, обязательно использование и векторного представления, что выдает метод *Word2Vec* или аналогичные ему. При этом для формирования уникального идентификатора слова вполне может использоваться и *one-hot encoding*, которому затем нужно поставить в соответствие векторное представление данного слова.

Список используемых источников:

1. Семантический анализ текста с применением нейросетевого анализа. морфологии и синтаксиса (электронный ресурс) URL: <https://cyberleninka.ru/article/n/semanticheskij-analiz-z-primeneniem-neyrosetevogo-analiza-morfologii-i-sintaksisa>.
2. А. Мамон Источники семантики: обзор инструментов и сервисов, анализ эффективности (электронный ресурс) URL: <http://semyadro.pro/osnovy/istochniki-semantiki-obzor-instrumentov-i-servisov-analiz-effektivnosti-3>.
3. Максимов, Н.В. Семантическое ядро цифровой платформы / Н.В. Максимов, О.Л. Голицына, М.Г. Ганчева, Д.В. Санатов // Онтология проектирования. – 2018. – Т.8, №3(29). С.412-426. – DOI: 10.18287/2223-9537-2018-8-3-412-426.
4. Вьюгин В.В. Математические основы машинного обучения и прогнозирования. М.: МЦНМО, 2013. – 304 с.
5. Педро Домингос Верховный алгоритм: как машинное обучение изменит наш мир; пер. с англ. В.Горохова; М.: Манн, Иванов и Фербер, 2016. – 336 с.
6. Архитектура модели *Word2Vec*: основы NLP-нейросетей (электронный ресурс) URL: <https://python-school.ru/blog/what-is-word2vec/>.
7. *Word2Vec* применение векторных семантических моделей языка (электронный ресурс) URL: <https://sysblok.ru/knowhow/obuchaem-word2vec-praktikum-po-sozdaniju-vektornyh-modelej-jazyka/>.
8. Colledanchise M., Ogren P. Behavior Trees in Robotics and AI: An Introduction. – CRC Press. – 2018. – 208 p.

Krivosogova E., Ryabov G.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Semantic analysis of texts with the help of artificial neural networks.

Currently, the volume of information stored in modern information systems is increasing, which leads to the creation of effective methods for processing texts in natural language, as well as systems for automated analysis and information retrieval. In this regard, the article discusses modern methods of semantic analysis of texts using artificial neural networks.

Key words: *semantic parsing, neural network, vector representation, CBOW algorithm, skip-gram algorithm.*

УДК 004.891.2
ГРНТИ 28.23.35

ПРОБЛЕМЫ ПРИМЕНЕНИЯ И РАЗРАБОТКИ ЭКСПЕРТНЫХ СИСТЕМ. ИСПОЛЬЗОВАНИЕ ЭКСПЕРТНЫХ СИСТЕМ В КРИМИНАЛИСТИКЕ

А. М. Лешукова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье раскрывается понятие экспертной системы. Рассматриваются проблемы применения и разработки экспертных систем, а также применение таких систем в криминалистической практике на конкретных примерах.

интеллектуальные технологии, экспертная система, база знаний, предметная область

Интеллектуальные технологии работают по принципу анализа сути проблемы и поиска путей её решения. Подход заключается в том, что необходимо описать предметную область и уже на основании описания предметной области можно начинать строить интеллектуальную систему.

Интеллектуальные технологии основываются на обработке знаний. Под знаниями может предполагаться абсолютно любая информация, например любые понятия, предметная область, объект или явления. И на основе полученных данных строится база знаний (БЗ). Соответственно система, в которой главной составляющей является база знаний, должна быть описана на языке сверхвысокого уровня [3].

Одним из примеров такой интеллектуальной технологии является экспертная система (ЭС). Её главной функцией является решение вопросов по извлечению и структурированию знаний. Также эта система берёт на себя технологические аспекты разработки системы, которые основаны на представлении знаний.

Современные ЭС – это сложные программные комплексы, задача которых накапливать знания специалистов (экспертов) в конкретных предметных областях и передавать собранный опыт менее квалифицированным пользователям.

Экспертная система имеет два этапа реализации: формализация знаний и формирование базы знаний.

В начале эксперт преобразует необходимые знания в форму, подходящую для выбранной модели представления знаний. И уже на основе преобразованных знаний формируется БЗ, путем вложения формализованных знаний в программную систему.

Интеллектуальные системы имеют способ логического вывода, а именно на основании применения метода дедукции, могут решить определенную задачу и выдать пользователю ответ, основываясь на своей базе знаний. Такие системы

хороши тем, что они могут анализировать информацию и выдвигать решения, абстрагируясь от человеческого фактора.

Такие экспертные системы широко развиты по ряду причин. В первую очередь они позволяют использовать знания тех специалистов, которых недостаточно в организации, таким образом нейтрализуя кадровую нехватку. Также ЭС используются там, где нецелесообразно использовать обычную программную систему, такое происходит, когда задача требует полного анализа сложного набора условий.

Но для создания экспертной системы необходимо наличие экспертов, готовых поделиться своим опытом. Соблюсти это условие не всегда удается потому, что некоторые эксперты боятся делиться своими знаниями, опасаясь, что в итоге их заменит программная система. Но подобных случаев крайне мало.

Задачи, к которым применяются экспертные системы, как правило, относятся к области диагностики. Если задача носит вычислительный характер, то она базируется на тех факторах, к которым не применима ЭС.

Еще одним недостатком является вопросно-ответный режим системы. Такой режим является достаточно медленным, но иногда единственным верным для решения задачи.

Таким образом можно сформулировать определение. Экспертная система – это набор программ, выполняющих функции эксперта при решении задач из некоторой предметной области.

Структура экспертной системы состоит из базы знаний, механизма логического вывода и подсистем, которые выполняют функции диалога, пополнения БЗ, моделирования и другие [1].

Экспертные системы широко используются во многих областях, таких как экономика, медицина, образование, промышленность, психология и другие.

Таким системам было найдено применение и в такой важной области, как уголовное право. Экспертные правовые системы (ЭПС) активно используются в следственной практике.

С помощью ЭПС стало возможно прогнозировать преступления, устанавливать личность преступника, анализировать место преступления, раскрывать кражи и другое.

Экспертные системы отчасти выполняют функцию по профилированию. Зарубежные криминалисты, например в США уже давно и эффективно используют способ профилирования преступлений, который значительно, с момента создания первого отдела в 1977 году, увеличил процент раскрываемости преступлений. Этот способ заключается в сборе информации, полученной путем бесед с уже арестованными преступниками. Полученные знания структурируются и в дальнейшем используются при раскрытии новых дел.

На практике в России до сих пор к этой методике, как и к составлению психологического портрета относятся предвзято и используют редко, только если следствие окончательно зашло в тупик. Следовательно, экспертов в этой области крайне мало. И решить эту проблему помогает ЭС, которая заменяет специалиста по профилированию. Имея постоянно пополняющуюся базу знаний

о совершенных преступлениях, получая новые вводные о не раскрытом деле, система эффективно помогает в расследовании.

Такая ЭС получила название «Маньяк». Первая версия этой системы была создана сотрудниками ВНИИ МВД РФ совместно с Учебно-научным производственным Центром "ЮрИнфоР" юридического факультета МГУ им. М. В. Ломоносова [2]. Кроме помощи в следствии эта систем применяется в обучение будущих оперативников и следователей.

Помимо ЭС «Маньяк» существуют и другие системы, дале в статье приведена кратка характеристика.

ЭС «Грабитель» предназначена для расследования грабежей и разбоев. ЭС «Блок» используется для борьбы в области экономических преступлений, позволяет расследовать хищения в строительстве с использованием экономических, технологических, товароведческих, бухгалтерских, оперативных материалов и признаков, а также данных о лицах и документах в этой области. ЭС «Автоэкс» проводит экспертизу дорожно-транспортных происшествий. И анализирует, мог ли виновник ДТП предотвратить происшествие. ЭС «Поиск» помогает установить личность преступника, что упрощает его поиск. Система получает первичные данные с места прошествия, анализирует их и выдает версии о личности преступника. Использование этой системы значительно сокращает круг подозреваемых.

Таким образом, несмотря на некоторые недостатки экспертные системы значительно могут упростить процесс работы. Более того ЭС могут быть реализованы в абсолютно любой сфере. Поэтому можно сделать вывод, что в будущем будет реализовано еще больше разновидностей данной системы, и эта тема будет актуальна еще многие годы.

Список используемых источников:

1. Буряченко В. В. Материалы курса Интеллектуальные системы и технологии СибГУ им. М.Ф. Решетнева " – 2021г.
2. Информатика и математика для юристов [Электронный ресурс]. URL: https://studref.com/455083/informatika/informatika_i_matematika_dlya_yuristov/ (дата обращения 12.11.2022).
3. Морозов В. А., Паутов В. И. Представление знаний в экспертных системах/ Учебное пособие Уральский Федеральный университет – 2017г.

Leshukova A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Problems of application and development of expert systems. The use of expert systems in criminology.

The article reveals a closed expert system. The problems and development of expert systems, as well as the use of such systems in forensic practice are considered on specific examples.

Key words: *intelligent technologies, expert system, knowledge server, subject area.*

УДК 004.946
ГРНТИ 28.17.33

РАЗВЕРТЫВАНИЕ МИКРОСЕРВИСНОЙ СИСТЕМЫ УПРАВЛЕНИЯ КОНТЕНТОМ В СИСТЕМАХ РАСПРЕДЕЛЕННОГО РЕЕСТРА

Г. И. Марзаганов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В представленном докладе рассмотрена концепция развертывания системы по управлению контентом с помощью распределенного реестра. Такая концепция позволит создать информационную систему, ключевой особенностью которой является отсутствие единого центра управления баз данных. Такой подход разработки и развертывания позволит добиться отказоустойчивости информационной системы.

распределенный реестр, распределенная система, киберсреда, система управления контентом

Особенностью развертывания приложения распределенного реестра по сравнению с традиционными решениями является то, что каждый участник такой системы развернут на разных рабочих станциях и хранит синхронизированную копию базы данных. Каждый участник системы может вносить изменения в свою базу данных независимо от других станций. После чего высылает новые изменения на валидацию данных всем участникам для добавления изменений в систему, а остальные узлы реестра голосуют за внесение изменений, и реестр дополняется новыми данными при достижении консенсуса, или отбрасывает их. Каждый участник сети при этом синхронизируется с реестром – получает новую копию базы данных с внесенными изменениями, что позволяет добиться повышенной отказоустойчивости информационной системы – гарантирует невозможность подделки данных при определенной доле достоверных узлов.

В данном докладе описан подход к созданию программного модуля для развертывания микросервисной системы управления контентом, архитектура которой рассмотрена в докладе [1], а ее концепция применения в открытых цифровых системах рассмотрена в докладе [2].

Распределенный реестр – это технология хранения данных, которая распределяет информацию среди множества узлов связи или между вычислительными устройствами. Такая схема распределения имеет несколько ключевых особенностей:

- отсутствие центрального администратора;
- совместное использование с синхронизацией по заданному алгоритму;
- децентрализованное географическое распределение копий базы данных

между всеми узлами связи.

По своей сути это первая база данных, которая лишает необходимости задействовать центральный сервис, распределяет базу по всем узлам связи, возлагая на них ответственность за поддержку системы и проверку информации [3, 4]. Концепт узлов распределенного реестра предоставлен на рис. 1.

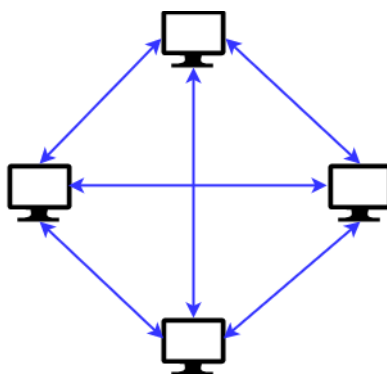


Рис. 1. Концепт узлов распределенного реестра

На рис. 2 предоставлена общая структура организации и синхронизации модуля распределенного реестра, находящимся поверх архитектуры приложения. Модуль состоит из двух объектов:

- API – объект, отвечающий за отправку и получения запросов с других узлов распределенного реестра.
- DistributedLedgerNode – объект, отвечающий за оповещение всех узлов о попытке изменении реестра в связи с новыми данными, вынесении решения за внесения данных в реестр и сохранение новых данных в свою базу данных или полной замены всех данных.

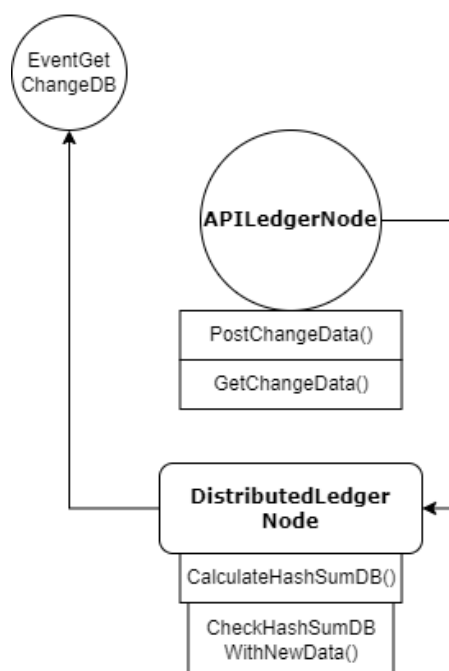


Рис. 2. Общая структура организации и синхронизации модуля распределенного реестра

После получения события об изменении базы данной, происходит оповещение всех узлов распределенного по средствам рассылки на каждый адрес развертывания приложения. Оповещение в себе содержит добавляемые новые данные в реестр, хэш-сумма новой измененной базы данных, и токен аутентификации пользователя.

Другие узлы, получившие оповещения, проверяют токен аутентификации пользователя со своими записями, вычисляют хэш-сумму своей базы данных с

новыми изменениями, и если аутентификация прошла проверку, и хэш-сумма базы данных уведомителя совпадает с хэш-суммой базы данных оповещаемого, то выносится положительный результат об изменении реестра.

Если же токен аутентификации не прошел проверку или высланная хэш-сумма разнится, то изменения отклоняются и узлом оглашается отрицательный результат. Результат сообщается всем узлам по средствам рассылки.

Каждый узел собирает статистику о результатах решения внесения изменений в распределённый реестр. При получении всей статистики каждый узел решает, как поступить:

- При непрошедшей проверке токена аутентификации, узел-отправитель изменений удаляет в своей базе данных новые данные, а остальные отклоняют их.

- При непрошедшей проверке хэш-суммы, изменения отклоняются и высылается копия базы данных узлу-отправителю в связи с несанкционированным изменением базы данных.

Список используемых источников:

1. Акимов С.В., Амелеченко Д. О., Марзаганов Г. И. - Разработка управления контентом с помощью микросервисной архитектуры // Сборник лучших докладов конференции «Подготовка профессиональных кадров в магистратуре для цифровой экономики 2021» Санкт-Петербург, 2021.

2. Акимов С.В., Амелеченко Д. О., Марзаганов Г. И. - Концепция применения MicroCMS в открытых цифровых системах // Сборник научных статей XI международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» Санкт-Петербург, 2022.

3. Технологии распределенного реестра. Подход к созданию баз данных, ключевой особенностью которого является отсутствие единого центра управления [Электронный ресурс].

URL: https://cdto.wiki/%D0%A2%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE_%D1%80%D0%B5%D0%B5%D1%81%D1%82%D1%80%D0%B0 (дата последнего обращения: 13.11.2022).

4. Технология распределенного реестра простыми словами. [Электронный ресурс]. URL: <https://blog-money.ru/resursy/sistemy-raspredeleennogo-reestra.html> (дата последнего обращения: 14.11.2022).

Marzaganov G.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Deployment of a micro-service content management system in distributed registry systems.

Deploying a microservice system for content management in distributed register systems.

In the presented report, the concept of deploying a content management system using a distributed registry is considered. Such a concept will make it possible to create an information system, the key feature of which is the absence of a single database control center. This approach to development and deployment will achieve fault tolerance of the information system.

Key words: *distributed registry, distributed system, cyber environment, content management system*

УДК 004.032.24
ГРНТИ 20.15.05

МЕТОД УВЕЛИЧЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ СИСТЕМЫ: БЛОКИ ВОССТАНОВЛЕНИЯ КОНСЕНСУСА

А. А. Марченко

Санкт-петербургский государственный морской технический университет

Для увеличения уровня отказоустойчивости компьютерных систем используются различные аппаратные и программные методы. К числу наиболее востребованных программных относятся такие как N -версионное программирование, контрольные точки, разделение системы на модули, дублирование процессов, переход на другие версии программного обеспечения. Для обработки ошибок и восстановления системы используется метод блоков восстановления консенсуса, основанный на алгоритме принятия решений по предыдущим результатам работы программы [1].

отказоустойчивость, системы управления, консенсус

Отличие метода блоков восстановления консенсуса от ранее указанных методов состоит в том, что вместо процедуры голосования применяется более продвинутая процедура принятия оптимального решения, а алгоритмы используют технологии машинного обучения, и корректируются вручную [2].

Для каждого датчика на базе предыдущих результатов его работы расставляются коэффициенты: если датчик чаще давал предположительно верные результаты, то его влияние на будущие результаты программы увеличивается.

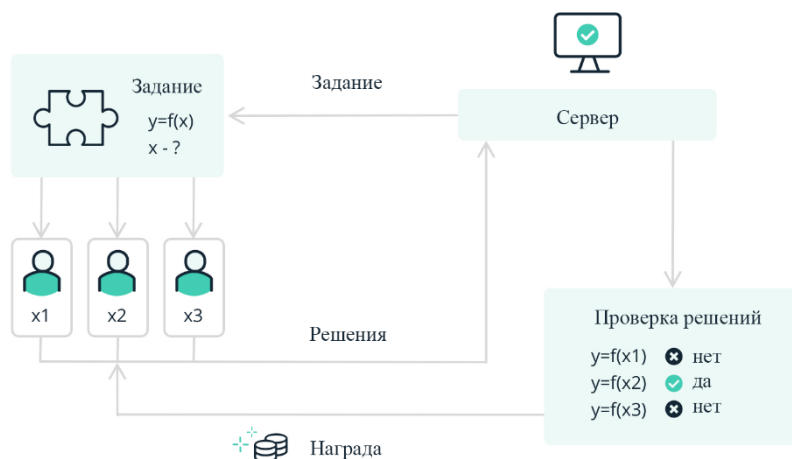


Рис. 1. метод достижения консенсуса подтверждением выполнения работы

Для расставления коэффициентов приоритетности данных могут использоваться следующие методы [3]:

- подтверждение выполнения работы;
- подтверждение доли;
- арендованное подтверждение доли;

- делегированное подтверждение доли;
- подтверждение важности.

Программа, реализующая возможные методы обеспечения отказоустойчивости к системе управления подводным аппаратом описывается следующим образом.

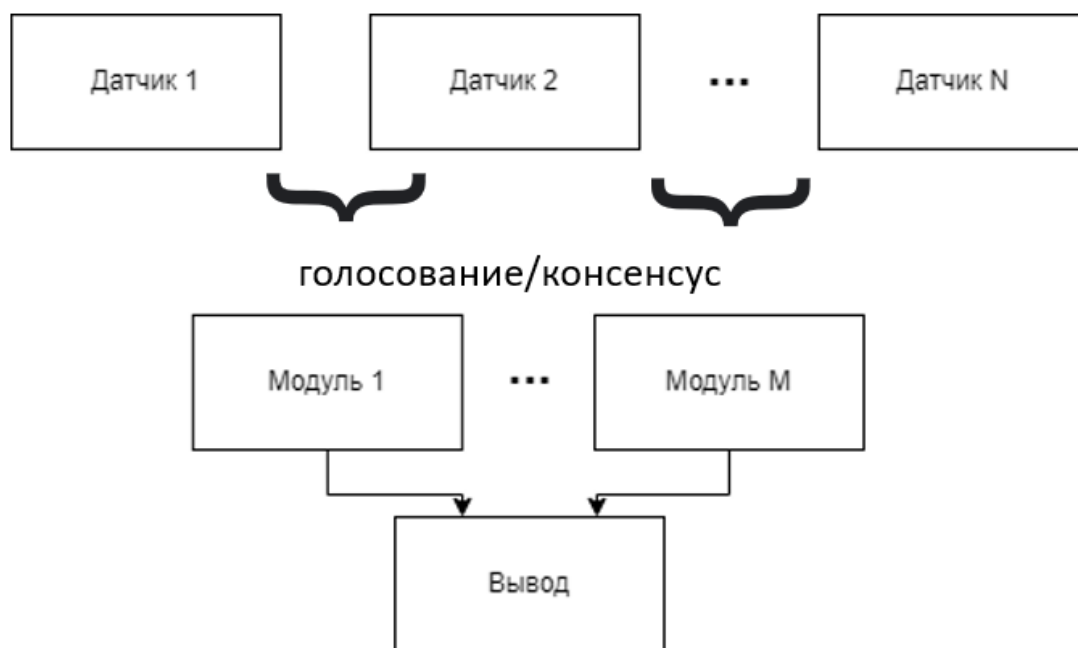


Рис. 2. Структура программы

Программа работает по следующему алгоритму:

1. создается определенное количество датчиков, предположительно расположенных в разных системах подводного объекта. Каждый из датчиков с определенной вероятностью показывает ошибку;
2. они распределяются по модулям, каждый из которых объединяет данные датчиков, подключенных к нему;
3. если хотя-бы один из модулей показывает ошибку, то решение программы считается неверным;
4. проводятся 1000 тестов, для того чтобы увидеть вероятность возникновения ошибок.

Тестирование проводится следующим образом:

1. без группировки датчиков в модули (без применения отказоустойчивости)
2. при объединении датчиков в модули используется метод голосования, где значение модуля определяется большинством
3. при объединении датчиков в модули используется один из методов нахождения консенсуса

Результаты тестов с динамическими параметрами представлены на графиках:

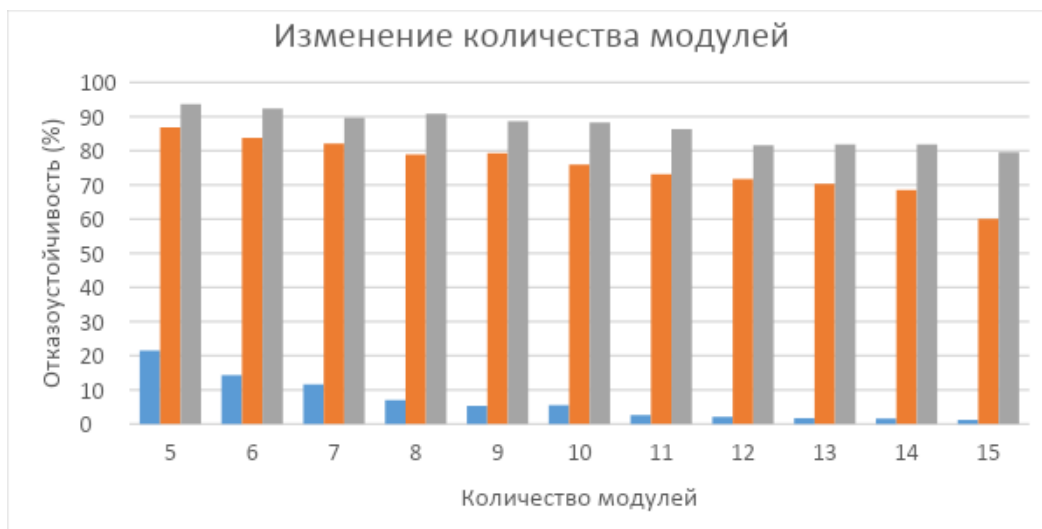


Рис. 3. График зависимости уровня отказоустойчивости от количества модулей

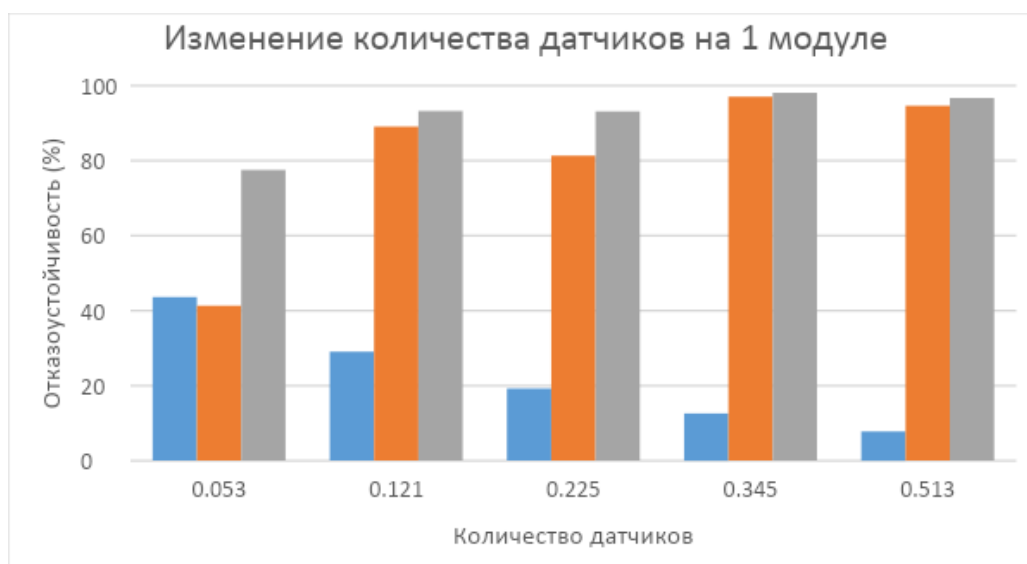


Рис. 4. График зависимости уровня отказоустойчивости от количества датчиков на 1 модуле

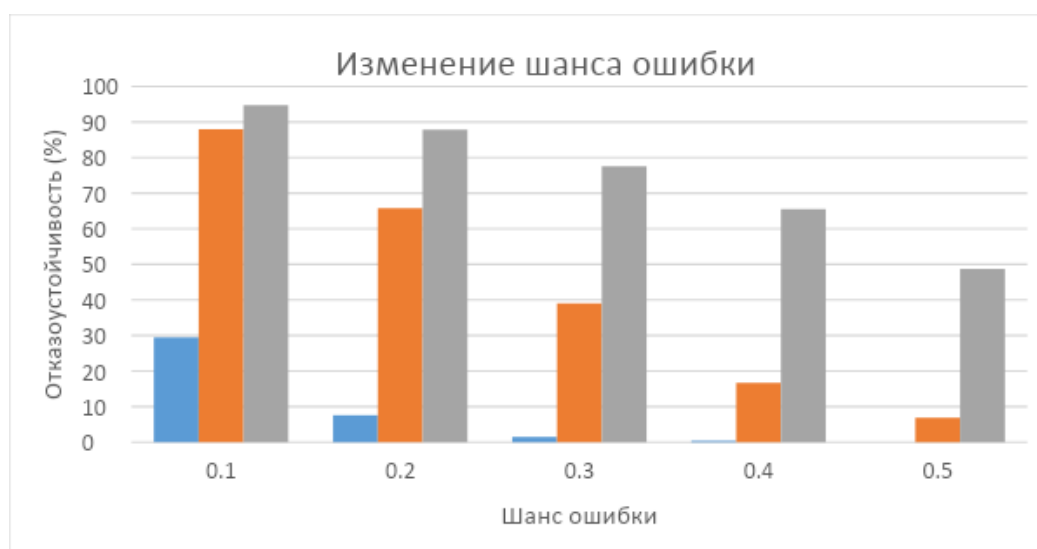


Рис. 5. График зависимости уровня отказоустойчивости от изменения шанса ошибки

По результатам работы программы видно, что метод блоков восстановления консенсуса дает более высокие результаты уровня отказоустойчивости, чем метод голосования и система без применения каких-либо методов отказоустойчивости. Однако стоит отметить, что модель является базовой, и в более сложных системах успешность применения метода будет зависеть от применяемых методов обучения.

Список используемых источников:

1. Michael g. Daughan - Seawolf Submarine Ship Control System: A Case Study of a Fault-Tolerant Design - Naval Engineers Journal, January 1994.
2. Егор Сергеевич Согомоян. Самопроверяемые устройства и отказоустойчивые системы. — Радио и связь, 1989. — 207 с. — ISBN 9785256003081.
3. Механизмы достижения консенсуса в блокчейне - Cassius-WavesPlatfor 2017.

Marchenko A.

Saint-Petersburg State Marine Technical University

A method to increase system fault tolerance: consensus recovery units.

Various hardware and software methods are used to increase the level of fault tolerance of computer systems. Some of the most popular software methods are N-version programming, checkpoints, dividing a system into modules, duplication of processes, migration to other software versions. For error handling and system recovery, the consensus recovery block method, based on a decision-making algorithm for previous program results, is used [1].

Key words: *fault tolerance, control systems, consensus.*

УДК 004.946
ГРНТИ 28.17.33

ИСПОЛЬЗОВАНИЕ ГЕОГРАФИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ В ОТРАСЛЯХ ЦИФРОВОЙ ЭКОНОМИКИ

И. В. Петров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире информационные технологии развиваются очень стремительно и отрасли вместе с ней. С каждым годом всё больше отраслей используют геоинформационные системы, которые являются по своей сути универсальными. Интеграция подобных систем осуществляется не только на государственном уровне, но также в среднем – крупном бизнесе.

ГИС, отрасли, цифровая экономика.

В настоящее время географические информационные системы (ГИС) используют обширное количество форматов и баз данных для сбора, хранения и анализа информации. Стоит отметить, что подобные системы помогают принимать решения, а не делать это за человека. На основе запроса и функций ГИС предоставляет результаты в удобном для восприятия виде, будь то картографическая форма, графики или диаграмма. Это всё позволяет интегрировать ГИС в любую сферу общества.

Государственные и социальные структуры занимают лидирующую позицию интеграции подобных систем [1], что представлено на рис. 1.

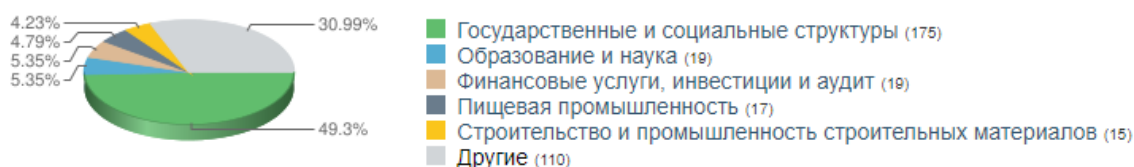


Рис. 1. Отраслевое распределение по количеству проектов интеграции

Благодаря внедрению и развитию ГИС во все возможные сферы деятельности, стало возможно:

- поиск оптимального пути между объектами(точками);
- планирование в градостроительстве;
- нахождение здания по критериям;
- мониторинг экологической ситуации;
- оценка работы филиалов;
- и многое другое.

Интеграция ГИС в единое цифровое пространство позволяет объединять информацию разных уровней власти и их подразделений, обеспечивая доступ руководства к разнородной информации о территории.

ГИС давно уже используются для решений задач муниципального управления [2]. При управлении городской территорией и решением задач городскими службами очень важен пространственный фактор. Местонахождение объекта, его характеристики и связь с другими объектами

позволяет принимать эффективные управленческие решения или оперативно решать задачи.

Муниципальные ГИС помогают оптимизировать дорожное движение и сократить время реагирования разнообразных служб. Например, можно смоделировать транспортные потоки и определить места частого скопления автомобилей. На основе этой информации уже можно будет настраивать светофоры и менять маршруты общественного транспорта. Стоит отметить, что некоторая информация открыта для жителей города в режиме реального времени, например, местоположение общественного транспорта.

На примере использования ГИС в качестве инструмента оценки общества [3], можно увидеть гибкость использования подобных систем. Благодаря публичным опросам и нанесению на карту важных объектов, можно сделать предположение, что является проблемной точкой в неблагополучном районе. На основе полученных сведений, можно принимать решения по реорганизации местоположений компаний предоставляющих услуги досуга и общественного питания. И использовать в дальнейших проектах градостроительства или общественной деятельности.

ГИС используется везде, где необходима территориальная привязка объектов, в особенности области добычи полезных ископаемых. Система помогает горнорудным компаниям и геологоразведочным предприятиям эффективно выполнять задачи по разведке, добычи и транспортировке. Помимо поиска новых месторождений, ГИС помогает развивать уже существующие. Информация представляемая в трех мерном пространстве, что при специфике данной работы, помогает прогнозировать будущие затраты и количество добываемого сырья.

В разведке водяных запасов ГИС крайне необходим, так как для быстрого реагирования в случаях загрязнения или иссушения, нужен постоянный контроль и много критериальная оценка. Вся эта информация также используется и переоценивается при строительстве домов, районов, городов и инфраструктуры в общем.

Многие организации, использующие ГИС, считают, что одно из основных преимуществ заключается в новых возможностях [4, 5]. Например, улучшить собственное управление организацией и корпоративными ресурсами. Возможность совместного использования и постоянного расширения и доработки базы данных различными структурными подразделениями позволяет повысить эффективность работы каждого подразделения и организации в целом. Так, компания, занимающаяся предоставлением связи может четко планировать ремонтные или профилактические работы. А также, получать полную информацию и отображать в удобном виде участки работ, и автоматически определять людей, на которых могут эти работы повлиять.

Стоит также упомянуть, что ГИС критически необходим в предприятиях с большим количеством филиалов или заводов, где критическим фактором в работе является непрерывность работы и время реагирования на ЧС. Постоянно обновляющаяся информация о каждом таком объекте и подобъектах состоящих в нём, позволяет проанализировать состояние и дать оценку работоспособности. Благодаря запросам и визуально понятным ответам, ГИС дополняет внутренние системы и помогает повысить и их эффективность.

Как можно увидеть, ГИС занимает неотъемлемую часть во всех сферах общества, что увеличивает эффективность работы не только государственных и муниципальных управлений, но и среднего – крупного бизнеса. Благодаря этому уровень и качество предоставления разнообразных услуг растёт с каждым годом, а время реагирования на запросы наоборот уменьшается.

Список используемых источников:

1. Данные о ГИС, использующихся в России [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/ГИС_-_Геоинформационные_системы (дата обращения 10.11.2022).
2. Ковалева О.А. Геоинформационные системы в муниципальном управлении // Материалы XIV Международной студенческой научной конференции «Студенческий научный форум». 2022. URL: <https://scienceforum.ru/2022/article/2018030907> (дата обращения: 11.11.2022).
3. Graham S.R., Carlton C., Gaede D., Jamison B. The Benefits of Using Geographic Information Systems as a Community Assessment Tool [Электронный ресурс] // Public Health: электрон. научн. журн. 2011. N 126(2). С. 298–303. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3056049> (дата обращения 11.11.2022).
4. Карин С.А. Интеграция в едином информационном пространстве разнородных геопространственных данных // Информационно-управляющие системы. 2012. N 2. С. 89–94.
5. Лебедев И.В. ГИС и геология // Материалы XIV Международной студенческой научной конференции «Студенческий научный форум». 2018. URL: <https://scienceforum.ru/2018/article/2018004438> (дата обращения: 12.11.2022).

Petrov I.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

The use of the Geographical Information Systems in digital economy branches.

In the modern world, information technology is developing very rapidly and branches along with it. Every year more and more branches use geographic information systems, which are inherently universal. The integration of such systems is carried out not only at the state level, but also in medium – large businesses.

Key words: *GIS, branches, digital economy.*

УДК 004.946
ГРНТИ 28.17.33

СОВРЕМЕННЫЕ ИСКУССТВЕННЫЕ НЕЙРОННЫЕ СЕТИ

Г. В. Рожков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире искусственные нейронные сети занимают многие ниши в производстве и автоматизации процессов. Они попадают под четыре основные категории: обычные искусственные нейронные сети, сверточные нейронные сети, пиковые нейронные сети и рекуррентные нейронные сети. Понимание их особенностей необходимо для работы с нейронными сетями.

нейронные сети, глубокое обучение, ANN, CNN, SNN

В современном мире искусственные нейронные сети начинают занимать многие ниши в производстве. Они подпадают под четыре основные категории [1]: искусственные нейронные сети (ANNs), сверточные нейронные сети (CNNs), пиковые нейронные сети (SNNs) и рекуррентные нейронные сети (RNNs), но последняя не будет рассмотрена в данной работе.

Искусственные нейронные сети (ANN) - это может звучать запутанным, поскольку все нейронные сети, используемые в вычислениях, являются искусственными нейронными сетями, однако мы оставляем это определение для всех нейронных сетей, которые распределены в нескольких слоях искусственных нейронов и выполняют только операции этих нейронов для получения выходных данных.

Типичную структуру этих нейронных сетей можно увидеть на рис. 1.

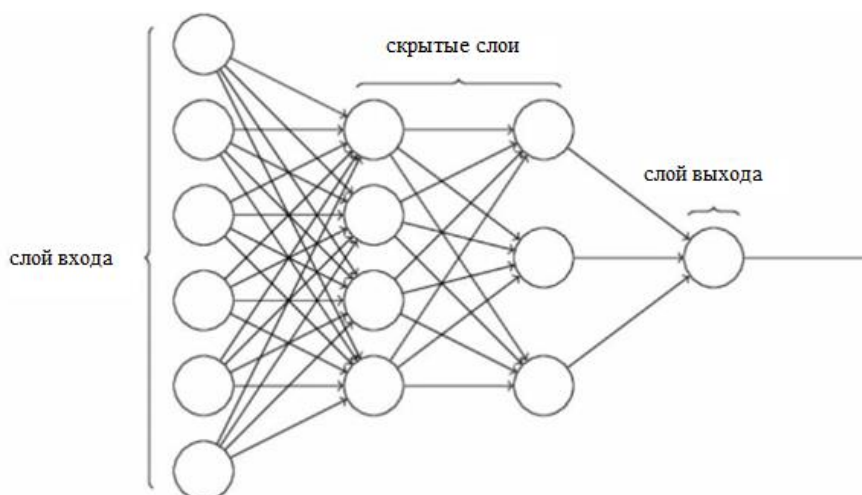


Рис. 1 Стандартная структура искусственной нейронной сети

Как видно по рисунку, у нас есть входные данные для нейронной сети, которая всегда формируется набором чисел, у нас есть входной слой, скрытые слои и выходной слой. Такова структура искусственной нейронной сети ANN.

Сверточные нейронные сети (CNN). Название этого типа искусственной нейронной сети происходит от двух операций, которые они выполняют над входными данными перед подачей их в одну обычную ANN. Эти две операции - свертка и объединение. Прежде чем увеличить масштаб, посмотрите на графическое представление CNN на рис. 2.



Рис. 2 Сверточная нейронная сеть

Чаще всего CNN используются для обработки изображений, поэтому на входе используется фигура — это изображение. Как мы можем видеть, первый и второй слои являются сверточным слоем и объединяющим слоем соответственно. Они шли рука об руку друг с другом, а это означает, что каждый раз, когда мы вставляем сверточный слой, нам приходится вставлять объединяющий слой позже. Мы могли бы вставить столько слоев, объединяющих свертки, сколько захотим, конечно, на самом деле это будет зависеть от нашего приложения и размера входных данных. Результатом последних операций объединения свертки будет матрица чисел. Эта матрица преобразуется в один вектор, который называется сглаженным вектором, поэтому иногда вы услышите название сглаженный слой. Затем сглаженный вектор вводится в полностью связанный слой, который представляет собой всего лишь слой нейронов ANN. Наконец, у нас есть выходной слой, который обеспечивает прогнозирование. Теперь давайте посмотрим, что означают операции свертки и объединения.

Свертка работает с двумя сигналами (в 1 измерении) или с двумя изображениями (в 2 измерениях). Мы могли бы рассматривать первый сигнал как входной, а второй сигнал, называемый ядром, как фильтр. Свертка принимает входной сигнал и умножает его на ядро, выводя третий модифицированный сигнал. Целью этой операции является извлечение высокоуровневых функций из входных данных.

На рис. 3 показана иллюстрация операции свертки. Изображение — это не что иное, как матрица, полная пикселей, операция свертки состоит в пропускании фильтра (матрицы ядра) через матрицу изображения, это означает, что матрица ядра скользит шаг за шагом, на одну позицию в каждом направлении, по матрице изображения. Он умножает значение каждой ячейки матрицы изображений на значение ячейки в матрице ядра, суммирует все

полученные значения и сохраняет результат в соответствующей ячейке выходной матрицы. Веса матрицы ядра по умолчанию инициализируются некоторым значением и обновляются в процессе обучения.

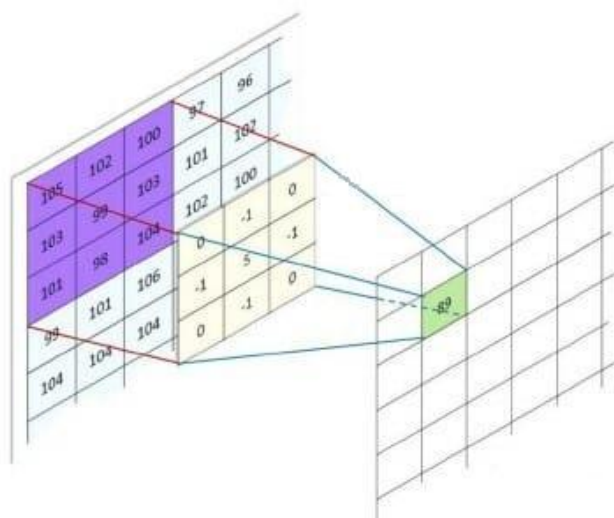


Рис. 3 Операция свертки

Идея операции свертки состоит в том, чтобы имитировать распознавание человеческим глазом признаков на одном изображении. Человек видит изображение автомобиля, на изображении есть некоторые особенности, которые помогают распознать, что это автомобиль (форма автомобиля, материал, дороги, перекрестки и т.д.). Умножение матрицы изображения на фильтр и обновление параметров фильтра с помощью обучения извлекает наиболее важные особенности изображения, те, которые позволяют нам понять, что на изображении есть автомобиль, но мы не знаем, как определить алгоритмически.

На рис. 4 показана иллюстрация операции объединения. Это процесс дискретизации на основе выборки, при котором мы уменьшаем выборку входных данных, уменьшая их размеры и позволяя делать предположения об особенностях, содержащихся в выбранных субрегионах. Существует два основных типа операций объединения. Максимальное объединение, графическое представление которого мы можем видеть на рис. 4, и среднее объединение. Как следует из их названия, один из них основан на выборе максимального значения из выбранного региона, в то время как другой основан на вычислении среднего значения всех значений.

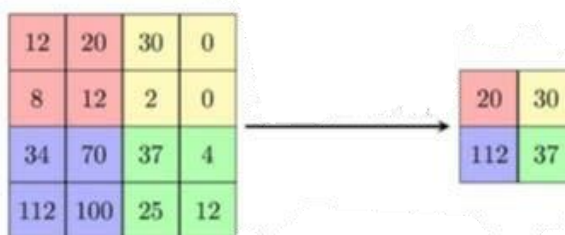


Рис. 4 Операция объединения

Результатом последнего объединяющего слоя в CNN является многомерная матрица с именем *pooled features map*. Нам нужно сгладить этот конечный результат в вектор, содержащий по одному значению на индекс, чтобы иметь возможность передавать его на полностью подключенный слой, это сглаженный вектор, представленный на рис. 5. Объекты, отфильтрованные на этапах объединения в свертку, кодируются в векторе сглаживания. Роль полностью связанного слоя состоит в том, чтобы принимать все векторные значения и комбинировать объекты, чтобы сделать прогноз о вероятности каждого класса.

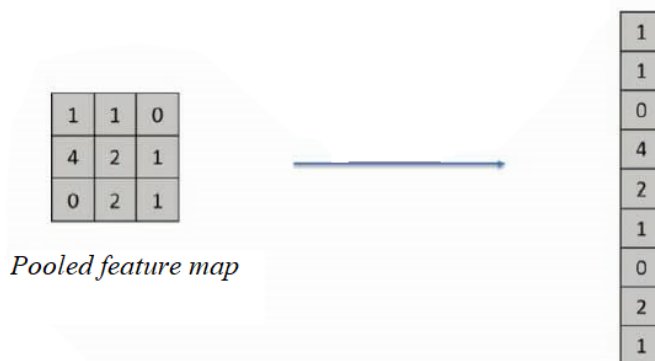


Рис. 5 Выравнивание выходного слоя объединения

Важным фактором является то, что мы должны быть согласованы с набором данных изображений, которые мы передаем CNN. Если вы обучаете CNN различать наземные транспортные средства, но не самолеты, тогда не вводите изображение самолета в свой обучающий набор.

Поскольку выходные данные CNN представляют собой вероятности принадлежности входных данных к каждому классу, сумма всех выходных данных всегда будет находиться в диапазоне от 0 до 1. Если вы используете обученный CNN для различения транспортных средств и вводите изображение самолета, в лучшем случае выходные данные четырех классов могут составлять 0,25 (это означает, что входные данные имеют одинаковую вероятность принадлежности к любому классу).

Перейдем к пиковым нейронным сетям (SNN). Они были разработаны для неврологических вычислений в попытке смоделировать поведение биологического мозга. Похоже, что они существуют уже некоторое время, но не вызвали интереса к глубокому обучению в основном из-за отсутствия обучающих алгоритмов и повышенной вычислительной сложности. SNN более точно имитируют нейронные связи в нашем мозге, таким образом, они являются наиболее вдохновленными биологией искусственными сетями.

Чтобы имитировать работу биологического мозга, нейроны пиковых нейронных сетей должны быть определены таким образом, чтобы их можно было активировать как можно быстрее и посылать импульсы в качестве выходных данных [2]. ANN не являются точными моделями мозга, потому что слои активируются синхронно, и они использовали функции активации с непрерывным значением. Каждый нейрон выдает непрерывное значение. В

нашем мозге после того, как возникает потенциал действия и нейрон передает нейромедиаторы, он возвращается в свое стабильное состояние, ожидая следующей активации.

До настоящего времени SNN использовались в вычислительной неврологии как попытка лучше понять, как функционирует наш мозг. Одной из интересных и активных областей исследований является нейроморфная инженерия [3], где мы проектируем компьютеры, реализующие SNN физического аппаратного уровня для выполнения задач биологической нервной системы.

С помощью нейроморфной инженерии у нас будет устройство (компьютер), в котором физические пиковые нейроны реализованы с использованием мемристоров на основе оксида, спинтронной памяти, пороговых переключателей и транзисторов. Датчики и исполнительные механизмы могут быть напрямую подключены к этому устройству, а затем SNN обучен активировать исполнительные механизмы на основе выходных сигналов датчика. Больше не требуется подключение к памяти, процессору, контроллерам и интегральным схемам.

Главным преимуществом нейроморфных устройств является энергоэффективность, поскольку информация может передаваться через нейронную сеть с использованием очень слабых сигналов.

Чтобы заставить пиковые нейронные сети учиться, необходимо использовать неконтролируемые алгоритмы обучения, то есть позволить им учиться самим. Некоторые используемые алгоритмы обучения, вдохновленные биологией — это обучение по Хеббиану. Это правило увеличивает веса приемников если активность подключенных нейронов коррелирует, и уменьшает, если активность не коррелирует. Следовательно, сила связи выше для нейронов, которые выполняют связанные действия. Более сильная связь означает, что передающий нейрон оказывает большее влияние на принимающий нейрон. Когда принимается входной сигнал, траектория пиков определяется прочностью соединения. В процессе обучения мы изменяем силу соединения, чтобы активировать тот же самый путь нейронов, когда подается аналогичный ввод. Тогда, независимо от того, приближается ли автомобиль, камень или любой другой объект в опасной близости. В обоих случаях будет активирован один и тот же путь нейронов, и действие будет заключаться в эвакуации. Все вычислительные мощности, необходимые для обнаружения объекта, определения опасности, расчета пути эвакуации и т.д., исключаются. На самом деле, мы не исключаем этот процесс, просто SNN изучил его автоматически, без необходимости определять эти шаги. Однако эта технология еще слабо развита.

Таким образом, искусственные нейронные сети занимают все большую часть цифровых исследований, но еще предстоит много работы для достижения желаемых результатов.

Список используемых источников:

1. Минчжэ Чен, Урсула Чаллита, Валид Саад. Машинное обучение на основе искусственных нейронных сетей для беспроводных сетей [Электронный ресурс]. URL:

https://www.researchgate.net/publication/320296934_Artificial_Neural_Networks-Based_Machine_Learning_for_Wireless_Networks_A_Tutorial (дата обращения 11.11.2022).

2. Майкл Нильсен, Тарик Рашид. Нейронные сети и глубокое обучение //Искусственные нейронные сети. – 2019. – Т. 7. – №. 4. – С. 17-39.

3. Монро, Д. "Нейроморфные вычисления готовятся к (действительно) большому времени". Сообщения АСМ. 2014. N 57: С 13-15.

Rozhkov G.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

IPTV Service Delivery Models.

In the modern world, artificial neural networks occupy many niches in manufacturing and process automation. They fall into four main categories: conventional artificial neural networks, convolutional neural networks, spike neural networks and recurrent neural networks. Understanding their features is necessary to work with neural networks.

Key words: neural networks, deep learning, ANN, CNN, SNN.

УДК 004.351, 004.353, 004.358
ГРНТИ 81.14.15

РАЗРАБОТКА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ДОПОЛНЕННОЙ РЕАЛЬНОСТИ ДЛЯ ОПЕРАТОРОВ СТАНКОВ ОПТОВОЛОКОННОГО ПРОИЗВОДСТВА

Д. В. Соловьев, И. Б. Бондаренко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья написана при поддержке Благотворительного фонда Владимира Потанина, предоставившего грант на разработку новых учебных курсов для кафедры интеллектуальных систем автоматизации и управления (ИСАУ) Санкт-петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича (СПбГУТ).

В настоящее время технологии дополненной, виртуальной и смешанной реальностей активно внедряются во все отрасли промышленности. Актуальными являются задачи автоматизации труда операторов станков для производства заготовок-преформ для последующей вытяжки оптического волокна, а так же задачи автоматизации труда операторов башен вытяжки оптического волокна. В настоящей статье приводится история технологий дополненной, виртуальной и смешанной реальностей, а так же ставится задача разработки программно-аппаратного комплекса для операторов станков оптоволоконного производства.

AR, VR, MR-технологии, автоматизация, вытяжка оптического волокна

История технологий

Широкую известность термин «дополненная реальность» приобрел благодаря появлению умных очков Google Glass в 2013 году [1,2], а затем появлению большого количества развлекательных приложений, позволяющих собеседнику по видеосвязи накладывать на свое лицо различные шуточные маски, далее в 2016 году появилась игра Pokemon Go [1,3]. Но это все были игровые, шуточные приложения, а на самом деле история AR уходит далеко в прошлое. Пожалуй, первое упоминание о такой «реальности» датируется 1901 годом в детской книге Фрэнка Баума «Master key», где рассказывается об устройстве-очках, позволяющем «помечать» людей буквами, означающими их уровень интеллекта и характер [1,4]. Однако некоторые исследователи считают, что появление технологий дополненной реальности стоит отнести к изобретениям древнего Рима, когда лучники надевали специальные маски для лучшего прицеливания. Следует понимать, что термин «дополненная реальность» тесно связан с термином «виртуальная реальность», первые упоминания данной технологии, т.е. погружения в другой, вымышленный, виртуальный мир можно отнести к ранней Солотрейской культуре (18-15 тыс. лет до н.э.), нашедшей свое отражение в рисунках в пещере Ласко во Франции [1,5,6]. В литературе 20-го века активно начинают описываться новые «виртуальные» миры и устройства для их создания. Так в 1932 году в романе «Brave New World» Олдоса Хаксли приводится кинотеатр будущего, где трехмерное изображение дополняется тактильными и обаятельными ощущениями [1,7]. Похожее описание виртуальной реальности сделал Рэй Брэдбери в рассказе «The Veldt» (оригинальное название "The World the Children

Made") в 1950 году [1,8]. В рассказе говорится о первой комнате виртуальной реальности, на стены которой могли проецироваться любые изображения.

Начало практических разработок в области VR следует отнести на вторую половину 20-го века. Первопроходцем в этой области принято считать Мортон Хейлинга благодаря созданию симулятора «Sensorama». С помощью этого симулятора человек погружался в виртуальный мир изображений, звуков и запахов городских пейзажей [1,9]. Например, человек мог прокатиться на мотоцикле по улицам Бруклина. Также Хейлингом была разработана модель «Театра ощущений», представляющая собой развитие «Сенсорамы» для возможности коллективного погружения в виртуальный мир.

Еще одна разработка в области VR принадлежит гарвардскому профессору Айвану Сазерленду, устройство называется «The Sword of Damocles» («Дамоклов меч») [1,10]. В 1968 году это было достаточно примитивное устройство как с точки зрения графики и реализма, так и с точки зрения интерфейса пользователя. Суть устройства состояла в отображении данных программы на стереоскопических очках. Человеку демонстрировалось изображение перспективы в зависимости от положения головы. Вес устройства был настолько велик, что его пришлось «подвесить» с помощью механической руки к потолку, собственно, поэтому и было выбрано название устройства «Дамоклов меч».

К следующим достижениям в области VR относят работы Майрона Крюгера, компьютерного художника их университета Висконсина. Он проводил эксперименты в лаборатории «Videoplase» в 1974 году, очень похожие на описанные в рассказе «The Veldt» Рэя Брэдбери, также проецировал фотографии своих слушателей на гигантские пейзажи. Основное отличие этих VR экспериментов было в том, что человеку не нужно было надевать специальные очки и шлемы. Для взаимодействия с участником в этом устройстве использовались телекамеры, видеопроекторы и другие устройства [1,6,11].

Еще одним проектом Крюгера была виртуальная игра «Maze», где игроки искали выход из лабиринта, изображение которого проецировалось на стены комнаты [1,6].

В 80-е годы 20-го века окончательно устоялся термин «виртуальная реальность» (до этого применялся термин «интерактивные среды»). В конце 80-х, Скотт Фишер из исследовательского центра Эймса НАСА разработал первый прототип устройства VR. Это были привычные нам экран, закрепленный на голове и перчатки для передачи данных. Цель проекта была в разработке устройства для астронавтов для возможности управления роботами-ремонтниками в космосе [1,12].

Первым устройством дополненной реальности следует считать EyeTap Стива Манна. В устройстве была задействована камера и дисплей, дополняющие среду в режиме реального времени. Многие считают Стива Манна отцом «носимых» компьютеров. Манн начал создавать прототипы различных версий компьютерного зрения с 1970-х годов и представил более раннюю версию EyeTap в MIT в 1990-х. В первые годы устройства Манна были достаточно большими: камера была прикреплена к шлему, а компьютер был закреплен на человеке. Современные функции EyeTap

претерпели большие изменения, как и его внешний вид, который теперь представляет собой элегантную пару футуристических очков [1,13].

Еще одно интересное изобретение Манна – «Цифровые очки для зрения» (Сварочная маска MannGlas). [1,14,15].

Однако массово технологии дополненной реальности стали использоваться благодаря Дену Рейтону в начале 80-х годов 20-го века, он применил данные с радара и камеры из космоса для демонстрации передвижения воздушных масс, ветров и циклонов в прогнозах погоды. Между прочим, технологии AR до сих пор применяются в телепрогнозах [1,16,17].

Следующее развитие технологий AR следует отнести к ученому Тому Коделлу, который как раз и озвучил термин «дополненная реальность». Для производства самолетов Боинг он разработал специальные шлемы, которые отображали информацию о разметке заводских зон сборки, что позволило не переписывать таблички с разметкой вручную, а изменять их с помощью программного обеспечения [1,16]. В настоящее время компания Боинг активно применяет технологии AR при сборке самолетов [1,18].

Постановка задачи разработки

Современные AR-технологии могут быть использованы в процессе обучения операторов станков, инструктаже по ремонту оборудования, аудита и контроля качества работ.

Предположим, что предприятию оптической промышленности нужно провести первичный инструктаж по работе за станочным оборудованием для изготовления оптического волокна. Инструктор-преподаватель может после изложения общих принципов безопасной работы со станками и оборудованием в учебном классе перейти непосредственно в цех с инструктируемыми, выдать им AR-очки и начать обучение уже на реальном оборудовании. Ученикам при этом будут транслироваться через AR-очки подробные инструкции по наладке, запуску, работе со станком. Очевидно, что такое обучение позволяет лучше усваивать материал, благодаря реализации процесса обучения на реальном оборудовании. Преподаватель при этом может и не присутствовать в цеху и проводить занятие удаленно, необходимым и достаточным условием является присутствие ответственных сотрудников в цеху.

Рассмотрим другую область применения AR-технологий на предприятии оптической промышленности. Предположим, что на производстве произошла поломка оборудования, а высококвалифицированный специалист, который может осуществить сложный ремонт «на лету» находится на больничном или вообще на другом полушарии. В таком случае все производство останавливается до устранения неисправности. Однако, в случае наличия интернет связи с сотрудником и технологий дополненной реальности на производстве другие сотрудники предприятия могут своими силами выполнить сложный ремонт станочного оборудования под внимательным присмотром и руководством удаленного специалиста. Им достаточно надеть очки дополненной реальности и запустить сеанс видеосвязи. Изображение оборудования и поломки в реальном времени транслируются удаленному специалисту, а он, в свою очередь, может контролировать ремонт с помощью голоса, трансляции на экран очков чертежей, схем и направляющих в нужное место для ремонта указателей или стрелок. В

результате успешного ремонта оборудование продолжает функционировать в рабочем режиме, производство не останавливается на долгий срок. После ремонта видеозапись можно выгрузить для обучения других сотрудников предприятия.

Для решения задачи аудита, удаленной инспекции или инструктажа можно так же активно использовать AR. Удаленный аудитор или консультант подключается через интернет соединение с сотрудниками на месте проведения аудита. Такой подход дает огромные перспективы для экономии бюджета предприятия в результате снижения командировочных расходов, затрат на работу аудиторов или консультантов. В свою очередь так же уменьшает простой оборудования.

Список используемых источников:

1. Д.В. Соловьев, И.Б. Бондаренко, Ю.А. Гатчин, В.И. Поляков, А.В. Исаева Перспективы использования технологий дополненной реальности в образовании. Труды Международного научно-технического конгресса «Интеллектуальные системы и информационные технологии – 2022» («ИС & ИТ-2022», IS&IT'22). Научное издание в 2-х т. Т.2. – Таганрог: Изд-во Ступина С.А., 2022. – 417 с.
2. Статья «Google Glass» [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Google_Glass(дата обращения: 08.11.2022).
3. Статья «PokemonGo» [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Pok%C3%A9mon_Go(дата обращения: 08.11.2022).
4. L. Frank Baum The Master Key: An Electrical Fairy Tale, Founded Upon the Mysteries of Electricity and the Optimism of Its Devotees is a 1901.
5. Статья «Пещера Ласко» [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%89%D0%B5%D1%80%D0%B0_%D0%9B%D0%B0%D1%81%D0%BA%D0%BE(дата обращения: 08.11.2022).
6. David Kushner Masters of Doom: How Two Guys Created an Empire and Transformed Pop Culture, 2003.
7. Aldous Huxley Brave New World, 1932.
8. Ray Bradbury "The World the Children Made" in the September 23, 1950 issue of The Saturday Evening Post.
9. Статья «Сенсорам» [Электронный ресурс]. – Режим доступа: <https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D0%BD%D1%81%D0%BE%D1%80%D0%B0%D0%BC%D0%B0>(дата обращения: 08.11.2022).
10. Статья «TheSwordofDamocles» [Электронный ресурс]. – Режим доступа: [https://en.wikipedia.org/wiki/The_Sword_of_Damocles_\(virtual_reality\)](https://en.wikipedia.org/wiki/The_Sword_of_Damocles_(virtual_reality)) (дата обращения: 08.11.2022).
11. Myron Krueger. Artificial Reality, Addison-Wesley, 1983.
12. Статья «Шаткие успехи и оглушительные провалы в долгой и странной истории виртуальной реальности» [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/post/399169/>(дата обращения: 08.11.2022).
13. Статья «EyeTap» [Электронный ресурс]. – Режим доступа: <http://www.digiart21.org/art/eyetap>(дата обращения: 08.11.2022).
14. IEEE Technology & Society 31(3).
15. Estimation-theoretic approach to dynamic range enhancement using multiple exposures Mark A. Robertson Sean Borman Robert L. Stevenson University of Notre Dame Department of Electrical Engineering Notre Dame, Indiana 46556
16. Статья «AR – Дополненная Реальность» [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/post/419437/>(дата обращения: 08.11.2022).

17. Статья «AR – История развития дополненной реальности» [Электронный ресурс]. – Режим доступа: <https://vr-game.ru/all-news/vr-v-mire/904-istorija-razvitija-dopolnenoj-realnosti.html>(дата обращения: 08.11.2022).

18. Статья «Boeing test augmented reality in the factory» [Электронный ресурс]. – Режим доступа: <https://www.boeing.com/features/2018/01/augmented-reality-01-18.page>(дата обращения: 08.11.2022).

Soloviev D., Bondarenko I.

St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevich

Development of an augmented reality software and hardware complex for operators of fiber-optic production machines.

The article was written with the support of the Vladimir Potanin Charitable Foundation, which provided a grant for the development of new training courses for the Department of Intelligent Automation and Control Systems (ISAU) of St. Petersburg State University of Telecommunications. prof. M.A. Bonch-Bruevich (SPbSUT). Currently, augmented, virtual and mixed reality technologies are being actively implemented in all industries. The tasks of automating the work of machine operators for the production of preforms for the subsequent drawing of optical fiber, as well as the tasks of automating the work of operators of optical fiber drawing towers, are topical. This article provides the history of augmented, virtual and mixed reality technologies, as well as the task of developing a software and hardware complex for operators of fiber optic production machines.

Key words: AR, VR, MR technologies, automation, optical fiber extraction.

УДК 004.512.4
ГРНТИ 50.41.25

СПОСОБЫ РЕШЕНИЯ ЗАДАЧИ АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ ДАННЫХ ПОЛЬЗОВАТЕЛЯ ПРИ ВЗАИМОДЕЙСТВИИ С ЧАТ-БОТАМИ

Ф. В. Филиппов, И. В. Цыварев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе приведены общие сведения об использовании чат-ботов в информационных системах, изучается задача авторизации и аутентификации пользователей при использовании чат-ботов, рассматриваются проблемы, возникающие вследствие хранения данных авторизации в чате, предлагаются способы решения данных проблем.

чат-боты, аутентификация аутентификационные данные, авторизация, валидация, проверка пользователя, SMS-аутентификация, токен, веб-сервис

подавляющая часть чат-ботов, с которыми взаимодействуют пользователи в сети Интернет, не требует какой-либо валидации или аутентификации пользователя – интерфейс предлагает воспользоваться предложенным функционалом через ответ на сообщение или через вход в чат. Однако в чат-ботах, находящихся в корпоративных сетях или взаимодействующие с рабочими сервисами через API, могут потребовать ввода данных пользователя – логина и пароля. В данном случае может возникнуть задача нарушения безопасности данных пользователя

В статье изучены причины возникновения данной задачи, основные уязвимости, возникающие в данном случае, и способы их решения.

В наше время в разных социальных сетях и сервисах повсеместно используются системы взаимоотношений с клиентом типа «чат-бот». Данный метод коммуникации с пользователями стал популярен благодаря множеству достоинств, таких как:

- возможность автоматизации и оптимизации повторяющихся задач;
- возможность круглосуточной непрерывной работы;
- исключение человеческого фактора из коммуникации;
- доступ к применению алгоритмов искусственного интеллекта.

Совокупность всех этих достоинств делает использование чат-ботов особенно полезным в сферах продаж, создания личных ассистентов, обеспечении технической поддержки и обслуживании клиентов.

В определенных случаях взаимодействие с чат-ботом требует от пользователя ввода различных аутентификационных данных – данных, требуемых для ввода от пользователя. К основным причинам использования аутентификационных данных можно отнести:

- Ограничение доступа к определенному функционалу, предоставляемому через чат-бот;

- Для получения личных данных пользователя (номера мобильного телефона, электронной почты) с целью дальнейшего использования;

Использование аутентификационных данных пользователя (зачастую это логин и пароль, но некоторые системы могут использовать имя и фамилию пользователя, адрес электронной почты e-mail, номер мобильного телефона и т.п.) в чат-ботах создает следующие опасности:

- данные для входа могут остаться в истории переписки, чем смогут воспользоваться нарушители в случае взлома устройства пользователя;
- вместо логина могут быть посланы запросы для SQL-инъекций, создавая окно уязвимости для нарушителей.

Можно увидеть, что угрозы, создаваемые требованием аутентификации пользователя в чат-боте, схожи с угрозами аутентификации в любой системе. Однако в случае с обычными системами, в которых ввод данных осуществляется через специальное поле ввода, аутентификационные данные нигде не хранятся – в большинстве случаев после их ввода данные отправляются в сервис авторизации, где они преобразуются (например, как при преобразовании пароля в хэш-код) и сверяются с данными, которые лежат в базе данных сервиса. В случае чат-ботов возникает опасность хранения аутентификационных данных в явном виде – например, пользователь вводит логин и пароль в чат-бот в мессенджере, и после их ввода данные остаются лежать в переписке. При этом даже удаление сообщений пользователем не гарантирует, что сообщения будут удалены из базы данных мессенджера, а не просто скрыты от пользователя.[1]
[2]

Исходя из вышеперечисленных рисков, возникает необходимость поиска альтернативных способов аутентификации пользователя, не создающих опасности утечки данных пользователя.

Одним из способов авторизации пользователя без использования логина и пароля, является авторизация через номер телефона и отправку сообщения с кодом для входа. Данный подход называется SMS-аутентификацией и уже используется в крупных компаниях для авторизации пользователей. Схема потоков данных при SMS-аутентификации представлена на рис. 1. На данной схеме изображен поток данных при использовании чат-бота, размещенного в мессенджере и использующего приложение Watson Assistant для отправки сообщения пользователю. [3]

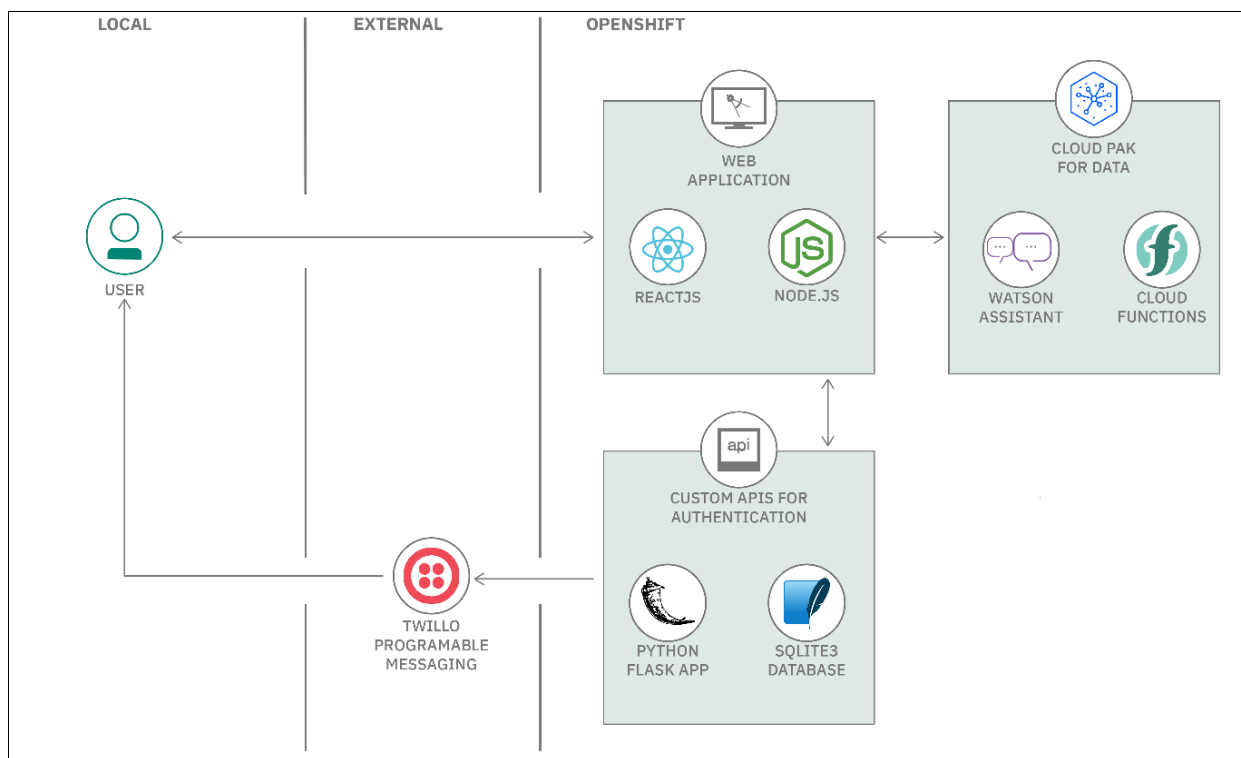


Рис. 1. Схема потоков данных в приложении – чат-боте, использующем SMS-аутентификацию

Порядок действий пользователя при авторизации в случае использования SMS-аутентификации следующий:

- пользователь начинает работу с чат-ботом;
- чат-бот запрашивает номер мобильного телефона у пользователя;
- пользователь отправляет номер мобильного телефона;
- чат-бот считывает номер телефона, отправляет его в сервис авторизации;
- сервис отправляет сообщение с кодом пользователю и в чат-бот;
- пользователь получает код, вводит его в окно чат-бота;
- чат-бот проверяет код пользователя и код сервиса, в случае положительной проверки дает пользователю доступ к функционалу.

Стоит заметить, что при использовании SMS-аутентификации могут возникнуть проблемы, связанные с каждой из сторон алгоритма – со стороны пользователя, чат-бота или сервиса – и если проблемы возникнут хотя бы с одной из трех сторон, то не будет работать весь процесс.

Также для авторизации пользователя можно использовать систему токенов и сторонние сервисы, как предлагается сделать в руководстве к использованию чат-ботов, созданных с помощью системы Power Virtual Agents, созданной Microsoft [4]. В данном случае, в процессе авторизации пользователя для его аутентификации используется сторонний сервис, представляющий из себя окно с логином и паролем.

Порядок действий пользователя при авторизации через сторонний сервис следующий:

- пользователь начинает работу с чат-ботом;
- чат-бот выводит ссылку на сервис для ввода данных;

- пользователь переходит по ссылке, вводит логин и пароль;
- сервис получает логин и пароль пользователя, сравнивает их с данными пользователя в базе данных;
- если данные пользователя и данные для авторизации совпали, сервис передает токен аутентификации в чат-бот;
- чат-бот получает токен аутентификации, хранит его во время работы пользователя с функционалом и удаляет по окончании работы пользователя.

Основываясь на способах, перечисленных выше, можно сказать, что задачу аутентификации пользователя в чат-боте можно решить с помощью интеграции сторонних сервисов, дающих дополнительный функционал верификации пользователя, однако внедрение данного функционала потребует выделения отдельного технического ресурса для обеспечения стабильной работы подключенных сервисов.

Список используемых источников:

1. WhatsApp doesn't permanently delete your chats, keeps all records saved [Электронный ресурс] // Deccan chronicle. 2015-2022. URL: <https://www.deccanchronicle.com/technology/in-other-news/290716/beware-whatsapp-silently-rolled-out-an-update-allows-recovery-of-deleted-chats.html> (Дата обращения 11.11.2022)
2. «ВКонтакте» вечно хранит все удаленные сообщения, файлы и другие данные: [Электронный ресурс] // АККет.com. 2013-2022. URL: <https://akket.com/raznoe/122186-vkontakte-vechno-hranit-vse-udalennye-soobshheniya-fajly-i-drugie-dannye.html> (Дата обращения 12.11.2022)
3. Authenticate chatbot users with SMS one-time passcode: [Электронный ресурс] // IBM. 2022. URL: <https://developer.ibm.com/patterns/authenticate-users-on-your-chatbot-with-sms-one-time-passcode-otp/> (Дата обращения 12.11.2022)
4. Add end-user authentication to a Power Virtual Agents bot: [Электронный ресурс] // Microsoft.com. 2022. URL: <https://learn.microsoft.com/en-us/power-virtual-agents/advanced-end-user-authentication> (Дата обращения 12.11.2022)

Filippov F., Tsyvarev I.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Methods for solving the authentication problem using user data in interaction with chatbots. The paper provides general information about the use of chat bots in information systems, the problems of authorization and authentication of users in process of using chat bots are studied, problems arising from the storage of authorization data in a chat are considered, and ways to solve these problems are proposed.

Key words: *chatbots, authentication authentication data, authorization, validation, user verification, SMS authentication, token, web service.*

УДК 004.83
ГРНТИ 20.23.29

СПОСОБЫ РЕШЕНИЯ ПРОБЛЕМЫ ТЕМАТИЧЕСКОГО ПОИСКА В БИБЛИОТЕЧНОЙ ДЕЯТЕЛЬНОСТИ

П. В. Юрченко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире количество информации несоизмеримо растет. Вследствие этого поиск документов определенной тематики становится трудоемким процессом. Эта проблема наиболее актуальна в библиотечной сфере. В статье дан краткий обзор нынешнего этапа развития библиотек. Рассмотрены основные структуры данных и методы для автоматической классификации текста и формирования их семантического представления. Предложено возможное решение проблемы тематического поиска в библиотечной деятельности.

тематический поиск, машинное обучение, библиографическое обслуживание

В настоящее время наблюдается лавинообразное увеличение цифровой информации.

К примеру, согласно опубликованному в январе 2021 г. международной компанией Statista отчёту, объём данных/информации, созданных, переведённых в цифровой вид, скопированных и потреблённых во всём мире в 2020 г. оценивается примерно в 74 зеттабайта [1].

В связи с этим люди тратят большое количество времени на поиск тематической информации и документов. Несмотря на наличие мощных поисковых систем для информационных ресурсов Интернета или для специализированных баз данных, процесс поиска продолжает оставаться трудоемким и слабо поддерживается программно и методологически [2].

Эта проблема особенно актуальна в образовательной и научной деятельности. Так, в книге «Реорганизация знаний» профессор Ким Вельтман отмечает, что в настоящее время «учёный, занимающийся научной деятельностью, тратит 90% своего времени на поиск документов, 5% на их изучение и всего 5% на науку» [3].

Библиотеки, являясь хранилищами знаний, переживают период информатизации, в области которой основным направлением их работы является комплексная автоматизация всех библиотечных процессов [4]. Применяются системы автоматизации библиотек, которые освобождают библиотечных работников от рутинной работы.

Библиографическое обслуживание автоматизируется созданием электронной библиотеки, с одной стороны, и появлением виртуальных форм библиографического обслуживания — с другой. В случае с электронной библиотекой имеет место быть поисковая система, работа с которой, как было сказано выше, может быть кропотливой. Виртуальное обслуживание предполагает общение читателя с библиографом в удаленном режиме, что является достаточно времязатратным способом получения нужной информации.

Таким образом, количественный рост объёмов библиографической информации обуславливает необходимость перехода к цифровому инструментарию её сбора, анализа, обработки и распространения [5]. Цифровые

технологии обладают потенциалом для улучшения процессов библиотечной деятельности.

Перспективным является внедрение в библиотечную сферу систем интеллектуального анализа текстов. Такая система включает в себя классификацию документов, извлечение из них шаблонов и знаний и формирование их семантического представления [6].

Построение структуры данных, которая может представлять документы, и построение классификатора, который можно использовать для определения метки класса документа с высокой точностью, являются ключевыми моментами в классификации текста [6].

Текстовый документ обычно представляется в виде вектора весов терминов (признаков слов) из набора терминов (словаря), где каждый термин встречается по крайней мере один раз в определенном минимальном количестве документов [6]:

$$\vec{d}_j = \langle \omega_{1j}, \dots, \omega_{|T|j} \rangle,$$

где T — словарь, и $0 \leq \omega_{kj} \leq 1$ определяет значимость термина t_k в документе d_j [7].

Семантический анализ — это процесс лингвистического разбора предложений и абзацев на ключевые понятия, глаголы и имена собственные [6]. Эти слова затем сравниваются с таксономией (категориями) и группируются в соответствии с релевантностью [6].

На практике применяется подход, при котором частота термина/обратная частота документа (TF-IDF) обычно используется для взвешивания каждого слова в текстовом документе в соответствии с тем, насколько оно уникально [6].

Задача автоматической классификации включает такие подходы к машинному обучению, как байесовский классификатор, K-ближайших соседей (k-NN), машины опорных векторов (SVM), нейронные сети и т. д. [6]. Различные исследования показали, что SVM превосходит другие алгоритмы классификации [6].

На текущий момент в библиотечной области существуют решения, реализующие цифровые технологии. Внимания заслуживает сервис от отечественной электронно-библиотечной системы (ЭБС) Znanium. Модуль Discovery Znanium — совместная разработка ИНФРА-М и Института системного анализа РАН [8], в основе которой лежат идеи и технологии системы Exactus [9]. К таким технологиям относятся: алгоритм построения инвертированного поискового индекса коллекций документов и алгоритм поиска информации по запросу, основанный на методе многокритериальной оценки сходства текстов [10].

Цель создания Discovery Znanium — предоставить исследователям возможность находить контент по интересующей их теме или дисциплине за минимальное время. Этому способствуют интеллектуальный поиск, основанный на алгоритмах искусственного интеллекта, и большой объем контента: в Discovery свыше 14,5 млн документов [11].

При интеллектуальном поиске у пользователя есть возможность: посмотреть автоматически сформированные, масштабируемые резюме и облако

ключевых слов документа; получить HTML-копию документа с подсветкой по тексту слов поискового запроса; найти документы, содержательно похожие на заданный документ [8].

После исследования данного сервиса можно сделать следующие выводы. Discovery Znanium действительно облегчает тематический поиск документов. Резюме документа позволяет быстро определить его полезность для пользователя, что значительно сокращает время знакомства с результатами поиска. Для каждого документа с помощью интеллектуального алгоритма выделены ключевые слова, которые могут быть не очевидны. Они позволяют пользователю найти дополнительные материалы, а также документы по своей тематике в смежных областях. Найдя подходящий документ, пользователь может найти семантически похожие документы, что также автоматизирует тематический поиск.

Однако у этого модуля есть существенный недостаток. В первую очередь он ориентирован на учёных. Поиск в данной системе производится по научным публикациям. Для того, чтобы эффективно пользоваться интеллектуальным (в т.ч. семантическим) поиском, нужно владеть языком запросов, а также уметь пользоваться различными фильтрами. Исходя из этого, модуль полезен только узкой категории людей и не ориентирован на массового пользователя. Для субъектов образовательной сферы, например для студентов и преподавателей, модуль будет малополезен.

Можно сделать вывод, что проблема тематического поиска для массового пользователя остается нерешённой.

Рассмотрим схему традиционного библиотечного взаимодействия: читатель – библиотека – библиотекарь – результат [12]. Читатель приходит со своим запросом в библиотеку, обращается к библиотекарю, получает результат (выполненная услуга, информационный ресурс — печатный и/или электронный) [12].

При выполнении тематического запроса от читателя особую важность приобретает первый этап — прием запроса [13]. Помочь читателю сформулировать тему — непростая задача, которую ежедневно решают библиографы. Кроме точно сформулированной темы, необходимо выяснить степень подготовки читателя (студент, аспирант и т.д.), цель запроса (курсовая работа, диссертация и т.д.), установить интересующие читателя виды документов (книги, статьи и т.д.), хронологические рамки и язык представления информации [13].

В условиях модернизации библиотечных процессов схема взаимодействия библиотеки и читателя изменилась: пользователь – проактивная библиотека – результат (электронные информационные ресурсы, выполненная услуга) [12]. Пользователь приходит в виртуальное пространство библиотеки со своим запросом, самостоятельно находит необходимый ему ресурс или обращается к цифровому сервису библиотеки и с его помощью получает необходимый результат [12].

В этой системе электронная библиотека получает сведения о пользователе из множества доступных источников, анализирует его персональные данные, историю поиска, запросы и предлагает информацию с опережением [12].

Информация является отражением индивидуально-личностных характеристик пользователя [12].

Следовательно, для решения проблемы тематического поиска при обработке запроса читателя должны учитываться его индивидуальные характеристики, такие как уровень подготовки, специальность, история поиска и др. Также должен быть разработан механизм, уточняющий запрос пользователя в удобном для него формате.

Очевидно, что следующим вопросом для рассмотрения является изучение способов хранения и использования личных данных пользователя, а также создания интерфейса, позволяющего уточнить запрос пользователя. Для последнего может быть целесообразно применение чат-ботов на основе машинного обучения.

Автором данной статьи было произведено исследование ЭБС СПбГУТ и обнаружены следующие недостатки: отсутствие мобильного приложения, трудоёмкий поиск, рассмотренный в этой статье. На данный момент времени идет разработка мобильного приложения. Следующим шагом после создания приложения является автоматизация тематического поиска.

Список используемых источников:

1. Юмашева, Ю. Ю. Историческая наука, архивы, библиотеки, музеи и искусственный интеллект: что день грядущий нам готовит? // Документ. Архив. История. Современность. 2021. № 21. С. 247-279.
2. Иванов В. К., Мескин П. И. Реализация генетического алгоритма для эффективного документального тематического поиска [Электронный ресурс] // Программные продукты и системы. 2014. №4 (108). С. 118-126. URL: <https://cyberleninka.ru/article/n/realizatsiya-geneticheskogo-algoritma-dlya-effektivnogo-dokumentalnogo-tematicheskogo-poiska> (дата обращения: 05.11.2022).
3. Арентова Т. Н. От доступа к информации – к пространству знаний и цифровой культуре: новые реалии для библиотек // Цифровое пространство библиотеки как среда интеллектуального развития личности : материалы межрегиональной науч.-практ. конф. 22–23 мая 2019 года / М-во культуры и архивного дела Сахалин. обл., Сахалин. обл. универс. науч. б-ка ; ред.-сост. Д. А. Ускова. – Южно-Сахалинск, 2019. С. 9-17.
4. Кутуева, Б. К. Информатизация вузовских библиотек Кыргызстана // М. Рыскулбеков атындагы Кыргыз экономикалык университетинин кабарлары. 2018. № 3(45). С. 78-80.
5. Нещерет, М. Ю. Цифровая библиография: библиотеки в поисках инновационных инструментов библиографической деятельности // Научные и технические библиотеки. 2021. № 7. С. 33-50.
6. Дементьев В. Е., Киреев С. Х. Выбор алгоритмов машинного обучения для классификации текстовых документов [Электронный ресурс] // Техника средств связи. 2022. №2 (158). С. 22-52. URL: <https://cyberleninka.ru/article/n/vybor-algoritmov-mashinnogo-obucheniya-dlya-klassifikatsii-tekstovyh-dokumentov> (дата обращения: 05.11.2022).
7. Епрев А. С. Автоматическая классификация текстовых документов [Электронный ресурс] // МСМ. 2010. №1 (21). С. 65-81. URL: <https://cyberleninka.ru/article/n/avtomaticheskaya-klassifikatsiya-tekstovyh-dokumentov-1> (дата обращения: 07.11.2022).
8. Электронно-библиотечная система Znanium Использование модуля Discovery Znanium [Электронный ресурс]: руководство читателя, 2020. 25 с. URL: <https://znanium.com/help/reader-discovery> (дата обращения: 06.11.2022).
9. Программно-аппаратный комплекс интеллектуального поиска и анализа больших массивов текстов TextAppliance [Электронный ресурс]. URL: <https://www.textapp.ru/> (дата обращения 07.11.2022).

10. Соченков И. В. Реляционно-ситуационные структуры данных, методы и алгоритмы решения поисково-аналитических задач : дис. ... канд. физ.-мат. наук: 05.13.17 / Соченков Илья Владимирович. Москва, 2014. 148 с.

11. «Znanium безвозмездно»: цивилизованный подход к ресурсам и технологиям открытого доступа [Электронный ресурс]. URL: <http://www.unkniga.ru/biblioteki/vuzbiblio/12817-znanium-bezvozmezdno-tsivilizovanniy-podhod-k-resursam-itehnologiyam.html> (дата обращения 06.11.2022).

12. Р. А. Барышев, И. А. Цветочкина, Е. Н. Касянчук, О. И. Бабина Модернизация процесса обслуживания пользователей университетских библиотек // Научные и технические библиотеки. 2022. № 3. С. 39-60.

13. Свирюкова В. Г. Организация и методика справочно-библиографического обслуживания: конспект лекций / отв. ред. Е. Б. Артемьева ; Гос. публич. науч.-техн. б-ка Сиб. отд-ния Рос. акад. наук. – 2-е изд., испр. и доп. – Новосибирск : ГПНТБ СО РАН, 2007. 64 с.

Yurchenko P.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Ways to solve the problem of thematic search in library activities.

In today's world, the amount of information is growing exponentially. As a result, the search for documents on a certain subject becomes a laborious process. This problem is most relevant in the library field. The article gives a brief overview of the current stage in the progress of libraries. The main data structures and methods for automatic text classification and formation of their semantic representation are considered. The possible solution to the problem of thematic search in library activities is proposed.

Key words: thematic search, machine learning, bibliographic service.

Секция 4.3.
Информационные технологии в дизайне

УДК 004.9
ГРНТИ 20.15.05

ПРОЕКТИРОВАНИЕ ВИЗУАЛЬНО-КОММУНИКАТИВНОЙ СОСТАВЛЯЮЩЕЙ ЭКОТРОП С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Д. М. Андрианов, А. А. Елькин, А. В. Федорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье доказывається актуальність і новизна застосування сучасних цифрових технологій в області екологічного туризму при розробці візуально-комунікативної складової екологічних троп. Дается визначення екотроп. Приводиться порівняльний аналіз кількох найбільш популярних в Ленінградській області екологічних маршрутів з точки зору використання на маршрутах цифрових технологій і сучасних засобів візуальної комунікації. Пропонується використання технологій доповненої реальності при проектуванні елементів візуально-комунікативної складової екологічних троп як один з варіантів застосування сучасних цифрових технологій в даній області

цифровые технологии, визуальные коммуникации, технологии дополненной реальности, экологический туризм, экологическая тропа

В настоящее время ни одну область современной жизни нельзя представить без инновационных IT-решений. Но степень внедрения цифровых технологий в различные аспекты нашей жизни также разная. С каждым годом все больше внимания уделяется окружающей среде, здоровому образу жизни. Вопрос оздоровления городского населения играет важную роль для формирования экологически культурного человека. Именно поэтому набирают популярность экологические тропы. Внедрение цифровых технологий в эту область благоприятно отразится на главных критериях: их привлекательности, доступности и информативности [1].

Сейчас в мире немало внимания уделяется вопросам решения экологических проблем. Именно поэтому набирает популярность ведение здорового образа жизни, экологический туризм (экотуризм). Также не стоит пренебрегать экологическим обучением и воспитанием тех, кто посещает природные территории.

Природную территорию можно с полным правом назвать музеем под открытым небом, если по ней проходит хорошо обустроенная экологическая тропа. Экологическая тропа (иногда ее называют учебно-туристическая тропа) – это специально разработанный познавательно-прогулочный маршрут или маршруты, прокладываемые обычно по территории парков, заповедников, заказников, оснащенные информационными указателями и служащие для экологического просвещения населения. Подобно тому как в музее экспонаты и тексты помогают разобраться в серьезных проблемах, экотропа в природе делает интересным и понятным то, на что раньше не было обращено внимание, что казалось непонятным и неизведанным [2].

В данный момент на уже существующих экотропах средств визуальной коммуникации и информационных объектов, использующих цифровых технологии, недостаточно. Некоторые тропы и вовсе не оснащены средствами, использующими современные технологии. На некоторых экологических тропах технологии применяются, но они являются устаревшими. Поскольку развитие технологий происходит повсеместно, то необходимо внедрять нововведения и в области цифровых технологий в совокупности с экологическим просвещением человека.

В результате изучения первоисточников и практического посещения мест, о которых идет речь, был проведен сравнительный анализ нескольких уже существующих экологических маршрутов в Ленинградской области. Итоги эксперимента представлены в таблице 1. По результатам этого анализа можно сказать, что большинство экологических и учебно-тренировочных троп в полной мере не оснащены элементами и средствами, использующими цифровые технологии. Имеется небольшое количество средств визуальных коммуникаций. В то время как маршрутный путь представлен разными уровнями сложностями и не всегда прост в освоении и навигации.

ТАБЛИЦА 1. Сравнительный анализ экологических маршрутов Ленинградской области

Название	Расположение	Протяженность	Уровень сложности	Цифровые технологии	Средства визуальных коммуникаций
Оредежская тропа	дер. Белогорка–Новосиверская	11,5 км	Тяжелый	Небольшое количество (Цифровой плакат маршрута)	Среднее количество
Экотропа в Гатчине	г. Гатчина	5 км	Умеренный	(Цифровой плакат маршрута, информационная статья)	Небольшое количество
Комаровский берег	п. Комарово	2,8 км	Умеренный	Отсутствуют	Небольшое количество
Западный Котлин	г. Кронштадт	1,5 км	Легкий	Отсутствуют	Небольшое количество
Сиверский	пгт. Сиверский	3 км	Легкий	Небольшое количество (Цифровой плакат маршрута, информационная статья)	Среднее количество

Таким образом, несмотря на развивающееся направление экологического туризма, цифровые технологии почти не нашли применения в данной области. Актуальность и новизна идеи также подчеркивается недостаточным количеством публикаций в данной области. На данный момент недостаточно реализованных проектов, проясняющих современные подходы и технологии проектирования, организации методической работы, а также средств визуальных коммуникаций в социоприродной среде [3, 4].

Исходя из вышесказанного, разработчикам проектов в области экотуризма и последователям распространения здорового образа жизни стоит обратить внимание на технологии дополненной реальности (AR). Они позволят внедрять недостающие элементы природных и архитектурных памятников, также воссоздать уже разрушенные объекты и демонстрировать их пользователям в

режиме реального времени с помощью смартфонов. Пользователи смогут окунуться в атмосферу прошлого, изучить информационную составляющую представленного объекта. А внедрение интерактивных средств визуальной коммуникации скажется на заинтересованности новых пользователей – потенциальных посетителей экотроп.

Список используемых источников:

1. ОСНОВНЫЕ АСПЕКТЫ СОЗДАНИЯ ЭКОЛОГИЧЕСКИХ МАРШРУТОВ В ГОРОДСКОЙ СРЕДЕ: Современные проблемы науки и образования [Электронный ресурс]. URL:<https://science-education.ru/ru/article/view?id=28198/> (дата обращения 12.11.2022).
2. Успехи современного естествознания: ЭКОТРОПА КАК СРЕДСТВО ФОРМИРОВАНИЯ ЭКОЛОГИЧЕСКОЙ КУЛЬТУРЫ И РАЦИОНАЛЬНОГО ПРИРОДОПОЛЬЗОВАНИЯ [Электронный ресурс]. URL: <https://natural-sciences.ru/ru/article/view?id=36200/> (дата обращения 12.11.2022).
3. В.С. Черняк., О.Н. Левшук/ РОЛЬ ЭКОТРОП В ФОРМИРОВАНИИ ЭКОЛОГИЧЕСКОГО ПРОСВЕЩЕНИЯ НАСЕЛЕНИЯ Г. ПИНСКА // ВКР. 2017г., страницы 352-353.
4. Чижова, В.П. Школа природы. Экологическое образование в охраняемых природных территориях. –М.:Эколого-просветительский центр «Заповедники» -1997. – 128с.

Andrianov D., Elkin A., Fedorova A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Designing the visual and communicative component of ecotrope using modern digital technologies.

The article proves the relevance and novelty of the use of modern digital technologies in the field of ecotourism in the development of the visual and communicative component of ecological trails. The definition of ecotrope is given. A comparative analysis of several of the most popular ecological routes in the Leningrad Region is given in terms of the use of digital technologies and modern means of visual communication on routes. The use of augmented reality technology in the design of elements of the visual and communicative component of ecological trails is proposed as one of the options for the use of modern digital technologies in this area

Key words: *digital technologies, visual communications, augmented reality technologies, ecotourism, ecological trail.*

УДК 004.946
ГРНТИ 28.17.33

ОБ ИСПОЛЬЗОВАНИИ ПРОГРАММНЫХ И АППАРАТНЫХ СРЕДСТВ ДЛЯ РАБОТЫ С ИНФОГРАФИКОЙ В VR

Е. П. Бояшова, М. В. Мельников

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена рассмотрению программных и аппаратных средств, которые могут использоваться для работы с инфографикой в виртуальной реальности. Аппаратные средства рассматриваются в том числе с точки зрения доступности для пользователей. В работе описываются создание и проверка работоспособности веб-приложения для отображения данных с временной привязкой с использованием API WebXR и JavaScript-библиотеки Three.js.

инфографика, виртуальная реальность, информация, данные, представление данных, WebXR, Three.js

Инфографика – графический способ подачи информации, обеспечивающий наглядное и гармоничное визуальное представление данных.

Использование инфографики способствует упрощению восприятия данных и скорости их обработки, потому что человеческий мозг обрабатывает визуальные образы значительно быстрее текста. Графическое представление информации считается наиболее удобным для восприятия.

Однако, несмотря на обширное использование инфографики, актуальной остаётся проблема восприятия сложных, объёмных данных, связей, структур и зависимостей, а также данных, изменяющихся в времени.

Кроме того, для повышения эффективности восприятия информации появляется необходимость использования новых способов взаимодействия с инфографикой.

Инфографика может быть представлена как на физических, так и на электронных носителях. С появлением технологий виртуальной и дополненной реальности, дающих новые возможности представления информации, стал возможным перенос инфографики в новую среду отображения [1].

Использование виртуальной реальности для отображения инфографики позволяет погрузить пользователя в трёхмерное пространство, сфокусировать его внимание на необходимой информации. Это способствует более широкому и полному восприятию представленных с помощью инфографики данных.

Использование инфографики в виртуальной реальности целесообразно для отображения сложных, объёмных многомерных данных, демонстрации процессов, временных шкал, визуализации сложных зависимостей, связей и др. Важно отметить, что в среду виртуальной реальности не имеет смысла помещать такой инфографики, которая может быть отражена на привычных носителях в достаточно удобном для восприятия и изучения виде [1].

Использование виртуальной реальности расширяет возможности взаимодействия пользователя с интерактивной инфографикой благодаря передаче информации о движениях человека и использованию манипуляторов.

Для погружения в виртуальную реальность необходимо использование VR-шлема или очков виртуальной реальности, представляющих собой устройство с линзами, устанавливаемое на смартфон. Среди распространённых систем виртуальной реальности можно выделить HTC Vive, Oculus Rift. Кроме того, требуется специальное программное обеспечение.

Самый доступный способ использования VR – очки виртуальной реальности. Они отличаются невысокой стоимостью, поскольку работают в качестве стереоскопа, а изображение отображается на экране смартфона.

Использование подобного решения для представления инфографики позволяет существенно расширить круг пользователей, которые смогут работать с информационной графикой в режиме виртуальной реальности, поскольку оно является достаточно доступным. Кроме того, его можно назвать портативным.

Для реализации приложений целесообразно использовать веб-технологии. В этом случае пользователям достаточно перейти по ссылке в браузере на смартфоне. Такой подход не требует установки дополнительного программного обеспечения, за исключением, например, Google VR Services на Android.

Обобщая приведённые материалы, можно выделить следующие преимущества отображения инфографики в виртуальной реальности на смартфонах с VR-очками в веб-браузере:

- низкий порог вхождения – для работы необходимы недорогие VR-очки и смартфон;
- отсутствие необходимости установки различного программного обеспечения;
- простота взаимодействия с виртуальной средой – возможна разработка таких приложений, которые не требуют отдельного манипулятора для работы.

Для доступа к виртуальной и дополненной реальности в браузере существует API WebXR [2]. Он описывает поддержку доступа к таким устройствам, как HTC Vive, Oculus Rift, устройствам, совместимым с Google Cardboard и др.

На мобильных устройствах WebXR поддерживается, по крайней мере, на смартфонах с ОС Android и браузером Google Chrome [3]. Для работы с WebXR требуется подключение к серверу по протоколу HTTPS.

Поддержка контента в виртуальной реальности обеспечивается различными фреймворками, среди которых можно выделить Three.js, Babylon.js, A-Frame и др.

Обозревая фреймворки для реализации функций AR и VR в веб-среде и выявляя оптимальные решения, А. В. Терентьев и А. С. Фролова отмечают, что оптимальным решением является Three.js, поскольку он имеет обширный функционал, проработанную документацию и понятный синтаксис JavaScript [4].

В рамках работы для демонстрации возможности использования инфографики в виртуальной реальности разработан прототип веб-приложения,

отображающего данные с временной привязкой на таймлайне (линии времени). Оно реализовано с использованием API WebXR и JavaScript-библиотеки Three.js. Для работы с джойстиком используется Gamedpad API [5], который позволяет разработчикам получить доступ к сигналам с джойстиков и других контроллеров и работать с ними.

Прототипами для представления данных подобным образом послужили проекты Museum of the World [6] и Tower of London 3D [7], где информация представлена на линии времени в 3D.

Работоспособность приложения и сама возможность отображения инфографики в виртуальной реальности протестированы на устройстве OnePlus 9RT с операционной системой Android 12 и браузером Google Chrome 107 с VR-очками SMARTERRA VR Sound Max с джойстиком.

Скриншот приложения в режиме VR представлен на рис. 1.

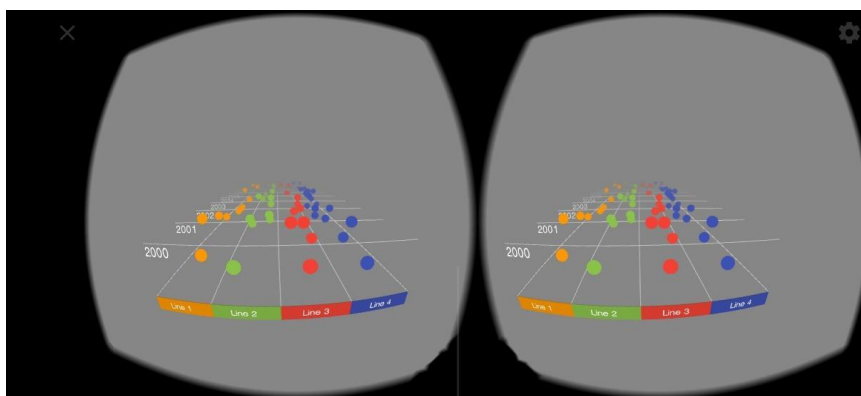


Рис. 1. Скриншот веб-приложения для отображения линии времени в VR

На рис. 2 показано отображение данных на дисплее устройства до переключения в режим VR.

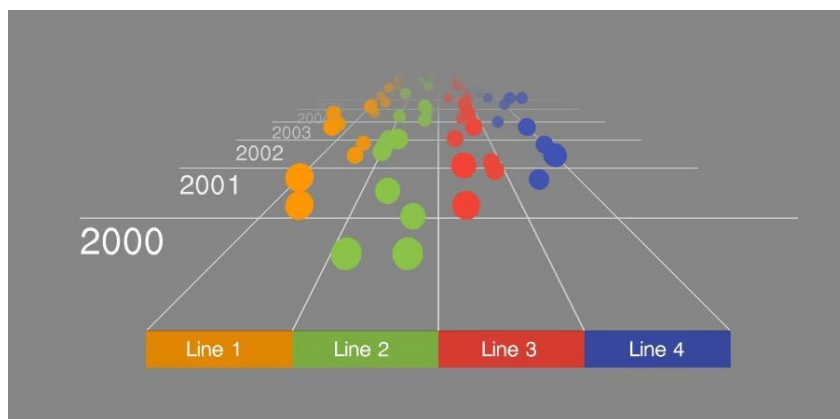


Рис. 2. Скриншот веб-приложения

Пользователь имеет возможность перемещаться по линии времени с помощью джойстика вперёд или назад, а также выбирать конкретную линию, отмеченную цветом (рис. 3). Кроме того, изображение зависит от того, на какую точку смотрит пользователь, что достигается за счёт передачи оборудованием (смартфоном) информации о движении человека.

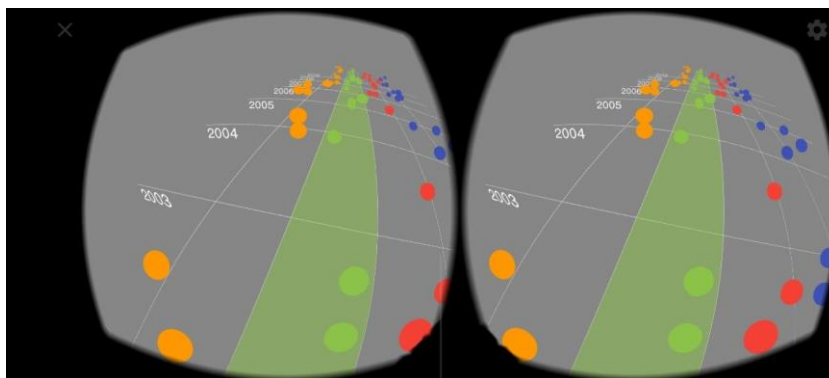


Рис. 3. Скриншот веб-приложения для отображения линии времени в VR

Подводя итоги, можно сделать вывод, что наиболее доступным способом использования VR являются очки для смартфона. Использование подобного решения для представления инфографики позволяет существенно расширить круг пользователей, которые смогут работать с инфографикой в режиме VR.

При этом доступ к приложению может осуществляться через браузер. В таком случае для разработки могут использоваться API WebXR и, например, JavaScript-библиотека Three.js.

Список используемых источников:

1. Бояшова Е. П., Мельников М. В. Возможности отображения инфографики в виртуальной реальности // Региональная информатика (РИ-2022) : материалы XVIII междунар. конф., СПб, 26–28 окт. 2022 г. СПб : СПОИСУ, 2022. С. 542–543.
2. WebXR Device API [Электронный ресурс]. URL: <https://www.w3.org/TR/webxr/Overview.html> (дата обращения: 25.10.2022).
3. WebXR Device API – Web APIs | MDN [Электронный ресурс]. URL: https://developer.mozilla.org/en-US/docs/Web/API/WebXR_Device_API (дата обращения: 25.10.2022).
4. А. В. Терентьев, А. С. Фролова Обзор фреймворков для реализации функций AR и VR в Web-среде // Интернаука. 2021. № 20 [Электронный ресурс]. URL: <https://internauka.org/journal/science/internauka/196> (дата обращения: 07.11.2022).
5. Gamepad API – Web APIs [Электронный ресурс]. URL: https://developer.mozilla.org/en-US/docs/Web/API/Gamepad_API (дата обращения: 10.11.2022).
6. Museum of the World [Электронный ресурс]. URL: <https://britishmuseum.withgoogle.com/> (дата обращения: 20.10.2022).
7. Tower of London 3D [Электронный ресурс]. URL: <https://www.tiki-toki.com/timeline/entry/137152/Tower-of-London-3D> (дата обращения: 20.10.2022).

Bojashova E., Melnikov M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

About using software and hardware to work with infographics in VR.

The work is devoted to the consideration of software and hardware that can be used to work with infographics in virtual reality. Hardware is also considered in terms of accessibility for users. The paper describes the creation and testing of a web application for displaying time-based data using the WebXR API and the Three.js JavaScript library.

Key words: infographics, virtual reality, information, data, data representation, WebXR, Three.js.

УДК 004.921
ГРНТИ 20.53.21

МЕТОДЫ ВИЗУАЛИЗАЦИИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ИНФОГРАФИКИ

Д. А. Джапарова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья посвящена применению инфографики как один из методов визуализации информации на примере применения её при разработке модели системы взаимодействие пользователя с интернет-магазином комнатных растений.

визуализация, инфографика, метод, графический способ, графический дизайн

Визуализация в общем смысле – это метод предоставления информации в виде оптического изображения (например, график, диаграмма, таблица и т.д.)

Рассматривая визуализацию данных как частный случай, то можно сказать, что инфографика есть графический способ представления данных, информации и знания. Инфографика имеет широкий спектр применения - используется в образовательных материалах, рекламе, статистике, журналистике, городской навигации, интернет-маркетинге и т.д. Она может быть представлена совершенно в разных формах, например, иконка, фавекон, карикатура, эмблема, опознавательные знаки, «линия времени», схема и т.д. Главное, чтобы это эффективно работала для выполнения поставленных целей, создателями инфографики.

Проще говоря, инфографика – это любая комбинация текста и графики с целью преподнесения сложной и объемной информации в упрощенной и наглядной форме.

Понятие «инфографика» будет определяется следующим образом: инфографика – это область графического и коммуникативного дизайна, в основе которого лежит представление информации, связей, числовых данных и знаний [1].

Отображение большого объема информации графическим способом это не главное преимущество инфографики. С помощью её откидывается вся второстепенная по значимости и важности информация и преподносится пользователю только суть данных. Также, это сильно влияет на скорость усваивания знаний, что является важным показателем при создании инфографики в любом её виде.

Первым делом при создании инфографики необходимо определить цели и задачи, достигаемые с помощью данного графического элемента.

Далее в зависимости от сложности и объемности информации нужно разбить данные на разделы или части. По возможности каждый раздел представляем отдельным изображением, подбирая наиболее знакомые и часто используемые визуальные образы вашей целевой аудитории.

И заключительным шагом надо выделить главный элемент, вокруг которого будет строиться инфографика, тем самым настраивая фокус внимания пользователя на главной цели создания.

При создании пользовательского интерфейса из-за обилия информации на странице необходимо тщательно продумывать каждый блок страницы и его наполнение.

Основываясь на ряде наблюдений, психологи утверждают о том, что пользователь в первые 8 секунд просмотра страницы сайта принимает решение о продолжении нахождения на данном ресурсе. Ключевую роль в данном решении играет представленный визуальный ряд, на котором акцентируется внимание посетителя страницы.

У инфографики в 30 раз больше шансов быть прочитанной, чем у статьи, содержащей ту же информацию. По статистике, контент-маркетинг с использованием визуальных элементов генерирует более 94% просмотров, а трафик сайтов, использующих инфографику, растёт на 12% быстрее, чем у остальных.

Тем самым инфографика помогает в продвижении ресурса следующим способом:

- преподносит информацию в простом и понятном виде;
- повышает юзабилити сайта;
- увеличивает трафик за счет количества просмотров ресурса;
- способствует вирусному распространению контента.

В разработке простой инфографики не стоит выбирать более трех цветов, в более сложной более пяти. Так восприятию элемента не будет мешать обилие цвета, вызывая раздражение. Желательно, при разработке придерживаться уже выбранной цветовой гаммы пользовательского интерфейса, выдерживая стиль проекта. Графические элементы не должны перегружать изображение.

На рис. 1 представлены элементы инфографики для пользовательского интерфейса интернет-магазина комнатных растений. Данные иконки располагаются в шапке меню, в карточке товара, в фильтрах каталога и на странице корзины.

Выполнены они в цветовой гамме данного ресурса, использовано всего два основных цвета. Используя представленную инфографику сложностей при считывании у пользователей не возникает, иконки передают четкие и однозначные образы и на странице смотрятся уместно.

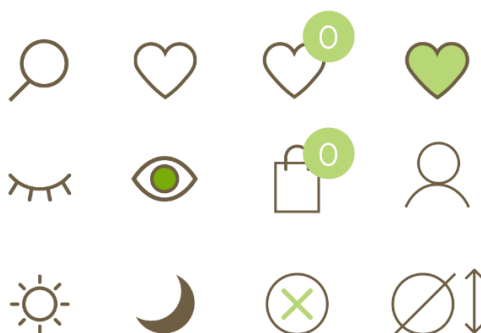


Рис. 1. Элементы инфографики

Для наглядности использования на странице представлен рис. 2. На данном рисунке изображена карточка товара. В верхнем правом углу располагаются иконки «Избранное» и «Быстрый просмотр», в нижней части знак диаметра и высоты растения с числовым обозначением.

Также предусмотрено взаимодействие с иконками, располагающимися в правом верхнем углу. Нажав на «Избранное», иконка меняет цвет, тем указывая на завершения действия по добавлению товара в список избранных, а наведя курсор на «Быстрый просмотр» иконка имитирует открытие глаза, предоставляя пользователю возможность открыть дополнительное окно для просмотра дополнительной детальной информации о товаре.

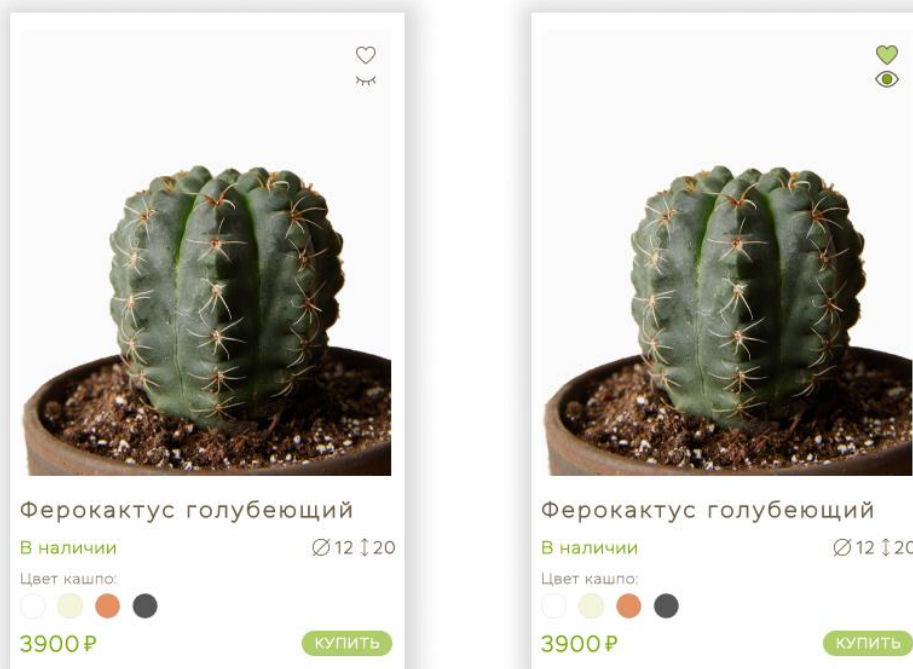


Рис. 2. Вариант использование графических элементов

Таким образом, внедрение даже такой простой инфографики на страницах сайта является мощным инструментом визуальной коммуникации, при этом временные и материальные траты являются минимальными. Такое визуальное отображение сильно ускоряет восприятие информации, побуждает к коммуникациям с ресурсом в дальнейшем приводя к продажам продукции.

Список используемых источников:

1. Reasons Infographics Are Poison And Should Never Be Used On The Internet Again // Business Insider [Электронный ресурс]. – URL: <http://www.businessinsider.com/infographics-mustdie-2013-6> (дата обращения 14.11.2022).

2. Лаптев, В.В. Изобразительная статистика. Введение в инфографику / Владимир Лаптев. – СПб.: Эйдос, 2012. – 180 с.

3. Джин Желязны «Говори на языке диаграмм: Пособие по визуальным коммуникациям» / Манн, 2016. - 290 с.

Dzhararova D.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Information visualization methods using infographics.

This article is devoted to the use of infographics as one of the methods of visualizing information on the example of its application in the development of a model of the user interaction system with an online store of indoor plants.

Key words: visualization, infographics, method, graphic method, graphic design.

УДК 004.51
ГРНТИ 50.41.29

К ВОПРОСУ ОБ ОРГАНИЗАЦИИ ЭФФЕКТИВНОГО ВЗАИМОДЕЙСТВИЯ ПРЕПОДАВАТЕЛЯ И СТУДЕНТА В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ ВУЗА

О. П. Диброва, Е. П. Бояшова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена проблеме взаимодействия обучающегося и преподавателя посредством использования элементов информационно-образовательной среды. Важность качества процесса коммуникации рассматривается со стороны влияния на уровень восприятия информации и эффективность учебного процесса. Автором предложен вариант решения проблемы посредством проектирования информационной системы с помощью UML-моделирования, а также построена диаграмма прецедентов. Рассматриваемая тема будет интересна специалистам информационных систем, разрешающих вопрос взаимодействия пользователей, в частности, в рамках образовательного процесса.

информационная система, личный кабинет, информационно-образовательная среда, коммуникация, образовательный процесс, восприятие информации

Обеспечение высокого и качественного уровня образования – это одна из важнейших целей современного общества. В 2020 году к уже существующим сложностям (ещё до начала эпидемии по статистике ЮНЕСКО на 2020 год почти 800 миллионов взрослых людей в мире оставались безграмотными) глобальная эпидемия добавила новые (недоступность учебного материала электронного формата, сложности с техническим обеспечением преподавателей и обучающихся, остановка учебного процесса в малоимущих странах и т.д.). Среди основных проблем образования, обостренных с течением эпидемии, невозможность организовать полноценное дистанционное обучение оказала достаточно значительное влияние на качество учебного процесса [1]. В условиях пандемии каждое образовательное учреждение по-своему подходило к реализации дистанционного формата и выбору подходящей среды, и чаще всего выбор сводился к их сочетанию, что создавало ряд проблем как для обучающихся, так и для преподавателей: разрозненность и дублирование данных, информационный шум в потоке получаемой информации [2]. Во многих учебных заведениях образование строится на тесном взаимодействии преподавателя со студентами. Помимо проблем с ограниченной функциональностью доступных платформ, остро встает вопрос низкого качества интерфейса образовательных информационных систем: проблема в отсутствии должной технической подготовки пользователей негативно сказалась на качестве коммуникации между обучающимися и преподавателями.

Среди прочего, уровень обеспеченности образовательного процесса цифровыми технологиями влияет и на успеваемость обучающихся, что является особо актуальной проблемой для высших учебных заведений. В рамках

исследований о влиянии использования элементов Персональной образовательной среды на успеваемость студентов и их мотивацию к обучению проверена гипотеза о взаимосвязи используемых элементов информационно-образовательной среды и показателями успеваемости: чем чаще студенты посещают личный кабинет, тем выше они оценивают его полезность, тем меньше у них средняя оценка за сессию, больше число пересдач. То есть частота использования студентами личного кабинета обратно пропорциональна успеваемости [3], но это не говорит о негативном влиянии информационно-образовательной среды на обучающихся. Напротив, помимо основных функций, доступных в личном кабинете, студенты с низким баллом и задолженностями чаще используют образовательный сервис для поиска учебного материала и связи с преподавателями, в отличие от успевающих студентов. Из этого следует, что данный сервис имеет особую важность в помощи отстающим студентам, а значит появляется потребность в упрощении алгоритма взаимодействия пользователя личного кабинета с объемом хранимой в нем информации (сообщения, полученные и отправленные файлы). Проще говоря, чем легче студенту будет разобраться во множестве учебного материала по разным дисциплинам и в сообщениях от разных преподавателей, тем в большей степени он будет замотивирован на закрытие долга.

Среди проблем, связанных со сложностями коммуникации, существует и сложность в адаптации иногородних студентов малых городов к обучению в вузе [4]. Так около 30% из них сталкиваются с барьерами в общении с профессорско-преподавательским составом, а у 19% вызывают трудности отличия системы школьного образования от вузовского. Студенты, находящиеся в процессе сепарации от родителей, испытывают тревожность и проявляют высокую необходимость в поддержке [5]. В связи с вышеперечисленным, для успешного прохождения адаптации студента к новой среде вузу необходимо предоставлять возможность беспрепятственного взаимодействия обучающегося с другими структурами университета в условиях информационно-образовательной среды.

Сегодня трудно представить обучение без использования онлайн-платформ. Основным из инструментов, при помощи которого может осуществляться обучение в заочном формате, в большинстве учебных заведений, как и в СПбГУТ, является сайт личного кабинета. Личный кабинет студента – это сервис доступа ко всей информации, необходимой для обучения (расписание занятий, результаты освоения программы, личные сведения студента, новости и основные события), а также портал для взаимодействия студента с другими структурами университета (преподавательский состав, деканат, администрация и др.).

Именно поэтому так важно уделить внимание разработке интуитивно понятного интерфейса и унифицированной модели общения внутри единого портала для образовательного учреждения.

Обратимся к примеру личного кабинета СПбГУТ. Одним из недостатков в существующей информационной системе является устаревшая модель системы сообщений: из-за отсутствия расширенного поиска, сортировки и упорядочивания, личных диалогов с историей переписки, а также пересечение с

другими разделами системы при выполнении задачи обмена файлами значительная часть пользователей пренебрегает чтением новых сообщений и с высокой долей вероятности упускает важную информацию.

Целью данной работы является подготовка к проектированию системы сообщений, упрощающей процесс восприятия информации, внутри информационно-образовательной среды посредством построения UML-диаграмм.

Помимо первостепенного назначения – отправки и получения сообщений – разрабатываемая система должна решать следующие задачи:

- расширенный поиск при выборе адресата;
- возможность добавления тэгов (меток для классифицирования данных) для автоматизирования процесса сортировки полученных сообщений;
- сортировка входящих сообщений по «папкам»;
- упорядочивание входящих и исходящих сообщений.

Начальная работа над проектированием системы осуществляется с помощью объектно-ориентированного подхода. В качестве языка моделирования выбран унифицированный язык объектно-ориентированного моделирования Unified Modeling Language (UML).

Система предполагает взаимодействие с 4 актерами:

- разработчик информационной системы (1 уровень доступа) – взаимодействует с системой с целью проверки и поддержания ее работоспособности, исправления ошибок и улучшения работы;
- студент (2 уровень доступа) – взаимодействует с системой в качестве ее пользователя с целью использования информации из системы и снабжения ее информацией, имеется возможность взаимодействия с актерами «Преподаватель», «Сотрудник администрации вуза»;
- преподаватель (2 уровень доступа) – взаимодействует с системой в качестве ее пользователя с целью использования информации из системы и снабжения ее информацией, имеется возможность взаимодействия с актерами «Студент», «Сотрудник администрации вуза»;
- сотрудник администрации вуза (2 уровень доступа) – взаимодействует с системой в качестве ее пользователя с целью использования информации из системы и снабжения ее информацией, имеется возможность взаимодействия с актерами «Преподаватель», «Студент».

Для более детального представления продукта, его функциональности и поведения, построена диаграмма прецедентов системы, представленная на рис. 1.

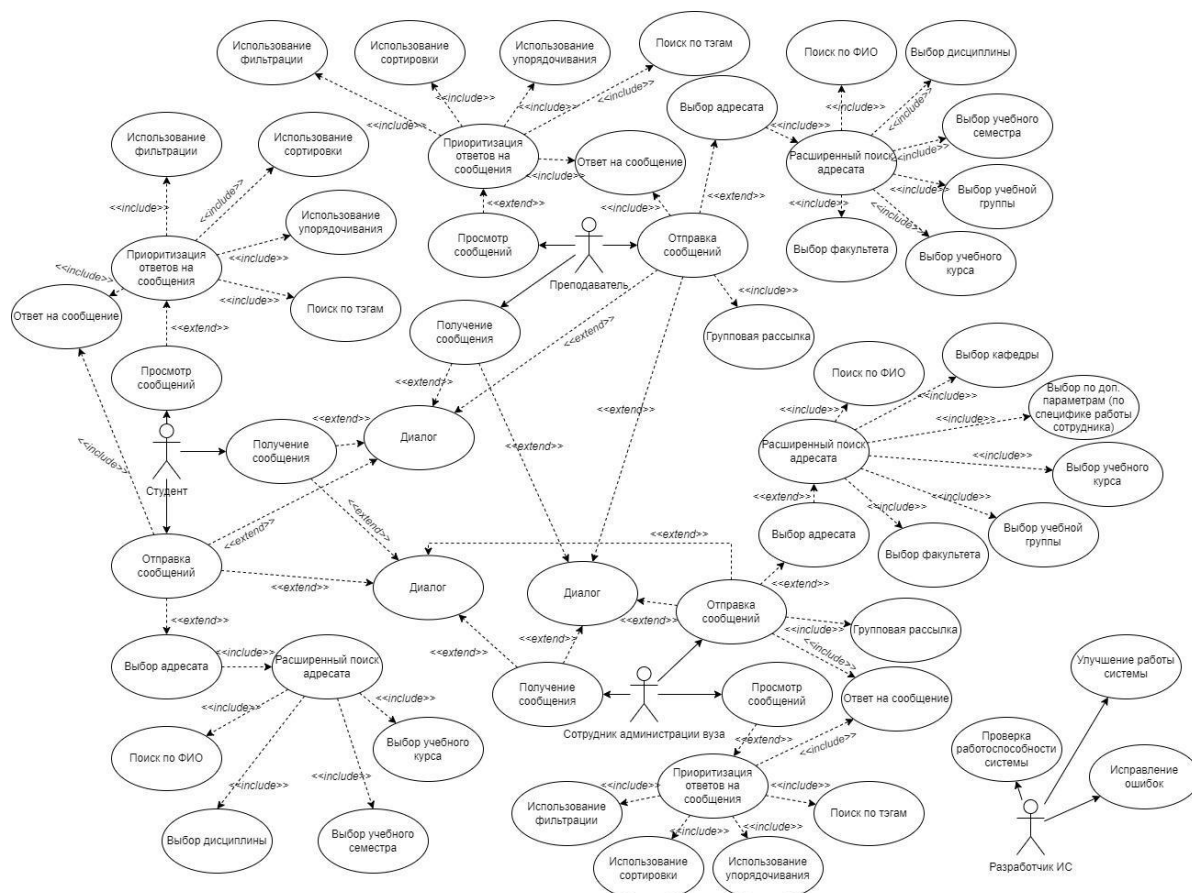


Рис. 1. Диаграмма прецедентов

Для отражения потока событий, происходящих в рамках варианта использования системы, необходимо построение диаграмм последовательности, как минимум, для следующих прецедентов: приоритизация ответов на сообщения, отправка сообщения от студента преподавателю, групповая рассылка от преподавателя, расширенный поиск адресата сообщения.

Произведенный анализ проблемной ситуации позволяет сделать выводы об острой необходимости в разработке системы для взаимодействия пользователей внутри информационно-образовательной среды с уклоном на упрощение процесса восприятия информации. С использованием описания информационной системы, спроектированной диаграммы прецедентов и поставленными задачами для диаграмм последовательности разработчик, минуя данные этапы, сможет перейти к детальной проработке системы для информационно-образовательного портала, в результате получит качественный продукт, использование которого положительно скажется на взаимодействии преподавателей и обучающихся, тем самым и на качестве уровня образования.

Список используемых источников:

1. Блог компании Zachnik: Как пандемия повлияла на образование [Электронный ресурс]. URL: <https://zaochnik.ru/blog/kak-pandemija-povlijala-na-obrazovanie/> (дата обращения 12.11.2020).
2. Васильченко В.Д. Вопросы исследования проблематики интерфейсов систем дистанционного обучения для определения концепции решения // Подготовка профессиональных кадров в магистратуре для цифровой экономики. С. 251-256.

3. Погребников А.К., Шестаков В. Н., Якунин Ю. Ю. Влияние использования элементов персональной образовательной среды на успеваемость студентов и их мотивацию к обучению // Информатика и образование. 2020. N 1 (310). С. 42–50.

4. Дворникова Е.В., Кошелева А. В. Практика адаптации иногородних студентов малых городов к обучению в вузе (на примере ФСПН ЯРГУ им. П.Г. Демидова). // International Journal of Medicine and Psychology. 2020. Т. 3. N 6. С. 51–55.

5. Сысоева Л.В., Петренко Т. В. Психолого-педагогическое сопровождение студентов в прохождении сепарационных процессов на различных этапах обучения в вузе // Гуманизация образовательного пространства. 2016. С. 530–536.

Dibrova O., Boyashova E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

On the issue of organizing effective interaction between a teacher and a student in the educational process of a university.

The article is devoted to the problem of interaction between the student and the teacher through the use of elements of the information and educational environment. The importance of the quality of the communication process is considered from the side of influence on the level of perception of information and the effectiveness of the educational process. The author offers a solution to the problem by designing an information system using UML modeling, and also a precedent diagram is constructed. The topic under consideration will be of interest to specialists of information systems that resolve the issue of user interaction, in particular, within the educational process.

Key words: *information system, personal account, information and educational environment, communication, educational process, information perception.*

УДК 004.422.832

ГРНТИ 50.41.25

ПРОЕКТИРОВАНИЕ АРХИТЕКТУРЫ РЕНДЕРЕРА ОБЩЕГО НАЗНАЧЕНИЯ НА ОСНОВЕ VULKAN API

Г. В. Ежов

Поволжский государственный университет телекоммуникаций и информатики

Vulkan API является самым обширным и функциональным средством взаимодействия с драйвером GPU, что делает процесс проектирования программ с его использованием нетривиальной задачей. Автор представляет собственный вариант реализации архитектуры рендерера в качестве одного из возможных решений данной проблемы.

проектирование архитектуры, графический API, Vulkan, рендерер, движок отрисовки

Vulkan является современной вариацией графического API, целью которого является предоставление слоя абстракции над работой драйвера графического процессора. Его преимуществом над более ранними API является изначальная архитектура взаимодействия с драйвером, позволяющая работать со всеми особенностями современных GPU в явном виде.

Под явной работой понимается подробное описание операций, производимых графическим процессором, которое позволяет значительно снизить нагрузку на драйвер видеокарты. Также Vulkan позволяет создавать и отправлять команды на выполнение графическому устройству в полноценном многопоточном режиме. Уменьшается несоответствие кода при компиляции программ разных шейдерных языков путём перехода на единый формат байт-кода под названием SPIR-V, который обрабатывается единственным компилятором, предоставляемым Vulkan.

Такое признание всех возможностей современных GPU с объединением всего графического и вычислительного функционала в единый API, предоставление интерфейса для работы с современными графическими технологиями приводят к одной известной инженерной задаче в виде проектирования эффективной архитектуры рендерера общего назначения на основе этого API [1].

Движок рендеринга может быть спроектирован разными способами. Единого общепринятого подхода в данном случае нет, но можно приблизиться к максимально удобному и гибкому решению, которое подойдёт для большинства проектов.

Часто программы для отрисовки графики проектируются, основываясь на некоторых фундаментальных принципах, определяемых аппаратной частью, от которой они зависят. В данном случае будет рассматриваться общий подход через призму интерфейса Vulkan, который может использоваться для широкого ряда целевых платформ.

Один из распространённых эффективных подходов к проектированию рендеринга состоит в том, чтобы использовать многоуровневую архитектуру, подобную представленной на рис. 1.



Рис. 1. Средства рендерера для низкоуровневой отрисовки

Низкоуровневый рендеринг охватывает все средства движка для предварительной обработки. На данном уровне абстракции важно представлять, что в первую очередь для отрисовки очередного кадра необходимо учесть все компоненты сцены, которые могут в нём участвовать. Пока что не рассматривается возможность отбраковки лишних объектов, лишь их отображение в виде набора геометрических примитивов и других концептуальных для кадра данных [2].

Следующий уровень абстракции представит более чёткое видение архитектуры рендерера. На этом этапе более подробно рассматривается разбиение отрисовщика на две принципиальных части – интерфейс графического устройства и, собственно, сами компоненты сцены.

Часть интерфейса графического устройства, в сущности, является ядром программы и представляет собой низкоуровневую реализацию рендерера на Vulkan. Оно производит всю основную инициализацию необходимых для отрисовки кадра ресурсов. При этом данная часть системы не привязана напрямую к пользовательскому приложению и при желании может быть выделена в отдельный фреймворк. В связи с этим ядро системы можно назвать бэкендом программы [3].

Пользовательское приложение представляет из себя программу, которая демонстрирует возможности реализованного движка рендерера. Оно использует низкоуровневое ядро отрисовщика для записи команд в очередной проход отрисовки, после чего результат работы рендерера возвращается в виде объекта изображения. Получившийся кадр отображается на экране в соответствии с выбранным режимом показа.

Абстрактное представление спроектированной системы представлено на рис. 2. Здесь изображены все ключевые элементы рендерера, которые разбиты на две основные части – Frontend и Backend. Данная терминология имеет отличие от Web-приложений и, как было ранее упомянуто, бэкенд в данном случае – это

часть программы, выполняющая низкоуровневую работу с памятью и графическим устройством, а фронтенд – это приложение, позволяющее загружать данные о двух/трёхмерных объектах и каким-либо образом взаимодействовать с отображаемой виртуальной сценой.

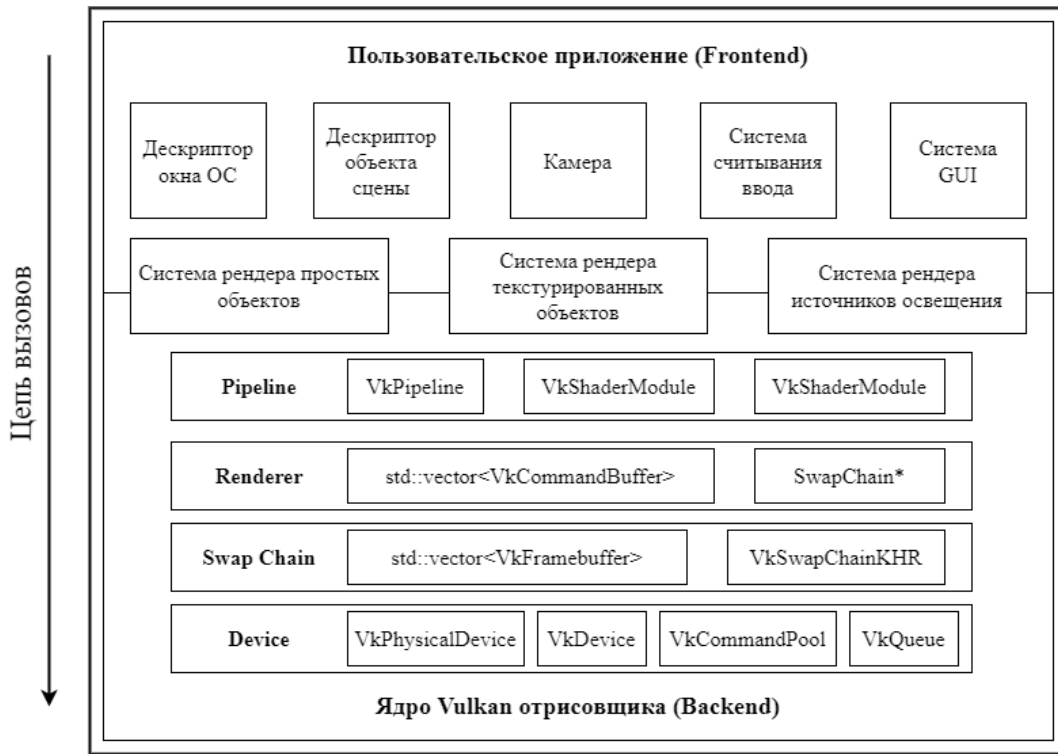


Рис. 2. Модель архитектуры системы рендера

Ядро отрисовщика состоит в основном из последовательной инициализации требуемых ресурсов. Важнейшие объекты для совершения вызовов к графическому устройству определяются в объекте Device. Он включает в себя дескрипторы для объектов физического и логического устройств, поверхности окна ОС, очереди для выполнения команд на отрисовку, а также пул команд, из которого выделяются специальные буферы для их записи команд.

В Vulkan отсутствует буфер для отрисовки кадра по умолчанию, в отличие от того же OpenGL, поэтому в нём для реализации хранения буферов кадров используется специальный объект, называемый цепью обмена (Swap Chain). Помимо простого хранения кадров, цепь обмена связывает их в очередь и создаёт специальные условия для их показа на поверхность окна.

Экземпляр Renderer – это именно тот объект, который используется приложением для записи команд на отрисовку объектов сцены. Рендерер предоставляет перечень функций, которые используются для получения буфера кадра, отвечающего за текущее изображение в цепи обмена, и отправки информации о содержимом сцены в очередь на обработку графическим устройством.

Объект Pipeline отвечает за создание такого экземпляра графического конвейера, который будет соответствовать общим задачам отрисовки графики. Пользовательское приложение наиболее тесно связано именно с данной частью

рендера, поскольку через неё можно тонко настроить параметры различных этапов отрисовки сцены.

После инициализации ресурсов Vulkan поток управления переходит к пользовательскому приложению. В начале своей работы приложения создаёт ряд необходимых для взаимодействия с виртуальной сценой объектов: унифицированные буферы, наборы дескрипторов, системы рендера объектов разного типа, объект камеры, подсистема пользовательского интерфейса.

Для каждого из типов объектов может существовать своя отдельная система отрисовки, но в своей основе они все выполняют примерно одинаковые операции.

В главном цикле пользовательского приложения создаются экземпляры классов всех нужных систем рендера. В процессе создания экземпляра инициализируются необходимые для работы системы ресурсы: унифицированные буферы (для передачи данных в память GPU), список пригодных для отрисовки объектов сцены, наборы дескрипторов (для предоставления пайплайну сведений о передаваемых текстурах и буферах), а также сам объект графического пайплайна, настроенный на отрисовку определённых объектов нужным образом. Каждая такая система имеет свой собственный набор этих ресурсов. Это позволяет приложению рендерить различные объекты сцены на свой манер, а пользователю реализовывать на экране своё творческое видение.

Алгоритм передачи данных об объектах в буфер команд для их последующего рендера представлен на рис. 3.

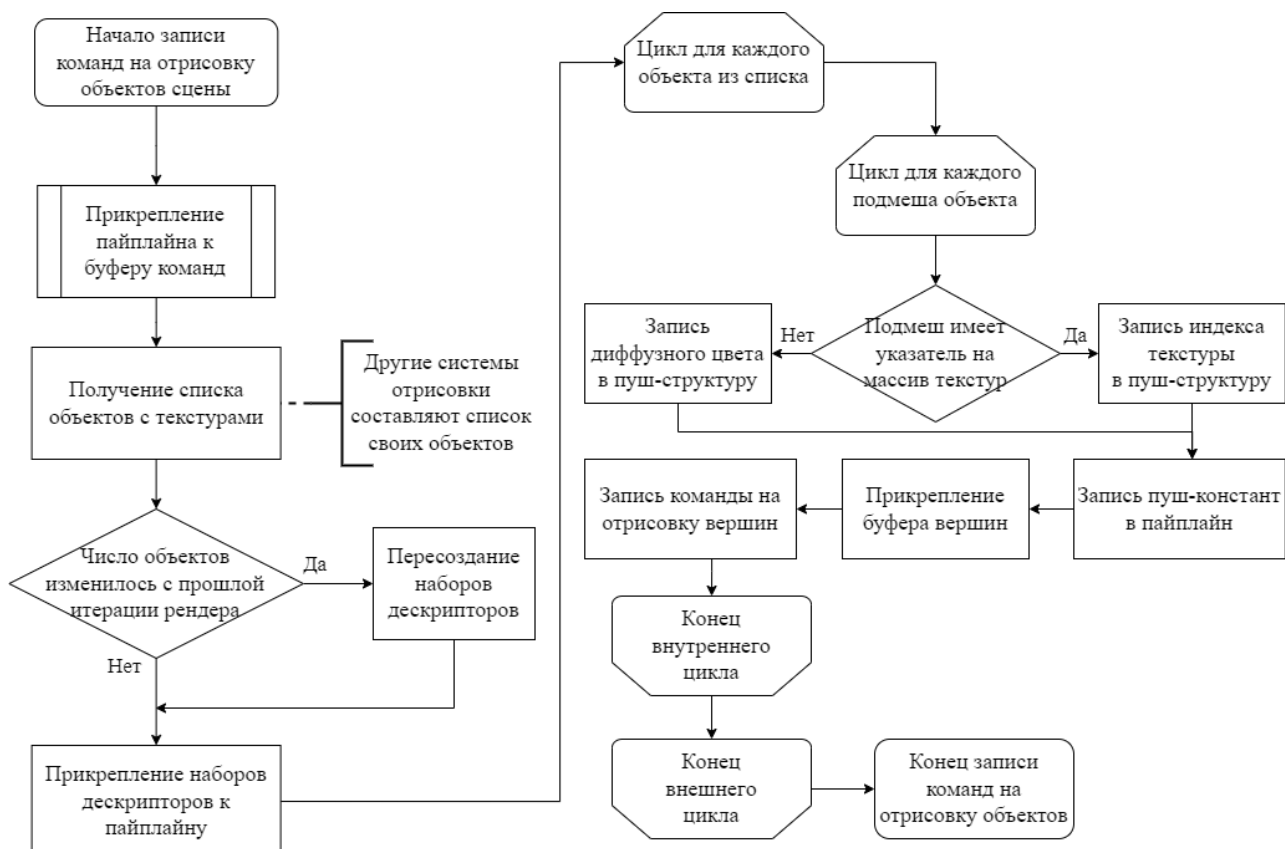


Рис. 3. Алгоритм работы системы рендера на базе Vulkan отрисовщика.

Продемонстрированная в данной работе архитектура рендера может использоваться в качестве универсальной основы для построения различных графических приложений на базе Vulkan API. Она способна к масштабированию за счёт внедрения дополнительных систем отрисовки, а самостоятельный модуль ядра отрисовщика может быть выделен в отдельный фреймворк.

Список используемых источников:

1. Overvoorde, A. Vulkan Tutorial [Электронный ресурс]. URL: <https://vulkan-tutorial.com> (дата обращения 11.11.2022).
2. Грегори, Д. Игровой движок. Программирование и внутреннее устройство. СПб. : Питер, 2021. 1136 с.
3. Селлерс, Г. Vulkan. Руководство разработчика : пер. с англ. М. : ДМК Пресс, 2017. 394 с.

Ezhov G.

Povolzhskiy State University of Telecommunications and Informatics

Architecture design of a general purpose Vulkan API based renderer.

The Vulkan API is the most extensive and functional tool of interaction with the GPU driver, which makes the process of designing software using it a non-trivial task. The author presents his own implementation of the renderer architecture as one of the possible solutions to this problem.

Key words: architecture design, graphics API, Vulkan, renderer, rendering engine.

УДК 004.514
ГРНТИ 50.41.29

РАЗРАБОТКА КОНЦЕПЦИИ ПРИЛОЖЕНИЯ ДЛЯ ОБУЧЕНИЯ И СОЦИАЛЬНОЙ АДАПТАЦИИ ДЕТЕЙ С ОСОБЕННОСТЯМИ РАЗВИТИЯ

В. Д. Карпова, Е. П. Бояшова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данный материал посвящен разработке концепции приложения для обучения и социальной адаптации детей с особенностями развития. Проведен анализ профильных статей и конкурентных информационных систем. На основе этого выдвинуты требования к будущему приложению и определен перечень технологий, необходимых для его реализации.

пользовательский интерфейс, обучение, социальная адаптация, дети, расстройства психического развития

О важности адаптации детей с расстройствами психического развития нет необходимости спорить. Такие диагнозы, как аутизм или синдром Дауна, ставятся с самого рождения и чем раньше начнется процесс адаптации таких детей в обществе, тем скорее будут видны его результаты.

Несмотря на то, что диагноз и возраст детей могут быть одинаковыми, уровень их умственного развития может различаться, поэтому важно, чтобы подход к обучению был индивидуальным для каждого.

Выполнение упражнений в специальном приложении для обучения и социальной адаптации детей с расстройствами и задержкой психического развития может стать прекрасным дополнением к занятиям со специалистами нейропсихологами и дефектологами. Важно понимать, что приложение не должно быть единственным средством реабилитации ребенка.

Анализ предметной области. Проблема социальной адаптации детей с расстройствами психического развития заключается в том, что их не всегда возможно вылечить медикаментозно. Они идут по особому пути, требующему специальных условий обучения и воспитания.

Так дети с расстройствами аутистического спектра (РАС), например, не любят, когда в их жизни появляются новые предметы и люди, то есть меняется их привычный жизненный стереотип [1], а дети с синдромом Дауна могут сильно отставать в развитии от своих сверстников [2]. И это лишь малая часть особенностей мышления таких детей.

При сохранных возможностях к выделению отдельных деталей изображения при аутизме страдает способность к восприятию целостного образа, интеграции элементов в единое целое. Было показано, что дети и

подростки с аутизмом опережают здоровых испытуемых в заданиях, направленных на поиск геометрической фигуры, которая является частью целостного изображения, абстрактного или смыслового [3].

Приложение для обучения и социальной адаптации должно учитывать все особенности мышления детей и решать ряд задач:

- быть понятным как для родителей, так и для детей;
- предоставлять возможность полностью настраивать материал для обучения под конкретного ребенка;
- собирать статистику выполнения упражнений ребенком для возможности отслеживания прогресса обучения.

Такое приложение поможет родителям коммуницировать с ребенком, а детям предоставит возможность обучаться в любом удобном месте.

Анализ конкурентных информационных систем. Основными конкурентными информационными системами являются приложения AR Tutor. Это пакет приложений, направленный на развитие разных социальных навыков у детей с задержкой психического развития.

Особенностью этих приложений является функция дополненной реальности (AR) – с помощью камеры сканируются специальные карточки, которые необходимо заранее распечатать. После сканирования на экране устройства показывается мультфильм, объясняющий, например, как работает тот или иной объект. Далее ребенку предстоит ответить на вопрос по теме ролика.

Такой подход охватывает незначительную часть необходимого к освоению материала. Также некоторым детям могут показаться пугающими и неприятными 3D-модели, с помощью которых сделаны мультфильмы, что может вызвать негативную реакцию и замедлить процесс обучения.

Тем не менее, использование технологии дополненной реальности достаточно интересно и может привлечь внимание целевой аудитории приложения.

Учитывая все достоинства и недостатки конкурентных информационных систем, предстоит разработать концепцию собственного приложения.

Описание проектируемой информационной системы.

При первом запуске приложения родителю будет предлагаться заполнить анкету о ребенке, на основе которой для него будут подобраны упражнения. Впоследствии взрослый сможет настроить уровень сложности упражнений, если они не будут удовлетворять уровню развития ребенка.

Упражнения будут разной направленности: для развития мелкой моторики, памяти, умения воспринимать форму и цвет и т.д.

Для отслеживания прогресса обучения приложение будет собирать статистику и предоставлять её родителю в специальном разделе. Далее эту

статистику можно предоставлять специалистам как некое дополнение к медицинской карте.

Помимо упражнений для развития ребенка в приложении будут другие функции:

1. Кнопки с потребностями, предназначенные для детей, которые по тем или иным причинам не хотят или не могут говорить. При нажатии на кнопку будет воспроизводиться сообщение, оповещающее родителя о том, чего хочет ребенок: поесть, лечь спать, послушать сказку, поиграть с родителем, сходить в туалет и т.д.

2. Полезные статьи для родителей по теме диагноза ребенка.

3. Аудиокниги/мультфильмы для детей.

Чтобы избежать возможной негативной реакции некоторых детей на определенные цвета, приложение будет предусматривать настройку цветовой темы.

Для будущей реализации приложения выбрана операционная система Android, являющаяся самой распространённой на рынке мобильных устройств. Программная часть может быть реализована на статически типизированном, объектно-ориентированном языке программирования Kotlin, так как подавляющее большинство Android-приложений написано с использованием именно этого языка. Для серверной части лучше всего подойдет Python – высокоуровневый объектно-ориентированный язык программирования. Он, в сравнении с аналогичными языками, позволяет работать с меньшим количеством строк кода и удобен в прочтении [4].

Перспективы развития информационной системы. Приложение может быть доработано таким образом, чтобы стать полноценной системой для отслеживания психического состояния ребенка, которую смогут применять не только родители, но и специалисты во время приемов.

Не стоит забывать о важности оффлайн-коммуникации, так как если ребенок полностью погрузится в гаджет, это может только ухудшить его состояние, поэтому выполнение упражнений должны проходить под контролем родителя, а не являться способом занять ребенка.

Список используемых источников:

1. Игнатьева, К.В., Кухарчук, О.В. Проблемы социальной адаптации детей с расстройствами аутистического спектра [Электронный ресурс] // СГУ им. Н.Г. Чернышевского. 2017. URL: https://www.sgu.ru/sites/default/files/conf/files/2017-03/kuharchuk_ignateva_idpo_2017.pdf (дата обращения 10.10.2022).

2. . Соколова, М.В., Халзанова, Т. В. Социальная адаптация детей с синдромом Дауна [Электронный ресурс] // Ярославский педагогический вестник. 2002. URL: <https://cyberleninka.ru/article/n/sotsialnaya-adaptatsiya-detey-s-sindromom-dauna> (дата обращения 12.10.2022).

3. Горбачевская, Н.Л., Переверзева, Д.С. Особенности зрительного восприятия у детей с расстройствами аутистического спектра [Электронный ресурс] // Современная зарубежная психология. №2. 2013. URL: https://psyjournals.ru/files/61197/jmfp_2013_2_n10_Pereverzeva.pdf (дата обращения: 12.10.2022).

4. Букреев, Л.В., Зариковская, Н.В., Калюжный, Е.Р., Красноусов, В.М. Технологии, используемые при реализации функционала мобильных приложений для платформы Android [Электронный ресурс] // Томский государственный университет систем управления и радиоэлектроники. 2021. URL: <https://cyberleninka.ru/article/n/tehnologii-ispolzuemye-pri-realizatsii-funksionala-mobilnyh-prilozheniy-dlya-platformy-android/viewer> (дата обращения: 16.10.2022).

Karpova V., Boyashova E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Development of the application concept for teaching and social adaptation of children with special needs.

This material is devoted to the development of the application concept for teaching and social adaptation of children with special needs. The analysis of profile articles and competitive information systems is carried out. Based on this, the requirements for the future application are put forward and a list of technologies necessary for its implementation is determined.

Key words: user interface, learning, social adaptation, children, mental development disorders.

УДК 004.514
ГРНТИ 50.41.25

ПРОГРЕССИВНЫЕ ВЕБ-ПРИЛОЖЕНИЯ ДЛЯ БИЗНЕСА: КАКИЕ ЗАДАЧИ ПОМОГАЮТ РЕШАТЬ, РОССИЙСКИЙ РЫНОК, УСПЕШНЫЕ КЕЙСЫ

Е. С. Кучинский, А. А. Шиян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В эпоху цифровизации у владельцев успешных веб-сайтов часто возникает потребность создать мобильное приложение, чтобы улучшить пользовательский опыт и сделать его наиболее надежным, быстрым и удобным. Для этого нужно нанять новых людей, которые фактически создали бы копию сайта, но в виде мобильного приложения. Это дорого, долго и не удобно. Но уже сегодня любой веб сайт можно легко превратить в мобильное приложение, используя один лишь JavaScript – такие приложения называются прогрессивными веб-приложениями

PWA, мобильные приложения, нативные приложения, кросс-платформенные приложения, UX

Что такое PWA

Прогрессивное веб приложение (оно же PWA) – это мобильное приложение в браузере. Оно не требует обязательной установки и при этом совмещают простоту использования и разработки веб-сайтов и технические возможности и мощь нативных приложений.

Для доступа к нему необходим лишь браузер, что делает PWA полностью кросс-платформенным – больше не нужно разрабатывать отдельно сайт и приложения под Android и iOS – достаточно иметь и поддерживать только сайт.

Главные достижения PWA – это гибкое управление кешированием и возможность использовать ресурсы операционной системы наравне с нативными приложениями: в PWA можно отправлять пуш-уведомления, взаимодействовать с файловой системой, обеспечить оффлайн доступ к приложению, использовать bluetooth, биометрию для аутентификации, NFC для быстрых платежей, распознавать речь, использовать камеру, считывать QR и многое другое. На сайте whatwascando.today [1] можно увидеть все технологии, которые сейчас поддерживаются в PWA.

Как сделать из сайта прогрессивное веб-приложение

Чтобы браузер пользователя смог предоставить контейнер для отображения приложения и оно стало прогрессивным необходимо соблюдение нескольких условий:

- HTTPS – сайту необходим SSL сертификат и все внешние ресурсы так же должны быть подключены через HTTPS;

- Application Shell – графическая обертка приложения, то есть минимальный набор из html, css и javascript для запуска приложения. Все эти ресурсы будут кэшироваться;
- Web App Manifest – это json файл, описывающий свойства приложения – его имя, цвет панели управления, иконки, ориентацию экрана, стартовую страницу приложения и так далее. Этот файл необходим для установки PWA на домашний экран, он подгружается через html-тег `<link>`;
- Service Worker – по функционалу – это проксирующий слой для браузера, через который проходят запросы к серверу. Далее он решает отправить пользовательский запрос на сервер или же отдать данные с кеша. Вся логика работы PWA будет описана в нем. Физически – это обычный js файл, подключенный в html. (на сегодняшний день все браузеры поддерживают технологию Service Worker [2]).

Какие задачи бизнеса может решать PWA

1. Значительная экономия средств – разработка и поддержка очень дешевая, т.к. больше не нужно разрабатывать отдельно сайт и приложения под iOS и Android, достаточно иметь и поддерживать только сайт. Кроме того появляется возможность экономить на комиссиях магазинам приложений – для PWA они не нужны, приложение можно скачать напрямую с сайта. (но при желании PWA можно загрузить в магазин, такая технология будет называться TWA – Trusted Web App).

2. Стимулирование повторных продаж, повышение среднего чека – с помощью пуш-уведомлений можно рекомендовать клиенту товары или услуги, напоминать завершить покупку, если он добавил товаров в корзину и не оплатил. А постоянный доступ к приложению с домашнего экрана только упростит достижение этих целей.

3. Повышение узнаваемости бренда – иконка (логотип) компании всегда на виду у пользователя.

4. Оставаться на связи с клиентом – через пуш-уведомления можно сообщать пользователю об обновлениях по его товарам, услугам и доставкам. Кроме того можно рассказывать о новых акциях и тем самым экономить на рекламе и повышать конверсию спецпредложений.

5. Уменьшить количество точек соприкосновения с конкурентами – клиенты обращаются к сервису через приложение, а не через поисковую выдачу, где могут быть конкуренты.

6. Расширить охват – PWA можно установить на любую ОС, будь то iOS, Android или Windows – это позволяет компании привлечь более широкую аудиторию и не ориентироваться на определенную платформу.

7. Хорошая индексация сайта поисковыми системами – они отдадут PWA преимущество перед обыкновенными сайтами. Кроме того, специалист по SEO стоит дешевле специалиста по продвижению мобильных приложений.

8. Повышение удовлетворенности пользователей – PWA используют кэширование для ускорения своей работы. Согласно исследованию ООО Deloitte в секторе B2C [3], ускорение работы приложения всего лишь на 1/10 секунды

повышает показатель удержания более чем на 5%, а конверсию продаж и средний чек более чем на 8%.

Итак, иметь мобильное приложение на B2C рынке очень выгодно – оно позволит повысить конверсию, снизить конкуренцию, повысить охват, обеспечить более комфортный пользовательский опыт, а кроме того сэкономит драгоценное время и деньги.

В чем плюсы PWA для пользователей

Технологии PWA разрабатываются с оглядкой на опыт веб-сайтов и нативных приложений, что позволяет давать пользователю преимущества обеих платформ – рис. 1.

	Приложение на технологии PWA	Веб-сайт	Обычное приложение
Работает без интернета	✓	✗	✓
Push уведомления	✓	✗	✓
Установка на главный экран	✓	✗	✓
Нет лишних элементов	✓	✗	✓
Индексируется поисковиками	✓	✓	✗
Одна система управления	✓	✓	✗
Работает на всех устройствах	✓	✓	✗
Не требует установки	✓	✓	✗
Не требует обновлений	✓	✓	✗

Рис. 1. Прогрессивные приложения берут лучшее от обоих миров [4]

PWA на российском рынке

В результате санкций в App Store и Google Play были заблокированы приложения российских компаний, таких как Сбербанк, ВТБ, Альфа-банк, Аэрофлот. Apple так же блокирует 2GIS и приложения от Mail.ru Group – ВК, почта, облако, голосовой помощник.

Блокировка социально важных российских приложений ограничивает возможности россиян в использовании современных мобильных сервисов, таких как онлайн банки, социальные сети, государственные приложения. Даже если у человека уже было установлено приложение, то он лишится возможности обновлять его, а значит не сможет использовать новые функции, не получит исправления багов и проблем с безопасностью.

Российская IT-отрасль продемонстрировала несколько возможных решений этой проблемы:

1. Выкладывать установочный файл прямо на сайте – Сбербанк, ВТБ, Альфа-банк и другие в качестве быстрого решения именно так и поступили. Однако у этого есть большие минусы – чтобы установить файл APK, нужно

пройти через множество предупреждающих и не всегда понятных экранов. Некоторые пользователи, в особенности старшее поколение, паникуют и останавливаются на использовании веб-версии. Обновления приложения возможно, но зачастую очень сложно – нужно удалить устаревшую версию, найти и скачать новую и заново аутентифицироваться. Кроме того, пользователям iOS устройств этот способ не подходит – платформа не доверяет сторонним программам.

2. Распространение через российские магазины приложений – уже разработаны не меньше трех альтернативных магазинов приложений для Android – NashStore, RuStore, RuMarket. Этот способ полностью решает проблему с обновлением приложений, но само приложение альтернативного магазина все равно нужно ставить вручную – так же скачивая через сайт, проходя через множество предупреждающих экранов. Пользователи iOS все еще могут использовать этот способ.

3. Распространение Progressive Web App (PWA). Из плюсов – они устанавливаются без устрашающих предупреждений – таким образом снижается входной барьер; одно и то же PWA работает везде – на iOS, Android, в десктопном браузере; очень маленький вес приложения; есть пуш-уведомления; клиенту не придется обновлять приложения – обновления приходят бесшовно; пользователи iOS наконец легко получают приложение с привычным им UX. Из подсанкционных банков так уже делают Альфа-банк, ВТБ и Совкомбанк, из неподсанкционных — Тинькофф и МТС Банк.

Наиболее успешные случаи внедрения PWA [5]

1. Сеть кофеен Starbucks в дополнение к обычному мобильному приложению разработала PWA для сбора заказов. В PWA был реализован тот же интерфейс, что и в мобильном приложении, но вес оказался меньше на 99,84%. В результате заказы через мобильный Интернет удвоились.

2. Сервис бронирования отелей Trivago – пользователи не хотели устанавливать мобильное приложения – места в телефоне мало, а бронировать нужно редко. После внедрения PWA более полмиллиона человек добавили ярлык Trivago на рабочий стол телефона – прирост вовлеченности составил 150%, а благодаря пуш-уведомлениям количество кликов по спецпредложениям вырос на 97%

3. Агрегатор такси Uber разрабатывала PWA, чтобы сделать заказ такси возможным даже в медленных 2G сетях. В итоге их приложение занимает всего лишь 50 KB и загружается менее чем за 3 секунды в 2G сетях.

4. Фотохостинг Pinterest разработал PWA, чтобы повысить конверсию в мобильной версии сайта – в результате компания увеличила время нахождения пользователя в приложении на 40%, заработок с рекламы на 44%, количество кликов и ключевых действий более чем на 50%, таким образом показатели PWA сравнялись с показателями их нативного приложения, а некоторых случаях показали результат лучше на 2-5% [6].

Кроме них отличные результаты после внедрения PWA получили такие бренды как Tinder, Twitter, Aliexpress и Alibaba, Forbes, Habr, Twitch, Spotify, Tiktok и множество других [5].

Заключение

PWA определенно является следующим витком развития веб-приложений. Такие приложения кросс-платформенны, дешевы и эффективны для бизнеса, удобны клиенту и самим разработчикам, так что в современном мире PWA – это отличное решение для развития бизнеса и выхода на новые рынки.

Список используемых источников:

1. What PWA Can Do Today. [Электронный ресурс]. URL: <https://whatpwacando.today/> (дата обращения 13.11.2022).
2. Can i use Service Worker [Электронный ресурс] URL: <https://caniuse.com/?search=%20service%20worker> (дата обращения 13.11.2022)
3. LLP Deloitte. Milliseconds Make Millions [Электронный ресурс]. URL: <https://www2.deloitte.com/ie/en/pages/consulting/articles/milliseconds-make-millions.html> (дата обращения 13.11.2022).
4. Евгений Данилюк. PWA-приложения. Что это такое и для чего бизнесу создавать приложение из сайта [Электронный ресурс]. URL: <https://vc.ru/marketing/141463-pwa-prilozheniya-cto-eto-takoe-i-dlya-chego-biznesu-sozdavat-prilozhenie-iz-sayta/> (дата обращения 13.11.2022).
5. PWA Stats [Электронный ресурс]. URL: <https://www.pwastats.com/> (дата обращения 13.11.2022).
6. Addy Osmani. A Pinterest Progressive Web App Performance Case Study [Электронный ресурс]. URL: <https://medium.com/dev-channel/a-pinterest-progressive-web-app-performance-case-study-3bd6ed2e6154> (дата обращения 13.11.2022)
7. Пользователь @altrus. PWA – это просто. [Электронный ресурс]. URL: <https://habr.com/ru/post/418923/> (дата обращения 13.11.2022).
8. ООО RooX. PWA — это новый черный? [Электронный ресурс]. URL: <https://vc.ru/dev/518237-pwa-eto-novyy-chernyy/> (дата обращения 13.11.2022).
9. ООО RooX. Как компании справляются с удалением приложений из сторов [Электронный ресурс]. URL: <https://vc.ru/dev/491391-kak-kompanii-spravlyayutsya-s-udaleniem-prilozheniy-iz-storov/> (дата обращения 13.11.2022).

Kuchinsky E., Shiyan A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Progressive web applications for business: what tasks help to solve, the russian market, successful cases.

In the era of digitalization, owners of successful websites often have a need to create a mobile application to improve the user experience and make it the most reliable, fast and convenient. To do this, you need to hire new people who would actually create a copy of the site, but in the form of a mobile application. It's expensive, long and inconvenient. But today, any website can be easily turned into a mobile application using JavaScript alone – such applications are called progressive web applications.

Key words: PWA, mobile apps, native apps, cross-platform apps, UX.

УДК 004.9
ГРНТИ 61.61.99

ВИДЫ ФИЛАМЕНТОВ ДЛЯ 3D-ПЕЧАТИ МЕТОДОМ ПОСЛОЙНОГО НАПЛАВЛЕНИЯ

Д. В. Лебедев, А. А. Шиян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире всё чаще применяется технология 3D-печати методом послойного наплавления. Для создания изделий таким методом применяются филаменты – пластиковые нити, состоящие из различных материалов или смесей. Среди наиболее универсальных филаментов можно выделить нити из ABS, PLA и PETG-пластика.

3D-печать, 3D-принтер, FDM, аддитивные технологии, филамент, пластик

В современном мире большое развитие получили аддитивные технологии. Аддитивные технологии – это технологии послойного наращивания и синтеза объектов на основе их цифровой модели. Аддитивные технологии активно внедряются в различных сферах жизни, начиная от производства предметов быта и заканчивая медициной и строительством, а объем рынка 3D-печати вырос до 21 миллиарда долларов [1].

Для послойного создания объектов используются 3D-принтеры. Эти устройства позволяют создавать различные объекты сложных форм, получая на входе лишь информацию о цифровой модели и расходный материал, будь то полиэфирная смола, пластик или даже металл.

Наибольшую популярность получила 3D-печать методом послойного наплавления (англ. *fused deposition modeling*, FDM). Печать таким способом происходит за счет расплавления филамента и нанесения его печатающей головкой 3D-принтера на печатную платформу слой за слоем [2].

Филамент – расходный материал, используемый для печати, который представляет собой пластмассовую нить сечением 1,75 или 3 мм. Общепринятым вариантом фасовки филамента является килограмм пластика, намотанный на катушку, однако нередки случаи фасовки по другим массам, например, 1.25 или 3 килограмма. Также филамент может поставляться без катушек в виде мотка нити. Пример фасовки филамента показан на рис. 1.



Рис. 1. Пример фасовки филамента

Акрилонитрилбутадиенстирол (ABS) – пластик, который активно применяется как в аддитивном производстве, так и в промышленности в целом. ABS-пластик активно используется в автомобилестроении, медицине, производстве игрушек, компьютерной периферии, спортивного инвентаря и др.

Из преимуществ применения ABS-пластика можно выделить:

- устойчивость к влаге и кислотам;
- ударопрочность;
- легкость механической обработки;
- низкую цену филамента.

Также ABS-пластик может быть растворён ацетоном, что позволяет получать крупные объекты из составных деталей путём склеивания. Применение паров ацетона для растворения внешних слоёв способствует сглаживанию, получения герметичности и усиления прочности модели.

ABS-пластик, несмотря на большое количество положительных свойств, имеет и свои недостатки. Так, во время печати ABS-пластиком выделяется токсичные пары акрилонитрила, хоть и в малом объеме, вследствие чего необходимо наличие вытяжки. Помимо этого, помещение для печати не должно иметь сквозняков, а принтер не должен охлаждать печатаемое изделие, поскольку пластик может изменить свою форму вследствие резкого перепада температур. Также изделия из ABS подвержены воздействию солнечного света, отчего они изменяют свой оттенок и становятся менее прочными. [3]

Полилактид (PLA) – пластик, производимый из кукурузы или сахарного тростника. Данный вид пластика отличается биоразлагаемостью и биосовместимостью.

PLA-пластик обладает следующими преимуществами:

- биоразлагаемый;
- низкая температура плавления;
- отсутствие усадок;
- гладкость поверхности напечатанного изделия;
- отсутствие необходимости использования клея при печати;
- точность и аккуратность печати.

Из недостатков печати полилактидом можно выделить:

- относительно невысокая прочность;
- подверженность к перегревам [4].

Полиэтилентерефталат (PET) активно применяется в пищевой промышленности. Однако для печати на 3D-принтерах применяется PET с добавлением гликоля – PETG. Такая модификация позволяет снизить температуры плавления и облегчить процесс печати.

Для PETG характерны положительные стороны как PLA, так и ABS:

- устойчивость к химии;

- ударопрочность;
- отсутствие усадок;
- точность и аккуратность печати;
- низкая в сравнении с ABS температура плавления;

Помимо этого, PETG без красителей является прозрачным, чем не может похвастаться ABS или PLA.

Среди негативных особенностей PETG можно выделить повышенное влияние влаги на процесс печати, а также сложности в механической обработке [5].

Детали, напечатанные из PLA и PETG, также можно обработать растворителем для получения эффекта, схожего с влиянием ацетона на ABS, однако для этого требуется использовать дихлорметан или дихлорэтан, являющиеся очень вредными для человека веществами.

Помимо ABS, PLA и PETG, встречаются филаменты из других видов пластика. Например, филаменты TPA и Nylon позволяют печатать изделия, в которых важна упругость и гибкость конструкции.

Также существуют композиты – филаменты, имеющие в своём составе различные примеси, изменяющие первоначальные свойства пластика. Так примесь из крошки токопроводящих металлов позволит сделать токопроводящий филамент, а добавление карбона улучшит прочность и эластичность изделия. Однако печать композитами нередко требует более совершенного аппаратного обеспечения для обеспечения соответствующего нагрева и охлаждения.

В лаборатории виртуальной реальности и 3D-печати кафедры информатики и компьютерного дизайна СПбГУТ для печати на 3D-принтерах Anycubic i3 Mega активно используются филаменты из ABS и PLA пластика, поскольку они позволяют получить точные и прочные изделия на имеющихся 3D-принтерах. Для создания эластичных деталей применяется филамент из TPA и нейлона. Также проводятся эксперименты по использованию в печати PET-филамента, отличающегося от PETG повышенными требованиями к настройкам печати, но отличительно низкой себестоимостью производства.

Список используемых источников:

1. 3D printing market size worldwide from 2013 to 2021 [Электронный ресурс]. URL: <https://www.statista.com/statistics/796237/worldwide-forecast-growth-3d-printing-market/> (дата обращения 15.11.2022).
2. Аддитивные технологии и аддитивное производство [Электронный ресурс]. URL: <https://globatek.ru/3d-wiki/chto-takoe-additivnyye-tehnologii> (дата обращения 15.11.2022).
3. Энциклопедия 3D-печати. ABS-пластик для 3D-печати [Электронный ресурс]. URL: https://3dtoday.ru/wiki/abs_plastic (дата обращения 15.11.2022).
4. Энциклопедия 3D-печати. PLA-пластик для 3D-печати [Электронный ресурс]. URL: https://3dtoday.ru/wiki/PLA_plastic (дата обращения 15.11.2022).

5. Энциклопедия 3D-печати. PET-пластик для 3D-печати [Электронный ресурс]. URL: https://3dtoday.ru/wiki/pet_plastic (дата обращения 15.11.2022).

Lebedev D., Shiyan A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Types of filaments for FDM 3D-printing.

Fused deposition modeling is a leading method of additive manufacturing. Printed products could be made from different types of filaments. The most common filament components are ABS, PLA u PETG plastic.

Key words: 3D-printing, 3D-printer, FDM, additive manufacturing, filament, plastic.

УДК 004.946
ГРНТИ 28.17.33

РАЗРАБОТКА СИСТЕМЫ ГЕНЕРАЦИИ АУДИАЛЬНОГО ОКРУЖЕНИЯ ДЛЯ МОДЕЛЕЙ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

А. П. Лосев, Г. Г. Рогозинский

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современные системы виртуальной реальности являются сложными модульными объектами, состоящими не только из систем генерации и визуализации графического контента, но и из систем формирования виртуального звукового окружения. Методы создания графики на данный промежуток времени представляют изображения, обладающие фотореалистичностью, то есть близки к изображению в реальном мире. Однако при формировании виртуальной сцены так же важна и аудиальная составляющая, формирующая общий пользовательский опыт от нахождения в сгенерированном мире: необходимы фоновые эффекты, формирование звуков при взаимодействии с поверхностями, и другое звуковое наполнение виртуальной сцены. Современные программные пакеты имеют базовый функционал по интеграции звуковых эффектов, однако возможности разработки и создания иммерсивных виртуальных сред значительно расширяются при использовании сторонних сред для генерации звука. Данная работа сфокусирована на исследовании возможных архитектурных паттернах для создания интерактивных систем генерации звука в виртуальной сцене, а также на создании примера взаимодействия программы для создания трёхмерной графики и программной среды для генерации звука.

виртуальная реальность, алгоритмическая генерация, мультимодальные системы, трёхмерная графика, Open Sound Control

Создание трёхмерного окружения для виртуальной реальности требует соблюдения множества факторов для того, чтобы создаваемый виртуальный мир создавал эффект погружения. Для создания данного эффекта используют процедурную генерацию ландшафтов, симуляцию физических процессов (потoki частиц, колебания ткани), а также создание объёмного акустического окружения. Кроме того, современные системы генерации и создания виртуального окружения используют полимодальный подход, то есть, эффект погружения создаётся не только за счёт зрительных образов, но также и за счёт аудиокомпонент, тактильных ощущений и ольфакторных составляющих (использование запахов) [1]. Комплекс данных ощущений формирует необходимый эффект присутствия, который позволяет человеку, находящемуся в виртуальной реальности, ощущать данную реальность более приближенной к ощущаемому миру.

Методология развития синтеза звука позволяет обратить внимание на такой способ формирования сигнала, как субтрактивный синтез. При данном виде синтеза источником сигнала выступает генератор гармонически насыщенного сигнала, с большим количеством гармоник на всём слышимом частотном спектре [2]. Данный насыщенный сигнал обрабатывается с помощью частотного фильтра (или блока фильтров), может модулироваться с помощью

низкочастотного осциллятора для автоматизации различных параметров, после блока модуляции сигнал попадает на усилитель мощности, управляемый огибающей громкости. Полученный в результате частотной обработки звуковой сигнал является итоговым тембром, созданным в ходе синтеза.

Полученные с помощью субтрактивного синтеза звуковые сигналы могут быть смоделированы как свертка исходного полигармонического сигнала $S_n(t)$ или шума с заданной функцией вероятности и импульсной характеристикой фильтра $h(t)$, также обычно имеющего общую огибающую $A(t)$ [3]. В большинстве случаев фильтр является объектом модуляции $M(t)$, особенно его частота среза ω_0 :

$$S_A(t) = A(t) \cdot S_n(t) * h(M(t) \cdot \omega_0) \quad (1)$$

Уравнение (1) является общим случаем для субтрактивного синтеза звука. Среди иных полигармонических сигналов, использующихся при субтрактивном синтезе, стоит выделить сигналы с различными комплексными формами волны (2-5):

Пилообразный сигнал с ограниченным количеством гармоник вплоть до N -ой гармоники (без элайзинга):

$$S_{saw}(t) = \sum_{k=1}^N \frac{\sin(k \cdot \omega_0 t)}{k}, N \cdot \omega_0 < \frac{\omega_s}{2} \quad (2)$$

где $\frac{\omega_s}{2}$ — частота Найквиста (половина частоты дискретизации); ω_0 — основная частота.

Массив пилообразных сигналов с отклонениями в высотах тона

$$S_{nsaw}(t) = \sum_{m=1}^L \sum_{k=1}^N A_m \frac{\sin(k \cdot (\omega_0 + \Delta\omega_m)t)}{k}, N \cdot \omega_0 < \frac{\omega_s}{2} \quad (3)$$

Прямоугольный сигнал, ограниченный в полосе частот:

$$S_{sq}(t) = \sum_{k=0}^N \frac{\sin((2k+1) \cdot \omega_0 t)}{2k+1}, (2N+1) \cdot \omega_0 < \frac{\omega_s}{2} \quad (4)$$

Треугольный сигнал, ограниченный в полосе частот:

$$S_{tri}(t) = \sum_{k=0}^N \frac{\sin((2k+1) \cdot \omega_0 t)}{(2k+1)^2}, (2N+1) \cdot \omega_0 < \frac{\omega_s}{2} \quad (5)$$

Субтрактивный метод синтеза звука является наиболее распространенным. Разнообразие звучания при использовании данного вида синтеза достигается посредством использования обширного спектра эффектов обработки. Общая схема работы субтрактивного синтезатора представлена на рис. 1:

Субтрактивный синтез

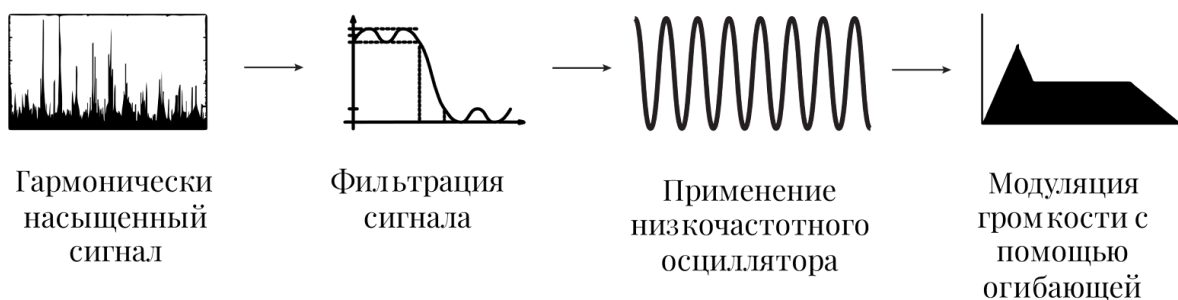


Рис. 1. Алгоритм формирования звукового сигнала в субтрактивном синтезаторе

Средой, в которой может быть имплементирован метод создания аудиоокружения, является любой программный пакет для работы с трёхмерной графикой и создания микромиров в виртуальной реальности. Лидирующие позиции в разработке трёхмерной графики занимают два программных продукта: Unreal Engine и Unity.

В качестве основного опорного программного продукта для имплементаций систем аудио в виртуальную реальность был выбран программный пакет Unity, так как он является портируемым на высокое количество устройств, как стационарных (персональные компьютеры, использующие операционные системы Windows, MacOS или Linux), так и портативных (Android, iOS), а также консолей (PS5, Xbox One, Nintendo Switch). Данный программный пакет поддерживает взаимодействие через протокол Open Sound Control (OSC), что позволяет формировать паттерны взаимодействия по схеме «запрос-ответ» [4]. Данный тип взаимодействия крайне удобен своей асинхронностью, поскольку он позволяет генерировать звук только после получения информации о произошедшем в трёхмерной сцене событии, и отправлять данный звук в используемую сцену, создавая звуковой эффект. В остальное время звуковой эффект не генерируется, что позволяет не задействовать ресурсы центрального процессора. Подход, при котором для обмена аудио используется OSC, позволяет использовать внешние системы генерации аудиосоставляющих, такие как Max/MSP, Csound и SuperCollider. В качестве примера практического взаимодействия была выбрана среда SuperCollider.

Структурная схема итерации среды разработки Unity и среды программирования звука SuperCollider представлена на рис. 2:

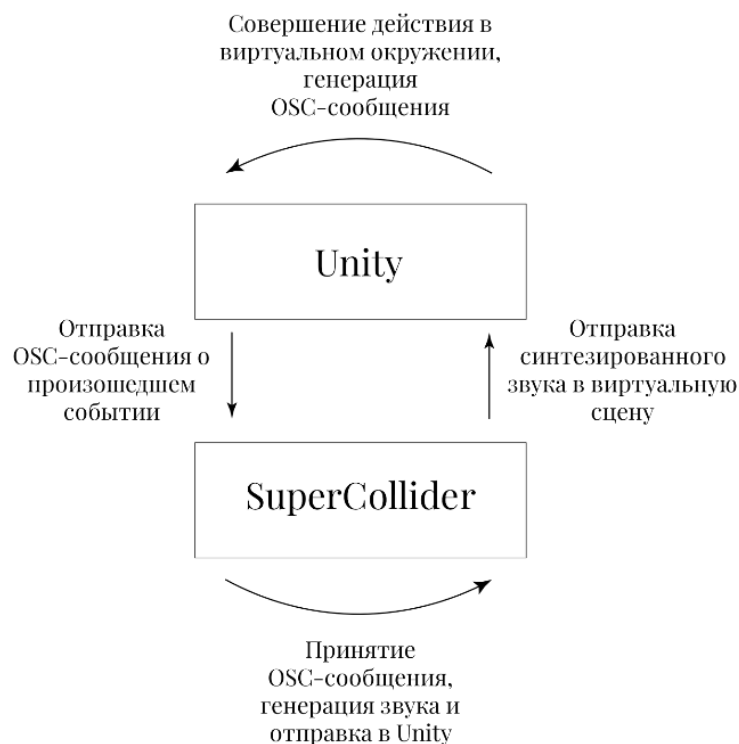


Рис. 2. Общая схема работы системы генерации звуковых сигналов для виртуальной реальности

Данные настройки могут служить при разработке для генерации звуковых эффектов в реальном времени [5]. Например, датчики шлема виртуальной реальности могут быть источниками данных об ориентации головы оператора, данные об ориентации могут приниматься в Unity и отправляться через OSC в среду SuperCollider. В среде SuperCollider принятые данные могут быть использованы для автоматизации панорамирования эффектов звукового окружения на основе того, как расположен пользователь, находящийся в виртуальной реальности, по отношению к виртуальному источнику звука.

Рассмотренный в данном примере случай является частным случаем взаимодействия среды разработки приложений виртуальной реальности Unity и среды генерации звука SuperCollider.

Список используемых источников:

1. Бондарь, М. С. Использование киберфизических объектов и их моделей в мультидоменной модели коммуникаций с целью полимодального представления данных / М. С. Бондарь, Г. Г. Рогозинский, Р. Уолш // Актуальные проблемы радио- и кинотехнологий : материалы IV Международной научно-технической конференции, посвященной 135-летию со дня рождения русского ученого, радиотехника и предпринимателя С. М. Айзенштейна, Санкт-Петербург, 12–15 ноября 2019 года. – Санкт-Петербург: Санкт-Петербургский государственный институт кино и телевидения, 2020. – С. 108-112.

2. Волченко, В. В. Субтрактивный синтез звука / В. В. Волченко // Музыкаведение в XXI веке: теория, история, исполнительство : сборник статей по материалам III Всероссийской

научно-практической конференции, Краснодар, 17 марта 2021 года. – Краснодар: Краснодарский государственный институт культуры, 2021. – С. 47-49.

3. Лосев, А. П. Создание математической модели и прототипирование электрической схемы звукового фильтра / А. П. Лосев, Д. А. Поленова, Г. Г. Рогозинский // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021): Всероссийская научно-методическая конференция магистрантов и их руководителей. Сборник лучших докладов конференции, Санкт-Петербург, 30 ноября – 02 декабря 2021 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2022. – С. 108-113.

4. Wright, M. Open Sound Control: an enabling technology for musical networking / M. Wright // Organised Sound. – 2005. – Vol. 10. – No 3. – P. 193-200.

5. Забелин, Л. Ю. 3D информационные технологии в мультимедиа индустрии / Л. Ю. Забелин, Ю. М. Шыырап // Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта (CAD/CAM/PDM - 2016) : труды XVI-ой международной молодежной конференции, Москва, 17–19 октября 2016 года. – Москва: ООО "Аналитик", 2016. – С. 102-104.

Losev A., Rogozinsky G.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development of a Sound Generation System for Virtual Reality Models.

Modern virtual reality systems are complex modular objects consisting not only of systems for generating and visualizing graphic content, but also of systems for forming a virtual sound environment. Methods of creating visual graphics for a given period of time represent images that are photorealistic, that is, close to the image in the real world. However, when forming a virtual scene, the auditory component is also important, which forms the overall user experience from being in the generated world: background effects, the formation of sounds when interacting with surfaces, and other sound content of the virtual scene are necessary. Modern software packages have basic functionality for integrating sound effects, but the possibilities of developing and creating immersive virtual environments are significantly expanded when using third-party environments for sound generation. This work focuses on the study of possible architectural patterns for creating interactive sound generation systems in a virtual scene, as well as on creating an example of the interaction of a program for creating three-dimensional graphics and a software environment for sound generation.

Key words: *virtual reality, algorithmic generation, multimodal systems, 3D graphics, Open Sound Control.*

УДК 514
ГРНТИ 27.21.17

ОБЛАСТЬ ПРИМЕНЕНИЯ И ТЕНДЕНЦИИ РАЗВИТИЯ ГЕОМЕТРИЧЕСКИХ АЛГОРИТМОВ

Люй Инчжэн

Санкт-Петербургский Политехнический университет Петра Великого

В настоящее время, с быстрым развитием информационных технологий и улучшением вычислительной мощности людей, чтобы удовлетворить потребности технологического развития в различных отраслях промышленности по всему миру, разработка геометрических алгоритмов для повышения эффективности компьютерных геометрических расчетов и операций является темой, достойной углубленного исследования.

геометрический алгоритм, информационные технологии, автоматизированный, принципы взаимодействия, повышение эффективности

История применения геометрических знаний человеком почти так же стара, как и сама человеческая цивилизация. Уже в древнегреческий период люди начали изучать геометрию из-за необходимости измерять землю и инженерные постройки. На протяжении тысячелетий человеческие исследования природы космоса значительно расширили человеческое понимание Вселенной и значительно повысили его собственную продуктивность. Основанная на традиционной геометрии, алгоритмическая геометрия имеет некоторые очевидные отличия от традиционной геометрии. Наиболее важным отличием является то, что основной задачей алгоритмической геометрии является разработка и реализация эффективных алгоритмов.

В настоящее время алгоритмическая геометрия широко используется в большом количестве прикладных областей, включая робототехнику, географические информационные системы, проектирование интегральных схем, автоматизированную инженерию, обработку медицинских изображений, компьютерное зрение, компьютерную графику, машинное обучение, а также медицинские и биологические приложения.[1] Популярные направления исследований в области вычислительной геометрии включают многомерную геометрию (High-dimensional Geometry), комбинаторную геометрию (Combinatorial Geometry), вычислительную топологию (Computational Topology) и задачи геометрических алгоритмов в машинном обучении и анализе данных.

Для лучшего понимания алгоритмической геометрии, в этой статье исследуется область применения и анализируются тенденции ее развития.

1. Область применения

1.1. Астрономический

Комбинация без фазы (Geometry-Frere, GF) (Рис. 1.) вводится в алгоритм обнаружения циклических скачков, чтобы избежать геометрических ошибок,

включая ошибки орбиты спутника, и получить высокоточные услуги навигации и позиционирования. [2]

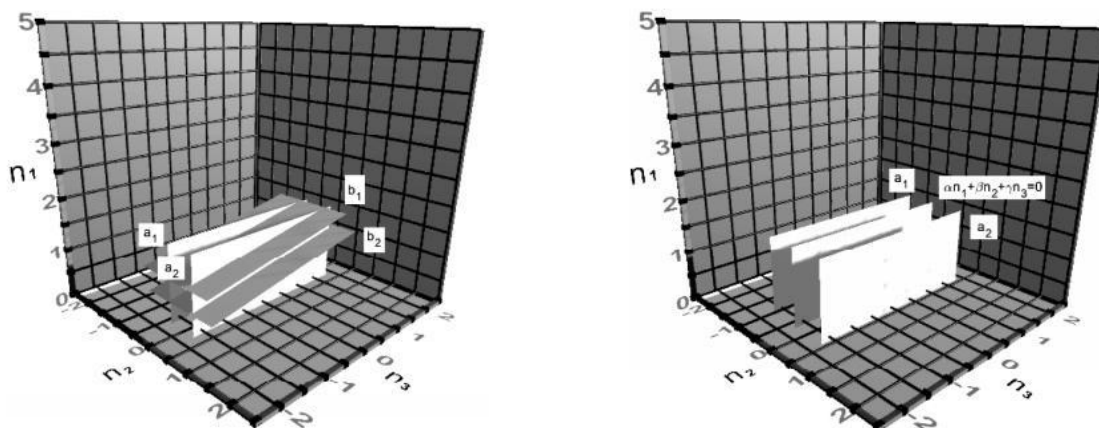


Рис. 1. Нечувствительный диапазон распределения скачков цикла

1.2. Аэрокосмическая техника

В соответствии с формой зоны ограниченного полета геометрические алгоритмы используются для надлежащего выбора путевой точки и планирования траектории путевой точки. Эффективно решить все более серьезную проблему задержек рейсов и повысить коэффициент использования воздушного пространства.

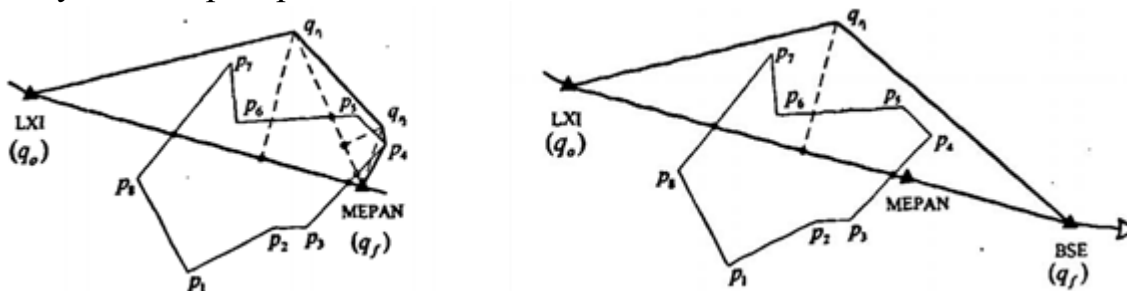


Рис. 2. Планирование изменения маршрута

1.3. Машинное обучение

Машина опорных векторов (Support Vector Machine) - это новый метод машинного обучения. Геометрический алгоритм использует геометрическую информацию в обучающем наборе "для решения задачи из геометрического значения SVM" и обладает преимуществами интуитивности, высокой точности вычислений и удобным применением. Он основан на теории статистического обучения, "отталкиваясь от принципа минимизации структурных рисков", и обладает хорошими возможностями обобщения.

1.4. Естественные науки

Технология 2D лазерного дальномера используется для бесконтактных измерений диаметра и положения деревьев.[3] Геометрические алгоритмы (метод длины дуги, метод касательной (Рис. 3.) и метод двойного косинуса (Рис. 4.)) могут быть использованы для компенсации измеренных значений на близком

расстоянии с использованием угла компенсации для достижения точности съемки и картографирования.

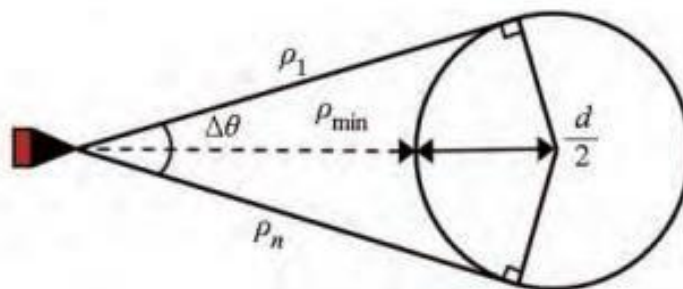


Рис. 3. Принципиальная схема расчета диаметра касательным методом

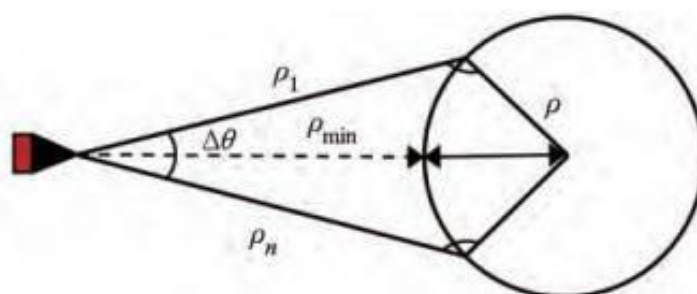


Рис. 4. Принципиальная схема расчета диаметра методом двойного косинуса

1.5. Многомерная геометрия

Посредством определения углов суперструны (Рис. 5.) в многомерном пространстве рисуется геометрический алгоритм для многомерного покрытия наименьшего шара в сочетании с нейронами и сетью сортировки по приоритету.[4] Многомерный алгоритм покрытия наименьшего шара может эффективно решить проблему классификации нескольких типов выборок при распознавании образов.

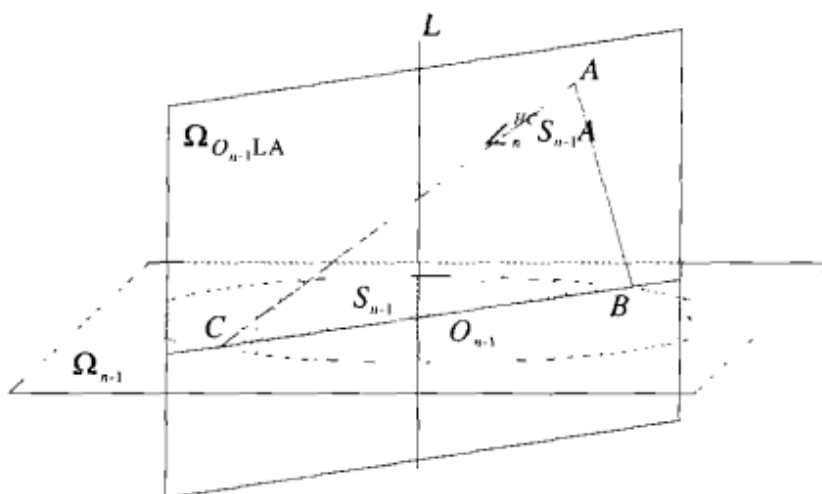


Рис. 5. Трехмерная диаграмма угла суперхорды

1.6. Компьютерное зрение

Используйте средства разработки Microsoft Visual C++ для разработки геометрических операций над цифровыми изображениями. Функция, которая устанавливает связь отображения между изображением и всеми точками в его преобразованном изображении.[5] Эти функции могут однозначно определять геометрическое соответствие между всеми пикселями входного изображения и выходного изображения. Различные геометрические преобразования изображения реализуются с помощью геометрических операций над пикселями.

1.7. Анализ данных

Сравнить полученные данные GPS-позиционирования с дорожным слоем и данными о траектории окружающего транспортного средства в геометрической модели, получить закон траектории, исследовать густые районы в городах и использовать геометрические алгоритмы для отображения огромных объемов данных, чтобы эффективно решить проблему пробок.

2. Тенденции развития

Современная алгоритмическая геометрия, как раздел теоретической информатики, в основном изучает эффективные алгоритмы для решения геометрических задач с крупномасштабными вопросами.

Как специализированная область исследований алгоритмическая геометрия появилась в 1970-х годах. В то время, в связи с потребностями промышленного дизайна и других областей, появился автоматизированный дизайн (CAD), и проблемы, которые он пытался решить, обычно были очень сложными или очень масштабными, далеко выходящими за рамки прямых расчетов людьми.[6] Поэтому исследование эффективных геометрических алгоритмов, которые легко реализуются компьютерами, имеет большое значение.

С развитием других областей теоретической информатики (особенно вычислительной сложности и теории проектирования алгоритмов), а также улучшением и популяризацией алгоритмической мощности человека в сочетании с огромным спросом, вызванным развитием самого общества, алгоритмическая геометрия как область исследований быстро развивалась с момента своего рождения. Сейчас алгоритмическая геометрия превратилась в дисциплину с масштабными журнальными конференциями высокого уровня и активным исследовательским сообществом.

Цели исследования: Исследовать больше областей применения геометрических алгоритмов, решить больше академических и жизненных проблем, обеспечить теоретическую основу алгоритмов для исследования высокоскоростных информационных технологий. Разработать теории автоматизации, алгоритмические методы и принципы взаимодействия геометрического моделирования, повысить эффективность компьютерного геометрического расчета и операций.

Для достижения поставленной цели следует решить следующие задачи:

1. Разобраться в областях применения и результатах исследований геометрических алгоритмов в стране и за рубежом.
2. Изучить сценариев применения геометрических алгоритмов в других областях.
3. Разработать автоматизированные инструменты геометрического алгоритма, которые могут быть применены к нескольким сценариям.
4. Удовлетворить потребности развития компьютерных геометрических алгоритмов в условиях высокоскоростных информационных технологий.

Список использованных источников:

1. Волошинов Д.В. Теория автоматизации проектирования объектов и процессов на основе методов конструктивного геометрического моделирования : автореф. дис. ... д-ра техн. наук :05.13.12 / Волошинов Денис Вячеславович. СПб., 2010. 3-5 с.
2. Сюн Сюй, Юй Хань, Цуй Лилу, Чэнь Кэцзе, Чжао Лэй. Алгоритм пространственной геометрии для обнаружения и исправления скачка трехчастотного цикла Бэйдоу. // Геодезия и картографирование Пекина. 2019. 33(08). С. 872-876.
3. Ван Яксун, Кан Фэн, Ли Вэньбинь, Чжэн Юнцзюнь. Оптимизация алгоритма геометрии диаметра вертикального деревянного сундука на основе 2D лазерного детектирования. // Журнал сельскохозяйственной техники. 2016. 47(06). С. 290-296.
4. Лай Цзянлян, Ван Шоуджуэ. Алгоритм геометрии минимального покрытия шара и его применение в распознавании образов. // Распознавание образов и искусственный интеллект. 2006. 19(02). С. 271-276.
5. Алгоритм вычислительной геометрии [Электронный ресурс]. URL: <https://www.zgbk.com/ecph/words?SiteID=1&ID=146755&Type=bkzyb&SubID=81672> (дата обращения 15.11.2022).
6. Ван Чжэньминь. Геометрические операции с цифровыми изображениями // Компьютерные знания и технологии. 2020. 16(03). С. 209-212+226.

Lyu Yingzheng

Peter the Great St.Petersburg Polytechnic University

Scope and development trends of geometric algorithms.

At present, with the rapid development of information technology and the improvement of human computing power, in order to meet the needs of technological development in various industries around the world, the development of geometric algorithms to improve the efficiency of computer geometric calculations and operations is a topic worthy of in-depth research.

Key words: *geometric algorithm, information technology, automated, principles of interaction, efficiency improvement.*

УДК 004.514
ГРНТИ 20.15.05

РАЗРАБОТКА ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА ПОИСКА ЧАТОВ ПО КАРТЕ, ПРИ ПОМОЩИ СУЩЕСТВУЮЩЕЙ ДИЗАЙН- СИСТЕМЫ ПОПУЛЯРНОГО МЕССЕНДЖЕРА

В. В. Макарова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрены основные этапы разработки пользовательского интерфейса поиска чатов по карте при помощи существующей дизайн-системы популярного мессенджера. В результате, проведено исследование целевой аудитории, разработан сценарий и спроектирован логичный и понятный интерфейс поиска чатов по карте для платформы iOS.

пользовательский интерфейс, мессенджер, целевая аудитория, социальная сеть, поиск собеседников, геолокационный сервис

В современном мире люди часто собираются в общие чаты с привязкой по месту, этим местом может быть, например, жилой комплекс, университет, спортивные занятия и другие. Но на данный момент в популярных мессенджерах отсутствуют способы поиска чатов с привязкой к локации.

Прежде чем приступить к разработке макетов, необходимо провести анализ конкурентов и исследование целевой аудитории для выявления проблем, которые пользовательский интерфейс должен будет решать.

Анализ конкурентов показал, что в популярных на сегодняшний день мессенджерах отсутствует поиск чатов по локации, пользователям приходится искать данные чаты через друзей или в специальных сообществах. Для подтверждения гипотезы необходимости внедрения функциональности «Чатов близости» в существующие мессенджеры, необходимо провести исследование целевой аудитории.

По итогам исследования целевой аудитории был проведен анализ результатов, где большинство респондентов подчеркнули важность визуализации месторасположения локации, 12 из 13 респондентов сталкивались с проблемой поиска чатов по локации более пяти раз, 9 из 13 респондентов определили наиболее удобную точку входа в функциональность – по нажатию на специальную иконку на основном экране мессенджера. Данный экран представлен на рис. 1.

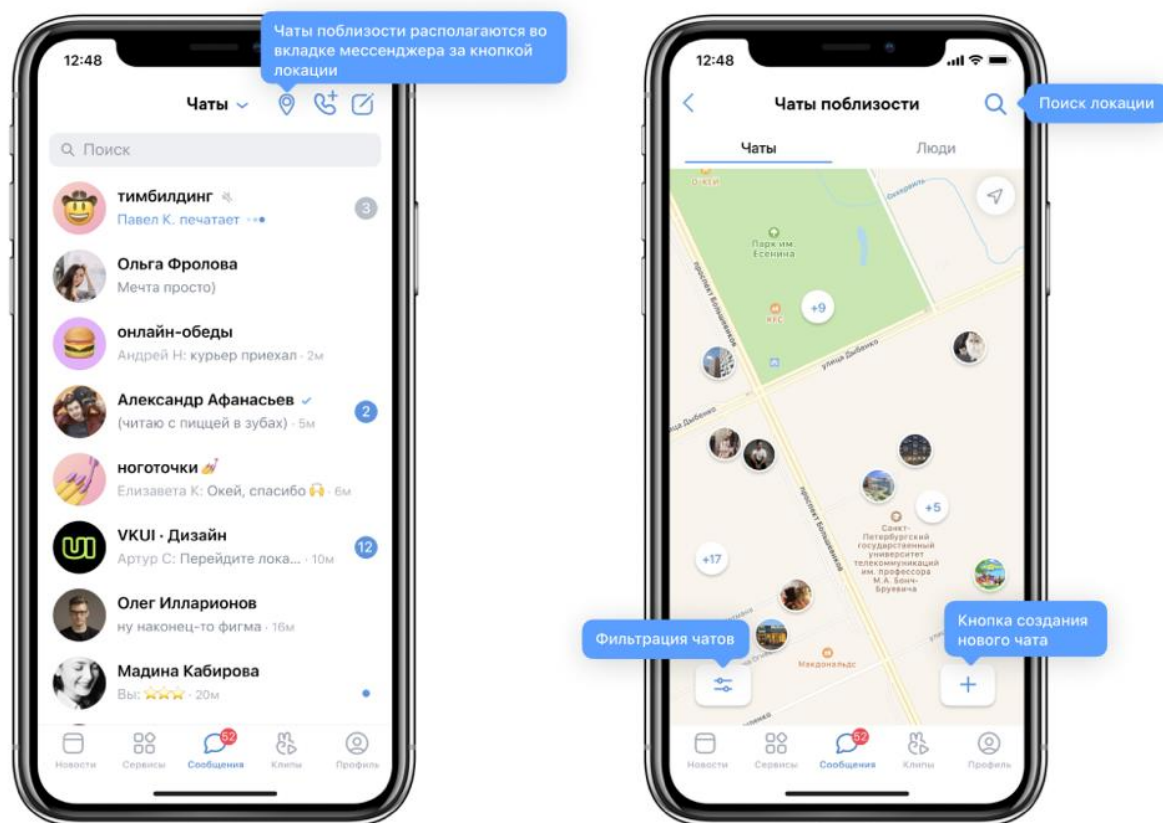


Рис. 1. Точка входа в чаты поблизости

Следующий шаг – разработка пользовательских сценариев. Сценарий – это сжатое описание способов применения интерфейса для достижения цели [1]. Например, вы хотите куда-то поехать, открываете приложение на своем девайсе, ставите конечную точку вашего маршрута, заказываете такси. Данный сценарий – это самый быстрый способ достижения пользователем целевого действия, но сценарий может быть шире, например, появление шага с подтверждением способа оплаты. Именно поэтому, необходимо разработать дерево сценариев, которое представлено на рис. 2.

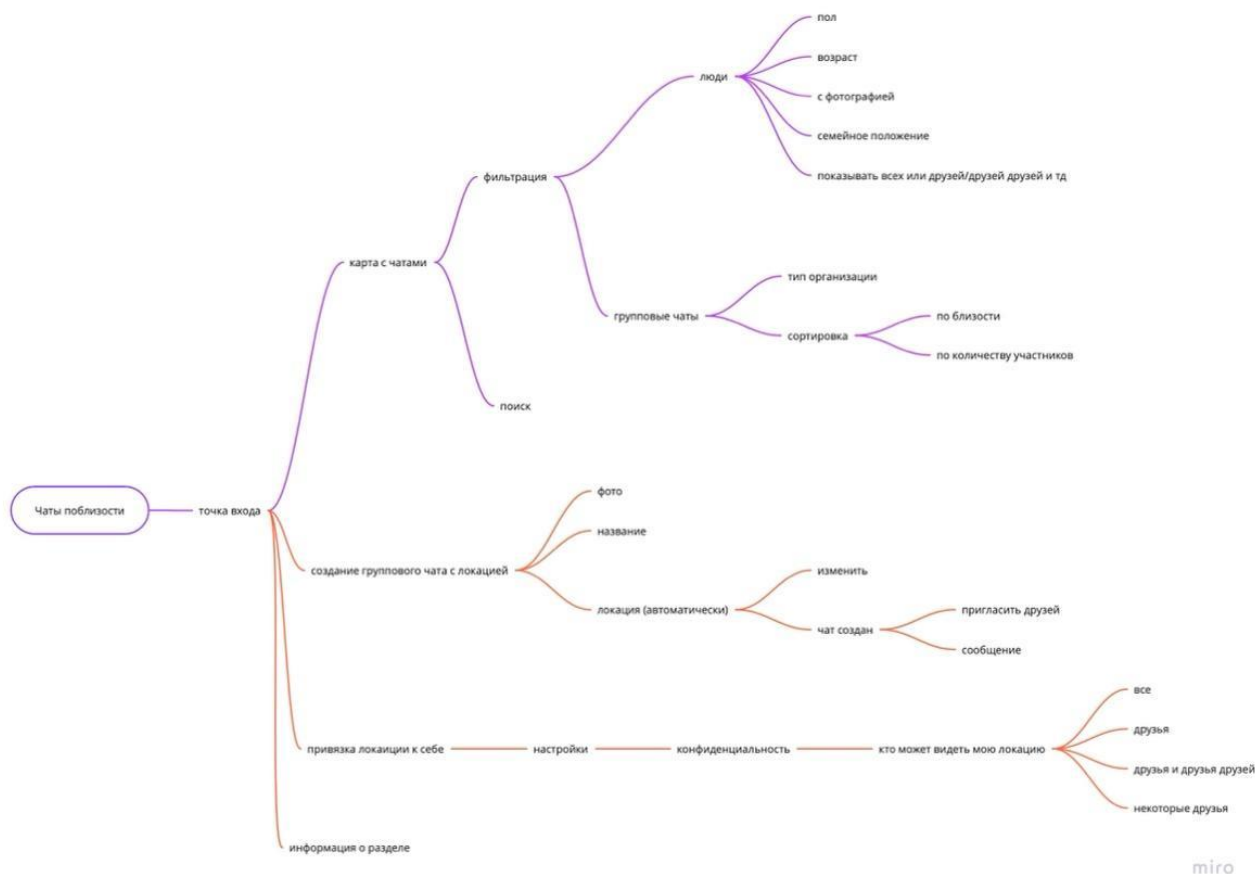


Рис. 2. Дерево сценариев

Построения макетов пользовательского интерфейса на основе дерева сценариев реализовано при помощи существующей дизайн-системы –VKUI, соединяющей визуальный язык с технической реализацией, компонентами и руководством по применению [2]. Для использования данной дизайн-системы необходимо понимать принципы работы существующих компонентов, например, снейкбар – это всплывающее уведомление о совершенном действии или случившемся событии, табы в виде сегментированного контроля – для переключения вкладок, только тогда данная система поможет сэкономить время при разработке макетов. Дизайн-система VKUI представлена на рис. 3.

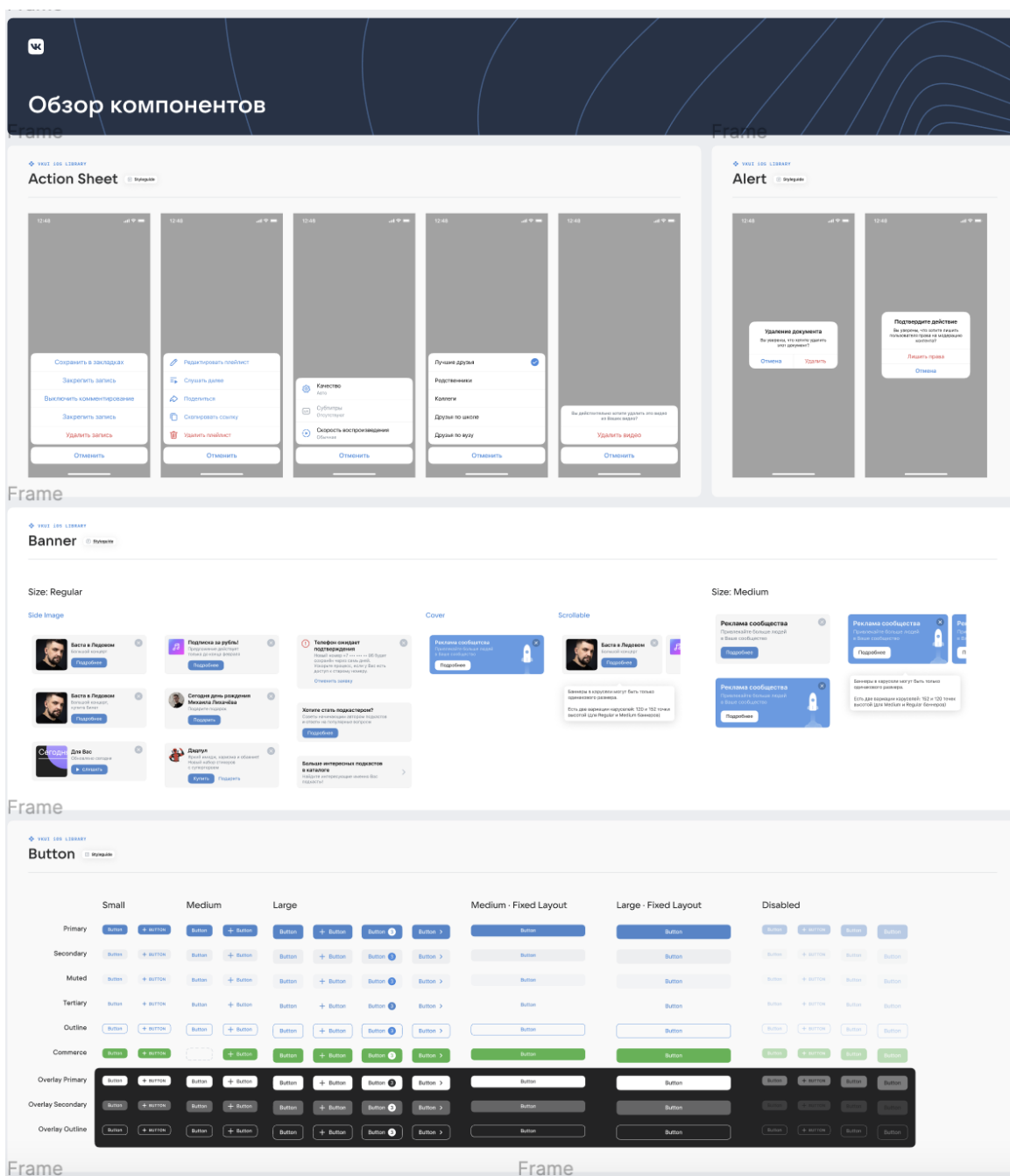


Рис. 3. Дизайн-система VKUI

При разработке макетов необходимо уделить внимание аккуратности верстки и отсутствию шума – всегда приятно пользоваться аккуратным интерфейсом, в котором ничего не отвлекает от выполнения задачи [3]. Необходимо исключить контрастные тени, разные по стилю иконки, использовать цвета и шрифты только из дизайн-системы, так как консистентность – одно из главных правил хорошего тона в дизайне.

Получившийся пользовательский интерфейс разработан для платформы iOS и представлен на рис. 4.

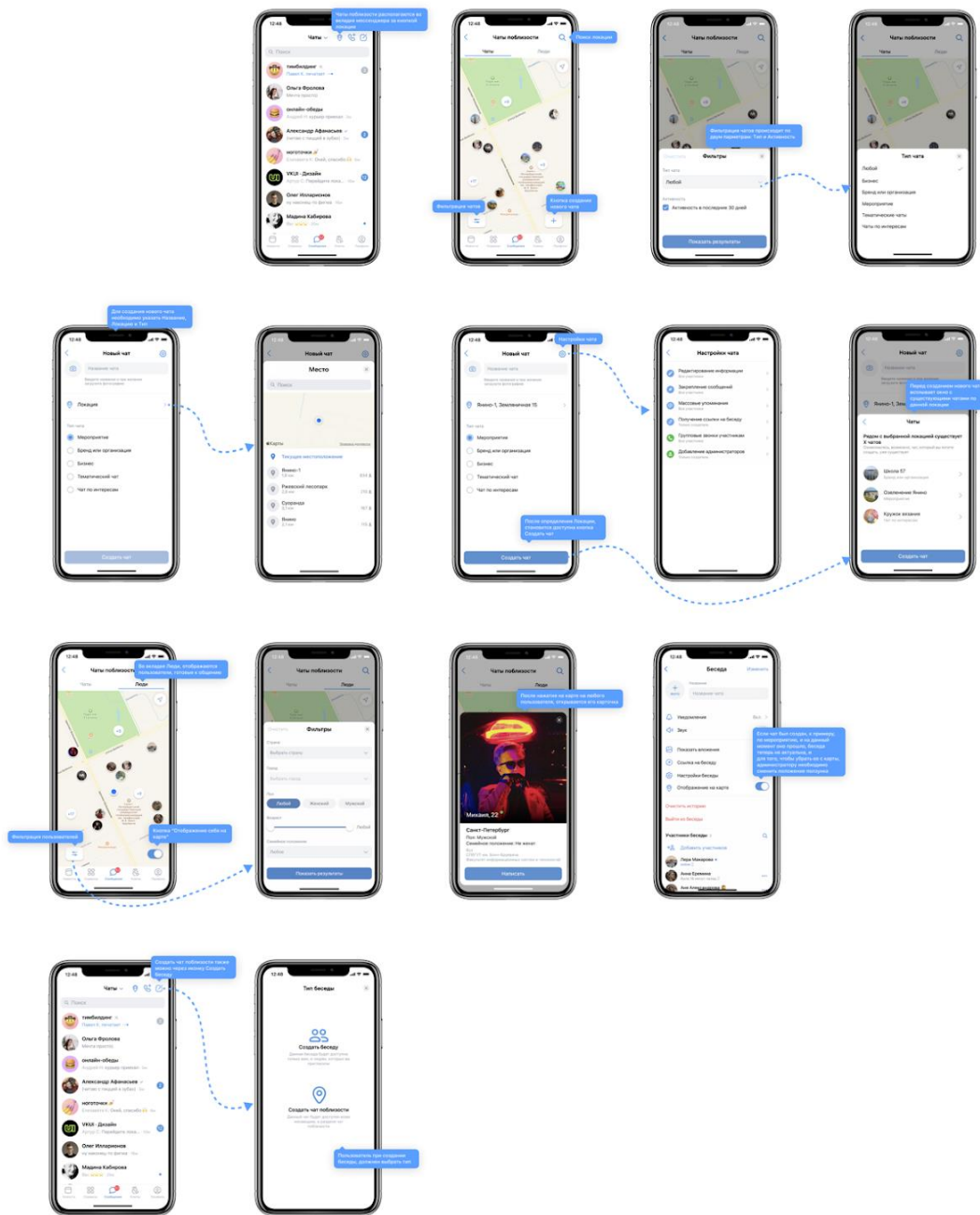


Рис. 4. Пользовательский интерфейс

Завершающим шагом стало проведение удаленного немодерируемого юзабилити-тестирования, данное тестирование отличается от «модерируемого», тем, что респонденты выполняют задания на специальном ресурсе самостоятельно [4]. Респондентам необходимо было познакомиться с прототипом пользовательского интерфейса, созданного в Figma и ответить на несколько вопросов:

- как быстро вы нашли точку входа в «Чаты поблизости»;
- оцените удобство поиска чатов на карте;
- оцените процесс создания «Чата поблизости»;

- оцените простоту и удобство разработанного интерфейса.

Анализируя результаты, большинству респондентов (6 из 7) понадобилось менее 10 секунд для поиска точки входа, у всех получилось разобраться, как искать и создавать «Чат поблизости», и благодаря использованию популярной дизайн-системы и общепринятых компонентов для iOS из Human Interface Guidelines, интерфейс получился простым и удобным в использовании.

Респондентами, также, были подмечены моменты, которые будут исправлены в следующей итерации, например, на главной странице мессенджера, три иконки в одном верхнем углу – перебор, зона нажатия стала меньше, шанс промахнуться – больше. Решение данной проблемы предлагает Human Interface Guideline: разделить иконки по разным углам, это привычный паттерн для пользователя iOS.

В результате данной работы описан стандартный жизненный цикл создания пользовательского интерфейса для платформы IOS при помощи готовой дизайн-системы популярного мессенджера.

Список используемых источников:

1. Use Case в дизайне: пример применения пользовательских сценариев от стартапа Trucker Path [Электронный ресурс]. URL: <https://vc.ru/flood/18197-trucker-path-design> (дата обращения 10.11.2022).
2. VKUI iOS Library [Электронный ресурс]. URL: <https://www.figma.com/community/file/842773796460998995> (дата обращения 10.11.2022).
3. Основные принципы верстки макетов [Электронный ресурс]. URL: <https://guides.kontur.ru/principles/layouts/> (дата обращения 10.11.2022).
4. Круг С. Как сделать сайт удобным. Юзабилити по методу Стива Круга: пер. с англ. М: Питер, 2010. 208 с. ISBN 978-5-49807-515-0.

Makarova V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Development of the user interface for searching chats on the map.

The article discusses the main stages of developing a user interface for searching chats on a map using the existing design system of a popular messenger. As a result, a study of the target audience was carried out, a script was developed and a logical and understandable interface for searching chats on the map for the iOS platform was designed.

Key words: user interface, messenger, target audience, social network, search for interlocutors.

УДК 004.514
ГРНТИ 81.95.33

ОБЗОР МЕТОДОВ УПРАВЛЕНИЯ ВИЗУАЛЬНЫМ ВОСПРИЯТИЕМ ПОЛЬЗОВАТЕЛЯ

С. В. Максимова, Т. В. Мусаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире человек постоянно сталкивается с графическими пользовательскими интерфейсами. Интерфейс должен выполнять цели и задачи, поставленные разработчиками. Для их достижения целесообразно использовать методы управления визуальным восприятием пользователя. В статье рассматриваются различные методы управления восприятием пользователя, действие которых обосновано особенностями работы человеческого мозга.

дизайн интерфейса, UI – дизайн, графический интерфейс, пользовательский интерфейс

В последние годы жизнь людей всё больше подвергается цифровизации [1]. Пользователи общаются в социальных сетях и мессенджерах, делают покупки в интернет – магазинах, заказывают доставку еды через приложения, предпочитая такой способ реальному походу в магазин. Интерфейсы веб – сайтов и мобильных приложений, с которыми современный пользователь сталкивается ежедневно, стали не просто дополнением к нашему миру, а неотъемлемой его частью.

При разработке дизайна графического интерфейса необходимо понимать его цели и назначение. Внимание пользователя должно направляться в соответствии с этими целями, интерфейс должен быть правильно воспринят, а также являться удобным и понятным для использования. Чтобы грамотно разработать дизайн пользовательского интерфейса необходимо учитывать психофизиологические особенности восприятия информации человеком.

Психофизиология – наука, изучающая нейрофизиологические механизмы психических процессов, состояний и поведения [2]. В контексте проектирования интерфейсов нам интересны психофизиологические аспекты поведения человека при взаимодействии с визуальной информацией.

Произведём обзор методов управления визуальным вниманием пользователя интерфейса, действие которых обусловлено психофизиологическими особенностями человека.

- Закон Миллера или правило 7 ± 2 . Число объектов, которые человеку комфортно одновременно воспринимать для решения задачи находится в диапазоне от 5 до 9. К такому выводу пришёл американский психолог Джордж Миллер после ряда проведённых экспериментов [3].

Пример использования принципа 7 ± 2 можно увидеть в дизайне интерфейса приложения «ВКонтакте» (рис. 1). В основном меню сервисов, находящемся в профиле пользователя, представлено 8 основных сервисов. Если бы

разработчики сразу добавили все сервисы в основное меню, то пользователю было бы неудобно в них ориентироваться. Если пользователю нужен другой сервис, то он целенаправленно перейдёт в меню «все сервисы».

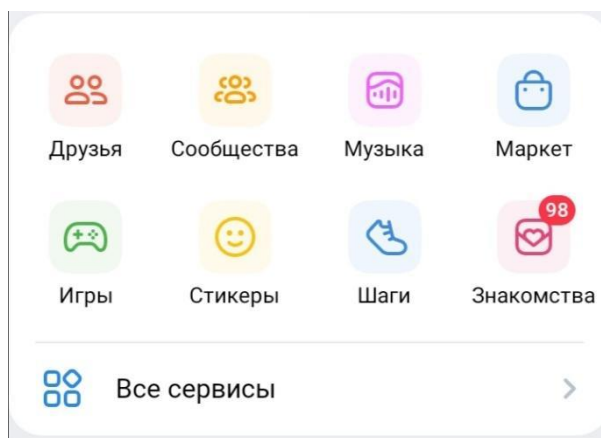


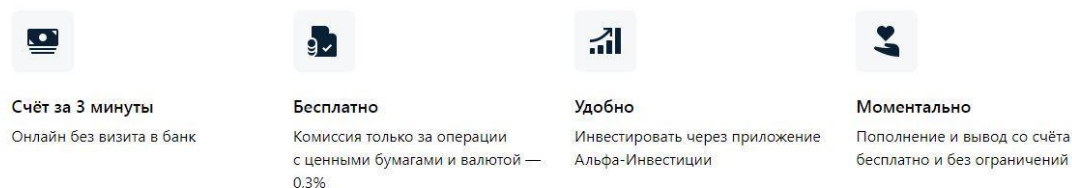
Рис. 1. Интерфейс мобильного приложения «ВКонтакте». Меню сервисов.

- Геометрическая память. Нобелевский комитет в 2014 году присудил премию в области медицины исследователям, открывшим клетки в мозгу человека, позволяющие точно определять местоположение, запоминать и прокладывать маршруты [4]. Существует интересная закономерность: при взаимодействии с объектами и в реальном и в виртуальном пространстве используются одни те же нейроны. Разработчик интерфейса облегчает задачу пользователя, выстраивая объекты по какому – то геометрическому закону. Пользователю не приходится задействовать дополнительные зоны мозга, если он знает путь до нужного объекта.

Рассмотрим примеры. В любых версиях операционной системы Windows кнопка «Пуск» находится в левом нижнем углу. К меню в различных мобильных приложениях, как правило, можно обратиться, нажав на иконку в верхней правой (реже левой) части экрана. Меню веб - сайтов также располагается в верхней части страницы. Переключение между экранами смартфона – тоже способ геометрической навигации. Пользователь приблизительно запоминает, какие приложения располагаются на каком экране. Таким образом, открывая незнакомый интерфейс, пользователь заранее интуитивно знает, где расположены те или иные объекты. Дизайн нового интерфейса необходимо выстраивать, не нарушая уже существующие пользовательские паттерны.

- Эффект края. Это особенность восприятия, согласно которой человек лучше запоминает начальные и конечные элементы группы. Ориентируясь на эту особенность, важные объекты (рекламные баннеры, товары, ссылки, кнопки) целесообразно располагать в начале и в конце страницы. Если информации достаточно много, например речь идёт о веб – сайте интернет – магазина с большим ассортиментом товаров, следует разделить товары на подгруппы, разделить список баннером с другим контентом или добавить страницы товаров с оптимальным количеством товаров на каждой.

- Визуализация данных. В интерфейсе продуктов, особенно сложных, например, банковских, очень много цифр, метрик, индикаторов и других разнообразных и сложно воспринимаемых данных. Для эффективного представления сложных данных пользователям целесообразно визуализировать их. Если оформить все эти данные в инфографику, пользователь быстрее разберется в этих данных и сможет проще решать свои задачи. Пример эффективной визуализации данных в интерфейсе веб – сайта банка представлен на рис. 2.



Как начать инвестировать



Рис. 2. Визуализация данных. Веб - сайт компании «Альфабанк».

- Принципы Гештальта [5]. К ним относятся: принцип негативного пространства, принцип сходства, непрерывности, завершения образа, близости, взаимодействия фигуры и фона. При правильном и уместном использовании эти принципы помогут в решении задач, стоящих перед дизайнером интерфейса. Рассмотрим каждый из принципов подробнее.

Негативное пространство. Теория Гештальта основана на идее, что человеческий мозг будет пытаться упростить и организовать сложные изображения или конструкции, состоящие из множества элементов, подсознательно упорядочивая части в организованную систему, которая создаст цельную картину, а не просто серию разрозненных элементов. Мозг человека создан так, что во всём склонен видеть структуру и модели, чтобы понять окружающую среду лучше и оперативней. Если оставить пустое пространство вокруг или внутри объекта, пробелы в изображении создадут целое, большее, чем сумма его частей (рис. 3).

Сходство. Согласно принципу Гештальта, подобные элементы визуально сгруппированы независимо от близости друг к другу. Они могут быть сгруппированы по цвету, форме или размеру. Сходство может быть использовано, чтобы связать элементы друг с другом, независимо от расстояния между ними. Например, глядя на иконки приложений на экране смартфона,

пользователь понимает, что это элементы одного порядка, так как они имеют сходство по форме и размеру.

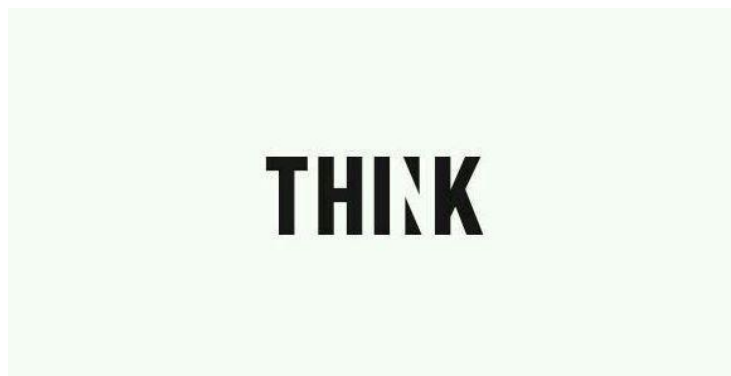


Рис. 3. Пример использования принципа негативного пространства.

Непрерывность. Человеческий глаз будет следовать по самой ровной, гладкой траектории при просмотре линий, независимо от того, как линии были нарисованы. Это продолжение может быть действенным инструментом, когда цель — направить взгляд посетителя в определенном направлении.

Завершение образа. Согласно этому принципу, мозг заполнит недостающие части дизайна или изображения, чтобы создать цельную картину.

Близость. В дизайне пользовательских интерфейсов принцип близости используется для того, чтобы заставить пользователей группировать определенные объекты вместе. При объединении объектов, пользователи будут воспринимать их как нечто связанное. Отличие от принципа сходства состоит в том, что при использовании принципа близости объектам не обязательно иметь сходства между собой, всё дело в расстоянии. Пример использования принципа близости представлен на рис. 4.

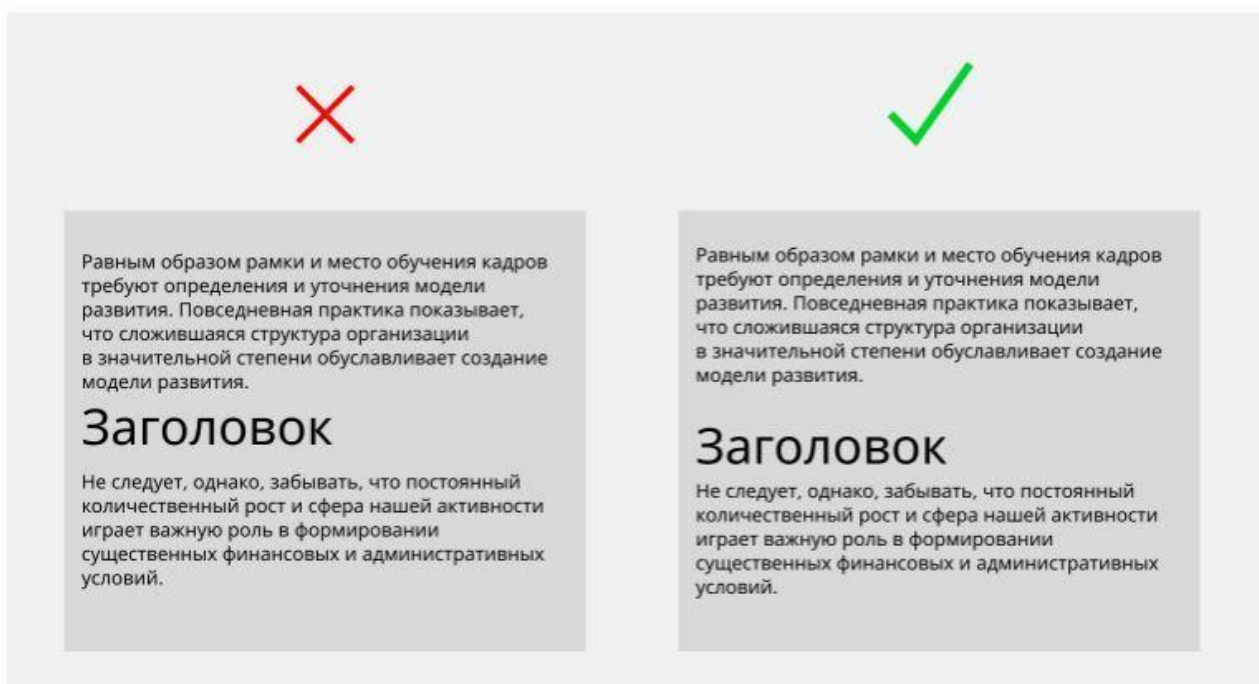


Рис. 4. Грамотное использование принципа близости.

Взаимодействие фигуры и фона. Аналогично первому принципу, он использует отрицательное пространство. Человеческий мозг будет различать объекты на переднем плане изображения. Использование данного принципа целесообразно, если необходимо сделать акцент на фокусе.

Таким образом, проведён обзор различных методов управления визуальным восприятием пользователя. Действие данных методов обусловлено с точки зрения психофизиологических особенностей восприятия визуальной информации человеком. Методы управления визуальным восприятием целесообразно применять при разработке графического дизайна пользовательских интерфейсов веб – сайтов и мобильных приложений, а также операционных систем.

Список используемых источников:

1. Анциферова Т. Н. Цифровизация как фактор трансформации современного общества [Электронный ресурс] // Цифровая наука. 2020. №5. URL: <https://cyberleninka.ru/article/n/tsifrovizatsiya-kak-faktor-transformatsii-sovremennogo-obschestva> (дата обращения: 10.11.2022).
2. Николаева Е. Психофизиология: учебник для вузов. Стандарт третьего поколения. – СПб.: Питер, 2019. – 704 с. ISBN 978-5-4461-0880-0
3. Миллер, Дж.А. Магическое число семь плюс или минус два. О некоторых пределах нашей способности перерабатывать информацию / Дж.А. Миллер // Психология памяти : Хрестоматия / Ред. Ю.Б. Гиппенрейтер, В.Я. Романов. – Москва : ЧеРо, 1998. – С. 564-582.
4. Moser EI, Roudi Y, Witter MP, Kentros C, Bonhoeffer T, Moser MB. Grid cells and cortical representation. *Nat Rev Neurosci*. 2014 Jul;15(7):466-81. doi: 10.1038/nrn3766. Epub 2014 Jun 11. PMID: 24917300.
5. Порозова Д. Ю. Гештальт как основа визуального восприятия [Электронный ресурс] // Человек в мире культуры. 2012. №3. URL: <https://cyberleninka.ru/article/n/geshtalt-kak-osnova-vizualnogo-voSPIriatiya> (дата обращения: 14.11.2022).

Maksimova S., Musaeva T.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Methods for managing the visual perception of the user.

In the modern world, a person is constantly faced with graphical user interfaces. The interface must fulfill the goals and objectives set by the developers. To achieve them, it is advisable to use methods for managing the user's visual perception. The article discusses various methods for managing user perception, the action of which is justified by the peculiarities of the work of the human brain.

Key words: interface design, UI - design, graphical interface, user interface.

УДК 004.514
ГРНТИ 20.53.21

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ДИЗАЙНЕ ИНТЕРФЕЙСОВ

Т. В. Мусаева, П. А. Титов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлен анализ существующих технологий использования искусственного интеллекта в дизайне интерфейсов и оценка эффективности их внедрения. Также были приведены примеры развития и расширения сфер использования искусственного интеллекта в дизайне. Были проанализированы вероятные проблемы, которые могли бы возникнуть при внедрении данных технологий в производственный процесс.

искусственный интеллект, дизайн интерфейсов, макет, дизайн система, алгоритм

Уровень технологического развития информационных технологий стремительно растет с каждым годом. Со времен создания отрасли науки искусственного интеллекта прошло уже более 65 лет и масштаб развития данной отрасли поражает в своих размерах. Данной технологией пользуется практически каждый современный потребитель элементарно используя навигацию. Многие процессы производства уже автоматизированы, в то время как различные компании разрабатывают способы внедрения искусственного интеллекта в создание продуктов [1].

Дизайн интерфейсов подразумевает собой проектирование пользовательских сценариев, взаимодействие с функционалом мобильных приложений и веб сервисов, прототипирование и тестирование макетов на пользователях, сбор информации для улучшения пользовательского опыта и внедрение полученных результатов в существующий продукт.

Создание дизайна посредством алгоритмов уже используется в крупных индустриях. Ежегодно появляются приложения и программы, автоматизирующие процесс проектирования и модерации.

Примером может служить приложение Zeplin, в котором исчезает необходимость создавать спецификации с описанием шрифтов, цветов и интервалов, приложение генерирует их автоматически [2]. Zeplin самостоятельно выводит результат на основе предполагаемой целевой платформы и предполагает прямое извлечение документации для разработки.

Существуют различные алгоритмы основанные на искусственном интеллекте для оценки юзабилити, что позволяет исключить присутствие респондентов в некоторых видах интервью и тестирований интерфейса. Примером может служить программа VisualEyes, которая предполагает исследование движения глаз пользователя и прогнозирование предпочтительных блоков с точность более 93%. Данная технология многократно ускоряет и оптимизирует процесс создания продукта за счет сокращения времени проведения эксперимента и ускорения цикла получения обратной связи. Результат работы данного сервиса представлен на рис. 1.

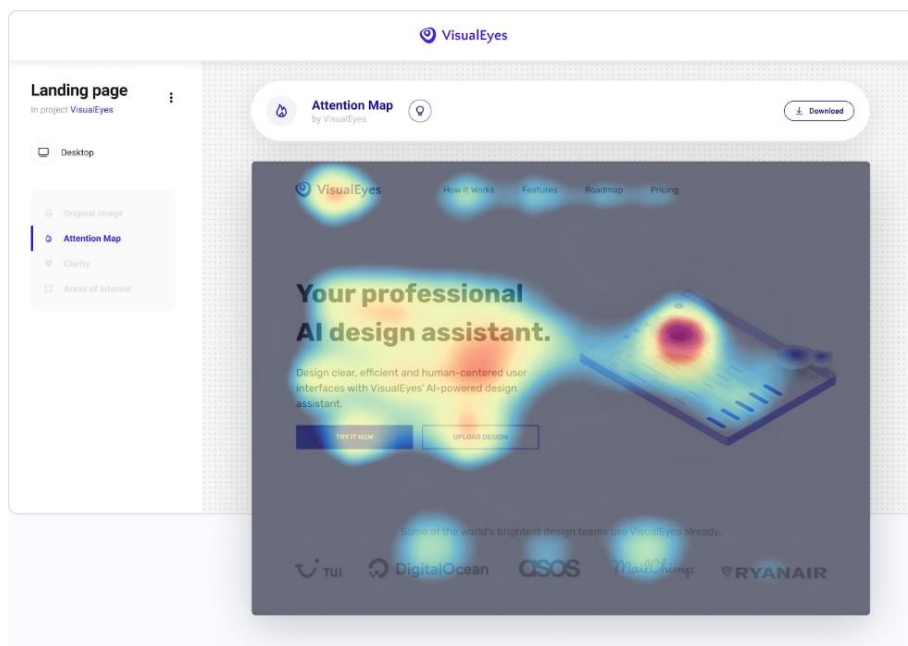


Рис. 1. Результат работы сервиса VisualEyes

Другим выдающимся примером служит искусственный дизайнерский интеллект “Николай Иронов”, который способен отрисовывать уникальные логотипы и формировать корпоративный стиль [3]. Даже самые прогрессивные и успешные дизайнеры ориентируются на чужие удачные работы, формируя тем самым собственный стиль. В свою очередь, искусственный интеллект открывает новейшие, смелые и неожиданные идеи, потому что он ориентируется только на самого себя и на техническое задание, предоставленное клиентом.

В рассмотренных примерах наглядно показано, как технологии искусственного интеллекта упрощают или автоматизируют некоторые процессы разработки дизайна интерфейса. Существует большое разнообразие автоматизированных программ, которые предоставляют дизайнерам возможность ориентироваться на выполнение незаменимой алгоритмами работы. Данные программы существенно увеличивают эффективность процесса создания дизайна.

Какой вектор развития держит искусственный интеллект в сфере дизайна интерфейсов?

Композиция, а именно гармоничное и нативное расположение блоков интерфейса включает в себя основу дизайна. Одним из способов использования технологии искусственного интеллекта может послужить система интегрированной генерации макетов, посредством которой алгоритм будет вычислять и представлять множество вариаций макетов, что глобально ускорит процесс итерации [4]. Разработчику необходимо будет по предпочтению или необходимости ввести максимальные и минимальные граничные параметры, уровень детализации, количество блоков и их рейтинг важности для компании и потребителя. В перспективе может появиться возможность по желанию загрузить рукописный макет расположения блоков. На текущий день уже

существует нейросеть, способная генерировать макет сервиса по текстовому описанию. Результат работы нейросети представлен на рис. 2.

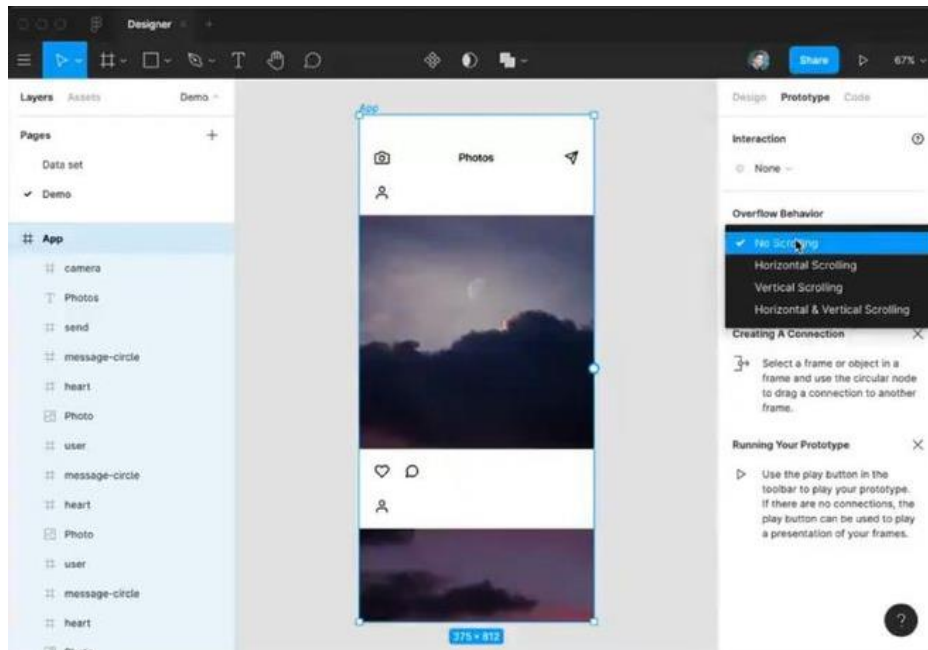


Рис. 2. Макет приложения, сгенерированный нейросетью по текстовому описанию

Другой основополагающей составляющей крупного цифрового продукта является дизайн система. Дизайн система это совокупность компонентов интерфейса и полная документация к ним, позволяющая существенно упростить и ускорить процесс разработки макетов. Дизайн система синхронизирует команду разработчиков и дизайнеров за счет единого свода правил работы элементов интерфейса. Искусственный интеллект может предполагать автоматизированное распознавание индивидуальности компонентов посредством написания их документации, которая включает в себя ключевые размеры, состояния и адаптацию для различных устройств, создание непосредственной коллекции всех компонентов с их характеристиками. Также технология будет предусматривать аналогичные компоненты в интерфейсе, что обеспечит чистоту и органичность дизайн системы. Использование искусственного интеллекта в создании дизайн системы освободит время на более важные задачи, такие как создание индивидуального стиля продукта, проработка пользовательских сценариев, анализ и улучшение пользовательского опыта.

Трудно представить заключительный результат продукта без корпоративного стиля, цветов и иллюстраций. В скором времени технологии искусственного интеллекта несомненно привнесут вклад и в эту область. Специальные алгоритмы смогут накапливать творческий интеллект посредством ключевых слов, которые в свою очередь будет формулировать дизайнер. Также дизайнеру необходимо будет проанализировать и определить детализацию изображения, граничные условия, цветовую гамму и количество различных вариантов макетов. На выходе алгоритм будет формировать и предоставлять необходимую вариацию иллюстраций для интерфейса. В перспективе процесс

работы дизайнера сократится до создания макета, загрузки скриншота в алгоритм и выделения приоритетных областей для иллюстраций.

Несомненно, технологии искусственного интеллекта - это вектор в будущее, где большую часть монотонной работы смогут выполнять алгоритмы. Однако, какие проблемы могут возникнуть с внедрением данных технологий без контроля дизайнера?

На данный момент технологии искусственного интеллекта полностью зависят от данных, которые им разрешено потреблять. Не имея рационального мышления, установленных ценностей, приличий и мировоззрения, алгоритмы могут бессознательно наносить вред пользователю, посредством создания неприемлемых убеждений в отношении расы, этнической принадлежности, национальности, дохода, способностей и религиозных убеждений. Для сглаживания этой проблемы необходим постоянный контроль куратора дизайнера [5].

Особенность идеального дизайна находится в его несовершенности. Порой самые смелые и новые дизайнерские подходы пользуются невероятным успехом у пользователей, несмотря на конструктивную критику. Главной задачей внедрения технологий искусственного интеллекта в дизайнерский процесс является увеличение эффективности работы, раскрытие большего потенциала дизайнера, создание осмысленного и работающего дизайна ориентированного на человека, избавляя дизайнера от необходимости выполнять рутинные и повторяющиеся действия. Технологии искусственного интеллекта должны стать незаменимым помощником творческого человека.

В результате исследования несомненно выделяются своей эффективностью технологии, которые максимально сокращают время итерационной работы дизайнера, такие как автоматизированная генерация макета и технология анализа юзабилити интерфейсов.

Рабочим алгоритмом конвертации текстового описания в изображение служит нейронная сеть DALL-E от компании Microsoft. В ее основу входят распознавание образов, интерпретация пользовательского опыта и обучение. Уже сейчас данный инструмент может существенно сэкономить время на некоторых задачах, и со временем его возможности будут заметно увеличиваться. Поэтому при проектировании интерфейса рекомендуется использовать данную нейронную сеть.

Список используемых источников:

1. Горбачевская Е.Н., Краснов С.С. История развития нейронных сетей // Вестник Волжского университета им. В. Н. Татищева, научный журнал 2015, с. 5.
2. Zeplin.io [Электронный ресурс]. URL: <https://zeplin.io/> (дата обращения 02.11.2022).
3. Habr.com // Нейросеть «Николай Иронов» [Электронный ресурс]. URL: <https://habr.com/ru/news/t/667010/> (дата обращения 02.11.2022).
4. Vc.ru // Искусственный интеллект в дизайне. С кем клиентам будет удобнее работать в будущем? Мнение профессионалов. [Электронный ресурс]. URL: <https://vc.ru/design/501255-iskusstvennyu-intellekt-v-dizayne-s-kem-klientam-budet-udobnee-rabotat-v-budushchem-mnenie-professionalov> (дата обращения 05.11.2022).

5. Jonyablonski.com // AI in Design [Электронный ресурс].
URL: <https://jonyablonski.com/articles/2021/ai-in-design/> (дата обращения 07.11.2022).

Titov P., Musaeva T.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Artificial intelligence in interface design.

The article presents an analysis of existing technologies for using artificial intelligence in interface design and an assessment of the effectiveness of their implementation. Examples of the development and expansion of the use of artificial intelligence in design were also given. The probable problems that could arise when introducing these technologies into the production process were analyzed.

Key words: artificial intelligence, interface design, layout, system design, algorithm.

УДК 004.031.42
ГРНТИ 50.43.17

ОСНОВНЫЕ ПРОБЛЕМЫ РАЗРАБОТКИ И ПРОЕКТИРОВАНИЯ СОВРЕМЕННЫХ ИНТЕРФЕЙСОВ

Д. И. Нефедов, Н. А. Сергеев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире вместе со сложной техникой и информационными системами, которые требуют эффективной и комфортной работы пользователя с ними, появилась резкая потребность в качественном пользовательском интерфейсе, который соответствует всем современным требованиям. Ведь качественный пользовательский интерфейс является одним из ключей к успеху любого проекта.

UI, пользовательский интерфейс, проектирование информационных систем

В настоящее время всё больше людей взаимодействуют со сложной микропроцессорной техникой и информационными системами в своей повседневной жизни. По статистике Gartner — исследовательской и консалтинговой компании, специализирующейся на рынках информационных технологий, расход на сектор информационных технологий неуклонно растёт, отсюда можно сделать вывод и о росте количества информационных технологий и техники.

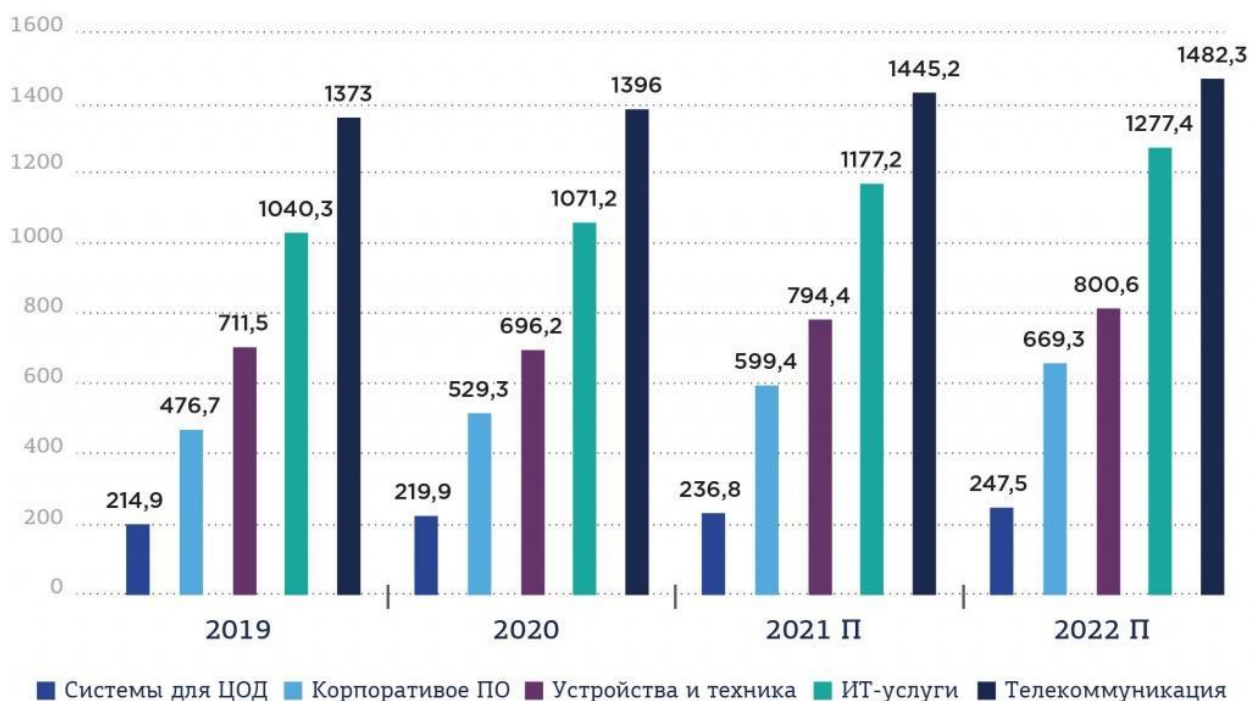


Рис. 1. Статистика Gartner о. Мировых расходах на ИТ-отрасль по сферам в 2019-2022 П, млрд долл.

Исходя из этого факта, проблемы, связанные с разработкой пользовательских интерфейсов, становятся более острыми, и решение таких проблем выходит на передний план при разработке интерфейсов.

Существует множество проблем при разработке пользовательских интерфейсов, но в этой статье мы хотим осветить, на наш взгляд, самые важные.

Адаптивность

Адаптивность — это способность интерфейса «подстраиваться» под различные технические условия, например, под различные размеры экранов. Адаптивный интерфейс хорошо смотрится и на мониторе персонального компьютера, на ноутбуке, и на экране смартфона. При этом качество отображения не зависит ни от диагонали, ни от позиционирования экрана.



Рис. 2. Пример адаптивного интерфейса

Не важно каким устройством вы пользуетесь, важно то, что интерфейс информационной системы автоматически подстраивается под ваше устройство, сохраняя весь функционал. В свою очередь достижение адаптивности очень трудоёмкий процесс, который имеет множество решений. Отсюда возникают вопросы, о том, как лучшим способом достичь адаптивности интерфейса?

Отзывчивость

Во время непрерывных действий, таких как прокрутка окна или же скролл, пользователь может допустить отсутствие визуальной обратной связи в течении ограниченного короткого периода. Если этот период очень долгий пользователь получит отрицательный опыт от использования приложения. Даже пропуск одного кадра в 16 миллисекунд вызовет отрицательные эмоции у человека. Для дискретных событий, таких как клик по кнопке, по данным некоторых исследований, обратная связь с пользователем должна составлять не менее 100 миллисекунд. В противном случае необходимо показывать визуальный индикатор рис. 3, но в некоторых случаях обработка дискретного события с индикатором воспринимается дольше чем без него. Из-за таких ситуаций возникают вопросы об отзывчивости интерфейса.

Loading dmitry@usabilitypost.com...



Рис. 3. Пример индикации загрузки

Навигация

Каждый пользователь ожидает от интерфейса стабильности при взаимодействии с ним. Элементы интерфейса не должны внезапно исчезать с экрана. Также и навигация внутри приложения должна придерживаться этого принципа. При переключении между разделами приложения пользователи ожидают, что состояние элементов интерфейса будет сохраняться. Это можно показать на примере ленты новостей. Если мы находимся в середине ленты и хотим переключиться на другой раздел, например музыка, после чего вернуться назад, мы точно не захотим заново листать ленту с начала или ждать пока прогрузится её прошлое состояние. Так возникают вопросы о том, как спроектировать приложение с удобной навигацией, которая поддерживает произвольную навигацию пользователя по приложению.

Энтропия

Для пользовательских интерфейсов почти невозможно предугадать действия отдельного пользователя и их последовательность. В любой момент наш интерфейс и приложение могут находиться в одном из множества состояний. Например, для простой кнопки, которая имеет 5 разных состояний, код должен учитывать 20 возможных переходов между ними или запрещать некоторые из них. При этом остро стоит вопрос о том, как нам лучше создавать предсказуемый вывод для каждого возможного состояния.

Целостность

При нажатии на кнопку лайка под видео появляется надпись: «Вам и ещё 100 000 пользователей понравилось это», надпись исчезла. На первый взгляд это просто. Но может случиться так, что эта надпись присутствует в нескольких местах в интерфейсе. Также может существовать дополнительная визуальная индикация для оценки (например, её цвет), которая тоже должна изменяться. А список аудитории, которой понравился пост, предварительно полученный с сервера отображается при наведении курсором, теперь должен включать ваш псевдоним или имя. А если вы перешли в другой раздел или нажали кнопку «Назад», то пост не должен «забыть» информацию о вашей оценке. Отсюда вытекает то что, локальная целостность для одного пользователя создает ряд непростых задач. При этом другие пользователи в режиме реального времени тоже могут взаимодействовать с данными, которые отображаются у вас в интерфейсе. При решении задачи о целостности возникает ряд вопросов: Как нам поддерживать данные синхронизированными в разных частях экрана? Как и когда нам сверять локальные данные с сервером и получать/отсылать изменения?

Вывод

В данной статье были приведены основные проблемы в области проектирования и разработки пользовательских интерфейсов. Конечно, приведённый в этой статье список проблем с пользовательскими интерфейсами, не полон, однако, мы попытались дать понять, что у всякой проблемы есть своя причина: будь то стремление снизить стоимость разработки или ошибочно высокие требования к пользователям. И при решении всякой проблемы очень

важно помнить о настоящей причине её возникновения: чинить крышу, а не подставлять под место протечки ведро побольше.

Как писал автор теории решения изобретательских задач Г.С.Альтшуллер, «лучшая система — это система, которой нет». Это высказывание применимо и к графическим интерфейсам пользователей, ведь лучший интерфейс — тот, которого не замечаешь, который не отнимает времени на своё изучение, а все усилия пользователя перенаправляет на решение поставленной задачи.

Список используемых источников:

1. Купер А., Рейман Р., Кронин Д. Алан Купер об интерфейсе. Основы проектирования взаимодействия. – Пер. с англ. – СПб.: Символ'Плюс, 2009. – 688 с., ил. ISBN 978'5'93286'132'5
2. Проектирование интерфейсов пользователя : пособие для студентов специальности 1-47 01 02 «Дизайн электронных и веб-изданий» / Т. П. Брусенцова, Т. В. Кишкурно. – Минск : БГТУ, 2019. – 172 с. ISBN 978-985-530-799-1.
3. Статья: Основные проблемы разработки современных интерфейсов [Электронный ресурс]. URL: <https://habr.com/ru/post/435912/> (дата обращения 10.11.2022).

Nefedov D., Sergeev N.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

The main problems of development and design of modern interfaces.

In the modern world, along with complex technology and information systems that require efficient and comfortable user work with them, there is a sharp need for a high-quality user interface that meets all modern requirements. After all, a high-quality user interface is one of the keys to the success of any project.

Key words: *UI, user interface, information systems design.*

УДК 004.514
ГРНТИ 20.15.05

ИССЛЕДОВАНИЕ МЕТОДОВ АВТОМАТИЗАЦИИ ТЕСТИРОВАНИЯ ЭРГОНОМИКИ ВЕБ-ИНТЕРФЕЙСОВ

Е. И. Онофрийчук

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Эргономика является одним из важнейших аспектов, которые учитываются при разработке и продвижении веб-интерфейсов. Основной целью повышения удобства использования интерфейсов является улучшение связей между компьютерными системами и пользователями путем создания интерфейсов, которые будут более чувствительными к потребностям пользователей. Данная статья посвящена изучению решений в области автоматизации тестирования эргономики веб-интерфейсов. В рамках исследования были выделены три группы основных подходов в автоматизации данного процесса, проведен их краткий обзор. На основе проведенного исследования были определены возможности и ограничения.

пользовательский интерфейс, эргономика, автоматизация, проектирование юзабилити, веб-дизайн

Со времен возникновения интернет претерпел существенные изменения, прежде чем стать таким, каким он является сейчас, параллельно менялись и подходы в бизнес-маркетинге. Эти перемены подтолкнули предпринимателей поддерживать и совершенствовать свои веб-сервисы. В настоящее время все больше организаций стремятся создать удобные в использовании сайты, которые будут привлекать конечных пользователей.

Эргономика веб-интерфейса – это качественный признак того, насколько продукт является комфортным, эффективным и результативным для достижения целей его посещения пользователями. Этот показатель влияет на отображение веб-сайта в поисковых системах, которые стали учитывать поведенческие факторы в ранжировании результатов поисковых запросов. Существует множество методов оценки удобства использования, но основной и самый эффективный – метод юзабилити-тестирования.

Понятие «юзабилити» в стандарте ISO 9241-11 (1998) определяется как степень, с которой продукт может быть использован определенными пользователями при определенном контексте использования для достижения определенных целей с должной эффективностью, продуктивностью и удовлетворенностью.

Продуктивность здесь означает полноту достижения пользователями своих целей и, как правило, измеряется следующими параметрами:

- соотношение между успешными и ошибочными действиями пользователя;
- доля используемого функционала и команд (чем выше, тем лучше);
- когнитивная нагрузка на пользователя, выражающаяся в потреблении ресурсов памяти, внимания и воображения (чем меньше, тем лучше).

Эффективность для веб-сайтов – это скорость, необходимая пользователям для выполнения своей задачи. Она оценивается по следующим критериям:

- легкость, с которой пользователи могут начать выполнение своих задач на пока незнакомом для себя сайте;
- время на выполнение задачи;
- ошибки (какое количество ошибок допустимо для пользователя, серьезность ошибок, сколько времени потребуется для их исправления);
- запоминаемость (насколько легко можно ориентироваться в работе с веб-сайтом после значительного перерыва).

Удовлетворенность – это субъективный эмоциональный аспект, специфичный с точки зрения пользователя, задачи и контекста из-за того, что исходят из различных факторов с точки зрения назначения сайтов. Тем не менее, этот параметр подчеркивает важность удобства использования. Его отсутствие разочарует пользователей и приведет к тому, что они покинут этот сайт и перейдут на другой конкурирующий [1].

На аналогичных основаниях Фишер утверждает, что качество навигации и простота в использовании существенно влияет на количество реально прочитанного содержания веб-сайта, эмоциональный отклик на него, степень разочарования пользователей и их намерение посетить этот сайт снова. Когда сайт считается удобным в использовании, когда сайт считается в достаточной степени эргономичным, пользователи на подсознательном уровне повышают доверие и лояльность к компании, которой он принадлежит [2].

Будучи атрибутом качества продукта, эргономичность веб-сайтов нуждается в тщательной оценке, так как влияет на количество продаж, конкурентоспособность, удовлетворенность пользователей, при этом сокращая бюджеты на обучение и потребность в поддержке пользователей.

Существуют ручные методы оценки удобства использования, такие как экспертная оценка, сегментация пользовательской аудитории, оценка производительности, анкетирование [3]. Все они имеют ряд недостатков:

- субъективность оценки;
- необходимость поиска большого количества респондентов для получения точных результатов;
- отсутствие универсальной методики оценки.

Автоматизация данного процесса позволит не только поможет снизить затраты и требования к квалификации задействованных в ходе оценки экспертов, но и даст возможность прогнозировать потери от вероятных ошибок и испытать несколько вариантов дизайна интерфейса в сжатые сроки. Методы автоматизации можно разделить на три категории:

Оценка, основанная на взаимодействии. Данный подход использует данные, полученные в результате реального или постановочного взаимодействия с сайтом, проходящим тестирование. Могут использоваться движение курсора мыши, манипуляции с клавиатурой. По этим данным реальное взаимодействие сравнивается с описанным эталоном, а также выявляются потенциальные ошибки и угрозы.

Недостатком такого подхода является то, что для проведения тестирования следует собрать достаточный объем данных о реальных взаимодействиях. В противном случае повышается риск создать некачественный веб-интерфейс, что может сказаться на репутации компании и повлечь к финансовым потерям.

Оценка, основанная на метриках. При использовании такого метода ставится задача определить и количественно проанализировать такие характеристики веб-сайтов, как соответствие рекомендациям по дизайну [4], степени визуальной сложности, соотношение объемов графики и текста на странице. Однако на сегодняшний день существует нерешенная проблема, связанная с учетом влияния разнообразия категорий пользователей и контекстов использования на сравнительную значимость этих характеристик.

Оценка, основанная на моделировании. Этот метод решает проблему, возникающую в случае оценки с использованием метрик за счет применения методов искусственного интеллекта проведения тестирования без реального взаимодействия. Модель задач, контекста использования, категорий пользователей и платформ в рамках модельно-ориентированного проектирования [5].

В связи с наблюдающимся активным развитием и внедрением технологий искусственного интеллекта в различные сферы жизни, такой метод является достаточно перспективным. Но несмотря на это, его использование может быть нецелесообразным из-за таких факторов, как:

- вероятная высокая сложность моделей;
- на обучение придется потратить много времени;
- слишком затратная адаптация моделей к меняющимся тенденциям в дизайне интерфейсов.

В рамках проведенного исследования были изучены методики по автоматизации тестирования эргономики веб-интерфейсов. Были выделены три группы основных подходов в автоматизации оценки: на основе взаимодействия, на основе метрик и основанная на моделировании. Рассмотренные возможности проведения оценки эргономики веб-интерфейсов позволяют относительно объективно оценить качество того или иного прототипа веб-интерфейса, выявить ряд проблем продукта.

Исследование показало, что несмотря на проведение тестирования интерфейсов существуют сложности, затрудняющие проведение подробного анализа удобства использования, а некоторые ошибки в проектировании остаются необнаруженными.

Список используемых источников:

1. J. Nielsen Usability ROI declining, but still strong [Электронный ресурс]. // nngroup.com., 2008. URL: <https://www.nngroup.com/articles/usability-roi-declining-but-still-strong/> (Дата обращения: 12.11.2022)
2. С. Flavian, M. Guinal'iu, and R. Gurrea, «The role played by perceived usability, satisfaction and consumer trust on website loyalty», Information and Management, pp. 1–14, 2006
3. Басок Б.М., Рожанская А.Н., Френкель С.Л. О тестировании удобства использования веб-приложений. Российский технологический журнал. 2019;7(6):9-24.

4. Gay G. and Qi Li C. AChecker: open, interactive, customizable, web accessibility checking. Proc. 2010 Intern. Cross Disciplinary Conf. on Web Accessibility (W4A'10), 2010, p. 23.
5. Бакаев М.А. Современные тенденции в автоматизированной оценке юзабилити и поведенческие факторы в алгоритмах поисковых систем // Программные продукты и системы. 2017. Т. 30. № 3. С. 447–455.

Onofriychuk E.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Research of methods to automate testing of web interface ergonomic.

Ergonomics is one of the most important aspects that are considered when designing and promoting web interfaces. The main goal of improving the usability of interfaces is to improve the communication between computer systems and users by creating interfaces that are more responsive to user needs. This paper explores solutions for automating web interface ergonomics testing. As part of the study, three groups of basic approaches to automating this process were identified and a brief overview of them was given. On the basis of the study opportunities and limitations were identified.

Key words: *user interface, ergonomics, automation, usability design, web design.*

УДК 004
ГРНТИ 20.51.15

ОСОБЕННОСТИ SEO-ПРОДВИЖЕНИЯ САЙТА АВТОДИЛЕРА

А. А. Патрухина

Санкт-Петербургский государственный институт телекоммуникаций имени профессора Бонч-Бруевича

Статья посвящена рассмотрению вопросов, связанных с возросшей конкуренцией в сфере продаж автомобилей официальными дилерами. Современное состояние рынка автотранспортных средств ставит новые задачи по организации сайтов, их продвижению. Предлагается акцентировать внимание на SEO-продвижении сайта как наиболее актуальном способе продвижения в нынешних реалиях.

SEO, SEO-продвижение, дизайн, автодилер

Конкуренция в сфере продаж автомобилей растёт невероятными темпами. Это происходит из-за сокращения ассортимента марок автомобилей, доступных в стране, что приводит к сужению их разнообразия на рынке. Многие компании из-за невозможности продавать то, что продавали ранее, переqualифицируются на другие, менее популярные ранее марки. Количество таких компаний растёт, следовательно, растёт и количество дилеров на рынке, которое приводит к усилению конкуренции. Кроме того, в период пандемии возросло число компаний, в том числе автодилерских, что обзавелись сайтами. Потому просто наличие хорошего сайта не является достаточным условием для равной конкуренции на рынке продаж автомобилей официальными дилерами – сайт необходимо продвинуть, и продвижение заключается не только в покупке рекламы через Яндекс.Директ, но и в оптимизации сайта таким образом, чтобы он выпадал в первых строках поиска, в дополнение к функциям рекламы в Яндексе. Целью исследования является изучение методов SEO-продвижения и вывод оптимальной их совокупности для продвижения сайта автодилера [1-2].

Продвижение сайта официального автодилера является интересной задачей. Как правило, дилерские сайты максимально ограничены в своих возможностях импортёром, который задаёт все шаблоны и методы сайтов. Дилерские компании, в основном, используют известное название марки автомобилей, которые продают, даже если эта марка на территории страны не очень распространена. Это обусловлено жёсткими рамками, которые ставит импортёр дилерам, фактически отдавая уже готовый сайт, изменения в котором могут быть минимальны. У таких компаний есть определенные стиль, функционал и дизайн которых должны придерживаться дилеры по всему миру. И не всегда эти параметры являются достаточно привычными для страны, в которой находится дилер.

Одним из основных методов SEO-продвижения является изменение дизайна сайта под нужды компании и требования потенциального клиента. Это не только перемещение кнопок и поисковых строк в привычные места и изменение иконок на более распространённые в данном регионе, но и работа с цветом, изображениями и текстом. Даже способ подачи информации отличается от

региона к региону [3]. Каждый дизайн всегда основывается на особенностях культуры и языка [4].

Японские и китайские сайты для пользователей кажутся слишком перегруженными информацией на начальных страницах, а израильские и арабские изначально вовсе интуитивно непонятны из-за правописания справа налево. Для японцев важно для начала полностью изучить всю информацию, прежде чем переходить к дальнейшему изучению товаров и услуг, поэтому их начальные страницы заполнены как можно большим количеством информации. Более привычные пользователю европейские сайты можно считать самыми аскетичными. В большинстве своём европейские сайты не имеют ярких кричащих изображений в своём дизайне, которые не уточняют товар, а если изображения и присутствуют, то это макрофотографии на заднем плане с пейзажами или абстракциями. В отличие от американских сайтов, где человеческий индивидуализм, наоборот, подчёркивается фотографиями улыбающихся счастливых людей. Европейские и американские сайты имеют весьма краткую характеристику компании и товаров на заглавной странице, а более подробная информация находится на соответствующей отдельной вкладке. Непривычный дизайн сайтов вызывает желание поскорее их покинуть, тогда как привычный не ведёт ни к какому дискомфорту для пользователя.

Импортёры же, как было сказано выше, зачастую оставляют уже созданные сайты, которые им удобно использовать и править у себя, чтобы был у всех сайтов единый стандарт, и не всегда этот стандарт подходит под культурные особенности и привычки потенциальных клиентов из нового региона [5].

Суммируя всё вышесказанное, можно говорить о том, что перед автодилерами стоит непростая задача: суметь продвинуть сайт минимальными методами SEO-продвижения, поскольку специалисты ограничены в манёврах. Практически сразу исключаются такие методы как изменение структуры сайта, работа над поведенческими и коммерческими факторами; из небольшого списка оставшихся методов — часть оптимизации, связанной с размерами изображений, наполнение уже имеющегося шаблона максимально интересной и понятной информацией, написание тегов и ключевых слов. Последние три пункта в вопросах сайта автодилера являются решающими: если в первом пункте к изображениям как графического, так и видеоформата у импортёра также могут быть жёсткие требования, то текст, теги и ключевые слова вещь уникальная не только с точки зрения просто языка, на котором они пишутся, но также региона и основной массы целевой аудитории, которая может совершить покупку автомобиля или приехать на сервис. Теги для простого водителя, который покупает легковой автомобиль для себя, и контрагента, который представляет компанию для перевозки грузов и покупает уже грузовой автомобиль, будут совершенно различны, недостаточно будет просто написать в теге название автомобиля и какие-то минимальные его параметры. По аналогии с автопрокатом [6], необходимо учитывать ряд особенностей, которые помогут выделить конкретно эту область и вывести в топы конкретный сайт.

Однако стоит помнить, что варианты запросов могут быть разные и указывать на разные группы тегов, например, «китайский автомобиль джак купить» имеет ключевое слово в значении модели автомобиля, тогда как запрос

«автомобиль джак запчасти купить» может больше отсылаться на группу с запчастями. Чтобы охватывать как можно большую аудиторию потенциальных клиентов и чаще выходить в топах при разного рода запросов, необходимо учитывать не только часто используемые слова для поиска, но и опечатки, некорректный перевод, случаи, когда раскладка не изменена и вместо слова на одном языке получается набор букв для другой. Например, в запросе «автомобиль офс запчасти купить» название марки JAC из-за неправильной раскладки стало набором букв, который также необходимо учесть. Для этого необходимо провести анализ конкурентов и создать топ из десяти наиболее привлекательной и качественно реализованной семантики, то есть, создать хорошее семантическое ядро [7]. Злоупотреблять ключевыми словами ни в коем случае нельзя: переизбыток ключевых слов на сайте может привести к бану на поисковом ресурсе.

Кроме того, нельзя забывать и о таком способе как продвижение в социальных сетях [8]. SEO и социальные сети имеют достаточно неочевидную связь, однако же при этом контент в социальных сетях уже достаточно долгое время учитывается такими крупными поисковиками как Яндекс. Оцениваются лайки, репосты, просмотры постов в группах. Социальные сети весьма удобны: если специалист добавил товар на сайт, то работу нельзя считать законченной, даже если при этом он разместил объявление об этом на главной странице сайта. Очень малое количество людей постоянно обновляет сайт и заходит на него, чтобы проверить новинки. Социальные сети значительно расширяют возможности: не только реклама, но и простое оповещение информационными постами даёт возможность большему числу потенциальных клиентов заинтересоваться новым предложением или моделью автомобиля, что приведёт к переходу по ссылке. Чем больше переходов по ссылке, тем больше это сказывается на его выдаче при поисковых запросах.

На основе вышесказанного можно сделать вывод о том, что SEO-продвижение сайта автодилера действительно является сложной задачей, которая имеет свои особенности и множественные ограничения из-за условий, налагаемых импортёрами, требующей пристального изучения. Основными предполагаемыми методами изучения данной проблемы будут такие методы SEO-продвижения как текстовый контент, семантическое ядро и ссылочная масса.

Список используемых источников:

1. Передерий, Р. Ю. Особенности SEO-продвижения для предприятия / Р. Ю. Передерий // Современные парадигмы развития цифровой экономики в исследованиях молодых ученых : Материалы Международной студенческой научной конференции. В трех частях, Белгород, 17–18 марта 2020 года. – Белгород: Автономная некоммерческая организация высшего образования «Белгородский университет кооперации, экономики и права», 2020. – С. 274-280. – EDN TOEZEW.
2. Голуб, Р. Р. Особенности продвижения туристского продукта / Р. Р. Голуб // Концепции современного образования: новации в системе научного знания : Сборник научных трудов. – Казань : ООО "СитИвент", 2020. – С. 197-201. – EDN BFCORF.
3. Дизайн в разных странах. Как культурные особенности формируют тренды [Электронный ресурс] // vc.ru URL: <https://vc.ru/design/283850-dizayn-v-raznyh-stranah-kak-kulturnye-osobennosti-formiruyut-trendy> (дата обращения: 05.11.2022).

4. Культурные различия в сайтах разных стран [Электронный ресурс] // Varlamoff studio. URL: <https://varnoff-studio.ru/newblogs/web-dizayn/kulturnye-razlichiya-v-saytakh-raznykh-stran/> (дата обращения: 05.11.2022).
5. Особенности продвижения автодилеров [Электронный ресурс] // Автомаркетолог. Профессиональное сообщество. URL: <https://automarketolog.ru/osobennosti-prodvizheniya-avtodilerov/> (дата обращения: 19.10.2022).
6. Лазорская, Д. Д. Особенности SEO-продвижения в сфере автопроката / Д. Д. Лазорская // Студенческая наука: актуальные вопросы, достижения и инновации : сборник статей V Международной научно-практической конференции, Пенза, 12 декабря 2021 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2021. – С. 156-159. – EDN NWRXES.
7. SEO-продвижение сайта автодилера: как превратить сайт в источник клиентов [Электронный ресурс] // impulse.guru. URL: <https://impulse.guru/blog/prodvizhenie-sajta-avtodilera/> (дата обращения: 10.10.2022)
8. Роль социальных сетей в SEO-продвижении сайта [Электронный ресурс] // SEORU. URL: <https://seo.ru/blog/rol-socialnyh-setej-v-seo-prodvizhenii-sajta/> (дата обращения: 03.11.2022).

Patrukhina A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Features of SEO promotion of a car dealer's site.

The article is devoted to the consideration of issues related to increased competition in the field of car sales by official dealers. The current state of the motor vehicle market poses new challenges for the organization of sites, their promotion. It is proposed to focus on SEO-promotion of the site as the most relevant way of promotion in the current realities.

Key words: *SEO, SEO promotion, design, car dealer.*

УДК 004.031.42
ГРНТИ 50.43.17

СИСТЕМА БРОНИРОВАНИЯ РАБОЧИХ МЕСТ КАК ИНСТРУМЕНТ ДЛЯ ОПТИМИЗАЦИИ ОФИСНОГО ПРОСТРАНСТВА

Н. А. Сергеев, Д. И. Нефедов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Оптимизация офисного пространства – одна из болевых точек большинства компаний на прямую связанных с офисной деятельностью. Бизнес нуждается в решении задач, связанных с проектированием. Сфере дизайна необходимо установить равновесие весов, между тенденциями моды, а также производственными показателями компании. Последние несколько лет, на рынке отсутствует фундаментальный подход, к решению данной проблемы. Однако явным кандидатом на занятие этого места, претендует технология HOT-DESCING.

HOT-DESCING, информационные системы и технологии, Web-разработка, оптимизация

В настоящее время, на рынке предложено две основных стратегии по решению проблемы с оптимизацией офисного пространства.

Хотелинг (Hotelling) – решение предлагает сотруднику постоянное рабочее место, однако занимать его он может только в определенное ему время.

Хот-дескинг (HOT-DESCING) – решение предлагает сотруднику свободный офис, не закрепляя его за конкретным рабочим местом. Пример на рис. 1.

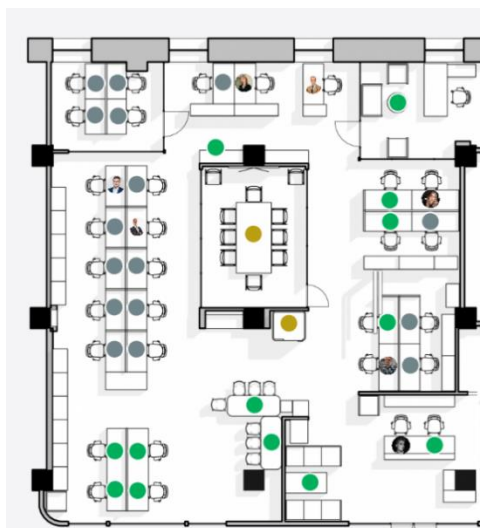


Рис. 1. Hot-Desking

Для ясности картины, необходимо постулировать задачи, которые решают данные стратегии.

Финансовая – при эффективном использовании офисного пространства, появляется возможность избежать затраты на аренду дополнительных офисных помещений.

Удобство – оптимизация существующих пространств создает комфортную среду для эффективного общения и совместной работы, освобождая место для других целей, например, для отдыха сотрудников.

Переход на «внутренний коворкинг» потребует кропотливой работы с отделами кадров и ИТ компании, так как это повлияет не только на то, как работают сотрудники, но и на физическую планировку офиса. Например, большая телевизионная панель может отображать интерактивный план этажа с аватарами сотрудников, чтобы быстро найти нужного человека в постоянно меняющемся их расположении.

Еще одним важным шагом является определение конкретных целей и ключевых показателей эффективности (KPI) для новой системы, будь то производительность сотрудников, экономия средств или другие факторы. Также важно привлекать сотрудников отдела кадров и ИТ к определению этих параметров (рис. 2). Это потому, что он может предоставить ценную информацию как с точки зрения технологий, так и с точки зрения управления персоналом.

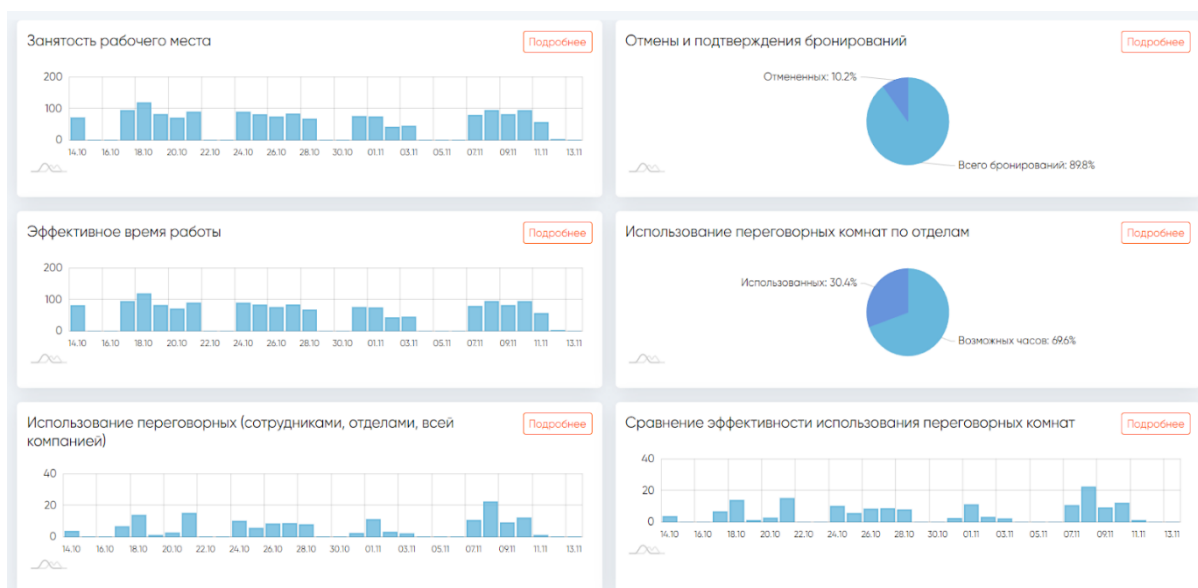


Рис. 2. Статистика

Кроме того, переход на зарезервированные столы требует новой кадровой стратегии. Такой переход невозможен без эффективной CRM-системы, измеряющей эффективность каждого отдельного сотрудника.

Внедрение системы бронирования требует первоначальных инвестиций в программное обеспечение и, возможно, ремонт офиса. Так что независимо от того, перевешивают ли выгоды от более низкой арендной платы или повышения производительности труда стоимость программного обеспечения, нам необходимо трезво смотреть на краткосрочную и долгосрочную отдачу от этих инвестиций.

В компаниях, где 40% или более сотрудников могут эффективно работать удаленно, общепризнано, что системы резервирования вакансий могут повысить

производительность и оптимизировать расходы на аренду. Объективная отчетность позволяет оценить эти результаты и отслеживать движение ресурсов.

Важно отметить система бронирований подойдет не каждому бизнесу, однако данная технология тем не менее заняла свою нишу на рынке решений по оптимизации офисного пространства.

Гибридный формат офиса необходим, когда:

- В компании работают преимущественно мобильные его работники.
- Наш персонал состоит из консультантов, торгового персонала или подрядчиков, которые работают неполный рабочий день в наших офисах.
- Офис имеет гибкую модульную планировку.
- Возможно компания имеет офисы в нескольких городах.
- Вам необходимо сэкономить на аренде, уменьшив площадь сдаваемой в аренду недвижимости.
- Логистика межведомственных рабочих процессов должна быть оптимизирована.
- Вам необходимо привлекать адаптируемых, современных сотрудников, которые ценят баланс между гибкостью и сбалансированностью рабочего времени.



Рис. 3. Рабочее пространство

Преимущества гибридного офиса

Согласно исследованию, Deloitte тенденций человеческого капитала, для трети респондентов баланс между работой и личной жизнью является важным фактором при выборе работы.

Исследование Gallup показало, что сотрудник, способный переключаться между разными работами, был в 1,3 раза более вовлеченным, чем другие сотрудники. Вовлеченность оказывает огромное влияние на увеличение прибыли компании.

Гибридный формат повышает эффективность работы по поставленным задачам и позволяет сотрудникам добиться максимальной производительности.

Использование системы бронирования вакансий показывает потенциальным сотрудникам, что ваша компания ценит их время и доверяет вам. Эта стратегия позволяет нам привлекать самые ценные, креативные и креативные таланты в штаты, где борются лидирующие на рынке HR-отделы.

Инвестирование в решение для резервирования мест — отличный способ сократить лишние офисные площади, мебель и ИТ-оборудование. Сэкономленные деньги можно инвестировать в дальнейшее развитие бизнеса.

Список используемых источников:

1. Алексеев А.. Введение в Web-дизайн. Учебное пособие. — М.: ДМК Пресс, 2019. — 184 с.
2. Что такое хот-деск?: IPG company [Электронный ресурс]. URL: <https://ipg-estate.ru/blog/что-такое-hot-desk-kakie-tehnologii-neobhodimy-dlia-bystrogo-i-nedorogo-vnedreniia-sistem-vremennyh-rabochih-mest> (дата обращения 14.11.2022).
3. Гарретт Д. Веб-дизайн. Элементы опыта взаимодействия / Д. Гарретт. — СПб.: Символ-плюс, 2015. — 192 с.
4. Мартишин, С.А. Проектирование и реализация баз данных в СУБД MySQL с использованием MySQL Workbench: Методы и средства проектирования информационных систем и техноло / С.А. Мартишин, В.Л. Симонов, М.В. Храпченко. - М.: Форум, 2018. - 61 с.
5. Техническая документация серверного языка программирования: Php manual [Электронный ресурс]. <https://www.php.net/manual/ru/index.php> (дата обращения 14.11.2022).
6. Техническая документация фреймворка CodeIgniter: CodeIgniter4 User Guide [Электронный ресурс]. https://www.codeigniter.com/user_guide/index.html (дата обращения 14.11.2022).
7. Дакетт Д. HTML и CSS. Разработка и дизайн веб-сайтов. — М.: Эксмо, 2019. — 480 с.

Sergeev N., Nefedov D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

The workplace reservation system as a tool for optimizing office space.

Office space optimization is one of the pain points of most companies directly related to office activities. Business needs to solve problems related to design. The design industry needs to balance the scales between fashion trends as well as company performance. Over the past few years, the market lacks a fundamental approach to solving this problem. However, HOT-DESCING technology claims to be a clear candidate for this place.

Key words: *HOT-DESCING, information systems and technologies, Web-development, optimization.*

УДК 004.921
ГРНТИ 28.17.33

ЦИФРОВАЯ МЕТАВСЕЛЕННАЯ, ВОЗМОЖНОСТИ ЕЕ ПРИМЕНЕНИЯ В СФЕРЕ ОБРАЗОВАНИЯ

Д. В. Сметюх, А. А. Шиян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Технологии виртуальной и дополненной реальности уже сейчас имеют активное применение в различных сферах. Благодаря таким гигантам, как Microsoft, Facebook, Google, эти технологии могут сделать значимый шаг на пути создания цифровой вселенной – метавселенной. В данной статье дано определение понятию метавселенная, рассмотрены преимущества данной среды виртуальной реальности. Изучены возможности применения метавселенной для образования и приведены существующие решения в сфере образования.

метавселенная, виртуальный миры, образование, виртуальная реальность, metaverse, virtusl words, education, augmented reality, virtual reality

С точки зрения конечных пользователей на текущий момент можно выделить три волны технологических инноваций: персональные компьютеры, интернет и мобильные устройства. Четвертой волной являются такие технологии как виртуальная (VR) и дополненная реальность (AR). Ожидается, что именно эти технологии станут началом развития полноценной метавселенной [3]. Цель данной работы заключается в рассмотрении текущего состояния развития метавселенной, изучение преимуществ и возможностей интеграции в виртуальную среду образовательного контента.

Метавселенная — это вселенная постреальности, вечная и постоянная многопользовательская среда, объединяющая физическую реальность с цифровой. Она основана на конвергенции технологий, которые обеспечивают мультисенсорное взаимодействие с виртуальными средами, цифровыми объектами и людьми, такими как VR и AR [1].

В октябре 2021 года компания Facebook сообщила о своем ребрендинге и изменила свое название на «Meta» и рассказала о своем видение будущего метавселенной (рис. 1). С тех пор крупные IT-гиганты по всему миру постепенно предпринимают попытки воплотить эту концепцию в реальность.


 Рис. 1. Метавселенная Facebook¹

Концепций метавселенной много, но самой известной является концепция венчурного инвестора Мэтью Болла. Мэтью Болл с 2015 года активно ведет блог в котором публикуют свои эссе с размышлениями о будущих технологиях. К его мнению прислушиваются крупные технологические гиганты, такие как Epic Games [4].

Мэтью Болл выделил семь характеристик метавселенной:

1. Метавселенная не может остановиться, перезагрузиться, она должна быть постоянной
2. Должна существовать синхронно и в реальном времени для всех
3. Метавселенная не должна быть ограничена на количество одновременных пользователей - каждый может стать частью метавселенной.
4. В виртуальном мире должна существовать собственная полностью функционирующая экономика. Пользователи могут не только покупать цифровые продукты, но и зарабатывать. Что еще более важно, пользователи могут владеть собственной цифровой собственностью и управлять ею, а технологии безопасности, такие как блокчейн, могут гарантировать безопасность и отслеживаемость их личной собственности.
5. Метавселенная включает в себя элементы реального мира, например пользователь может работать на своем компьютере внутри виртуальной среды.
6. Предоставить полную совместимость данных. Например, купленный цифровой продукт или контент в одной виртуальной среде, будет также доступен в другой.
7. Должна быть открытой для создания различного авторского контента. Пользователи могут создавать практически все, что только могут себе представить.

Метавселенную можно определить как трехмерное цифровое пространство, смешанное с реальным и виртуальным мирами, которое преодолевает множество ограничений физического мира, таких как время и местоположение пользователя. Это позволяет пользователям участвовать в различных видах деятельности, например, работать, учиться, тренироваться, социализироваться

¹ Запрещенная социальная сеть в РФ

через аватары и взаимодействовать с другими игроками и виртуальными объектами, а также предоставляет пользователям возможности редактировать содержимое.

На наш взгляд образование является одним из наиболее значимых перспектив применения метавселенной в ближайшем будущем. Метавселенная может быть использована в качестве новой образовательной среды. С помощью технологии VR обучение может стать более интерактивным и интересным, с его помощью можно визуализировать разные процессы и модели, которые не всегда можно получить с помощью стандартных средств. Также технология может быть полезна в рамках дистанционного образования, когда нет возможности напрямую взаимодействовать с необходимыми инструментами, например, с лабораторными установками.

В 2022 году технологии метавселенной начали более активно внедряться в сферу образования. В августе этого года во Флориде, США начал работу Optima Classical Academy — первая в мире школа, «построенная» в метавселенной. Это бесплатное общеобразовательное учебное заведение на 1300 мест для учеников 3-8-х классов. По задумке основателей школы, обучение в ней поможет немотивированным и слабо социализированным ребятам преодолеть себя и наконец-то увлечься учебой. Всем ученикам школа предоставляет VR-оборудование и оказывает техническую поддержку на протяжении всего обучения. Надевая VR-очки, дети могут посещать занятия в виртуальной школе, не выходя из дома. В расписании учеников начальной школы (3-5 класс) значатся математика, английский, история, наука, музыка, искусство и латинский язык. В средней школе в учебном плане появляется грамматика и физкультура, которой дети будут заниматься во внеурочное время [5].

Виртуальной лаборатории для изучения физических явлений, ее интеграции в метавселенную упростит понимание многих физических явлений и концепций, которые по-прежнему являются сложными для многих студентов и школьников (рис. 2). Технологии метавселенной и VR позволят повысить интерес к изучаемым наукам и улучшить усвояемость предмета. В виртуальной среде с помощью технологий моделирования могут быть смоделированы различные реалистичные сцены для обучения. Перенос классических инструментов для изучения физики, таких как лабораторные установки, в метавселенную позволит избавиться от реальных, которые часто требуют обслуживания и обновления. В данной среде могут быть созданы виртуальные агенты с разными ролями, которые могут сопровождать обучающегося и направлять его (например, рассказывать теоретический материал). В этом смысле предоставление этих интеллектуальных агентов может в значительной степени удовлетворить индивидуальные потребности и улучшить взаимодействие как для учащихся, так и для преподавателей.

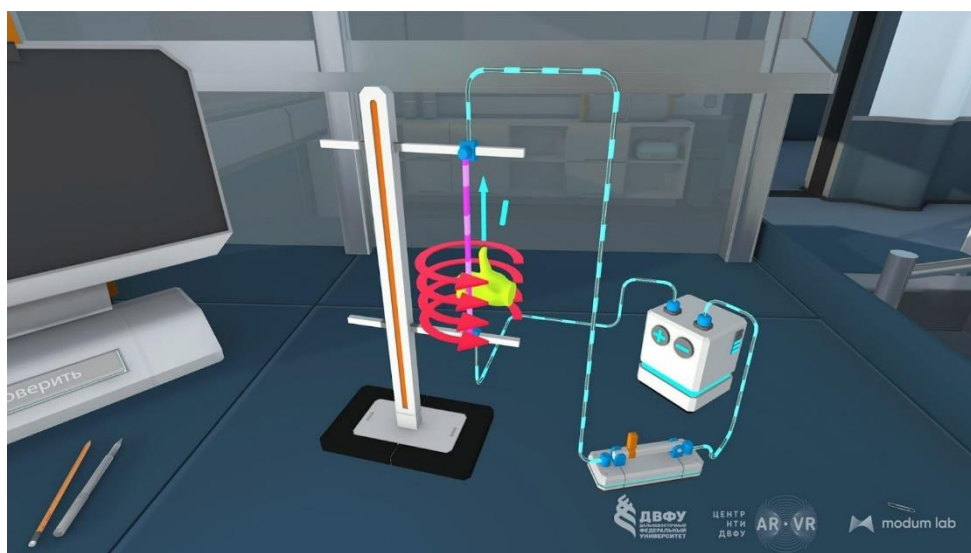


Рис. 2. Виртуальная лаборатория

Развитие VR технологии за последние годы позволило сделать виртуальный опыт более комфортный для пользователей. Так в одном из ведущих шлемов виртуальной реальности Oculus Quest 2 с программным обновлением появилась возможность отслеживание рук (рис. 1) без дополнительных устройств (контроллеров). Данная технология открывает новые возможности для взаимодействия с виртуальными объектами, что в свою очередь позволит обучающимся испытать более реальный опыт в виртуальной лаборатории.

Таким образом, развивающаяся метавселенная становится одним из востребованных направлений в образовании. Образование в метавселенной станет совершенно новой концепцией обучения по сравнению с существующими образовательными технологиями. Помимо повышения вовлеченности в обучение и лучшему пониманию материалов, образование в метавселенной решает ряд проблем и ограничений благодаря возможности дистанционных занятий.

Список используемых источников:

1. Stylianos Mystakidis, Ahmad Taher Azar and Raffaele Barretta. Metaverse. Материалы: School of Natural Sciences, University of Patras, February 2022
2. Xinli Zhang , Yuchen Chen , Lailin Hu and Youmei Wang. The metaverse in education: Definition, framework, features, potential applications, challenges, and future research topics. College of Education, Wenzhou University, Wenzhou, China, October 2022
3. Immersive experience—The 4th wave in tech: Learning the ropes [Электронный ресурс]. // [accenture.com](https://www.accenture.com/gb-en/blogs/blogs-immersive-experience-wave-learning-ropes). URL: www.accenture.com/gb-en/blogs/blogs-immersive-experience-wave-learning-ropes (Дата обращения 05.11.2022)
4. The Metaverse: What It Is, Where to Find it, and Who Will Build It [Электронный ресурс]. // [www.matthewball.vc](https://www.matthewball.vc/all/themetaverse) URL: www.matthewball.vc/all/themetaverse (Дата обращения 05.11.2022)
5. Будущее уже здесь? Как выглядит образование в метавселенной [Электронный ресурс]. // [pedsovet.org](https://pedsovet.org/article/budusee-uzhe-zdes-kak-vygladit-obrazovanie-v-metavselelnoj?ysclid=lagi2ep21p272615811) URL: <https://pedsovet.org/article/budusee-uzhe-zdes-kak-vygladit-obrazovanie-v-metavselelnoj?ysclid=lagi2ep21p272615811> (Дата обращения 05.11.2022)

Smetyukh D., Shiyan A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Digital metaverse, the possibilities of its application in the field of education.

Virtual and augmented reality technologies are already actively used in various fields. Thanks to such giants as Microsoft, Facebook, Google, these technologies can make a significant step towards creating a digital universe – a metaverse. This article defines the concept of the metaverse, discusses the advantages of this virtual reality environment. The possibilities of using the metaverse for education are studied and existing solutions in the field of education are presented.

Key words: metaverse, virtual worlds, education, virtual reality, metaverse, virtual work, education, augmented reality, virtual reality.

УДК 004.89
ГРНТИ 28.23.37

АНАЛИЗ ПЕРСПЕКТИВ ПРИМЕНЕНИЯ ИЗОБРАЖЕНИЙ СГЕНЕРИРОВАННЫХ ПОСРЕДСТВОМ НЕЙРОСЕТИ STABLE DIFFUSION ПРИ ФОРМИРОВАНИИ ЛИЧНОГО БРЕНДА

Г. А. Урванцев, Д. В. Волошинов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящей статье рассматриваются возможности синтеза графических изображений с использованием генеративной нейронной сети Stable Diffusion. В качестве модели для синтеза используется Stable Diffusion v1.4, изменённая алгоритмом Dreambooth. Рассмотренный метод может использоваться для синтеза высокоточных изображений или фотографий любого человека в различных контекстах и ситуациях.

медиаконтент, современные технологии, нейронные сети, машинное обучение, Stable Diffusion, DreamBooth

В современном постиндустриальном обществе преобладающей отраслью является сфера услуг и развлечений, к которым в том числе относится производство видеоконтента, блогинг и другое. Для привлечения большего внимания к продукту, блогеры используют различные методы, один из которых – формирование личного бренда.

Например, видео на сервисе *youtube.com* сопровождаются изображением-превью, привлекающим внимание и известные медийные личности используют на превью свой образ – так пользователи в общем списке опубликованных видео сразу отличают видео конкретного автора и изначально причисляют материалу качества присущие предыдущим его работам. Более интересные превью привлекают больше внимания [1], но требуют также большее время на создание, а также оплату работы дизайнеров или художников.

Облегчить процесс создания необычных стилизованных изображений на основе изображений конкретного человека могут технологии генерации изображений на основе нейронных сетей. Существующие технологии уже достигли достаточно высокого уровня синтеза изображений по текстовому запросу [2]. Основные представители генеративных нейросетей, доступных широкому кругу пользователей являются *MidJourney*, *DALL-E* и *Stable Diffusion*.

По качеству генерируемых изображений и доступности *DALL-E* и *MidJourney* превосходят *Stable Diffusion*, благодаря использованию более качественных исходных натренированных моделей “изображение-текст”, однако они имеют ограничение по количеству бесплатно синтезированных изображений, а возможности создавать изображения по исходным образам объектов не обладают высокой точностью. Общие черты объекта в процессе сохраняются, однако происходит сильное искажение ключевых особенностей, например черт лица или иных особенностей внешности, что неприемлемо в данной ситуации.

В свою очередь, *Stable Diffusion* обладает открытым исходным кодом и широким спектром настраиваемых параметров, которые позволяют вмешиваться в процесс синтеза изображений для получения различных результатов. Исключительной особенностью данного продукта является возможность использовать для синтеза изображений нестандартные модели, тогда как её конкуренты имеют фиксированную предустановленную модель.

Эта особенность позволяет решить описанную выше проблему, используя нестандартную модель. Получить такую модель можно, например, обработав стандартную модель *Stable Diffusion* алгоритмом *Dreambooth* [3], разработанным компанией *Google*. Алгоритм встраивает в существующую натренированную модель новые объекты, используя всего несколько исходных изображений. Созданная “уточнённая” модель позволяет синтезировать их в различных контекстах с сохранением высокой точности ключевых черт.

В качестве примера, можно рассмотреть возможности синтеза изображения будильника, представленный разработчиками алгоритма. Изображение было синтезировано методом “текст в изображение” на стандартной и уточнённой моделях *Imagen*, а также *DALL-E2*, с использованием синтеза “изображения из изображения” и стандартной модели.

Как показывают результаты (рис. 1), метод синтеза “изображение из изображения” искажает исходный объект, а также не позволяет изменить контекст, а стандартная модель *Imagen* не обладает достаточной точностью повторения исходного объекта.



Рис. 1. Пример применения алгоритма *Dreambooth*

В свою очередь, изображения синтезированные после уточнения *Imagen* алгоритмом *Dreambooth* на основе трёх изображений объекта, сохраняют высокую точность и возможность изменения контекста изображения, недоступную при синтезе “изображения из изображения”. Кроме того, важно отметить, что в хорошем качестве были воспроизведены числа на циферблате. Из-за обилия исходных данных, существующие модели могут сильно исказить любые символичные конструкции. Данный недостаток был устранён после уточнения модели, но только в рамках исходного объекта.

Для проверки точности работы алгоритма была создана модифицированная версия модели «*stable-diffusion-v1-4*», с внедрением объекта-мужчины (рис. 2)

при помощи алгоритма *Dreambooth*. Новому объекту был присвоен текстовый идентификатор “*george_Urv*”.



Рис. 2. Исходные изображения

В результате, даже такого малого количества изображений оказалось достаточно, чтобы нейросеть могла синтезировать исходный объект (рис. 3) с высокой точностью черт лица. Был использован текстовый запрос “*Portrait of teenager [, george_Urv looking left sight,] with red hair and with cute face, blue background, perfect composition, hyperrealistic, super detailed, 8k, high quality, trending art, trending on artstation, sharp focus, studio photo, intricate details, highly detailed, by greg rutkowski*”.

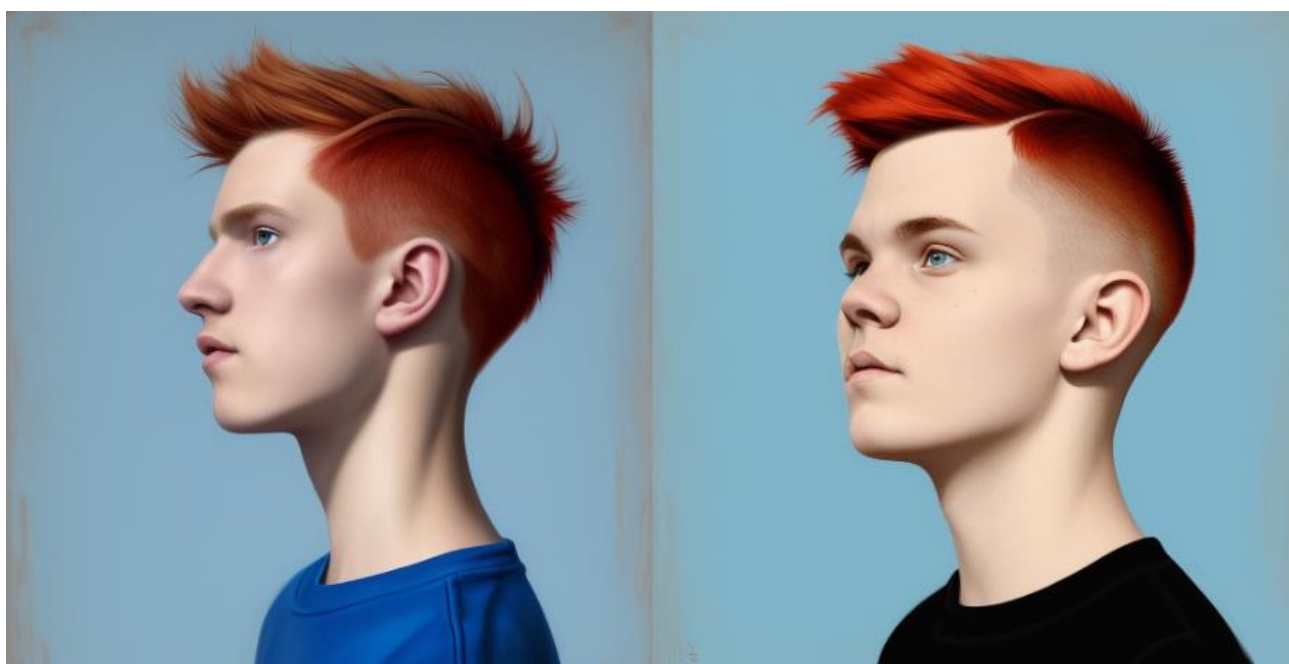


Рис. 3. Пример синтеза изображений на обычной и уточнённой модели

На рис. 4 представлено больше вариантов синтезированных изображений с различными текстовыми запросами.



Рис. 4. Примеры синтезированных изображений с идентификатором “george_Urv” в различных контекстах

Так или иначе, сгенерированные изображения несовершенны. Отличительными чертами и аксессуарами, присутствующими на исходных изображениях (например: цепочка на шее, изображения на одежде, родимые пятна и прочее), искажают результат. Алгоритм *Dreambooth* обладает возможностью настройки процесса внедрения объектов, что может позволить создавать более точные результаты, однако, данная гипотеза требует дальнейших исследований.

Технологии генеративных нейронных сетей в настоящий момент уже практически приблизились по качеству к фотореалистичным результатам в случае синтеза фотографий и близких к качеству графических произведений созданных человеком, в случае синтеза изображений. Технология *Dreambooth* позволяет дополнительно изменить функционал существующих генеративных моделей для конкретных целей, причём не только добавляя объекты-людей, но также и прочие уникальные объекты, однако возможности их применения требуют дополнительных исследований.

Список используемых источников:

1. Нестеренко Н. Ю. Особенности продвижения компании при помощи YouTube // Вестник науки и образования. 2019. N 11-1 (65). С. 62-64.
2. Rombach R., Blattmann A., Lorenz D., Esser P., Ommer B., High-Resolution Image Synthesis with Latent Diffusion Models [Электронный ресурс] // arXiv.org. 2022. Дата обновления: 13.04.2022. URL: <https://arxiv.org/abs/2112.10752> (дата обращения: 11.11.2022).
3. Ruiz N., Li Y., Jampani V., Pritch Y., Rubinstein M., Aberman K., DreamBooth: Fine Tuning Text-to-Image Diffusion Models for Subject-Driven Generation [Электронный ресурс] // arXiv.org. 2022. Дата обновления: 25.08.2022. URL: <https://arxiv.org/abs/2208.12242> (дата обращения: 11.11.2022).

Voloshinov D.V., Urvantsev G.A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Perspectives analysis of application the images generated by neural network in the formation of a personal brand.

This article reviews the possibilities of graphic image synthesis using the generative neural network Stable Diffusion. Stable Diffusion v1.4, modified by the Dreambooth algorithm, is used as the model for synthesis. The considered method can be used to synthesize high-precision images or photos of any person in different contexts and situations.

Key words: media content, modern technologies, neural networks, machine learning, stable diffusion, DreamBooth.

УДК 004.946
ГРНТИ 28.17.33

АЛГОРИТМИЧЕСКИЙ КОМПЛЕКС ДЛЯ РЕШЕНИЯ ЗАДАЧ ПРОЕКТИРОВАНИЯ ИНТЕРФЕЙСОВ ДЛЯ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ В ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ НА ОСНОВЕ ГЕОМЕТРИЧЕСКОГО МОДЕЛИРОВАНИЯ

С. Ченарани

Санкт-Петербургский политехнический университет Петра Великого

Одной из самых больших проблем, с которыми сталкивается система образования в 21 веке, является отсутствие визуализации контента в книгах и других источниках образования. Студент не может полностью погрузиться в информацию, которую он получает в процессе обучения.

иммерсивность, виртуальная реальность, интерфейс, геометрическое моделирование, приложение

Развитие технологий виртуальной реальности (VR) в последнее десятилетие вызвало значительный интерес к данной области среди простых потребителей. Всего за несколько лет количество научных статей на эту тему значительно увеличилось. В некоторых предлагается использовать виртуальную реальность в качестве конечной среды для обучения. Тем не менее, отсутствие способа получения исследований и противоречивые предварительные данные указывают на то, что мы все еще очень мало знаем о том, как происходит обучение в виртуальной реальности.

Актуальность этого исследования заключается в плане изучения взаимосвязи между обучением и иммерсивными виртуальными технологиями, чтобы определить пути разработки более эффективных инструментов виртуального обучения.

1. Технологии виртуальной реальности (VR)

Пользователь всегда ищет более интересный способ взаимодействия со своим устройством. Вместо того чтобы просто смотреть видео на мониторе, они хотят войти в виртуальный мир и взаимодействовать с ним. Эта технология, которая становится все более популярной в текущем десятилетии, называется виртуальной реальностью (VR).



Рис. 1. Использование стекла виртуальной реальности

Было проведено исследование иммерсивности интеллектуального интерфейса симбиотической системы управления удаленными динамическими объектами, использующими технологии виртуальной реальности, с целью получения более глубоких знаний о характеристиках погружения и взаимодействия с виртуальным миром. Точно так же, как наушники могут быть сконструированы так [2], чтобы блокировать посторонние звуки, очки виртуальной реальности могут либо пропускать свет, либо полностью заменять ваше зрение. На момент написания этой статьи полная замена зрения называется виртуальной реальностью (VR) [1].

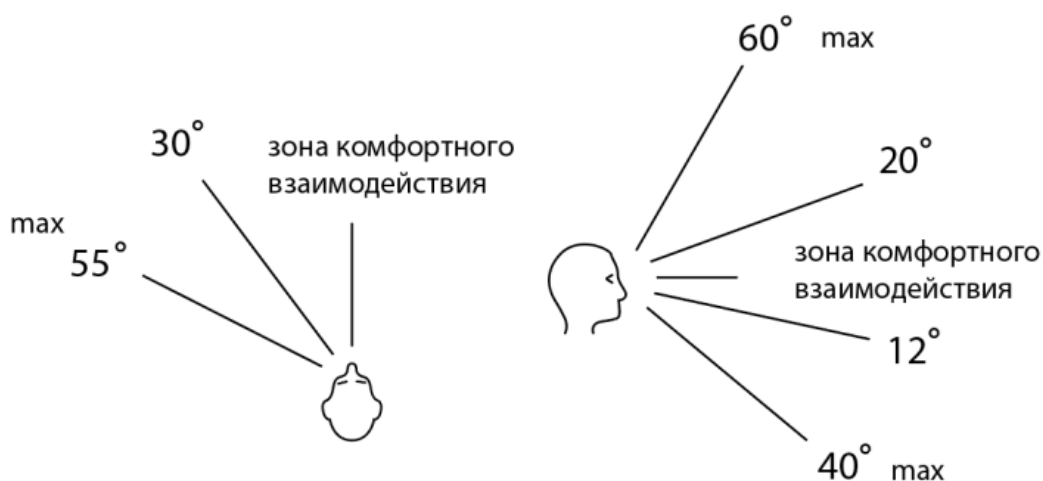


Рис. 2. Зона комфортного взаимодействия с интерфейсом

2. Методы геометрического моделирования

Исследование предполагает использование методов геометрического моделирования для открытия новых форм и нового расположения сложных поверхностей. Кроме того, в области геометрического моделирования также

предложен метод разработки интерактивного и удобного для пользователя интерфейса. Это сократит время, затрачиваемое на изучение интерфейса, и позволит пользователю больше сосредоточиться на важной информации.

В результате этого исследования предполагается создать алгоритм для использования геометрического моделирования и генеративных концепций дизайна при создании образовательного контента с использованием технологий виртуальной реальности.

Для достижения поставленной цели следует решить следующие задачи:

- Проанализировать варианты объединить знания из области человеческого познания, психологии и поведенческих идей, чтобы понять эффективность обучения в виртуальной реальности
- Обозначить основные факторы, определяющие разработку приложений виртуальной реальности, которые улучшают обучение и тренинг.
- Разработать дизайн и расположение виртуальной учебной среды.
- Разработать автоматизированные инструменты геометрического моделирования для проектирования интерфейсов управления настройками учебной среды.

Список используемых источников:

1. Бычков В. В., Маньковская Н.Б. Виртуальная реальность как феномен современного искусства // Эстетика: Вчера. Сегодня. Всегда. Вып. 2 – М.: ИФ РАН, 2006 – С. 32.
2. Ченарани, С., & Шур, С. Ю. (2021). ИССЛЕДОВАНИЕ УСЛОВИЙ ИММЕРСИВНОСТИ ИНТЕЛЛЕКТУАЛЬНОГО ИНТЕРФЕЙСА СИМБИОТИЧЕСКОЙ СИСТЕМЫ С ПРИМЕНЕНИЕМ VR ТЕХНОЛОГИЙ. In Неделя науки ИСИ (pp. 331-333).

Chenarani Sasan

Peter the Great St. Petersburg Polytechnic University

Algorithmic complex for solving design problems interfaces for the educational environment in virtual reality based on geometric modeling.

One of the biggest problems facing the education system in the 21st century is the lack of visualization of content in books and other sources of education. The student cannot fully immerse himself in the information that he receives in the learning process.

Key words: immersiveness, virtual reality, interface, geometric modeling, application.

УДК 778.2
ГРНТИ 60.33.15

МЕТОДЫ ВИЗУАЛИЗАЦИИ ТРЁХМЕРНЫХ ОБЪЕКТОВ В ПРОСТРАНСТВЕ И ПЕРСПЕКТИВЫ ИХ ПРИМЕНЕНИЯ В ХУДОЖЕСТВЕННОМ ОБРАЗОВАНИИ

А. Д. Щербатюк

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье описываются технологии в области визуализации трехмерных объектов в пространстве. Рассматривается понятие голограммы и существующие решения в данной сфере. Целью работы является оценка возможностей и перспектив использования голографических технологий в художественном образовании.

голограмма, художественное образование, визуализация

Современные технологии создают множество новых возможностей для модернизации процесса получения образования в сфере изобразительного искусства. Среди существующих решений популярность набирают виртуальная (VR) и дополненная (AR) реальность. VR обеспечивает визуализацию среды и полное погружение в неё, AR добавляет в окружающее человека пространство мнимые объекты, воспринимаемые как элементы реального мира [1]. Данные технологии имеют значительный потенциал как средства виртуальной визуализации объектов и/или окружения для практики рисования с натуры. Они также могут выступать в качестве способа представления, например, материала для изучения анатомии в виде интерактивной трёхмерной модели человеческого тела. Достоинствами виртуальной и дополненной реальностей является качественная визуализация и иммерсивность, то есть эффект погружения в пространство и взаимодействия с объектами в нём. Однако обе технологии предусматривают использование специальных очков, смартфонов или планшетов, которые могут привести к чувству дискомфорта при длительной эксплуатации.

Альтернативным вариантом технологии для использования в сфере художественного образования может являться голография. Под голографией понимают, с одной стороны, метод получения трехмерного образа объекта, позволяющий в дальнейшем восстанавливать его облик, с другой – метод объемной визуализации, достигшей в своем развитии хорошего уровня точности и качества. Голограмма как продукт голографии должна хранить в себе информацию, достаточную для того, чтобы восстановить виды модели с разных ракурсов из некоторой ограниченной области просмотра.

Развитие компьютерной техники и информационных технологий породило множество технологий получения объемных изображений в пространстве:

Голографический проектор. Имеет вид вентилятора, в лопасти которого встроены светодиоды. Получение голографического изображения основывается на синхронизации вспышек светодиодов с частотой вращения. Благодаря

тонкости лопастей вентилятора и высокой скорости их вращения, вращение не заметно глазу. Кроме того, очень быстрые вспышки светодиодов формируют изображение, сглаживаясь из-за специфики человеческого зрения [2]. Данная технология получила широкое распространение. Голографические вентиляторы, вращаясь, способны воспроизводить как статичную картинку, так и видео файлы во множестве форматов (JPG, GIF, MP4, AVI). Размер получаемого изображения может достигать 1 метра в диаметре, а разрешение доходит до значений в 1920*1920 dpi.

Голографический проекционный экран. Представляет собой полностью прозрачный отрезок из оргстекла, на который нанесена пленка обратной проекции невидимая человеческому глазу. Данная технология способна также воспроизводить видеоролики. Достоинством такого экрана может являться размер проецируемого изображения и его качество. Снабженный дополнительным сенсорным слоем, проекционный экран может обеспечивать дополнительную функцию - обратную связь с пользователем [3].

У этих двух видов голограммы есть один общий недостаток — это маленький угол обзора. Так как изображение, по сути, плоское и объем его иллюзорен, если смотреть на него под большим углом, то вся иллюзия пропадает.

Конструкция 3D пирамиды. Технически простой и понятный порядок проецирования изображения на основе законов физики, который был придуман ещё в XVI веке. Пирамида представляет собой поверхность, на которую проецируется изображение с экрана устройства [2]. При этом, современные модификации пирамиды таковы, что на каждую сторону фигуры можно передать конкретную область изображаемого предмета, и это позволяет рассмотреть его со всех сторон.

Трёхмерный дисплей, основанный на звуковой левитации. Суть технологии заключается в использовании ультразвуковых волн для организации движения маленьких шариков в пространстве. С помощью потока света, падающего на летающие по заданной траектории объекты, создаётся трёхмерное изображение. Дисплей на основе акустической левитации, по мнению его разработчиков, имеет потенциал для добавления тактильного отклика.

Волномерический дисплей. Имеет схожий принцип действия с предыдущей описанной технологией. В данном случае поверхностью для проекции является быстро вращающаяся поверхность [4]. Такие дисплеи в целях безопасности закрыты прозрачным куполом, поэтому взаимодействовать с голограммой можно лишь при помощи дополнительных устройств.

Гаптоклон. Наиболее приближённая к фантастике технология. Позволяет создавать осязаемые тактильные голограммы с помощью лазеров сверхкоротких импульсов. За счёт возбуждения атомов кислорода и азота фокусированными лучами происходит образование крайне маленьких облаков плазмы. Голографическое изображение образуется из множества последовательных вспышек, которые происходят достаточно высокой скоростью, чтобы в глазах человека сливаться в единое изображение. По изменению формы можно

отслеживать касания пальцами и на этой основе строить взаимодействие. Другой способ – использование ультразвука в качестве средства для имитации силы давления от соприкосновения рук с голограммой [5].

Рассматривая применение голографических проекций в сфере художественного образования, можно выделить два основных критерия, которым должна соответствовать картинка, созданная той или иной технологией:

- Точность изображения. В области изобразительного искусства качество визуализации имеет большое значение.
- Многокурность. Это свойство голограммы, когда положению глаз наблюдателя соответствует свой ракурс, благодаря чему обеспечивается возможность наблюдения объекта под разными углами.
- Возможность взаимодействия. Наличие способов влияния на изучаемый объект является важным фактором в построении процесса обучения с применением технологий визуализации в пространстве. Например, возможность двигать части тела трехмерной модели человека повысит эффективность изучения пластической анатомии.

В соответствии с критерием многокурности, для применения в художественном образовании не подходят такие технологии, как голографический проектор и проекционный экран, так как они создают плоское изображение, которое кажется трехмерным из-за оптической иллюзии.

Создание голограммы с помощью 3D пирамиды позволяет рассмотреть объект с разных сторон. Однако эта технология тоже основана на иллюзии. Транслируемый объект по сути является специально подготовленным статичным изображением или видеорядом, с ним невозможно полноценно взаимодействовать.

Волюметрические дисплеи имеют хорошее качество картинки, позволяют просмотр с любого ракурса, а также дают возможность взаимодействия с помощью сторонних приборов. Поэтому данная технология является перспективной с точки зрения её использования в художественном образовании.

Трёхмерные дисплеи на основе акустической левитации и технология гаптоклона имеют одно большое преимущество над другими описанными методами визуализации. Их отличие заключается в возможности реализации взаимодействия через прямое прикосновение с проекции. Это делает данные технологии наиболее интересными и многообещающими.

Наиболее перспективным методом визуализации трехмерных изображений можно назвать гаптоклон, поскольку в данном случае проецирование изображения происходит прямо в воздухе, что говорит о потенциальном отсутствии ограничений, связанных с размерами дисплеев, чего нельзя сказать о технологии акустической левитации. На данный момент размер получаемого изображения достаточно мал, однако с развитием данной технологии возможно увеличение создаваемых проекций.

Таким образом, в рамках статьи описаны существующие технологии визуализации трехмерных объектов в пространстве. На основе проведённого

анализа перспектив использования данных технологий в сфере художественного образования, можно сделать вывод о том, что текущая стадия развития голограмм не отвечает всем требованиям, предъявляемым к голографической проекции в качестве способа изучения тех или иных аспектов изобразительного искусства. Наиболее продвинутыми решениями являются гаптоклон и дисплей на основе акустической левитации. Данные технологии нуждаются в расширении возможностей взаимодействия с человеком и в увеличении размера получаемой проекции. Однако, уже на данном этапе можно заметить перспективность использования голограмм в процессе художественного образования, что делает актуальным рассмотрение вопроса об их дальнейшем развитии и применении.

Список используемых источников:

1. Бутов, Р. А. Технологии виртуальной и дополненной реальности для образования / Р. А. Бутов, И. С. Григорьев // Про-ДОД. – 2018. – № 1(13). – С. 18-29. – EDN UUPYAA.
2. Ечмаева, Г. А. Анализ современных технологий получения пространственных объемных изображений / Г. А. Ечмаева, И. Т. Ахундова // Наука. Исследования. Практика : Сборник избранных статей по материалам Международной научной конференции, Санкт-Петербург, 25 декабря 2019 года. Том Часть 1. – Санкт-Петербург: Частное научно-образовательное учреждение дополнительного профессионального образования Гуманитарный национальный исследовательский институт «НАЦРАЗВИТИЕ», 2020. – С. 67-69. – EDN KKQEXH.
3. Голографический проекционный экран. Штука дня: футуристичный голографический дисплей с трёхмерной графикой. Дополнительные опции голографических экранов [Электронный ресурс] URL: <https://sukachoff.ru/virusy/golograficheskii-proekcionnyi-ekran-shtuka-dnya-futuristichnyi/> (дата обращения 12.11.2022)
4. Никитюк О. Голограммы: из чего выбрать и как использовать [Электронный ресурс] // Информационный портал event-индустрии. URL: <https://event.ru/instruments/gologrammyi-iz-chego-vyibrat-i-kak-ispolzovat/> (дата обращения 13.11.2022)
5. Ильина, И. В. Голограммы: от истоков к будущему / И. В. Ильина, К. А. Моисеева, И. А. Проворных // Инновационный дискурс развития современной науки и технологий : Сборник статей III Международной научно-практической конференции, Петрозаводск, 23 декабря 2021 года. – Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская И.И.), 2021. – С. 218-223. – EDN AAFFRH.

Shcherbatyuk A.D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Methods Of Visualization Of Three-Dimensional Objects In Space And Prospects Of Their Application In Art Education.

The article describes technologies in the field of visualization of three-dimensional objects in space. The concept of hologram and existing solutions in this area are considered. The aim of the work is to evaluate the possibilities and prospects of using holographic technologies in art education.

Key words: hologram, art education, visualization.

УДК 004.946
ГРНТИ 28.17.33

ПРОЕКТИРОВАНИЕ ОБЪЕКТОВ ГЕНЕРАТИВНОГО ДИЗАЙНА НА ОСНОВЕ ГЕОМЕТРИЧЕСКОГО МОДЕЛИРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ РАСШИРЕННОЙ РЕАЛЬНОСТИ

С. Ю. Щур¹, Д. В. Волошинов²,

¹ Санкт-Петербургский политехнический университет Петра Великого

² Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Процесс проектирования с каждым годом усложняется. Появляются новые входные данные, методы проектирования, технологии. Однако интервал между выпуском изделий становится все короче. Изделия выпускаются и обновляются значительно чаще. Однако несмотря на интенсификацию процесса разработки, автоматизацию систем 3-х мерного моделирования и увеличение рынка труда для специалистов подобной отрасли, заметна тенденция к копированию основополагающих элементов изделий с незначительными изменениями и доработками. Ассортимент продукции изобилует повторяющимися изделиями, а разработчики избегают принципиально новых решений.

генеративный дизайн, геометрическое моделирование, расширенная реальность, XR

Актуальность данного исследования заключается в поиске нового подхода к проектированию объектов промышленного дизайна через использование методов геометрического моделирования с применением технологий расширенной реальности.

Даже у самых опытных дизайнеров их интуиция может быть ограничена, когда они вручную исследуют такое беспрецедентно большое дизайнерское пространство. Чтобы расширить возможности дизайнеров, разрабатываются компьютерные алгоритмы для создания желаемых проектов в соответствии с заданными целями проектирования и ограничениями. Такой процесс проектирования, основанный на алгоритмах, теперь известен как генеративный дизайн. Примеры подходов варьируются от оптимизации формы и топологии до определения формы на основе машинного обучения. [1]

Существует ряд ПО, использующих современные технологии генеративного проектирования для автоматического поиска и генерации вариантов дизайна. Из этих вариантов пользователи могут выбрать понравившиеся образцы. Появляется возможность создавать проекты в ограниченных и неограниченных проектных пространствах, как показано на рис. 1. [2]

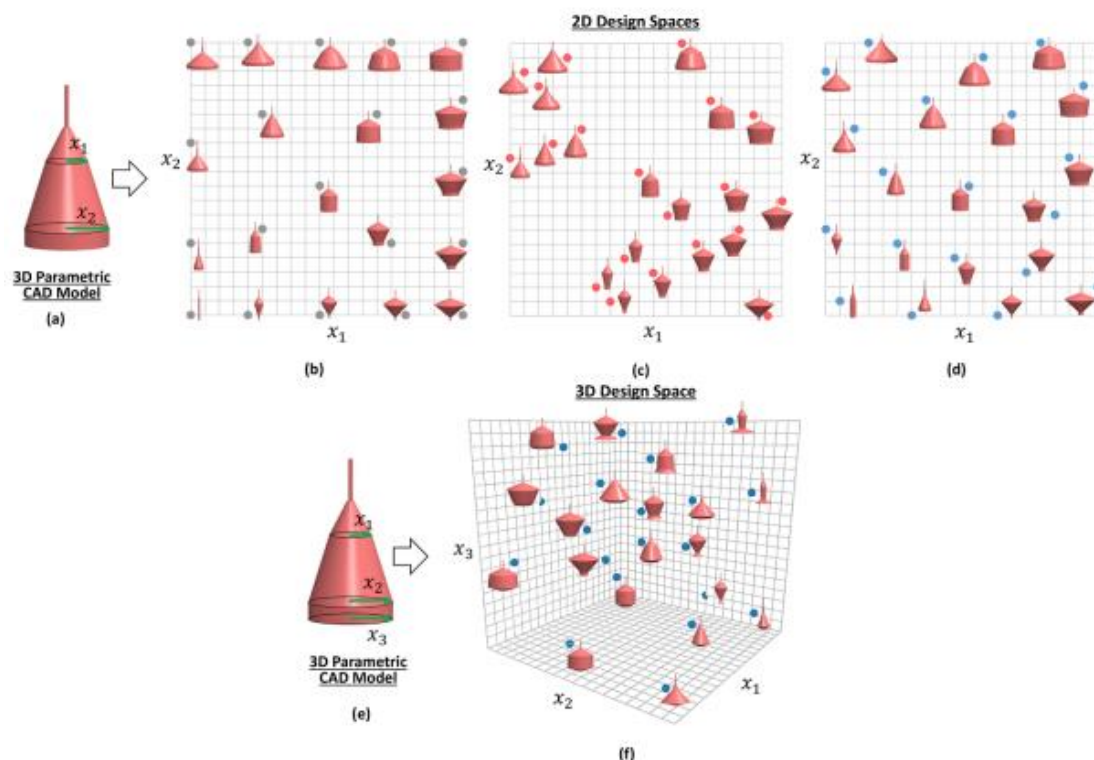


Рис. 1. Стек расширенной реальности

В рамках взаимодействия с интерфейсом проектирования и генерации новых форм предлагается использовать технологии XR. Данное понятие охватывает работу в средах дополненной, виртуальной и смешанной реальности, позволяя строить алгоритмы на стыке представленных подходов, как показано на рис. 2.

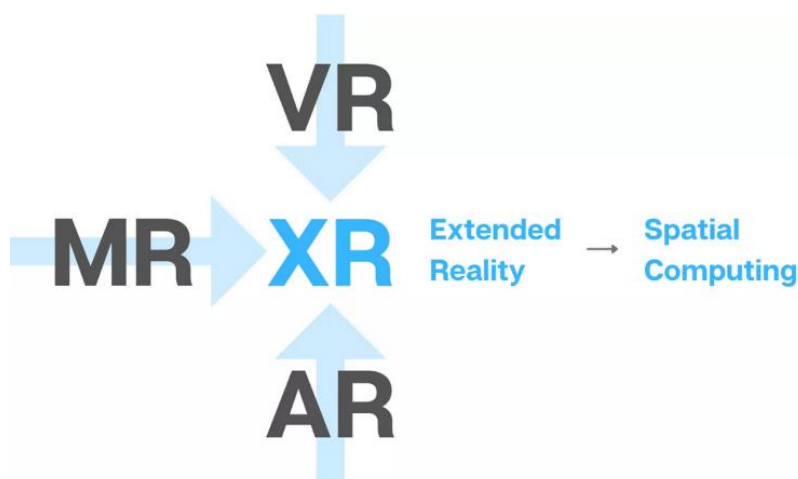


Рис. 2. Стек расширенной реальности

Для лучшего понимания особенностей погружения и взаимодействия с виртуальной средой проведено исследование условий иммерсивности интеллектуального интерфейса симбиотической системы управления удаленными динамическими объектами с применением VR технологий. Виртуальная реальность позволяет создавать среды наиболее приближенные к

реальности. Связано это с тем, что в виртуальной среде задействуется зрение человека в полном объеме, то есть кроме фокального зрения работает и периферическое зрение, как показано на рис. 3. [3]



Рис. 3. Фокальная и периферическая зона взаимодействия с интерфейсом

Использование подходов геометрического моделирования позволит расширить поиск новых форм и новой компоновки сложных поверхностей. Помимо этого планируется сформулировать подход к проектированию изделий, заложенный в области геометрического моделирования. Это позволит оптимизировать трудозатраты и получить необходимый результат.

В результате данной работы планируется выполнить разработку алгоритма использования принципов геометрического моделирования и генеративного дизайна в процессе проектирования объектов промышленного дизайна с использованием технологий смешанной реальности.

Для достижения поставленной цели следует решить следующие задачи:

- проанализировать особенности геометрического моделирования и средств его автоматизации на данный момент.
- проанализировать особенности аппаратной и программной составляющей современных устройств расширенной реальности (XR).
- сформировать алгоритмический комплекс решения задач, связанных с генеративным проектированием поверхностей в области промышленного дизайна.
- сформулировать принципы взаимодействия алгоритмического комплекса с технологиями расширенной реальности (XR).

Список используемых источников:

1. J Wu, X Qian, MY Wang Advances in generative design. Computer-Aided Design. 2019. DOI:10.1016/j.cad.2019.102733.
2. Shahroz Khan, Muhammad Junaid Awan, A generative design technique for exploring shape variations, Advanced Engineering Informatics, Volume 38, 2018, Pages 712-724, ISSN 1474-0346, <https://doi.org/10.1016/j.aei.2018.10.005>.
3. Влияние высоко ярких объектов на обнаружение периферийных целей в условиях сумеречного зрения / Дженгиз Д., Максимаинен М., Пуолакка М., Халонен Л.- Светотехника - Москва- 2016.

Shchur S.¹, Voloshinov. D²

- 1. Peter the Great St.Petersburg Polytechnic University (SPbPU)*
- 2. The Bonch-Bruевич Saint-Petersburg State University of Telecommunication*

Design of generative design objects based on geometric modeling using augmented reality technologies.

The design process becomes more complicated every year. New input data, design methods, and technologies are emerging. However, the interval between the release of products is getting shorter. Products are produced and updated much more often. However, despite the intensification of the development process, automation of 3-dimensional modeling systems and an increase in the labor market for specialists in this industry, there is a noticeable tendency to copy the fundamental elements of products with minor changes and improvements. The product range is replete with repetitive products, and developers avoid fundamentally new solutions.

Key words: generative design, Geometric modeling, Augmented Reality, XR.

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ, ИННОВАЦИИ, БИЗНЕС

Секция 5.1.

Цифровая трансформация, инновации, бизнес

УДК 347.77
ГРНТИ 62.01.75

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ В BIOTECH-СТАРТАПАХ: ПРАВОВОЙ И ТЕХНИЧЕСКИЙ АСПЕКТЫ

Ф. Т. Александров, Г. К. Сидоров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Цель исследования - оценить особенности организации процесса защиты информации наукоемких предприятий (стартапов) в России, создаваемых в сфере биотехнологий. Авторами статьи предложено разделение процесса защиты информации на внутренний и внешний аспекты: технический и правовой соответственно. Исследование сфокусировано как на инновационном характере создаваемого продукта, так и на особенностях хранения и защиты большого потока персональных данных пользователей.

интеллектуальная собственность, стартап, биотехнологии, защита информации, патентное право

В качестве примера для рассмотрения организационно-правовых аспектов защиты информации в Российской Федерации авторами статьи была выбрана область биотехнологий (*Life Science*, дословно “науки о жизни”), являющаяся актуальной и инвестиционно привлекательной на сегодняшний день. В сферу деятельности таких предприятий входят: биоинженерия, био- и наномедицина, технологическая фармакология, биоинформатика и др.

Согласно статье №16 ФЗ-149 Российской Федерации “Об информации, информационных технологиях и о защите информации” защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2. соблюдение конфиденциальности информации ограниченного доступа;
3. реализацию права на доступ к информации [1].

Таким образом, по мнению авторов, процесс защиты информации в случае рассмотрения биотехнологического стартапа, зарегистрированного в РФ, должен быть подразделен на внутренний и внешний аспекты. К внешнему аспекту относятся проектируемые системы в сфере biotech, являющиеся в своей основе инновационным наукоемким продуктом, отличающимся технической новизной – это интеллектуальная собственность и следующая из нее необходимость патентного регулирования. В узком смысле слова наукоемкое биотехнологическое предприятие является (с точки зрения закона) обладателем информации, извлекающим персональные данные граждан (п. 7 ст. №16 ФЗ-149, введен ФЗ №242 от 21.07.2014). Данным фактом объясняется внутренний аспект: с ростом количества биомедицинских стартапов остро встает вопрос безопасности хранимых данных: биомедицинские технические системы

обладают огромным количеством данных о пользователях (пациентах) – непосредственно защита информации.

Патентная аналитика как процесс, включающий в себя аналог анализа рынка: разведку патентных решений, почву (антураж) для анализа целесообразности и необходимости проведения НИОКР, определения перспективности области исследований, является неотъемлемой частью разработки нового высокотехнологичного продукта. [2] Вопросы организации операционной деятельности, включающие правовое регулирование взаимодействия участников, лицензирование проделанной работы и передачу исключительных прав (что для стартапов во всем мире непосредственно связано с “выходом” на *IPO* - публичным размещением акций компании), регулярно становятся проблемной областью для начинающих компаний. К тому же эти компании несут большие финансовые издержки при несвоевременной проработке защиты интеллектуальной собственности.

Начинающим предпринимателям стоит учитывать и патентный ландшафт (с англ. *Patent Landscape*) - инструмент анализа технологического контекста потенциального проекта в сфере интеллектуальной собственности. Важным также становится вопрос определения так называемого уровня техники (определяется приказом Роспатента №236 от 27.12.2018) - любых общедоступных в мире сведений до даты приоритета изобретения, по сравнению с которыми определяется новизна изделия.

Рассматривая искусственный интеллект (далее - ИИ) как совокупность математических моделей и методов, его нельзя классифицировать как изобретение. В соответствии с публикациями Всемирной Организации Интеллектуальной Собственности (ВОИС или *WIPO*), поскольку ИИ внедряется прежде всего через программное обеспечение, вопросы патентного права для программ для ЭВМ будут актуальными и для технологий ИИ. В соответствии со статьей №1350 Гражданского Кодекса Российской Федерации “Условия патентоспособности изобретения”, программа для ЭВМ (наиболее вероятный метод работы *biotech*-стартапа) не является изобретением или полезной моделью. Авторские права на программы для ЭВМ охраняются так же, как права на произведения литературы (творческий характер создания). Также необходимо защищать авторским правом бизнес-логику в виде блок-схемы бизнес-процессов, описывая их как сценарий. Бизнес-модель как основа для построения операционной деятельности компании, включающая в себя регламенты, инструкции и порядок масштабирования организации могут быть защищены свидетельством о депонировании. Деятельность биотехнологических организаций, помимо преобразования и автоматизации экспертных заключений, часто несет в себе характер НИОКР, в которых стороны обязаны обеспечивать конфиденциальность сведений, описываемых в предмете договора, хода его исполнения и полученных результатов (ГК РФ статья №771 “Конфиденциальность сведений, составляющих предмет договора”). Все упомянутые патентные особенности можно отнести к внешнему аспекту.

Также, во внешнем аспекте исключительно важно учитывать сотрудников компании (разработчиков, экспертов, консультантов, высший менеджмент), обладающий коммерческой тайной (ноу-хау). *NDA (non-disclosure agreement, договор о неразглашении)* - наиболее распространенная мера защиты информации и данных (в том числе, в рассматриваемом примере с биомедициной, и данных для обучения нейронных сетей, датасетов, алгоритмов и математических моделей, используемых в создаваемых программах), внедряемая в организации приказом как особый режим работы с информацией.

Внутренний аспект раскрывается с технической точки зрения, исходя из того факта, что основой для функционирования всего предоставляемого функционала biotech-стартапа являются клиентские данные. Они могут быть представлены в разном формате (в виде текстовых записей, фото- и видеосъемки) - чаще всего, результаты медицинских анализов. Стартап использует эти данные для моделей машинного обучения. Дальнейшая польза от таких моделей - помощь врачу в качестве ассистента (алгоритмы машинного обучения учитывают общие тенденции заболеваний, опираясь на опыт большого количества клиентов и пациентов), следовательно, это влечет за собой ряд положительных последствий - минимизируются ложные диагнозы, упрощается работа с личными картами пациентов (данные хранятся в базе данных) и, как итог, происходит уменьшение финансовых издержек для клиники. Упомянутый ранее ФЗ № 149 РФ “Об информации, информационных технологиях и о защите информации” устанавливает обязательства обладателя информации о недопущении воздействия на технические средства обработки информации, постоянном контроле за обеспечением уровня защищенности и нахождении баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

Стоит обратить внимание на критерии выбора архитектур моделей машинного обучения. Отметим два ключевых фактора: требования со стороны сложности задачи (внутренние) и требования со стороны закона (внешние). Внутренние требования подразумевают выбор архитектуры, опираясь только на сложность самой задачи. В свою очередь, сложность задачи напрямую зависит от типа предоставляемых данных. Она может варьироваться от самых простых архитектур (линейная регрессия, решающие деревья и т.д. - для табличных данных) до самых сложных архитектур (нейронные сети, архитектуры компьютерного зрения: сегментационные модели, модели для детекции объектов - снимки КТ - компьютерной томографии, ПЭТ - позитронно-эмиссионной томографии, рентгенографии или видеосъемка колоноскопии). Внешние требования заключаются в интерпретируемости - все происходящее внутри модели машинного обучения должно быть исключительно прозрачно, результаты работы алгоритмов должны быть объяснимы. Когда речь идет о человеческом здоровье, то метод “чёрного ящика” (изучение реакции системы на изменяющиеся воздействия как целого явления вместо изучения свойств и взаимосвязей ее составных частей) является недопустимым [3].

В данной работе был затронут ключевой аспект для всех протекающих процессов - данные пользователя. Используемые данные имеют личный характер и несут в себе информацию о состоянии здоровья пациента и его антропометрических характеристиках. Также имеет большую значимость информация о медицинском персонале, медучреждениях (физических, оффлайн-клиниках), сведения о системе здравоохранения. Такая информация обладает очень высокой ценностью для злоумышленников. В свою очередь, это влечет ряд проблем для стартапа - нужно заботиться о конфиденциальности пользовательских данных и всей информационной безопасности продукта. Забота о безопасности пользовательских данных начинается с малого - пресечения утечек персональных данных.

Исходя из этого, авторами было предложено проводить превентивные действия по обезличиванию, оперативной обработке и шифрованию данных. Внешний характер подразумевает контроль за доступом к самим данным - к данным имеет доступ непосредственно сам специалист и круг лиц, обладающих правом доступа. В таком случае осуществляется контроль за доступом к данным. Высокотехнологичное предприятие, предоставляющее медицинские услуги в сфере здравоохранения должно быть признано учреждением здравоохранения Федеральной службой по надзору в сфере здравоохранения. Следовательно, в соответствии с ФЗ №152 “О персональных данных”, администрация учреждения здравоохранения обязана нести ответственность за обеспечение конфиденциальности и защиты медицинской информации о пациенте, являющейся профессиональной медицинской тайной. Не допускается использование автоматизированных баз данных (далее - БД), включение их в сети, связывающие их с другими БД. Во внутренней сети организации передача персональных данных пациентов должна осуществляться с использованием технических и программных средств защиты информации. Лицензионным требованием для организации, осуществляющей медицинскую деятельность является наличие у заместителей руководителя организации, ответственных за осуществление медицинской деятельности, высшего медицинского образования и стажа не менее 5 лет. Эксперты, принимающие участие в разработке системы и предоставляющие свои консультационные услуги, должны иметь образование, предусмотренное квалификационными требованиями к медицинским и фармацевтическим работникам, и иметь пройденную аккредитацию (сертификацию) специалиста [4].

Список используемых источников:

1. Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ “Об информации, информационных технологиях и о защите информации” (последняя редакция) // Консультант-Плюс - справочная правовая система. URL : http://www.consultant.ru/document/cons_doc_LAW_61798/. Дата обращения: 28.06.2022.
2. Николаев А. С., Кириллов Н.Н. Применение патентной аналитики при сопровождении инновационных проектов в технических ВУЗах // Университет ИТМО, Санкт-Петербург, Россия. Экономика. Право. Инновации. 2021. №4. С. 18. URL : <http://dx.doi.org/10.17586/2713-1874-2021-4-15-25>.

3. Christopher M. Bishop. Pattern Recognition and Machine Learning // Издательство Springer, 2006, P. 225.

4. Постановление Правительства РФ от 01.06.2021 №852 (ред. от 16.02.2022) “О лицензировании медицинской деятельности” // Консультант-Плюс - справочная правовая система. URL :

http://www.consultant.ru/document/cons_doc_LAW_385633/0c7bf8d00f19dbae8d6d2053e9f9971b0b4f9a31/. Дата обращения: 29.06.2022.

Alexandrov F., Sidorov G.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Fundamentals of information security in biotech startups: legal and technical aspects.

Abstract. The purpose of the study is to evaluate the features of the organization of the information protection process of high-tech enterprises (startups) in Russia created in the field of biotechnology. The authors of the article proposed the separation of the information protection process into internal and external aspects: technical and legal, respectively. The research focuses both on the innovative nature of the product being created and on the features of storing and protecting a large flow of personal data of users.

Key words: intellectual property, startup, biotechnology, information protection, patent law.

УДК 658.52.011.56
ГРНТИ 50.47

АНАЛИЗ ЭФФЕКТИВНОСТИ ВНЕДРЕНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ НЕФТЕБАЗОВЫМ ХОЗЯЙСТВОМ

Д. В. Дороганов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Передовые информационные технологии все глубже проникают в структуру сегодняшнего бизнеса, все теснее интегрируются с производственными и управленческими процессами компаний, все активнее используются функциональными подразделениями предприятий в их собственной деятельности, во взаимоотношениях с другими службами и окружающим миром. Наличие комплексной информационной системы на предприятиях – это объективная необходимость сегодняшнего бизнеса.

ИТ-проекты, бизнес-анализ, АСУП, оценка эффективности, MES

Цифровизация бизнеса становится новым трендом развития компаний, желая упрочить свое положение на рынке, снизить издержки и повысить продуктивность персонала иницируются ИТ-проекты, направленные на цифровую трансформацию процессов из аналогового представления в электронный. Такие проекты стоят очень дорого и проходят на достаточно длинном промежутке времени, в связи с чем важно грамотно и всесторонне оценить будущие эффекты как с финансовой точки зрения, так и процессной [1].

Объектом научного исследования будет служить автоматизированная система управления нефтебазовым хозяйством уровня MES (по градации существующих КИС), внедряемая на одном из предприятий группы компаний в нефтегазовой сфере. Предприятие занимается перевалкой, автомобильной транспортировкой и контролем качества светлых нефтепродуктов. Является 100% дочерним обществом ПАО «Газпром нефть». Численность сотрудников 2366 чел. Собственный парк нефтебаз насчитывает 28 объектов по РФ. Основной вид деятельности организации: Хранение и складирование нефти и продуктов ее переработки (код по ОКВЭД 52.10.21).

Актуальность исследования обусловлена необходимостью получить целостную картину о течении проекта, его влиянии на процессы компании, о достижении планируемых качественных и количественных показателей.

Основным поводом для инициации проекта автоматизации операционных процессов послужило низкое проникновение информационных технологий в производственные процессы компании, связанные с приемом, отпуском и хранением светлых нефтепродуктов, а также сильная их зависимость от человеческого фактора. Многие производственные объекты не оборудованы автоматизированными средствами измерения, учета и контроля, что приводило к искажению данных, которые принимаются к учету ERP системами, что в свою очередь приводило к несоответствиям данных до входа в глобальный бизнес-процесс перевалки на этапе получения топлива на нефтебазе и после, на этапе продажи и получения топлива заказчиком. В идеальном сценарии эти данные должны были сходиться почти на 100% [2].

Также, так как данные заносились в учетные и технологические системы вручную, процесс не защищен от мошенничества с данными, что сильно затрудняет раскрытие и расследование недостатков и технологических потерь. Достаточно высокой является нагрузка персонала работой в разрозненных информационных системах, заполнения журналов и ручным заполнением учетных документов (ТТН, актов, справок). Зачастую, единственным фактом отгрузки нефтепродукта была запись в бумажном журнале или строка в общедоступной Excel таблице.

Все указанные проблемы приводили к удлинению бизнес процессов, увеличению издержек и потерь компании, к отсутствию прозрачности происходящих процессов для поставщиков и потребителей глобального бизнес-процесса «Перевалки светлых нефтепродуктов» всей группы компаний.

Общий жизненный цикл системы начался с реализации пилотного проекта, который был инициирован в 2019 году. В рамках капитальной модернизации нефтебазового хозяйства в Ленинградской области было принято решение провести пилотирование системы управления производственными процессами нефтебазы.

Первостепенной задачей стояло сформулировать требования к системе. В общем виде она должна была обеспечивать автоматизацию операций, поддержку принятия решений, агрегацию и передачу данных по 4 основным бизнес-процессам нефтебазы, а именно приему, отпуску, хранению и контролю качества нефтепродуктов. Также, в рамках пилотного проекта была выбрана и протестирована платформа для реализации решения. Конкурс проводился на основе балльной системы по трем критериям: функциональность, оценка вендора и опыт, финансовые параметры.

По итогам было решено реализовывать на российской платформе Tibbo Aggregate (рис. 1). Немаловажным фактором в условиях санкционного давления также являлась импортнезависимость вендора, что помогло избежать части рисков остановки проекта.

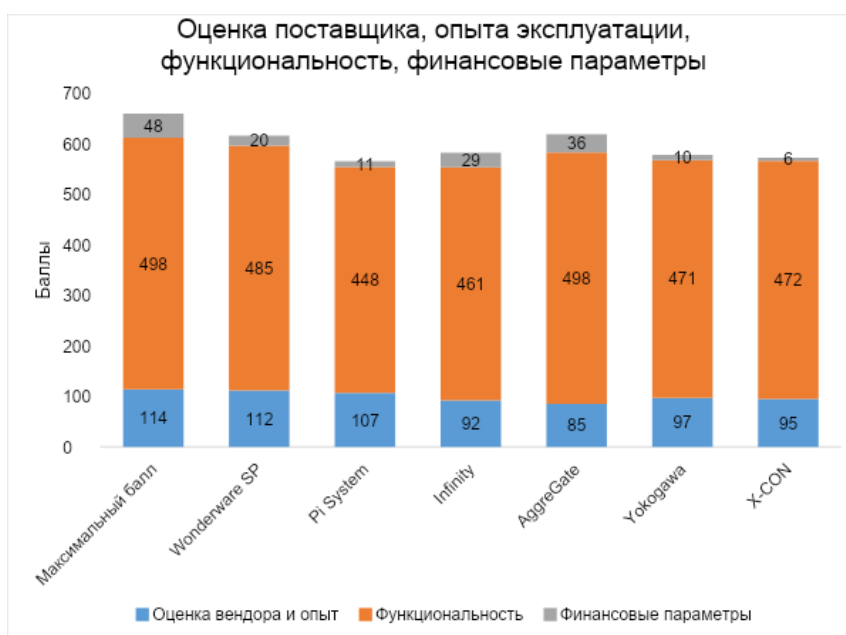


Рис. 1. Сравнительная диаграмма платформ для реализации MES

По результатам проекта был реализован MVP системы (от англ. Minimum Viable Product) – продукт, имеющий минимальный набор параметров и функций, но при этом выполняющий поставленную узкую задачу [3].

В продолжение реализации системы в 2020 году был инициирован проект доработки функционала системы до целевого и тиражирование полноценного решения на 12 объектов общества. Проект подразумевает создание проектной команды и выбор подрядчика для развертывания инфраструктуры и прикладного программного обеспечения.

На данном этапе можно выделить ряд эффектов, достижение которых можно измерить качественно и количественно (таблица 1).

ТАБЛИЦА 1. Представление эффектов в формате Balanced Scorecard

Стратегические цели:							
<ul style="list-style-type: none"> • обеспечение бесперебойного и максимально эффективного процесса перевалки нефтепродуктов, • повышение уровня прослеживаемости процессов на каждом этапе, • снижения количества прямых потерь НП вследствие утраты качества (аварийное смешение) или количества (технологические потери и кражи) 							
Финансы		Бизнес процессы		Клиенты		Персонал	
Описание эффекта	Ожидаемое влияние	Описание эффекта	Ожидаемое влияние	Описание эффекта	Ожидаемое влияние	Описание эффекта	Ожидаемое влияние
Снижение издержек на оплату штрафов	до 37 млн. руб.	Снижение длительности процессов	20%	Снижение времени налива бензовоза	50%	Снижение одновременно количества АИС для ключевых пользователей	3 ->1
Оптимизация ФОТ	-5%	Снижения объема бумажной отчетности	20%	Снижения минимального остатка НП	5%	Получения опыта участия в цифровых проектах	б.р
		Снижения количества операций ручного ввода данных	7	Снижения риска прямых потерь НП	до 5 млн. руб. в годовом выражении	Снижения количества операций с участием персонала НБ	10%

Так как компания-заказчик не работает в условиях свободного рынка, то повлиять на рост доходов система не может, а только на снижения затрат и издержек. Таким образом, по результату анализа финансовой документации по профилю операционной деятельности было посчитано, что в среднем по статьям штрафов различным контрагентам компания тратит 46 млн. рублей ежегодно.

При реализации 100% целей внедрения системы риск получения штрафов снижается приблизительно на 82%. Соответственно, в бюджет можно будет заложить всего 9 млн. рублей, финансовый эффект 37 млн. рублей. Тем не менее, по результату расчета чистой текущей стоимости (NPV) заметно, что система не окупается в течение длительного периода времени (рис. 2).

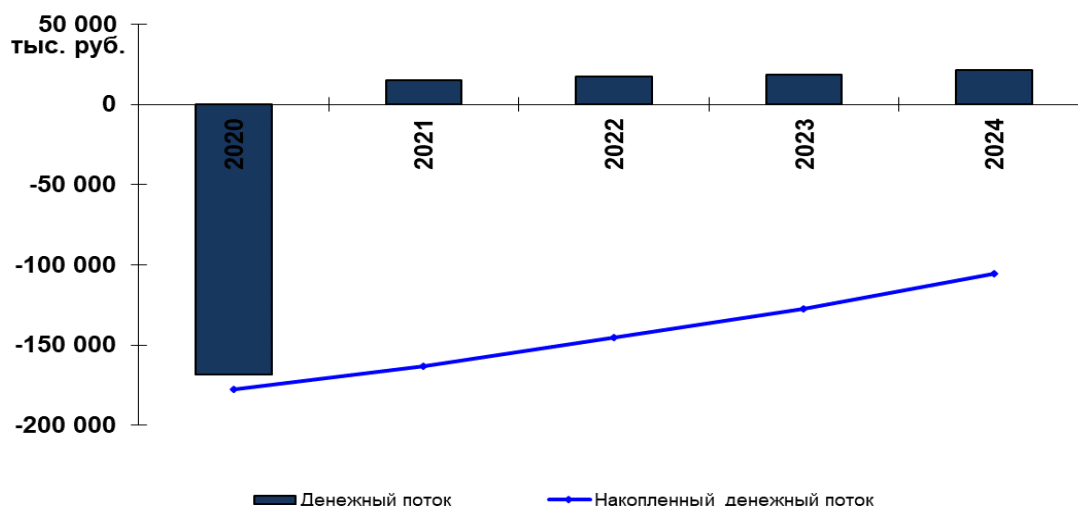


Рис. 2. График NPV

Но нельзя не отметить положительные эффекты качественного порядка. Безусловно, в первую очередь серьезно сократилась длительность бизнес-процессов, снизился объем составляемой вручную бумажной отчетности, объем заполняемых вручную полей в коммерческих учетных системах за счет автоматизированной интеграции систем. Снизилась вероятность мошенничества с использованием подделки данных технологических измерительных систем.

Для оперативного персонала снизилось количество информационного шума в виде небольших разрозненных узкоспециализированных систем, и появилась возможность работать в режиме «единого окна». Для менеджмента организации появился понятный источник производственных данных о состоянии объектов в 4 часовых поясах.

Также снизилось время обслуживания бензовозов, что влияет на совокупные издержки всех дочерних компаний, входящих в цепочку обеспечения вторичной логистики светлых нефтепродуктов.

Итогом исследования служит вывод о необходимости всеобщей оценке эффективности внедряемых систем, в том числе со стороны труднооцениваемого эффекта на процессы и ресурсы организации. Сложностью данного проекта является преобладание качественных эффектов над количественными, в связи с чем необходимо четкое позиционирование результатов проекта с точки зрения накопительного эффекта для всей цепочки производственных процессов компании, без привязки к финансовому прогнозу снижения издержек.

Список используемых источников:

1. Успешность IT-проектов. Мировая статистика выполненных проектов [Электронный ресурс]. URL: https://project-management.zis.by/drugoe/vestibulum_iaculis/ (Дата обращения 09.11.2022)
2. Дороганов Д. В. Анализ эффективности внедрения автоматизированной системы управления нефтебазовым хозяйством: отчет о НИР. СПб. : СПбГУТ, 2021. 35 с.
3. Николаенко В. С. Разработка принципов управления IT-проектом // Вестник Томского государственного университета. 2015. N 390. С. 155–160.

Doroganov D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Efficiency analysis of deployment MES system for tank farm business.

Advanced information technologies penetrate deeper into the structure of today's business, integrate more closely with the production and management processes of companies, and are increasingly used by the functional divisions of enterprises in their own activities, in relationships with other services and the outside world. The availability of a comprehensive information system at enterprises is an objective necessity of today's business.

Key words: IT-projects, business intelligence, efficiency analysis, MES.

УДК 65.011.56
ГРНТИ 20.51.23

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ БИЗНЕС-ПРОЦЕССОВ В КОМПАНИИ НА ПРИМЕРЕ MDM СИСТЕМЫ

Д. Д. Дускаев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Цифровая трансформация на сегодняшний день является неизбежным явлением, определяющим конкурентоспособность. В нынешних реалиях преимущество в бизнесе получает тот, кто одним из первых подключиться к процессу глобальной цифровизации. Множество цифровых каналов и способов связи пользователя с компанией позволяют собирать и изучать огромное количество данных о предпочтениях клиентов. Данные становятся основой экономического анализа, исследующего закономерности функционирования современных социально-экономических систем. Для решения подобной задачи существуют MDM системы.

MDM система, цифровая трансформация, корпоративные информационные системы

Цифровая трансформация бизнеса — это значительная перестройка бизнес-процессов предприятия с применением новейших цифровых технологий. Данный подход предусматривает не только покупку нового оборудование и внедрение нового ПО, трансформация заключается в готовности глобального пересмотра структуры всего предприятия и бизнес-процессов, в частности, поэтому является сложной и комплексной задачей.

В то же время, цифровизация позволяет создавать и внедрять новые форматы работы, оптимизировать повторяющиеся рутинные задачи и всегда иметь доступ к статистической и аналитической информации. При работе над трансформацией любая компания ставит целью достичь экономических результатов, оптимизировать издержки бизнеса и повысить качество сервиса.

Трансформация сегодня происходит как в экономике государства в целом, так и в отдельных направлениях бизнеса.

Сложно представить цифровизацию промышленного предприятия без большого количества упорядоченных данных и «умной» аналитики. На современном производстве ежедневно создается огромное количество разнообразных данных: информация с датчиков, приборов, «умных устройств», камер видеонаблюдения, таблицы, тестовые документы и т.д. и не всегда этот поток информации используется в полном объеме, зачастую выделяется лишь небольшая часть, на основе которой делаются те или иные выводы. Так, по оценке специалистов около 95% получаемой информации предприятиями не используется вообще, а собирается из соображений «чтобы было». Получая собственные данные, а также информацию из внешней среды, большинство предприятий не имеют инструментов и технологий для их обработки, анализа, выявлению зависимостей и взаимосвязей между ними, на основе которых

возможны принятие обоснованных решений, корректировка производственных и бизнес-процессов. Используя традиционные методики обработки и анализа, невозможно охватить постоянно растущий объем гигабайтов информации. Поэтому MDM системы в настоящее время рассматриваются как основной инструмент для структурирования огромного количества неоднородных данных как в промышленности, так и в других сферах жизни общества.

Исходя из диаграммы рис. 1 предоставленным консалтинговой компанией KMDA [1] отображается представление о статусе цифровой трансформации в России по разным отраслям на основе усредненных данных. Значение может отличаться от показателей каждой конкретной компании. Для расчета стадии цифровой трансформации отрасли KMDA использовали совокупность оценок по ключевым вопросам цифровой зрелости с компенсацией в сторону мнения топ-менеджеров. Эти вопросы по отдельности подробно разобраны в последующих разделах отчета. Сферы жилищно-коммунального обслуживания, государственного управления, нефтегаза и ритейла показали наибольшую динамику относительно показателей предыдущего исследования от 2018 года.

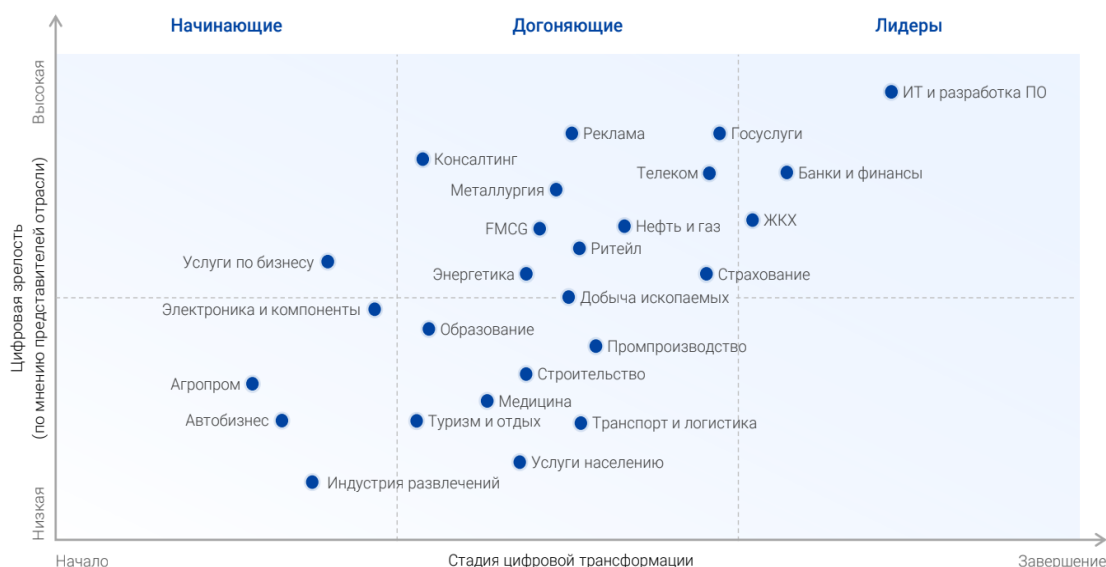


Рис. 1. Статус цифровой трансформации в России по разным отраслям

Видно, что лидирующие позиции по уровню трансформации занимают кампании в B2C-секторе: например, медиа, в котором уже произошли фундаментальные изменения, а также розничная торговля, телекоммуникации, страхование и банковское обслуживание. Цифровизация уже существенно повлияла на эти отрасли, но окончательный результат еще предстоит определить в дальнейшем.

Для полноты хранимых и обрабатываемых данных в предприятиях используются не одна отдельно взятая система, а связка систем с настроенными интеграционными потоками и коннекторами между ними. На примере рассматриваемой в данной статье, MDM системе используя данных хранящейся в ней VI-приложение способна проанализировать и вывести статистику или необходимые ключевые показатели на дашборд для отслеживания метрик и принятия своевременного решения. При этом в саму MDM систему поступают

данные от ERP системы, например для хранения актуального справочника «Сотрудников» или другого общекорпоративного справочника НСИ.

MDM-системы – системы, представляющие собой ПО, структурирующее разнородную информацию компании, объединяя ее из различных источников и систем и отображая стандартизированные данные внутри информационных систем компании. К основным данным, контролируемым MDM-системами относят следующие типы данных:

- обозначения клиентов; перечень сотрудников; перечень поставщиков; перечень заказчиков;

- детали и продукты;

- элементы бухгалтерского учета; контракты и т.д;

- описание элементов данных, используемых в бизнес-процессах;

При правильном внедрении MDM системы в бизнес-процессы, компании получают:

- Ускорение бизнес-процессов, уменьшение расходов – рост производительности труда.

- Обеспечение согласованной отчетности и улучшение процесса принятия решений: при использовании MDM системы создание различных отчетов обеспечивается управляемыми процессами. Согласованность информации, предоставляемая MDM, способствует формированию высококачественных данных в бизнесе и позволяет принимать более четкие, быстрые, лучшие бизнес-решения.

- Улучшение управления, соответствия нормативным требованиям и управления рисками: фрагментация основных данных имеет негативное влияние на процессы управления, соблюдения и управления рисками, затрудняя согласование данных. MDM устраняет несоответствия в основных данных и позволяет наладить эффективное управление процессом.

- Повышение уровня контроля и качества аналитики. Искусственный интеллект обрабатывает собранные о клиенте данные, чтобы создавать для него подходящие предложения.

В ходе работы над статьей был произведен анализ проекта по внедрению MDM системы в корпоративную информационную сеть ООО «ГПН-ЦР». Планируемый срок реализации проекта 10 месяцев, внедрение осуществляется ресурсами подрядчика и департамента организации управления данными.

Внедрение системы происходило с применением каскадного метода управления проектами, где все этапы реализовываются последовательно. По завершению проекта было выявлено ряд недостатков в виде ошибок самой системы, комментариями заказчика и изменившиеся условия самой среды. Что привело к увеличению времени при сдаче продукта и соответственно в увеличение стоимости.

Недостатком выбранного подхода является в его последовательности, где нет промежуточных версии и нет возможности изменить проект. Проблематика при выборе подхода для управления проектами на сегодняшний день является наиболее актуальной среди прочих.

Проанализировав существующие методы и подходы для управления проектами можно выделить Agile методологию.

Agile — это итеративный подход к управлению проектами и разработке программного обеспечения, который помогает командам быстрее и с меньшими проблемами поставлять ценность клиентам. Вместо того чтобы выпускать весь продукт целиком, команда, следующая принципам Agile, выполняет работу в рамках небольших, но удобных инкрементов. Требования, планы и результаты оцениваются непрерывно, благодаря чему команды могут быстро реагировать на изменения.

Применив Agile подход для реализации проекта по внедрению MDM системы в корпоративную сеть ООО «ГПН-ЦР», на этапе реализации все задачи разбиваются на спринты состоящие по времени 2-3 недели. По завершению спринта тестируется функционал, и заказчик может внести некоторые доработки. Список задач для следующего спринта приоритезируется исходя из плана проекта. В данном подходе каждый из членов команды получают детализированную задачу что упрощает её решение, что в итоге повысит качество продукта.

Таким образом техническая реализация проекта по внедрению, планируемая в 43 дня, разбивается на 4 спринта. План этапа реализации представлен в виде диаграмма ганта на рис. 2.



Рис. 2. План этапа реализации проекта по внедрению MDM системы

На начальных этапах запрашиваются необходимые доступы, подготавливается инфраструктура для внедрения новой системы во внутрикорпоративную сеть. После подготовки устанавливается базовая версия системы, настраиваются хранилища данных и тестируется промежуточных результатов.

Третий спринт включает в себя настройку интеграции с другими системами источниками и экранами. По сколько MDM система создана для работы с данными данный этап является ответственным для создания ценности бизнесу. При возможности получать неоднородные данные с разных источников, система структурирует все данные по выбранному алгоритму и дает возможность отобразить актуальную статистику по производственному процессу либо реализации проекта.

Четвертый спринт включает в себя задачи по настройке штатного функционала самой системы. В штатный функционал входят элементы бизнес-гlossария, описание элементов данных участвующих в бизнес-процессах, объекты качества данных и справочники.

Для элементов бизнес-гlossария, элементов данных и качества данных настраивается жизненный цикл для утверждения объектов, тем самым за каждым

объектом системы закрепляется ответственное лицо, что по итогу повысит качество вводимых данных в систему.

Настройка жизненного цикла происходит по утверждённой методологией разработанной ООО «ГПН-ЦР» для удовлетворения своих бизнес-требований.

Таким образом при правильном подходе в соответствии с современными методиками и инструментарием, проект по внедрению MDM системы в корпоративную среду ООО «ГПН-ЦР» возможно реализовать в срок сохранив качество конечного продукта и удовлетворим требования заказчика.

Рассмотренная MDM система является одним из примеров при цифровой трансформации в корпоративной среде и при правильном подходе создаются бизнес ценности организации. В данном случае бизнес-ценностью являются данные. Структурированные данные дают возможность BI-приложениям составлять аналитику и отображать на экранах статистику по производству. Создается каталог внутрикорпоративных терминов, для единого понимания и хранения НСИ документации.

Ценность имеет не одна отдельно выделенная система, а построения интеграции с другими бизнес-системами уже существующих в компании. Корпоративная среда обладает множеством количества систем, техническими решениями, базами данных и соответственно хранимой информацией. Применяв современные решения для работы с большими данными и использование современных программных средств, открывается возможность для переработки «сырых» данных по их принадлежности и структурированию для дальнейшего переиспользования.

Список используемых источников:

1. Консалтинговая компания в области цифровой трансформации KMDA: [Электронный ресурс]. URL: https://komanda-a.pro/projects/dtr_2020. (Дата обращения 13.11.2022).

2. Terrar David What is Digital Transformation?: [Электронный ресурс] Theagileelephant.com. . URL: <http://www.theagileelephant.com/what-is-digital-transformation>. (Дата обращения 13.11.2022).

Duskaev D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Digital transformation of business processes in a company on the example of an mdm system. Digital transformation today is an inevitable phenomenon that determines competitiveness. In the current realities, the advantage in business is given to the one who is one of the first to connect to the process of global digitalization. A lot of digital channels and ways of user communication with the company allow you to collect and study a huge amount of data about customer preferences. The data become the basis of economic analysis that examines the patterns of functioning of modern socio-economic systems. MDM systems exist to solve this problem.

Key words: MDM system, digital transformation, corporate information systems.

УДК 001.895
ГРНТИ 14.01.75

ЦИФРОВОЙ ПРОФИЛЬ ГРАЖДАНИНА КАК ЭЛЕМЕНТ ПРОФОРИЕНТАЦИИ УЧАЩИХСЯ

М. С. Казакова

Поволжский государственный университет телекоммуникаций и информатики

Одной из проблем современного общества является то, что учащиеся учебных заведений часто отказываются от работы по специальности. Для уменьшения процента учащихся, неудовлетворённых полученной специальностью, необходимо серьезно подходить к вопросу профориентационной работы, которая должна помочь выпускникам определиться с будущим направлением подготовки. Для осуществления профориентационной работы предлагается разработать программное обеспечение с использованием элементов цифрового профиля в качестве элемента профориентационной работы со школьниками и студентами.

абитуриент, вуз, цифровой профиль, инновации в сфере профориентации, профориентация

Одной из проблем современного общества является то, что учащиеся учебных заведений часто отказываются от работы по специальности. Таким образом предприятия теряют высококвалифицированные кадры, а молодым людям приходится получать еще одно образование для того, чтобы развиваться в иной профессиональной области. Для уменьшения процента учащихся, неудовлетворённых полученной специальностью, необходимо серьезно подходить к вопросу профориентационной работы, которая должна помочь выпускникам определиться с будущим направлением подготовки. В статье предлагается концепция профориентационного приложения, которое с помощью использования механизмов цифрового профиля должно способствовать пониманию учащегося, какая профессиональная область ему интересна.

Сегодня проект цифрового профиля постепенно входит во все сферы жизни общества, значительно упрощая многие рутинные процессы. [1] В связи с этим целесообразно рассмотреть возможность использования цифрового профиля в качестве элемента профориентационной работы со школьниками и студентами по нескольким направлениям:

- помощь в выборе направления подготовки и вуза для выпускников школ и ССУзов;

- помощь в подборе вакансий для выпускников высших учебных заведений.

В основу развития обоих направлений ляжет процесс анализа интересов учащихся.[2] Цифровой профиль учащегося может быть сформирован с помощью информации о мероприятиях, которые он посещает (конференции, мастер-классы, научные лекции и т.д.), научной или развивающей литературе, пройденных в режиме онлайн и офлайн курсах. Для учащихся регионов будет разработана мобильное приложение, а также банками-эмитентами будет выпускаться специальная карта «Я-будущее своей страны». Приложение позволит пользователю узнавать об определенных мероприятиях, а карта – приобретать товары со скидкой. Рассмотрим каждый из вариантов подробнее.

Мероприятия

В мобильном приложении в разделе «Мероприятия» пользователю будет доступен перечень профориентационных и познавательных мероприятий в разных сферах общественной жизни. В разделе «Выбираю вуз» будет представлен перечень мероприятий, проводимых образовательными учреждениями региона, например, дни открытых дверей, дни факультетов и другие мероприятия для абитуриентов. В разделе «Исследователь» будет размещаться информация о проводимых в регионе конференциях, конкурсах и т.д. Данный раздел будет оснащен возможностью фильтрации по направлению (гуманитарные, технические, смешанные направления), по уровню (районный, городской, областной, межрегиональный), по дисциплине (история, математика, информатика и т.д.). Также по каждому мероприятию будет предоставлена информация о дате и месте проведения, требованиям к докладу (при необходимости), а также возможность регистрации, которая будет проводиться по уникальному идентификатору пользователя и не требует заполнения никаких полей, кроме возможности редактировать телефонный номер и адрес электронной почты.

В приложении будет реализована возможность настройки напоминания о выбранных мероприятиях, возможность настройки уведомлений о новых мероприятиях в выбранной области.

Мастер-классы

В разделе «Мастер-классы» пользователь получит возможность ознакомиться с перечнем мастер-классов, проводимых в регионе. Используя функции фильтрации, пользователь будет иметь возможность найти интересующее событие по ряду параметров (например, направление, время и место проведения, стоимость и т.д.). Пользователь будет иметь возможность записаться на мероприятие и, при необходимости, оплатить участие в нем, не покидая приложения. При оплате картой «Я-будущее своей страны» пользователь получит скидку или кешбек в зависимости от условий компании, реализующей мастер-класс.

Курсы

Партнерство проекта с онлайн-школами позволит пользователю в разделе «Курсы» выбирать курсы по разным направлениям. Будет реализована возможность выбрать курс по таким параметрам, как профессиональное направление, продолжительность, стоимость и т.д. При оплате картой «Я-будущее своей страны» пользователь получит скидку или кешбек в зависимости от условий компании, реализующей курс.

Практика и стажировка

Данный раздел будет предназначен для студентов и выпускников высших учебных заведений. В нем будет размещена информация о проводимых компаниями региона стажировках, грантовых программах и практиках. В приложении будет реализована возможность направить резюме для прохождения стажировки.

Все грамоты и сертификаты, полученные учащимся в процессе участия в тех или иных мероприятиях, автоматически подгружаются в личный кабинет, формируя, таким образом, портфолио пользователя, которое он может использовать при поступлении в высшее учебное заведение. Такая

информационная система позволит учащемуся иметь удобный доступ ко всем учебным мероприятиям региона, а также упростит процесс регистрации и подачи документов.

Также пользователю приложения будет доступна вкладка статистика, где он сможет отследить, какое количество мероприятий по каждому из профессиональных направлений он посетил за определенный период времени.

Еще одним элементом предлагаемого программного обеспечения будет являться модуль тестирования. Данное средство поможет пользователю определиться с перечнем интересным ему областей развития путем реализации различных групп тестов, призванных определить разнообразные склонности обучающегося.

Предлагаемая система на основе анализа цифрового профиля позволит повысить уровень профориентации учащихся и, как результат, позволит более осознано подходить к вопросу выбора будущей профессии.

Процесс работы системы представлен на рис. 1.

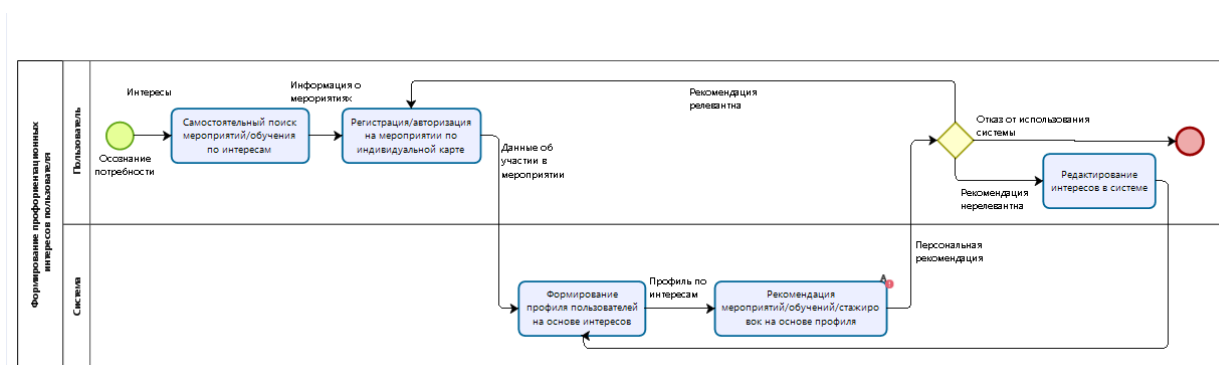


Рис. 1. Бизнес-процесс работы системы

Список используемых источников:

1. Гордеева Е. В., Мурадян Ш. Г., Жажоян А. С. Цифровизация в образовании // Economy and Business. 2021 С. 113.
2. Петров А. А. Российская матрица цифрового профиля россиянина // Национальная ассоциация ученых. N 52. 2020. С. 47.

Kazakova M.

Povolzhskiy State University of Telecommunications & Informatics

Digital profile of a citizen as an element of career guidance for students.

One of the problems of modern society is that students of educational institutions often refuse to work in their specialty. In order to reduce the percentage of students dissatisfied with their specialty, it is necessary to seriously approach the issue of career guidance, which should help graduates decide on the future direction of training. To carry out career guidance work, it is proposed to develop software using digital profile elements as an element of career guidance work with schoolchildren and students.

Key words: *university, digital profile, innovations in the field of career guidance, career guidance*

УДК 338.465:630(470.12)

ГРНТИ 68.47.75

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ПРЕДОСТАВЛЕНИЯ ГОСУДАРСТВЕННЫХ УСЛУГ В СФЕРЕ ЛЕСНОГО ХОЗЯЙСТВА ВОЛОГОДСКОЙ ОБЛАСТИ НА ОСНОВЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Н. А. Кремлёва, А. В. Папышкова

Вологодский государственный университет

Государственные услуги – фундаментальная часть современного общества и основа для реализации социально-экономической политики в Вологодской области. Одним из главных направлений административной реформы является повышение качества предоставления государственных услуг в сфере лесного хозяйства [1]. В статье проведен анализ современной литературы в области предоставления государственных услуг, который показал, что цифровизация и совершенствование государственных услуг в лесной отрасли проходит медленно и недостаточно эффективно. Результаты исследований могут быть применены на практике в Департаменте лесного комплекса Вологодской области для совершенствования информационно-коммуникационных технологий, освоения полноценного и непрерывного цикла лесозаготовки, модернизации имеющихся информационных систем, а также обеспечат увеличение процента заявителей, которые обращаются за государственными услугами через электронную систему. Разработаны подходы к совершенствованию системы предоставления государственных услуг в сфере лесного хозяйства, заключающиеся в создании облачного сервиса с целью обеспечения единообразного качества предоставления госуслуг; оперативном реагировании Единого портала госуслуг на запросы со стороны населения; повышении квалификации работников органов исполнительной власти по предоставлению государственных услуг с применением цифровых технологий; необходимости совершенствования как организационных, так и технических аспектов взаимодействия всех участников данного процесса. Основные направления дальнейших исследований: анализ процесса предоставления государственных услуг в Департаменте лесного комплекса области, сравнение количества поданных заявлений через Портал Государственных услуг, в ходе личный приема и МФЦ, выявить проблемы, с которыми сталкиваются заявители и государственные служащие в работе информационных систем.

государственные услуги, цифровизация процесса предоставления государственных услуг, лесное хозяйство, Департамент лесного комплекса

Государственные услуги – основа для реализации социально-экономической политики в Вологодской области, а также фундаментальная часть современного общества [1].

Пандемия в 2020 году внесла значительные коррективы в предоставление государственных услуг в сфере лесного хозяйства. Специалисты были переведены на дистанционный формат взаимодействия с заявителями, личный прием граждан был ограничен.

На сегодняшний день многие государственные услуги, предоставляемые Департаментом лесного комплекса Вологодской области, полностью переведены в электронный формат. Например, с 1 июля 2021 года по 1 января 2025 года отчеты об использовании лесов предоставляются исключительно в форме электронного документа с использованием единого портала государственных и

муниципальных услуг (п. 8 Федерального закона РФ от 20.01.2021 года «О внесении изменений в Лесной кодекс Российской Федерации и отдельные законодательные акты РФ в части совершенствования правового регулирования лесных отношений»).

Рассмотрим динамику поступления заявлений в Вологодский территориальный отдел – государственное лесничество за 2020-2022 гг. Так, в 2020 году было получено 827 отчетов непосредственно в Департамент, 168 отчетов – принято через Портал Государственных услуг, а в 2021 году количество отчетов, поданных через портал увеличилось до 1134. причем число поданных заявлений через ЕГПУ увеличилось в третьем квартале (таблица 1).

ТАБЛИЦА 1. Прием отчетов об использовании лесов от граждан, юридических лиц, осуществляющих использование лесов

Г од	1 квартал			2 квартал			3 квартал			4 квартал		
	Лесни чест во	Е П Г У	М Ф Ц	Лесни чест во	Е П Г У	М Ф Ц	Лесни чест во	Е П Г У	М Ф Ц	Лесни чест во	Е П Г У	М Ф Ц
20 20	254	12	0	180	0	0	204	8	0	189	148	1
20 21	239	171	0	148	40	0	0	233	0	0	590	0
20 22	0	481	0	0	313	0	0	181	0	0	125	0

Подать заявление о «Принятии решения о предоставлении права заготовки древесины и подготовке проекта договора купли-продажи лесных насаждений для собственных нужд» через Портал Государственных услуг стало возможным с января 2022 года. Исходя из приведенных данных таблицы, можно отметить, что граждане стали активно пользоваться данной возможностью (таблица 2).

Полученные аналитические данные подтверждают актуальность проводимых исследований в области совершенствования государственных услуг в сфере лесных отношений в Вологодской области.

ТАБЛИЦА 2. Прием заявлений для заключения договоров купли-продажи лесных насаждений для собственных нужд граждан

Г од	1 квартал			2 квартал			3 квартал			4 квартал		
	Лесни чест тво	Е П Г У	М Ф Ц	Лесни чест тво	Е П Г У	М Ф Ц	Лесни чест тво	Е П Г У	М Ф Ц	Лесни чест тво	Е П Г У	М Ф Ц
20 20	479	0	107	90	0	1	149	0	2	637	0	112
20 21	409	0	100	169	0	48	132	0	37	661	0	93
20 22	309	48	54	250	5	61	212	4	6	99	5	13

В качестве объекта исследования выбран процесс предоставления государственных услуг Департаментом лесного комплекса Вологодской области. Предметом исследования являются методы и инструменты, используемые при формировании системы предоставления государственных услуг.

Цель работы – разработка подходов к совершенствованию системы предоставления государственных услуг в сфере лесного хозяйства Вологодской области, обеспечивающее эффективное взаимодействие органов исполнительной власти с заявителями.

Исходя из цели можно выделить следующие задачи:

1. Провести анализ современных научных публикаций российских авторов по теме исследования.
2. Разработать подходы к совершенствованию системы предоставления государственных услуг.
3. Обосновать возможность реализации предложений на примере Департамента лесного комплекса Вологодской области.

В работе использованы следующие методы исследования: анализ и синтез, индукции и дедукции, логический метод, системный подход. Информационная база – материалы научно-практических конференций, учебно-методическая литература и Интернет-ресурсы по теме исследования.

Проведен анализ современных публикаций по теме исследования. В статье Морковиной С.С., Панявиной Е.А., Ивановой А.В. «Оценка развития информационно-коммуникационных технологий в лесном хозяйстве Российской Федерации: методический подход» [2] приведена оценка эффективности использования существующих информационно-коммуникационных технологий и сложившейся организационной структуры управления лесами в области лесных отношений на уровне субъектов Российской Федерации. Для оценки эффективности применения информационно-коммуникационных технологий в процессах государственного управления лесами авторы предлагают использовать следующие критерии: «Уровень развития ИК инфраструктуры, %», «Кадровая обеспеченность ИКТ, %», «Интенсивность использования ИКТ, %». Авторами статьи также разработаны алгоритмы расчета индикаторов и критериев, которые позволяют анализировать применение в лесном хозяйстве информационно-коммуникационных технологий. Результаты данных исследований могут быть применены на практике в Департаменте лесного комплекса Вологодской области для совершенствования информационно-коммуникационных технологий.

Н. Г. Жаворонкова и Ю. Г. Шпаковский в статье «Правовые аспекты цифровизации лесной отрасли» [3] отмечают, что в настоящее время лесной комплекс в России имеет огромную потребность в цифровых технологиях управления. Цифровизация в лесной отрасли предусматривает коренную модернизацию уже имеющихся информационных программ, обмен данными с информационными системами, которые используют органы государственной власти, а также с системами и программами используемыми гражданами и бизнес-сообществом. По мнению авторов, цифровой основой для оказания государственных услуг, а также выполнения государственных функций должна

стать именно цифровизация лесного хозяйства. Для этого необходимо заменить или интегрировать разрозненные отраслевые и региональные информационные системы, используемые в настоящее время в лесном комплексе. В статье показано, что цифровизация лесной отрасли имеет свои, вполне ограниченные, возможности и критерии эффективности. Повлиять на смену технологического уклада, осуществить переход с низкого (вырубка леса и продажа древесины) уровня на более высокие (изготовление продукции), поиск новых торговых путей в лесопользовании должны сопровождать инновационную деятельность в лесопользовании. Результаты данных исследований могут быть применены на практике в Департаменте лесного комплекса Вологодской области для освоения полноценного и непрерывного цикла лесозаготовки, а также для модернизации имеющихся информационных систем.

Пескарева В. А. в статье «Предоставление государственных и муниципальных услуг в электронной форме» [4] для развития механизма предоставления государственных и муниципальных услуг в электронной форме предлагает:

1) обеспечить его организационное, законодательное, техническое и методическое обеспечение, повысить квалификацию органов власти в сфере электронного документооборота, а также распространить успешный отечественный и зарубежный опыт реализации услуг в электронном формате;

2) повысить заинтересованность граждан в использовании систем предоставления государственных услуг органами власти (посредством многообразия различных видов услуг, которые предоставляются в электронном виде, их надежности и широкой доступности, быстрого получения результата, экономической выгоды и других преимуществ). Использование результатов исследования обеспечит возможность Департамента лесного комплекса области увеличить процент заявителей, которые обращаются за государственными услугами через электронную форму.

Предложены следующие подходы к совершенствованию предоставления государственных услуг на основе информационных технологий:

– создание облачного сервиса с целью обеспечения единообразного качества предоставления госуслуг в сфере лесного хозяйства, условий их предоставления;

– оперативное реагирование Единого портала госуслуг на запросы со стороны населения, а при невозможности такого ответа – осуществление общения с операторами сервиса;

– повышение квалификации работников органов исполнительной власти по предоставлению государственных услуг с применением цифровых технологий;

– необходимость совершенствования как организационных, так и технических аспектов взаимодействия всех участников данного процесса.

Исходя из вышеизложенного, можно сделать следующие выводы. Анализ представленных научных публикаций показал, что цифровизация и совершенствование предоставления государственных услуг в лесной отрасли проходит медленно и недостаточно эффективно. Разработаны подходы к совершенствованию системы предоставления государственных услуг. Также

проведен анализ имеющихся данных по предоставлению Департаментом лесного комплекса Вологодской области государственных услуг.

Основные направления дальнейших исследований: провести анализ процесса предоставления государственных услуг в Департаменте лесного комплекса области, сравнить количество поданных заявлений через Портал Государственных услуг, в ходе личный приема и МФЦ, выявить проблемы, с которыми сталкиваются заявители и государственные служащие в работе информационных систем.

Список используемых источников:

1. Костина С. Н. Организация предоставления государственных и муниципальных услуг : учебное пособие. Екатеринбург : Издательство Уральского университета, 2019. 111 с.
2. Морковина С. С. Оценка развития информационно-коммуникационных технологий в лесном хозяйстве Российской Федерации: методический подход // ФЭС: Финансы. Экономика. 2019. №10. С. 16-25.
3. Жаворонкова Н. Г. Правовые аспекты цифровизации лесной отрасли // Право и цифровая экономика. 2021. №4. С. 77-83.
4. Пескарева В. А. Предоставление государственных и муниципальных услуг в электронной форме // Актуальные проблемы и современные тенденции социально-экономического развития региона и страны : материалы Междунар. научно-практич. конф., 13 апр. 2017 г. Саратов: Саратовский социально-экономический институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Российский экономический университет им. Г.В. Плеханова», 2018. С. 220-222.

Kremlyova N., Papushkova A.

Vologda State University

Improving the system of providing public services in the field of forestry of the Vologda region on the basis of information technologies.

Public services are a fundamental part of modern society and the basis for the implementation of socio-economic policy in the Vologda Oblast. One of the main directions of administrative reform is to improve the quality of public services in the field of forestry [1]. The article analyzes the modern literature in the field of public services, which showed that digitalization and improvement of public services in the forest industry is slow and insufficiently effective. The research results can be applied in practice in the Vologda Oblast Forestry Department to improve information and communication technologies, develop a full and continuous logging cycle, modernize existing information systems, and also help increase the percentage of applicants who apply for public services via electronic form. Approaches have been developed to improve the system of providing public services in the field of forestry, consisting in the creation of a cloud service in order to ensure uniform quality of public services; prompt response of a Single portal of public services to requests from the public; professional development of employees of executive authorities for the provision of public services using digital technologies; the need to improve both organizational and technical aspects of the interaction of all participants in this process. The main directions of further research: analysis of the process of providing public services in the Department of the Forestry Complex of the region, comparison of the number of applications submitted through the Portal of Public Services, during personal reception and MFC, to identify the problems faced by applicants and civil servants in the work of information systems.

Key words: *public services, digitalization of the process of providing public services, forestry, Forestry Department.*

УДК 338.1
ГРНТИ 06.81.25

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ, ИННОВАЦИИ И БИЗНЕС

Д. С. Крещенко

Казанский (Приволжский) федеральный университет

Статья посвящена правовым аспектам эффективного функционирования и координирования бизнес-компаний в условиях становления цифровой экономики и ее трансформации. Выделены основные инновации, направленные на развитие и усовершенствование бизнеса, с помощью которых можно разработать процесс для эффективного управления организацией. Раскрыты такие понятия, как смарт-контракт, нейромаркетинг и цифровая трансформация, кастомизация а также их влияние на развитие бизнеса в современных условиях.

смарт-контракт, нейромаркетинг, цифровая трансформация, кастомизация

С учетом быстроразвивающейся цифровой экономики организациям необходимо соответствовать новым требованиям и стремительно перестраивать все необходимые бизнес-процессы - для эффективного управления организацией, чтобы оставаться на рынке конкурентоспособными.

Исследование различных подходов к определению содержания категории «цифровая трансформация» позволяет сделать вывод, что термином «**цифровая трансформация**» необходимо обозначать определенный процесс, который направлен на введение в систему управления организации цифровых технологий, сопровождаемый оптимизацией системы управления основными технологическими процессами. Цифровая трансформация работает со всеми сферами развития организации, она служит ускорителем роста всего бизнеса в целом. Также цифровая трансформация предполагает вложение денег в высокие информационные технологии, что в последующем окупается – применение этих технологий ведут к увеличению роста продаж.

В юриспруденции наблюдается всплеск интереса к вопросам правового сопровождения сделок между хозяйствующими субъектами в цифровой среде.

Большую роль в цифровой трансформации бизнеса стали играть смарт-контракты. Они, в свою очередь, являются виртуальными документами, с помощью которых можно усовершенствовать финансовую сферу деятельности организаций. Именно благодаря смарт-контракту предоставляется возможность обойти участие различных социальных институтов общества, с помощью которых формируется рынок корпоративных ценных бумаг.

Указом Президента Российской Федерации регламентированы стратегии развития информационного общества на 2017-2030 гг.

В этом документе ключевым направлением является цифровая экономика. Термин «цифровая экономика» раскрывается как хозяйственная деятельность, в которой одним из показателей производства является информация в цифровом виде, обработка больших объемов по сравнению с традиционными формами

хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг.

Еще одним новым направлением в сфере цифрового развития бизнеса является нейромаркетинг. Нейромаркетинг активно внедряется ведущими организациями мира. Под данной инновацией стоит понимать одно из направлений в науке, которое соединяет в себе как нейробиологию, психологию, так и маркетинг. В данном случае исследуются та часть личности, которая отвечает за организационное управление в бизнесе.

Также в эпоху цифровизации происходит увеличение требовательности к специалистам по работе с персоналом. К его традиционным умениям должны добавляться способность к нетворкингу и умение обучать. Именно поэтому аналитики предполагают, что в эйчар подразделения перейдут такие специалисты как финансисты и экономисты.

Эйчар в условиях цифровизации переходит на уровень реального бизнес-партнера.

Бизнес является деятельностью, которая никогда не стоит на месте. Необходимо реализовывать новые знания, технологии и стремиться к усовершенствованию своего товара (продукта). Современные инновации необходимо активно внедрять в систему управления бизнесом - именно они способствуют экономическому развитию не только на локальном уровне, но и на международном. Конкурентное преимущество на рынке получает та организация, которая активно внедряет все тренды, реализует новые знания, применяет инновации и совершенствует модели управления бизнесом.

С учетом эпохи цифровизации компаниям, которые не принимают в оборот данные инновации невозможно будет оставаться конкурентоспособными на рынке.

Также еще одним из направлений цифровизации является введение кастомизации, которая активно внедряется во все ведущие компании мира.

Человеку в современном обществе часто стали нужны личные, индивидуальные вещи, не похожие на остальные. Именно из этой потребности отталкивались создатели концепции кастомизации в развитии маркетинга компании.

На данный момент кастомизация является одной из самых трендовых концепций маркетинга. Данную концепцию внедрила международная компания Build-A-Bear, с помощью нее компании удалось увеличить свои продажи на 23% уже в первые три месяца после введения кастомизации.

Совсем недавно, всего нескольких лет назад, кастомизация и вовсе нигде не применялась, но с учетом цифровизации общества потребность в кастомизации стала увеличиваться. Многие эксперты и исследователи заявляют, что именно кастомизация в XXI веке является одной из самых главных стратегий, которая определяет успех компании.

Сет Годин, например, говорит о том, что благодаря кастомизации компании могут выстраивать близкие и доверительные отношения с самими покупателями.

По своей сути кастомизация содержит в себе массовое производство однотипных вещей, но при этом к данным вещам добавляются отдельные, индивидуальные элементы по заказу конкретного покупателя, которые делают эти вещи уникальными и единственными в своем экземпляре.

Таким образом, массовая кастомизация является смешением массового и единичного производства.

Развитие кастомизации позволяет максимально эффективно обеспечить разнообразие товаров для потребителя. Levi_Strauss продает джинсы, подогнанные под конкретного покупателя. Andersen Windows изготавливает окна для конкретного дома. Покупатели могут увидеть свои имена напечатанными, нашитыми или выбитыми в камне.

Суть концепции заключается в создании такой системы организации производства и управления, когда на основе массового производства конечный продукт производится под индивидуального потребителя. При этом стратегия строится на том, что все затраты на доведение базовой производственной основы продукта полностью окупаются еще на стадии изготовления продукта.

Список используемых источников:

1. Указ Президента РФ от 9 мая 2017 г. N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»: [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: <https://base.garant.ru/> (Дата обращения 14.11.2022)
2. Годин С. Доверительный маркетинг. Как из незнакомца сделать друга и превратить его в покупателя. Альпина Бизнес Букс. 2008. С. 138 – 150.
3. Котин М. Частный случай: [Электронный ресурс] // Журнал "Коммерсантъ Секрет Фирмы". URL: <https://www.kommersant.ru/> (Дата обращения 10.11.2022)

Kreshchenko D.

Kazan Federal University

Digital transformation, innovation and business.

The article is devoted to the legal aspects of the effective functioning and coordination of business companies in the context of the formation of the digital economy and its transformation. The main innovations aimed at the development and improvement of business are identified, with the help of which it is possible to develop the process of the management efficiency. Such concepts as a smart contract, neuromarketing and digital transformation, customization, as well as their impact on business development in modern conditions, are disclosed.

Key words: smart contract, neuromarketing, digital transformation, customization.

УДК 005.8
ГРНТИ 50.51.17

ИНФОРМАЦИОННАЯ СИСТЕМА КАК ИНСТРУМЕНТ АВТОМАТИЗАЦИИ ПРОЦЕССОВ ПРОЕКТИРОВАНИЯ В ПРОЕКТНОЙ ОРГАНИЗАЦИИ

В. Э. Миков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время информационные системы управления проектами (ИСУП) являются неотъемлемой частью успешного осуществления проектов различной степени сложности и, как следствие, важным инструментом по увеличению эффективности работы компании в целом. Целью доклада является рассмотрение функциональных возможностей ИСУП и осуществить обоснованный выбор и внедрение информационной системы в бизнес-процесс проектной организации.

информационная система управления проектами, программное обеспечение, проектная организация

Целью работы является внедрение отечественной информационной системы управления проектам (ИСУП) в проектной организации. Данная потребность возникла в связи с необходимостью импортозамещения и перехода на отечественное программное обеспечение. Второй предпосылкой внедрения ИСУП стало требование государства ведения всех проектов в сфере дорожного строительства с помощью автоматизированного документооборота с предоставлением доступа для всех участников проекта, включая заказчика и подрядчиков.

Информационная система управления проектами представляет собой - программное обеспечение, используемое для планирования проектов, распределения ресурсов и управления изменениями. Она предназначена для повышение эффективности сотрудников компании при работе над проектами, улучшение качества управления проектами руководителями проектов, повышение эффективности управления всем портфелем проектов компании – больше проектов в срок и в рамках бюджета с меньшими затратами [1].

Деятельность проектной организации, выступающей в качестве объекта исследования, направлена на комплексное проектирование автомобильных дорог различного назначения и технических категорий, включая федеральные и городские магистрали высшей категории сложности.

Процесс выбора ИСУП для проектной организации основывался на следующих шагах:

1. Сформировать общие требования к ИСУП на основе бизнес-потребностей проектной организации
2. Проанализировать рынок ИСУП
3. Сформировать бизнес-критерии к ИСУП на основе возможностей представленного ПО и потребностей проектной организации.

4. Провести анализ по сформированным критериям и сделать вывод о наиболее подходящей ИСУП.

В результате анализа деятельности проектной организации были выявлены следующие функциональные требования:

1. Создать в информационной системе хранилище документации.
2. Автоматизировать создания документов на основе шаблонов.
3. Создать реестр замечаний к документации.
4. Автоматизировать подписание документа с помощью электронной подписи.
5. Разработать в систему доступа к данным, в зависимости от ролевой функции пользователей.
6. Разработать рабочие процессы, обеспечивающие полный жизненный цикл документации.
7. Осуществить внедрение ИС, опытную и промышленную эксплуатацию на производстве [2].

Был проведен анализ представленных сегодня на рынке ИСУП по следующим критериям:

1. Возможность удаленной работы и непрерывности проектной деятельности – основной критерий к ИС в настоящее время.
2. Наличие плагинов в офисных и САД-приложениях.
3. Гибкость настроек интерфейса (гибкий и простой интерфейс, позволяющий пользователям быстро разобраться в системе и выполнять задачи без потери времени на изучение руководства).
4. Наличие модуля планирования проектов с возможностью назначения исполнителей на роли в команде проекта.
5. Наличие модуля создания бизнес-процессов, автоматизирующих производственный процесс.
6. Возможность управления процессом: отслеживание статусов задач и документации, сроков выполнения задач и фактическими трудозатратами.
7. Возможность интеграции с другим ПО (в проектных организациях используется ПО для выполнения иных задач: расчеты, разработка чертежей и 3D-моделей, вывод документации на печать, коммуникации между подрядчиками и т.д.).
8. Возможность модификации и доработки по желанию заказчика (необходима возможность индивидуальной настройки ИСУП для получения еще больших бизнес- и организационных преимуществ).

Стоит отметить, что стоимостные критерии вторичны по отношению к функциональным критериям, следовательно, сначала выбираются ИСУП, удовлетворяющие максимальному количеству функциональных критериев, а из них в свою очередь выбирается ИСУП по стоимостным критериям. При этом в стоимостные критерии входит не только стоимость системы на момент покупки, но и стоимость индивидуальных модификаций, стоимость технической поддержке, сроки ввода ИСУП в эксплуатацию.

В результате анализа всех систем ИСУП была выбрана ИС, которая удовлетворяла большинству критериям бизнеса проектной организации — это ИСУП Vitro-CAD.

Реализована исходное коробочное решение Vitro-CAD, которая была модифицирована по требованиям заказчика, а именно:

- Оптимизирован удаленный доступ к системе.
- Добавлены новые плагины офисных приложений и CAD-система
- Модифицирован Web-интерфейс
- Информационную безопасность
- Реализована интеграция с системами планирования проектов и управления персоналом.

• Разработаны новые рабочие процессы в соответствии с регламентом организации.

Рассмотрим работу ИСУП на примере бизнес-процесса «Разработка, проверка и согласование документа ПСД» после внедрения информационной системы Vitro-CAD в проектной организации (таблица 1).

Стоит отметить, что вышеописанный процесс до внедрения ИСУП Vitro-CAD выполнялся довольно продолжительное время, и текущий статус документа зачастую был неизвестен, но после внедрения ИСУП бизнес-процесс стал автоматизирован, что уменьшило время и затраты для получения готового комплекта ПСД.

Аналогично были автоматизированы остальные бизнес-процессы жизненного цикла проектно-сметной документации проектной организации.

Результатом внедрения ИСУП стало автоматизация бизнес-процессов организации, что изменило основные показатели проектной организации, а именно, по состоянию до внедрения ИСУП Vitro-CAD и после внедрения:

1. Снизились трудозатраты на разработку и подписания ПСД на 40%.
2. Увеличение скорости согласования ПСД на 27%.
3. Фиксация текущих статусов документации на 100% (ранее отсутствовала).
4. Отслеживания жизненного цикла ПСД на 70%.
5. Хранение версий ПСД и отслеживания историй изменений по замечаниям на 100% (ранее отсутствовала).
6. Возможность согласования и подписания ПСД с любого устройства на 100% (ранее отсутствовала).

ТАБЛИЦА 1. Этапы реализации бизнес-процесса

№ этапа	Описание этапа
1	<ul style="list-style-type: none">• В форме планирования комплекта заполняются параметры, которые в дальнейшем лягут в основу рабочих процессов отдельным документам и комплектам в целом.• Каждый отдельный блок формы отвечает за планирование отдельного документа.

№ этапа	Описание этапа
	<ul style="list-style-type: none"> После того, как запланированы все документы, создаются рабочие процессы «Разработка, проверка и согласование документа ПСД» по каждому заполненному блоку. Сроки всех задач задаются на форме планирования комплекта
2	<ul style="list-style-type: none"> Получив задачу, разработчик документа должен выполнить чертеж и загрузить его в систему.
3	<ul style="list-style-type: none"> Выбрав необходимый проект из представленной структуры проекта, он должен открыть комплект, к которому относится загружаемый документ ПСД, и переместить документ в комплект. Необходимо отметить, что загружаемый документ автоматически займет место в нужном комплекте документации.
4	<ul style="list-style-type: none"> После загрузки документа в систему открывается его форма, которую должен заполнить разработчик документа.
5	<ul style="list-style-type: none"> Документу ПСД автоматически присвоится статус «В разработке».
6	<ul style="list-style-type: none"> Далее разработчик выполняет задачу «Разработать <Наименование документа ПСД>», документу ПСД автоматически присвоится статус «На проверке». Права на созданный документ ПСД изменяются на «Чтение».
7	<ul style="list-style-type: none"> После выполнения задачи на разработку документа ПСД документ отправляется на проверку Проверщику и Нормоконтролеру.
8	<ul style="list-style-type: none"> В случае, если в ходе проверки Проверщиком или Нормоконтролером или в ходе согласования Согласующими или РГ участники рабочего процесса создали замечаний к документу ПСД, разработчику придет уведомление. В Реестре замечаний хранятся все замечания к документу.
9	<ul style="list-style-type: none"> Для доработки документа ПСД сформируется задача с темой «Доработать <Документа ПСД>». Разработчику необходимо доработать документ ПСД по замечаниям проверяющих, изменить статусы замечаний и выполнить задачу.
10	<ul style="list-style-type: none"> После выполнения задачи на доработку документа ПСД документ повторно отправляется на проверку Проверщику и Нормоконтролеру с задачей принять исправления.
11	<ul style="list-style-type: none"> При получении задачи «Принять <Наименование документа ПСД>» Проверщику и Нормоконтролеру необходимо ознакомиться с исправленным по замечаниям документом, вложенным в задачу и принять исправления
12	<ul style="list-style-type: none"> При получении задачи с темой «Согласовать <Наименование документа ПСД>» РГ и ГИП необходимо ознакомиться с вложенным в задачу документом ПСД и убедиться, что все замечания сняты
13	<ul style="list-style-type: none"> В ходе прохождения рабочего процесса «Разработка, проверка и согласование документа ПСД» ГИП получает уведомления от системы На протяжении всего рабочего процесса ГИП, как руководитель, может контролировать статусы всех документов на форме планирования комплекта.

Таким образом, бизнес-процесс «Разработка, проверка и согласование документа ПСД» проектной организации был полностью автоматизирован с помощью информационной системой управления проектами.

Список используемых источников:

1. Что такое Информационная система управления проектами (ИСУП)?: [Электронный ресурс] // ADVANTA. М., 2022. URL: <https://www.advanta-group.ru/blog/cto-takoe-informacionnaa-sistema-upravlenia-proektami-isup> (Дата обращения: 17.09.2022)

2. Project Management Software: [Электронный ресурс] // Techopedia. 2022. URL: <https://www.techopedia.com/definition/13132/project-management-software> (Дата обращения 17.09.2022)

Mikov V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Information system as a tool for automation of design processes in a project organization. Currently, information about the project management system (PMIS) is part of the successful implementation of projects of great complexity and, as a result, an increase in the company's efficiency. The purpose of the report is to consider the possibility of PMIS functionality and make reasonable choice and implementation of the system in the business process of the project organization.

Key words: *project management information system, software, design organization.*

УДК 658.8
ГРНТИ 06.81.55

РАЗРАБОТКА МОДЕЛИ УПРАВЛЕНИЯ ВЗАИМООТНОШЕНИЯМИ С КЛИЕНТАМИ ПУТЕМ ВНЕДРЕНИЯ CRM СИСТЕМЫ

А. В. Митюрева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Необходимость внедрения CRM на предприятиях в современном мире обусловлена глобальными изменениями в обществе, в самих потребителях и проведением повсеместной цифровизации, то есть глубокой реорганизации бизнес-процессов с широким применением цифровых инструментов для их исполнения, которая приводит к улучшению характеристик процессов (сокращению времени выполнения, исчезновению целых групп подпроцессов, сокращению ресурсов, затрачиваемых на выполнение процессов) и/или появлению принципиально новых их качеств и свойств. В настоящий момент конкуренция на всех уровнях рынка настолько высока, что для того, чтобы компания выиграла конкурентную борьбу, она должна не только привлекать новых клиентов, но и удерживать существующих. Все это вынуждает компании – собирать информацию о клиентах, хранить истории покупок и учитывать их предпочтения, работать в сфере поддержки. В данной статье выявлены проблемы эффективности бизнес-процесса взаимодействия с клиентами в организации ООО «Cheeseria» и предложены мероприятия по стандартизации функционала работы (создание регламента) сотрудников в CRM-системе.

CRM система, цифровизация, управление, информационное обеспечение, эффективность управления, взаимоотношения с клиентами, автоматизация процессов предприятия

В связи с растущей цифровизацией пищевой индустрии внедрение передовых программных решений по упрощению процесса взаимодействия малого бизнеса и клиента становится ключевой задачей в рамках повышения эффективности управления и обслуживания и обеспечения конкурентного преимущества организации, в частности. [1]

Предлагаемые товары и услуги достигли такого уровня, на котором различие между предложениями минимальны – можно сказать, что они одинаковы и не оказывают влияние на выбор потребителя, что в корне меняет ранее применяемые инструменты маркетинга. [2]

Производители в конкурентной борьбе за каждого клиента осознают, что в текущей ситуации, стоимость привлечения нового клиента сопоставима с приносимой прибылью на одного клиента. И для выхода на устойчивое развитие необходимо увеличение продолжительности продуктивного сотрудничества клиентом для повышения количества прибыли. Это возможно только в случае перехода на клиентоориентированность как на основную стратегию компании. Повсеместная цифровизация повышает уровень взаимосвязи «клиент - компания». Сарафанное радио об одиножлы некачественном товаре или услуге может обрушить продажи, и окончательно подорвать имидж организации лишая ее многочисленных потенциальных клиентов. Это ставит перед организацией

важные вопросы: как удержать клиента, как наладить с ним взаимовыгодные отношения, как продлить жизненный цикл повторных покупок одного клиента, чем удержать его от ухода к конкурентам. Решить эти вопросы поможет внедрение CRM-системы. Внедрение CRM-системы для галочки не решит все проблемы организации, не приведет клиентов и не заставит их быть преданными вашей компании в целом или продукту в частности. CRM – это инструмент, мастерством владения которым нужно овладеть. Если говорить про современные CRM, то это набор инструментов, который помогает бизнесу выстраивать взаимоотношения с клиентами. [3]

При изменении бизнес-процесса взаимоотношениями с клиентами в компании ООО «Cheeseria» была внедрена CRM-система. Сначала была составлена и проанализирована схема As Is. После анализа схемы было выявлено 2 существенных недостатка.

В рассматриваемой компании процесс управления взаимоотношений с клиентами выполняется в ручном (бумажном) режиме. Это является основным недостатком компании в плане работы с клиентами.

1. Трафик формировался случайным образом. Компания не занималась формированием входящего трафика розничного клиента и соответственно история взаимоотношений с клиентом не велась.

2. Аналитические данные компании за последние три года (2020-2022) продемонстрировали существенное падение розничных продаж более чем на 50%, что привело к падению общих продаж более, чем на 15%. В следствии чего был сделан вывод, что розничные продажи играют существенную роль в общих продажах и управление ими необходимо.

3. Существует зависимость продаж от трафика расположенного рядом ресторана и в случае снижения потока клиентов в ресторане трафика сыроварня испытывает проблемы в продажах без возможности влиять на эту ситуации.

После всех выявленных проблем были поставлены следующие цели:

4. Найти дополнительный покупательский трафик в сфере онлайн и оффлайн продаж. Выстроить долгосрочные отношения с покупателями и получить возможность влиять на потребительские предпочтения, стимулируя тем самым дополнительный сбыт.

5. Разработка и стандартизация функционала работы (создание регламента) сотрудников в CRM-системе.

6. Организация хранения информации по заказчикам, (пол, возраст, имена, контактная информация, история покупок) которые будут заносится в единую информационную базу

7. Организовать эффективную работу отдела сбыта и отдела маркетинга с ежедневным контролем.

8. Управлять производством в соответствии с потребительскими предпочтениями.

9. Добиться независимости продаж от сторонних организаций путем развития продаж в онлайн

Выявленные проблемы заставили задуматься об автоматизации. Работа с клиентской базой, выстраивание долгосрочных отношений – важная составляющая для развития бизнеса.

Изучив рынок IT-решений в сфере управления работой с клиентской базой, руководством компании был сделан выбор в пользу программы "1С: CRM КОРП. Редакция 3.0. Это цифровое решение в полной мере отвечает задачам бизнеса ООО «Cheeseria».

Рассмотренные в ходе работы проблемы позволили не только найти наиболее релевантные решения по улучшению процесса взаимодействия с клиентами, но и стандартизировать работу сотрудников с клиентской базой в компании ООО «Cheeseria». В ходе проекта удалось организовать хранение информации по заказчикам. пол, возраст, имя, контактная информация, история покупок заносится в единую информационную базу. Каждому сотруднику доступны: управление клиентской базой, подробная характеристика о каждом клиенте и контактном лице, динамика изменения состояния отношений с клиентами, возможность быстрого ввода и доступа к информации о клиенте. Создан регламент работы с клиентами и шаблоны типовых действий, по продаже, сервисному обслуживанию рекламациям. Внедрен электронный календарь менеджера, где планируются встречи, переговоры. Рабочее время тратится эффективнее, а руководство всегда в курсе, какая загрузка сотрудников, что запланировано на рабочий день. Используются механизмы выборки клиентской базы по разным параметрам, что позволяет формировать целевые аудитории и проводить маркетинговые мероприятия. Разработан план маркетинговых мероприятий, позволяющий доносить различные предложения до определенных целевых аудиторий на длительный период, отслеживается эффективность и на основании этого формируется отчет об изменении вкусовых предпочтений отдельных категорий потребителей.

Стандартизированы типовые бизнес-процессы работы с заказчиками. При прохождении каждого этапа сотруднику понятен план дальнейших действий. Достигнута 100% получение обратной связи по входящим запросам. Директор компании контролирует работу персонала и принимает управленческие решения на основании детального анализа ситуации.

Список используемых источников:

1. Пейн Э. С., Полное руководство по продуктам CRM. Путь к совершенству управления клиентами : учебное пособие. М.: Гревцов Паблицер, 2012. 257с.
2. Носова Н. С. Как добиться лояльности клиентов, или как удержать существующих и привлечь новых клиентов : учебное пособие. СПб. : Дашков и Ко., Анлейс, 2014. 304 с.
3. Терский. А. А. Экономическая эффективность CRM-систем: [Электронный ресурс] // Новая наука: Проблемы и перспективы. 2016. N 1. С. 30–39. URL: <https://cyberleninka.ru/article/n/rol-crm-sistem-v-povyshenii-effektivnosti-deyatelnosti-organizatsii?ysclid=ladxpbzqlq707130325> (Дата обращения 17.12.2017).

Mityureva A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Development of a customer relationship management model through the implementation of a CRM system.

The need to introduce CRM at enterprises in the modern world is due to global changes in society, in consumers themselves and the implementation of widespread digitalization, that is, a deep reorganization of business processes with the widespread use of digital tools for their execution, which leads to an improvement in the characteristics of processes (reduction of execution time, disappearance of entire groups of subprocesses, reduction of resources spent on execution processes) and/or the emergence of fundamentally new qualities and properties. At the moment, competition at all levels of the market is so high that in order for a company to win the competition, it must not only attract new customers, but also retain existing ones. All this forces companies to collect information about customers, store purchase histories and take into account their preferences, and work in the support field. This article identifies the problems of the efficiency of the business process of interaction with customers in the organization of Cheeseria and considers measures to standardize the work (creation of regulations) of employees in the CRM system.

Key words: *CRM system, management, information support, management efficiency, customer relations, automation of enterprise processes.*

УДК 65.011.56
ГРНТИ 82.01.85

ВЫБОР ВРМ-СИСТЕМЫ ДЛЯ АВТОМАТИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ КРУПНЫХ ИНТЕРНЕТ ПРОВАЙДЕРОВ.

Д. А. Михайлов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обоснован выбор программного продукта для автоматизации бизнес-процессов крупного интернет провайдера. Рассмотрены требования к их использованию, проблемы, а также трудности, связанные с внедрением.

программный продукт, автоматизация бизнес-процессов

В настоящее время автоматизации бизнес-процессов в интернет компаниях является важным направлением в теории и практике управления компаний. Постоянно изменяющийся рынок, высокая скорость принятия решений, необходимость минимизация рисков требуют использования современных подходом в управлении. Автоматизация бизнес-процессов является первоочередных фактором для большого количества компаний, которые стремятся к масштабированию. В результате автоматизации бизнес-процессов руководители получают больше информации, необходимой для анализа бизнес-процессов, что в свою очередь способствует качественному принятия решений в развитии интернет компании.

Не секрет что автоматизация бизнес-процессов повышает продуктивность деятельности компании. Это позволяет обеспечить высвобождение ресурсов, которые в свою очередь необходимо для стратегического планирования. Так же автоматизация бизнес-процессов повышает эффективность деятельности компаний за счет внедрения аппаратных и программах систем. Последние тенденции развития компаний заставили руководителей осознать необходимость внедрения различных инструментов автоматизации бизнес-процессов в свою деятельность. Использование данных инструментов благоприятно сказывается на скорости и повышение точности выполнения бизнес-процессов компании. Еще одним из важных критериев является минимизация ошибок, связанных с человеческим фактором.

Целью данной работы является обоснование выбора ВРМ-системы для решения конкретных задач автоматизация бизнес-процессов в крупном интернет провайдере.

Критерии оценки ВРМ-систем:

- базовая функциональность системы и дополнительные возможности;
- количество и разнообразие используемых бизнес-процессов, гибкость их подстройки под различные задачи и масштабы;
- формат поставки, интеграция системы на предприятии;
- стоимость обслуживания и готового решения;
- возможность самостоятельной интеграции системы и ее обслуживании.

Рынок BPM-систем в России на данный момент достаточно разнообразен в данной статье рассмотрим такие системы как:

- Comindware
- ELMA
- Первая форма
- Creatio
- Битрикс

Программный продукт Comindware Business Application Platform — Low-code платформа для максимально быстрого построения прикладных бизнес-приложений с помощью бизнес-аналитиков. В основе Comindware — управление бизнес-процессами (BPMS), кейсами (АСМ), работа с данными и документами, социальное взаимодействие.

Данный продукт позволит быстро разработать гибкое ИТ-решение для управления взаимоотношениями с поставщиками (SRM) или клиентами (CRM), автоматизации операционной деятельности, документооборота.

Среди преимуществ Comindware Business Application Platform быстрая скорость создания приложений, использование типовых шаблонов, построение процессной архитектуры компании, и визуализации связей и отношений между процессами, пользовательский интерфейс на уровне лучших online сервисов, развитые средства интеграции со сторонними системами, а также поддержку исполнения творческих задач. BPM-решения на базе данного продукта от Comindware не зациклены на бизнес-процессах как традиционные BPMS. Это дает творческое пространство в работе с данной системой.

Из недостатков можно отметить ограниченные отчеты, не полный набор KPI и создание регламента (набор правил). Отсутствие мобильного приложения, роботизации процессов RPA и использование интеллектуальных технологий.

Сильным недостатком данного решения является отсутствие коробочной версии, пользователя нет возможности однократно купить «вечную» лицензию.

ELMA — одна из самых быстрорастущих систем на рынке, в которую ежемесячно добавляются новые функции. В отличие от своих конкурентов, у него нет излишеств, только его инструменты BPM, необходимые для вашего бизнеса.

Позволяет полностью автоматизировать задачи, связанные с документооборотом. Присутствует воронка продаж и интеграция с 1С. Имеется BPM Lab Messengers для Blinger — инструмент для омниканального общения с клиентами в системе ELMA через аккаунты популярных социальных сетей и мессенджеров (Telegram, Facebook, ВКонтакте, WhatsApp, Viber и другими).

Плюсом является эффективный и простой дизайн БП, который позволяет самостоятельно интегрировать данную платформу, так же наличие большого количества уроков и курсом совершенно бесплатно. Конкурентная лицензия позволяет купить лицензию на сервер, что дает возможности каждому ПК иметь все возможности.

Из минусов ELMA фокусируется на решение задач BPM, и не имеет большого количества других модулей. Также всю систему придется целиком, без дополнительных плат после.

Первая форма — на 100% российская разработка, предназначенная для автоматизации бизнес-процессов, организации единого информационного пространства для эффективных коммуникаций, обеспечения безопасного хранения и использования корпоративных данных.

Представляется большой инструментарий для настройки различных бизнес-процессов в торговых, производственных, фармацевтических и страховых компаниях, консалтинге и в других сферах. Безусловно, Первая форма — это один из самых быстро развивающихся и постоянно растущих проектов, с дополнительными качествами и возможностями.

Среди преимуществ Первой формы отметим:

- идеальную приспособленность к российским реалиям ведения бизнеса;
- управление продажами. В системе можно вести цикл продажи от первого обращения до завершения сделки, настроить KPI по процессам и сотрудникам.
- проекты под контролем;
- наличие полнофункционального веб-интерфейса и мобильного приложения;
- интеграцию с 1С, почтовыми клиентами и т.п.

Среди недостатков отмечается:

- отсутствие возможности выгружать регламенты по реализации бизнес-процессов;
- демоверсия отсутствует;
- стоимость лицензии узнается индивидуально по заказу клиента;
- это относительно новая система с ограниченной клиентской базой, пока находится на стадии развития.

Creatio (Террасофт). Интеллектуальная Low-code платформа Studio Creatio предназначена для организации эффективного взаимодействия бизнеса и ИТ. Low-code технологии позволяют выполнять автоматизацию бизнес-процессов и настройку программных решений без навыков программирования.

Плюсы Studio Creatio на рынке:

- готовые решения и шаблоны для автоматизации стандартных бизнес-задач компаний;
- интеграция приложений в цифровую экосистему организации. Расширенные возможности интеграции, а также мощная система администрирования и контроля доступа позволяют быстро и безопасно встраивать Creatio в информационную среду предприятия.

- визуальные редакторы, преднастроенные шаблоны и визарды помогают настраивать структуру данных, интерфейс и логику работы приложения.

Из минусов отметим:

- отсутствие автоматизации бизнес-процессов;
- уход компании с отечественного рынка.

Битрикс24 — это корпоративный интернет со своей CRM, социальной сетью, планировщиком, мессенджером и другими модулями. Прежде всего, среди преимуществ внедрения BPM-системы на Битрикс24 выделяют многофункциональность. Система может быть настроена под любой вид деятельности. Также отмечают скорость внедрения, закрепление инструкций и

регламентов, контроль каждого шага реализации бизнес-процессов, моделирование процессов с закреплением ответственного лица, возможность посмотреть историю, доработку и улучшение текущих регламентов. В конструкторе есть набор готовых блоков и функций: задача, событие календаря, уведомление и другие. Можно перенести элементы и соединить их в цепочки. Есть второй вариант — готовые шаблоны: счет на оплату, обработка исходящих и входящих, выдача наличных, заявление на командировку и отпуск.

Минусами данной системы является:

- отсутствие On-premise, что не дает заказчикам хранить данные на личных серверах и оплачивать модуль по подписке;
- сложный интерфейс для новых пользователей;
- огромное количество функций, пользование будет затруднено.

Подведем итог проделанной работы, можно сказать с уверенностью отечественный рынок богат разнообразными решениями для автоматизации бизнес-процессов. Все системы достаточно быстро развиваются и имеют разнообразные функции для реализации поставленных задач. Но все ли эти функции так нужны провайдеру. Отметим что провайдеры обладают собственной серверной инфраструктурой, телефонией, почтовым клиентом и специалистами обладающими навыками программирования. Основываясь на данной информации самая подходящей системой является ELMA. В данном продукте отсутствуют не нужные функции для оператора связи, платформа сконцентрирована на решении задач BPM. Внедрение системы пройдет гладко за счет большого количества уроков и документации о работе с системой. Установка решения на собственный сервер даст компании дополнительную защиту и не нуждаться в интернет соединении при работе в офисе, так же данным программным комплексом можно пользоваться удалённо.

Список используемых источников:

1. Трефиоров А. Обзор систем управления бизнес-процессами: сравнение и особенности: [Электронный ресурс]. // elma365.com., М., 2021. URL: <https://elma365.com/ru/articles/business-process-management-tools-review-comparison-and-features/> (Дата обращения 13.11.2022).

2. Игнатов А. ТОП-11 систем для управления бизнес-процессами в 2021 году: [Электронный ресурс]. // kickidler.com., 2021. URL: <https://www.kickidler.com/ru/info/top-11-sistem-dlya-upravleniya-biznes-procprocessami.html> (Дата обращения 13.11.2022).

Mikhailov D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Choosing a BPM system for automating business processes of large Internet providers. The choice of a software product for the automation of business processes of a large Internet provider is justified. The requirements for their use, problems, as well as difficulties associated with implementation are considered.

Key words: *software, project management, automation.*

УДК 65.016.7
ГРНТИ 44.01.75

СОВЕРШЕНСТВОВАНИЕ МОДЕЛИ БИЗНЕС-ПРОЦЕССОВ В ЭЛЕКТРОСЕТЕВОЙ КОМПАНИИ (НА ПРИМЕРЕ ПАО «РОССЕТИ ЛЕНЭНЕРГО»)

Э. В. Никольский

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Основная цель совершенствования бизнес-процессов - при наименьших ресурсах, получить максимум результата. Очень важно понимать, что, занимаясь повышением эффективности работы процессов в компании, процесс оптимизации длится постоянно. Вместе с развитием предприятия меняются и его процессы, которые тоже развиваются. Совершенствование бизнес-процессов должно происходить на каждом этапе жизненного цикла компании, только в этом случае компания может быть конкурентоспособна на постоянно изменяющемся рынке. Организация становится более гибкой и устойчивой к изменениям за счет отлаженных и стандартизированных процессов.

бизнес-процессы, оптимизация, энергетика, технологическое присоединение

Электроэнергетика — базовая отрасль российской экономики, на которую приходится значительная доля ВВП. Изменение спроса на энергию прямым образом зависит от темпов роста экономики России и существенно коррелирует с ВВП.

Постоянное совершенствование бизнес-процессов ПАО «Россети Ленэнерго» необходимо для обеспечения надежного и бесперебойного снабжения потребителей Санкт-Петербурга и Ленинградской области качественной и экологически чистой электроэнергией и удовлетворение возрастающего спроса на электрическую энергию и мощность.

В России электросетевые компании имеют две основные компетенции: технологическое присоединение к электрическим сетям и передача электроэнергии.

В декабре 2019 года утверждена новая стратегия Группы компаний «Россети», определяющая цели и направления развития до 2030 года.

В электроэнергетике цифровая трансформация направлена на повышение надежности и качества электроснабжения, доступности оказания услуг по передаче электроэнергии и снижению сроков по технологическому присоединению потребителей, ограничение роста цен на электроэнергию, а также развитие новых форматов (сервисов) взаимодействия с потребителями.

По оценкам ИСИЭЗ НИУ ВШЭ, цифровая трансформация обеспечит дополнительный рост производительности труда в ТЭК на 13,38% до 2030 г. (накопленным итогом) [1].

Ключевыми бизнес-процессами ПАО «Россети Ленэнерго» являются:

- услуги по передаче электроэнергии,
- услуги по технологическому присоединению к электрическим сетям,

- услуги по ремонту и техническому обслуживанию линий электропередач и трансформаторных подстанций,
- выполнение проектно-изыскательских и строительно-монтажных работ.

Вспомогательными бизнес-процессами ПАО «Россети Ленэнерго» являются:

- корпоративное управление,
- управление финансами,
- закупки, материально-техническое обеспечение,
- инвестиционная деятельность,
- техническое обслуживание и ремонты собственного оборудования,
- управление персоналом.

Описание основных бизнес-процессов Общества и ресурсов, необходимых для результативного функционирования основных процессов, выполненное по стандарту IDEF0, представлено на рис. 1.



Рис. 1. Описание основных бизнес-процессов ПАО «Россети Ленэнерго» по стандарту IDEF0

По результатам горизонтального и вертикального анализа матрицы ответственности (по функциональным ролям) сделаны следующие выводы.

Для выполнения бизнес-процессов в ПАО «Россети Ленэнерго» характерна функциональная схема, матричная структура взаимодействий. Исполнителями являются специалисты и технический персонал отделов и служб, отвечающих за определенный бизнес-процесс.

В стадии согласования подключаются заместитель генерального директора по направлениям и профильные сотрудники смежных служб и департаментов.

В связи с большим масштабом организации можно отметить забюрократизированность исполнительного аппарата с четко обозначенными полномочиями начальников служб и подразделений.

Ключевой задачей развития компании на ближайшее время является интеграция сторонних сетевых организаций в группу ПАО «Россети Ленэнерго», что приведет к увеличению доли рынка, росту количества новых абонентов и росту полезного отпуска электрической энергии, что ориентировочно позволит увеличить прибыль организации на 5% в год [2].

Применение процессного подхода для анализа и организации деятельности электроэнергетического предприятия включает:

- выделение отдельных организационных процессов,
- закрепление персональной ответственности руководителя за отдельный организационный процесс,
- разработку показателей результативности проведения каждого из процессов,
- выделение возникающих проблем и методов их решения,
- анализ отдельных процессов и их взаимосвязи.

В настоящей статье предложены пути по совершенствованию бизнес-процесса «Технологическое присоединение».

Технологическое присоединение является комплексной услугой, оказываемой сетевыми организациями юридическим и физическим лицам в целях создания возможности для потребления (выдачи) электрической мощности и предусматривающая организационное, правовое и фактическое присоединение энергетических установок (энергопринимающих устройств) заявителей к объектам сетевого хозяйства.

Бизнес-процесс «Технологическое присоединение» можно разделить на пять этапов:

- прием и обработка заявки на ТП,
- подготовка технических условий,
- подготовка правовых документов на ТП,
- исполнение обязательств по ТП,
- выдача акта о технологическом присоединении.

До 2020 года при выполнении бизнес-процесса по каждому из этапов выявлялись следующие проблемы: повышенная длительность обработки документов; бюрократизация процедур в случае нестандартных заявок на ТП; негибкий и не нацеленный на результат персонал; слабая автоматизация процесса; недостаточная системность процессов; отсутствие унификации документов; несистематизированная информация в центрах обслуживания клиентов.

Структурная схема процесса ТП, на которой показаны потоки информации и внутреннее взаимодействие, представлена на рис. 2.

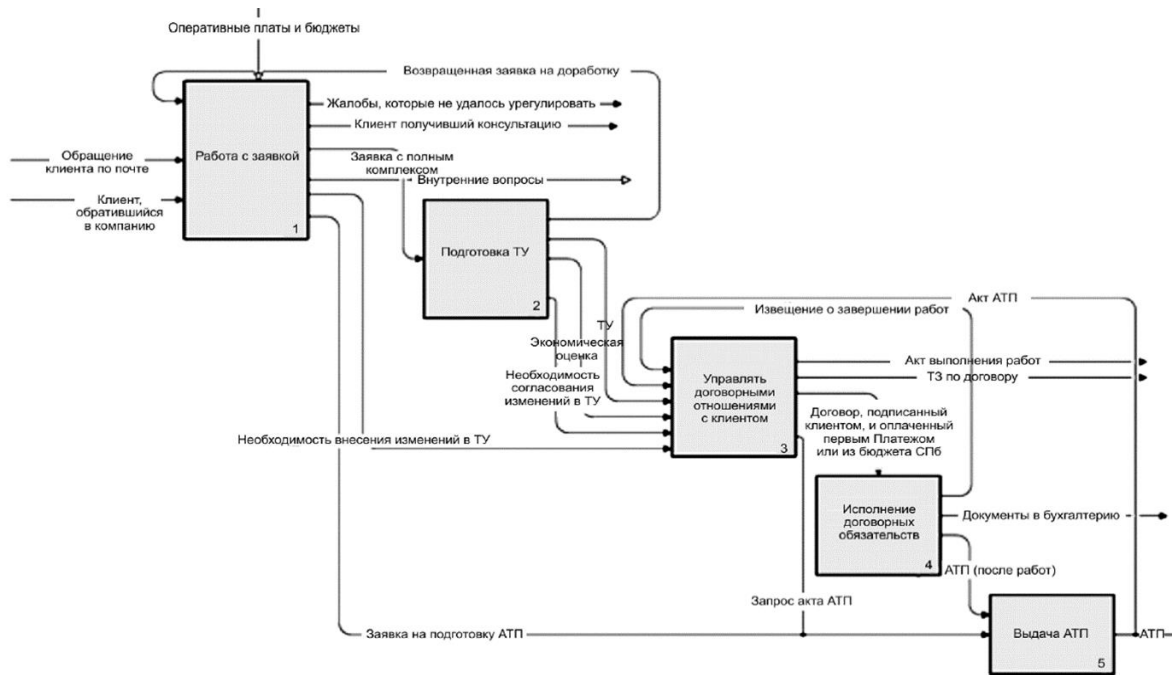


Рис. 2. Структурная схема осуществления процесса технологического присоединения

В 2012 году Россия занимала 188 место из 190 стран в рейтинге Doing Business по показателю подключения к системе энергоснабжения. В 2020 году — уже 7 строчку и продолжает ее удерживать. По показателю «подключение к электрическим сетям» в рейтинге «Ведение бизнеса – 2020» Россия получила 97,5 балла из 100 возможных. За 5 лет количество процедур, необходимых для подключения к электросетям группы «Россети» в столичных регионах, сократилось с 3 до 2, а срок подключения со 162 до 41 дня. Стоимость технологического присоединения снизилась с 93% дохода на душу населения до 5% в 2019 году [3].

По результатам декомпозирования бизнес-процесса верхнего уровня «Технологическое присоединение к электрическим сетям», сделаны выводы, что улучшения рассматриваемого бизнес-процесса «Заключение договора с Заявителем на осуществление технологического присоединения» и сокращение сроков можно достичь за счет:

- сокращения количества бюрократических процедур,
- исключения дублирования функций,
- упрощения и сокращения времени рассмотрения заявки,
- внедрения автоматизации и стандартизации процедуры.

Наиболее существенные факторы, способные вызвать нарушения сроков выполнения процесса:

1. большой объем накопленных и просроченных обязательств,
2. срыв сроков проведения подрядных работ,
3. человеческий фактор (несоблюдение внутренних регламентных документов, ошибки персонала и т.п.).

Список используемых источников:

1. Абдрахманова Г. И., Быховский К. Б., Веселитская Н. Н., Вишневецкий К. О., Гохберг Л. М. и др. Цифровая трансформация отраслей: стартовые условия и приоритеты : материалы XXII Апрельской междунар. науч. конф. по проблемам развития экономики и общества, Москва, 13–30 апр. 2021 г. / рук. авт. кол. П. Б. Рудник, науч. ред. Л. М. Гохберг, П. Б. Рудник, К. О. Вишневецкий, Т. С. Зинина. НИУ ВШМ. М. : Издательский дом ВШМ 2021. С. 80-81.
2. Впервые Россия по показателю «Подключение к системе электроснабжения» поднялась на 7 место в рейтинге Всемирного банка Doing Business: [Электронный ресурс] // ПАО «Россети Ленэнерго». СПб., 2016-2022. URL: <https://rosseti-lenenergo.ru/press/projects/74903.html> (Дата обращения 10.11.2022)
3. Годовой отчет ПАО «Россети Ленэнерго»: [Электронный ресурс]. URL: <https://storage.lenenergo.ru/iblock/3f0/3f072128e98d660de56b334792f6ea7b/Lenenergo-GO-2021.pdf> (Дата обращения 10.11.2022)

Nikolsky E.

Student of the Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Improving the business process model in an electric grid company (on the example of PJSC ROSSETI LENENERGO).

The main goal of improving business processes is to get maximum results with the least resources. It is very important to understand that, while improving the efficiency of processes in the company, the optimisation process lasts constantly. Along with the development of the enterprise, its processes are also changing. The improvement of business processes should occur at every stage of the company's life cycle, only in this case the company can be competitive in a constantly changing market. The organization becomes more flexible and resistant to change due to well-established and standardized processes.

Key words: business processes, optimisation, energy, electrical grid.

УДК 65.011.56
ГРНТИ 20.51.01

ЭФФЕКТИВНОСТЬ ВНЕДРЕНИЯ ИННОВАЦИОННЫХ ИКТ РЕШЕНИЙ НА ПРЕДПРИЯТИИ

И. В. Свиридов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Информация выступает сегодня как один из первостепенных ресурсов, значение, которого не меньше, чем значение материальных, сырьевых и других ресурсов. Использование последних в значительной степени зависит именно от состояния и использования информации. В отличие от большинства ресурсов, которые способны истощаться, информационный потенциал может использоваться многократно как коллективами, так и индивидуальными работниками. При этом он постоянно увеличивается и обогащается. Различные информационно-технические новшества следует воспринимать как средство сокращения и удешевления аппарата управления.

информация, информационный потенциал, ресурсы, информационно-технические средства

В деятельности современных предприятий информация является неперенным и первостепенным фактором нормального функционирования. При этом особое значение приобретает обеспечение оперативности и достоверности сведений, а также принятие правильных решений на основе этой информации. Существенную роль в принятии решений играет научно-техническая информация, содержащая новые научные знания, сведения об изобретениях, технических новинках предприятия и предприятий - конкурентов.

Потребность в информации различных субъектов и управленческих звеньев неодинакова и определяется прежде всего теми задачами, которые решает в процессе управления тот или иной субъект, руководитель, другой работник управленческого аппарата. Она также зависит от таких факторов, как: масштаба и важности принимаемых решений, количества и характера управляемых, регулируемых параметров; количества вариантов возможного состояния и поведения управляемого объекта; величины и разнообразия внутренних и внешних воздействий на управляемую систему, количества и качества показателей, характеризующих результаты функционирования данной системы.

Наиболее простыми и распространенными инновационными технологиями являются системы электронного документооборота (СЭД), позволяющие решать все типовые задачи для работы с документами - регистрация и ввод документов, поиск документов, обмен документами, создание отчетов, ведение архива, установка прав доступа к отдельным документам и системы в целом. Если использование информационных технологий накладывается на малый и средний бизнес крупными заказчиками или поставщиками, особенно для электронного документооборота, это в свою очередь, увеличивает их зависимость от этих потребителей или поставщиков.

В настоящем большинство предприятий устанавливают связи со своими клиентами, устанавливая терминалы любого размера, что значительно

уменьшает маневренный простор для своих клиентов. Инновации на рабочих местах помогают компаниям лучше адаптироваться к изменяющейся экономической среде [3].

Бизнес, который работает на основе современных информационно-коммуникационных технологий - это эффективный и конкурентоспособный бизнес, который будет готов к мировым интеграционным процессам и выходу на международные рынки. Предприятия, испытывающие большую экономическую эффективность, то есть выгоды от внедрения новых коммуникационных технологий, терпят больше расходы, более вероятно, будут теми, кто внедряет эти технологии.

Сфера деятельности информационных технологий имеет ряд особенностей, которые отражаются на инновационной политике:

- динамичность сферы информационных технологий;
- новизна предлагаемых продуктов и услуг, и отсюда бурный рост рынка информационных услуг;
- использование передовых технологий в сфере информационных технологий, что обеспечивает стратегические преимущества для бизнеса [1].

Разработка информационных технологий (систем) для конкретного бизнеса - это проект разработки дорожной карты цифровой трансформации бизнеса. Этот проект требует немалого финансового обеспечения, качественной и высокой подготовки специалистов и наукоемкой техники, знаний из многих областей, а именно: проектного управления, управления цифровым развитием и др.

Главное стратегическое значение информационных технологий базируется на трех ключевых концептуальных основах в стратегической теории: конкурентные силы системы, структура цепочки создания стоимости и рыночная рамка иерархии. Информационные технологии могут создать существенные и устойчивые конкурентные преимущества путем изменения характера конкуренции: изменить отраслевую структуру, создать новые преимущества и породить целый новый бизнес. Транзакционные информационные технологии - это те системы, где технология используется для обеспечения качества других видов деятельности. Информационные технологии играют важную роль в реструктуризации и создании рыночных секторов.

Можно определить такие специфики бизнеса относительно стратегических информационных технологий: экологическую, организационную, психосоциологическую, специфику конкретности решения и специфику информационных технологий. В то же время специфика информационных технологий представляет собой функционирование, сложность и успех информационных технологий.

Таким образом, эффективный и проверенный способ достижения успеха предприятия - это его постоянное развитие. Это можно сделать благодаря постоянному росту уровня инноваций. Как утверждает А. Волошин, при осуществлении инновационного процесса, интернационализированы малые и средние предприятия могут привлекать иностранный опыт в своей деятельности [2]. Как указывает И. Струтинская, большое внимание развитию цифровой экономики уделяет ЕС, считая, что уровень экономики континента будет зависеть от того, насколько эффективно предприятия применяют цифровые технологии.

Предприятия, не интегрированные в цифровые пространства, не будут принадлежать к Мировому рынку [4]. Нам трудно представить современное предприятие без использования компьютеров, Интернета и специфических ИТ-систем. Информационно-коммуникационные технологии позволяют ускорить циркуляцию и обмен информацией, собрать необходимые данные, которые являются основой для принятия решений и влияют на эффективное управление малыми и средними предприятиями. Средства массовой информации отражают трансформацию общества и освещают потенциальные возможности технологий.

Список используемых источников:

1. Епифанцева Д. Д. Факторы, влияющие на эффективность внедрения инновационных технологий на производстве: [Электронный ресурс] // Молодой ученый. 2018. № 22 (208). С. 402-403. URL: <https://moluch.ru/archive/208/50979/> Дата обращения: 11.10.2022)
2. Стеллман Э., Грин Д., Постигаг Agile. Ценности, принципы, методологии. М. : «Манн, Иванов и Фербер», 2017. 448 с.
3. Макаров В. В., Шувал-Сергеева Н. С. Управление внедрением инноваций на рынке программного продукта. СПб. : СПбГУТ, 2018. С. 128.
4. Макаров В. В., Верединский С. Ю. Организационно-экономическое проектирование инновационных процессов : учебное пособие. СПб. : СПбГУТ, 2019. С. 42.

Sviridov I.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

The effectiveness of the implementation of innovative ICT solutions in the enterprise. Information acts today as one of the primary resources, the value of which is even more than the value of material, raw materials and other resources. The use of the latter largely depends on the state and use of information. The most resources that can be depleted, the information capacity can be used repeatedly by both teams and individual workers. At the same time, it is constantly growing and enriching. Various information and technical innovations should be perceived as a means of reducing and reducing the cost of the management teams.

Key words: *information, information capacity, resources, information technology.*

УДК 658.846.5
ГРНТИ 71.31.75

E-COMMERCE. СОВРЕМЕННЫЕ РЫНКИ СБЫТА И МАРКЕТИНГ

А. С. Трищенко, С. Ю. Верединский

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С развитием телекоммуникационных технологий сформировался и развивается рынок электронной коммерции. Рынок онлайн торговли (покупки в интернете) с каждым днем создает более высокую конкуренцию офлайн торговле (покупки в магазинах). В статье рассматривается актуальность перехода компаний на стратегию e-commerce для расширения рынка сбыта, сохранения и увеличения клиентской базы. Определяется понятие маркетплейса и его роль в современном бизнесе.

маркетплейс, e-commerce, конкурентная борьба, маркетинговые операции

Сегодня ситуация на рынке вынуждает розничную торговлю переходить в интернет, так как в интернете найти и купить товар проще - можно не выходить из дома, продавец и покупатель могут находиться на разных концах света.

Малые и большие предприятия используют готовые площадки для предоставления товаров и услуг, а также закрывают собственные вопросы.

Маркетплейс - платформа электронной коммерции, онлайн-магазин электронной торговли, предоставляющий информацию о продукте или услуге третьих лиц.

В России соучаствует порядка 200 маркетплейсов, самые популярные перечислены ниже.

Для купли-продажи авто: Авто.ру; Дром.ру; Авито.

Для купли-продажи, а также аренды недвижимости: Циан; Авито; Юла.

Для поиска работы: hh.ru; Авито; Работа.ру.

Для продажи еды с доставкой: Яндекс. Еда; Деливери; Самокат.

Для продажи товаров: Ozon; Wildberries; Яндекс. Маркет.

Площадка маркетплейса – тоже бизнес, система их заработка заключается в предоставлении каких-либо платных услуг покупателям или продавцам.

Более подробно будут рассмотрены 2 самых крупных маркетплейса России Ozon и Wildberries.

За 2020 год продажи товаров на маркетплейсах выросли с 89% до 691% и продолжают расти. А в начальный период пандемии новой Коронавирусной инфекции на Ozon (ООО «Интернет решения») количество регистраций новых продавцов выросло на 60% по сравнению с 2019 годом [1].

Ежедневно на двух самых крупных маркетплейсах России продается товара более чем на 3,3 млрд. рублей. Годовой оборот на Wildberries за 2021 год составил 900 млрд рублей, годовой оборот на Ozon 445 млрд. рублей. На диаграммах ниже видно развитие маркетплейсов и их годовые обороты (рис. 1).

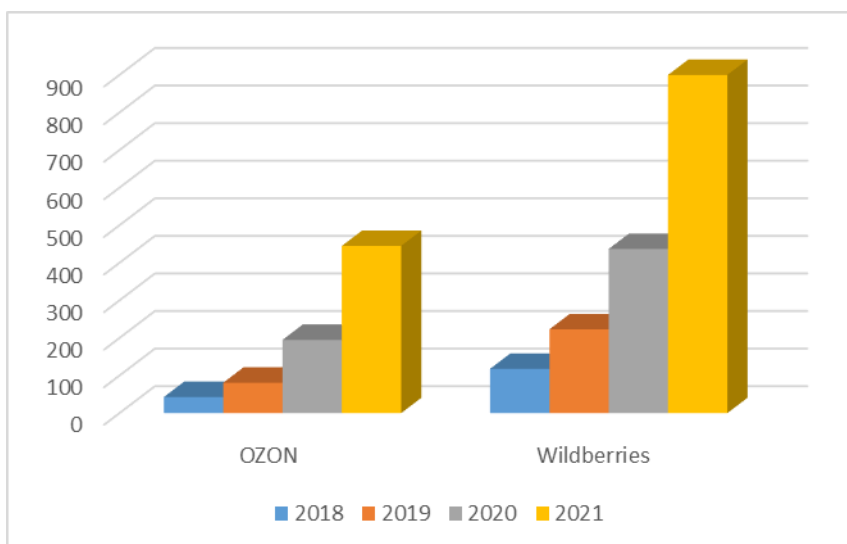


Рис. 1. Годовые обороты Озон и Вайлдберриз

Период пандемии в РФ оказался катализатором для маркетплейсов. Резкий подъем популярности такого вида бизнеса привлек большое количество ИП и ООО переориентировать свой рынок сбыта с локальной территории, где клиентом может быть человек, проживающий в радиусе 5-15 км от обычного магазина, или до 50 км специализированного тематического магазина. Маркетплейсы предоставляют возможность продавать товары по всей России, а также в некоторых странах СНГ.

Описать работу маркетплейса можно с помощью этой картинки (рис. 2):



Рис. 2. Обобщенная схема работы маркетплейса

Продавцы поставляют товары на склад маркетплейса, предварительно заключив договор и оформив карточки товаров. Покупатель находит понравившийся товар на площадке и покупает его. Маркетплейс этот товар отправляет на пункт выдачи заказов товар, указанный покупателем. Часть суммы от стоимости товара маркетплейс удерживает, чтобы покрыть расходы логистики и свои услуги, а остальную часть отправляет на расчетный счет продавца.

На сегодняшний день некоторые категории товаров имеют более 3-х тыс. карточек, и тенденции на снижение количества этих карточек не наблюдается.

[2] Продавцам сегодня предстоит решить главную задачу: «Как сделать так, чтобы карточка товара была как можно выше в поисковой выдаче?». В этот момент нужно использовать маркетинговые операции.

В некоторых вопросах продвижения сама площадка может помочь. Ozon и Wildberries предоставляют услуги рекламы. Сейчас эти услуги работают по принципу аукциона, и не всегда оправдывают надежды продавцов. Простор Интернета настолько огромен, что найти где и как прорекламить свой продукт дешево очень легко. Различные группы в социальных сетях, тематические блогеры.

Для продавцов, имеющих свои шоурумы или точки продаж, можно запустить дополнительный стимул начать покупать через маркетплейсы раздачей промокодов при покупке в магазине. Постепенно перенос своих клиентов в онлайн магазины приведет к экономии на сотрудниках и площадях. Появляется возможность находить клиентов в разных городах.

Создание своей группы в социальных сетях позволит ускорить знакомство клиентов с новой продукцией, оповещать о закрытых распродажах, и напрямую ссылать их на товар на площадках маркетплейсов.

Внешний трафик, который приходит на площадки маркетплейсов, так же будет иметь положительный эффект для продвижения продукции.

Самый важный момент во всей схеме работы с покупателями на маркетплейсе это контент. Фото, видео, описание карточки товаров обязательное условие для продажи товаров. Основной минус онлайн торговли – это отсутствие возможности клиенту потрогать товар руками и увидеть его вживую, и продавцу очень важно через фото и видео показать, что это за товар, как он работает, какого он качества, и чем он лучше конкурентов. Стоимость фотосессии и видеосъемки с обработкой сегодня стоит не более 10000 рублей за 1 товар.

Сейчас бизнес на маркетплейсах набирает обороты. До сих пор нельзя сказать, что на рынке маркетплейсов присутствует конкуренция. Все больше людей приходит в этот бизнес и имеют успехи, терпят провалы, получают опыт и работают. Стартовый капитал для такого бизнеса маленький и привлекает новых людей начать заниматься предпринимательством, а существующим компаниям трансформироваться и покорять рынок e-commerce, находя все больше клиентов.

Для начала торговли необходимо зарегистрироваться на портале маркетплейса. Указать данные юридического лица и расчетного счета в банке. Загрузить карточки товара, загрузить фото и видео контент, подробно заполнить описание и характеристики товара с использованием наибольшего количества ключевых слов. Запустить рекламу, и провести маркетинговые операции по продвижению товара.

В качестве примера можно рассмотреть компанию ТК «Домос». Компания сегодня имеет актуальную линейку товаров из 38 артикулов. Месячный оборот на маркетплейсах более 2-х миллионов рублей.

Список используемых источников:

1. 2019 год для основных российских маркетплейсов: данные "СПАРК": [Электронный ресурс] // E-pepper by Aero. М., 2010-2020. URL: <https://e-pepper.ru/news/2019-god-dlya-osnovnykh-rossiyskikh-marketpleysov-dannye-spark-.html> (Дата обращения 10.11.2022).
2. Аналитическое агентство MPstat: [Электронный ресурс]. М., 2022. URL: <https://wiki.mpstats.io/> (Дата обращения 10.11.2022).

Trishchenko A., Veredinsky S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

E-commerce. Modern markets and marketing.

With the development of telecommunication technologies, the e-commerce market has been formed and is developing. The online trading market (online shopping) creates higher competition for offline trading (shopping in stores) every day. "e-commerce", maintaining and increasing the customer base. The concept of a marketplace and its role in modern business are defined.

Key words: marketplace, e-commerce, competition, marketing operations.

УДК 004.056.53
ГРНТИ 81.93.29

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА РЫНКЕ ЦЕННЫХ БУМАГ

А. А. Хачатрян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются способы трактовки ценных бумаг, выполнен анализ законодательного характера изучаемого вопроса, рассмотрены труды отечественных и зарубежных авторов, специализирующихся на изучении информационной безопасности рынка. Рассматриваются кибератаки, основные риски, связанные с ними и способы их предотвращения.

рынок ценных бумаг, информационная безопасность, цифровизация экономики, экономические риски, кибератаки

Процедура становления рынка ценных бумаг представляет собой наиболее важный аспект в рамках стабильного развития экономики. Проведение научного анализа деятельности мировых экономик помогает сделать вывод о важности использования ценных бумаг не только с точки зрения эффективного распределения.

Основной функционал ценных бумаг сконцентрирован на реализации операций по перераспределению капитала. Именно ценные бумаги в рамках макроэкономики способны вносить значимые экономические преобразования. Для увеличения доходов граждан и организаций на микроэкономическом уровне ценные бумаги выступают в роли альтернативного варианта банковских продуктов.

Актуальность исследуемого вопроса подтверждается значительным количеством дискуссий в рамках экономической науки, информационной безопасности и финансовой сферы. Не менее важным аспектом является популяризация изучаемого вопроса в научном сообществе, значительном количестве исследований, публикаций и научных работ.

Финансовые учреждения являются основными объектами кибератак. Финансовые компании трансформируются в связи с появлением новейших технологий. Внедрение новых технологий не только приносит реальные выгоды компании и её клиентам, но также приводит к новым рискам информационной безопасности компаний.

Финансовые учреждения, в отличие от большинства других, хранят особенно конфиденциальную и ценную информацию, которая манит как преступные группы, так и спецслужбы иностранных государств. От банков до брокерских компаний - киберпреступники нацеливаются на финансовые учреждения с целью хищения данных о сотрудниках, клиентах и бизнесах. Они угрожают как репутации компаний и безопасности клиентов, так и операционной деятельности компании в целом [1].

Теоретическая и методологическая база исследуемого вопроса, связанного с информационной безопасностью рынка ценных бумаг опирается на труды отечественных и зарубежных авторов, специализирующихся на вопросах

изучения природы корпоративных ценных бумаг и их информационной безопасности.

Среди западных исследователей можно выделить: Левайна С., Андерсона С.В. и др. Теоретическая составляющая данного исследования имеет в основе труды российских исследователей: Алехина Б.И., Миркина Я., Матовникова М., Михайленко М. Н., Шершеневича Г. В. и других.

Важным документом для изучения ценных бумаг в целом, является ФЗ «О рынке ценных бумаг» № 39-ФЗ. Вторая статья Закона о рынке ценных бумаг содержит в себе информацию о различных видах ценных бумаг [2]. В тексте статьи фигурируют такие виды ценных бумаг как акция, облигация, депозитарные расписки и опционы эмитента. А также иные ценные бумаги, названные в таком качестве в законе или признанные таковыми в установленном законом порядке.

Стоит учитывать, что согласно содержанию 128 статьи ГК РФ, ценные бумаги принято рассматривать в качестве объектов гражданского права [2]. Они могут отличаться по форме и физическому характеру. Учитываются как документарные ценные бумаги, так и бездокументарные ценные бумаги. Подобная градация не лишает ценности каждого из указанных документов. Для понимания и оценки бумаги важна не физическая, а экономико-правовая составляющая в рамках имущественного права.

Оценка стоимости ценной бумаги характеризуется следующими параметрами: размерами её доходности, и надёжностью эмитента. Динамика уровня доходности ценной бумаги также рассматривается в рамках финансовой устойчивости эмитента. Уровень стоимости ценной бумаги можно оценить по текущему уровню её доходности, и по доходности, которую можно спрогнозировать на ближайшее время. Именно этот фактор лежит в основе рисков, связанных с повышенной активностью кибератак и создания условий для их предотвращения [3].

Сложность измерения рисков информационной безопасности представляет собой ещё одну проблему.

Поставщикам финансовых услуг, таким как банки, кредитные союзы, компании, выпускающие кредитные карты, и инвестиционным фирмам доверена личная информация (PII) каждого клиента. Высокая ценность этих данных в даркнете делает этот сектор привлекательной мишенью для киберпреступников [4].

В 2019 году мировой рынок финансовых услуг оценивался примерно в 22 триллиона долларов [5, с. 36]. В этой отрасли наблюдается устойчивый рост безналичных платежей, особенно после коронавируса, захватившего мир в 2020 году. Безналичные платежи множатся из-за растущего проникновения Интернета и использования мобильной связи в развивающихся странах и глобального перехода к схемам мгновенных платежей в режиме реального времени.

Достижения в области интернет-банкинга, мобильных приложений и мгновенных платежей требуют новых технологий. Повышенное использование технологий неизменно увеличивает вектор атак отрасли и создаёт новые уязвимости.

Растущий уровень кибератак на финансовые компании является свидетельством того, как этот сектор обратился к технологиям для решения многих проблем, с которыми сталкивается. Чтобы увеличить долю рынка, многие финансовые учреждения ориентируются с помощью больших данных. Используя социальные сети, базы потребительских данных и новостные ленты, финансовые компании могут лучше понимать своих клиентов и привлекать новых.

Неотъемлемые риски, связанные с технологиями, создают давление на академические круги, требуя создания новых и постоянно растущих кадров высококвалифицированных специалистов в области информационной безопасности. В борьбе за то, чтобы оставаться на шаг впереди киберпреступников, финансовая индустрия, вероятно, споткнулась на стартовых позициях. В блоге веб-сайта Университета Сан-Диего говорится: “В то время как финансовые учреждения знают, что безопасность является проблемой, многие из них не подготовлены и не знают, как бороться со всё более изощрённой тактикой киберпреступников [5].

Существует два типа компаний, оказывающих финансовые услуги. Те, кто подвергся кибератаке, и те, кто подвергнется ей в будущем. Финансовым компаниям настолько сложно защитить данные клиентов, что многие из них столкнулись с многочисленными нарушениями.

В период с 2009 по 2019 года некоторые из самых узнаваемых имён в этом секторе были взломаны более одного раза. American Express и SunTrust Bank были взломаны пять раз, а Capital One и Discover были взломаны по четыре раза каждый за этот период [6].

Согласно отчёту IBM Security Cost of a Data Breach Report, в 2019 году средняя стоимость одного нарушения в сфере финансовых услуг составила 5,86 миллиона долларов. Эта стоимость за нарушение уступает только отрасли здравоохранения и почти в полтора раза превышает расходы государственного сектора [6].

Заключение. Экономическая защищённость любого субъекта экономики как на глобальном, так и на национальном уровне не может обеспечиваться за счёт использования ресурсов других субъектов рынка. Только при сохранении целостности отдельных субъектов обеспечение безопасности в области экономических отношений будет эффективным.

К основным предложениям по совершенствованию механизмов и повышению экономической безопасности рынка ценных бумаг можно отнести:

- проведение анализа и мониторинга индексов рынка ценных бумаг;
- принятие мер, по повышению экономической безопасности на основании роста (снижения) индексов рынка ценных бумаг;
- более тщательное осуществление правового регулирования рынка ценных бумаг, тем самым защищая права инвесторов и резидентов;
- привлечение финансовых средств крупных компаний, что в свою очередь позволит наладить стабильность и сохранять экономическую безопасность рынка ценных бумаг и др.

Список используемых источников:

1. Сидельникова Н. В., Беседина Т. В. Информационная безопасность // Образование. Карьера. Общество. 2018. № 1 (56). С. 71-72.
2. О внесении изменений в Федеральный закон «О рынке ценных бумаг» и отдельные законодательные акты Российской Федерации»: Законопроект № 57 618877-7. URL: <https://sozd.duma.gov.ru/bill/618877-7/> (Дата обращения 13.11.2022 г.)
3. Грачева Е.А. Информационная безопасность // The Newman in Foreign Policy. 2020. Т. 3, № 54 (98). С. 57-59.
4. Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Информационная безопасность: учеб. пособие. Нижний Новгород : НГУ им. Н.И. Лобачевского, 2017. 198 с.
5. Красов А. В., Штеренберг С. И., Фахрутдинов Р. М., Рыжаков Д. В., Пестов И. Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // Т-Сomm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36-40.
6. Буйневич М. В., Покусов В. В., Израилов К. Е. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации // Информатизация и связь. 2021. № 4. С. 6673. DOI: 10.34219/2078-8320-2021-12-4-66-73.

Khachatryan A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Information security in securities market.

The article discusses ways of interpreting securities, analyzes the legislative nature of the issue under study, considers the works of local and international authors specializing in the study of information security of the markets. Cyberattacks, main risks associated with them and ways of preventing them are considered.

Key words: *securities market, information security, digitalization of the economy, economic risks, cyberattacks.*

УДК 65.011.56
ГРНТИ 82.01.85

АВТОМАТИЗАЦИЯ ПРОЦЕССА УПРАВЛЕНИЯ РАБОТЫ КОМАНДЫ НА ПРИМЕРЕ ПРОЕКТА BONCH AVALANCHE FORECAST (BAF)

А. И. Хорахордин, А. М. Хохлова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассказана важность автоматизации процесса внутреннего взаимодействия между разработчиками, описаны конкретные программные продукты и их актуальность, а также влияние данных методик на процесс разработки микросервисных приложений на примере проекта Bonch Avalanche Forecast.

автоматизация управления, управление проектами, командная работа, облачные вычисления

1. Введение

Современные инфокоммуникационные услуги имеют большое количество функций. Для разработки проекта требуется много разнопрофильных специалистов, при этом с приходом современных концепций микросервисной архитектуры компетенции конкретных разработчиков сильно видоизменяется. Каждый участник команды отвечает за отдельный процесс. Поэтому управление микросервисной архитектурой становится отдельной задачей, для решения которой требуется devOps инженер. А для организации работы разнопрофильной команды разработчиков и решения различных специфических задач требуется большая система управления и менеджмента от руководителя проекта.

Эффективность автоматизации процесса заключается в мобильности и высокой концентрации специалистов на задачах и выполнении плановых работ, направленных на проект. Чтобы ускорить выполнение ежедневных задач и обеспечить большую прозрачность процессов проекта необходимо использовать программное обеспечение для управления проектами, в небольших командах для этого используется Trello, функции работы более подробно описаны в пункте 2.

В связи с быстрым ростом инфраструктуры проекта необходимо организовать базу знаний где собрана вся документация продуктов, описание процессов работы каждой команды, организация сетевой инфраструктуры и т.д. Для этого была разработана система хранения данных в облаке Nextcloud, подробнее о процессах программного обеспечения в пункте 3. Особенность такого решения – наличие готовой платформы для коллективной работы. Имея доступ к облаку, каждый человек в команде может вести работу независимо от других.

Такие инструменты позволяют автоматизировать большинство рутинных задач, делая работу всей команды более эффективной. При этом доступ к проекту обеспечивается из любой точки мира, где есть интернет, также данное решение комфортно для администраторов: достаточно настроить права каждого участника и отслеживать внесенные правки. Новые люди, которые приходят в

проект, могут начинать работу с первого дня, так как все процессы описаны, а документация и архитектура в виде диаграмм сразу дает представление о том, чем занимается команда.

На основании вышеописанного можно сделать вывод, что программный продукт должен быть прост в использовании и внедряться в рабочий процесс без долгой адаптации со стороны персонала, должен осуществлять безопасное хранение данных и быть доступен только причастным к определенному проекту сотруднику.

2. Trello:

Это облачная программа для управления проектами, которая преимущественно используется небольшими компаниями и стартапами. Бесплатность данного приложения, это существенное преимущество над его аналогами.

Весь интерфейс выстроен на основе канбан-досок. Администратор проекта может легко организовать комфортную среду для работы, сформировать список каждой команды специалистов, в которые можно будет поместить карточки с задачами, установить их срок и отслеживать на каком этапе находится разработка [1].

Программный продукт создан таким образом, чтобы каждый член команды мог планировать (создавать, перенаправлять и выполнять задачи, а также планировать спринты и распределять задания в своей команде), отслеживать (выставлять приоритеты в зависимости от сроков поставленной задачи, обсуждать работу в команде в условиях абсолютной прозрачности) и выполнять необходимые функции для проекта.

Главное преимущество данного программного обеспечения это возможность скачать приложение для смартфона или ноутбука и пользоваться системой в пути.

3. Nextcloud:

Nextcloud — это open source программное обеспечение, которое позволяет создавать облачное хранилище, отправлять туда файлы и контролировать их место и условия хранения.

Была разработана оптимальная схема хранения данных в облаке

Существует множество приложений, которые можно интегрировать и использовать совместно с Nextcloud. Чтобы наладить продуктивное общение в команде необходимо использовать приложения для обмена сообщениями. Также важно не забывать и о словесном общении. Видеоконференции и регулярные брифинги по проектам могут пригодиться для разрешения недопонимания и повышения качества общения. Для организации этого процесса в данном программном обеспечении есть возможность установить NextCloud Talk [2].

Данный продукт дает возможность разработчикам совместно работать над проектом в онлайн формате.

Важной особенностью использования Nextcloud в качестве облачного хранилища является безопасность данных. Информация хранится на собственном сервере, и администраторы могут сами настроить защиту,

разграничить права доступа. Важно разграничить права доступа и на внутренней инфраструктуре проекта. Для каждого участника команды создается соответствующий пользователь в системе управления базами данных, которому раздаются необходимые права. Преимущество такого подхода: его простота и прозрачность. По логам системы управления базами данных легко увидеть, какие запросы выполняют пользователи.

4. Автоматизация работы внутренней инфраструктуры

Следующее, что необходимо организовать для автоматизации процесса разработки - создать систему автоматического развертывания микросервисов, которая реализуется с помощью Docker, Docker Hub, Jenkins и Git.

Автоматизация состоит в том, чтобы контейнер с кодом, будь то скрипт или приложение, разворачивался на машине сразу после того, как программист сделает push в GitHub.

Для этого сначала на рабочую машину устанавливается Docker и Jenkins.

Чтобы снизить нагрузку на основную машину, выполнение сборки образов для развертывания будет производиться на отдельной виртуальной машине. Далее, в Jenkins необходимо создать пайплайны и назначить агентов, которые будут автоматически разворачивать наши контейнеры.

Для успешной автоматизации, в репозитории разработчика должны находиться DOCKERFILE, описывающий наш контейнер и Jenkinsfile, описывающий наш пайплайн. (Jenkinsfile также может быть написан и в самом Jenkins, но все же удобнее, когда можно редактировать эти файлы по мере необходимости, не выходя из репозитория разработчика).

Сам Jenkinsfile можно разделить на 2 части: часть, которая собирает образ и делает push в DockerHub, и часть, которая удаляет старый контейнер и образ и создает новый контейнер с помощью образа из Dockerhub.

Успешность создания образа, его push в DockerHub и создания нового контейнера можно отследить через Web-интерфейс Jenkins. Также внутри самого пайплайна можно организовать уведомления в Telegram через бота посредством функции post и url-запроса для отправки сообщения (например, в чат команды разработчиков).

Итогом исследованной работы стала разработка окружения для автоматизации процесса управления командой разработчиков, которое состоит из облачной платформы для хранения документации проекта и удаленного взаимодействия разработчиков внутри команды, также создание облачного программного продукта для обеспечения прозрачности проекта и удобного решения поставленных задач.

Создание окружения с помощью Jenkins в сочетании с Docker позволяет существенно сократить время на развертывание микросервисов, а также снизить нагрузку на команду программистов, предоставляя им больше времени на написание кода и упрощая отладку программного продукта.

В ближайшем будущем планируется проанализировать другие решения для автоматизации управления внутренней работы, исследовать новые методики и выявить оптимальную для проекта Bonch Avalanche Forecast (BAF).

Список используемых источников:

1. Руководство Trello: [Электронный ресурс] // Trello.com. 2022. URL: <https://trello.com/guide> (Дата обращения: 10.11.2022).
2. Обзор документации Nextcloud: [Электронный ресурс] // Nextcloud.com. 2022. URL: https://docs.nextcloud.com/server/stable/admin_manual/apps_management.html (Дата обращения: 10.11.2022).
3. Документация Docker: [Электронный ресурс] // Docs.docker.com. 2013-2022. URL: <https://docs.docker.com/engine/reference/builder/> (Дата обращения: 10.11.2022).
4. Документация Jenkins: [Электронный ресурс] // Jenkins.io. 2022. URL: <https://www.jenkins.io/doc/book/using/> (Дата обращения: 10.11.2022).

Khorakhordin A., Khokhlova A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

Automation of the team work management process on the example of the Bonch Avalanche Forecast (BAF) project.

The importance of automating the process of internal interaction between developers is described, specific software products and their relevance are described, as well as the impact of these techniques on the process of developing microservice applications using the Bonch Avalanche Forecast project as an example.

Key words: management automation, project management, teamwork, cloud computing.

УДК 65.011.56
ГРНТИ 06.81.12

КЛАССИФИКАЦИЯ «ЧАТ-БОТОВ» И АНАЛИЗ ЖИЗНЕННОГО ЦИКЛА

Д. А. Черепанов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье анализируются различные классификации чат-ботов. Описан и проанализирован жизненный цикл чат-ботов, который включает в себя создание, тестирование и реализацию.

чат-бот, мессенджер, мобильное приложение

Чат-бот – это компьютерная программа, фактически виртуальный собеседник, который функционирует на основе установленных правил и алгоритмов. Он умеет имитировать человеческое поведение, общаясь с потенциальным клиентом.

Работает на основе:

- Мессенджеров;
- социальных сетей;
- платформ Slack, Skype и т.д.;
- сайтов.

Чат-боты ведут переписку и отвечают на вопросы, которые возникают у пользователей или же рассказывают о полезной информации или функциях той или иной компании. Начать переписку с чат-ботов можно в любой момент времени. Это очень удобно, как для клиентов, так и для бизнеса целевая аудитория которых, склонна совершать импульсивные покупки.

Существуют разные виды чат-ботов. Одна группа нацелена на информирование потенциальных клиентов, другая группа больше нацелена на продажи, третья же используется исключительно в целях личного помощника. Выбор группы зависит от функционала, заложенного в чат-бот. Хотя, другими словами, чат-бот, является хорошо настроенной программой-помощником.

Чат-боты классифицируют по алгоритмам и видам как представлено на рис. 1 и рис. 2.

Рассмотрим каждый их алгоритмов подробнее:

1. Ограниченный. Такой чат-бот следует четко последовательности, и если что-то пойдет не по заранее заготовленному скрипту, то чат-бот просто сломается и выдаст ошибку. Такую программу можно создать, используя специальные сервисы, которые как раз помогут создать и настроить таких простых чат-ботов совершенно бесплатно. Это позволит протестировать и понять, нужен ли такая программа-помощник бизнесу.

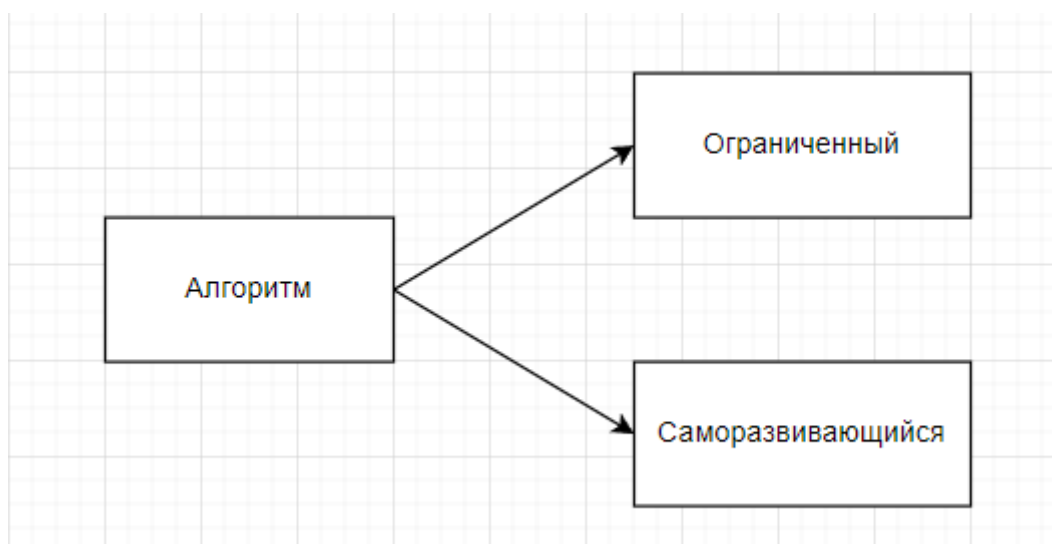


Рис. 1. Классификация чат-ботов по алгоритмам

2. Саморазвивающийся. Такой тип чат-бота, является сильно улучшенной версией. В основе заложена искусственная нейронная сеть, способная к самообучению. Общение с таким чат-ботом более быстрое и приятное, и с каждым диалогом нейронная сеть становится умнее. Такой помощник разрабатывается для крупных предприятий, так-как затраты на его разработку, поддержку и управление существенно-выше затрат ограниченного чат-бота.

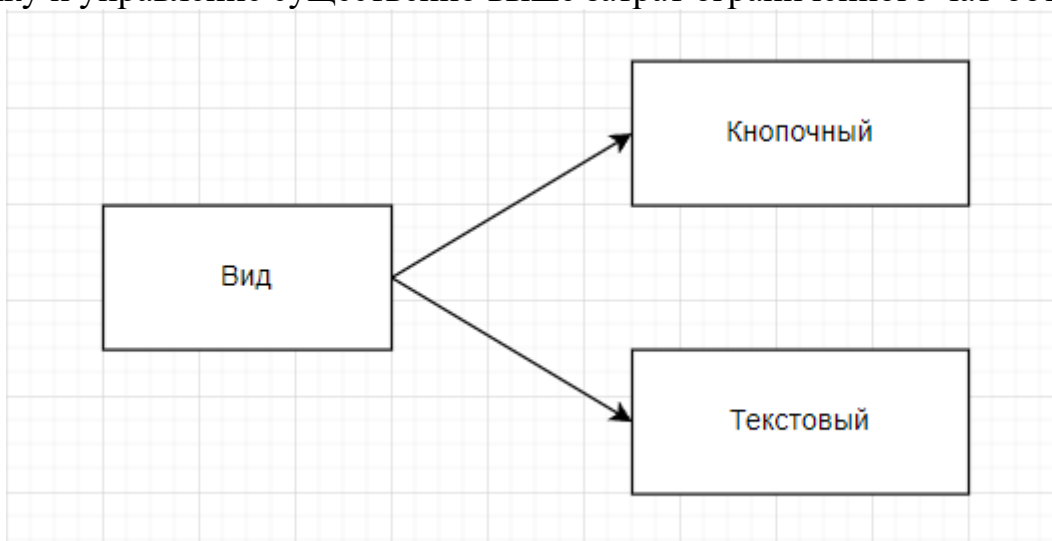


Рис. 2. Классификация чат-ботов по виду

Рассмотрим каждый их алгоритмов подробнее:

1. Кнопочный. Для общения с ботом, пользователю заранее прописывают все варианты ответов, которые по мнению разработчиков, могут потребоваться пользователю, и далее разработчик закладывает верные ответы в самого бота. Большая часть чат-ботов работает по такому принципу. Это позволяет сильно сэкономить на разработке.

2. Текстовый. Программа способная распознать ключевые слова в запросе пользователя, а после вывести готовые шаблоны ответов, по ключевым словам, из базы данных. Чаще всего это саморазвивающийся чат-бот, но бывают и

смешенные модели в качестве ответа на запрос, пользователь получит кнопочные варианты вопросов, а уже они приведут программу к правильному ответу.

В проектах, больших и малых, зачастую используются методологии разработки программ, которые необходимы для верного проектирования, разработки и последующего сопровождения программного продукта. Эта методология может полностью отсутствовать в мелких проектах, для создания, которых необходимо от одного до двух разработчиков, но кардинально меняется подход, когда для разработки программного продукта задействуется команда разработчиков, аналитиков и тестировщиков. В данном случае необходима строгая методология разработки и реализации проектов, называемая жизненным циклом.

Шаги жизненного цикла чат-бота, представленные на рис. 3.



Рис. 3. Жизненный цикл чат-ботов

Рассмотрим каждый шаг подробнее:

1. **Требования.** Необходимо собрать данные: о потенциальном рынке, целевой аудитории, провести анализ преимуществ и недостатков внедрения чат-бота.

2. **Спецификация.** Необходимо разработать спецификацию продукта, которая будет определять функции и возможности чат-бота.

3. **Сценарий.** На третьем шаге, важно правильно разработать ветку диалогов по которым будет функционировать чат-бот. Заготовленные реплики должны быть максимально похожи на человеческую речь, а также обрабатывать широкий диапазон ответов от пользователей.

4. **Архитектура.** На данном этапе происходит создание инженерного проекта диалоговой системы. В этот шаг, также включается «фронтенд» и «бекенд» разработка.

5. **Разработка.** На пятом этапе, Разработчики создают программный продукт используя собранные данные с предыдущего шага.

6. Тестирование. Тестирование тесно переплетается с процессом разработки. Важно знать принципы работы платформы на котором будет базироваться чат-бот для быстрого и эффективного тестирования.

7. Развертывание. Этап, который включает в себя размещение программы на серверах, которые должны обеспечить бесперебойную работу на всем этапе жизни программы.

8. Публикация. Завершающий шаг разработки, доступен только после полного тестирования и прохождения всех требований платформ, на котором будет работать программа.

9. Мониторинг. Когда чат-бот будет опубликован, важно контролировать процесс обработки пользовательских вопросов, и следить за правильностью данных ответов.

10. Продвижение. На этом шаге необходимо привести трафик чат-боту.

11. Анализ. Заключительный этап реализации чат-бота, на котором нужно провести анализ производительности и результатов работы программы.

Все полученные данные в ходе одиннадцатого шага, могут быть возвращены в процесс развития чат-бота, для его постоянного совершенствования, если это ограниченная программа, но существуют и саморазвивающиеся, которые могут самостоятельно обновлять себя.

Данный жизненный цикл при использовании его с крупной задачей, поможет достичь успехи с большей вероятностью, так как в нем учтены почти все шаги разработки и реализации программного обеспечения, которые будут отвечать всем требованиям и в конечном итоге смогут помочь предприятию.

Список используемых источников:

1. Компания-разработчик в области искусственного интеллекта: [Электронный ресурс] // Expert.ai. 2022. URL: <https://www.expert.ai/blog/chatbot/> (Дата обращения 25.09.22).
2. Компания-разработчик в области искусственного интеллекта: [Электронный ресурс] // BotsCrew. 2022. URL: <https://botscrew.com/blog/e-commerce-chatbot-for-customer-service-automation/> (Дата обращения 27.09.22).
3. Разработчики платформы по созданию корпоративных чат-ботов: [Электронный ресурс] // Botcore.ai. 2022. URL: <https://botcore.ai/blog/evolution-of-chatbots/> (Дата обращения 27.09.22).
4. Платформа для электронной коммерции: [Электронный ресурс] // Bigcommerce. 2003-2022. URL: <https://www.bigcommerce.com/blog/chatbots/> (Дата обращения 07.11.22).

Cherepanov D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Classification of chatbots and life cycle analysis.

The article analyzes various chatbot filters. The life cycle of chatbots, which includes creation, testing and testing, is described and analyzed.

Key words: *chat bot, messenger, mobile application.*

**ГУМАНИТАРНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОГО
ПРОСТРАНСТВА**

**Секция 6.1.
Вопросы регионоведения и межкультурных коммуникаций в
цифровую эпоху**

УДК 993.32.1400.
ГРНТИ 23.40.11.25.

МЕЖДУНАРОДНАЯ ДЕЯТЕЛЬНОСТЬ ХРИСТИАНСКИХ РЕЛИГИОЗНЫХ ОРГАНИЗАЦИЙ В ЕВРОПЕ

Н. А. Бондарь

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В конце двадцатого века исследователями прогнозировалось, что будущее религий в Европе печально и 21 столетия станет для неё последним. Однако ситуация к 21 веку соответствовала прогнозам с точностью до наоборот. Перемены действительно наступили, религия не только начала возвращается в обычную жизнь людей, но теперь и религиозные организации претендуют на роль актора в международных отношениях. Сегодня вероисповедание в Европе является свободным, и теперь люди могут выбирать, во что верить.

религия, христианство, международные отношения, Европа

По данным Евростата в Европе на 2018 год религией с наибольшим количеством последователей по-прежнему является христианство, где 44.5% населения – последователи католической конфессии, а 25% населения – последователи других христианских конфессий.

Основа моральных ценностей, система воспитания и мировосприятие, всё это имеет глубокие религиозные корни. Религия таким образом является одной из частей складывания менталитета народов, хотя этого мы можем не понимать или не замечать. Но по этой причине религия оказывает долгосрочное влияние на людей, и отражается на формировании направлений внутренней и внешней политики той или иной страны.

В состав Евросоюза входят страны, жители которых относятся к разным конфессиям, в связи с этим, христианские религиозные организации пытаются утвердить своё влияние в процессе евро-интеграции. И стоит отметить, что в наши дни их роль внутри Евросоюза продолжает расти [].

Деятельность данных организаций также многообразна, как и количество христианских конфессий. И так как католическая вера на данный момент является самой распространённой, то и организаций подобного рода в Европе значительно больше. По этой причине международная деятельность христианских организаций будет разделена на две категории: деятельность католических и некатолических христианских организаций.

Деятельность католической церкви направлена в разные русла, по этой причине существует огромное количество организаций, призванных для выполнения данных задач. По этой причине в данном исследовании будут рассмотрены самые влиятельные организации. Некоторые организации выполняют в себе только одну функцию, другие же сочетают в своей деятельности несколько задач. Католическая церковь существует уже на протяжении двух тысяч лет и до нас также дошли и организации, которые также

действуют на протяжении сотен лет. Объединяет и курирует работу этих организаций – Святой Престол, в связи с чем, непосредственным главой большинства католических организаций является Папа Римский.

И говоря о древнейших организациях римской католической церкви, в первую очередь необходимо упомянуть орден рыцарей-госпитальеров имени Святого Иоанна. Признанный суверенным с 1113 Папой Римским, Мальтийский орден существует по сей день. Однако по поводу статуса данного ордена до сих пор идут споры. Орден Святого Иоанна является признанным субъектом международного права и обладает дипломатическим суверенитетом. Он имеет статус организации-наблюдателя при ООН и в Совете Европы. Но в данном исследовании орден Мальтийских рыцарей рассматривается не как государственное образование, а как религиозная организация. В этом статусе Орден святого Иоанна имеет огромное влияние в международных отношениях. Активность Мальтийского Ордена на данный момент осуществляется в 120 странах, оказывая помощь нуждающимся людям посредством своей медицинской, социальной и гуманитарной деятельности. Из года в год его широкий спектр социальных проектов обеспечивает постоянную поддержку забытым или исключенным членам общества. Она особенно заинтересована в оказании помощи людям, живущим в условиях вооруженных конфликтов и стихийных бедствий, путем оказания медицинской помощи, ухода за беженцами и распространения лекарств и основного оборудования для выживания [2].

Не менее древняя религиозная организация – Орден Святого Игнатия или Орден Иезуитов является самым могущественным орденом римской католической церкви и существуют уже около пятисот лет. Не существует ни одного католического ордена, схожего с Иезуитами, так как в XVI веке Папа Римский сделал орден независимым, что было первым в истории случаем. Орден Святого Игнатия занимается образовательной, просветительской, миссионерской, благотворительной и экологической деятельностью, а также оказывают социальную и гуманитарную помощь по всему миру. Они ведут активный светский образ жизни, в связи с чем пользуются большими привилегиями и влиянием по всему миру. В их юрисдикции находится огромное количество школ и университетов, институтов и культурных центров, приходов и церквей, а численность данного ордена составляет 16700 человек. Достоинно упоминание и то, что нынешний Папа Римский Франциск I был членом ордена Иезуитов [3].

Также стоит отметить и монашеские ордена, среди которых наиболее выделяется орден бенедиктинцев. Орден бенедиктинцев является своего рода конфедерацией монастырей и общин римской католической церкви. Орден объединяет в себе деятельность таких организаций, как: Альянс за международное монашество (AIM), который способствует гуманитарному, культурному и религиозному развитию монастырей по всему миру и их окружающего населения; Монашеский Межрелигиозный диалог (DIMMID), который способствует и поддерживает диалог между христианами монахами и женщинами и последователями других религий, особенно диалог на уровне

религиозного опыта и практики; Международная комиссия по бенедиктинскому образованию (ICBE), которая продвигает школы в бенедиктинской традиции по всему миру. Для большей эффективности орден имеет региональное управление. В Европе это: Ассоциация бенедиктинских женских монастырей на немецкоговорящих территориях и Монашеская конференция Франции [4].

Под некаатолическими организациями в данной работе подразумеваются все протестантские конфессии, Вселенская православная церковь, а также экуменистические организации. Деятельность православных религиозных организаций схожа с деятельностью организаций католиков, в большинстве случаев эти организации также номинально подчинены Вселенскому патриархату и призвана действовать в его интересах. У протестантов же единого главы нет, по этой причине и организации действуют сугубо в своих интересах.

Первое, с чего стоит рассматривать вопрос нехристианских организаций – это «Юношеская христианская организация» (YMCA) – чья активность заключается в молодёжной волонтерской деятельности. По своему происхождению и целям, эта организация была и остаётся христианской, её нельзя отнести ни к одной конфессии, так как она была создана для развития нравственных ценностей у всей, без исключений, молодёжи, тем самым её можно назвать экуменистической. По этой причине она не имеет официальных связей ни с одной церковью, правительством или организацией. Начав свою деятельность в Англии, YMCA распространила своё влияние по всему миру и теперь предоставляет молодым людям пространство для получения важнейшего опыта, а также начальное финансирование – для того, чтобы они могли возглавить процесс решения мировых проблем, которые они унаследуют. Основная деятельность YMCA заключается в четырёх областях: Здоровье - "Воспитание молодежи телом, разумом и духом"; Экология - "Привитие для молодёжи ценности окружающей среды"; Гражданское участие - "Усиление голоса молодых людей в сообществе"; Занятость - "Достойное трудоустройство для молодых людей с устойчивым источником дохода" [5].

Следующая организация – это Армия Спасения, которая также распространила свою деятельность на весь мир. Христианская и благотворительная организация, основанная в 1865 году в Великобритании, была призвана для оказания помощи нуждающимся. Хотя Организация и отличается от церквей в практике и управлении, доктрина армии следует основным принципам христианской веры. Целями Армии Спасения являются – продвижение христианской религии, образование, благотворительность и социальная помощь, а также любая другая деятельность, полезная для общества [6].

Далее необходимо отметить активную деятельность организации – Межпарламентская Ассамблея Православия (МАП). Своей главной задачей Ассамблея считает – призыв всех православных народов использовать возможности Православия в вопросах преодоления наблюдаемых тенденций национализма и самодержавности для сохранения целостности Европы и ее мирового влияния. Они также подчёркивают особое значение Балкан и

Восточной Европы в создании плюрализма общего европейского дома, а также в поисках путей достижения и установления мира и справедливости в новой Европе. В структуре МАП работают различные комиссии, в том числе по международной политике [7].

Далее речь пойдёт об организациях, деятельность которых довольно схожа, однако обе имеют в религиозных сообществах Европы значительное влияние по отдельности. Это Всемирный Совет Церквей (ВСЦ) и Конференция Европейских Церквей. ВСЦ – это крупнейшая международная христианская организация, в которую входят 348 христианских Церквей из 100 стран мира. Ее основная цель – содружество Церквей, достижение христианского единства. Однако в ее деятельность входит такое направление, как урегулирование конфликтных ситуаций, прежде всего возникающих на религиозной почве [8]. Кроме того, ВСЦ занимается исследованием актуальных политических, социально-экономических, научно-технических и экологических проблем, оказывает помощь антирасистским организациям. Аналогичной ситуация и с организацией Конференции Европейских Церквей. В их структуру входят различные комиссии, одна из которых «Церковь и общество». Эта комиссия оценивает экономические и социальные процессы, происходящие в европейских странах, вовлекает Церкви в обсуждение современных проблем с христианских позиций. Комиссия также стремится способствовать интеграционным процессам в Европе и поддерживает постоянные контакты с Европейским Союзом, Советом Европы, ОБСЕ, ООН [9].

Подводя итоги, стоит отметить, что религия как играла большую роль в Европе, так и продолжает играть, а значит прогнозы исследователей 20 века ошибочны. Исследование показало, что для христианства сейчас характерна тенденция на сближение конфессий, и вышеперечисленная деятельность организаций является тому прямым доказательством. Полное преодоление Схизмы невозможно, однако сотрудничество и дружественные отношения между конфессиями, а значит и между религиозными организациями, вполне достижимо.

Влияние религиозных организаций в Европе постепенно растёт и их мнение теперь необходимо учитывать не только на уровне государства, но и в международной системе в целом. Европейским политикам всё чаще приходится сталкиваться с вопросами, касающимися роли и места религии и религиозных институтов в интеграционном процессе Европы. Это говорит о том, что существует большая категория людей, для которых вера не просто традиции, а смысл жизни и путь ко спасению. В будущем это скажется на рост количества религиозных организаций, а также на их влиянии на общество.

Список используемых источников:

1. Канунников А. А. Церкви и религиозные организации: участие в европейском интеграционном процессе: [Электронный ресурс] // Известия Иркутского государственного университета. Политология. Религиоведение. 2017. Т. 36. С. 1-9. URL: <https://cyberleninka.ru/article/n/rol-musulmanskih-organizatsiy-v-soobshchestvah-velikobritanii-germanii-frantsii-i-italii/viewer>. (дата обращения: 02.11.2021).

2. Order of Malta [Электронный ресурс] URL: <https://www.orderofmalta.int/government/> (Дата обращения: 26.09.2021).
3. Иезуиты [Электронный ресурс] URL: <https://jesuit.ru/category/библиотека/мультимедиа/> (дата обращения: 26.09.2021).
4. OSB. ORG [Электронный ресурс] URL: <https://www.osb.org/> (Дата обращения: 26.09.2021).
5. World YMCA [Электронный ресурс] URL: <https://www.ymca.int/about-us/> (Дата обращения: 26.09.2021).
6. THE SALVATION ARMY INTERNATIONAL [Электронный ресурс] URL: <https://www.salvationarmy.org/ihq/about> (Дата обращения: 26.09.2021).
7. Вершинина В. Ю. Религиозный фактор международных отношений в XXI веке: [Электронный ресурс] // Актуальные проблемы современных международных отношений. 2013. № 10. С. 2-3. URL: <https://cyberleninka.ru/article/n/rol-musulmanskih-organizatsiy-v-soobschestvah-velikobritanii-germanii-frantsii-i-italii/viewer>. (Дата обращения: 02.11.2021).
8. World Council of Churches [Электронный ресурс] URL: <https://www.oikoumene.org/> (Дата обращения: 26.09.2021).
9. CEC [Электронный ресурс] URL: <https://www.cECEurope.org/> (Дата обращения: 26.09.2021).

Bondar N.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

International activities of Christian religious organizations in Europe.

At the end of the twentieth century, researchers predicted that the future of religions in Europe was sad and the 21st century would be its last. However, the situation by the 21st century corresponded to forecasts exactly the opposite. Changes have really come, religion has not only begun to return to the ordinary life of people, but now religious organizations claim to be an actor in international relations. Today, religion in Europe is free, and now people can choose what to believe.

Key words: *religion, Christianity, International relations, Europe.*

УДК 316.4
ГРНТИ 00.17

РАЗВИТИЕ МЕЖКУЛЬТУРНОЙ КОММУНИКАТИВНОЙ КОМПЕТЕНЦИИ В ЭПОХУ ЦИФРОВИЗАЦИИ

И. В. Дукальская

Поволжский государственный университет телекоммуникаций и информатики

В данном исследовании автор изучает влияние цифровизации на процессы межкультурной коммуникации и на формирование соответствующей компетенции. Цифровизация стала причиной серьезных изменений в образовательном процессе, в социальной и деловой жизни. Цифровая эпоха открыла доступ к глобальным рынкам для малых и средних предприятий, а также для отдельных людей. Социальные сети и другие цифровые платформы значительно облегчили экономические и образовательные процессы. Новые возможности повысили интерес к навыкам межкультурной коммуникации и формированию соответствующих компетенций.

цифровая эпоха, межкультурная коммуникация, межкультурная компетенция, навыки делового общения на английском языке

Под цифровизацией понимается принятие и расширение использования цифровых или коммуникационных технологий организацией, отраслью, страной и т.д. Роль цифровой компетентности в организациях предельно важна. Исследователи подчеркивают, что с одной стороны, цифровизация снижает количество общения и взаимодействия лицом к лицу. С другой стороны, дигитализация облегчает коммуникативные практики лидеров и тем самым влияет на результаты различных образовательных или экономических процессов [1]. Главный экономист Google, профессор Х. Вэриан отметил, что информационные технологии - это великий уравниватель [1].

Цифровые технологии сводят соискателей с работодателями (миллионы профессионалов имеют свои профили на LinkedIn), фрилансеров с заказчиками (миллионы людей находят работу на цифровых платформах), малые стартапы получают капитал на таких платформах, как Kickstarter и т.д. Можно действовать глобально из своего дома или офиса, просто используя свой аккаунт в социальной сети.

В связи с глобализацией и цифровизацией образования и экономики остро встает вопрос межкультурного общения и формирования межкультурных коммуникативных компетенций. Вопросы межкультурной коммуникации являются актуальной проблемой в современном обществе и приобретают все большее значение в последнее время, служат полем для ведения глобального диалога, для поиска пути к уважению и толерантности.

Информационно-коммуникационные технологий (ИКТ) создали возможности для людей познакомиться на практике с различными культурами и языками, а также создали среду, в которой могут взаимодействовать люди

различных социальных, культурных и образовательных уровней, с целью обмена информацией, участия в двусторонних проектах, мероприятия, дискуссиях и т.д.

Целью настоящего исследования является изучение роли межкультурной коммуникации в современной социальной и деловой среде и возможностей, которые предоставляет цифровизация для облегчения процессов межкультурной коммуникации. Межкультурная коммуникация, осуществляемая в виртуальной среде с использованием ИКТ, подразумевает не только широкое изучение и использование английского языка, но и изучение различий в прагматических системах и лингвистических тенденциях, например, восточной и западной культур, требует формирования соответствующих компетенций. Успешная межкультурная коммуникация создает диалог, непрерывную передачу информации. Этот обмен информацией проясняет непонятные моменты. Он также дает возможность задавать вопросы и подтверждать полученную информацию. Диалог уменьшает количество конфликтов, поскольку культурные недоразумения можно устранить, когда они возникают. Диалог возникает только тогда, когда обе стороны согласны делиться информацией и следить за тем, чтобы передача информации не блокировалась.

Цель коммуникации - передача идей и знаний от одного субъекта к другому. Коммуникация считается успешной, когда получатель демонстрирует, что он или она понимает, что было передано. С точки зрения организации существует множество барьеров, которые могут препятствовать потоку коммуникации. Эти барьеры включают культуру, технологии, язык, рабочую силу и окружающую среду.

Кросс-культурная коммуникация направлена на улучшение и облегчение взаимодействия между партнерами, сотрудниками, клиентами и менеджерами, представляющими разные нации или культуры [2]. Культурные различия могут привести к недопониманию, которое может стать причиной конфликта, но они также могут стать конкурентным преимуществом для глобальных компаний [3]. На современном этапе требуется стратегическое понимание важности компетенции межкультурной коммуникации в организациях, сообществах и странах по всему миру. Эффективность межкультурной коммуникации зависит от многих факторов. Гловер и Фридман отмечают, что успешное функционирование в рамках различных культур может стать проблемой для многих специалистов, и по мере того, как мир меняется, становится ясно, что работа с другими культурами, как внутренними, так и международными, требует компетентности в определении и преодолении культурных барьеров [4]. Языковой барьер, различия в ценностях и нормах поведения, недостаток опыта, отсутствие доверия, недостаток знаний о других культурах или стереотипное мышление являются одними из самых распространенных препятствий для межкультурной коммуникации. Существуют высококонтекстные и низкоконтекстные культуры: в то время как в низкоконтекстных культурах произносимые слова имеют прямое значение, в высококонтекстных культурах коммуникация представляет собой сложный процесс, в котором все невербальные элементы играют большое значение, например, возраст, а не пол

или национальные характеристики, является ключевым фактором, который влияет на то, как люди взаимодействуют с Интернетом.

Кросс-культурная компетенция является необходимым навыком в нашем глобализованном мире. Навыки общения с представителями разных культур могут помочь как в личных, так и в деловых вопросах. Цифровые коммуникационные технологии (электронная почта, социальные сети, мессенджеры и т.д.) облегчают межкультурную коммуникацию не только благодаря своей скорости и доступности, но и потому, что они более "безличны". Цифровая межкультурная коммуникация меньше подвержена влиянию культурных особенностей по сравнению с общением лицом к лицу. Языковой барьер является меньшим препятствием при онлайн-коммуникации. Цифровая межкультурная коммуникация значительно снижает языковой барьер.

Инструменты цифровой эпохи действительно упрощают процесс межкультурной коммуникации: многим людям легче общаться с представителем другой культуры, когда они не находятся "лицом к лицу", особенно когда языковой барьер является реальным препятствием. Онлайн-переводчики, автокорректоры могут добавить уверенности в процессе межкультурной коммуникации. Использование Интернета способствовало появлению глобальной культуры, в которой люди могут легко получить информацию, позволяющую им понять социокультурный контекст своих коллег. Изучение профиля в социальных сетях потенциального партнера или коллеги по работе может предоставить очень важные данные для будущей межкультурной коммуникации. Использование WhatsApp, Viber или других мессенджеров может упростить процесс общения, так как цифровые коммуникации стирают некоторые межкультурные различия. Например, текстовые сообщения решают проблему различных акцентов. Китайские бизнесмены смогут без проблем переписываться со своими партнерами в Лондоне, в отличие от обычной встречи, им не придется заботиться о национальных обычаях, связанных с рукопожатием, объятиями или чайной церемонией и т.д. Возрастающая роль социальных сетей - еще один фактор, способствующий росту важности цифровых коммуникаций. В настоящее время при поиске информации о компании, бренде или продукте люди чаще используют социальные сети, чем корпоративные сайты [5]. Кроме того, компании строят эффективные стратегии коммуникации со своими клиентами со всего мира, что требует навыков межкультурной коммуникации. Автор подчеркивает, что языковой барьер является одним из основных препятствий для эффективной межкультурной коммуникации, цифровизация частично помогает решить эту проблему. Многие транснациональные корпорации из неанглоязычных европейских стран используют английский в качестве основного корпоративного языка, но не все жители неанглоязычных стран владеют английским языком. Разговор лицом к лицу с партнером, владеющим английским на значительно более высоком уровне, может оказаться сложным для обеих сторон. В этом случае цифровые технологии могут сделать ваше общение более комфортным. С другой стороны, иногда онлайн-общения недостаточно для того, чтобы выстроить доверительные деловые

взаимоотношения между людьми. Невозможно произвести впечатление или убедить партнера невербальными приемами, общаясь с ним через один из мессенджеров или даже по Skype. Цифровые технологии могут упростить межкультурную коммуникацию. Это еще одно доказательство важности цифровых информационно-коммуникационных навыков. Цифровые навыки рассматриваются как важнейшие в 21 веке, поскольку они определяют конкурентоспособность и инновационный потенциал, а коммуникация как один из основных навыков в целом находится под сильным влиянием технологического прогресса [5].

Тенденции социальной и деловой среды способствуют развитию навыков межкультурной коммуникации. Межкультурное взаимодействие становится более частым. Люди стремятся получить новый опыт, открывая для себя новые страны и культуры. Компании ищут новые возможности для бизнеса, выходя на новые рынки или ища более дешевые ресурсы за рубежом, а цепочки поставок можно интерпретировать как глобальные многонациональные цепочки создания стоимости. Транснациональные корпорации всегда больше полагаются на многонациональные команды, чтобы добиться более высокой эффективности в процессах принятия решений и стимулировать инновации. Межкультурная коммуникативная компетенция является тем преимуществом, при помощи которого можно сплотить многокультурную проектную команду.

В современном обществе интеллектуальный ресурс становится доминирующим, а роль знаний как неотчуждаемого капитала возрастает. Количество людей, работающих в культурно разнообразной глобализированной среде, увеличивается. Овладение межкультурной коммуникативной компетенцией является конкурентным преимуществом. Дальнейшая глобализация делает важным изучение межкультурных взаимодействий и общности, а не межкультурных различий.

Список используемых источников:

1. Barker, K.; Day, C.; Day, D.; Kujava, E.; Otwori, J.; Ruscitto, RSmith, A. & Xu, T. Global Communication and Cross-Cultural Competence: Twenty-First Century Micro-CaseStudies. Global Advances in Business and Communications Conference & Journal, 2017 - 6(1), Article 5. [Электронный ресурс]. URL: <http://commons.emich.edu/gabc/vol6/iss1/5>. (дата обращения 08.10.2022).
2. Ester van Laar; A.; van Deursen; J. & van Dijk; J.. The relation between 21st-century skills and digital skills: A systematic literature review. Computers in Human Behavior, 2017- 72:577-588. [Электронный ресурс]. URL: <https://doi.org/10.1016/j.chb.2017.03.010>. (дата обращения 08.10.2022).
3. Gelfand, M.; Aycan, Z.; Erez, M. & Leung, K. Cross-Cultural Industrial Organizational Psychology and Organizational Behavior: A Hundred-Year Journey. Journal of Applied Psychology, 2017- 102(3): 514-529.
4. Glover, J. & Friedman, H. Transcultural competence: Navigating cultural differences in the global community. Washington, DC: American Psychological Association. 2015.
5. Hesse, A. Digitalization and Leadership – How Experienced Leaders Interpret Daily Realities in a Digital World. 2018 - Proceedings of the 51st Hawaii International Conference on System Sciences (pp. 1853-1864).

Dukalskaya I.

The Volga Region State University of Telecommunications and Informatics

Developing cross-cultural communicative competence in the digital age.

In this study, the author examines the impact of digitalization on the processes of cross-cultural communication and on the formation of relevant competences. Digitalization has caused major changes in the educational process and in social and business life. The digital age has opened up access to global markets for small and medium-sized enterprises, as well as for individuals. Social media and other digital platforms have greatly facilitated economic and educational processes. New opportunities have increased interest in cross-cultural communication skills and the building of relevant competencies.

Key words: the digital age, cross-cultural communication, cross-cultural competence, business communication skills in English.

УДК 811.111'42
ГРНТИ 16.21.27

ЦЕННОСТИ В ТВИТТЕР-БЛОГАХ ПРЕМЬЕР-МИНИСТРОВ ВЕЛИКОБРИТАНИИ (НА ПРИМЕРЕ Т. МЭЙ И Б. ДЖОНСОНА)

Р. А. Жадан

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается метод анализа ценностной направленности политических Твиттер-блогов британских премьер-министров на примере Терезы Мэй и Бориса Джонсона. Ценностями называются важные для автора блога идеи, к которым он обращается повторно на протяжении некоторого взятого отрезка времени. Методика подсчета, предложенная в статье, позволит оценивать ценностные ориентиры политической коммуникации представителей власти в любых цифровых каналах.

медиадискурс, социальные сети, аккаунт, политический блог, ключевые слова, смысл, ценностная картина дискурса, политическая картина мира

Введение

На сегодняшний день Интернет играет важную роль в современном мире, он приобретает все большую популярность в деловой, образовательной, научной, политической и личной жизни общества. Доля политического сегмента в Интернете значительно растет, на данный момент он оказывается и пространством политической коммуникации, и средством ее осуществления. Использование таких технологий, как социальные сети, размывает географические границы между аудиториями с помощью интернет-каналов. Многие исследователи сходятся во мнении [1; 2; 3], что социальные сети имеют значительные преимущества для политиков. Во-первых, представители власти могут донести до граждан свои политические взгляды. Во-вторых, социальные сети дают возможность создать положительный имидж политика, а именно образ современного, коммуникативного чиновника, постоянно находящегося на связи с населением. В-третьих, большинство СМИ ссылаются на информацию, полученную в социальных сетях, это позволяет считать, что личные профили политиков различного уровня принимаются безоговорочной истиной [2]. Следовательно, население больше доверяет таким источникам. Зарубежные политики используют Твиттер не только в период подготовки выборов различных органов власти, но и для других серьезных и важных событий. Социальные сети – также важный инструмент для того, чтобы граждане и общество наиболее эффективно и быстро доносили до власти свои интересы.

Проанализировав научные работы, можно выделить несколько задач, которые преследуют политики и государственные деятели в социальных сетях, например, желание показать свою вовлеченность в общественную жизнь и взаимодействие с народом. По мнению Н. В. Кобрин [3], коммуникаторы социальных медиа могут параллельно выполнять функции комментатора, репортера, фотокорреспондента, редактора, т. е. как производителя

информационного продукта, так и его потребителя. Именно поэтому в медиатекстах социальных медиа особую значимость приобретает личность самого коммуниканта.

Медиатексты Твиттера стали мощным средством воздействия на массовую аудиторию, одновременно отражая и создавая новую реальность в интересах доминирующей идеологии правящей группы. Наличие повторяющихся ключевых слов, репрезентирующих ценности, способствует пониманию читателями реальности. Они задают читателям нужную траекторию восприятия смыслов. Политический медиадискурс Твиттера как разновидность политического дискурса социальных сетей представляет собой лингво-политическое действие, развивающееся в рамках платформы Твиттера и направленное на продвижение определенной идеологии и установки [3]. Поэтому постоянное обращение к одним и тем же смыслам (ценностям) в блоге политика уже задает определенное понимание со стороны подписчиков, читателей.

Как пишет Т. Н. Москвитина, ценность сообщения определяется не длиной, но тем, что ново или уже известно, учтено адресатом и включено им в его внутреннюю структуру [4], то есть смысл всего высказывания может уместиться в одном-двух ключевых словах. Объем текста не равен его содержанию, а длинный пост может быть равен, по сути, всего одному слову. С этих позиций представляет интерес тот факт, что в кратких твитах (постах) может помещаться от одного до 2-3 смыслов, именно благодаря заданным ценностным словам, которые несут на себе основную нагрузку, задают определенный стимул для читателя и не требуют вербального разворачивания до большого текста, поскольку это «разворачивание» происходит в сознании избирателей, подписчиков после прочтения поста.

Мы хотим доказать, что своей коммуникации политик несет свои убеждения, как те, что диктует ему текущая повестка, например, экология, равенство, экономика, дискриминация, свобода, так и свои личные: поездка в другую страну, интервью с различными популярными изданиями, запись подкастов.

Методы и материал исследования

Мы составили случайную выборку твитов из аккаунтов двух политиков в количестве 100 штук. Твиты Терезы Мэй датированы июнем 2019 г., Бориса Джонсона – маем 2021 г. [5; 6]. С помощью приемов контекстуального и концептуального анализа мы выявили, какие ценностные концепты важны для двух британских премьер-министров, занимавших пост главы государства один за другим. Ценностные установки можно выявить через ключевые слова, слованомианты ценностей. Они могут звучать у политика напрямую, дословно, например: *The UK and Japan are natural partners and we will continue to work together to uphold the global rules by which we seek to ensure a peaceful and prosperous world* (в данном посте можно выделить ценность безопасности); или могут подразумеваться, быть скрыты в общем содержании поста, например:

Everyone in this country can look ahead to a future in which each of us has a safe, affordable place to call home (забота).

Ключевые слова представляют собой сгустки смысла, и за ними разворачивается целый пласт фрагментов ценностной картины. И по ним, в свою очередь, из анализируемых постов можно конструировать ценности.

Результаты исследования и их интерпретация

Список выявленных ценностей, характерных для коммуникации изучаемых британских политиков в сети Твиттер, представлен в таблице 1.

ТАБЛИЦА 1. Ценностные ключевые слова Твиттер-коммуникации британских премьер-министров

Ценность	Т. Мэй		Б. Джонсон	
	примеры	кол-во контекстов	примеры	кол-во контекстов
Поддержка	very proud of you; We are all behind you; need to treat mental health; He has the passion and the drive to be an excellent Member of Parliament; We will never forget those who lost their lives	10	give them all our support; My thoughts are with the Israeli; My thoughts are with her friends and family; giving our children the best education; Make us proud in South Africa.	16
Экология	helping our efforts to get to #netzero emissions; cut greenhouse gas emissions; achieve net zero emissions; reach; cut plastic pollution; #BeatAirPollution	15	tackle climate change; The fight against climate change; Green Industrial Revolution; protect at least 30% of their land	5
Историческая память	#DDay75; #LestWeForget	10	#VEDay	1
Здоровье	linked with mental health issue; measures to end unequal mental health; rise in mental health problems; improve mental health; transformation in mental health	7	#MentalHealthMinute; Thank you to the many scientists and clinicians who have worked on this research	3
Безопасность	enhance good governance and security in this region; threat from terrorist; ensure a peaceful; ongoing peace effort	7	8,771 new police officers; officers on our streets to cut crime; more police on the beat; want safer streets	9
Свобода			Step 3 of our cautious roadmap to freedom	1
Забота	programme to expand diversity in theatre; who play their part in making our Armed Force; each of us has a safe; #LetsTalkLoneliness; Independent Review of the Mental Health; never forget	5	need to secure long-term jobs; will give young people skills for life; positive wellbeing in schools; I'd like to thank nurses; brighter future for everyone; stronger for the people of Northern Ireland	7

	those who lost their lives; #CarersWeek			
Партнерство	partnership between our two countries; friendship will continue long; celebration of the special relationship between	3		
Лидерство, единство	Together we can harness the power of the state; issue firmly on the domestic and international agenda	9	Queen Elizabeth is a symbol of what can be achieved by investing in British ingenuity	2
Развитие страны	local economy, innovation; regulations to create bigger, wages are growing faster	7	new jobs to the area; create 65,000 new jobs; keeping your taxes low	6
Здравоохранение	will help save millions of lives; will help the fight against AIDS; break down barriers faced by disabled people	6	United Kingdom stronger, healthier and more prosperous than before	6
Вакцинация	–	0	rolling out vaccines; book your COVID-19 vaccine; 50 MILLION doses of coronavirus vaccine	15
Образование	We're home to four out of the top ten global universities	1	giving our children the best education	1
Итого		80		72

Исходя из данных, отраженных в таблице, мы видим, что распределение ценностей в постах двух политиков не равномерны, что естественно объясняется причинами общественного порядка и событий, происходящих в политике и общественной жизни и соответствующих временному периоду пребывания у власти. Видим, что ценность вакцинации не представлена в блоге Т. Мэй, поскольку пандемия пришлась на годы осуществления полномочий Б. Джонсона. Приблизительно равномерно распределяются базовые ценности: забота, поддержка, безопасность. Также присутствует примерно равновесное распределение по ценностям, связанным с внешней или внутренней политикой Великобритании: это историческая память, экология, лидерство, развитие страны, патриотизм.

Выводы.

Итак, количественный подсчет представленных в Твиттер-аккаунтах ценностях свидетельствует о том, что политики с регулярной частотой обращаются к определенному набору смыслов, которые звучат повтором, с некоторой периодичностью в постах. Видим, что, по ключевым словам, можно выделять основные понятия, ценные для того или иного лидера, соотносить их с проводимыми мерами и с событиями политической жизни. Предложенная процедура анализа ценностей по ключевым словам в блоге может быть также применена для анализа любых других видов общественной коммуникации

политиков в социальных сетях. Данное исследование вносит вклад в конструирование ценностной картины англоязычного политического дискурса.

Список используемых источников:

1. Землякова К. В. Когнитивно-дискурсивная интерпретация концепта President в Твиттер-коммуникации Д. Байдена // Когнитивные исследования языка. – 2022. – № 3(50). – С. 210–214.
2. Козырева А. А. Почему социальные сети являются инструментом политической власти? // Вестник КемГУ. 2015. №2-2 (62). URL: <https://cyberleninka.ru/article/n/pochemu-sotsialnye-seti-yavlyayutsya-instrumentom-politicheskoy-vlasti> (дата обращения: 09.11.2022).
3. Кобрин Н.В. Особенности политического медиадискурса твиттера // Филологические науки. Вопросы теории и практики. Тамбов: Грамота, 2015. – № 2. – С. 94-99.
4. Москвитина Т. Н. Свойства и функции ключевых слов в различных типах дискурса // Когнитивные исследования языка. – 2022. – № 2(49). – С. 70–75.
5. Theresa May // Twitter. – URL: https://twitter.com/theresa_may.
6. Boris Johnson // Twitter. – URL: <https://twitter.com/BorisJohnson>.

Zhadan R.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

Values in Twitter Blogs of British Prime Ministers (Examples of T. May and B. Johnson).

The paper deals with the method of analyzing the value orientation of political Twitter-blogs of British Prime Ministers, taking Theresa May and Boris Johnson as examples. The values are the ideas important for the author of the blog, which he refers to repeatedly during a certain taken time interval. The counting methodology proposed in the article will make it possible to assess the value orientations of the political communication of the representatives of power in any digital channels.

Key words: *media discourse, social networks, profile, political blog, keywords, meaning, value image of a discourse, political worldview.*

УДК 327.3
ГРНТИ 87.05.33

ЭКОЛОГИЧЕСКОЕ СОТРУДНИЧЕСТВО ЕС И ЗАПАДНЫХ БАЛКАН

П. В. Лещинский, А. В. Неровный

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Региональное сотрудничество является важным компонентом процесса расширения, дополняющим двустороннее сотрудничество. В последние годы процесс регионального сотрудничества поддерживался в форме программ сотрудничества в области окружающей среды, направленных на содействие общению и сотрудничеству между странами-бенефициарами в решении трансграничных экологических проблем, а также на содействие обмену информацией и передовым опытом.

Зеленый курс, региональное сотрудничество, Зеленая повестка дня

Европейский зеленый курс является ответом на текущие планетарные вызовы, такие как изменение климата, утрата биоразнообразия и загрязнение окружающей среды. Это новая стратегия роста, направленная на преобразование ЕС в справедливое и процветающее общество с современной, ресурсоэффективной и конкурентоспособной экономикой, где к 2050 году не будет чистых выбросов парниковых газов и где экономический рост не связан с использованием ресурсов. Он также направлен на защиту, сохранение и приумножение природного капитала ЕС, а также на защиту здоровья и благополучия граждан от рисков и воздействий, связанных с окружающей средой. В то же время он гарантирует, что переход должен быть справедливым и инклюзивным [1].

Региональное сотрудничество дает возможность решать общие проблемы и обмениваться знаниями и передовым опытом. ЕС уже несколько лет финансирует специализированные проекты регионального сотрудничества в области окружающей среды и климата. Проект Региональной экологической сети для вступления способствовал улучшению состояния окружающей среды и климата на Западных Балканах и приближению региона к стандартам ЕС. Региональная сеть по присоединению к окружающей среде и климату продолжала укреплять региональное сотрудничество между странами-кандидатами и потенциальными кандидатами.

Но экологический переход для Европы может быть полностью эффективным только в том случае, если соседи ЕС также предпримут эффективные действия. Таким образом, параллельно с Планом экономических инвестиций для поддержки региона европейская комиссия представила руководящие принципы реализации Зеленой повестки дня на Западных Балканах.

Зеленая повестка дня предусматривает действия по пяти основным направлениям: климатические действия, включая обезуглероживание, энергию и мобильность; экономика замкнутого цикла, в частности решение проблемы

отходов, переработка, устойчивое производство и эффективное использование ресурсов; биоразнообразие, стремление для защиты и восстановления природных богатств региона; борьба с загрязнением воздуха, воды и почвы; устойчивые продовольственные системы сельских районов.

Зеленую повестку дня для Западных Балкан следует рассматривать как план возможных мер, которые должны быть приняты совместно ЕС и каждым из западнобалканских партнеров на основе существующих структур политического и технического сотрудничества. Повестка дня должна позволить Западным Балканам и ЕС установить более тесную связь между действиями в области климата и окружающей среды, политическими реформами и сближением с ЕС. Он также должен служить руководством для определения стратегий финансовой и технической помощи как на двустороннем, так и на региональном уровне [2].

Реализация масштабной «Зеленой программы» для Западных Балкан потребует значительного государственного и частного финансирования на национальном, региональном и международном уровнях. Внешние инструменты в рамках следующей Многолетней финансовой программы ЕС в настоящее время обсуждаются с Советом и Европейским парламентом. Это государственное финансирование ЕС в дальнейшем потребует для привлечения частного финансирования, чтобы заполнить значительный дефицит инвестиций. Кроме того, необходимо будет мобилизовать дополнительную поддержку со стороны государств-членов ЕС и собственные средства бенефициаров. В этой связи Комиссия может рассмотреть возможность поддержки инновационных финансовых инструментов, таких как «зеленые» облигации, которые могут мобилизовать государственные и частные инвестиции в масштабе, необходимом для реализации «Зеленой повестки дня».

Инвестиционная структура Западных Балкан (WBIF) является одним из таких смешанных финансовых инструментов, которые могут поддерживать «зеленую повестку дня». Он уже активно работает в экологическом и энергетическом секторах. Региональная программа энергоэффективности (REEP) может поддерживать перенос и внедрение законодательства ЕС в области энергоэффективности в сочетании с финансированием предприятий, домашних хозяйств и организаций государственного сектора, осуществляющих инвестиции в энергоэффективность.

Финансирование также будет иметь решающее значение для исследований и инноваций. Европейский совет по инновациям (EIC) – самая амбициозная инициатива ЕС в области прорывных и прорывных инноваций, полностью включающая Западные Балканы. Регион также может воспользоваться финансовыми инструментами InnovFin в рамках Horizon 2020.

Западные Балканы уже участвуют в Horizon 2020 – Рамочной программе ЕС по исследованиям и инновациям, в которой в 2019 году было выделено около 200 заинтересованных сторон и выделено 30 миллионов евро. Новая рамочная программа исследований и инноваций Horizon Europe будет уделять больше внимания распространению передового опыта и сокращению разрыва в НИОКР, что принесет особую пользу экономике Западных Балкан. На Западных Балканах

реализуются две макрорегиональные стратегии ЕС с сильным инновационным компонентом: Дунайская стратегия и Адриатико-Ионическая стратегия, и они поддерживают инновации и трансграничное сотрудничество в среднесрочной перспективе для регионов [3].

Список используемых источников:

1. A European Green Deal [Электронный ресурс] / An official website of the European Union [Сайт]. – URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en (дата обращения: 05.11.22).
2. Candidate Countries and Potential Candidates [Электронный ресурс] / An official website of the European Union [Сайт]. – URL: https://ec.europa.eu/environment/enlarg/reg_cooperation.htm (дата обращения: 05.11.22).
3. Commission staff working document. Guidelines for the Implementation of the Green Agenda for the Western Balkans. – Brussel: European Commission, 2020. – 20 p.

Leshchinskii P., Nerovnyi A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Environmental cooperation between the EU and the Western Balkans.

Regional cooperation is an important component of the expansion process, complementing bilateral cooperation. In recent years, the process of regional cooperation has been supported in the form of environmental cooperation programmes aimed at facilitating communication and cooperation between beneficiary countries in solving transboundary environmental problems, as well as facilitating the exchange of information and best practices.

Key words: Green course, regional cooperation, Green Agenda.

УДК 304.44
ГРНТИ 23.43

АДАПТАЦИЯ ИММИГРАНТОВ В КУЛЬТУРНУЮ СРЕДУ ШВЕЦИИ

Г. М. Пуртова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья рассматривает адаптацию иммигрантов в культурную среду Швеции как одно из ключевых направлений культурной политики в отношении новых членов шведского общества.

Швеция, культурная политика, иммиграция, адаптация, культурная среда

Швеция – одна из самых передовых стран нашего времени. Ее культура породила таких всемирно известных деятелей и явления как лагом, Астрид Линдгрэн, АВВА, Карл Линней, шведский социализм, Нобелевская премия, Ингмар Бергман и многое другое.

Чтобы шведская культура не переставала приносить богатые плоды и достойно переносила вызовы современного мира государству необходимо проводить культурную политику, которая обеспечит планирование, проектирование, реализацию культурной жизни государства и общества, что делает ее неотъемлемой и значимой частью государственной политики в целом.

Основными направлениями культурной политики Швеции являются: сохранение культурного наследия, популяризация шведской культуры в мире и культурная политика в отношении иммигрантов, важной частью которой является адаптация новых членов общества к культурной среде страны.

В 2020 году в мире насчитывалось около 280 миллионов международных мигрантов. Это люди, которые по разным причинам переехали, из страны в которой они родились, в другую страну.

В Швеции около 2 миллионов человек, родившихся в другой стране, или каждый пятый человек. Одной из наиболее частых причин переезда в Швецию, помимо работы, является воссоединение с близкими членами семьи. Что касается убежища, Швеция подписала Конвенцию ООН о беженцах, что означает, что страна пообещала проверять и предоставлять убежище людям, признанными беженцами в соответствии с Конвенцией [1].

17 ноября 2021 года министр финансов Швеции Магдалена Андерссон произнесла свою первую речь в качестве главы Шведской социал-демократической партии и напрямую обратилась к более чем 2 миллиону беженцев и мигрантов в стране. «Если вы молоды, - сказала она, - вы должны получить аттестат о среднем образовании и продолжить работу или получить высшее образование». Если вы получаете финансовую помощь от государства, «вы должны изучать шведский язык и работать определенное количество часов

в неделю». Более того, «здесь, в Швеции, и мужчины, и женщины работают и вносят свой вклад в благосостояние». Шведское гендерное равенство применяется «независимо от того, что думают и чувствуют отцы, матери, супруги или братья» [2].

Из речи Магдалены Андерссон можно выделить две наиболее актуальные проблемы адаптации иммигрантов, так или иначе связанные с культурой: образование и гендерное равенство.

Одним из органов власти, который помогает вновь прибывшим беженцам и иммигрантам влиться в общество и получить образование является Шведская государственная служба занятости [3]. Люди, принадлежащие к группе, которая соответствует требованиям программы трудоустройства, получают всю необходимую информацию от службы занятости о том, что необходимо для начала поиска работы. В первую очередь они получают план, содержащий различные мероприятия, которые помогут им адаптироваться в обществе и впоследствии найти работу. План включает в себя: шведский язык для иммигрантов, подготовку к трудовой деятельности (например, стажировки или подтверждение образовательного и профессионального опыта) и введение в общество, которое направлено на предоставление базовых знаний о шведском обществе. Отправной точкой является то, что в запланированных мероприятиях люди должны работать полный рабочий день, то есть 40 часов в неделю. Участие в программе обычно длится 24 месяца, что позволяет дать людям базовые навыки проживания в шведском обществе и знания о ее культуре [4].

Что касается гендерного аспекта, влияние культуры на поведение женщин-иммигрантов на рынке труда, уменьшается по мере того, как они проводят время в своей новой принимающей стране, Швеции. Принимая во внимание институциональную среду Швеции, вероятно, что количество учреждений, поощряющих участие женщин в рабочей деятельности, таких как системы ухода за детьми и отпуска по уходу за ребенком, помогает устранить культурные барьеры [5].

Решая обозначенные и другие проблемы государство активно сотрудничает и поддерживает иммигрантские организации. Исследование Олле Фрёдин, Акселя Фредгольма и Йохана Сандберга показывает, что почти все шведские иммигрантские организации, получившие государственную поддержку, устраивали различные культурные мероприятия [6]. Они часто проводились параллельно с рядом мероприятий, способствующих интеграции, и эти мероприятия, как оказалось, были как совместимыми, так и часто совпадающими. Среди ассоциаций, представляющих членов из стран Ближнего Востока, деятельность по содействию интеграции сообщалась чаще, чем в европейских ассоциациях. Это указывает на довольно спонтанную гражданскую ориентацию среди иммигрантских организаций, которые определили потребность в деятельности по продвижению интеграции, поскольку ни одна из

организаций не была прямо принуждена продвигать интеграцию как условие для государственной поддержки. Этот вывод предполагает, что контекст государства всеобщего благосостояния и активная политика интеграции со стороны национальных и местных органов власти не вытесняли организационные инициативы иммигрантов. Скорее, иммигрантские организации, были вынуждены занять определенные ниши в контексте государства всеобщего благосостояния, где они предлагали дополнительные услуги, часто с целью помочь членам ориентироваться в системе шведского общества.

Сейчас в Швеции происходит процесс культурной интеграции между коренными жителями и иммигрантами. Можно ожидать первоначальных различий в многочисленных культурных показателях между коренными жителями и иммигрантами, поскольку именно эти различия, по крайней мере частично, определяют культурные нормы большинства населения. Ожидается, что из-за последующей адаптации как в большинстве, так и в меньшинстве населения первоначальные различия будут уменьшаться со временем и между поколениями [7].

И так, в перспективе целью адаптации и культурной политики Швеции в отношении иммигрантов в целом следует считать поддержание терпимости и содействие формированию новых проявлений культуры. Культура и ее понимание будет при этом все разнообразнее. Только тогда она будет развиваться, и будет расти ее значение в обществе и мире.

Список используемых источников:

1. Sweden and migration // sweden.se [site]. URL: <https://sweden.se/culture/history/sweden-and-migration> (requested: 05.11.2021).
2. James Traub Even Sweden Doesn't Want Migrants Anymore // Foreign Policy [site]. URL: <https://foreignpolicy.com/2021/11/17/even-sweden-doesnt-want-migrants-anymore-syria-iraq-belarus/> (requested: 07.11.2021).
3. Om oss// Arbetsförmedlingen [site]. URL: <https://arbetsformedlingen.se/> (requested: 05.11.2021).
4. Integration i Sverige// informationsverige.se [site]. URL: <https://www.informationsverige.se/sv/jag-har-fatt-uppehallstillstand/samhallsorientering/boken-om-sverige/att-komma-till-sverige/integration-i-sverige/> (requested: 05.11.2021).
5. Emma Neuman Source country culture and labor market assimilation of immigrant women in Sweden: evidence from longitudinal data// Springer Link [site]. URL: <https://link.springer.com/article/10.1007/s11150-018-9420-6#Sec10>
6. Olle Frödin, Axel Fredholm, Johan Sandberg Integration, cultural preservation and transnationalism through state supported immigrant organizations: a study of Sweden's national ethnic associations// Springer Open [site]. URL: <https://comparativemigrationstudies.springeropen.com/articles/10.1186/s40878-021-00245-1#Sec10> (requested: 06.11.2021).
7. Yann Algan, Alberto Bisin, Alan Manning, Thierry Verdier Cultural Integration of Immigrants in Europe// Oxford Scholarship Online [site]. URL: <https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780199660094.001.0001/a-cprof-9780199660094-chapter-6> (requested: 06.11.2021).

Purtova G.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Adaptation of immigrants to the cultural environment of Sweden.

This article considers the adaptation of immigrants to the cultural environment of Sweden as one of the key directions of cultural policy towards new members of Swedish society.

Key words: Sweden, cultural policy, immigration, adaptation, cultural environment.

УДК 81373.45
ГРНТИ 16.41.21

АНГЛИЦИЗМЫ В КИБЕРСПОРТЕ

В. Д. Сидоренко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье речь пойдет о влиянии англицизмов на киберспортивное сообщество. Рассмотрены способы образования и виды англицизмов с примерами использования.

киберспорт, англицизмы, английский язык

Киберспорт – это абсолютно новая сфера для изучения, с точки зрения ведения бизнеса, тим-билдинга, образование игровых составов, так же язык в киберспорте используется иной. К киберспорту относятся различные дисциплины, то есть игры, которые отличаются от других игр тем, что в них есть спортивная или же соревновательная онлайн составляющая. Каждая такая дисциплина имеет свой вокабуляр, который иногда схож, а иногда крайне сильно отличается от других [1].

Киберспорт – это отличное новое информационно-коммуникационное пространство, так как является новой сферой общения, в которой появляются новые слова, а также новые речевые обороты. Дополнительно знакомит новых пользователей с англицизмами, так еще и не с самыми простыми, а как правило сленговыми оборотами, сравнительными с диалектами Лондонских кокни. Данное явление подкреплено тем, что не всегда в одной команде и одном игровом лобби могут находиться люди из одной страны, но коммуникация – это одно из главных отличий киберспорта от большого спорта, так как без должного уровня понимая друг друга – невозможно добиться победы. Поэтому сленговые англицизм, увеличивающие темп общения могут помочь в этом игровом аспекте [2].

Англицизмы в киберспорте, из-за своей актуальности и простоты словообразования, обладают низким уровнем вхождения в язык, что популяризирует его среди игроков и СМИ.

Способы образования англицизмов бывают нескольких видов. Среди материальных заимствований есть устные, происходящие «на слух», без учёта письменного образа слова в языке – источнике, и заимствования из письменных текстов или с учётом письменного облика слова. Устные заимствования характерны для более старых исторических эпох – до возникновения или широкого распространения письма, а в новое время они отличаются там, где имеют место массовые бытовые контакты между носителями разных языков без систематического использования письменных форм общения. Письменные заимствования проникают через книгу, газету, через сознательное изучение соответствующего языка и т.д [3].

Займствования образуются несколькими способами. Прямые займствования. Слово встречается в русском языке приблизительно в том же виде и в том же значении, что и в языке – оригинале. Это такие слова, как уик-энд – выходные; мани – деньги.

Гибриды. Данные слова образованы присоединением к иностранному корню русского суффикса, приставки и окончания. В этом случае часто несколько изменяется значение иностранного слова – источника, например: аскать от английского to ask – просить, бузить от busy – беспокойный, суетливый.

Калька. Слова, иноязычного происхождения, употребляемые с сохранением их фонетического и графического облика. Это такие слова, как меню, пароль, диск, вирус, клуб.

Полукалька. Слова, которые при грамматическом освоении подчиняются правилам русской грамматики (прибавляются суффиксы). Например: драйв – драйва (drive) «Давно не было такого драйва» – в значении «запал, энергетика».

Экзотизмы. Слова, которые характеризуют специфические национальные обычаи других народов и употребляются при описании нерусской действительности. Отличительной особенностью данных слов является то, что они не имеют русских синонимов. Например: чипсы (chips), хот-дог (hot-dog), чизбургер (cheeseburger).

Иноязычные вкрапления. Данные слова обычно имеют лексические эквиваленты, но стилистически от них отличаются и закрепляются в той или иной сфере общения как выразительное средство, придающее речи особую экспрессию. Например: о'кей (OK); вау (Wow).

Композиты. Слова, состоящие из двух английских слов, например: секонд-хенд – магазин, торгующий одеждой, бывшей в употреблении; видео-салон – комната для просмотра фильмов.

В различных играх используется свой язык, основанный на англицизмах, один из самых известных и языков, который вобрал в себя все основы, из которых вытекают языки других дисциплин – это язык Dota 2 [4].

Англицизмы в киберспорте можно распределить на несколько групп:

А) Процессуальные – Слова указывающие на перемещения и различные процессы внутри игрового лобби.

1) Стакнуться – (От англ. Stuck – собраться) Используется по отношению к команде, своей или чужой, означает, что команде нужно собраться вместе и быть рядом (Пример: Парни, нам нужно стакнуться и пойти драться).

2) Ганг – (От англ. Gang – как просторечие, банда, но в киберспорте имеет значение – неожиданное нападение) Используется, как просьба или предлог о неожиданное нападение. (Пример: Соперник оказался сильнее, я один не справляюсь, нужен ганг).

3) Чейз – (От англ. Chase – следовать) Призыв или предупреждение о преследовании. (Пример: У них нет ресурсов на драку, они отходят, надо чейзить их).

Б) Механические – Слова используемые по отношению к механике игры.

1) Скил – (От англ. Skill – способность)

(Пример: Мой скил перезаряжается)

2) КД – (От англ. CoolDawn – перезарядка)

(Пример: Мой скил на кд)

3) Юнит – (От англ. Unit – ед. измерения) – Любой передвигающийся персонаж в игре.

4) Рут – (От англ. Root – связать) Механика игры Dota 2, которая способна связать, оцепенеть юнита в игре.

В) Личностные или Неймовые – англицизмы, которые можно адресовать личности, исполнителю на герое.

1) НН (Сокр. от англ. Noname) – неизвестный игрок.

2) Хай скил (От англ. Highskill) – человек, показывающий высокий уровень игры.

3) ЛС (Сокр. от англ. LowSkill) – человек, показывающий низкий уровень игры.

4) Бот (От англ. Bot, буквально, робот) – слабо играющий человек, не проявляющий инициативы для победы.

Г) Результативные – англицизмы, выражающие события и результаты игрового матча.

1) Луз (От англ. Lose) – проигрыш

2) Вин (От англ. Win) – победа

3) Лузербрэйкет (От англ. LowerBracket) – Нижняя сетка, при проведении турнира формата Doubleilluminate нижняя сетка представляет собой игры на вылет между командами, проигравшими уже единожды.

4) Винер брэйкет (От англ. WinnerBracket) – Верхняя сетка, при проведении турнира формата Doubleilluminate верхняя сетка представляет собой матчи между командами, которые не потерпели поражений.

Д) Ментальные – англицизмы, обозначающие настроенческое состояние индивида.

1) Тильт – (От англ. Tilt) Состояние человека, совокупное из злости и обиды.

2) Вайб – (От англ. Vibe) Состояние человек, совокупное из атмосферы и настроения, как благоприятного, так и нет (Пример: В этом коллективе просто нет вайба. Парни, я так счастлив, меня так вайбит!)

3) Токсик – (От англ. Toxic) Состояние человек, когда индивиду свойственно быть колким и излагать агрессивным посыл в любом его проявлении.

Примеры популярных англицизмов в диалоге:

«Андаинг, встань мид! Встань бэйбисить меня! Ты регаешь по двадцать ммов в день, зачем? Ты же все равно крип-крипочек».

Андаинг- (Undying – бессмертный) это герой из игры Dota 2, иногда его называют «зомби».

Встать мид – означает приход героя в центральный коридор карты. В других играх мид имеет значения центральной позиции на карте.

Бэйбиситить – (BabySit) выражение из английского языка, которое можно заменить на «нянька». В играх это выражение используется, как объяснение движения игроков, когда во благо другого игрока или героя они тратят свое

время на опекунство такого героя или игрока.

Регать – (Сокращение от Регистрировать) запускать поиск игры.

ММ – (сокращение от англ. MatchMaking) Рейтинговые матч.

Крип – нейтральное существо в игре Dota 2 и схожих с ней ММО-RPG играх, самое слабое существо, которое работает по принципу заранее написанных кодов. Если это используется, как обращение к игроку, то это эквивалентно оскорблению.

«-Помочь мне можно?

-Форс будет!

-Панго рольнулся

-После роллинга дам в панго блинк

-Сларк без БКБ, можем его?

-Я на ШД сяду

-Я даст нажал

-Под вард бежите к ним

-Держим позиционку!

-Сларк без ульта, дайте стан!

Это пример голосовой коммуникации Российской профессиональной команды PuckChamp [5].

Форс – (Сокращение от англ. ForceStaff – толкающий жезл) Предмет, который может передвинуть союзника на некоторое расстояние.

Панго – Сокращенное имя героя Pangolier.

Рольнулся – использовал способность RollingThunder – раскаты грома.

Роллинг – Сокращение способности RollingThunder – раскаты грома.

Блинк – Процесс телепортации.

Сларк – Slark, герой Dota 2.

БКБ – Сокращенное название предмета BlackKingBar – Палка черного короля.

ШД – Сокращенное имя героя ShadowDemon.

Сесть на героя или фоллоу он хиро – Процесс следования за героем оппонента в драке, не дать ему комфортно играть, создать проблем для конкретного героя.

Даст – (Сокращение от англ. Dustofappearance) предмет, который раскрывает невидимость.

Вард – От англ. Ward, предмет, который позволяет подсветить поле сражения и видеть больше положенного.

Бежать под вард, значит идти в территорию, которая находится под взором оппонента.

Позиционка – Положение героев в драке. Держать позиционку, значит принять правильное положение героев, как военные построения, например, у Римлян.

Ульт – Способность, которая изучается героем позже других, так как является самой сильной.

Стан – (От англ. Stun) оглушение. Дать стан, значит оглушить героя оппонента.

«У них керри сильнее нашего, давайте пикнем мидера, который расфармится и запушит их быстро»

Керри – (От англ. Carry) Герой, который получает большую часть опыта и золота в своей команде.

Пикнем – (От англ. Pick) Выбор.

Расфармить – Набрать пиковую форму.

Запушить – Процесса сноса сооружений оппонента.

Многочисленные англицизмы, проникающие в язык – явление закономерное, отражающее активизировавшиеся в последнее десятилетие экономические, политические, культурные. Создание новых выражений и слов, которые становятся англицизмами лежит, как правило, на плечах носителей языка, а углубление в язык со стороны его андерграунда – является реактивным способом, который помогает начать изучать чужой язык.

Каждое поколение считает, что оно столкнулось с ранее неизвестной ситуацией, и что данная проблема является уникальной. Однако если обратиться к истории, то станет понятно, что данная проблема является цикличной и уже возникала ранее. Так, например, во время пика популярности футбола в СССР в языке появились такие слова как «корнер», «форвард», «хавбек», «голкипер», которые в последствии превратились в «угловой», «нападающий», «полузащитник», «вратарь». Стоит ожидать, что лексика киберспортивной дисциплины DotA2 будет развиваться согласно данному закону. Заимствуя большинство слов и впоследствии заменяя их русскими аналогами. Стоит только надеяться, что такие слова как «керри» и «мидер» в последствии приобретут русскоязычные аналоги.

Список используемых источников:

1. Степанцева О. А. "СОЦИАЛЬНЫЙ ПОРТРЕТ" ГЕЙМЕРА // Известия Российского государственного педагогического университета им. А. И. Герцена. СПб., 2007. Т. 6. № 24. С. 80-83.
2. Лутовинова О. В. Виртуальный дискурс как одно из направлений в исследовании киберпространства // Вестник Московского государственного областного университета. Сер. Лингвистика. 2009. № 1. С. 26-32.
3. Полозова С. В. Иноязычные заимствования как источник пополнения лексико-фразеологического состава современных русских жаргонов: научная статья. ... канд. фил. наук: 28.05.2008 / С. В. Полозова // - Воронежская государственная технологическая академия, 2008. - С. 5.
4. Греховодова В. А. «СПЕЦИФИКА ФУНКЦИОНИРОВАНИЯ ЛЕКСИКИ КИБЕРСПОРТИВНОЙ ДИСЦИПЛИНЫ DOTA2» // Белгородский государственный национальный исследовательский университет» Белгород 2017 № 3. С. 37-43.
5. TeamSpeak PuckChamp Dota2 - играем с young G// URL: <https://www.youtube.com/watch?v=KHMBaoYACiY&t=205s>.

Sidorenko V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Anglicisms on the esports community.

The article will focus on the influence of Anglicisms on the esports community. The methods of formation and types of Anglicisms with examples of use are considered.

Key words: *Esports, Anglicisms, English language.*

**Секция 6.2.
Реклама и связи с общественностью**

УДК 378.1
ГРНТИ 14.35.07

К ВОПРОСУ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ LMS MOODLE В СОВРЕМЕННОМ ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

И. А. Андриянов, А. В. Кульназарова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С появлением различных инноваций в коммуникационных сетях и при влиянии различных внешних факторов, традиционные средства передачи знаний в школах, колледжах, высших учебных заведениях и программах повышения квалификации также в значительной степени потерпели изменения. Использование образовательной среды Moodle позволяет создавать новые форматы обучающей коммуникации в международном пространстве.

LMS Moodle, дистанционное образование, образовательная среда, новые технологии в образовании, онлайн-образование

Дистанционные технологии позволяют проходить обучение в любом месте и в любое время, интенсифицировать работу с любым дополнительным учебным материалом и компенсировать нехватку фонда по учебно-методической литературе в учебных заведениях, что актуально для традиционного режима получения новых источников. А также применение дистанционных технологий для вузов в настоящее время становится конкурентным преимуществом, используется в продвижении и влияет на имидж и репутацию.

Учебные организации, предлагающие частичное или даже полное онлайн-образование, часто используют системы управления обучением, чтобы помочь студентам отслеживать как свои учебные материалы, так и прогресс в обучении. На рынке доступны различные программные инструменты для решения самых разных задач в процессе получения знаний. Это определенные технологии, которые предоставляют широкие возможности и известны как LMS – платформы (Learning Management System – система управления обучением).

Одна из самых популярных систем управления обучением - Moodle.

Moodle - это виртуальная образовательная среда с бесплатным программным обеспечением, в основе которой лежат динамичные и интерактивные концептуализации различных курсов и учебных программ[1].

«Moodle» является аббревиатурой названия «Modular Object-Oriented Dynamic Learning Environment» (модульная объектно-ориентированная динамическая среда обучения). Основанная на сетевых технологиях система управления обучением была разработана преподавателем университета Пэрт из Австралии Мартином Доугиамасом (Martin Dougiamas) и введена в эксплуатацию в 2002 г [1].

Moodle означает модульную объектно-ориентированную динамическую среду обучения. Система имеет открытый код (под лицензией GPL (General Public License – универсальная общественная лицензия, которая предоставляет пользователю право копировать, модифицировать и распространять программу).

Статистика показывает, что около 14 миллионов пользователей посещают около 1,4 миллиона курсов, распространяемых этой системой по всему миру.

Moodle представляет некоторые общие возможности, свойственные практически для всех подобных инструментов электронного обучения: лекции, тексты, презентации, гиперссылки, но он также предоставляет определенные варианты подключаемых модулей, отвечающие современным трендам и потребностям студентов форматы:

- блоги;
- чаты;
- базы данных;
- глоссарии;
- графика;
- анкеты;
- тесты.

Текущие средства инфраструктуры, принятые Moodle, позволяют ему поддерживать множество опций подключаемых модулей, процессы регистрации и аутентификации, а также шаблоны баз информации вопросов [1].

Далее стоит отметить ключевые преимущества системы управления обучением Moodle.

Централизованная информация. Информация, предоставляемая в LMS Moodle, централизована. Это означает, что к каждой конкретной области можно подойти с помощью системы управления обучением независимо от дизайна и содержания курса. Студенты, использующие LMS, получают доступ к учебным модулям всякий раз, когда они им нужны. Кроме того, учащимся легко работать с педагогами и с другими обучающимися. Это дает учащимся ощущение контроля над процессом обучения.

Эффективное обучение. Moodle - это платформа с открытым исходным кодом. Система управления обучением Moodle поддерживается большим мировым сообществом экспертов и разработчиков Moodle. Оно постоянно обновляется и понимает требования учащихся, предлагая лучший пользовательский опыт.

Простота отслеживания и отчетности. Система управления электронным обучением Moodle обеспечивает постоянное и поступательное обучение. Это не мешает рабочему процессу учащегося и экономически эффективно. Для преподавателя прогресс учеников можно легко отслеживать.

Система обратной связи. Она необходима для анализа успеваемости учащихся и требований. А также понимания уровня достижений. Это также помогает в сборе ответов на содержание курса.

Экономия времени. Поскольку система управления электронным обучением предоставляет информацию в соответствии с потребностями учащихся, то занятия могут проходить в удобное для пользователя время. Отчеты об успеваемости создаются автоматически, а оценки предоставляются учащимся [2].

В России большой основной опыт использования системы можно увидеть, прежде всего, в технических направлениях обучения. А также ее активное использование пришлось на период пандемии 2021 года [2].

Примером практического применения системы на международном уровне можно назвать обучение на курсе академического английского языка в Канадском колледже Conestoga (Conestoga college).

В рамках программы «Advanced English» с применением инструментов Moodle и интеграции на страницу курса учебных материалов и комментариев к ним, а также коммуникации с преподавателем в режиме реального времени, слушатели дистанционных курсов из России, Китая, Индии, Бразилии и Казахстана создали социальный проект «Place attachment», включающий исследования по причинам привязанности людей к определенному географическому месту и являющийся итоговым для получения аттестации.

В Австралийском университете Wollongong, в рамках факультета Media and Communications, система Moodle используется в каждой из дисциплин и интегрирована в официальный сайт вуза. При попадании на главную страницу Moodle на ней представлено несколько блоков, каждый из которых является определенным предметом. Как пример можно взять «Global mediascape». При переходе на предметный блок можно увидеть несколько подблоков: 1) communication with the teacher (связь с преподавателем, где все его ссылки и контакты; 2) subject outline (расписание предмета); 3) assignments (задания); 4) calendar of topics (тематический календарь с распределением информации по каждой неделе курса, в котором написано что будет изучено и какие материалы дополнительно прочитать или посмотреть (вместе с ссылками)). Пройденный материал отмечается после выполнения всех заданий и изучения всего материала. Также вся обратная связь и комментарии от преподавателя видны под каждым заданием

Существует конкуренция с появлением на рынке других систем управления обучением. Но обновления и постоянные улучшения в Moodle делают ее самой популярной платформой до сих пор. Moodle используется в качестве системы управления электронным обучением благодаря необычным функциям и плагинам, которые она предлагает. В связи с непрерывным ростом индустрии онлайн-обучения будет интересно посмотреть, чего еще она предложит в будущем.

Список используемых источников:

1. Содикова, Ф. С. Обучение с Moodle в высшем образовании / Ф. С. Содикова, Р. Б. Сариев. — Текст : непосредственный // Молодой ученый. — 2019. — № 19 (257). — С. 19-22. — URL: <https://moluch.ru/archive/257/58547/> (дата обращения: 15.11.2022).
2. Тальшева И. А., Салимуллина Е.В. Работа в системе дистанционного обучения LMS Moodle: методические рекомендации. Учебно - методическое пособие. Елабуга: Изд-во Елабужского института К(П)ФУ, 2018. — 42 с URL: <https://kpfu.ru/portal/docs/F2121314189/Rabota.v.LMS.MOODLE.pdf> (дата обращения 08.11.22).

Andriyanov I., Kulnazarova A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

On the issue of using the LMS Moodle system in the modern educational process.

With the advent of various innovations in communication networks and under the influence of various external factors, the traditional means of transferring knowledge in schools, colleges, higher education institutions and professional development programs have also undergone a significant change. The use of the educational environment Moodle allows you to create new formats of educational communication in the international space.

Key words: LMS Moodle, distance education, educational environment, new technologies in education, online education.

УДК 659.13/.17
ГРНТИ 19.71

ПЕРСПЕКТИВЫ И РИСКИ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНТЕРНЕТ-РЕКЛАМЕ

И. Е. Астафьева-Румянцева, С. О. Аминов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Технологии интернет-рекламы за 20 лет совершили огромный скачок от продажи рекламных площадей, до создания персонализированного опыта для каждого из более пяти миллиардов пользователей Интернета. Искусственный интеллект – стремительно развивающаяся технология, которая меняет способы распространения рекламы, сегментирования аудиторий, и принятия маркетинговых решений. В статье обобщаются перспективные направления и вероятные риски развития ИИ-технологий в области интернет-рекламы.

искусственный интеллект, интернет-реклама, потребительский опыт, персонализация.

Искусственный интеллект постепенно входит во все сферы экономики, от армии до юриспруденции, от медицины до тяжелой промышленности. Цифровая реклама – главная статья заработка крупнейших IT-компаний мира: Google, Meta* (организация, деятельность которой запрещена на территории Российской Федерации), совокупная выручка которых составляет более 300 млрд. долларов [1]. За 10 лет выручка этих компаний от сегмента интернет-рекламы выросла на 641%, как видно на рис. 1. В прошлом году глобальные совокупные затраты на рекламу в цифровом пространстве компаний составили 521 млрд. долларов, что в 5 раз больше чем сумма трат на наружную рекламу, рекламу на радио, в газетах и журналах. 81.5% годового дохода Google в 2021 году пришлось на рекламу [2].

Являясь крупнейшей компанией в сфере интернет-рекламы, Google постоянно инвестирует в разработку искусственного интеллекта для роста эффективности и прибыльности этого сектора. Google справляется с этой задачей. Выручка от рекламы выросла на 380%, от с 43.6 млрд. долларов в 2012 до 209.5 в 2022. Осенью 2016 года исполнительный директор Google Пичаи Сундарараджан заявил, что Google меняет вектор развития: вместо первой компании в сфере разработок для мобильных телефонов, Google станет передовой компанией в отрасли искусственного интеллекта. Опрос среди руководителей IT-компаний внедряющих ИИ-решения, показал, что важнейшими целями внедрения ИИ для них являются: автоматизация, оптимизация процессов и улучшение продуктов [3]. Крупнейшей площадкой для размещения и рекламы, а также главным источником прибыли для Google является платформа Google Ads. Через эту платформу рекламодатель может разместить рекламу, а она, с помощью искусственного интеллекта, проведет аукцион и покажет релевантную для пользователя рекламу, в нужном месте, в нужное время и по оптимальной для компании цене. Такая практика называется программная реклама, она начала внедряться Google с 2012 года. Со временем эту

модель переняли большинство интернет-компаний, в том числе Яндекс и ВКонтакте.

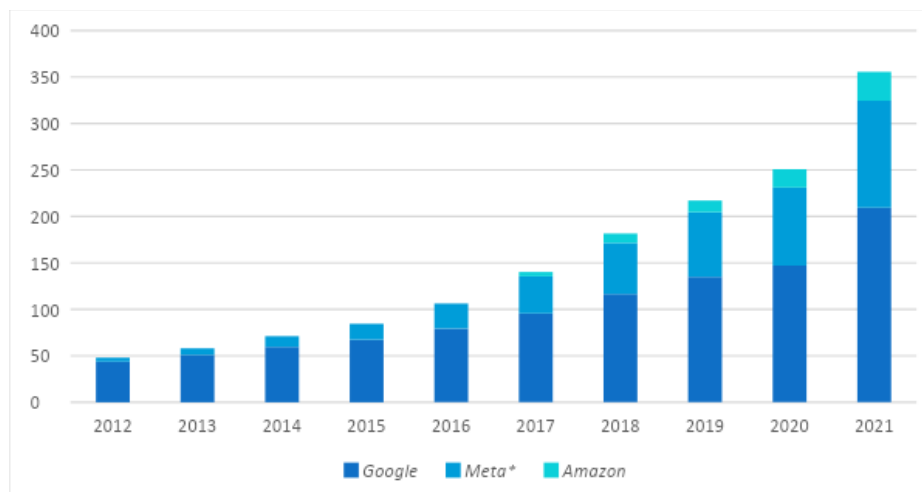


Рис. 1. Выручка от сегмента интернет-рекламы у Google, Meta и Amazon (2012-2021) в млрд. долл.

Использование таких платформ позволяет персонализировать опыт потребителя, и повысить конверсию рекламы. Достигнуть такого уровня персонализации используя труд маркетологов было бы невозможно. 26% руководителей IT-компаний, использующих ИИ, отмечают, что они смогли добиться значительного превосходства над теми конкурентами, кто не использует ИИ-решения.

В ближайшие три года искусственный интеллект в рекламе и маркетинге будет стремительно развиваться в следующих областях: персонализация рекламы, сегментирование аудиторий, создание рекламы и принятии решений [4].

Персонализация в рекламе строится на автоматическом сборе и анализе данных о пользователе. ИИ анализирует демографические и поведенческие характеристики, привычки и желания. Комплекс этих характеристик дает возможность алгоритмам подобрать релевантную для пользователя рекламу. Исследования показывают, что 71% потребителей хотели бы видеть более индивидуализированную рекламу, но в меньших количествах [5]. По статистике, такая реклама имеет повышенную кликабельность CTR (*click through rate*) и рентабельность. Персонализированный потребительский опыт повышает конверсию на 8%. Важным направлением в использовании ИИ для создания индивидуального опыта является разговорный маркетинг. Разговорный маркетинг – это максимально персонализированный подход к посетителю сайта в режиме реального времени. Наиболее часто реализуется через онлайн-чат, который работает либо по заранее написанному сценарию, либо с помощью искусственного интеллекта. Последний становится более перспективной технологией, так как разработки в области разговорного ИИ приближаются к моменту, когда пользователь не сможет отличить реального человека от компьютера. Исследования показывают, что 40% потребителей не волнует, кто отвечает на сообщения: реальный человек или чат-бот, а 48% предпочли бы

общаться с компанией и делать покупки через чат бот. Таким образом, глубокая индивидуализация и создание персонализированного потребительского опыта становятся отраслевым стандартом и невозможны без обширного использования ИИ-технологий.

Машинное обучение – класс методов искусственного интеллекта. В рекламе эти методы используются для сегментирования аудитории: разбиения ее на отдельные группы (кластеры), схожие по интересам, демографии и прочим признакам. Для этого алгоритмы анализируют всю имеющуюся информацию о пользователе, и определяет наиболее релевантный для него контент. Эта технология оптимизирует расход рекламного бюджета, сокращая процент случаев, когда аудитория видит неподходящую для себя рекламу. Нерелевантная реклама снижает вовлеченность пользователей и процент конверсии [6].

Также искусственный интеллект выводит A/B тестирование на новый уровень. Предиктивные модели позволяют прогнозировать потенциальный CTR и релевантность новой рекламы, основываясь на успехах предыдущей. Используя искусственный интеллект можно тестировать и улучшать рекламные сообщения еще до выпуска. ИИ дает больше творческой свободы маркетологам, позволяя больше экспериментировать, находить новые решения.

ИИ находит применение в оптимизации расхода рекламного бюджета. Поскольку алгоритмы постоянно обучаются на поступающей информации, они могут самостоятельно анализировать ключевые показатели эффективности текущих и будущих рекламных кампаний, регулировать расход бюджета и повышать ROI (окупаемость инвестиций).

При всех преимуществах, новые технологии всегда несут неизвестность и потенциальные риски. Руководители 56% компаний, внедряющих ИИ-решения, отмечают, что скорость внедрения искусственно замедляется из-за растущих рисков. Основными рисками от внедрения ИИ-решений в интернет-рекламе являются: предвзятость в работе алгоритмов, некачественные данные для обучения и нарушение законов о персональных данных.

В ходе растущей автоматизации ИИ все чаще принимает решения за человека. Поскольку алгоритмы создаются программистами и обучаются на подготовленных наборах данных, они воспроизводят человеческие предубеждения, обычно в отношении маргинальных слоев населения. Часто алгоритмы воспроизводят расовые и гендерные стереотипы, дискриминацию по возрасту, заработку, месту проживания. Особенность проблемы заключается в том, что маркетологи и лица принимающие решения часто не знают, как работает алгоритм, поэтому выявить эти ошибки могут только специалисты. По этой причине маркетологи не могут узнать кокой из заданных целевых аудиторий, как и когда ИИ показывает рекламу. Например, ИИ может нерационально таргетировать отдельный сегмент целевой аудитории, сокращая расходы на остальные. Такие действия могут повредить имидж бренда и снизить ROI рекламных кампаний [7].

Топливом для работы искусственного интеллекта являются данные, на них происходит обучение. Нерепрезентативные, неполные данные могут нарушить обучение алгоритма и снизить рентабельность использования.

Большинство стран мира начинают ужесточать законы о защите персональных данных. Поскольку работа искусственного интеллекта постоянно сопряжена с анализом и обработкой данных, в том числе и персональных, компаниям необходимо придерживаться стандартов и законов (например, ФЗ "О персональных данных") в противном случае есть риск получить штрафы и высокие репутационные издержки.

Сегодня, без внедрения ИИ-решений в интернет-рекламе бизнес быстро теряет преимущество в конкурентной борьбе. Поскольку все большее число компаний уже внедряют ИИ-технологии в маркетинговую стратегию, преимущества от опережения конкурентов постепенно сходят на нет. Индустрия искусственного интеллекта стремительно развивается, а крупнейшие корпорации и страны тратят все большее количество средств. Ожидается, что до 2030 года рынок ИИ будет расти на 35% в год. Помогая оптимизировать, автоматизировать и улучшить процессы создания и распространения рекламы и маркетинга, искусственный интеллект вносит новые, до этого неизвестные риски.

Список используемых источников:

1. Global Digital Advertising and Marketing Industry report. 2022. 1 с.
2. How does google make money? Oberlo Advertising [Электронный ресурс]. – Режим доступа: <https://www.oberlo.com/statistics/how-does-google-make-money> (Дата обращения 10.11.2022)
3. Beena Ammanath, Susanne Hupfer, David Jarvis. Report by the Deloitte AI Institute and the Deloitte Center for Technology, Media & Telecommunications. 2020. 7 с.
4. How AI is changing advertising. IBM Watson Advertising [Электронный ресурс]. - Режим доступа: <https://www.ibm.com/watson-advertising/thought-leadership/how-ai-is-changing-advertising#:~:text=AI%20in%20advertising%20refers%20to,smarter%20decisions%20in%20the%20> (Дата обращения 10.11.2022)
5. Adlucent Data. 1000 USA responses. 2016. 4 с.
6. Savica Dimitrieska, Aleksandra Stankovska, Tanja Efremova Artificial intelligence and marketing // Entrepreneurship. 2018. 4 с.
7. Jisu Huh, Ronald J. Faber. Asking Questions of AI Advertising: A Maieutic Approach // Journal of Advertising. 2022. 538 с.

Astafieva-Rumyantseva I., Aminov S.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Opportunities and risks of the use of AI technologies in internet advertising.

Internet advertising technology has taken a huge step forward in 20 years from manual selling advertising space to creating a deep personalized experience for more than five billion Internet users. Artificial intelligence is a disrupting technology that is changing the way advertising is distributed, audience segmentation, and how marketing decisions are made. In this article, we review promising areas and potential risks of using of AI technologies.

Key words: artificial intelligence, online advertising, consumer experience, personalization.

УДК 7.092
ГРНТИ 14.35.19

АНАЛИЗ СТУДЕНЧЕСКИХ КОНКУРСОВ В ОБЛАСТИ РЕКЛАМЫ И СВЯЗЕЙ С ОБЩЕСТВЕННОСТЬЮ

И. Е. Астафьева-Румянцева, В. В. Левченко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Конкурсы в области рекламы и связей с общественностью способствуют повышению интереса студентов к преподаваемым дисциплинам, развитию коммуникативных навыков, творческого мышления, а в конечном счете – совершенствованию качества подготовки будущих специалистов. Участие в профессиональных конкурсах дает возможность начать формировать портфолио специалиста уже в процессе обучения в вузе.

студенческие конкурсы, реклама, связи с общественностью

Вектор обучения в высших учебных заведениях направлен на изучение и усвоение теоретической базы профиля обучения, поэтому участие в конференциях, фестивалях, конкурсах и премиях является дополнительным способом набрать опыта, сформировать портфолио и заявить о себе на рынке. Специфика студенческих конкурсов, ориентированных на отработку профессиональных навыков, заключается в разработке проекта, отвечающего теме номинации или кейс-задаче компании. Как правило, номинации не ограничивают будущий проект определенными критериями, например, фиксированным бюджетом, кейс-задача формулируется в виде конкретного технического задания от компании. Проект должен быть реалистичным и отвечать поставленной цели, креатив и фантазию участники могут реализовать в выборе инструментов и стратегии.

Для анализа были выбраны конкурсы, реализуемые Национальной премией в области развития общественных связей «Серебряный Лучник» при поддержке Российской ассоциации по связям с общественностью и конкурс, проводимый организацией ООО «Серебряный Меркурий» «Young mercury». Данные конкурсы предполагают участие студентов специальности реклама и связи с общественностью, а также смежных направлений и могут быть проанализированы по ряду критериев: уровень, цель, форма участия, номинации, этапы реализации, жюри и критерии оценивания.

Студенческий конкурс «Лучник Future» от Национальной премии в области развития общественных связей «Серебряный Лучник» — это Всероссийский конкурс студенческих команд на лучшее решение бизнес-задач. К участию допускаются команды от 5 до 7 студентов бакалавриата или магистратуры, обучающихся по специальностям, связанным с менеджментом организации, рекламой, связями с общественностью, маркетингом. Впервые конкурс был реализован в 2021 году. Участие бесплатное, регистрационный взнос отсутствует, что, безусловно, увеличивает количество участников. Основная цель – «организовать работу студенческой команды с существующими

проблемами и затем дать возможность воплотить решение в жизнь в коллективе бизнес-структуры» [1]. Номинации формулируются в виде задач от общественных или коммерческих организаций, отражают реальные проблемные ситуации или специфику современного уровня развития отдельных направлений экономической и социальной жизни страны.

Конкурс проходит в два этапа: первый – регистрация команд и их решений, работа Экспертного совета и определение шорт-листа – списка команд на публичную защиту перед жюри; второй этап – презентация решений команд, участие в церемонии награждения [1]. Оценивание решений проводит экспертный совет конкурса. Критерии оценивания на каждом этапе разные: первый этап включает аналитическое обоснование решения, эффективность решения в соответствии с заявленными KPI, креативность, применение подхода Helicopter View, оформление решения — визуальный успех презентации, возможность применения готового решения в настоящем времени (каждый критерий равен 100 баллам). Второй этап включает мастерство изложения материала и общения с аудиторией, презентационную креативность, точность и содержательность ответов на вопросы (каждый критерий равен 100 баллам). Команда может подать заявку на решение как одного, так и нескольких кейсов одновременно.

Конкурс «Хрустальный апельсин», являясь молодежным образовательным проектом, существует с 2000 года, организаторами которого выступают: Молодёжный центр развития связей с общественностью «Хрустальный Апельсин», Общественная палата Российской Федерации, Российская Ассоциация по связям с общественностью (РАСО), Ассоциация преподавателей по связям с общественностью (АПСО), Ассоциация директоров по коммуникациям и корпоративным медиа России (АКМР) [2]. «Хрустальный апельсин» — Северо-запад» — региональный этап Всероссийского конкурса студенческих работ в области связей с общественностью и медийных технологий «Хрустальный апельсин». Его целью является - выявление талантливых студентов, содействие «их успешному карьерному старту и профессиональному росту», что, по мнению организаторов, становится вкладом в «формирование будущей интеллектуальной элиты страны» [2]. В конкурсе принимают участие студенты в области связей с общественностью и медийных технологий северо-западного региона. Конкурсные номинации делятся на три блока: «Флагманские номинации – тема года», «Базовые номинации» и «Специальные номинации». На конкурс могут быть представлены реализованные проекты, проекты готовые к реализации, аналитика, исследования, учебные кейсы.

Региональный этап включает в себя регистрацию проектов, оценивание проектов и церемонию награждения. Оценивание проектов проводит экспертный совет конкурса, попечительский совет и жюри. Оценка работ осуществляется в два этапа: первый этап - оценка экспертного совета, второй - оценка попечительского совета и жюри. Совокупная оценка выражается в формировании шорт-листа победителей региональной премии Конкурса. Определение победителей осуществляется на основе следующих критериев:

аналитическая обоснованность стратегии и тактик проекта, оригинальность и творческий замысел проекта, социальная значимость проекта, эффективность и результативность проекта, презентационная креативность проекта. Количество баллов, начисляемых согласно перечисленным критериям, в положении конкурса не указано. Организационный взнос отсутствует.

Конкурс «Young mercury» – конкурс рекламных проектов для студентов по направлениям подготовки, специальностям и профилям: «Реклама и связи с общественностью», «Маркетинг», «Дизайн». Участие в конкурсе индивидуальное или командное (не более 3 человек), участие в конкретной номинации предполагает оплату организационного взноса в размере 350 рублей за одну номинацию. Участники имеют право участвовать в нескольких номинациях одновременно [3]. Цель конкурса – способствовать совершенствованию мастерства студентов через взаимодействие с экспертами компаний-брифодателей и повышению конкурентоспособности в образовательном и профессиональном пространстве. Номинации представляют собой рекламные брифы от российских компаний.

Конкурс проходит в два этапа. Первый этап объединяет: регистрацию команды на сайте конкурса, оплату взноса, размещение проекта в личном кабинете команды, анализ и оценку работ для формирования шорт-листа. На втором этапе осуществляется публичная защита проектов, торжественное награждение. Жюри формирует рейтинг проектов ориентируясь на следующие критерии: соответствие теме; наличие исследовательской части как обоснования предлагаемых решений; коммуникативная составляющая презентации и её дизайн; нестандартность и креативность решения задачи; качество защиты проекта [3]. Максимальное количество баллов, выставляемое членами жюри - 15 баллов.

На сегодняшний день «Лучник Future», «Хрустальный апельсин» — Северо-запад» и конкурс «Young mercury» наиболее популярные конкурсы студенческих проектов в области связей с общественностью. Они ежегодно объединяют несколько тысяч студентов из российских регионов. За 2022 год в конкурсе «Лучник Future» приняло участие более 400 студентов из 17 городов России; 70 команд из 34 вузов подали заявки на участие в первом заочном туре; представили 86 решений для задач от партнеров проекта в области рекламы, связей с общественностью, медийными коммуникациями, брендинга, профессионального образования и менеджмента, организации движения донорства и благотворительности. «Хрустальный апельсин» — Северо-запад» охватил 35 высших учебных заведений региона, студенты предложили более 800 проектов в области связей с общественностью и медийных технологий, победители отправили проекты на федеральный уровень конкурса «Хрустальный апельсин». На «Young mercury» за 2022 год было подано более 50 проектов, в шорт-лист попало 9 проектов из разных высших заведений страны. Каждый год данные конкурсы объединяют между собой более 3000 студентов России заряжая мотивацией, и стремлением увлечься в мир коммуникационной индустрии, выбранной профессии.

Список используемых источников:

1. Официальный сайт конкурса «Лучник Future» [Электронный ресурс]. URL: <https://luchnik.ru/competitions/future/> (Дата обращения: 11.11.2022).
2. Положение о региональном этапе XXII открытого Всероссийского конкурса студенческих работ в области связей с общественностью и медийных технологий «Хрустальный апельсин» — Северо-запад 2022 [Электронный ресурс]. URL: <https://rso.spbstu.ru/userfiles/files/docs/polozhenie-NA.pdf> (Дата обращения: 11.11.2022).
3. Официальный сайт конкурса «Young mercury 2022» [Электронный ресурс]. URL: <https://young.silvermercury.ru> (Дата обращения: 11.11.2022).

Astafieva-Rumyantseva I., Levchenko V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Analysis of student competitions in the field of advertising and public relations.

Competitions in the field of advertising and public relations help increase students' interest in the disciplines taught, develop communication skills, creative thinking, and ultimately improve the quality of training of future specialists. Participation in professional competitions makes it possible to start building a portfolio at the time of training.

Key words: student competitions, advertising, public relations.

УДК 792.03
ГРНТИ 18.45.07

«БДТ DIGITAL» КАК ПРОСТРАНСТВО ТЕАТРАЛЬНОЙ КОММУНИКАЦИИ

И. Е. Астафьева-Румянцева, Я. Г. Добычина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Принимая во внимание современные способы коммуникации человека с миром с помощью мобильных технологий, театр адаптирует свой продукт к новым условиям взаимодействия человека с культурой и стремится составить конкуренцию другим медиапродуктам, которыми располагает современный пользователь смартфона. Пандемийные ограничения позволили российскому театру укрепить позиции в интернет-пространстве, существенно расширив свой функционал. Взаимодействие с соцсетями, видеохостинговыми и стриминговыми сервисами, а также сайтами театров в короткие сроки развивается из способа обслуживания имиджевых потребностей театра в полноценную художественную стратегию, объединяющую и демонстрацию записей спектаклей, и создание новых постановок, с расчетом на сетевые возможности, (компьютерная игра, сервисы для видеоконференций, чат-боты, программы, и актуальную коммуникацию со зрительской аудиторией).

digital-teatr, экспериментальный театр, цифровые коммуникации, Zoom-спектакль, Minecraft-спектакль

Растущий интерес российских театров к цифровизации и технологизации искусства, основан на нескольких объективных предпосылках. Во-первых, это пандемия коронавируса 2020 года, видоизменившая коммуникационный пласт и поспособствовавшая максимально ускоренному развитию альтернативных площадок для демонстрации художественных манифестов. Платформы Zoom, Skype, Google Meet, а также голосовые чаты в Telegram, прямые трансляции в Instagram и «ВКонтакте» послужили бескрайним полем для самовыражения и открытию целого ряда жанров, объять и исследовать которые пока не представляется возможным по причине отсутствия конкретной методологии. Однако театрално-критическая общественность и простые зрители имеют право рефлексировать на эту тему, так как отдельные особенности цифрового театра роднят его с театром традиционным.

Во-вторых, технологический прогресс не мог не сказаться на развитии театра, так как в его компетенции – поиски ответов на «вечные» вопросы посредством адекватного времени инструментария. Соцсети, вооруженные внушительным спектром коммуникативных возможностей, позволяют расширить эстетические горизонты и взглянуть на проблемы искусства по-другому, нестандартно и современно. В рамкой данной статьи мы ещё столкнёмся с обоснованием эффективности цифровых коммуникаций в связке с театралной практикой. Это и пресловутое правило четвертой стены, которое молодые режиссёры из команды БДТ стремятся преодолеть, и точное попадание

в изначальный драматургический рисунок спектакля посредством digital-инструментов.

Пандемийные ограничения вынудили российские театры решать задачу виртуализации своей деятельности различными путями. Причём для одних это было вынужденной мерой, а для других – шагом вперёд, своеобразным путем решения давным-давно назревавших вопросов. Для петербургского Большого драматического театра цифровизация началась задолго до пандемии. Локдаун внёс коррективы в этот процесс. Претерпевшая изменения концепция развития театра показала и доказала, что даже в стеснённых обстоятельствах театральное искусство способно эффективно развиваться, а театр – осваивать новые формы и приобретать новые аудитории. Обновлённый проект получил ёмкое название «БДТ Digital», где аббревиатура сочетается с наименованием виртуального стиля жизни театра, существующего как бы параллельно с «офлайн»-сценой. Эта любопытная дихотомия существует и по сей день – недаром «БДТ Digital» составлен по принципу «сезонности» с чётким планом, отдельной командой создателей и веб-сайтом с архивами постановок 2020, 2021 и 2022 годов.

Создание полноценной многофункциональной онлайн-площадки легко адаптировало театр к особенностям существования в среде Интернет. Художественный руководитель БДТ Андрей Могучий весной 2020 года так описывал общую структуру проекта: «Сейчас, когда мы все разобщены, как никогда возросла ценность человеческого контакта. Профессия артиста предполагает коллективное творчество, предполагает обмен энергии со зрителем. И отсутствие такого контакта, такого обмена губительно не только в человеческом, но и в профессиональном смысле слова. Именно поэтому, прежде всего поэтому, и возник «БДТ Digital» <...> Для меня это, в первую очередь, социальный проект». Назвав «БДТ Digital» «социальным проектом», Могучий задал ещё один уникальный вектор развития онлайн-площадки, трансформировавший её в большую миссию и бесконечное путешествие в поисках идеальной театральной формы.

Структура «БДТ Digital» [1] довольно проста – она подразумевает большие рубрики с контентом, опубликованным на официальном сайте проекта. Каждая рубрика сопровождается популярным в интернет-пространстве знаком хэштега: #Сегодня (раздел, похожий на репертуарные сводки, афиши), #СетевойТеатр, #Радиотеатр, #ФизикиЛирики, #СоциальныйТеатр, #Лаборатория №3, #Стрим и #Архив. Впрочем, хэштеги – не только дань трендам, но и простейший способ структурирования, отсылающий к временам расцвета блогов «Живого Журнала» и микро-форматов наподобие «Твиттера» или стены во «ВКонтакте». Разумеется, чёткая структурность обусловлена как техническими, так и эстетическими критериями – так, раздел #Радиотеатр имеет вполне очевидную историческую подоплёку, возрождение традиций и возобновление интереса к разговорным жанрам «театра у микрофона», отдельного вида искусства, положившего начало революции радио, подтверждение его влияния на умы широкой публики. На контрасте с ним – #Стримы, тренд, с которым на ты молодая аудитория. Стримы актуальны для платформ YouTube, «ВКонтакте»,

Instagram – то есть тех соцсетей, где целевая аудитория нацелена на общение в режиме реального времени, невзирая на расстояние, социальный статус и другие объективные препятствия.

#СетевойТеатр включает в себя экспериментальные форматы. Постановки в этом разделе рассчитаны на юную публику, проводящую свой досуг у компьютера за выполнением виртуальных квестов, проще говоря – игровых задач, не обременённых сложностью и детальностью. Данный раздел тем не менее интересен своими нестандартными ходами в сфере осмысления художественной классики, золотого фонда русской и мировой драматургии. #ФизикиЛирики – родственен #Стримам и объединяет размышления артистов БДТ о синтезе науки и искусства, их слияния под влиянием объективных технологических процессов. В частности, это дискуссии со специалистами в области высокочастотных измерительных систем и проблем хранения опасного ядерного топлива. #Лаборатория №3 также характеризуется дискуссионностью и глубиной обсуждаемых вопросов. Онлайн-формат позволяет задать вопрос в рамках представленной на суд публики проблемы – как и в случае с вышеописанным разделом, речь идёт о синтезе науки и искусства. Художники и учёные пытаются найти взаимопонимание в оценке вопросов социальной, политической и, так получилось, эпидемиологической ситуации (первые выпуски проекта записывались и публиковались в первую волну коронавируса).

Остановимся подробнее на тех структурных элементах «БДТ Digital», которые вызвали наибольший интерес у критиков и зрителей, разберёмся в их специфике и наметим общие художественные тенденции, позволяющие назвать проект самостоятельным явлением в российской и мировой театральной экосистеме.

#Радиотеатр – раздел, стоящий как бы особняком по нескольким причинам. Во-первых, в нём за основу берётся жанр «театр у микрофона» (зародился в 20-е годы XX столетия), утративший свое прежнее значение с расцветом телевидения. Сегодня на новом витке развития интернет-коммуникаций радиотеатр возродился в формате подкастинга. Его обновлённая популярность и полноценная альтернативность классической радиодраме очевидна – через подкасты прикосновение к классике театра стало реальным. Жанры и эстетические каноны радиотеатра, конечно, претерпели существенную эволюцию – и тем не менее ключевой принцип (выход искусства речи за пределы театральных сцен) остался неизменным. На это и опирались создатели проекта – они не только возродили старую традицию, но и придали ей современную огранку. Подкасты позволяют транслировать для аудитории более разнообразный контент и повышают охват площадки, на которой размещаются. В этом смысле Андрей Могучий выступает своего рода пионером жанра, который можно определить как «театрального подкастинга» (в отличие от подкастов о театре как таковом, размещаемых, например, на портале «Культура.РФ»).

Zoom-спектакли и дискуссионные формы постановок – отличительная черта «БДТ Digital», где артисты не просто входят в образ, но конструируют его в режиме реального времени. В результате получается спектакль-стрим, онлайн-версия театрального принципа «здесь и сейчас». В проекте «Выживальщики» [2] (автор – Дмитрий Юшков) артисты БДТ произносили импровизационные монологи перед камерой. В спектакль включались танцевальные перформансы Евгения Шолохова и диджейский сет Ильи Деся – стрим превращался в подобие молодёжных вечеринок со световыми эффектами. Параллельно развивается живое обсуждение пьесы. В комментариях «разворачиваются судьбы» (термин Сергея Азеева) на фоне основного сценического зрелища, что создаёт ощущение театра в театре.

Полноценной площадкой для воплощения рискованных идей виртуальной сцены стала рубрика #СетевойТеатр. В ней режиссёрский коллектив преодолевает грань между реальным миром и кибер-фантазией, на первый взгляд симулирующей реальность в её искажённом, причудливом и местами неприглядном виде. Интересны в этой связи спектакли, созданные студентами Могучего в формате детской компьютерной игры Minecraft – полигональной вселенной, где персонажи и окружающая их действительность конструируются из пикселей. Примечательно ещё и то, что постановки опубликованы на платформах YouTube и «ВКонтакте», где за долгие годы укоренился жанр летсплеев – нише русскоязычного сегмента, где блогеры играют и одновременно общаются с аудиторией, преимущественно подросткового возраста. За основу команда Эдгара Закаряна и Андрея Воронова взяла классические сюжеты: «Недоросль» Дениса Фонвизина, «Моцарт и Сальери» Александра Пушкина и «Вишнёвый сад» Антона Чехова [3]. Все три спектакля имеют одну и ту же специфику: действие погружает зрителя в атмосферу компьютерного экшена. Персонаж оказывается в «пиксельном» мире, изображающем интерьеры самого БДТ, а в зрительном зале он видит перед собой сцену, выполненную всё в том же пиксельном формате. Режиссёр и художник, действуя в тандеме, стремились создать симулятор игры как локальный эксперимент, привлекающий новую аудиторию. Minecraft – как и всё, что связано с подростковыми увлечениями – имеет ярко выраженный эмоциональный вектор, что в полной мере отображено и в «Вишнёвом саду», и в «Моцарте и Сальери», и в «Недоросле».

Эти спектакли не похожи на классические театральные постановки, отражающие детализацию времени или моральных метаний персонажей. Но нарочитая схематичность не является отвлекающим моментом в интерпретации Minecraft-спектаклей «БДТ Digital»: присутствует чётко заданная структура, текст (хоть и упрощённый, наполненный жаргонизмами или укороченными формами оригинальных драматургических реплик), система персонажей, продуманная сценография и простор для пост-рефлексии. Важно, что режиссёр не ставит перед собой цель перенести классическую пьесу в виртуальный симулякр, вместо этого он намеренно упрощает структуру, текст и сюжетную концепцию. Персонажи обмениваются обрывками фраз, схематична и общая презентация разыгрываемой на сцене истории. Нетрудно догадаться, что столь

примитивный стиль изложения истории отсылает к популярным веб-сайтам с пересказом для школьников классических сюжетов в целях наилучшего запоминания логики и последовательности действий.

В рецензии Алексея Исаева «Почувствуй себя подростком» в «Петербургском театральном журнале» фигурирует следующая характеристика Minecraft-спектакля: «В этом точном совмещении (старого и нового, разрушения и создания нового – Я.Д.) — целая бездна смыслов и исторических отголосков, которые поданы в простом и доступном игровом (геймерском) ключе» [4]. У Исаева Minecraft-спектакли и само явление игры Minecraft характеризуются как «мощная образовательная платформа», альтернативным способом общения учителей с учениками на простом и понятном языке. Театральный эквивалент подростковой забавы, таким образом, несёт в себе два ярко выраженных пласта: художественный и дидактический. И прежде всего это диалог режиссёров с новым поколением зрителей, к которым необходим особый подход, не вписывающийся в традиционные рамки. Коммуникативный аспект Minecraft-постановок «БДТ Digital» любопытен не только из-за нестандартного формата – записи спектаклей, опубликованные на YouTube-канале БДТ, сопровождаются возможностью комментариев, каждый пользователь волен высказать свою точку зрения об увиденном. Изначально «Недоросль», «Вишнёвый сад» и «Моцарт и Сальери» транслировались в прямом эфире с опцией онлайн-чата: своего рода упрощённой, экспресс-формой театрально-критической рецензии, но при этом – максимально сжатой.

В истории развития «БДТ Digital» очень важна роль зрителя, его восприятие и обратная связь. «Цифровой театр – ничто иное как игровая коммуникация на расстоянии. А значит нет существенной разницы между онлайн-спектаклем и онлайн игрой» [5]. Этот нехитрый принцип актуален и для отдельной части большой структуры (в частности, вышеупомянутых Minecraft-спектаклей), и для всего проекта «БДТ Digital», существующего в обновлённой театральной реальности, пережившей серьёзную трансформацию, которая пока не до конца отрефлексирована современной критикой.

Список используемых источников:

1. БДТ Digital. [Электронный ресурс]. URL: <https://www.bdtdigital.ru> (дата обращения 11.10.2022).
2. #bdtdigital — Ольга Семенова в проекте «Выживальщики» [Электронный ресурс]. URL: https://vk.com/video-57311413_456239646 (дата обращения: 16.10.22).
3. Например, Minecraft-версия спектакля «Вишневый сад»: Электронный ресурс]. URL: <https://www.youtube.com/watch?v=L9FfoPSzNRY&t=866s> (дата обращения: 06.11.22).
4. Исаев, А. Почувствуй себя подростком [Электронный ресурс]. URL: <https://ptj.spb.ru/blog/pochuvstvuj-sebya-podrostkom/> (дата обращения: 29.09.22)
5. Хитров, А. Спектакли в зуме и вotsape. Как на карантине зарождался цифровой театр – и чем он лучше трансляций обычных постановок [Электронный ресурс]. URL: <https://meduza.io/feature/2020/05/10/spektakli-v-zume-i-votsape> (дата обращения 02.11.2022).

Astafjewa-Rumianzewa I., Dobychina Y.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

«BDT digital» as a space of theatrical communication.

Taking into account modern ways of human communication with the world using mobile technologies, the theater adapts its product to the new conditions of human interaction with culture and strives to compete with other media products available to the modern smartphone user. Pandemic restrictions allowed the Russian theater to strengthen its position in the Internet space, significantly expanding its functionality. Interaction with social networks, video hosting and streaming services, as well as theater websites in a short time develops from a way of serving the image needs of the theater into a full-fledged artistic strategy that combines both the demonstration of recordings of performances and the creation of new productions, with the expectation of network capabilities (computer game, video conferencing services, chatbots, programs, and up-to-date communication with the audience).

Key words: digital theater, experimental theater, digital communications, Zoom performance, Minecraft performance.

УДК 659.443/446

ГРНТИ 71.01.14

ОСОБЕННОСТИ МАСКОТОВ И ИХ СОЗДАНИЯ ДЛЯ КОММЕРЧЕСКИХ БРЕНДОВ

И. Е. Астафьева-Румянцева, М. А. Богданова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Маскоты в наши дни становятся всё более популярным средством продвижения. Многие бренды придумывают своих персонажей. Но не все четко понимают, для чего они нужны и как правильно создать маскота, чтобы он стал эффективным средством продвижения, а не просто красивой статичной картинкой. В данной статье рассматривается роль маскотов (персонажей-талисманов) в деятельности брендов, а точнее упомянуты следующие вопросы. Что такое маскот? Для чего нужны маскоты? Как создать удачного маскота? А также рассмотрены несколько кейсов.

маскот, продвижение, бренд, рекламная деятельность, SMM

Маскот или персонаж-талисман — это какой-либо герой, олицетворяющий собой некое сообщество людей, организацию, бренд и т.д. Сам термин маскот известен с 1867 и произошел от французского «La Mascotte», что означает «счастливый талисман», «колдовство», «очарование» или «амулет». Сегодня маскоты это ещё не заезженный в SMM маркетинговый-инструмент, помогающий привлекать аудиторию и вовлекать её в коммуникацию [1].

Понятие «маскот» зародилось в начале двадцатого века, в футбольной среде. «La Mascotte» — так называли символических животных, которые были талисманами футбольных клубов. Впоследствии эти образы перекочевали в тематические товары, посвящённые клубам. Первый полностью придуманный маскот впервые был использован лишь в 1966 году для чемпионата мира по футболу в Англии – львёнок Вилли.

Маскоты могут быть изображены в различных образах: человек, животное, какой-либо предмет или выдуманное существо. Выбор образа маскота зависит от идеи бренда, его позиционирования и целевой аудитории. Он должен максимально соответствовать своей первостепенной задаче – созданию эмоциональной связи с потребителем [2]. Поэтому чаще всего бренды стараются придумать для себя как можно более милых персонажей. И именно на этом этапе создание маскота порой заканчивается, он помещается на страницу сайта или продукцию и останется лишь пустой красивой картинкой.

Какие задачи выполняют маскоты в сфере продвижения брендов?

1) Повышают узнаваемость бренда. Хорошо продуманный маскот порой запоминается целевой аудиторией даже лучше, чем слоган или логотип.

2) Налаживают контакт пользователей с брендом или компанией. Маскоты делают стиль общения с клиентами более доступным и легким. Многие из персонажей имеют собственные аккаунты в социальных сетях, что позволяет им общаться с аудиторией на темы, связанные с товарами или услугами бренда.

3) Стимулируют желание купить продукт или услугу. Особенно хорошо маски работают на детскую аудиторию, так как чаще всего выглядят как герои мультиков. Их изображение на продукции или участие в рекламе как магнит притягивает потенциальных клиентов. Но также их симпатичный вид привлекает и более взрослую аудиторию, так как воздействует на эмоции и чувства.

4) Делают сложное обслуживание проще. Маскотов используют, чтобы в более простой форме объяснять суть бренда и почему он необходим потребителям, кроме того, через персонажа легче показать правильное использование продвигаемых товара или услуги и создать необходимые ассоциации, связанные с изображением героя, цветами, звуками и т.д.

5) Выделяют бренд на фоне конкурентов. Порой, если бренд визуально скучный и не имеет особых отличий от конкурентов, только необычные маски помогают обратить на себя внимание аудитории, выделить его и сделать привлекательным для приобретения.

6) Помогают создавать визуальный контент про бренд. Странички маскотов в социальных сетях привлекают большую аудиторию, особенно если используется сторителлинг. Наличие готового персонажа облегчает создание визуального контента, включающего как изображения, так и видео ролики про жизнь бренда и маскаота. [3]

Маскот — это в первую очередь персонаж. С отдельной историей, со своим характером и своим стилем, нельзя просто сгенерировать случайную картинку и назвать её своим персонажем. При создании своего фирменного персонажа-талисмана бренду следует придерживаться ряда правил:

1) **Маскот должен быть «живым».** Нельзя создать один единственный рисунок, разместить его на всех площадках и продукции. Несколько различных поз, разнообразная мимика и одежда сделают героя более настоящим и интересным. И самое главное – у маскаота должно быть имя, по которому его и будут опознавать.

2) **Использование анимации усиливает эффективность.** Этот пункт идейно продолжает предыдущий. Анимированный персонаж не только будет «живее», но и более харизматичным. Это позволит ему получить ещё один необходимый для успешного маскаота пункт – характер. Не стоит забывать и об «недостатках». Небольшие выделяющиеся особенности помогут заполучить внимание той части аудитории, которая также имеет эти черты (торопливость, косолапость, такие внешние черты как необычные анатомические возможности, характер, цвет, украшения и т.д.).

3) **Маскоту необходим уникальный характер.** Красивый внешний вид — это не самая важная часть при разработке маскаота. Он может быть самым привлекательным, но если у него не будет запоминаемых и узнаваемых черт характера, то такой маскот не принесет успеха. Смешные фразы, уникальная мимика и поведение – через эти мелочи аудитория будет лучше узнавать маскаота и больше проникаться к нему симпатией. Маскот может практически напрямую общаться с аудиторией, потому его характер должен быть приятным, но и иметь

уникальные черты, чтобы коммуникация с ним была более интересна общественности.

4) **Персонаж должен быть гибким.** Маскот должен легко адаптироваться к особым событиям. Так как маскот это олицетворение бренда в реальном мире, то, соответственно, он должен реагировать на различные мировые события, такие как Рождество, День святого Валентина и другие праздники, и процессы.

5) **Окружение и быт сделают героя интереснее.** Маскот не должен существовать в отрыве от мира. Наличие у маскота «дома», интерьер которого обустроен в стиле персонажа, друзей и семьи, с которыми он контактирует, также повышают заинтересованность в нем общественности. Некий бэкграунд делает образ персонажа многогранным. Так как наличие уникального прошлого, которое маскот может раскрывать через коммуникацию с аудиторией, уже сделают его не просто картинкой, а героем истории, которая и привела его к этой компании.

6) **Для персонажа важна проработка оптимального способа коммуникации.** При создании маскота нужно определить, на какую аудиторию он будет работать и какие задачи решать при коммуникации. Тот персонаж, что будет работать на детей, не сработает с молодежной аудиторией, как и тот, что направлен на взрослую.

Персонажи-маскоты могут играть следующие роли:

- друг. Маскот выполняет типичные приятельские функции: развлекает, поддерживает, советует, помогает;

- эксперт. Цель бренд-персонажей — повышать знания у аудитории о товарах или услугах компании, делиться опытом;

- супергерой. Маскот помогает решать проблемы пользователей, причем обычно делает это с помощью предлагаемого товара или услуги;

- гарант качества. По задумке, этот бренд-персонаж участвует в производстве товаров, знает все от и до и подтверждает высокое качество продуктов.

- герой- антагонист. Отрицательные персонажи тоже иногда становятся маскотами. Правильная проработка его истории характера и мотивации могут сделать из персонажа любимчика аудитории, за которого будут болеть, даже если он совершает пакости [4].

7) **Медийность – одно из ключевых качеств для маскота.** Маскот должен выходить за рамки лишь рекламного персонажа. Он часть не только лишь фирменного стиля, он олицетворение компании, её структурная единица. Присутствие маскота на публичных выступлениях как в цифровом, так и в физическом формате – необходимая часть его функционала. Если позиционирование и направленность компании позволяют, то маскот может даже стать постоянным «ведущим» каких-либо встреч, конференции и т.д.

8) **Ведение социальных сетей поможет привлечь аудиторию.** При создании аккаунтов маскота в социальных сетях нужно подробно прописать его историю. Аккаунт должен быть максимально персонализированным и выглядеть

реалистично. Для более успешной деятельности маскота в социальных сетях следует придумать ему уникальный хештег.

9) **Персонаж должен ассоциироваться только с собственным брендом.** Маскот не должен копировать образ кого-либо из других брендов, как в характере, так и во внешности. Он не должен делать перегибы в сторону борьбы с конкурентами, чтобы не запомниться только этим. Вся его история должна сводиться к личному бренду и быть неразрывно с ним связана.

Рассматривая маскотов коммерческих брендов, необходимо упомянуть одних из наиболее известных и эффективных персонажей.

Одним из самых популярных и узнаваемых маскотов мира является клоун по имени Рональд Макдональд, олицетворяющий компанию быстрого питания McDonald's. С 1963 года он практически не менялся. Несмотря на то, что в последние годы на персонажа обрушился шквал критики, его обвиняли в пропаганде продуктов, влияющих на детское ожирение, и связали его образ с кровожадным клоуном из экранизации произведения Стивена Кинга, Рональд всё равно продолжает появляться в рекламе, вести активные странички в соц. сетях, принимать участие в праздниках и является любимым героем нескольких поколений [5].

Не всегда нужно много лет, чтобы маскот стал любим и популярен у аудитории. Маскот анимационного стримингового сервиса «Crunchyroll» – девушка-дух по имени Химэ, появилась она лишь в 2012 году, но уже успела стать любимицей пользователей и поклонников анимационной культуры Азии. Она активный пользователь социальных сетей: отвечает на вопросы аудитории, пишет комментарии, делится постами и видео. Она играет роль ведущей на трансляциях и подкастах бренда. Персонаж является «голосом» и символом компании, полностью отражая её суть: образ персонажа основан на логотипе и на фирменном цвете сервиса. Химэ стала главной героиней многих комиксов, появлялась в мультфильмах, транслирующийся по сервису, и видео играх, а недавно успела посотрудничать с американским брендом одежды Benny Gold, выпустив уникальный мерчендайз [6].

В России одним из известнейших маскотов стал персонаж Сбера – СберКот. Появился он в ноябре 2017 года в социальной сети ВКонтакте в роли чат-бота и героя собственного сообщества, где он рассказывал о правилах финансовой грамотности, продуктах Сбербанка и актуальных новостях. Постепенно СберКот обзавелся друзьями и уже вместе с ними он вырос до важного элемента программы продвижения банка, за которым следят более 14 миллионов человек. На странице СберКота от его имени выкладываются комиксы, мини-истории и ролики, а также происходит рассылка анимированных стикеров и сообщений и предлагается мерч с изображением героя и его команды. Популярность Кота выросла до такого уровня, что с его изображением уже чеканят подарочные монеты и даже открывают памятники [7].

Таким образом, можно сказать, что маскоты – это простой и эффективный маркетинговый инструмент, к помощи которого всё чаще обращаются различные бренды. Но, при всей простоте, разработка персонажа, который будет

эффективной частью продвижения, требует тщательного анализа своей компании и аудитории. Хорошо продуманный персонаж-талисман легко сможет заявить о себе, влюбить в себя, пленить умы и сердца целевой аудитории бренда. Если бренду нужно взбодрить аудиторию в социальных сетях, то маскот может стать источником уникального контента, который будет привлекать внимание и выделяться на фоне череды обычных новостных сообщений.

Список используемых источников:

1. Автомонова В. С. Маскот как эффективный способ продвижения бренда // Научное сообщество студентов. Междисциплинарные исследования : материалы СХVI студенческой междунар. научно-практич. конф., Новосибирск, 06 мая 2021 г. Новосибирск : ООО "Сибирская академическая книга", 2021. С. 123-129.
2. Роль маскота в жизни компании. Нужно ли создавать персонажа-талисмана?: [Электронный ресурс] // VC.ru, 2021. URL: <https://vc.ru/u/645624-webmedia/289569-rol-maskota-v-zhizni-kompanii-nuzhno-li-sozdavat-personazha-talismana/> (Дата обращения 12.11.2022)
3. Маскоты: новый источник визуального контента: [Электронный ресурс] // Smmplanner.com., 2017. URL: <https://smmplanner.com/blog/maskoty-novyj-istochnik-vizualnogo-kontenta/> (Дата обращения 12.11.2022)
4. Личный бренд без личности: как продвигать бизнес с помощью маскотов: [Электронный ресурс]. // Icontextgroup. 2021. URL: <https://blog.icontextgroup.ru/articles/lichnyj-brend-bez-lichnosti-maskoty/>(Дата обращения 12.11.2022)
5. Ronald McDonald: [Электронный ресурс]. // Fandom.com., 2018. URL: https://mcdonalds.fandom.com/wiki/Ronald_McDonald (Дата обращения 12.11.2022)
6. Crunchiroll-Hime: [Электронный ресурс] // Fandom.com., 2021. URL: <https://hero.fandom.com/wiki/Crunchyroll-Hime> (Дата обращения: 12.11.2022).
7. СберКоту исполнилось четыре года: [Электронный ресурс] // Lenta.ru. 2021. URL: <https://lenta.ru/news/2021/11/29/sberkot/> (Дата обращения: 12.11.2022).

Astafieva-Rumyantseva I., Bogdanova M.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Features of mascots and their creation for commercial brands.

Mascots are becoming an increasingly popular means of promotion these days. Many brands come up with their own characters. But not everyone clearly understands what they are for and how to create a mascot correctly so that it becomes an effective promotional tool, and not just a beautiful static picture. This article discusses the role of mascots (characters-mascots) in the activities of brands, or rather, the following issues are mentioned. What is a mascot? What are mascots for? How to create a successful mascot? Several cases have also been reviewed.

Key words: mascot, promotion, brand, advertising activity, SMM.

УДК 659.4
ГРНТИ 19.21.07

СОРЕВНОВАНИЯ WORLDSKILLS КАК ИНСТРУМЕНТ ФОРМИРОВАНИЯ ИМИДЖА ВУЗА

И. Е. Астафьева-Румянцева, Д. А. Щетинина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Для того, чтобы оставаться востребованным вузу необходимо постоянно адаптироваться под условия внешней среды, и осуществлять мероприятия направленные на формирование позитивного общественного мнения о собственной деятельности, для сохранения актуальности и привлекательности. В данной статье рассматривается, как влияет участие вуза в соревнованиях Worldskills на его восприятие целевыми аудиториями.

высшее учебное заведение, конкурентоспособность, имидж, репутация, Worldskills, работодатель

Развитие рынка образовательных услуг в России сделало актуальной проблему конкурентоспособности высших учебных заведений. Для того, чтобы оставаться востребованным вузу необходимо постоянно адаптироваться и трансформироваться, реагируя на изменения внешней среды, и осуществлять мероприятия, направленные на формирование позитивного общественного мнения о собственной деятельности, для сохранения актуальности и привлекательности среди других представителей рынка образования. Для высших учебных заведений основными факторами оценки конкурентоспособности является имидж, кадровый потенциал, качество обучения, востребованность выпускников на рынке труда [1].

Проблема несоответствия специалистов, которых готовят в высших учебных заведениях, реальным требованиям рынка сейчас особенно актуальна. Выпускники российских вузов сталкиваются с низкой заинтересованностью со стороны работодателей, в частности, из-за недостатка практических навыков (отмечают 91% работодателей) [2]. В связи с этим задачей высшей школы становится развитие прикладных навыков будущего специалиста, что важно для студентов, нацеленных на карьеру в реальном секторе экономики.

В 2012 году Россия присоединилась к международному движению Worldskills, целью которого является повышение статуса и стандартов профессиональной подготовки и квалификации кадров, популяризация рабочих профессий путем проведения международных соревнований [3]. На чемпионатах Worldskills оцениваются прикладные компетенции участников. Изначально участниками чемпионата традиционно являлись обучающиеся образовательных учреждений среднего профессионального образования, но в 2016 году в числе ассоциированных партнеров движения Worldskills Russia появились первые пять вузов страны: Северный Арктический федеральный университет им. М. В. Ломоносова (САФУ), Дальневосточный федеральный университет (ДВФУ), Московский политехнический университет (Московский Политех), Санкт-

Петербургский государственный университет аэрокосмического приборостроения (СПб ГУАП) и Северо-Осетинский государственный университет им. К.Л. Хетагурова [4]. Участие в движении в качестве ассоциированных партнеров позволяет организациям проводить свои отборочные чемпионаты и участвовать в мероприятиях Worldskills Russia.

На сегодняшний день в движении Worldskills Russia участвует 3.500 образовательных учреждений СПО и 160 высших учебных заведений по всей России [5].

Образовательная организация может выступать не только в качестве партнера движения, но и являться специализированным центром компетенций (СЦК), то есть центром развития профессий и экспертных сообществ по определенной компетенции движения Ворлдскиллс Россия. Аккредитация организации как СЦК, гарантирует наличие современного оборудования и технологий, отвечающих требованиям стандартов движения Ворлдскиллс, а также наличие в штате экспертов для проведения обучения и оценки уровня профессионального мастерства в соответствии со стандартами движения Ворлдскиллс [6].

Сегодня в Санкт-Петербурге на уровне университетского образования действует два специализированных центра компетенций, аккредитованных по стандартам Ворлдскиллс Россия [7]:

- Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича (СПбГУТ), компетенция: программные решения для бизнеса;
- Санкт-Петербургский государственный университет аэрокосмического приборостроения (СПб ГУАП), компетенция: инженерия космических систем.

Участие и организация подобных мероприятий обеспечивает для высшего учебного заведения конкурентные преимущества и яркий информационный повод, оказывающий сильный имиджевый эффект.

Проведение соревнований по стандартам Ворлдскиллс повышает профессиональный уровень студентов и преподавателей [8]:

- подготовка технического описания, конкурсных заданий, критериев оценок требует от экспертов анализа большого объема материала, что определенным образом влияет на повышение их профессионального уровня;
- студенты приобретают профессиональные навыки выполнения заданий, развивают профессиональную самостоятельность, вызывают азарт и тягу к соревнованиям, формируют опыт творческо-конструкторской деятельности.

Профессиональные соревнования, рассматриваемые как внеучебная деятельность, имеют большое образовательное значение и позволяют выявить способных студентов и педагогических работников, создают условия для обмена опытом, способствует популяризации профессий и специальностей, стимулирует мотивацию саморазвития, личностный и профессиональный рост.

Получение прикладных компетенций, соответствующих международным профессиональным стандартам и их апробация в соревновательной среде, создает условия для того, чтобы окончившие вуз выпускники оказывались

востребованными на рынке труда, что, в свою очередь, повышает репутацию высшего учебного заведения среди работодателей.

Формированию положительного имиджа движения способствует широкое освещение событий Worldskills в СМИ, в том числе на центральном телевидении, продвижение новостей в социальных сетях [9]. Информация о движении Worldskills Russia регулярно размещается на официальном сайте и социальных сетях проекта: ВКонтакте, Одноклассники, YouTube, Telegram и Flickr. Медиа высших учебных заведений также активно распространяют информацию о проведении мероприятий Ворлдскиллс и результатах участия в них.

Упоминания высших учебных заведений в контексте Ворлдскиллс, особенно при условии достижения высоких результатов студентами даже на региональном уровне, позволяет формировать имидж вуза как прогрессивного, осуществляющего образовательные программы, соответствующие времени и запросам современного рынка. Это может оказывать существенное влияние на абитуриентов, если в качестве ключевых критериев выбора учебного заведения рассматривается качество образования и ценность диплома конкретного вуза.

В связи с обострением геополитической ситуации в России в начале 2022 года возможность дальнейшего участия страны в международном движении оказалось под вопросом. Worldskills International приостановило членство страны в движении, Worldskills Russia лишилась права участвовать в соревнованиях и мероприятиях за пределами страны, кроме того, международный чемпионат 2023 года, который должен был пройти в Санкт-Петербурге, решено перенести в другой европейский город [10]. Министерство просвещения России предлагает проект национального чемпионатного движения по профессиональному мастерству, которое должно заменить Worldskills. Но в проекте Минпросвещения говорится об участии только обучающихся по программам среднего профессионального образования.

Участие образовательной организации высшего образования в мероприятиях движения Worldskills позволяет затрагивать сразу несколько целевых групп:

- внутреннюю: студенты и преподаватели. Внедрение в образовательные программы лучших мировых практик и стандартов повышает качество обучения и положительно влияет на квалификацию преподавательских кадров;
- внешнюю: работодатели и широкая общественность. Рынок получает кадры, обладающие необходимыми компетенциями, а вуз, выпускающий таких специалистов, улучшает свои позиции на рынке образовательных услуг.

Востребованность высшего учебного заведения на рынке образовательных услуг определяется его возможностями и стремлением к реализации новых стратегий в области предоставления образовательных услуг, позиционирования вуза. Участие в соревнованиях Worldskills позволяет достигать репутационных и имиджевых целей вуза, направленных на продвижение и создание конкурентных преимуществ на рынке образования. Формирование эффективного имиджа высшего учебного заведения и его поддержание влияет не только на усиление

позиций на локальном рынке образовательных услуг, но и позволяет свидетельствовать об уровне развития образования в регионе и в стране.

Список используемых источников:

1. Ангелова О. Ю. Использование маркетинговых инструментов для оценки качества образовательных услуг // Разработка образовательных программ в условиях повышения конкурентоспособности экономического образования: материалы методич. конф. ННГУ им. Н.И. Лобачевского, Нижний Новгород, 6–8 фев. 2017 года. Нижний Новгород : ННГУ, 2017. С. 5–9.

2. Высшее образование: контроль не ослаблять, качество повышать: [Электронный ресурс] // ВЦИОМ новости. М., 2022. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/vysshee-obrazovanie-kontrol-ne-oslablyat-kachestvo-povyshat> (Дата обращения 01.11.2022)

3. Старков А. Н., Стащук П. В., Мовчан И. Н. Проблема формирования у студентов вуза профессиональной компетенции "Сетевое и системное администрирование" по стандарту WorldSkills: [Электронный ресурс] // Мир науки. Педагогика и психология. 2019. №1. URL: <https://cyberleninka.ru/article/n/problema-formirovaniya-u-studentov-vuza-professionalnoy-kompetentsii-setevoe-i-sistemnoe-administririrovanie-po-standartu-worldskills> (Дата обращения: 02.11.2022)

4. К WorldSkills Russia впервые присоединились вузы: [Электронный ресурс] // Агентство развития профессионального мастерства. М., 2014-2022. URL: <https://worldskills.ru/media-czentr/novosti/k-worldskills-russia-vpervie-prusoedunulus-vyzi.html> (Дата обращения 02.11.2022)

5. WorldSkills Russia: [Электронный ресурс] // Агентство развития профессионального мастерства. М., 2014-2022. URL: https://worldskills.ru/assets/docs//16522/ObshchayaPrezentaciya_2022.08.16.pdf (Дата обращения 03.11.2022)

6. Положение о деятельности специализированных центров компетенций № 01.02.2021-45: утв. автономной некоммерческой организацией «Агентство развития профессионального мастерства (Ворлдскиллс Россия)»: [Электронный ресурс] // Агентство развития профессионального мастерства. М., 2014-2022. URL: <https://worldskills.ru/assets/docs//179/Положение%20о%20деятельности%20ЦК.pdf> (Дата обращения 03.11.2022).

7. Список специализированных центров компетенций, аккредитованных по стандартам Ворлдскиллс Россия: [Электронный ресурс] // Агентство развития профессионального мастерства. М., 2014-2022. URL: <https://worldskills.ru/assets/docs//179/spisok-akkreditovannykh-SCK-31.10.2022.pdf> (Дата обращения 04.11.2022)

8. Гареев И. Ф. Участие университета в движении WorldSkills: [Электронный ресурс] // Российское предпринимательство. М., 2017. №23. URL: <https://cyberleninka.ru/article/n/uchastie-universiteta-v-dvizhenii-worldskills> (Дата обращения: 05.11.2022)

9. Самойленко И. С., Кочетков В. В. Особенности восприятия движения WorldSkills у различных аудиторий: [Электронный ресурс] // История и педагогика естествознания. М., 2019. URL: <https://cyberleninka.ru/article/n/osobennosti-vozpriyatiya-dvizheniya-worldskills-u-razlichnyh-auditoriy> (Дата обращения: 05.11.2022)

10. WorldSkills statement and position on the conflict in Ukraine: [Электронный ресурс] // WorldSkills. 2022. URL: <https://worldskills.org/media/news/worldskills-statement-and-position-conflict-ukraine/> (дата обращения 05.11.2022).

Astafjewa-Rumyantseva I., Shchetinina D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Worldskills competitions as a tool for the formation of the image of the University.

In order to remain in demand, the university needs to constantly adapt to the conditions of the external environment, and carry out activities aimed at forming a positive public opinion about its own activities, in order to maintain relevance and attractiveness. This article examines how the university's participation in Worldskills competitions affects its perception by target audiences.

Key words: *higher education institution, competitiveness, image, reputation, Worldskills, employer.*

УДК 31.748
ГРНТИ 05.01.03

СОЦИАЛЬНАЯ РЕКЛАМА КАК ИНСТРУМЕНТ БОРЬБЫ ПРОТИВ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ НИКОТИНОВЫХ УСТРОЙСТВ У МОЛОДЕЖИ В МЕДИАПРОСТРАНСТВЕ

Р. В. Быстров, Н. С. Листвина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире множество вещей переходят в интернет пространство, социальная реклама тоже адаптируется под новый формат. В статье приведены основные темы, использующиеся в социальной рекламе, а также статистика об использовании электронных устройств доставки никотина в организм человека. В связи с популярностью этих устройств, была запущена в сети интернет антитабачная социальная компания от национального проекта «Демография».

социальная реклама, электронные сигареты, нацпроект «Демография»

С приходом в информационное общество новых технологий произошло изменение в жизни людей. И как следствие, они дали человечеству прогресс в разных отраслях производства, экономики и т.д. Но у этого явления есть и обратная сторона. В России за пять лет курильщиков электронных сигарет стало почти втрое больше. И это только начало. Производители подобных устройств готовятся в ближайшую пятилетку довести оборот на своем рынке до четырех миллиардов долларов. А ведь значительная часть покупателей – подростки, для которых этот сладковатый, но при этом токсичный пар доступен. Минздрав России сейчас торопится принять меры, чтобы приравнять вейпы к сигаретам и ограничить их употребление [1].

Социальная реклама выступает важным инструментом формирования ценностей в массовом сознании, ориентации ценностных приоритетов, социально опасной модели поведения и т.п. Вместе с тем, социальная реклама является элементом сложного коммуникационного процесса, в который также входят социальный PR и социальный маркетинг. Этот комплекс видов коммуникации служит эффективным и действенным инструментом в решении общественно значимых проблем.

Сам термин «Социальная реклама» используется только в России. Во всем мире его заменяют понятие «общественная реклама» или же «некоммерческая реклама». В нормативно-правовом документе, а именно, Статья 3 Федерального закона от 13.03.2006г. № 38-ФЗ «О рекламе», дается следующая трактовка данному термину: социальная реклама - информация, распространенная любым способом, в любой форме и с использованием любых средств, адресованная неопределенному кругу лиц и направленная на достижение благотворительных и иных общественно полезных целей, а также обеспечение интересов государства. [2]

Тем не менее, социальная реклама всегда отображает самые злободневные проблемы в обществе. И чем острее стоит проблема, тем более чаще всего она

находит отражение в социальной рекламе. Сегодня в социальной рекламе выделяют следующие наиболее часто поднимаемые ею темы:

- борьба с пороками, предупреждение катастроф, нежелательных последствий. Например, это экологическая проблема, проблема наркомании, алкоголизма, низкого уровня жизни и другие;
- декларирование важных для населения ценностей. Например, здоровье, работа, личное счастье, доход и т.д.;
- призывы к созиданию, в основании которых лежит стремление к достижению индивидуальных и социальных идеалов;
- социальная психотерапия. Такая реклама возникает в периоды всеобщего чувства тревоги, страха за будущее своих близких, себя и т.д. [3]

Важно отметить, что целевая аудитория у социальной рекламы — это все общество или его значительная часть. В данную категорию полностью входит исследуемый нами объект — молодежь. В то время как у коммерческой рекламы она довольно узкая. Поэтому социальная реклама должна вызывать более сильные эмоции. А в связи с этим у нее должна быть более эффективная психологическая сторона.

Характеризуя молодежное сознание и систему ценностей современной молодежи, социологи выделяют:

- возросший уровень образованности и недостаточную согласованность социального и личностного смысла образования;
- признание молодежи социальной значимости участия в общественной жизни и стремление самоутвердиться в непроизводственной сфере, главным образом в сфере досуга;
- приоритет потребительских ориентаций над творческими, созидательными;
- вытеснение ценностей национальной культуры западными образцами поведения и символами;
- слабую индивидуализированность и избирательность культуры, связанную с диктатом групповых стереотипов. [4]

В 2019 ВЦИОМ провел исследование об использовании электронных никотиновых устройств и общественной реакции на возможные ограничения их использования. Исходя из полученных результатов удалось установить:

- Среди использующих электронные устройства россиян, 98% ранее курили традиционную табачную продукцию.
- Использующих электронные устройства россиян половина (49%) объяснили выбор в пользу электронных сигарет меньшим вредом для здоровья, а также отсутствием неприятного запаха на одежде (48%).
- Для 25% респондентов онлайн-опроса переход на электронные сигареты – это шаг на пути к отказу от обычных сигарет.
- Среди курящих россиян почти половина (48%) хотели бы знать о предлагаемых вариантах нового регулирования продажи и использования электронных сигарет и сами хотели бы принять участие в их общественном обсуждении.

- При введении неприемлемых для курящих россиян ограничений свободной продажи и использования электронных сигарет 54% респондентов не откажутся от них, несмотря на неудобства [5].

Опираясь на приведенные данные можно говорить о том, что половина курильщиков электронных сигарет пытаются избавиться от вредной привычки с помощью вейпа. Также респонденты готовы терпеть ограничения со стороны государства и не отказываться от привычки.

Вместе с тем, в зарубежные практики тоже есть исследования на подобную тему. Так организация ASH (Action on Smoking and Health) опубликовала результаты ежегодного опроса «YouGov» о вейпинге среди молодежи за 2022 год. В опросе 2022 года приняли участие 2613 человек. Основные выводы по результатам исследования:

- Значительное большинство (83,8%) никогда не пробовали электронные сигареты или не знают о них.

- Наблюдается рост числа 11-17-летних, которые когда-либо пользовались вейпом — с 11,2% в 2021 году до 15,8% в 2022 году.

- В настоящее время 7% подростков 11-17 лет являются курильщиками по сравнению с 3,3% в 2021 году [6].

Эти данные говорят о том, что производители электронных сигарет нацелены на мало-возрастную целевую аудиторию, чтоб как можно скорее привить им вредную привычку. Отсюда следуют, что упор в социальной рекламе должен идти на подростков чей возраст находится от 11 до 17 лет.

ASH подчеркивает значительное увеличение числа пользователей одноразовых вейпов по сравнению с 2021 годом. Также отмечается, что осведомленность об электронных сигаретах в целом высока — 90%. Но регулярное использование все еще крайне низкое. При этом 3,1% респондентов парят регулярно (более одного раза в неделю) и 3,9% — время от времени (менее одного раза в неделю).

Отсюда мы можем понимать какая социальная реклама будет эффективна. Ученые Комплексного онкологического центра UNC Lineberger сравнили эффективность социальной рекламы против электронных сигарет у подростков. Они выяснили, что эффективная реклама против вейпинга оказывает наибольшее влияние, когда она подчеркивает неблагоприятные последствия и вред электронных сигарет, использует негативные образы и избегает мемов, хэштегов и других стилей общения, ориентированных на подростков. Исследователи также обнаружили, что определенный контент для обмена сообщениями, используемый в настоящее время, особенно изображения, связанные с фруктовыми и сладкими «конфетными» ароматизаторами, повышает привлекательность вейпинга, и его следует избегать при разработке профилактических сообщений. В онлайн-исследовании полутора тысячам подростков было предложено оценить семь рекламных объявлений о профилактике вейпинга. В онлайн-исследовании полутора тысячам подростков было предложено оценить семь рекламных объявлений о профилактике вейпинга. Социальная реклама, которая четко сообщала о вреде для здоровья или сравнивала вейпинг с курением сигарет, была сравнительно более эффективной.

Нейтральный или менее релевантный контент, такой как ссылки на воздействие вейпа на окружающую среду или нацеленность табачной промышленности на молодежь, был менее эффективен [7].

На сегодняшний день в России была запущена антитабачная социальная реклама, призывающая бороться с новой зависимостью от электронных сигарет. Нацпроект «Демография» представил коммуникационную кампанию «Электронные сигареты и что они скрывают». Так, на улицах городов России можно увидеть баннеры с антитабачными призывами, которые подчеркивают негативное влияние электронных сигарет на организм. Приятный аромат жвачки, исходящий от «электронки», значительно усложняет жизнь, напоминают авторы кампании.

Отдельного внимания заслуживает социальная реклама в сети интернет в рамках коммуникационной кампании от нацпроекта «Демография», в нее входят:

- Радиореклама, где слушателям рассказывается о том, что электронное потребление табака так же вредно, как и обычные сигареты.

- Сообщество «Давай бросать» в социальной сети «ВКонтакте». В группе публикуются мотивирующие посты, истории от бросивших курить, различные последствия от табака и никотина, техники бросания курения и различные советы.

- Чат в социальной сети «ВКонтакте». Там люди мотивируют друг- друга, делятся своими советами, общаются на тему курения.

- Портал о правильном питании, ЗОЖ и избавлений от зависимостей. Это официальные ресурс Министерства здравоохранения РФ. На главной странице сайта размещены: статьи, калькулятор калорий, обследование по поводу ЗОЖ, рекомендации по интересующей проблеме, видеоролики, интерактивные сервисы и авторские колонки.

- Телефон «горячая линия» Минздрава России по вопросам здорового образа жизни.

- Канал на видео хостинге «YouTube» с размещением коротких социальных видео на тему здоровья и зависимости.

Здесь мы можем наблюдать важное явление. Социальная реклама от нацпроекта «Демография» делает упор на цифровой формат. Это связано с особенностью целевой аудитории. Ведь подростки часто проводят время в социальных сетях, где и нужно распространять социальную рекламу. Поэтому новая антитабачная кампания имеет большую популярность, чем социальные рекламы прошлого десятилетия. Весь этот комплекс направлен на борьбу с новой зависимостью у молодежи.

Список используемых источников:

1. Информационный портал «1tv.ru»: [Электронный ресурс]. URL: <https://1tv.ru.turbopages.org/1tv.ru/s/news/2019-09-15/372291> (Дата обращения 13.11.2022).

2. Федеральный закон от 13.03.2006 №38-ФЗ (ред. от 07.05.2022) «О рекламе» (принят ГД ФС РФ 22.02.2006).

3. Хорошкевич Н. Г. Социальная и политическая реклама: учебно-методич/ пособие. Екатеринбург : УрФУ, 2015. 146 с.

4. Маньков Ю. В., Оганян К. М. М. Социология молодёжи : учеб. пособие. СПб. : Петрополис, 2008. 316 с.

5. Информационный портал «ВЦИОМ»: [Электронный ресурс]. М., 2022. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/elektronnye-sigarety-vykhod-ili-tupik> (Дата обращения 13.11.2022) .

6. Информационный портал «BELVAPING»: [Электронный ресурс]. URL: <https://belvaping.com/news/rezultaty-issledovaniya-ash-youth-vaping-survey-2022/> .

7. Информационный портал «MedAboutme» [Электронный ресурс]. URL: https://medaboutme.ru/news/eksperty_vyuasnili_kakaya_reklama_protiv_veypinga_rabotaet_luchsh_e_vsego/ .

Bystrov R., Listvina N.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Social advertising as a tool to combat the use of electronic nicotine devices among young people in the media space.

In the modern world, a lot of things are moving into the Internet space, social advertising is also adapting to the new format. The article presents the main topics used in social advertising, as well as statistics on the use of electronic nicotine delivery devices in the human body. In connection with the popularization of these devices, an anti-smoking social company from the national project "Demography" was launched on the Internet.

Key words: social advertising, electronic cigarettes, national project «Demography».

УДК 608.
ГРНТИ 19.01

НЕОБХОДИМОСТЬ В ИССЛЕДОВАНИИ МАСКОТОВ И ИХ ПРИМЕНЕНИИ УЧЕБНЫМИ ОРГАНИЗАЦИЯМИ

В. М. Васильев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На сегодняшний день всё большее количество компаний прибегают к использованию персонажей талисманов в своей деятельности. Начиная с единичных случаев их использования в прошлом, со временем же данная тенденция получила свое дальнейшее активное развитие. Позже талисманы стали полноценным маркетинговым инструментом, часто используемым различными как крупными, так и не очень фирмами. Наблюдая за подобным стремительным развитием, возникает закономерный вопрос: «Как это происходит?».

маскоты, персонажи талисманы, образовательные организации, имидж

Чаще всего компании идут на такой шаг чтобы быть привлекательнее для своей целевой аудитории и увеличить лояльность своих клиентов. Однако создание и применение талисмана сложно назвать простым и заурядным процессом. Успешное внедрение и использование персонажей-талисманов обеспечивается множеством факторов, начиная ещё с этапа его создания. Несмотря на возникающие в процессе сложности, применение персонажей талисманов не ограничивается только коммерческими компаниями. Их выгоду открыли для себя и некоммерческие организации – ассоциации и государственные учреждения, а также фонды.

Работа является актуальной ввиду потребности компаний и организаций повысить эмоциональную привязанность и лояльность потребителей к своему бренду, а также улучшить непосредственную связь с её аудиторией. Маскоты, в свою очередь являются эффективным маркетинговым инструментом, позволяющий удовлетворить эту потребность, представляя организацию в виде располагающего к себе персонажа. Таким образом, она перестаёт быть безликой и становится более привлекательной для конечного потребителя.

Объектом работы является собственный маскот Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича.

Предметом выпускной квалификационной работы является поэтапное создание маскота, начиная с идеи и заканчивая графической реализацией персонажа.

Целью работы является исследование маскотов и их использование образовательными организациями.

Слово «маскот» происходит от английского слова «mascot», которое напрямую переводится на русский язык как «талисман». В свою очередь, английский термин уходит корнями в Францию XIX века. Во Франции термин «mascoto» переводился как «колдовство» или «магия». Именно поэтому в нашем исследовании слова «маскот» и «персонаж талисман» тождественны, то есть используются как синонимы. Изучим различные трактовки данного термина в научной литературе этого термина. Маскотом называют персонажа,

олицетворяющего собой некий коллектив: школу, спортивную команду, сообщество, воинское подразделение, мероприятие или бренд. В зависимости от организации, использующей персонажа талисмана, его роли и задачи могут меняться.

К задачам персонажей-талисманов относят: апелляцию к эмоциям, вовлечение потребителей, упрощение образа бренда в глазах потребителя.

Через маскотов, можно вызвать положительные эмоции у аудитории, в особенности, если компания работает с аудиторией детского возраста. Выполнение этой задачи напрямую зависит от разработки дизайна внешнего вида маскота и организации процесса его представления общественности. Очевидно, что если персонаж получается безликим, а его представление аудитории произведено неудовлетворительно, то достижение данной задачи ставится под угрозу.

Вовлечение потребителей является второй задачей маскота. Наиболее эффективно эта задача выполняется, если маскот присутствует на местах продаж и зазывает потенциальных потребителей товара. Маскот может присутствовать в магазине в виде изображения на штендере или костюма. Если мы говорим о некоммерческих организациях, то задача привлечения внимания может быть выполнена если маскот используется совместно с логотипом компании, а также участвует в процессе мерчендайзинга (персонаж расположен на значках, кружках, воздушных шариках). Успешное выполнение этой задачи зависит от двух факторов. Первый – яркий дизайн персонажа. Второй – удачное применение готового дизайна персонажа. Речь идёт о сочетаемости маскота с выбранным предметом мерчендайзинга и имиджем организации. В противном случае талисман может привлечь внимание нецелевой аудитории.

Задача упрощения бренда в глазах потенциального и конечного потребителя тоже лежит «на плечах» маскота. Подобную формулировку можно также слышать услышать под термином «симплификация». Это слово происходит от английского «Simplification», что напрямую переводится как «упрощение». Данная задача возникает, если организация является большой корпорацией или организацией, работающей в условиях высокой конкуренции.

Главная роль маскота – налаживание постоянной связи между организацией и её аудиторией. Персонаж талисман выступает коммуникативным «мостом», меняющим отношение потребителя к компании, как правило, на более лояльное, работая на имидж компании.

Имидж – это целенаправленно сформированный образ, который оказывает эмоционально-психологическое влияние на человека или на группу людей, другими словами, это искусство управлять впечатлением [1].

Опыт создания и использования университетских маскотов по праву можно назвать очень необычным. Западный опыт и его развитие в виде использования маскотов для российских университетов, представляет для нас наибольший интерес. Мы ставим иностранных и отечественных талисманов в один ряд благодаря удобству их сравнения, легкости и простоте заимствования между ними удачных идей и наиболее перспективных, актуальных дизайнерских решений.

Почему же опыт использования персонажей талисманов можно назвать необычным? Разобраться в этом вопросе стоит более подробно и

основательно. Дело в том, что учебные заведения практически полностью заимствуют опыт у спортивных маскотов. Таким образом, основное направление в области разработки, создания и дальнейшей интеграции персонажа рассматривается с точки зрения тех же спортивных, имиджевых мотивов и делается с расчётом на реализацию в виде ростовой куклы. Именно их подавляющее число можно очень часто увидеть, если ввести в строке поиска в сети Интернет «Университетские маскоты». В этом случае можно с уверенностью говорить о том, что «учебные маскоты» отстают от других своих «собратьев».

Главной функцией американских персонажей талисманов является агитация абитуриентов и привлечение внимания к университету или колледжу. Маскоты университетов, присутствуют на днях открытых дверей, но в отличие от российских талисманов, они играют гораздо большую роль – непосредственное общение, выступление перед абитуриентами и агитация. Практически за каждым американским колледжем и университетом закреплен свой персонаж талисман.

Примером такого персонажа талисмана может выступить Медведь Оски – маскот Калифорнийского университета в Беркли. Прообразом персонажа является Калифорнийский золотой медведь – спортивный талисман. Персонаж был создан Уильямом «Рокки» Роквеллом, первым учеником университета, впоследствии сыгравшим роль самого персонажа в виде ростовой куклы. После презентации и успешного дебюта, руководство Калифорнийского университета заинтересовалось персонажем талисманом и взяло на себя шефство над маскотом. Помимо ростовой куклы персонаж имеет собственную песню, повышающую настроение и «боевой дух» абитуриентов [2].

Одним из интересных представителей российского ответвления «классической школы» талисманов образовательных учреждений является маскот Пермского университета – учёный кот. Данный персонаж был выбран в ходе конкурса, организованного профсоюзной организацией ПГНИУ. Маскот был выбран благодаря своему реальному прообразу – коту Мариску, который жил в одном из учебных корпусов университета. Популяризация кота не остановилась на создании персонажа талисмана и с четверным маскотом ВУЗа регулярно появляются записи в социальных сетях. В Пермском университете талисман выполняет свою прямую функцию. В учебном заведении существует примета – встретить кота Марсика к удаче на экзамене. Таким образом необходимость в маскоте многократно вырастает в экзаменационный период [3].

Также интересным и актуальным примером для нашего исследования может выступить талисман Высшей Школы Экономики (НИУ ВШЭ). Их маскот – Вышкинская ворона (имя персонажа отсылает на название учебного заведения). Персонаж был создан в 1997-м году и присутствует на сувенирной продукции Высшей Школы Экономики. Легенда, расположенная на официальном сайте НИУ ВШЭ гласит, что Вышкинская ворона была создана как компаньон для персонажа талисмана Лондонской школы экономики – бобра. Поскольку маскоты университетов хорошо смотрелись вместе, руководство Высшей Школы Экономики рассмотрело и успешно реализовало официальную версию персонажа талисмана [4].

Таким образом, ознакомившись с теоритическими основами маскотов и проведя анализ использования персонажей-талисманов, можно сделать вывод о их важности и ценности для образовательных организаций, таких как Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича.

Список используемых источников:

1. Овчинникова А. М., Шульга Н. В. Основы имиджологии определение имиджа: учебное пособие М. : «ЛитРес: Самиздат», 2019. с.10
2. Oski at Larry Leung's Homepage: [Электронный ресурс]. URL: <https://web.archive.org/web/20060424065011/http://www.oski.com/> (Дата обращения 12.11.2022)
3. МЭЛ: 6 самых необычных маскотов российских вузов – кот Марсик: [Электронный ресурс]. URL: <https://mel.fm/blog/yuliya-annenkova/34895-6-samykh-neobychnykh-maskotov-grossyskikh-vuzov> (Дата обращения 12.11.2022)
4. Национальный исследовательский университет «Высшая школа экономики»: Вышкинская ворона: [Электронный ресурс] // НИУ ВШЭ. М., 1993-2022. URL: <https://www.hse.ru/org/persons/188576283>.

Vasilyev B.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

The need for research on mascots and their application by educational organizations. Today more and more companies have resorted to using mascot characters in their work. Starting from sporadic cases of their use in the past, over time, this tendency has been actively developing. Later, talismans became a full-fledged marketing instrument often used by various firms, both large and not so large. Observing this kind of rapid development, a logical question arises: "How does this happen?"

Key words: *mascots, mascot characters, educational organizations, image.*

УДК 694.1
ГРНТИ 19.21.91

СОТРУДНИЧЕСТВО МЕЖДУ КОМПАНИЯМИ ДЕРЕВЯННОГО ДОМОСТРОЕНИЯ И ПРОФЕССИОНАЛЬНЫМИ СООБЩЕСТВАМИ НА ПРИМЕРЕ АДД

В. Н. Николаев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье на примере АДД (Ассоциации деревянного домостроения) проанализированы методы, с помощью которых профессиональное сообщество продвигает компании и отрасль деревянного домостроения в целом. Также исследовано влияние Ассоциации деревянного домостроения на развитие отрасли в Российской Федерации.

деревянное домостроение, профессиональное сообщество, продвижение, сотрудничество

В условиях нынешней экономической ситуации российские профессиональные сообщества играют особенную роль в развитии отрасли. Они значимы тем, что в них организации и группы делятся полезной информацией для людей, объединенных одним делом. Предпринимательство может быть трудным и монотонным, а также неблагодарным занятием, особенно на начальном этапе. Поздние ночи и выходные в офисе - обычное дело для этой работы. Участие в данном объединении, где проводятся живые мероприятия, может принести много пользы и веселья, облегчив монотонные будни для компаний. Сообщество поможет связаться с единомышленниками-предпринимателями, которые имеют одинаковые интересы. Это может стать началом дружеских отношений на всю жизнь, и поможет создать прочную сеть людей, к которым можно обратиться в трудные и неприятные времена [1].

Одним из таких профессиональных сообществ в отрасли деревянного домостроения является Ассоциация деревянного домостроения (АДД), созданная в 2003 году для развития деревянного домостроения в России. Ассоциация включает в себя более 75 компаний из разных стран, куда входят архитекторы, проектировщики, компании-производители, строители, поставщики материалов, вузы и колледжи. АДД активно включена в деятельность государственных структур, работает с органами местного управления, сотрудничает с комитетами по физкультуре и спорту, сельскому хозяйству, МЧС и др. Члены ассоциации работают в составе технического комитета № 465 «Строительство», ТК № 144 «Строительные материалы», Комитета по деревянному домостроению ТПП Российской Федерации. Интересы АДД представлены в Экспертном совете при Комитете Государственной Думы по строительству, промышленности строительных материалов и проблемам долевого строительства [2].

Главной целью ассоциации является объединение усилий компаний участников по развитию рынка деревянного домостроения и обеспечение его устойчивого роста. К задачам профессионального сообщества относятся:

1. увеличение рынка деревянного домостроения;
2. проработки государственных мер поддержки;
3. актуализации нормативной базы;
4. формирование доступного кредитования;
5. популяризация через СМИ;
6. популяризация среди архитекторов;
7. объединение с архитектурным профессиональным сообществом для увеличения проектирования с применением деревянных конструкций;
8. развитие технологичности рынка;
9. популяризация новых технологий через обучение, пилотные проекты, СМИ;
10. снижение дискредитации технологий;
11. информационная прозрачность рынка деревянного домостроения;
12. разработка, внедрение и продвижение собственных независимых систем аккредитации и рейтинговой оценки;
13. формирование доступной информационной платформы;
14. формирование правил добросовестной конкуренции и ведения бизнеса;
15. экспертиза деятельности участников ассоциации с публикацией результатов;
16. маркетинговые исследования [2].

Продвижение товаров и услуг происходит на коммерческой и безвозмездной основе, как между участниками АДД, так и от внешних контрагентов. Это делается для модернизации производств, выстраивания прямой внутренней интеграции между участниками ассоциации и выстраиванию деловых отношений с поставщиками товаров и услуг, не являющихся участниками Ассоциации, для снижения себестоимости и повышения прибыльности. Кроме этого, компаниям-участникам АДД активно содействуют в продвижении товаров, услуг и технологий через Интернет, профессиональные форумы, прессу, выставки, социальные сервисы и мероприятия для профессиональной аудитории, куда также входят студенты строительных институтов, архитекторов, технологов и инженеров.

Помимо продвижения компаний деревянного домостроения, ассоциация занимается организацией своих проектов, через которые продвигает отрасль. Одним из таких мероприятий является международный конгресс по деревянному строительству, которое объединяет застройщиков, архитекторов, производителей материалов, маркетологов, представителей министерств и ведомств. Благодаря формату встреч построен прямой диалог между властью и бизнесом, что даёт возможность из первоисточника услышать потребности министерств и ведомств, а также в режиме реального времени предложить собственные решения для реализации поставленных задач [3].

Также АДД является организатором отраслевой премии в области деревянного строительства Prowood Awards. В конкурсе могут принять

участие введенные в эксплуатацию жилые, общественные и административные здания, основным материалом для строительства которых является дерево. Уникальность Премии — разносторонняя оценка представленных объектов с применением деревянных конструкций, построенных в 2020-2022 гг. [4]

Кроме мероприятий АДД предлагает широкий спектр товаров и услуг, а также оказывает рекламные, маркетинговые и консультационные услуги. Профессиональное сообщество также оказывает услуги по подбору технологий, подрядчиков и архитекторов для индивидуальных и корпоративных заказчиков с учетом технико-экономических, эстетических и региональных запросов.

Компании-участники АДД могут получить специальные условия на страхование строительства загородного дома до завершения строительства, а так же специальные условия на страхование уже построенного загородного дома. Специальные страховые тарифы распространяются на участников ассоциации, производящих дома по технологиям индустриального деревянного домостроения. За счет высокой заводской готовности минимизируются риски, связанные с качеством и невыполнением обязательств подрядчиком, поэтому с рядом ведущих страховых компаний есть договоренности предоставления специальных тарифов для участников АДД.

Клиенты, которые заказывают дом у компании-участника ассоциации, смогут получить трехсторонние договоры, включающие контроль качества и технический надзор. Это позволяет клиентам получить дополнительный контроль строительства дома от специалистов АДД [2].

АДД имеет Экспертно-консультационный центр (ЭКЦ), который с 2004 года занимается популяризацией строительства из дерева. Центр включает в себя высокопрофессиональных специалистов, а также объединяет и продвигает компании деревянного домостроения с подтвержденной репутацией и опытом.

Помимо услуг АДД ведёт на своём сайте новостной блог, в котором рассказывает о деятельности объединения, а также рассказывает о происходящих мероприятиях и событиях в этой сфере. Сам блог обновляется каждые несколько дней. Чаще всего, в блоге рассказываются новости об участии АДД в мероприятиях и действиях российской власти по развитию деревянного домостроения [2].

Из всего вышесказанного можно сделать вывод, что АДД оказывает огромную поддержку компаниям по строительству деревянных домов, выступая посредником между компаниями и властью, а также продвигая их услуги и товары через средства массовой информации и организацию мероприятий и проектов в сфере деревянного домостроения.

Список используемых источников:

1. Профессиональное сообщество: понятие, структура, причины создания, цели и задачи: [Электронный ресурс] // FB. М., 2022. URL: <https://fb.ru/article/455369/professionalnoe-soobshchestvo-ponyatie-struktura-prichinyi-sozdaniya-tseli-i-zadachi> (Дата обращения 05.11.2022).
2. Ассоциация деревянного домостроения: [Электронный ресурс]. М., 2003-2022. URL: <https://npadd.ru/> (Дата обращения 05.11.2022).
3. Международный конгресс по деревянному строительству: [Электронный ресурс]. М., 2017-2021. URL: <http://woodcongress.ru/> (Дата обращения 08.11.2022).

4. Премия ProWood Awards: [Электронный ресурс]. М., 2019-2022. URL: <https://pro-wood.pro/> (Дата обращения 08.11.2022).

Nikolaev V.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Cooperation between wood construction companies and professional communities on the example of ADD.

Using the example of ADD (Association of Wooden Housing), the article analyzes the methods by which the professional community promotes companies and the wooden housing industry as a whole. The influence of the Association of Wooden Housing Construction on the development of the industry in the Russian Federation was also studied.

Key words: wooden housing construction, professional community, promotion, cooperation.

УДК 338.012
ГРНТИ 19.01.07

ПЕРЕГОВОРЫ КАК СПОСОБ РАЗВИТИЯ ДЕРЕВЯННОГО ДОМОСТРОЕНИЯ В РОССИИ

В. Н. Николаев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обсуждения в современном мире являются довольно важной частью при строительстве деревянных домов. Статья посвящена актуальности переговоров в развитии деревянного домостроения, а также в ней показаны важные моменты, где обсуждения сыграли важную роль в развитии деревянного домостроения в Российской Федерации. Определяется понятие, сущность и содержание переговоров с современными примерами их использования.

деревянное домостроение, переговоры, строительство дома, импортозамещение, коммуникация

В настоящее время сфера деревянного домостроения, несмотря на свой недавний подъём в результате пандемии, находится в довольно сложной ситуации, порождённой рядом факторов. Из-за ограничений, вызванных политической ситуацией, под запрет импорта попали такие важные для производителей из РФ категории товаров, как фанера, древесные плиты, топливные гранулы. Также под санкциями находятся немелованная крафт-бумага и картон и древесная масса, полученная сочетанием механического и химического способов [1]. Последний пакет санкций, который вступил в силу осенью, запретил импорт российских целлюлозы и бумажных изделий.

В сложившихся условиях компаниям деревянного домостроения приходится трансформировать свои коммуникации, ориентируясь на внутренний рынок. Сложности в их изменении связаны с тем, что большинство поставок было направлено на внешний рынок, а внутренний оказался не подготовлен к последствиям западных санкций. Очень многие эксперты, в частности вице-спикер Совфеда РФ Юрий Воробьев, отмечают, что развитие и поддержка внутреннего рынка деревянного домостроения является очень важной задачей и необходимо создавать условия для того, чтобы люди получали выгоду от строительства деревянного дома. В целях привлечения новых покупателей, необходимо устанавливать каналы связи как с внешними (власть, инвесторы и т.п.), так и с внутренними аудиториями (клиенты, сотрудники). При продаже дома необходимо также учитывать и предпочтения клиента, учёт которых способствует успешной продаже деревянного дома.

Одним из самых важных инструментов для поддержки сообщения являются переговоры как «процесс принятия совместного решения двумя или более сторонами о дальнейшем их поведении» [2]. Они являются важнейшей частью любого делового партнерства. От их качества проведения во многом зависит дальнейшая работа с клиентом или поставщиком, и именно на этом этапе

определяются главные условия сотрудничества. Помимо выбора дома и участка, а также конфигурации и материалов, такие обсуждения позволяют решать конфликты по сроку сдачи дома из-за логистики или замены определенных элементов, особенно во время импортозамещения.

Институт экономической политики им. Е. Т. Гайдара отметил, что лесная отрасль сегодня оказалась в наиболее невыгодном положении и испытывает серьёзные трудности с поставками из-за рубежа, которые так и не смогла успешно «импортозаместить». По данным института, масштабы недостаточной обеспеченности предприятий лесопромышленного комплекса (ЛПК) импортными комплектующими и сырьём выросли до 60%, в то время как в июне этот показатель не превышал 38% [3]. Это особенно показательно, поскольку на выездном заседании совета по вопросам развития лесного комплекса РФ при Совете Федерации, которое состоялось в июле этого года в Красноярске, одной из стратегических задач лесной отрасли эксперты назвали именно импортозамещение и вместе с тем расширение внутреннего рынка.

Чаще всего в деревянном домостроении задействованы следующие типы переговорного процесса.

Собрания акционеров позволяют им получить актуальную информацию о его деятельности и реализовать свои права на участие в его управлении, голосуя по тем или иным вопросам повестки дня. Например, общие годовые и внеочередные собрания компаний.

Деловые совещания – это возможность руководства донести основные цели и задачи сразу до всех структурных подразделений, получить обратную связь и на основании полученных данных скорректировать план действий для компании. Среди видов совещаний особенно часто проводятся:

- собрания сотрудников компаний (обычно – руководители структурных подразделений) для решения стратегических вопросов по развитию бизнеса;
- переговоры между компаниями ЛПК, отраслевыми объединениями (АДД, областные союзы лесопромышленников и лесозэкспортёров и т.п.), научно-исследовательскими институтами (ЦНИИСК, ВНИИПО) и органами власти (Минпромторг, Минстрой, Минсельхоз, Минфин и т.п.);
- дискуссии - открытое обсуждение важных вопросов внутри компаний, обсуждения между представителями власти, производителей изделий из древесины глубокой переработки, застройщиков, кредитных организаций и т.д.

Конференции очень часто используются для обсуждения ключевых проблем и результатов в сфере деревянного домостроения. В них часто вовлекаются руководители и маркетологи деревообрабатывающих компаний, представители власти, архитекторы, производители материалов и т.д. В сфере деревянного домостроения проводятся такие конференции, как Woodindex, 100+ TechnoBuild, ПМЛФ (Петербургский лесопромышленный форум) и т.п.

Съезды используются для обсуждения важных вопросов ЛПК на национальном или международном уровне. На съезде может избираться руководство организации, определяются основные направления деятельности, заслушивается отчёт руководства о проделанной работе, могут быть внесены

изменения в уставные документы. Формат съездов позволяет напрямую налаживать прямой контакт между бизнесом и властью, а также позволяет предложить собственные решения для реализации поставленных задач. В сфере деревянного домостроения проводятся такие съезды как Международный Съезд по деревянному строительству, съезды-конгрессы Ассоциации деревянного домостроения и т.п.

Профессиональные **выставки** предполагают проведение неформальных переговоров в непринужденной обстановке. Любая форма общения на выставке позволяет решить сразу несколько задач: получить или передать необходимую информацию; найти новых деловых партнеров; рассказать о достижениях компании. В отрасли деревянного домостроения проводятся такие международные мероприятия как выставки «ЛесДревМаш», «Woodex», «Красивые дома. Строительство. Архитектура. Интерьер» и «Уралстройиндустрия», а также городские выставки «Izbushka», «Загородный дом. Весна», RosBuild и т.д. Все эти мероприятия имеют отдельные экспозиции и салоны, посвященные строительству из дерева.

Переговоры являются одной из наиболее эффективных и доступных способов разрешения противоречий, поскольку они не предполагают участия третьих лиц и не нуждаются в санкционировании государством, законодательном регулировании, не требуют каких-либо серьезных затрат.

Важно отметить и ключевые преимущества переговорного процесса перед другими организационных коммуникаций:

- в процессе переговоров происходит непосредственное взаимодействие сторон;
- участники конфликта имеют возможность максимально контролировать различные аспекты своего взаимодействия, в том числе самостоятельно устанавливать временные рамки и пределы обсуждения, влиять на процесс переговоров и на их результат, определять рамки соглашения;
- переговоры позволяют участникам конфликта выработать такое соглашение, которое удовлетворило бы каждую из сторон и позволило избежать длительного судебного разбирательства, которое может закончиться проигрышем одной из сторон;
- принятое решение, в случае достижения договоренностей, нередко имеет неофициальный характер, являясь частным делом договаривающихся сторон.

Принципиальная особенность переговоров состоит и в том, что их участники взаимозависимы. Поэтому, прилагая определенные усилия, стороны стремятся разрешить возникшие между ними противоречия. Эти усилия направлены на совместный поиск решения проблемы.

Однако переговоры при всех своих преимуществах также имеют некоторые сложности, которые связаны с тем, что часто из-за крайне противоположных позиций сторон переговоров по спорному вопросу «существует вероятность недостижения желаемого результата». Ко всему этому переговоры также требуют определенной профессиональной и психологической подготовки.

Таким образом, можно сделать вывод, что переговоры являются частью коммуникационного процесса и они постоянно используются для продвижения компаний и продажи их товаров и услуг. При успешном проведении данный вид обсуждений позволяет достигнуть целей, решать определенные проблемы и реализовывать необходимые сделки или мероприятия в деревянном домостроении. Сами переговоры очень часто используются на мероприятиях, так как они дают решать большое количество задач, устанавливая контакт между компаниями, властью и клиентами.

Список используемых источников:

1. Санкции и деревянное домостроение: как «выживает» отрасль в 2022 году [Электронный ресурс]. URL: <https://forestcomplex.ru/wh-building/sankcii-i-derevyannoe-domostroenie-kak-vyzhivaet-otrasl-v-2022-godu/> (Дата обращения: 24.10.2022);
2. Вельмакина Т. П. Переговоры как альтернативный способ урегулирования конфликтов // Евразийский научный журнал. 2016. №5. [Электронный ресурс]. // cyberleninka.ru., 2016. URL: <https://cyberleninka.ru/article/n/peregovory-kak-alternativnyy-sposob-uregulirovaniyakonfliktov> (Дата обращения: 26.10.2022);
3. Как стимулировать развитие внутреннего рынка ЛПК? [Электронный ресурс]. URL: <https://forestcomplex.ru/forestry/kak-stimulirovat-razvitie-vnutrennego-rynka-lpk/> (Дата обращения: 29.10.2022).

Nikolaev.V

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Negotiations as a way to develop wooden house construction in Russia.

Negotiations in the modern world are quite an important part in the building of wooden houses. The article is dedicated to the relevance of negotiations in the development of wooden house construction, and it also shows important points where negotiations played an important role in the development of wooden house construction in the Russian Federation. The concept, essence and content of negotiations with modern examples of their use are defined.

Key words: *wooden house construction, negotiations, house construction, import substitution, communication.*

УДК 659.443/.446
ГРНТИ 19.01.11

ФАКТОРЫ УЗНАВАЕМОСТИ БРЕНДА

А. А. Русова, А. В. Кульназарова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье затрагивается тема важности узнаваемости бренда и рассматриваются факторы, влияющие на нее. Выделяется 6 факторов влияния на узнаваемость бренда: история бренда, реклама и связи с общественностью, конкурентная среда, географическое положение, частота использования и сарафанное радио. Каждый фактор объясняется и подтверждается примерами.

бренд, узнаваемость бренда, имидж компании, коммуникации, целевая аудитория

Узнаваемость бренда – это, во-первых, одна из главных целей маркетинга, во-вторых, это осведомленность целевой аудитории о компании, способность вспомнить ее и распознать при разных условиях.

От степени узнаваемости бренда, а значит и способности целевой аудитории идентифицировать его и вспомнить напрямую зависит уровень продаж и его конкурентное преимущество. Зачастую, потребители отдают предпочтение каким-либо товарам только потому, что узнали бренд, слышали о нем ранее.

Безусловно, одной узнаваемости недостаточно, клиенты должны чувствовать доверие к бренду, быть уверенным в качестве и знать все положительные и отрицательные стороны, чтобы иметь полную картину и не быть шокированным неожиданными новостями и «молчанием» на эту тему компании.

Узнаваемость зависит от выбранной маркетинговой стратегии и степени продвижения, но не всегда они могут оставаться под контролем и не всегда она зависит только от этого. Также стоит понимать, что узнаваемость среди целевой аудитории – это хорошо и конкурентоспособно, а «всеобщая» узнаваемость – это, зачастую, становится внеконкурентным преимуществом.

Возможные причины становления узнаваемости брендов и что за ними стоит:

Факторы, влияющие на всеобщую узнаваемость

1. История бренда.

Чем дольше у бренда история, тем более надежным он кажется в глазах потребителей. Это применимо, как с хрестоматийными примерами, например, история «Ford», так и с относительно более новыми, например, «Аэрофлот» (бывший «Добролет») – первая и единственная авиакомпания на территории СНГ, занимающаяся гражданскими авиаперевозками. ПАО «Аэрофлот» считается его преемником). На истории таких крупных брендов росли поколениями и их «всеобщая узнаваемость» объясняется масштабом деятельности компании, отношении к потребителям.

2. Реклама и СО

Многие компании держат в своем штате сотрудников, отвечающих за продвижение брендов – маркетологов, специалистов по рекламе, связям с общественностью и т.д. Именно они формируют представление бренда аудитории, стиль его общения с ней и в целом стратегию его взаимодействия. Все ошибки в коммуникации с аудиторией напрямую влияют на имидж бренда в ее глазах. Одно неизменно – позитивные или негативные кейсы повышают уровень его узнаваемости.

Например, рекламные ролики авиакомпании S7 Airlines сравнивают с искусством, они получают награды на фестивале рекламы «Каннские львы» и не только [3]. Потому что компания продает не просто авиабилеты – это «больше, чем просто перелет из одного города в другой. Это настоящее чудо, и с него начинаются поиски еще большего чуда, которое мы называем счастьем» [2]. Компания продает эмоции и рекламное обращение построено на передаче их ощущений, и это служит одной из причин запоминаемости и узнаваемости.

В целом, существует множество способов взаимодействия с аудиторией как через рекламные сообщения, так и через мероприятия из категории связей с общественностью. Чем они будут необычнее, тем больше вероятности запомниться. Для таких креативов мало учитывать существующие кейсы, важно придумывать что-то совершенно новое, либо модифицировать и дополнять имеющиеся кейсы. К примерам из СО коммуникаций можно отнести продвижение через СМИ, причем как оплаченные публикации, так и размещенные по желанию редакции (а это желание не всегда совпадает с правообладателем бренда, так как такие публикации могут быть негативно окрашены, что напрямую влияет на имидж бренда). Частой причиной публикации о компании в СМИ может стать событие. Оно может быть преднамеренным – специально созданным (фестивали, акции и т.д.) и непреднамеренным – случайное стечение обстоятельств, незапланированное событие, поступок какого-либо представителя бренда (от рядового сотрудника до совета директоров), действие с товаром или услугой потребителем, получившее популярность, например, в сети Интернет. Если же публикация оплаченная, то ее популярность среди читателей будет зависеть от сенсационности, инфоповода, однако стоит отметить, что, в наши дни, даже не разбирающийся в сфере рекламы и СО может отличить оплаченную публикацию от других и с высокой долей вероятности не будет тратить на нее свое время в современном огромном потоке информации.

Так, авиакомпания S7 Airlines на фоне масштабных лесных пожаров в сибирской части России запустила акцию «Мы-Сибирь», где для привлечения внимания российских СМИ к проблеме переименовалась в старое название «Сибирь» и привлекла волонтеров, сотрудников, а позже и другие бренды откликнулись и стали помогать в высадке деревьев на выжженных местах. В социальных сетях выкладывалось множество контента под хештегом #WeAreSiberia и #МыСибирь. Тогда российские федеральные СМИ «ожили» и стали рассказывать о смене названия авиакомпании и упоминать о лесных пожарах, привлекая еще больше внимания общественности. Это пример

непреднамеренных событий (природное бедствие) и преднамеренных мероприятий компании по влиянию на них. Как следствие – привлечение внимания СМИ, общественности, других брендов, органов власти. Эта кампания успешно повлияла не только на всеобщую узнаваемость бренда, но и уважение его.

Другой пример непреднамеренного события, повлекшего за собой инфоповод – успешное аварийное приземление самолета компании «Уральские авиалинии» в кукурузном поле в августе 2019 года. Эта новость была позитивной, так как никто из пассажиров и экипажа не погиб. Практически все СМИ тогда написали об этом событии и бренд «Уральских Авиалиний» и пилоты воздушного судна получили известность. Повысилась как узнаваемость бренда, так и его имидж.

3. Конкурентная среда

Рынок, на котором находится бренд, наличие конкурентов на рынке и их деятельность также играют большую роль в узнаваемости. В Российской Федерации монополии запрещены и фактически эти требования соблюдены во всех отраслях. Правда, например, железнодорожный комплекс в России представлен «РЖД», который разделил бизнес и, по сути, разделил сферы влияния. В эту среду высокий барьер входа для новых конкурентов и потому в такой сложной, а ранее государственной отрасли, конкурентная среда почти отсутствует, а пользование услугами происходит повсеместно, что и дает высокую узнаваемость бренда – отсутствие альтернативы. При упоминании отрасли – это будет первым, что вспомнит потребитель.

4. Географическое положение

Знание определенных брендов зависит от их географического расположения и влияния. Одна из причин тому – Рекламная и СО-деятельность на определенных территориях, то есть, на территориях, где находится потенциальная целевая аудитория.

Например, авиакомпания «Хабаровские авиалинии» выполняет рейсы внутри региона, о ее существовании, в лучшем случае, знают жители Дальневосточного федерального округа. Обратная ситуация с брендом «Газпром». Его первоначальное предназначение – доставка газа в квартиры домов. Компания на сегодня выросла, создала множество дочерних компаний и департаментов и все они будут узнаваемы, так как в своем названии содержат слово «Газпром...». Также эта компания для некоторых регионов является градообразующей, по всей России предоставляет рабочие места и прочее. Поэтому такой бренд имеет повсеместную узнаваемость.

5. Частота использования

При запоминаемости бренда и его узнаваемости не менее важна частота использования товаров или услуг бренда. Чем чаще потребитель контактирует с ним – тем более высока вероятность его запоминания. Так, например, бренды молока потребителю будет легче вспомнить и перечислить несколько, чем бренды авиакомпаний.

6. Сарафанное радио

Такой феномен может быть запущен стихийно – пользователю действительно понравился продукт, он искренне посоветовал его другим, и личная рекомендация распространилась на большое число потенциальных потребителей. Считается, что личная рекомендация – это самый эффективный способ рекламы [1]. Однако не всегда качество продукта настолько восхищает пользователя, чтобы он его рекомендовал, поэтому некоторые компании, особенно производители/дистрибьютеры косметики прибегают к рекламе под прикрытием личной рекомендации у инфлюенсеров, которые, зачастую, являются лидерами мнений для своей целевой аудитории.

Подводя итоги, можно отметить, что совокупность всех факторов будет гарантировать абсолютный успех бренда у аудитории. Но не всегда у компаний есть такие возможности, это может объясняться ее масштабами, регионами присутствия, частотой контактов с аудиторией и конкурентной средой. На остальные факторы, вроде рекламной и СО-деятельности, сарафанное радио компании могут влиять. Хотя бы этих действий будет достаточно для общения с аудиторией и запоминания ею бренда. В статье был приведен пример коммуникации с аудиторией через СМИ платным и бесплатным способами. Для запуска «сарафанного радио» бренду достаточно будет производить качественный товар, не забывать про маркетинг упаковки, а для того, чтобы пользователь хотел порекомендовать услугу важно проработать и зарегистрировать сервис на достойном уровне с запоминающимися действиями.

Список используемых источников:

1. Бородин М. Преимущество частного мнения: инструменты продвижения // Prod&Prod: продвижение продовольствия. 2009. N 7-8 С. 9-10.
2. Официальный сайт «S7 Airlines». [Электронный ресурс]. М., 2022. URL: <https://www.s7.ru/ru/info/s7-airlines/brand/> (Дата обращения 13.11.2022)
3. Электронный журнал «Sostav». [Электронный ресурс]. М., 1998-2022. URL: <https://www.sostav.ru/publication/reklama-s7-airlines-pokorila-kanny-17425.html> (Дата обращения 13.11.2022)

Rusova A., Kulnazarova A.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Brand awareness factors.

The article touches upon the importance of brand awareness and discusses the factors influencing it. There are 6 factors influencing brand awareness: brand history, advertising and public relations, competitive environment, geographic location, frequency of use and word of mouth. Each factor is explained and supported by examples.

Key words: *brand, brand awareness, company image, communications, target audience.*

УДК 7.067
ГРНТИ 19.45.91

КИНОФИЛЬМ «БРАТ» РЕЖИССЕРА АЛЕКСЕЯ БАЛАБАНОВА КАК ПРИМЕР РОЛИ МЕДИА В ИНТЕРПРЕТАЦИИ ПЕРИОДА 90-ЫХ ГОДОВ

К. А. Стоноженко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье проводится анализ кинофильма 1997 года режиссера Алексея Балабанова «Брат». Кинематография является одним из средств коммуникации, которая способна воздействовать на человеческое сознание благодаря аудио и видео восприятию. Ярким примером данного феномена является кинофильм «Брат». Проведенное исследование позволяет выделить наиболее острые социальные проблемы в период 90-ых, а также кинематографические техники, которые Алексей Балабанов использует в данной картине.

кинематография, кинематографические приемы, Алексей Балабанов, «Брат», 90-ые

В современном мире отрицать возрастающую роль медиа достаточно сложно. Средства коммуникации обрели множество форм и видов, которые включают в себя всю совокупность технологических средств и приёмов взаимодействия для передачи конкретному потребителю информационного сообщения в том или ином виде: текст, музыка, изображение и многое другое. Одним из наиболее массовых средств коммуникации является кинематограф. Кинематография – это уникальное явление, которое способно передавать информацию о целых эпохах или о малейших существах посредством воздействия на массу через аудио или видео восприятие. Режиссеры, как важные деятели синематографа, способны не меньше других вносить свой вклад в историю человечества, интерпретируя в кино свой субъективный взгляд и используя для этого профессиональные навыки. Ярким примером данного феномена может служить кинематографическая работа 1997 года режиссера Алексея Балабанова – «Брат». В данной статье рассматривается социальная проблематика, выдвинутая Балабановым на первый план в картине «Брат», а также его способы взаимодействия с массовым потребителем посредством кинематографических техник.

Кинофильм «Брат» раскрывает множество социально-острых тем, стоящих перед обществом в период 90-ых. Главный герой кино – Данила Багров – недавно вернулся со службы в армии. Знакомство с Данилой началось с конфликта между ним и общества «богатых». Данила случайно попадает на съемки картины, мешая съемочной группе выполнять свою работу. Режиссер фильма в состоянии агрессии просит охрану вывести Данилу со съемочной площадки. Затевадается драка, в последствии которой Багров попадает в полицейский участок. Балабанов неспроста делает эту сцену вступительной. Тем самым, он с самого начала объясняет зрителю то, что главный герой не способен идти на поводу «богатого» общества. После этой сцены зритель узнает то, что Данила продолжительное время рос без отца, его заменил старший брат Виктор. Также главный герой во время вступительной сцены впервые слышит песню группы Наутилус Помпилиус [1] «Крылья», и песни именно этой группы будут сопутствовать

герою на протяжении всей картины, строки песен символизируют внутренний мир, ценности и приоритеты Данилы.

Далее путь главного героя развивается в городе Санкт-Петербург. Он едет туда с целью найти своего брата - происходит завязка фильма. В этот момент Балабанов раскрывает зрителям других персонажей фильма: немец Гофман, Кэт, Круглый. Каждый из этих героев символизирует своё общество. Круглый – глава преступной группировки, часто вставляющий в свою речь поговорки. Балабанов как будто бы высмеивает криминальных авторитетов того времени, показывая зрителю интеллектуальную ограниченность Круглого, а также его хитрость и жестокость. Кэт – представитель молодежи 90-ых. Этот персонаж открывает для зрителя новую остросоциальную проблему 90-ых – наркоманию. Ценности девушки ориентированы на западную культуру, Кэт открыта всему новому и незнакомому, но все это ограничивается ее зависимостью наркотическими веществами. Кэт не единственный представитель молодежи в этой картине. На протяжении всего фильма зритель может увидеть разных представителей молодежных субкультур: рокеры, панки, рейверы, хиппи. Однако, Балабанов выставляет центральной фигурой молодежи именно Кэт, которая не вписывается ни в одну молодежную субкультуру. Это объясняется тем, что молодежь того времени объединяет одна общая проблема – зависимость от наркотических веществ. Далее режиссер представляет зрителю крайне важного персонажа картины – немца Гофмана. Данила знакомится с немцем на рынке во время того, как у того вымогал денежные средства рэкетиры (еще один вид преступности того времени). Данила защитил немца, а тот в свою очередь познакомил Данилу со своим обществом. Посредством персонажа немца Гофмана, режиссер не только показывает мнение Данилы в отношении различных проблем того времени, учит светлой истине, оказывает помощь в трудной ситуации, но и осуждает за уподобление преступному обществу.

Уподобление Багрова криминальному обществу начинается тогда, когда его старший брат Виктор просит оказать ему помощь в трудной ситуации. Данила соглашается, ведь родственные связи являются для него одной из ценностей жизни. Балабанов помещает героя в типичную обстановку того времени. Засада бандитов и Данилы в квартире криминального элемента с целью убийства – это нередкое явление преступности в 90-ые. Во время длительного ожидания Данила решает посетить соседскую квартиру, в которой на тот момент праздновалось День Рождения. Это еще один ловкий прием Балабанова, показывающий несовместимость главного героя с преступным миром, а также его взаимоотношение с интеллигентным обществом, которое присутствовало на празднике. Интеллигенция там представлена в образах режиссеров, музыкантов и научных деятелей. Главному герою нравится в этом обществе, но его внутренняя жесткость и сила воли интеллигентное общество принять не сможет. Это доказывает то, что во время засады в квартире случайным образом оказался режиссер на радио, который по пути на празднование ошибся квартирой и стал заложником у бандитов. В последствии он соглашается против своей воли помочь главному герою, но при первой же возможности уходит от Данилы.

Одним из немаловажных персонажей картины становится Света, водитель грузового трамвая. Она оказала помощь главному герою, когда тот вступил в

перестрелку с бандитами. Любовная линия между Данилой и Светой раскрывает данных персонажей как чувственных, робких, готовых идти на риски ради любви. Света оказалась в опасности из-за Данилы, но при встрече с ним не стала обвинять его в этом. Багров, узнав о том, что муж Светы избивает ее, встал на защиту девушки. После того, как Данила спасает своего брата и заканчивает свой путь в Санкт-Петербурге, он навещает Свету для того, чтобы забрать ее с собой. Однако, Света была со своим мужем, который уже намеревался причинить ей боль. Главный герой снова спасает Свету выстрелом в ее мужа, но та просит Данилу уйти, акцентируя внимание на его преступной деятельности: «Что тебе стоит убить человека?» [2]. Данила дарит Свете прощальный подарок и уходит. Образ Светы в картине связан не только с любовной линией главного героя. Балабанов вкладывает в данного персонажа судьбы русских женщин в период 90-ых. Сильные, волевые, отважные женщины работали на тяжелом производстве, подвергались насилию, но все больше укоренялись в данную систему и боялись препятствовать ей. Света не решилась идти с Данилой, она осталась вместе со своим мужем, помогая ему и, наверное, понимая, что жесткость с его стороны по отношению к ней не прекратиться.

Кадры кинофильма показывают зрителю главного героя, идущего посреди живой и необъятной толпы. Данила выделяется среди всех остальных. Он не вписывается в рамки толпы, он не вписывается ни в одно из обществ, существовавших в период 90-ых. Последним, кого Данила встречает на своем пути стал шофер-дальнобойщик. Данная профессия вынуждает человека всегда находиться в пути, изредка останавливаясь. Став пассажиром данного транспорта, Данила снова оказался в пути, о конце которого он может только догадываться. На вопрос дальнобойщика о конечной станции пути, главный герой ответил – Москва. Данила не знает, что станет местом его конечного пребывания, но знает только то, что Москва – это место силы (по словам своего старшего брата). Однако, немец Гофман предупредил его о том, что большие города наоборот человека «ломают». [3] Данила решил испытать свою судьбу в новом месте, не слушая мнение немца.

Режиссер способен воздействовать на сознание зрителя, наделяя персонажей теми или иными качествами. Зритель же, исходя из своих собственных чувств, ценностей и принципов выбирает наиболее понравившегося персонажа. Кинофильм «Брат» Алексея Балабанова стал культовым и продолжает знакомить новые поколения с социальной составляющей 90-ых. Данила Багров – это идеал человека того времени, по мнению режиссера. Балабанов наделил его разнообразными качествами: справедливость, верность, отважность, искренность, надежность. Присудив все эти качества Даниле, режиссер выпускает его в мир 90-ых. Данила там находит себе любовь, друзей, врагов, но так и не становится частью какого-либо общества. Он делает это ненамеренно, ведь все те качества, которыми наделил его режиссер, не вписываются в рамки обществ того времени. Предательство, глупость, подлость и хитрость – этими качествами были пропитаны люди того времени в кинофильме. Данила не смог им соответствовать и подчиниться, и именно поэтому решил испытать свою судьбу в другом месте. Однако,

дальнейшую судьбу героя зритель сможет узнать, посмотрев вторую часть данной картины, режиссированную Алексеем Балабановым.

Список используемых источников:

1. Музыкальное творчество группы Наутилус Помпилиус: [Электронный ресурс] // Butusov.ru. 2022. URL: <http://butusov.ru/music> (Дата обращения 06.11.2022).
2. «Брат» (реж. Алексей Балабанов, 1997).
3. «Брат» (реж. Алексей Балабанов, 1997).

Stonojenko X.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

The film "Brother" directed by Alexey Balabanov as an example of the role of the media in the interpretation of the period of the 90s.

This article analyzes the film directed by Alexey Balabanov "Brother". Cinematography is one of the means of communication that is able to influence human consciousness through audio and video perception. A striking example of this phenomenon is the movie "Brother". The conducted research allows us to identify the most acute social problems in the period of the 90s, aslso the cinematographic techniques that Alexey Balabanov uses in this picture.

Key words: *cinematography, cinematographic techniques, Alexey Balabanov, "Brother", the 90s.*

УДК 659.4
ГРНТИ 06.81

ПРОДВИЖЕНИЕ БРЕНДА SNKRS Clean В Telegram

В. А. Ядрышников, Д. В. Шутман

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Продвижение своего бренда за последние годы сильно изменилось. Сегодня это сделать намного проще и дешевле. В связи с этим малый и средний бизнес начал лучше развиваться, что позволяет улучшать и сферу маркетинга. Кто-то продает вещи, кто-то предлагает свои услуги. Продвижение своих знаний, навыков и умений выходит на совершенно другой уровень.

бренд, продвижение, химчистка

История создания

На сегодняшний день каждый из нас носит кроссовки и как правило многие даже не задумываются о том, как правильно ухаживать за своей обувью. Именно из-за этого мы и решили начать предоставлять свои услуги и поднимать эрудированность людей в этом вопросе.

Компания SNKRS Clean занимается профессиональной химчисткой кроссовок. Все пары, которые попадают к нам проходят исключительно ручную химчистку с использованием профессиональных средств.

Миссия компании заключается в том, чтобы привить людям культуру ухода за своей обувью.

Особенностью можно считать, что мы индивидуально общаемся с каждым клиентом и рассказываем какие именно действия мы проводить с их обувью. Мы стараемся быть полностью открытыми по отношению к своим клиентам.

Перед тем как отдать пару своим клиентам мы упаковываем всё в брендированный пакет.

Целевая аудитория

Основной нашей целевой аудиторией являются люди от 16 до 45 лет, которые увлекаются культурой кроссовок. Как правило эти люди стараются ухаживать за своей обувью и чаще всего прибегают к услугам профессионалов.

Конкуренты

Рынок услуг в сфере химчистки кроссовок в России только начал развиваться, но в крупных городах уже есть примеры успешных проектов в данном сегменте.

Основными нашими конкурентами в Санкт-Петербурге являются 3 компании:

1. Clean Step
2. 2 Brata
3. Sneaker Клин

Продвижение

Наша компания выбрала Telegram основным видом продвижение. На это есть несколько причин:

1. Возможность публиковать как фото-видео контент, так и текстовые сообщения
2. Возможность быстро набрать аудиторию
3. Большая клиентская база

Есть несколько вариантов развития своего бизнеса в данном мессенджере:

1. Площадка бренда. Публикация информации от лица компании
2. Чат-боты. Ответы на часто задаваемые вопросы
3. Публикация в каналах. Покупка публикаций у инфлюенсеров
4. Публичные чаты. Создание комьюнити
5. Стикеры
6. Техподдержка

Для продвижения нашей компании мы выбрали основной канал, для публикации примеров наших работ.

Закупку рекламных мест у инфлюенсеров таких как Сергей Стилиов, который является профессиональным дрифт гонщиком, а также в каналах, связанных с обувью.

Так же мы решили добавить стикеров связанных с культовыми парами для культуры кроссовок.

Создание публичного чата поможет людям с тягой к кроссовкам общаться друг с другом, обмениваться интересными новостями в мире кроссовок и обмениваться друг с другом парами. Мы хотим создать площадку, где люди со схожими интересами смогут знакомиться, встречаться и создавать совершенно новое комьюнити на территории Санкт-Петербурга. Так же через этот чат мы хотим информировать людей о мероприятиях, которые мы будет проводить оффлайн. Мы хотим проводить ивенты связанные с кроссовками, проводить лекции и просто общаться со своей аудиторией.

Список используемых источников:

1. Чумиков А.Н., Бочаров М.П. Связи с общественностью: теория и практика: учеб. пособие. М.: Дело, 2006. – 552 с.
2. Ольшанский Д. В. Психология масс. СПб.: Питер, 2002. – 368 с.
3. Myacademy.ru

Yadryshnikov A., Shutman D.

The Bonch-Bruевич Saint-Petersburg State University of Telecommunication

Promotion of the SNKRS Clean brand on Telegram.

Brand promotion has changed a lot in recent years. Today it is much easier and cheaper to do this. In this regard, small and medium-sized businesses began to develop better, which makes it possible to improve the marketing sphere. Someone sells things, someone offers their services. Promoting your knowledge, skills and abilities goes to a completely different level.

Key words: brand, promotion, dry clining.

СВЕДЕНИЯ ОБ АВТОРАХ

- АБИТОВ Илья Дамирович студент группы ИКТУ-98 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ilyaabitov9@gmail.com
- АБРАМЕНКО Георгий Тимофеевич студент группы ИКТБ-17м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, georgabramenko@gmail.com
- АГОШТИНЬЮ Пенаш Созинью студент группы ИКТФ-26м, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, apsgeral21@gmail.com
- АКОНЯ Джон студент группы ИКТЗ-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, john.akonya@gmail.com
- АЛЕКСАНДРОВ Фёдор Тарасович студент группы РК-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, f-alexandrov@mail.ru
- АЛЕКСАНДРОВА Агата Георгиевна студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, agatka.aleksandrova27@mail.ru
- АСТАФЬЕВА-РУМЯНЦЕВА Ирина Евгеньевна кандидат философских наук, доцент кафедры социально-политических наук Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rina.astafjewa@yandex.ru

АМИНОВ Станислав
Олегович

студент группы РСО-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aminovstanislav1@yandex.ru

АНАНЬЕВ Михаил
Андреевич

студент группы ИСТ-112м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, deadok51@gmail.com

АНДРЕЕВА Елена
Ивановна

кандидат физико-математических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andreevaelenafil@gmail.com

АНДРИАНОВ Дмитрий
Максимович

студент группы ИСТ-931 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dimon60thief@gmail.com

АНДРИЕВСКИЙ Никита
Константинович

студент группы ИКТК-01 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andrievskynikita@gmail.com

АНДРИЯНОВ Игорь
Андрьянов

студент группы РСО-11м Санкт-Петербургского государственного университета телекоммуникаций им проф. М. А. Бонч-Бруевича, igor.andriyanov17@yandex.ru

АНДРЮНИН Александр
Игоревич

студент группы ИКТФ-16м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sasha4365@gmail.com

АНТИПИН Борис
Маврович

кандидат технических наук, доцент кафедры телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, boris_antipin@mail.ru

АСКЕРОВ Марат Тагирович	студент группы Р-22м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, marat.askerov.2000@mail.ru
АФАНАСЬЕВ Никита Андреевич	студент группы РТ-11м, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, plaffy.cs@gmail.com
БАБЕНКО Максим Сергеевич	студент группы Р-22м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maximsergeevich12@gmail.com
БАБКОВ Иван Николаевич	кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ib9809@mail.ru
БАБУРИН Евгений Владимирович	студент группы РМ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, evgenii-0406@mail.ru
БАЛАБАНОВ Сергей Витальевич	аспирант, младший научный сотрудник ИХС РАН, sergeybalabanov@yahoo.com
БАРАКАТ Абдельрахман	студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ayb.jo.93@hotmail.com
БАТАЛИН Никита Сергеевич	студент группы ИКТГ-24м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nikbat97@gmail.com

БЕРЕЗКИН Александр Александрович	кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники, преподаватель базовой кафедры «Программной инженерии и вычислительной техники» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pcdreams@mail.ru
БЕЛОЗЕРОВ Клим Владимирович	студент группы ИКТК-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, milk8490@gmail.com
БЕЛОУС Константин Владимирович	кандидат технических наук, доцент кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kostos2@yandex.ru
БЕЛОЦЕРКОВСКИЙ Максим Вадимович	студент группы ЭП-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hellboysatan@icloud.com
БИРИХ Эрнест Владимирович	старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, be1982@mail.ru
БОВШИК Павел Павлович	студент группы ИСТ-111м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pbovshik@mail.ru
БОГАТЫРЕВ Кирилл Денисович	студент группы ФП-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kiry.bog@mail.ru

- БОГДАНОВА Екатерина Игоревна студент группы ИКТМ-11 Поволжского государственного университета телекоммуникаций и информатики, k.bogdanova.99@mail.ru
- БОГДАНОВА Мария Алексеевна студент группы РСО-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mary.bogdanova.01@mail.ru
- БОГОМАЗ Мария Эдуардовна студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maria.bogomaz15@gmail.com
- БОГОМЕДОВА Карина Магомедовна студент группы ИКБ-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, thenadaka@gmail.com
- БОЖЕДОМОВ Артём Юрьевич студент группы ИКТМ-22м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artembozhedomov@internet.ru
- БОНДАРЕНКО Игорь Борисович кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, igorbnd@gmail.com
- БОНДАРЬ Николай Алексеевич студент группы ЗР-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, khv27.rus@yandex.ru
- БОРИСОВ Владимир Игоревич студент группы ИКТБ-18м, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, architectxor@gmail.com,

- БОЯШОВА Елена
Петровна
старший преподаватель кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, helen.glass@mail.ru
- БЫЛИНА Мария
Сергеевна
кандидат технических наук, доцент, заведующий кафедрой фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bylinamaria@mail.ru
- БЫСТРОВ Роман
Владиленович
студент группы РСО-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rom-fantom7@mail.ru
- БЫЧКОВ Алексей
Викторович
аспирант кафедры «Фотоники и линий связи» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, freezqq@yandex.ru
- ВАСИЛЬЕВ Владимир
Михайлович
студент группы РСО-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
- ВАСИЛЬЕВ Николай
Сергеевич
студент группы ИКФ-11 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
vasilievmenkolian123456@gmail.com
- ВЕРБИЦКИЙ Алексей
Владимирович
студент группы Р-11м, заведующий лабораторией базовой кафедры «Цифровое телевизионное и радиовещание» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, A_verbitsky@mail.ru

- ВИТКОВА Лидия Андреевна кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук СПб ФИЦ РАН
- ВОЛКОВА Анастасия Ивановна студент группы Р-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nastusha1838@gmail.com
- ВОЛОКУШИНА Ксения Павловна студент группы ИКБ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ksylik@gmail.com
- ВОЛОШИНОВ Денис Вячеславович доктор технических наук, профессор, заведующий кафедрой информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, denis.voloshinov@yandex.ru
- ВОРОБЬЕВ О. В. к.т.н., профессор, Заведующий кафедры Радиосвязи и Вещания (РСиВ) Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
- ВОРОПАЕВ Павел Валерьевич студент группы ФП-91, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, phoropaev1@gmail.com
- ВОРОШНИН Григорий Евгеньевич студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, voroshnin.g@yandex.ru

ВТОРЫХ Виталий Станиславович	студент группы Р-12м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vitas-vv1998@mail.ru
ВЫБОРНОВА Анастасия Игоревна	кандидат технических наук, доцент и преподаватель кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.vybornova@spbgut.ru
ВЫЖЛОВА Ангелина Кирилловна	студент группы ИСТ-241м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, angelsurvivor13@gmail.com
ГАВРИКОВ Илья Игоревич	студент группы РД-01 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, техник АО "Котлин-Новатор", homsyck@gmail.com
ГЕЛЬФАНД Артем Максимович	старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича amgelfand@mail.ru
ГЕРАСИМОВА Яна Александровна	студент группы ИКТГ-14м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gerasimova.jana2014@yandex.ru
ГЕРАСЬКИН Валерий Кириллович	студент группы ИКТГ-14м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, geraskin.valery@gmail.com

- ГЕХТ Антон Борисович кандидат исторических наук, доцент, заведующий кафедрой истории и регионоведения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.geht@yandex.ru
- ГИНИЯТУЛЛИН Александр Эдуардович студент группы ИКТФ-26м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kompot26452@mail.ru
- ГЛУХОВ Николай Иванович старший преподаватель кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glukhov_nikolay@mail.ru
- ГЛУШАНКОВ Евгений Иванович доктор технических наук, профессор, профессор кафедры радиосистем и обработки сигналов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glushankov57@gmail.com
- ГОЛОВКИНА Мария Вилевна кандидат физико-математических наук, доцент кафедры «Физики» Поволжского государственного университета телекоммуникаций и информатики, nauka77@yandex.ru
- ГОНЧАРОВ Егор Евгеньевич студент группы ИКМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vip.egostar@mail.ru
- ГОНЧАРОВ Федор Михайлович студент группы V4121 Национального исследовательского университета ИТМО, инженер лаборатории квантовых коммуникаций национального исследовательского университета ИТМО

ГОРЦУЕВА Александра Сергеевна	студент группы Р-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ddhearted@icloud.com
ГРАДОВСКИЙ Максим Владимирович	студент группы ИКТК-96 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maksonmda@yandex.ru
ГРЕБЕШКОВ Александр Юрьевич	доктор технических наук, профессор кафедры «Информационные технологии» Самарского государственного технического университета, algre@mail.ru
ГРИГОРЕНКО Иван Константинович	студент группы ИКМ-02з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, griga24@mail.ru
ГРИГОРЬЕВ Андрей Алексеевич	студент группы ИКПИ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, grigoriew.ron@yandex.ru
ГРИГОРЬЕВ Максим Николаевич	студент группы Р-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, grigorjev.maksi2011@yandex.ru
ГРИГОРЬЕВА Рината Григорьевна	студент группы ИСТ-211м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, honey.lottu@gmail.com
ГРИШИН Валерий Валерьевич	студент группы ФП-01 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, valeriy.01@bk.ru
ГРОХОЛЬСКИЙ Артём Викторович	студент группы ФП-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artem.groh2110@yandex.ru

ГУБИН Александр Николаевич	кандидат технических наук, доцент, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gan50_60@mail.ru
ГУЛЬТЯЕВА Людмила Александровна	студент группы ИКТФ-16м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lyudmila150@gmail.com
ГУЛЯЕВ Руслан Сергеевич	студент группы ФП-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, GRulan526@gmail.com
ДАВЫДОВ Вадим Владимирович	доктор физико-математических наук, профессор кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ДАМДИНОВ Баир Булатович	студент группы ИСТ-112м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, damdinov99@mail.ru
ДАНИЛОВА Юлия Сергеевна	студент группы ИКТБ-17м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, danilovajulia123@gmail.com
ДЕМЕНТЬЕВ Роман Игоревич	студент группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hjvf128@mail.ru
ДЕМИДОВ Павел Сергеевич	студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pushad187@gmail.com

ДЕРЖКО Дмитрий Ярославович	студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dimaderzhko@gmail.com
ДЖАПАРОВА Диана Абдрашитовна	студент группы ИСТ-131м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dzhaparovadiana@yandex.ru
ДЖОРАЕВ Хангелди	студент группы ИКТБ-17м Санкт-Петербургского государственного университета телекоммуникаций им. М.А. Бонч- Бруевича, jorayev.net@yandex.com
ДИБРОВА Олеся Павловна	студент группы ИСТ-933 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dibrovals5861@gmail.com
ДМИТРИЕВА Диана Владимировна	студент группы ИКТО-08 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, howaitohu@gmail.com
ДМИТРИЕВА Диана Сергеевна	студент группы ИКТФ-16м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitrievadiana1405@gmail.com
ДОБРАЯ Олеся Павловна	студент группы РМ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, olesadobraa@gmail.com
ДОБЫЧИНА Ярослава Германовна	театровед, корреспондент информационного агентства «Невские новости»
ДОРОГАНОВ Дмитрий Валерьевич	студент группы БИМ-01з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dimac100d@yandex.ru

- ДРЕПА Владислав
Евгеньевич студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladikdrepa@mail.ru
- ДУДЕВИЧ Диана
Николаевна студент группы Р-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shoroh010@gmail.com
- ДУКАЛЬСКАЯ Ирина
Владимировна кандидат филологических наук, доцент, доцент кафедры иностранных языков Поволжского государственного университета телекоммуникаций и информатики, dukalskaya_psuti@mail.ru
- ДУНАЕВ Николай
Павлович студент группы РК-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ndunaev@inbox.ru
- ДУСКАЕВ Денис
Данилович студент группы БИМ-01з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, duskaev.dd@gmail.com
- ДЮБОВ Андрей
Сергеевич кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, blip@bk.ru
- ДЯТЧЕНКО Анастасия
Андреевна студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dyatchenko-a@kiszi.ru
- ЕГОРОВА Анастасия
Леонидовна студент группы ИКТБ-17м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egorovaucheba@gmail.com

ЕДЕМСКАЯ Екатерина Дмитриевна	студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, katerina.edemskaya51@gmail.com
ЕЖОВ Глеб Владимирович	студент группы ПриМ-21 Поволжского государственного университета телекоммуникаций и информатики, glebid76@gmail.com
ЕЛАГИН Василий Сергеевич	кандидат технических наук, доцент кафедры инфокоммуникационных систем, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elagin.vas@gmail.com
ЕЛИЗАРОВА Лия Романовна	студент группы ИКБ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elizarovaaliya@gmail.com
ЕЛИСЕЕВА Ксения Алексеевна	студент группы ИКТИ-15м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, drami6869@mail.ru
ЕЛФИМОВ Александр Владимирович	студент группы ИКТЗ-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича Elfim4212@mail.ru
ЕЛЬКИН Александр Александрович	студент группы ИСТ-132м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vash.gospodin01@gmail.com
ЕМЕЛЬЯНЕНКО Георгий Юрьевич	студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gogoshanin2000@gmail.com

- ЕРМОЛАЕВ Данила Андреевич
студент группы ИСТ-212м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, danku3377@gmail.com
- ЕРМОЛАЕВ Егор Евгеньевич
студент группы ИКТГ-14м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egoulya@mail.ru
- ЕРОХОВА Нина Александровна
студент группы ИКПИ-292м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ninel_e@icloud.com
- ЕСЕНБЕКОВ Рустем Муратович
студент группы РК-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, esenbekov.rm@net.sut.ru
- ЖАДАН Роман Алексеевич
студент группы ЗР-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Zhadan_2000@bk.ru
- ЖЕЛТОВА Елена Петровна
кандидат педагогических наук, доцент кафедры иностранных и русского языков Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elena_gzeltova@mail.ru
- ЖИКИН Сергей Александрович
студент группы ФП-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zhikin.20001@gmail.com
- ЗАБЗЕЕВ Егор Алексеевич
студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zabzeev.ea@yandex.ru

ЗАВАЦКАЯ Анастасия Александровна	студент группы ИКПИ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zaa.3007@yandex.ru
ЗАГРЕБАЕВА Надежда Михайловна	студент группы ЭБМ-113 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nzagrebaeva12@gmail.com
ЗАЙЦЕВА Ярослава Сергеевна	студент группы РТ-01 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nyashkakekusik@gmail.com
ЗАЙЧЕНКО Анна Александровна	студент группы Р-22м Санкт-Петербургского университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ZaichenkoAnn@mail.ru
ЗАЯЦ Максим Петрович	студент группы ИКТС-13м Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maksim-zajac29@yandex.ru
ЗЕНЧЕНКО Андрей Константинович	студент группы ИКТИ-25м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zozh920@gmail.com
ЗРЕЛОВА Анастасия Леонидовна	студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nastyzr@gmail.com
ИВАНИЛОВА Юлия Александровна	студент группы ИКТЗ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, juliatee777@gmail.com
ИЗМЕСТЬЕВА Екатерина Александровна	студент группы РД-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chainlo@yandex.ru

ИЗРАИЛОВ Константин Евгеньевич	кандидат технических наук, доцент кафедры защищенных систем связи, преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, konstantin.izrailov@mail.ru
ИЗРЯДНОВ Владислав Дмитриевич	студент группы ИСТ-141м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, izr2017vlkad@gmail.ru
ИСАЕНКО Дмитрий Игоревич	аспирант группы 2215А-22 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, isaenko-d@mail.ru
ИСКРА Илья Игоревич	студент группы ИКПИ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ilya.iskra2020@gmail.com
ИСУПОВ Александр Ильич	студент группы ИКТФ-26м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Is.alex60@gmail.com
КАЖАЕВ Максим Валерьевич	студент группы ИКМ-02з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, warcons8@gmail.com
КАЗАКОВ Никита Игоревич	студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КАЗАКОВА Мария Сергеевна	аспирант кафедры «Цифровой экономики» Поволжского государственного университета телекоммуникаций и информатики, kazaova.m93@yandex.ru

КАЗАЧЕНКО Ирина Олеговна	студент группы ИКТМ-22м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kazachenko_ira22@mail.ru
КАКУСИЛУМЕЗО Сандру Эдуарду	студент группы ИКТО-08 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fillixnet@gmail.com
КАЛАШНИКОВА Людмила Ивановна	студент группы ИКМ-02з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, blip@mail.ru
КАРАНОВА Евгения Есимжановна	студент группы РТ-12м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, karanova-zhenya@mail.ru
КАРЛИН Владимир Эдуардович	аспирант Сибирского Государственного университета телекоммуникаций и информатики
КАРПЕКИН Артур Андреевич	студент группы ЭП-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, korolev.2195@gmail.com
КАРПОВ Евгений Евгеньевич	аспирант группы 7797, национального исследовательского университета ИТМО,
КАРПОВА Виктория Денисовна	студент группы ИСТ-933 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, karvikd96@gmail.com
КАЧУРОВСКИЙ Юрий Олегович	студент группы ИКТЗ-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, eter4eter@gmail.com

- КИРИЛЛОВА Мария Кирилловна студент группы ИСТ-951 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kirmary2001@gmail.com
- КИРИЛЛОВА Анна Кирилловна студент группы ИСТ-951 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kiranja2001@gmail.com
- КИРСАНОВ Дмитрий Михайлович студент группы РТ-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kersa1999@gmail.com
- КИСЕЛЁВ Тимофей Витальевич студент группы РД-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2895@list.ru
- КИСЛЯКОВ Сергей Викторович кандидат технических наук, доцент кафедры инфокоммуникационных систем, преподаватель базовой кафедры «Инновационные технологии телекоммуникаций» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, s.v.kislyakov@gmail.com
- КИРИК Дмитрий Игоревич кандидат технических наук, декан факультета радиотехнологий связи, заведующий кафедрой конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, d_i_kirik@mail.ru
- КИРИЧЕК Р. В. доктор технических наук, доцент, заведующий кафедрой ПИиВТ, преподаватель базовой кафедры ИТТ Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

- КИСТРУГА Антон Юрьевич студент группы 1001А-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anton.kistruga@gmail.com
- КЛАБУКОВ Сергей Александрович студент группы ИКПИ-292м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, klabser@gmail.com
- КЛИМЕНКО Василий Павлович студент группы ИКф-11 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, klimencko.vasilij2018@yandex.ru
- КНИГИНИЦКИЙ Егор Игоревич студент группы ФП-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egor.knig@yandex.ru
- КОВАЛЕВ Илья Алексеевич студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cov.cov.cov70@gmail.com
- КОВАЛЕВА Ольга Петровна кандидат технических наук, доцент, преподаватель кафедры «Технологии древесных и целлюлозных композиционных материалов» Санкт-Петербургского государственного лесотехнического университета им. С.М. Кирова, olga-kovaleva-cbp@yandex.ru
- КОВАЛЬЧУК Анастасия Васильевна студент группы ИСТ-212м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kovana9951@ya.ru
- КОВЦУР Максим Михайлович доктор технических наук, доцент кафедры защищенных сетей связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxkovzur@mail.ru

- КОЛОМИЙЦЕВ Руслан
Константинович студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, russlankot@mail.ru
- КОЛОСЬКО Анатолий
Григорьевич кандидат физико-математических наук, доцент, преподаватель кафедры конструирования и проектирования радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, agkolosko@mail.ru
- КОНИЧЕВ Дмитрий
Альбертович студент группы ИКТК-96 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dimakonichev@gmail.com
- КОНСТАНТИНОВ Егор
Сергеевич студент группы РТЦ-92 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
- КОРНЮШКИН Дмитрий
Александрович аспирант группы 0906А-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kornyushkin_98@mail.ru
- КОРОВИН Константин
Олегович кандидат физико-математических наук, заведующий кафедры радиосистем и обработки сигнала, доцент кафедры радиосистем и обработки сигнала Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, konstkor@mail.ru
- КОРОТИН Владимир
Евгеньевич кандидат технических наук, доцент, доцент кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

- КОСЕНКОВ Виталий
Владимирович студент группы ИКТЗ-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича kosimp331@gmail.com
- КОСЬЯНОВ Михаил
Николаевич студент группы Р-22м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, misha.kosjanov@yandex.ru
- КОТОВ Михаил
Александрович студент группы ИКТГ-14м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, misha73251@mail.ru
- КРАВЦОВА Валерия
Андреевна студент группы ИКТЗ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kravtsova_valeria@mail.ru
- КРАСАВЦЕВА Ксения
Алексеевна студент группы ИСТ-212м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Krasavtseva.Ks@yandex.ru
- КРЕМЛЁВА Наталия
Анатольевна кандидат экономических наук, доцент кафедры «Инновационного менеджмента и управления проектами» Вологодского государственного университета, kremlevana@vogu35.ru
- КРЕСТЬЯШИН Никита
Антонович студент ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kaktuz28@mail.ru
- КРЕЩЕНКО Дарья
Сергеевна студент группы 08-246 Казанского (Приволжского) федерального университета, dashakreshchenko@gmail.com
- КРИВОНОГОВА
Екатерина Владимировна студент группы Р-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krivonogovae798@gmail.com

КРЫЛОВ Андрей
Альбертович

кандидат технических наук, доцент кафедры инфокоммуникационных систем, преподаватель курсов «Сети связи и системы коммутации», «Корпоративные системы связи», «Call-центры в инфокоммуникационных системах». Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

КРЫЛОВ Дмитрий
Александрович

студент группы ИСМ-11з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krylovdm@bk.ru

КУЗЕНОВ Сергей
Ризабекович

ассистент кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, skuzenov@yandex.ru

КУЗЬМИН Андрей
Александрович

студент группы Р-12м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mrskippi@yandex.ru

КУЗЬМИНА Виктория
Эдуардовна

студент группы ИКМ-02з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, movetton@yandex.ru

КУЗЬМИНА Ольга
Ивановна

студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Olgakuzmina2000@mail.ru

КУКУНИН Дмитрий
Сергеевич

кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, coux@yandex.ru

КУКУШКИН Павел Сергеевич	студент группы ИКПИ-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, polposhta@gmail.com
КУЛИГИНА Екатерина Эдуардовна	студент группы ИКПИ-04 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, squarekatet@gmail.com
КУЛЬНАЗАРОВА Анастасия Витальевна	кандидат политических наук, доцент кафедры социально-политических наук Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, av-spn@ya.ru
КУСИКОВ Кирилл Сергеевич	студент группы ИСМ-11з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, novitskykirill@gmail.com
КУЧЕРЯВЫЙ Александр Игоревич	студент группы ФП-22м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, can4oys@list.ru
КУЧИНСКИЙ Егор Станиславович	студент группы ИСТ-261 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egor-kuch@yandex.ru
ЛАВРОВ Максим Николаевич	студент группы РТ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Lavrov_mn@mail.ru
ЛАКОМКИНА Елена Александровна	студент группы ИСМ-11з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vip.lakomkina@mail.ru

- ЛАПЦЕВИЧ Григорий Петрович студент группы ИКТГ-24м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, grisha_laptsevich14@mail.ru
- ЛАРИОНОВ Александр Юрьевич студент группы РТ-12м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, larionovaleks97@mail.ru
- ЛАРИОНОВА Александра Константиновна студент группы ФП-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 06012000larionova@gmail.com
- ЛЕБЕДЕВ Александр Константинович студент группы РТ-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sanek.lebedev1337@gmail.com
- ЛЕБЕДЕВ Даниил Владимирович кандидат технических наук, доцент кафедры инфокоммуникационных систем, преподаватель базовой кафедры «Инновационные технологии телекоммуникаций» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, s.v.kislyakov@gmail.com
- ЛЕВЧЕНКО Владислава Витальевна студент группы РСО-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, levchenko_vladislava@bk.ru
- ЛЕОНОВА Елизавета Александровна студент группы ИСТ-111м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, jolose2012@gmail.com
- ЛЕОНОВА Мария Дмитриевна студент группы ИКТИ-25м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maria_240600@outlook.com

ЛЕОНТЬЕВ Александр Сергеевич	аспирант группы 0301А-21, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЛЕШУКОВА Анастасия Михайловна	студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, n.leshukova98@gmail.com
ЛЕЩИНСКИЙ Павел Валерьевич	студент группы ЗР-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЛИКОНЦЕВ Алексей Николаевич	кандидат технических наук, доцент кафедры радиосистем и обработки сигналов, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, likontsev-rts@mail.ru
ЛИСТВИНА Наталья Сергеевна	студент группы РСО-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, listvinanatalya@gmail.com
ЛИТВИНОВ Алексей Сергеевич	студент группы РД-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lex415961@gmail.com
ЛИТВИНОВ Владислав Леонидович	кандидат технических наук, доцент, доцент кафедры информационных управляющих систем, заместитель декана по научной работе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vlad.litvinov61@gmail.com
ЛИХТЦИНДЕР Борис Яковлевич	профессор кафедры «Сети и системы связи» Поволжского государственного университета телекоммуникаций и информатики, вице-президент РОО АТИ, Заслуженный работник высшей школы РФ, доктор технических наук, профессор, lixt@psuti.ru

ЛОСЕВ Арсений Павлович	студент группы ИСТ-131м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, техник НОЦ "Медиацентр", aplosev@mail.ru
ЛОЧКАРЕВ Егор Андреевич	студент группы ИКТК-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sega.omich@gmail.com
ЛОХОВ Денис Александрович	студент группы ИКТИ-25м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ldenis.17@bk.ru
ЛЫКОВ Глеб Романович	студент группы ОБ-81з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
Люй Инчжэн	аспирант группы 6020501/20004 Санкт-Петербургского политехнического университета Петра Великого, lyuyz83@gmail.com
МАКАРОВА Александра Константиновна	студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Alex-ecureuil@mail.ru
МАКАРОВА Валерия Вячеславовна	студент группы ИСТ-131м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, makarovalerra@gmail.com
МАКЕЕВ Никита Андреевич	студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

- МАКОЛКИНА Мария Александровна доктор технических наук, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, makolkina@list.ru
- МАКСИМОВА Серафима Вячеславовна студент группы ИСТ-232м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, simamaximoff@gmail.com
- МАЛАХОВ Сергей Валерьевич кандидат технических наук, доцент кафедры «Программной инженерии» Поволжского Государственного Университета Телекоммуникаций и Информатики, malakhov-sv@psuti.ru
- МАНВЕЛОВА Наталья Евгеньевна кандидат технических наук, доцент кафедры экологической безопасности телекоммуникаций, преподаватель базовой кафедры «Экологическая безопасность телекоммуникаций» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, manvelova@inbox.ru
- МАРЗАГАНОВ Георгий Игоревич студент группы ИСТ-913 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, marzaganov.g.i@gmail.com
- МАРКОВЕЦ Вероника Александровна студент группы РМ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, veronika.markovets@gmail.com
- МАРТЫНОВА Елена Алексеевна студент группы Р-12м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lenchikmartunova@mail.ru
- МАРЧЕНКО Антон Александрович студент группы 3110 Санкт-Петербургского государственного морского технического университета, anton.m55@mail.ru

МАСЮТИН Михаил Дмитриевич	студент группы ИСТ-921 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, capslock228322@gmail.com
МАТЮЩЕНКО Марк Сергеевич	студент группы ИКМ-02з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, marcas7ms@mail.ru
МАХАЛОВ Евгений Александрович	студент группы РК-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, djeka3@bk.ru
МАШОШИН Евгений Сергеевич	студент группы ИСТ-232м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pb@svyatmtk0.ru
МЕБОНИЯ Маргарита Алексеевна	студент группы РТ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, margarita.meboniya@gmail.com
МЕДВЕДЕВ Илья Николаевич	студент группы ИКМ-12з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, medveddyson@yandex.ru
МЕЛЬНИК Максим Владимирович	студент группы ИКТБ-17м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mkmxvh@gmail.com
МЕЛЬНИКОВ Максим Владиславович	студент группы ИСТ-932 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxim.mel4985@gmail.com
МЕНДУС Роман Дмитриевич	студент группы ИСТ-111м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, judo.gel@gmail.com

МИКОВ Владислав Эдуардович	студент группы БИМ-01з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vlados-mikos@yandex.ru
МИНЕЕВА Варвара Дмитриевна	студент группы ИКТГ-24м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, varvaramineyeva@gmail.com
МИРОНОВ Павел Васильевич	студент группы ИСМ-01з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, passhok2008@yandex.ru
МИТЮРЕВА Анастасия Вячеславовна	студент группы БИМ-01з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mityureva.anastasiya@mail.ru
МИХАЙЛОВ Даниил Александрович	студент группы БИМ-01з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mixl-den@yandex.ru
МИХАЙЛОВ Даниил Михайлович	студент группы ИКПИ-292м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, danny.mhlv@gmail.com
МИХАЙЛОВА Екатерина Александровна	студент группы ИСМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kate200197@gmail.com
МИХАЛЬ Георгий Андреевич	студент группы ИСТ-111м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, georgemihal@yandex.ru

- МИШАКОВ Владимир
Алексеевич студент группы ИКПИ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 01.vladimir.mishakov@gmail.com
- МОГИЛАТОВ Антон
Викторович студент группы ФП-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, antonmogilatov@yandex.ru
- МОИСЕЕВА Алия
Вадимовна студент группы ИКТС-13м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alia.vm01@gmail.com
- МОЛЧАНОВ Александр
Павлович студент группы Р-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cach22a@yandex.ru
- МОРДОВИН Владимир
Николаевич кандидат педагогических наук, доцент, преподаватель кафедры конструирования и производства радиоэлектронных средств, ученый секретарь совета факультета «Радиотехнологий связи» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mvn6767@mail.ru
- МОРОЗ Елена Евгеньевна студент группы ЭП-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tsorelen@yandex.ru
- МОРОЗОВА Екатерина
Антоновна студент группы Р-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, morwaykate@gmail.ru
- МУРАШКИН Никита
Анатольевич студент группы ИКПИ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, niwhalea23@gmail.com

МУСАЕВА Татьяна
Вагифовна

кандидат технических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, neli_6868@mail.ru

МУТХАННА Аммар
Салех Али

доцент кафедры телекоммуникационных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, muthanna.asa@spbgut.ru

НАГАЕВА Анна
Дмитриевна

студент группы ИКТ3-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nagaeva_anna30@mail.ru

НАЗАРОВ Илья
Викторович

студент группы ЭП-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ilnaz5@icloud.com

НАСЕДКИН Борис
Александрович

аспирант группы 7720 национального исследовательского университета ИТМО, научный сотрудник лаборатории квантовых процессов и измерений национального исследовательского университета ИТМО, научный сотрудник лаборатории квантовых коммуникаций национального исследовательского университета ИТМО

НАУМЕНКО Виталия
Евгеньевна

студент группы Р-12м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, persikvita@mail.ru

НЕКРАСОВ Вадим
Николаевич

студент группы ИКТК-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nekrasoww645@gmail.com

НЕРОВНЫЙ Артём Викторович	старший преподаватель кафедры истории и регионоведения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч- Бруевича, art830@yandex.ru
НЕФЕДОВ Виталий Владимирович	студент группы ИКТБ-17м Санкт- Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vit02.08.19992@mail.ru
НЕФЕДОВ Даниил Ильич	студент группы ИСТ-232м Санкт- Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича ne.danya2011@yandex.ru
НЕЧАЕВ Андрей Александрович	студент группы ИКТБ-27м Санкт- Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lcme.nechaev@mail.ru
НИКИТИН Егор Денисович	студент группы ИКТИ-15м Санкт- Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yagor187@gmail.com
НИКИТИН Игорь Александрович	студент группы Р-12м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч- Бруевича, northsaren@ya.ru
НИКИТИН Максим Андреевич	студент группы РТ-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч- Бруевича, manikitin2008@mail.ru
НИКИТИН Юрий Александрович	кандидат технических наук, доцент, старший научный сотрудник кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч- Бруевича, yuriyan@list.ru

НИКОЛАЕВ Владимир Нгокович	студент группы РСО-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича valdonikolaev99@mail.ru
НИКОЛАЕВ Евгений Викторович	студент группы ИКМ-02з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yevgeniy_nikolayev_19@bk.ru
НИКОЛАЕВА Лада Андреевна	студент группы ИКПИ-292м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nicklada94@gmail.ru
НИКОЛАЕВА Оксана Андреевна	студент группы ЭП-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, oksanka.nikolaeva.1999@mail.ru
НИКОЛЬСКИЙ Эдуард Владимирович	студент группы БИМ-01з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, eduard-ipp@mail.ru
НИКОНОВА Елена Юрьевна	студент группы ИКТИ-25м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 214365444@mail.ru
НОВИКОВ Семен Сергеевич	студент группы ИКПИ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, semennovikov1@yandex.ru
ОНОФРИЙЧУК Екатерина Игоревна	студент группы ИСТ-131м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, konofriychuk7264@gmail.com

ОРЛОВ Михаил Алексеевич	студент группы ИКТК-96 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, miha5033@yandex.ru
ОСИПОВА Вероника Анатольевна	студент группы РТ-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, osipovaonline@mail.ru
ПАНЧЕНКО Анастасия Александровна	студент группы ИКВТ-291м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, panchenkoff@gmail.com
ПАПЫШКОВА Анна Вячеславовна	студент группы 7М38УТР-21/з Вологодского государственного университета, ann.pa1999@gmail.com
ПАРАМОНОВ Александр Иванович	доктор технических наук, доцент, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alex-in-spb@yandex.ru
ПАРШИН Евгений Александрович	студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, jpnvk@yandex.ru
ПАСКИДОВ Никита Владимирович	студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, paskidov.nv@spbgut.ru
ПАТРУХИНА Алиса Алексеевна	студент группы ИСТ-132м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, patruhina_alisa@mail.ru

- ПАЧИН Андрей Владимирович кандидат технических наук, преподаватель базовой кафедры «Программной инженерии и вычислительной техники» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pachin.andrej@bk.ru
- ПЕНЬКОВА Ю.Е. студент группы 2-ИАИТ-112М Самарского государственного технического университета, Penkovajuliasam@gmail.com
- ПЕРВУШИН Борис Евгеньевич студент группы V42041 национального исследовательского университета ИТМО, инженер лаборатории квантовых коммуникаций национального исследовательского университета ИТМО
- ПЕРЕДИСТОВ Евгений Юрьевич кандидат технических наук, доцент кафедры физики, заведующий кафедрой физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, peredistov.eu@net.sut.ru
- ПЕТРОВ Илья Валерьевич студент группы ИСТ-141м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, petrov9846@mail.ru
- ПЕТРОВ Павел Евгеньевич студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, petrulya_2000@mail.ru
- ПЕТРОВА Татьяна Васильевна студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tanya26012001@mail.com
- ПЕТУШКОВ Илья Олегович студент группы ИКТИ-25м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, computerilya@gmail.com

ПИЛИПОВА Валерия Михайловна	студент группы ИКТФ-16м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, valeriapilipova@gmail.com
ПНЕВСКИЙ Семен Борисович	студент группы ФП-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, spnevskiy@mail.ru
ПОДОПРИГОРА Андрей Николаевич	студент группы ИКТФ-16м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ПОЗДНЯКОВ Артём Андреевич	студент группы ИКФ-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artemka.pozdnyakov@gmail.com
ПОЛЕНОВА Дарья Алексеевна	студент группы РК-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, da.polenoval8@gmail.com
ПОМОГАЛОВА Альбина Владимировна	старший преподаватель кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.l.b.i.n.a@bk.ru
ПОПОВ Аликс Алексеевич	студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cloudyd3d@gmail.com
ПОПОНИН Антон Сергеевич	студент группы ИСТ-111м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ajhtcn9@gmail.com

ПОТОМАКО Денис Олегович	студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, den.potomako@mail.ru
ПРОСВЕТОВ Антон Юрьевич	студент группы ИКТМ-22м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, big_zebra@bk.ru
ПРИЛУЦКАЯ Ульяна Ивановна	студент группы РМ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Prilutskaia@yandex.ru
ПТИЦЫНА Лариса Константиновна	доктор технических наук, заведующий кафедрой информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ptitsina_lk@inbox.ru
ПУРТОВА Галина Михайловна	студент группы ЗР-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pur_ga89@mail.ru
ПУРШЕЛЬ Валерия Викторовна	студент группы РТ-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, valeriya-purshel@yandex.ru
ПУЧКОВ Владимир Викторович	ассистент кафедры защитных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, аспирант Санкт-Петербургского Федерального исследовательского центра Российской академии наук, puchkov-81@bk.ru
ПЧЕЛКИН Григорий Александрович	аспирант группы 1113А-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

РАЗУМОВ Дмитрий
Александрович

студент группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,
dimas245.razumov@yandex.ru

РАКОВСКИЙ Олег
Владимирович

кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

РЕЗНИКОВ Богдан
Константинович

преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rznkff@gmail.com

РЕКЕЛЬ Павел
Францевич

студент группы Р-12м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, инженер-проектировщик, ПАО "Гипросвязь" pavel.rekel.00@mail.ru

РОГОЗИНСКИЙ Глеб
Гендрихович

доктор технических наук, доцент кафедры информатики и компьютерного дизайна, начальник НОЦ "Медиацентр Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gleb.rogozinsky@gmail.com

РОДИНА Карина
Андреевна

студент группы РТ-22м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kovalyova-karina99@mail.ru

РОЖКОВ Глеб Вадимович

студент группы ИСТ-141м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gleb.2000-2001@yandex.ru

РОМАНЮК Дмитрий
Романович

аспирант группы 7762, национального исследовательского университета ИТМО, dimos1999@yandex.ru

РОЩИНСКИЙ Роман Сергеевич	студент группы Р-22м, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rosh.rs@bk.ru
РУЗМАНОВ Евгений Юрьевич	студент группы ИКТЗ-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ruzmanov1999@mail.ru
РЯБОВ Геннадий Анатольевич	старший преподаватель кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, grif999@mail.ru
РУСОВА Альбина Александровна	студент группы РСО-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Rusova.albina@mail.ru
РЮТИН Константин Евгеньевич	студент группы Р22-м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ryutin.sut@gmail.com
САДКОВА Алена Сергеевна	студент группы ИКТм-03 Поволжского государственного университета телекоммуникаций и информатики, alena-sadkova@mail.ru
САЛИТА Андрей Сергеевич	студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, salita@internet.ru
САМОХИНА Наталья Эдуардовна	студент группы ИКПИ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nataliezire@gmail.com

СВИНТУХОВСКИЙ
Павел Викторович

студент группы ИКФ-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, svintuhovskiy@gmail.com

СВИРИДОВ Игорь
Владимирович

студент группы БИМ-01з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivsconnected@gmail.com

СЕДЫШЕВ Эрнест
Юрьевич

кандидат технических наук, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, laboratoria-mw@yandex.ru

СЕРГЕЕВ Николай
Алексеевич

студент группы ИСТ-232м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, www_nick2690@mail.ru

СЕРЕГИН Андрей
Геннадьевич

студент группы ИКПИ-292м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.seregin.g@gmail.com

СИДОРЕНКО Виктор
Дмитриевич

студент группы ЗР21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vitononly1337@gmail.com

СИДОРКИНА Дарья
Сергеевна

студент группы Р-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, drsdrkn@gmail.com

СИДОРОВ Геннадий
Константинович

студент группы РК-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gennadiysidorov56@gmail.com

СКЛЯРОВ Александр Александрович	студент группы ИСТ-112м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zemmaran@mail.ru
СКОРОБОГАТОВА Светлана Алексеевна	студент группы ИКТГ-24м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, skorobogatova_sa@mail.ru
СКОРОХОДОВ Никита Евгеньевич	студент группы ФП-22м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, skor2000@bk.ru
СКОРЫХ Марк Андреевич	аспирант группы 1001А-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mark.skorykh@bk.ru
СКРЫЛЕВ Савелий Александрович	студент группы РМ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, saveliysk36@gmail.com
СМЕТЮХ Дмитрий Владимирович	студент группы ИСТ-131м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dimasmet@mail.ru
СМИРНОВА Алёна Алексеевна	студент группы ИКТГ-24м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alena_a.smirnova@mail.ru
СМОРОДИН Геннадий Николаевич	кандидат технических наук, доцент кафедры информационных управляющих систем, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
СОЛОВЬЕВ Артем Сергеевич	студент группы ИСМ-113 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.solovev.add@gmail.com

СОЛОВЬЕВ Денис Викторович	кандидат технических наук, доцент кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
СТЕПАНЕНКОВ Григорий Викторович	ассистент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 261199g@gmail.com
СТЕПАНОВ Александр Михайлович	студент группы ИКТИ-25м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2705201@bk.ru
СТОНОЖЕНКО Ксения Александровна	студент группы ЗР-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, stonojenko@bk.ru
СТРАШНОВ Антон Андреевич	студент группы РД-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, strahnov2001@mail.ru
СТУПНИКОВА Александра Алексеевна	студент группы МГИ-22 Сибирского Государственного Университета Телекоммуникаций и Информатики, sanya.sano1.1@gmail.com
СТУРМАН Владимир Ицхакович	доктор географических наук, профессор кафедры экологической безопасности телекоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, stv031055@mail.ru
СУДЬИНА Екатерина Владимировна	студент группы ЭП-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sudina_00@mail.ru

СУХОМЛИНОВ Даниил Игоревич	студент группы Р-12 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, d.sukhomlinov.spb@gmail.com
СУШКО Яков Геннадьевич	студент группы ИКМ-11з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yashasush@yandex.ru
СЫЧЁВА Екатерина Сергеевна	студент группы ЭБМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sychevastudent@mail.ru
ТАРОВ Евгений Викторович	студент группы ИКБ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tarov25@mail.ru
ТАТАРЕНКОВ Дмитрий Александрович	старший преподаватель кафедры телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, duferob@gmail.com
ТЕРНОВАЯ Анастасия Константиновна	студент группы Р-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ternovaya_00@bk.ru
ТИМОФЕЕВ Владислав Сергеевич	студент группы РТ-12м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bjjad228@gmail.com
ТИТОВ Павел Александрович	студент группы ИСТ-231м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, wowpointblog@gmail.com

ТКАЧУК Ангелина Васильевна	студент группы ИТКТ-96 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, angelina_tkachuk@bk.ru
ТИХОНОВ Алексей Максимович	студент группы ИКТГ-24м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexeyushaki@yandex.ru
ТОЛКАЧЕВ Александр Сергеевич	студент группы ИКПИ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexander050901@gmail.com
ТРИАНДАФИЛИДИ Иоанис Иванович	студент группы ИСТ-211м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mr.ioanis@gmail.com
ТРИЩЕНКО Александр Сергеевич	студент группы БИМ-01з Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича alex.trishchenko@mail.ru
ТУРАЕВ Содикджон Муродович	студент группы ИКТС-23м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, turaev_sodik@mail.ru
ТЯЖЕВ Даниил Вячеславович	студент группы Р-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, начальник инженерной службы АСБ, Государственная телевизионная и радиовещательная компания «Санкт-Петербург», dany61571@gmail.com
УЛЬЯНОВ Дмитрий Александрович	студент группы ИКТБ-17м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dimaulyanov99@gmail.com

- УРВАНЦЕВ Георгий
Александрович
студент группы ИСТ-232м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, minehaka@yandex.ru
- УШАКОВ Игорь
Александрович
кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakovia@gmail.com
- УШАКОВА Валерия
Андреевна
студент группы РМ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, veleryushakova@gmail.com
- УШКОВА Ирина
Геннадьевна
студент группы Р-22м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushkova.irina2015@yandex.ru
- ФЕДОРОВ Алексей
Алексеевич
студент группы ИКПИ-292м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lexa.f14@gmail.com
- ФЕДОРОВ Сергей
Леонидович
кандидат технических наук, доцент кафедры телевидения и метрологии, заведующий кафедрой телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sergf7@mail.ru
- ФЕДОРОВА Алина
Владимировна
кандидат экономических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, asp@spbgut.ru
- ФЕДОРОВА Злата
Анатольевна
студент группы ИКТ3-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zf_sweetday@mail.ru

- ФЕДОРОВА Ольга Вячеславовна студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, olgafedorova666@gmail.com
- ФЕДОТОВ Илья Олегович ведущий системный инженер ООО "Естественный интеллект"
- ФИЛИППОВ Артём Александрович студент группы ИКТЗ-11м Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artm.filippov98@mail.ru
- ФИЛИППОВ Феликс Васильевич кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
- ФОКИН Григорий Алексеевич доктор технических наук, заместитель декана по научной работе, профессор кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, harley_84@mail.ru
- ХАРЛАМОВ Максим Алексеевич студент группы ИКТИ-15м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hma99@mail.ru
- ХАСАНОВА Владлена Александровна студент группы ИКТИ-25м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kxasanovavlada@yandex.ru
- ХАЧАТРЯН Армине Арамовна студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, armine4.khachatryan@gmail.com

ХОРАХОРДИН Артем Иванович	студент группы ИКТК-96 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artemh7@mail.ru
ХОХЛОВА Анастасия Максимовна	студент группы ИКТК-96 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hohlova22@bk.ru
ХРАМЦОВ Дмитрий Олегович	студент группы ИКТЗ-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, khramtsov2010@mail.ru
ЦЫВАРЕВ Илья Васильевич	студент группы ИСТ-112м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cyvarev.ilya156@gmail.ru
ЦЫГАНОК Антон Эдуардович	студент группы ИКТО-08 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, antoni3105@yandex.ru
ЧАБАЕВА Елена Алексеевна	студент группы ЭБМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, лаборант испытательной аналитической лаборатории ООО "ГорМаш-Юл", gluscharik@gmail.com
ЧЕБОТАРЕВА Анастасия Владимировна	студент группы Р-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anastas1ache2403@gmail.com
ЧЕНАРАНИ Сасан	аспирант группы 6020501/20004 Санкт-Петербургского политехнического университета Петра Великого, sasanchenarani@gmail.com

ЧЕРВИНКО Евгений Игоревич	студент группы РТ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, proleaveprod@gmail.com
ЧЕРЕПАНОВ Денис Александрович	студент группы БИ-11м Санкт-Петербургского государственного университета телекоммуникаций им. Проф. М. А. Бонч-Бруевича, sveny@inbox.ru
ЧИЧКО Тимофей Андреевич	студент группы РМ-94 Санкт-Петербургского университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chichko-t@yandex.ru
ШАБЛОВСКИЙ Ярослав Константинович	студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, y.shablovskiy@gmail.com
ШАЙГАРАЕВА Татьяна Нажиповна	ассистент кафедры «Радиотехнические системы» Сибирского государственного университета телекоммуникаций и информатики, shaigaraeva@mail.ru
ШАЙХЛЕЕВА Назиля Ильгизаровна	студент группы РТ-12м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nazilyashaix@gmail.com
ШВЕЦ Максим Анатольевич	студент группы Р-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maximshvets2000@mail.ru
ШЕМЯКИН Сергей Николаевич	кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, s4421764@yandex.ru
ШЕРСТОБИТОВ Александр Андреевич	студент группы ФП-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shbeetov@yandex.ru

- ШИПИЦЫН Юрий Сергеевич студент группы ИКТГ-14м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ship.romeo@gmail.com
- ШИЯН Андрей Анатольевич кандидат педагогических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 1001digit@gmail.com
- ШОЙТОВ Иван Алексеевич студент группы РД-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shoitov@yandex.ru
- ШОРГИН Олег Олегович студент группы ИКФ-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kazbegmountain@gmail.com
- ШУТМАН Денис Валерьевич кандидат политических наук, доцент, декан факультета социальных цифровых технологий Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gf@spbgut.ru
- ЩЕГЛОВ Сергей Александрович студент группы ИКТГ-24м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shew341@gmail.com
- ЩЕРБАТЮК Анастасия Дмитриевна студент группы ИСТ-132м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, n.d.shcherbatyuk@mail.ru
- ЩЕТИНИНА Дарья Александровна студент группы РСО-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, darya.shchetinina@inbox.ru

- ЩУР Семён Юрьевич доцент Высшей школы дизайна и архитектуры Санкт-Петербургского политехнического университета Петра Великого, semmyon@yandex.ru
- ЭЛЕЖБИЕВ Алимхан Русланович студент группы ИКМ-11з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alikhanelezhbiev@mail.ru
- ЮРАКОВ Дмитрий Михайлович студент группы Р-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitry.yurackov@yandex.ru
- ЮРОВА Валентина Александровна кандидат физико-математических наук, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cathseugut@gmail.com
- ЮРЧЕНКО Павел Вячеславович студент группы ИСТ-922 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pactmon9@mail.ru
- ЯГУНОВ Павел Алексеевич студент группы ИСТ-112м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yagunovpavel@yandex.ru
- ЯДРЫШНИКОВ Владислав Александрович студент группы РСО-11м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yadryshnikov_vlad@mail.ru
- ЯКОВЛЕВ Николай Викторович студент группы ИКФТ-16м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yakovlev.nv_spbopen@mail.ru

ЯКУПОВ Денис Олегович ассистент кафедры программной инженерии
Поволжского Государственного Университета
Телекоммуникаций и Информатики,
d.yakupov@psuti.ru

ЯССЕР Марк студент группы ИКБ-91 Санкт-
Владимирович Петербургского государственного
университета телекоммуникаций им. проф. М.
А. Бонч-Бруевича, yasser.mark@yandex.ru

ЯШИН Алексей студент группы ИСМ-113 Санкт-
Владимирович Петербургского государственного
университета телекоммуникаций им. проф. М.
А. Бонч-Бруевича, alexey.morris@gmail.com

Анонс публикации

В настоящем сборнике материалов Всероссийской научно-технической и научно-методической конференции магистрантов и их руководителей «Подготовка профессиональных кадров в магистратуре для цифровой экономики» (ПКМ-2022) размещены доклады, представленные на конференции 2022 года, за исключением докладов, признанных лучшими по итогам работы секций научных направлений конференции и опубликованных в отдельном сборнике.

*Сборник лучших докладов конференции ПКМ-2022 публикуется в электронном виде на сайте конференции **pkm.sut.ru** и будет дополнительно издан в бумажном виде в I квартале 2023 года.*



всероссийская научно-методическая
конференция магистрантов и их руководителей

ПКМ

**ПОДГОТОВКА ПРОФЕССИОНАЛЬНЫХ КАДРОВ
В МАГИСТРАТУРЕ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ**