СПб ГУТ)))

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

ПКМ

ПОДГОТОВКА ПРОФЕССИОНАЛЬНЫХ КАДРОВ В МАГИСТРАТУРЕ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ

МАТЕРИАЛЫ КОНФЕРЕНЦИИ ПКМ-2023

Том 1

СПб ГУТ)))

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

ПОДГОТОВКА ПРОФЕССИОНАЛЬНЫХ КАДРОВ В МАГИСТРАТУРЕ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ (ПКМ-2023)

ПКМ

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Том 1

5 декабря – 7 декабря 2023 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-2023). Всероссийская научно-техническая и научно-методическая конференция магистрантов и их руководителей; материалы конф.: в 2 т. Т. 1. / Сост. Н.Н. Иванов. СПбГУТ. – СПб., 2024. – 937 с.

ПРОГРАММНЫЙ КОМИТЕТ
Председатель
Киричек Р.В. - доктор технических наук, доцент, ректор СПбГУТ
Заместители председателя
Абилов А.В. - кандидат технических наук, доцент, первый проректор – проректор по учебной работе СПбГУТ
Брусиловский С.А. - кандидат технических наук, 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
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

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ
Сопредседатели
Ивасишин С.И. – кандидат технических наук, директор департамента организации и качества образовательной деятельности СПбГУТ
Альховик А.В. – директор департамента по эксплуатации и развитию материально-технического комплекса.
Ответственный секретарь
Родакова А.О. – начальник учебного отдела института магистратуры
Члены организационного комитета
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
Нестеров А.А. – кандидат технических наук, доцент, начальник управления организации научной работы и подготовки научных кадров
Эмексузян А.Р. – директор департамента экономики и финансов СПбГУТ

В материалах конференции размещены доклады, представленные на научно-методической конференции 2023 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
А. Н. Данилова, Д. А. Рожкова
Дизайн логотипа Г. И. Юрьев
Подписано к изданию 11.06.2024г.
117,13 усл.печ.л. Заказ 1598

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

СПбГУТ, 2024

ISBN 978-5-89160-332-5 (Т. 1)
ISBN 978-5-89160-331-8

СОДЕРЖАНИЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАДИОЭЛЕКТРОНИКИ 13

1.1. Микроволновая техника: материалы, компоненты, устройства 13

Верликов Н.В., Седышев Э.Ю. (СПбГУТ) Выбор активного элемента для генератора шума СВЧ диапазона 14
Воропаев П.В., Седышев Э.Ю. (СПбГУТ) Антенный терминал для систем спутниковой связи 17
Гуляев Р.С., Седышев Э.Ю. (СПбГУТ) Управляемый аттенюатор Ku диапазона..... 21
Книгиницкий Е.И. (СПбГУТ) Разработка волноводного генератора в объемном интегральном исполнении 25
Коробейников А.Н., Никитин Ю.А. (СПбГУТ) Проектирование СВЧ тракта для детектирования и подготовки СВЧ сигналов к последующей обработке 29
Седышев Э.Ю., Смирнова Д.А. (СПбГУТ) Инженерный метод синтеза устройств частотной селекции масштабированием 33

1.2. Промышленная электроника 38

Ерчуков И.И. (СПбГУТ) Разработка и исследование Н-моста для реверсивного управления двигателем постоянного тока 39

РАДИОТЕХНОЛОГИИ СВЯЗИ 43

2.1. Медиатехнологии и телерадиовещание 43

Вербицкий А.А., Вербицкий А.В. (СПбГУТ) Исследование работы сплайсеров различных производителей в одночастотной сети стандарта DVB-T2 в г. Санкт-Петербург 44
Воронин Н.С., Татаренков Д.А. (СПбГУТ) Облако точек и методы его получения 51
Жиряков В.П., Федоров С.Л. (СПбГУТ) Акустическая подготовка современных студий звукозаписи 55
Клыков Д.Д., Попков С.В. (СПбГУТ) Использование генеративно-состязательных нейросетей в процессе создания динамического медиаконтента 60
Куликов С.П., Поляков А.И. (СПБГУТ) Разработка системы IPTV..... 64
Мамонов М.А. (СПбГУТ) Анализ возможностей камер Sony и Canon для осуществления цветокоррекции изображений 68
Минаев Н.В. (СПбГУТ) Технологии построения иммерсивного пространства 74
Попов А.А. (СПбГУТ) Система мониторинга и контроля одночастотной сети ЦЭТВ 79

2.2. Подвижная связь и радиодоступ 84

Арефьев А.С. (СПбГУТ) Анализ городских связей и покрытия с использованием трассировки лучей 85
Воробьев О.В., Дубаков А.В. (СПбГУТ) Обзор применения интернета вещей (IoT) в системе "умное поле" 89
Воробьев О.В., Рябиков Д.С. (СПбГУТ) Беспроводная связь 6G: перспективы и потенциальные технологии 93
Гайлит Д.Д., Чернышов А.Г. (СПбГУТ) Алгоритм многопараметрической адаптации декаметровой радиолинии специального назначения 98
Добрая О.П. (СПБГУТ) Требования к СШП радиолинии управления БЛА ближнего действия 103
Дюдин А.И. (СПбГУТ) Спутниковые орбиты в сетях 5G NTN 107
Занозин Е.В. (СПбГУТ) Оценка помех в сверхплотной сети 5G с использованием цифровых моделей местности в MATLAB 111
Кравец Е.В., Чернышова А.В. (СПбГУТ) Методы борьбы с коллизиями в системе радиочастотной идентификации 116
Маковчик Д.В. (СПбГУТ) Развитие технологии 5G и 6G 119
Максимов А.М. (СПбГУТ) Проектирования архитектуры 6G 122
Подлевских А.П. (СПбГУТ) Моделирование спутникового канала связи в среде MATLAB SIMULINK 127
Попович С.И., Чернышов А.Г. (СПбГУТ) Организация системы связи для беспилотных летательных аппаратов на основе LoRa с целью передачи данных управления на большие расстояния 132
Романова Е.А. (СПбГУТ) Анализ ограничений передачи видеоинформации для связи с наземными роботехническими комплексами 137
Рютин К.Е., Фокин Г.А. (СПбГУТ) Оценка влияния погрешности синхронизации базовых станций на точность определения местоположения пользовательских устройств 141
Смирнов Д.П. (СПБГУТ) Исследование возможностей построения перестраиваемого фильтра диапазона частот от 30 до 80 МГц 146
Стрельников В.М. (СПбГУТ) Оптимизация надежности при проектировании и внедрении систем 6G «автомобильных-инфраструктур» для управления чрезвычайными ситуациями в среде «умного города» 151
Ушкова И.Г., Фокин Г.А. (СПбГУТ) Моделирование отслеживания gps-приемника с помощью с/а-кода 153
Хименкова Д.А., Чернов И.Н. (СПбГУТ) Программно аппаратные средства повышения точности беспилотной картографии 159
Шеремет Н.В. (СПбГУТ) Использование алгоритмов адаптивного диаграммообразования в сетях 5G 164
Яндиев А.А. (СПбГУТ) Моделирование сети IIoT в пакете WOKWI 169

2.3. Проектирование и технология радиоэлектронных средств 173

Дунаев Н.П., Макаров В.А. (СПбГУТ) Применение синхронного интерфейса при быстром прототипировании фазированных антенных решеток 174
Дунаев Н.П., Макаров В.А. (СПбГУТ) Радиометр на основе спутникового конвертора и SDR-RTL приемника 178
Зарубин И.М. (СПбГУТ) Исследование современных возможностей применения аддитивных технологий в производстве радиоэлектроники 182

Кирик Д.И., Михайлова З.В. (СПбГУТ) Обзор САПР Cadence Allegro и анализ отечественных аналогов 187
Пугач М.С. (СПбГУТ) Беспроводная система противопожарной сигнализации с использованием технологии ZigBee 192
Старицын Н.Е. (СПбГУТ) Исследование современных методов изготовления зеркальных антенн с применением аддитивных технологий 197
Тарасов В.В. (СПБГУТ) Исследование системы “Умный дом”, построенной на основе гибридных технологий передачи данных 200

2.4. Радиотехнические системы и антенны 204

Агаян Д.А., Чернов И.Н. (СПбГУТ) Разработка алгоритма адаптации статистического набора данных для нейронной сети, анализирующей внештатные ситуации на промышленных объектах 205
Баранов М.А., Коровин К.О. (СПбГУТ) Анализ характеристик передающих антенн ОНЧ диапазона 209
Васильев А.Г., Чернов И.Н. (СПбГУТ) Разработка аппаратной платформы для обработки видеоизображения с использованием искусственного интеллекта 213
Лавров М.Н. (СПбГУТ) Алгоритм управления амплитудно-фазовым распределением тока в антенных элементах передающей фазированной антенной решетки 219
Ликонцев А.Н., Нев Д.А. (СПбГУТ) Применение алгоритмов формирования луча для адаптации диаграммообразования в спутниковых кооперативных системах 223
Максимова А.В., Чернов И.Н. (СПбГУТ) Разработка универсального модуля гамма-коррекции на ПЛИС 228
Оноприенко В.В., Чернов И.Н. (СПбГУТ) Разработка универсального модуля обработки видеопотока на ПЛИС 233
Чернов И.Н., Швецов Ф.П. (СПбГУТ) Разработка универсального генератора тестовых изображений на ПЛИС 238

2.6. Экология формирования информационного пространства 243

Белоцерковский М.В. (СПбГУТ) Измерение электромагнитных полей промышленной частоты в городе Ржев Тверской области 244
Бобер А.Д. (СПбГУТ) Экотоксикологическое состояние поверхностных вод реки Черная и Карповка 247
Бобер А.Д. (СПбГУТ) Исследование деградации нефтепродуктов в почвенном профиле на примере подзолистых и дерново-подзолистых почвах Ленинградской области 250
Борисова А.А., Казанцева А.Г. (СПбГУТ) Исследование зависимости величины выброса оксидов азота от калорийности топлива 254
Виноградова Н.А. (СПбГУТ) Условия и результаты эксперимента по биодеградации полимерных отходов в естественных условиях 258
Губашева А.А. (СПбГУТ) Анализ шумового загрязнения территории муниципального округа гагаринское московского района Санкт-Петербурга с применением ГИС-технологий 264
Загребаева Н.М. (СПбГУТ) Определение основ нормирования выбросов в цементной промышленности при использовании альтернативных видов топлива 269
Казанцева А.Г., Цветкова И.Ю. (СПбГУТ) Исследование влияния температуры на величину выброса 274
Казанцева А.Г., Чурынина М.В. (СПбГУТ) Исследование метода оценки вредности природной пыли сложного компонентного состава 279

Коноплёва А.В. (СПбГУТ) Определение токсичности почв в парке Александрино методом биотестирования 284
Кочерёжкина У.А. (СПбГУТ) Раковые озера Выборгского района Ленинградской области в исторической перспективе сегодня и завтра 289
Логиновская А.Н., Стурман В.И. (СПбГУТ) Сравнение измерительных возможностей приборов и новые результаты исследования проблем электромагнитного загрязнения 293
Макина М.А. (СПбГУТ) Геоинформационное картографирование электромагнитных полей острова декабристов Санкт-Петербурга 296
Назаров И.В. (СПБГУТ) Исследование шумового загрязнения городской среды и рекомендации по его снижению на примере Васильевского острова 301
Петров М.А. (СПбГУТ) Влияние полимерных отходов на биологическую активность почв 305
Тукмачева М.А., Шестаков А.В. (СПб УГПС МЧС России) Ноксологический подход моделирования рисков киберугроз в пожарной надзорной деятельности опасных производственных объектов 310
Упоров М.Е. (СПбГУТ) Геоинформационное картографирование электромагнитных полей Адмиралтейского муниципального округа Санкт-Петербурга 314
Флейшман А.А. (СПбГУТ) Проект экологической тропы на территории государственного природного заказника регионального значения «Шунгеровский» 319

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ 325

3.1. Безопасность компьютерных систем и сетей связи 325

Александрова А.Г. (СПбГУТ) Определение ТОП-10 актуальных угроз безопасности информации для информационных систем, функционирующих в сфере топливно-энергетического комплекса 326
Алексейчук П.Д. (СПбГУТ) Модель процесса разработки безопасного программного обеспечения для критических информационных инфраструктур 331
Алькаттан С., Петрив Р.Б. (СПбГУТ) Study and analysis of the Automated Adversary Emulation Platform MITRE CALDERA 336
Аль-Нами Б.А., Коваленко Д.Д., Шиян П.А. (СПбГУТ) Развитие тенденций в области нейросетей 341
Ахрамеева К.А., Жиляков Г.В. (СПбГУТ) Исследование возможности вложения информации в изображения при помощи GAN-СИСТЕМ 344
Батин Е.А., Поляничева А.В. (СПбГУТ) Анализ угроз безопасности изолированного сегмента сети 348
Бенч М.Н. (СПбГУТ) Разработка системы определения оптимальных средств защиты персональных данных на основе анализа их защищенности 351
Богомаз М.Э. (СПбГУТ) Система PKI на основе блокчейна с использованием смарт-контрактов 355
Бударин М.Э. (СПбГУТ) Беспроводные прокси станции как угроза корпоративной WLAN 360
Бусыгин К.Н., Малания М.Т. (СПБГУПТД) Представление способов реактивного программирования 368
Васьков А.А. (СПбГУПТД) Анализ моделей угроз информационной безопасности беспроводных сетей 370
Винников С.А., Трезоров В.И. (СПбГУТ) Разработка портативного детектора сетевых атак 375

Висал Инг, Штеренберг С.И. (СПБГУПТД) Обеспечение безопасности цифрового мира: комплексное руководство по информационной безопасности 379
Виткова Л.А., Зрелова А.Л. (СПбГУТ) К вопросу о защите персональных данных от утечки компрометации 385
Виткова Л.А., Крестьяшин Н.А., Пучков В.В. (СПбГУТ) Исследование функциональных возможностей системы мониторинга событий информационной безопасности 388
Воробьев А.В. (СПбГУПТД) Информационная безопасность в области медицинских устройств и электронного здравоохранения 392
Воронцов А.А., Шемякин С.Н. (СПбГУТ) Основные виды атак на систему квантовой криптографии 395
Грохольский А.В. (СПбГУТ) Исследование путей оценки производительности веб-серверов 400
Груздев А.С. (СПбГУТ) Проблема выявления нежелательной нформации в социальных сетях 403
Гудочкина А.Р. (СПбГУПТД) Влияние социальных сетей на информационную безопасность 407
Гусенов С.Ю. (СПбГУПТД) Принципы разработки экспертной системы для поиска проблем в телекоммуникационной инфраструктуре предприятия 410
Дмитриев С.С., Шестакова В.А. (СПбГУПТД) Анализ эффективности этичного хакинга в защите информационной безопасности 415
Дмитриева И.Н. (СПбГУТ) Контроль внешней поверхности атаки: обеспечение защиты конфиденциальной информации в организации 419
Догадаев А.С. (СПбГУТ) Выбор регулятора для безопасного управления конвейером 424
Домбровский Р.М., Филипов Э.О. (СПбГУТ) Перспективы внедрения кибериммунного подхода для защиты операционных систем 429
Дрепа В.Е. (СПбГУТ) Методика выбора допустимых значений RSSI для системы определения местоположения Wi-Fi клиента методом fingerprinting 434
Дюсметова А.А. (СПбГУТ) Компьютерная атака dns amplification: механизмы, инструменты и защита от угрозы 439
Дятченко А.А. (СПбГУТ) Методика аудита процесса «Обеспечение защиты информации при управлении доступом» 444
Егорова П.Ю., Охлопкова Ю.В., Шиян А.А. (СПбГУТ) Особенности применения искусственного интеллекта в кибербезопасности 448
Емельяненко Г.Ю. (СПбГУТ) Обеспечение СОВ ПНП для проведения мониторинга РИС 453
Ермачкова М.В. (СПбГУПТД) Анализ эффективности интеллектуальных систем в задачах информационной безопасности 458
Зебзеев Е.А. (СПбГУТ) Исследование механизмов обеспечения информационной безопасности сети на базе WPA3 ENTERPRISE 462
Иванилова Ю.А., Ушаков И.А. (СПбГУТ) Исследование основных функций построения MAXPATROL SIEM 467
Игнатьева Д.А., Камалова А.О., Пестов И.Е., Романюк Е.О. (СПбГУТ) Разработка виртуального стенда для анализа метрик безопасности виртуальных машин и контейнеров 472
Ильин Я.А. (СПбГУТ) Перспективы развития устройств на базе технологии NFC 476
Казанцев А.А., Махорин А.С. (СПбГУТ) Угрозы сетевой безопасности в сфере высшего образования 480

Караханова Е.К., Светова А.В. (СПбГУТ) Проблемы обеспечения информационной безопасности облачных вычислений 486
Кирилова Д.С. (СПбГУТ) Выявление уязвимостей электронный подписей в системах электронного документооборота и методы обеспечения криптографической защиты документов 490
Ковалева А.А., Курманов И.О. (СПбГУТ) Исследование и реализация метода шифрования данных по ГОСТ для ОС ASTRA LINUX 494
Коломийцев Р.К. (СПбГУТ) Усовершенствованный вариант корпоративного honeypot-решения для обеспечения безопасности корпоративной сети 499
Коньков В.В. (СПБГУТ) Внедрение цифрового водяного знака в модуль, отвечающий за корпоративную безопасность операционной системы LINUX, с целью проверки целостности операционной системы в процессе ее работы 503
Коршунов И.Д. (СПбГУПТД) Исследование технологий IOT в сельском хозяйстве 507
Кравцова В.А., Сухомлинов Д.И. (СПбГУТ) Исследование принципов аутентификации посредством openldap в операционных системах LINUX 510
Кравцова В.А., Сухомлинов Д.И. (СПбГУТ) Эффективность использования DKIM, DMARK, SPF в доменах электронной почты 514
Красов А.В., Масютин М.Д., Черник Я.В. (СПбГУТ) Разработка концепции мессенджера на основе использования методов стеганографии 517
Кузьмина О.И. (СПбГУТ) Разработка концепции решения для разграничения прав доступа пользователей WLAN на основе LBS 521
Курманов И.О., Лешукова А.М., Петрова Т.С. (СПбГУТ) Нейросети для анализа тональности текста 525
Курманов И.О., Синельщиков В.С. (СПбГУТ) Инновационные подходы к обеспечению кибербезопасности в корпоративных сетях: роль оборудования S-TERRA CSP и шифрования ГОСТ 531
Кутуев Т.Т. (СПбГУТ) Концепт кибериммунных операционных систем на примере KASPERSKY OS 537
Лободина Е.А., Наумова Т.Д., Шестаков С.М. (СПбГУПТД) Оценка угроз безопасности, связанных с применением дипфейков 541
Любащенко Т.Д. (СПбГУТ) Применение технологии LORA для создания защищённых радиомаяков БПЛА 544
Макарова А.К., Поляничева А.В. (СПбГУТ) Обзор возможностей машинного обучения для обеспечения безопасности VoIP 548
Марочкин Д.А., Павленко А.С. (СПбГУПТД) Сравнение брокеров сообщений 553
Мартыненко Д.Р., Шиян А.А. (СПбГУТ) Уязвимости, возникающие при переносе кода с 32-битной на 64-битную платформу и их устранение 560
Муравьев М.И. (СПбГУПТД) Исследование систем искусственного интеллекта для обнаружения вторжений в распределённых информационных системах 564
Нечаев А.А. (СПбГУТ) Приемущества системы управления идентификацией на основе блокчейна 568
Никонов Е.Р. (СПбГУТ) Обеспечение безопасности систем при использовании блокчейн узлов на примере системы голосования 573
Новиков Д.С. (СПбГУТ) Подходы к тестированию безопасности веб-приложений 578
Овсянников Е.Б. (СПбГУПТД) Методики обфускаций и деобфускаций JAVA кода 581
Олейник А.А. (СПБГУТ) Исследование и разработка методов стегоанализа для лингвистических стегосистем 586
Павловская А.А., Павловский М.В. (СПбГУТ) Разработка алгоритма анализа образования высших учебных заведений по северо-западному округу по направлениям обучения 10.00.00 588
Панков А.В., Ушаков И.А. (СПбГУТ) Алгоритм настройки DMVPN на устройствах российского вендора 593

Панфилов А.А. (СПбГУПТД) Анализ эффективных сред Больших Данных в сфере облачных технологий и машинного обучения 598
Перминова Я.А. (СПбГУТ) Преимущества хостовых IDS в обнаружении ботнет-сетей 603
Петрив Р.Б., Чизиба Э. (СПбГУТ) Research on web-application security testing using metasploit framework 608
Петров П.Е. (СПбГУТ) Синтез метода выявления фишинговых сайтов 611
Потомако Д.О. (СПбГУТ) Анализ специфичных для АСУ ТП тактик и техник, используемых для реализации угроз безопасности информации 615
Проничев В.Д., Ушаков И.А. (СПбГУТ) Разработка модели инсайдера и алгоритмов их обнаружения в компьютерных сетях с использованием технологии искусственного интеллекта 621
Романюк Е.О. (СПбГУТ) Анализ воздействия различных методов шифрования на пропускную способность сетевого трафика в облачной инфраструктуре 625
Руденко С.А. (СПбГУТ) Будущее кибербезопасности с использованием нейронных сетей 630
Самохин Г.А. (СПбГУПТД) Анализ методов аутентификации в информационной безопасности 634
Саразова И.А., Чахир А.А. (СПбГУПТД) Методики обнаружения уязвимостей в сетях умного дома 638
Севостьянов В.А. (СПбГУТ) Модель ассоциативной памяти в среде обработке больших данных 642
Скородумов Н.В. (СПбГУПТД) Анализ инновационных IT-технологий в образовании. 647
Спиридонов Д.П., Федорченко Е.В. (СПбГУТ) Сравнительный анализ и применение матриц атак Microsoft Kubernetes Threat Matrix и Mitre Att&ck Matrix 650
Степанов М.П. (СПбГУТ) Сравнительный анализ основных типов кибератак на веб-приложения и способы борьбы с ними 653
Стукалов А.Н. (СПбГУПТД) Применение технологии Блокчейн в различных отраслях 658
Талакин Е.Н. (СПбГУТ) Пакетные нейросетевые программы в распределённых информационных системах 661
Таратынов И.Д. (СПбГУТ) Сравнительный анализ решений для генерации компьютерных атак с заданными характеристиками 665
Тур В.С. (СПбГУПТД) Анализ эффективности алгоритмов глубокого обучения на примере задачи распознавания речи 670
Урсегов А.К. (СПбГУТ) Масштабируемое honeypot-решение для анализа и учета статистики сетевых атак 675
Федорова З.А. (СПбГУТ) Современная SIEM-система: что важно для эффективного выявления инцидентов 680
Фомичев В.А. (СПбГУПТД) Исследование уязвимостей в операционной системы Android 686
Хамед Мохамед (СПбГУПТД) Обеспечение безопасности цифрового мира: комплексное руководство по информационной безопасности 688
Хачатрян А.А. (СПбГУТ) Методика определения вероятности реализации киберугроз с использованием honeypot 694
Шагисултанов Т.А. (СПбГУТ) Современные угрозы и перспективы развития тестов Тьюринга в области веб-приложений 699
Шайер А.В. (СПбГУПТД) Уязвимости системы NFC: риски и методы защитыУязвимости системы NFC: риски и методы защиты 703
Штеренберг О.М. (СПбГУТ) Методика защиты организации от атак с использованием социальной инженерии механизмами автоматизированных программ ... 707

Шуваев Д.В. (СПбГУПТД) Системы резервного копирования данных 712
Юрова У.С. (СПбГУТ) Защита периметра сети с использованием open source-инструментов. Регулярный пентест 715
Якубович С.А. (СПбГУТ) Социальная инженерия: психологические аспекты кибератак и методы защиты 721
Якубовский И.А. (СПбГУПТД) Социальная инженерия: психологические аспекты кибератак и методы защиты 726
Яссер М.В. (СПБГУТ) Автоматизация проверки выполнения лабораторных работ на базе беспроводного отечественного оборудования Eltex 729

3.2. Интернет вещей и гетерогенные сети 735

Белая Т.И., Воробьева В.В. (СПбГУТ) Особенности тестирования Интернета вещей ... 736
Владимиров С.С., Волков В.Д., Скакунов И.Р., Шалагинов М.Н. (СПбГУТ) Применение сигнально-кодовых конструкций на основе элементов троичного поля Галуа и кодов Рида-Соломона для сетевого кодирования 740
Козлова А.А., Минеева В.Д. (СПбГУТ) Технологии кроссчейн систем в DeFi: исследование и моделирование 745
Лохов Д.А. (СПбГУТ) MANET-сеть и ее протоколы. Двухранговая MANET-сеть 750
Матукас М.Р., Парамонов А.И. (СПбГУТ) Кластеризация как метод уменьшения помех в сетях высокой плотности 755
Никифоров С.С. (СПбГУТ) Конвергенция технологий 5G и WI-FI 6 759
Парамонов А.И., Тихонов А.М (СПБГУТ) Задачи анализа трафика и качества обслуживания в самоорганизующихся сетях с подвижными пользователями 763
Смирнова А.А. (СПбГУТ) Предсказание доли повторных передач при использовании кодирования LDPC в сетях Wi-Fi 767
Степанов А.М. (СПбГУТ) Исследование методов уменьшения задержек для URLLC в СЕТЯХ 5G 773
Щеглов С.А. (СПбГУТ) Исследование технологии STBC на рынке клиентских устройств Wi-Fi 778

3.3. Мультисервисные телекоммуникационные системы и технологии 783

Бойко А.А., Кисляков С.В., Османов Д.М. (СПбГУТ) Анализ модели управления услугами 5G, предлагаемой в открытой цифровой архитектуре от TM FORUM 784
Воинков Е.Б., Елагин В.С. (СПбГУТ) Возможности применения нейронных сетей в сетях связи 789
Елагин В.С., Мельниченко А.А., Швидкий А.А. (СПбГУТ) Анализ возможностей использования методов отслеживания сетевых пакетов для повышения производительности сетей передачи данных 793
Елагин В.С., Щегольский Ю.Е. (СПбГУТ) Перспективные аспекты применения нейронных сетей в системах видеоконференцсвязи 798
Камуежи Й.Г., Кисляков С.В (СПбГУТ) Анализ применения инструментов DEVOPS при развёртывании систем автоатизации, разработанных на основе ODA-компонентов 803
Митин Е.О. (СПбГУТ) Обзор системы слайсинга сети с помощью IBN для сетей 5G 807
Шестакова В.А. (СПбГУТ) Анализ применимости методов автоматизированного развёртывания облачной инфраструктуры для рабочих мест пользователей 812

3.4. Оптоэлектронные технологии (фотоника) в инфокоммуникациях 816

Беляев А.А., Слепогин А.Ю. (СПбГУТ) Исследование различных форматов модуляции для увеличения радиуса сетей 817
Бовбель Я.А., Дубовиков Л.О., Юклутов Д.А. (СПбГУТ) Классификация подводных линий связи 822
Бутиков З.Э., Каадзе Н.Т., Славуцкий Д.С. (СПбГУТ) Влияние дизайна сети на ее стоимость..... 828
Былина М.С., Гоменица В.А. (СПбГУТ) Моделирование и исследование интегрально-оптического направленного ответвителя..... 832
Воробьев Я.В., Маринова В.К., Панкова Е.А. (СПбГУТ) Исследование оптического усилителя EDFA 836
Делла-Корте Ф.В.С., Чесноков К.Э., Шенхорова Д.Н. (СПбГУТ) Оценка качества связи в оптическом тракте ВОСС по результатам измерения отношения сигнала к шуму 841
Лоншаков М.А., Резников Б.К., Чемодуров Д.Д., Шиян А.А. (СПбГУТ) Перспективы модернизации городских систем связи и передачи данных в условиях мегаполиса..... 845
Пылаев В.К., Самарин В.В., Чернов М.Д. (СПбГУТ) Исследование мультиплексора AWG для систем DWDM..... 849
Шишкина В.Ю. (СПБГУТ) Исследование методов оценки качества связи в волоконно-оптических системах..... 854

3.5. Программная инженерия 859

Ежуров А.П. (СПбГУТ) Сравнение оптимизаторов в задаче классификации изображений MNIST на примере трех нейронных сетей 860
Конак В.Е. (СПбГУПТД) Значимость математических методов в системах машинного обучения и анализа данных 865
Правдин А.А., Родионов А.Л., Соловьев А.С. (СПБГУТ) Разработка приложения для формирования обучающих наборов данных с помощью сервисов вертикальных коротких видеороликов..... 868

Сведения об авторах 871

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 621.373.52
ГРНТИ 47.45.99

ВЫБОР АКТИВНОГО ЭЛЕМЕНТА ДЛЯ ГЕНЕРАТОРА ШУМА СВЧ ДИАПАЗОНА

Н. В. Верликов, Э. Ю. Седышев
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе рассматривается возможность создания широкополосного шумового генератора посредством схемы Пирса на лавинно-пролетном диоде в режиме пробоя. Предложена эквивалентная схема кварцевого генератора с низкой добротностью для расширения полосы частот.

ЛПД, генераторы, СВЧ

На сегодняшний день электроника развивается в диапазоне СВЧ, захватывая с каждым годом всё более высокие частоты. Высокая частота сигнала не только означает большее количество передаваемых данных, но она влияет и на скорость их передачи. Тенденция к миниатюризации также является одной из причин развития СВЧ электроники. Работа в СВЧ диапазоне наблюдается во всех отраслях радиоэлектроники. Примером могут служить новые 5G и 6G системы, сотовая и спутниковая связь.

Перспективным решением дальнейшего развития микроволновой электроники считается СВЧ шум. Если решить проблему с генерацией и эффективной передачей шума СВЧ диапазона в широкой полосе частот, то можно развивать область шумовой радиолокации, телекоммуникации и спутниковую связь.

Дадим определение шума. Шум – это электрический фон, который существует одновременно во всём диапазоне частот, при этом его спектральная плотность примерно одинакова.

В качестве генераторов шума могут использоваться диоды в режиме лавинного пробоя и усилители, охваченные широкополосной положительной обратной связью (ПОС). В этом режиме коэффициент усиления устремляется к бесконечности, что приводит к превращению усилительной структуры в генерационную [1]. В качестве диода можно взять диод Зенера, который работает за счёт обратимого лавинного пробоя p-n перехода. Когда обратное напряжение на стабилитроне выше рассчитанного напряжения стабилизации, то его лавинообразно пробивает. Интенсивный шум при таком режиме возможно наблюдать в начале лавинного пробоя и при определённых значениях тока. В цепи ПОС могут использоваться резонаторы, представляющие собой различные объемные и планарные структуры. Одними из простейших видов резонаторов являются разомкнутые микрополосковые линии, от геометрии которых будут зависеть выходные характеристики устройства.

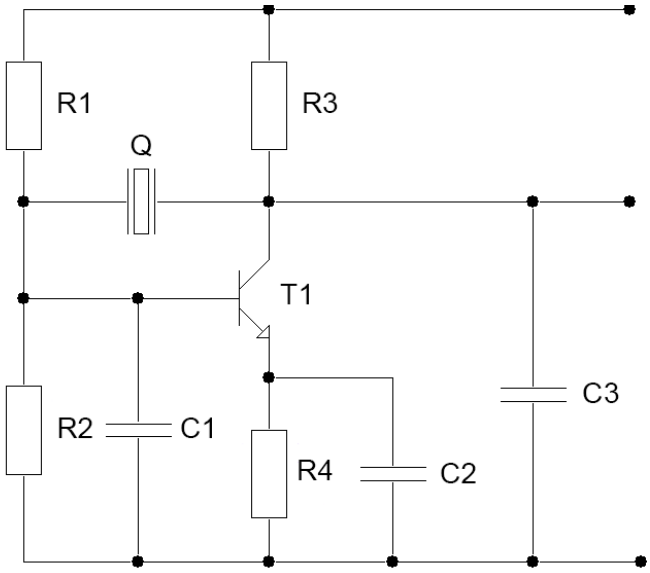


Рис. 1. Схема генератора Пирса

Можно рассмотреть схему генератора Пирса (рис. 1), ключевым элементом которой является кварцевый резонатор. Это высокоизбирательный элемент с довольно высокой добротностью, поэтому частотная характеристика подобной схемы представляет из себя высокий резонанс на основной гармонике кварца. У кварцевого резонатора есть эквивалентная схема (рис. 2), которая состоит из параллельно соединенного последовательного резонансного контура и конденсатора, который характеризует статическую емкость кварца. Этот элемент можно заменить на резонатор с низкой добротностью для расширения полосы генерации шума. Это произойдет, если параллельно эквивалентной схеме кварцевого резонатора подключить резистор. В качестве активного элемента в генераторе Пирса оптимально использовать лавинно-пролетные диоды (ЛПД) и мощные биполярные транзисторы.

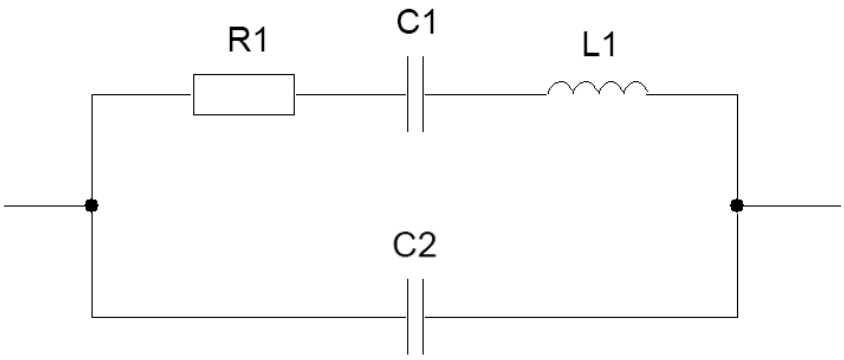


Рис. 2 Эквивалентная схема кварцевого резонатора

ЛПД отличаются от других подобных полупроводников тем, что они имеют отрицательное сопротивление, работают на больших мощностях и на СВЧ. Чаще всего их основным недостатком считают наличие высокого уровня фазового шума, но для нашей цели шум является самим сигналом, а потому этот диод можно использовать вместо транзистора в схеме Пирса.

Так, используя схему Пирса с изменённой эквивалентной схемой кварцевого резонатора и шумовой сигнал с ЛПД, можно создать широкополосный высокочастотный шумовой сигнал.

Помимо генерации шума его нужно определённым образом передавать. В качестве передающей структуры была предложена многозаходная спиральная антенна, представляющая из себя диэлектрическое основание, прикреплённое к металлическому экрану, с навитыми на неё заходами токопроводящей спирали [2]. К экрану, в свою очередь, присоединены коаксиальные линии. Их центральные проводники соединены с концами заходов спиралей, а внешние – с экраном. Подобная структура обеспечивает широкополосность, что как раз является одним из ключевых моментов для передачи шумового сигнала.

Таким образом, шум, чаще всего рассматриваемый как паразитное явление, можно использовать как полезный широкодиапазонный по частоте сигнал для хранения, передачи и защиты данных. В данной работе был рассмотрен способ генерации СВЧ шума, а также его передачи.

Список используемых источников:

1. Ларионова А. К., Седышев Э. Ю. Генератор шума СВЧ на полупроводниковом диоде в интегральном исполнении // Подготовка профессиональных кадров в магистратуре для цифровой экономики : материалы Всерос. науч.-технич. и науч.-методич. конф. магистрантов и их руководителей, Санкт-Петербург, 06-08 дек. 2022 г. СПб. : СПбГУТ, 2023. С. 33-36.

2. Федоров С. И., Ларионова А. К., Седышев Э. Ю. Исследование микроволнового генератора шума, нагруженного многозаходной спиральной структурой // Электроника и микроэлектроника СВЧ : материалы XII Всерос. научно-технич. конф., Санкт-Петербург, 29 мая-2 июня 2023 г. СПб. : СПбГЭТУ «ЛЭТИ», 2023. С. 672-676.

Verlikov N., Sedishev E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Selecting the active element for a microwave noise generator.

This work considers the possibility of creating a broadband noise signal using the Pierce oscillator with a quartz resonator and IMPATT-diodes. An equivalent circuit of a quartz oscillator with a low Q-factor for frequency band expansion is proposed.

Key words: IMPATT-diode, generators, microwave

УДК 629.072.116
ГРНТИ 47.45.29

АНТЕННЫЙ ТЕРМИНАЛ ДЛЯ СИСТЕМ СПУТНИКОВОЙ СВЯЗИ

П. В. Воропаев, Э. Ю. Седышев
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматриваются антенные терминалы для систем спутниковой связи. Определяются конструктивные особенности мобильных терминалов для систем спутниковой связи. Рассматриваются вопросы использования фазированных антенных решеток и их эффективность.

антенный терминал, спутниковая связь, фазированные антенные решётки, электромагнитные помехи, спутниковая связь, планарные антенные решётки, бегущая волна, направленность луча

Мобильные терминалы спутниковой связи – это устройства, предназначенные для обеспечения связи со спутниками. Они могут использоваться как в городе (обычный «роутер»), так в удаленных и труднодоступных местах, где отсутствует инфраструктура сотовых сетей.

Часто используются такие терминалы в экспедициях, аварийных ситуациях, научных исследованиях и других областях, где необходима надежная связь. С точки зрения СВЧ технологий, мобильные терминалы для спутниковой связи обычно включают в себя следующие компоненты: антенна, трансивер, интерфейсы и управляющая электроника.

Системы спутниковой связи предоставляют коммуникационные услуги с использованием искусственных спутников, находящихся в орбите Земли. Они могут находится на:

- низкая орбита (НО): Орбиты до 2 тыс. км. Отличаются низкой задержкой, но требуют большего числа спутников.
- средняя орбита (СО): Орбиты от 2 тыс. до 35 тыс. км. Обеспечивают баланс между покрытием и количеством спутников.
- геостационарная орбита (ГО): На высоте около 35,8 тыс. км. Спутники стационарны относительно поверхности Земли.

Частоты в таких системах представляют собой крайне большой диапазон от КВЧ (Крайне высокие частоты, 30 – 300 МГц) до ММВЧ (Миллиметровый диапазон 30 ГГц). Естественно, сюда входит частотный диапазон, называемый СВЧ – 300 МГц – 3 ГГц.

Сейчас, зачастую, фазированные антенные решётки (ФАР) используются в системах спутниковой связи (ССС) для управления направлением излучаемых сигналов, но в ФАР ССС могут возникнуть несколько проблем(1).

Эффективность ФАР зависит от точности управления фазой антенных элементов. Возможны проблемы с точностью установки фазы, что может снизить производительность системы.

ФАР подвержены влиянию различных видов интерференции, таких как электромагнитные помехи или межсистемное влияние, что может привести к потере качества связи.

ССС могут столкнуться с проблемами, связанными с электромагнитными помехами, которые могут исказить сигналы, передаваемые через ФАР.

Технические сбои и промышленные помехи в ФАР ССС могут вызвать нарушение связи и снижение производительности системы.

ФАР обычно требуют сложного технического обслуживания и регулировки для поддержания оптимальной производительности.

Разработка, установка и поддержание работоспособности системы ССС с ФАР обычно дорогостоящий процесс, что вызвано как высокой стоимостью технологии создания ССС, так и необходимостью поддержания ее работоспособности (ССС нуждаются в постоянном обслуживании).

С другой стороны, существуют планарные ФАР, которые образуют свой класс устройств (2). Они представляют собой тип антенных систем, где антенные элементы расположены в плоскости, обеспечивая плоский конструктив. Этот подход обладает несколькими преимуществами, такими как компактность, улучшенная производительность и облегченная интеграция в различные устройства (рис. 1, рис 1.1).

Плоские антенные системы легко интегрируются с MEMS (микроэлектромеханическими системами), что позволяет реализовать более сложные функции, такие как электромеханическое управление направлением луча. Плоские ФАР могут использовать фазовые массивы, где каждый элемент обладает собственной фазой. Это обеспечивает гибкость в управлении направлением луча, а также формировании различных диаграмм направленности. ПФАР могут быть реализованы на основе технологий печатных плат, что делает их относительно дешевыми и эффективными в массовом производстве.

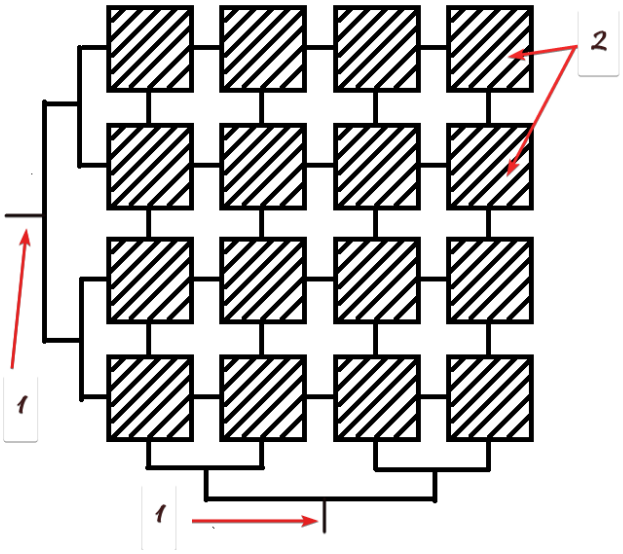


Рис. 1. Планарные антенные решетки. Двухчастотная (1- входы, 2 - излучатели)

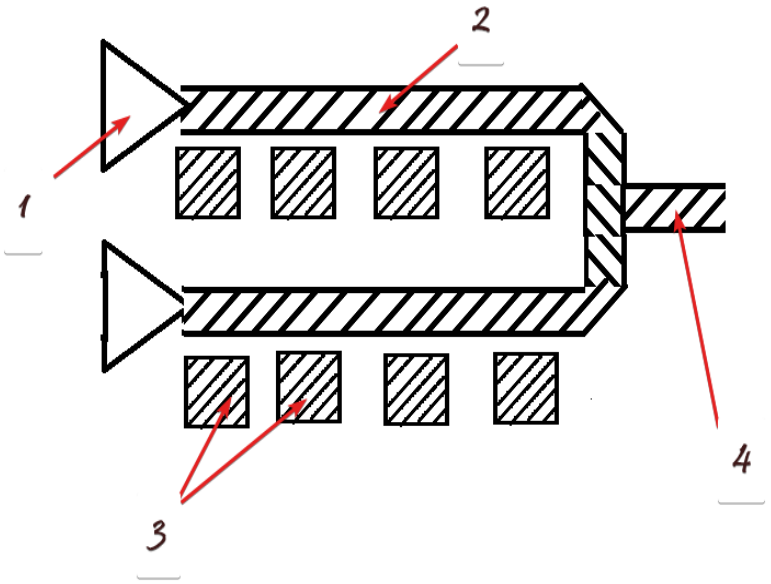


Рис. 1.1. С последовательной схемой питания (1 – нагрузка, 2 – микрополосковая линия, 3 – излучающие элементы, 4 – делитель мощности)

Одной из возможных вариаций антенной решетки бегущей волны, состоящей из фидерной линии и множества излучательных элементов, расположенных на расстоянии друг от друга вдоль самой линии, в конце которой стоит нагрузка (рис. 2). Каждый элемент состоит из отрезка полосковой линии, одни конец которого соединён с фидерной линией, а другой разомкнут. Фидерная линия разрывается щелью и, фактически, эта

конструкция является – свернутой полосковой линией с согласованной нагрузкой.

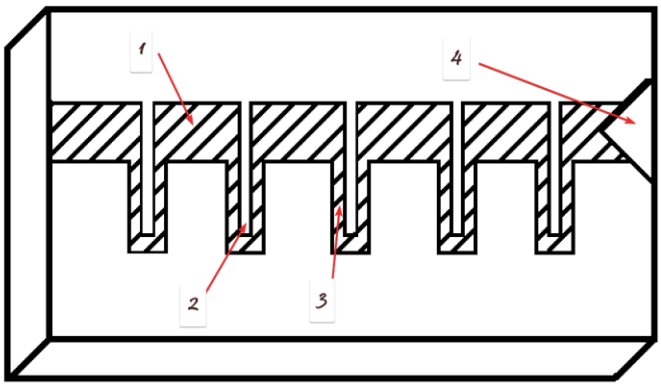


Рис. 2. АР на бегущей волне (1 – фидерная линия, 2 – щель, 3 – полосковая линия, 4 – согласованная нагрузка)

Список используемых источников:

1. Левченко В. Н. Спутниковое телевидение в вашем доме. СПб. : Полигон, 1998. 272 с.

2. Базанова А. Д., Лайко К. А., Филимонова Ю. О. Плоские антенные решетки с различными способами расположения излучателей [Электронный ресурс] // Вестник ВГТУ. 2022. N 3. URL: https://cyberleninka.ru/article/n/ploskie-antennye-reshetki-s-razlichnymi-sposobami-raspolozheniya-izluchateley (дата обращения: 16.11.2023).

Voropaev P., Sedyshev E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Antenna terminal for satellite communication systems.

This article discusses antenna terminals for satellite communication systems. The design features of mobile terminals for satellite communication systems are determined. The issues of using phased array antennas and their effectiveness are considered.

Key words: antenna terminal, satellite communications, phased array antennas, electromagnetic interference, satellite communications, planar antenna arrays, traveling wave, beam directivity

УДК 537.86.029
ГРНТИ 47.45.31

УПРАВЛЯЕМЫЙ АТТЕНЮАТОР KU ДИАПАЗОНА

Р. С. Гуляев, Э. Ю. Седышев
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе рассматривается синтез устройства управления мощностью на основе управляемого электрического аттенюатора в Ku диапазоне на полупроводниковом элементе.

KU-диапазон, управляемый аттенюатор, pin-диод

В настоящее время широко применяются системы, работающие в Ku – диапазоне. Ku – диапазоном называется диапазон сантиметровых волн с диной волны от 1,67 см до 3 см. На данный момент практически все частоты в диапазоне 10 − 18 ГГц заняты малыми спутниковыми станциями и телевещанием. Спутниковое вещание в Ku-диапазоне осуществляется главными российскими спутниковыми операторами, такими как ФГУП «Космическая связь», АО «Газпром космические системы».

К способам управления усилением, получившим широкое распространение, относится введение в состав усилительных трактов сложных пассивных цепей, коэффициент передачи которых изменяется в заданных пределах в зависимости от условий приема информационного сигнала и особенностей его прохождения через усилительный тракт. Такие цепи, называемые управляемыми аттенюаторами, выполняют в виде комбинации линейных резисторов и нелинейных элементов, сопротивление которых меняется под действием управляемого электрического, ручного или электромеханического воздействия. Аттенюатор, будучи включенным в приёмно-усилительный тракт дает возможность обеспечить требуемый характер управления коэффициентом усиления и уровнем выходного сигнала. Управляемый аттенюатор может быть отнесен к классу систем управления усилением. В зависимости от назначения аппаратуры, в состав которой входит приемно-усилительный тракт, и от условий ее работы управление параметрами элементов аттенюатора может быть механическим либо электрическим.

В работе представлено устройство управления мощностью KU-диапазона. На входе и выходе схемы используются волноводы, так как система рассчитана на высокие частоты более 10 ГГЦ. Элементом управления является pin-диод, управляющий электрическим сигналом. За основу согласованного по входу и выходу микроволнового аттенюатора взята симметричная Т-образная структура, в которой пленочные резисторы соединены между собой отрезком МПЛ без диссипативных потерь с волновым сопротивлением ρ2, как показано на рис. 1.

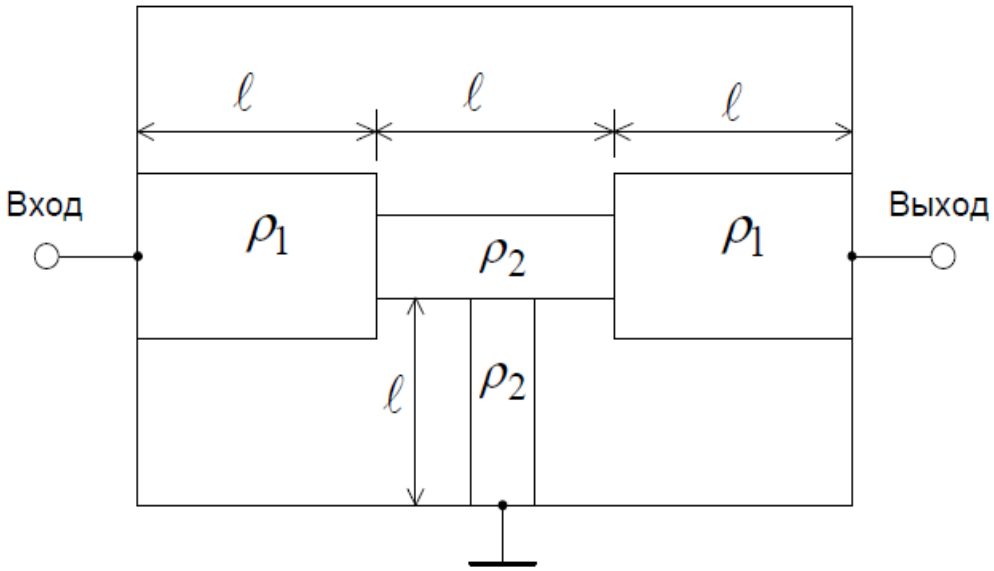


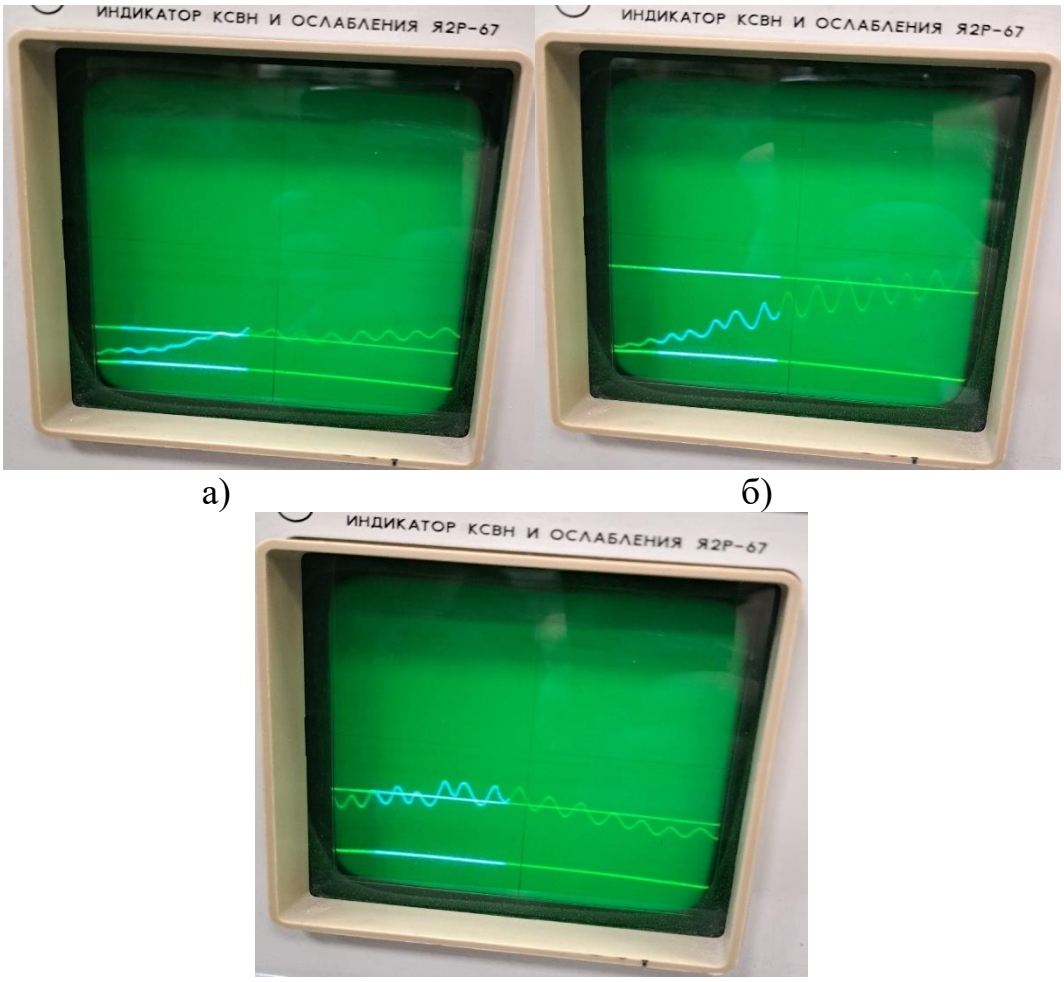
Рис. 1. Схема аттенюатора

Сигнал проходит через аттенюатор и выходит по волноводу. Регулировать сигнал, проходящий через аттенюатор, можно с помощью напряжения, подаваемого на диод. А сам pin-диод должен быть установлен в волновод с помощью специального П-образного «штатива», именно этот узел и представляет особый интерес.

Было проведено исследование влияния pin-диода на характер излучения щели в широкой стенке волновода при коммутации его сопротивления. В данной работе в качестве замещающего pin-диод компонента, перекрывающего щель, использовался smd резистор в силу того, что сопротивление последнего заранее известно. Были взяты резисторы номиналами 10 Ом, 1,8 кОм, 3,2 кОм. В поставленном эксперименте волновод перекрывался резисторами как показано на рис. 2.

Рис. 2. Сечение волновода

Измерения проводились в диапазоне 12 – 18 ГГЦ. Результаты выходного сигнала приведены на рис. 3.



а) б)

в)

Рис. 3. Осциллограммы выходного сигнала для разного номинала сопротивления: а) 3,2 кОм б) 1,8 кОм в) 10 Ом

Для сопротивления 3.2 кОм ослабление -6 дБ, для 1.8 кОм -2.3 дБ, для 10 Ом -3.8 дБ. Наибольшие потери показывает резистор 3.2 кОм. В дальнейшем планируется улучшение и модернизации схемы для дальнейших исследований.

Элементы с электрическим управляемым сопротивлением применяются в радиоэлектронной аппаратуре при решении разнообразных технических задач, в частности при необходимости обеспечить определённую связь между имениями выходного параметра устройства и интенсивности электрического воздействия.

Особенность данной работы в том, что анализ проводится для высокого частотного диапазона и возможностью гибкой подстройки управления в зависимости от задаваемых технических требований.

Список используемых источников:

1. Крылов Г. М., Хоняк Е. И., Тынныка А. Н. и др. М.: Радио и связь Управляемые аттенюаторы 1985, 120 с.

2. Богомолов П. Г, Рубанович М. Г., Хрусталев В. А., Разинкин В. П. Широкополосный пленочный СВЧ аттенюатор [Электронный ресурс] URL:

https://mwelectronics.etu.ru/assets/files/2014/oral/o03_06_bogomolovpg_shirokopolosnyi_plenochnyi.pdf (дата обращения: 29.10.2023).

3. Вабищевич Д. А. Влияние параметров pin-диода на излучение щели в волноводе // Подготовка профессиональных кадров в магистратуре для цифровой экономики: материалы Всерос. науч.-технич. и науч.-методич. конф. магистрантов и их руководителей, Санкт-Петербург, 01-03 дек. 2020 г. СПб. : СПбГУТ, 2021. С. 46.

Gulyaev R., Sedyshev E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Controlled Ku band attenuator.

In this paper, the synthesis of a power control device based on a controlled electric attenuator in the Ku range on a semiconductor element is considered.

Key words: KU-range, controlled attenuator, pin diode.

УДК 621.373.52
ГРНТИ 47.45.99

РАЗРАБОТКА ВОЛНОВОДНОГО ГЕНЕРАТОРА В ОБЪЕМНОМ ИНТЕГРАЛЬНОМ ИСПОЛНЕНИИ

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

Работа посвящена разработке интегрального генератора электромагнитных волн СВЧ диапазона для круглого волноводного тракта. Описана структура генератора, разработана модель и создан макет возбудителя колебаний. Зафиксирована его работоспособность. Обозначена стратегия дальнейшего развития.

объемная интегральная схема, микроволны, генератор, круглый волновод

Повышение частот работы радиоэлектронной аппаратуры (РЭА) до значений, на которых работа коаксиального тракта невозможна возникает необходимость создания устройств, которые имеют исключительно волноводный интерфейс. На данный момент широко известны оконечные нагрузки, фильтры, вентили, аттенюаторы и другие пассивные устройства волноводного тракта. Однако сложной конструктивной задачей остаются активные устройства, такие как генераторы и усилители.

В данной работе речь пойдет о генераторах для круглого волноводного канала. Круглая форма выбрана по той причине, что она позволяет пренебречь взаимной поляризацией элементов тракта при работе с колебанием типа E_{01}. Однако возбуждение такого колебания остается сложной задачей так-как подразумевает осевое расположение активного элемента. Аналогичное расположение активного элемента осуществляется в цилиндрическом резонаторе в режиме E_{010}, поэтому он выбран в качестве частотозадающего элемента.

Главной задачей данной работы является разработка структуры интегральной вставки в волновод. Таким образом устройство должно представлять собой объемную интегральную схему (ОИС), располагаемую в волноводе и имеющую выводы питания. Предполагается, что устройство будет состоять из основного частотозадающего цилиндрического резонатора и проставки для установки последнего в волновод требуемого диаметра. Вывод энергии в волновод должен осуществляться через щели параллельные линиям магнитного поля, исходя из этого удобно расположить щели по периметру резонатора (см. рис. 1). При этом частота резонанса E_{010} рассчитывается по формуле[1]:

$f = \frac{c}{\lambda_{кр}\sqrt{\varepsilon\mu}}$, где c - скорость света, ε и μ - диэлектрическая и магнитная проницаемость заполнения резонатора, $\lambda_{кр}$ - критическая длина волны вычисляемая по формуле[1]:

$\lambda_{кр} = 2.61a$, где а - радиус цилиндра

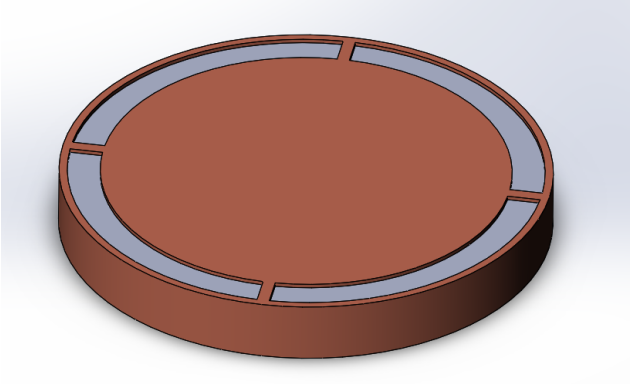


Рис. 1. Внешний вид модели объемного резонатора

В связи с тем, что резонатор имеет диэлектрическое заполнение при выходе колебания в волновод происходит скачок длины волны равный показателю преломления заполнения резонатора. Поэтому для разных материалов соотношение оптимального диаметра волновода и диаметра резонатора оказывается различным. На рис. 2 представлен разрез генератора, с установленной в него ОИС, являющийся наконечником на волновод.

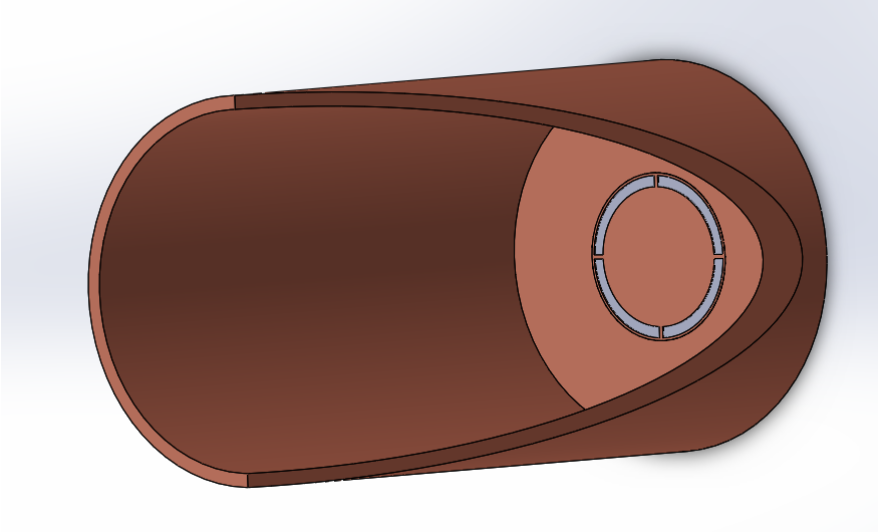
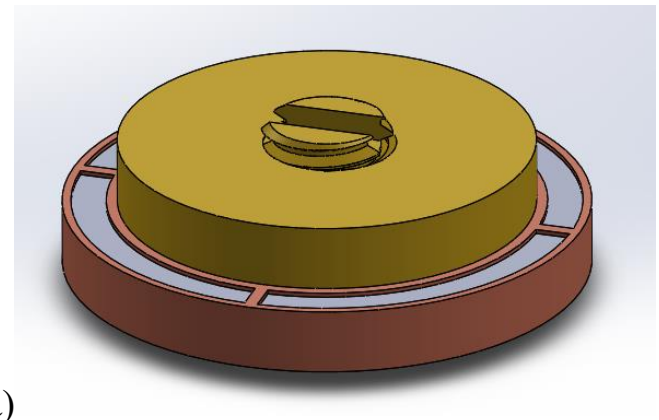
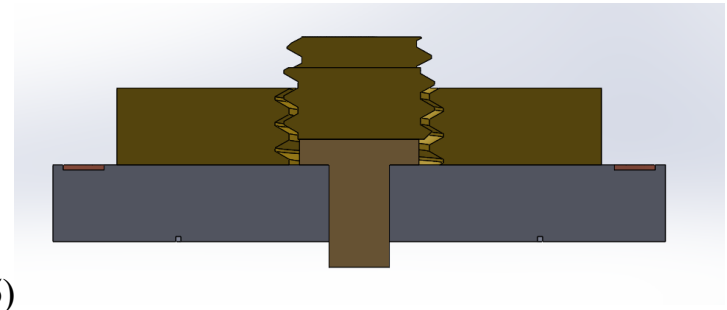


Рис. 2. Разрез генератора с вставкой возбудителя

В связи с широким разнообразием корпусов генераторных диодов, которые зависят как от частотного диапазона, так и от генерируемой мощности разработка конструкции посадочного места под диод должна производиться индивидуально. Пример конструкции для корпуса КД-107 для частоты 12 ГГц на фторопластовой подложке с ε=2.6 и μ=1 представлен на рис. 3.



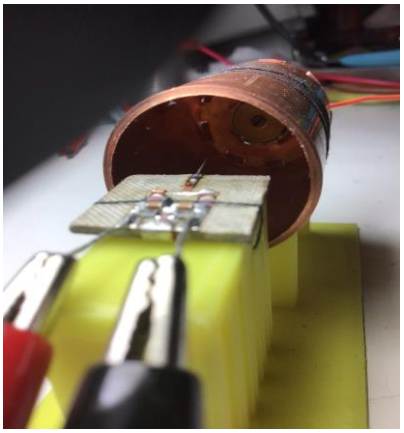
а)



б)

Рис. 3. а) Установка диода б) разрез

а)



б)

Рис. 4. Макет генератора а) ОИС, б) генератор на стенде с детектором

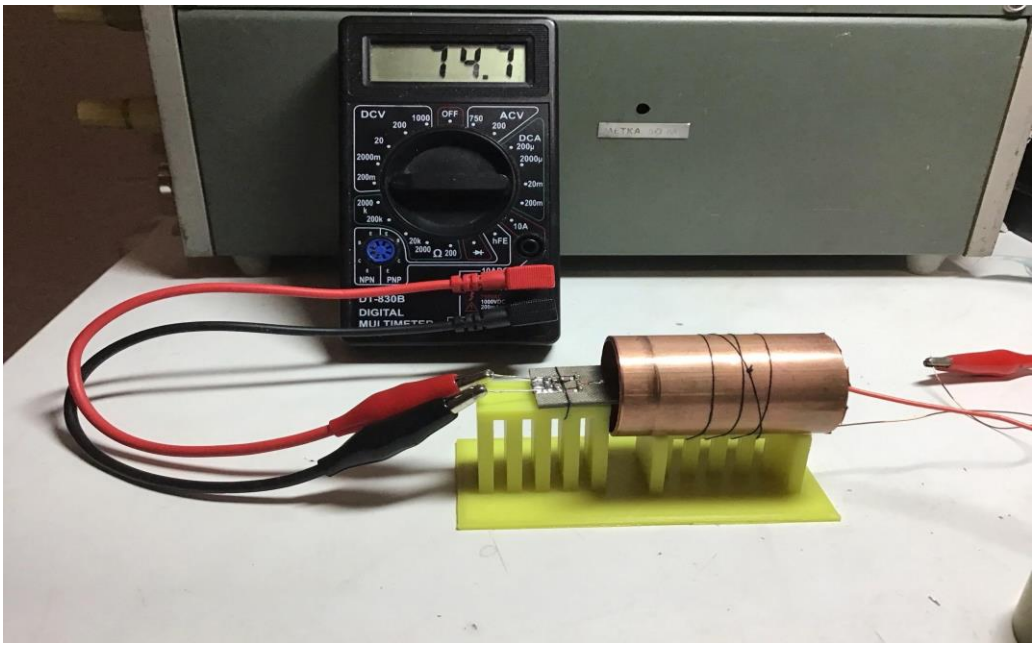


Рис. 5. Детектирование излучения

По результатам разработки получен генератор (рис. 4) и зафиксирована излучаемая мощность (рис. 5). В дальнейшем планируется установить точную частоту работы генератора, сопоставить её с рассчетным значением, а также продумать механизм и измерить диапазон подстройки частоты.

Список используемых источников:

1. Фальковский О. И. Техническая электродинамика : учебник. СПб. : Лань, 2009. ISBN 978-5-8114-0980-8. EDN QMUAZL.

2. Книгиницкий Е. И. Волноводный генератор с интегрированным резонатором // Подготовка профессиональных кадров в магистратуре для цифровой экономики : материалы регион. научно-методич. конф., Санкт-Петербург, 06-08 дек. 2022 г. СПб. : СПбГУТ, 2022. С. 29-32

3. Бочаров Е. И. Исследование генератора на активном двухполюснике в сферическом резонаторе / Е. И. Бочаров, Е. А. Коновалова, Э. Ю. Седышев // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы IX Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 26–27 фев. 2020 г. Т. 3. СПб. : СПбГУТ, 2020. С. 401-403. EDN BNGVIY.

Kniginickii E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Engineering of integral microwave generators for circle waveguide.

The article deals with the engineering microwave generator for circle waveguide. Structure of generator is presented. Model and prototype microwave initiator are created. Radiation is detected. Strategy of future promotion is marked.

Key words: volumetric integrated circuit, microwaves, generator, circle waveguide.

УДК 53.084.2
ГРНТИ 47.59.37

ПРОЕКТИРОВАНИЕ УВЧ ТРАКТА ДЛЯ ДЕТЕКТИРОВАНИЯ И ПОДГОТОВКИ МИКРОВОЛНОВЫХ СИГНАЛОВ К ПОСЛЕДУЮЩЕЙ ОБРАБОТКЕ

А. Н. Коробейников, Ю. А. Никитин
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Вот уже многие десятилетия развитие электронной техники идёт по пути увеличения быстродействия, уменьшения габаритов и увеличения вычислительной мощи. Это неизбежно приводит к использованию всё более и более высоких частот. Проектирование тракта для ультравысоких частот – актуальная и сложная задача для начинающего инженера в сфере электроники.

УВЧ, активный щуп осциллографа, разработка РЭА

Ультравысокие частоты (300МГц – 3ГГц) прочно вошли в нашу жизнь и используются повсеместно. В основном это конечно радиовещание, телевидение и связь, однако, они находят применение и в медицине, радиоастрономии. Многие цифровые системы всё ещё используют тактовые частоты до 3ГГц, поэтому изучение принципов построения передающих цепей и каскадов работающих в диапазоне ультракоротких волн является актуальной задачей для современного специалиста в области электроники и схемотехники.

Особая сложность в проектировании систем, работающих с УВЧ диапазоном, связана с большим влиянием реактивного сопротивления на импеданс:

$$Z = \sqrt{R^2 + \left(\omega L - \frac{1}{\omega C}\right)^2}$$

где Z – импеданс, R – активное сопротивление, L – индуктивность, C – ёмкость, ω – частота.

Поскольку частота имеет порядки 10^8 – 10^9 Герц, то даже на первый взгляд незначительные паразитные параметры дорожек и элементов могут оказать серьёзное влияние на работу схемы. Зачастую, это влияние столь серьёзно, что является определяющим в выборе компонентов и материалов для устройства, а также его геометрии.

В качестве показательного примера можно рассмотреть щуп электронного осциллографа. Поскольку осциллографы работают с непрерывными аналоговыми сигналами, влияние различного рода искажений сильно отразится на форме полученных осциллограмм, что подразумевает повышенные требования к качеству тракта.

Разработка электронного устройства начинается с определения его качественных характеристик. Поскольку осциллограф – измерительный прибор, его влияние на исследуемый объект должно быть минимальным. Стандартные щупы, которые идут в комплекте к большинству приборов, имеют большую ёмкость и малое входное сопротивление, что в некоторых случаях может привести к некорректным измерениям или даже нарушению работы схемы. Другими словами – чем больше входное сопротивление и меньше ёмкость, тем лучше. Это позволит производить измерения в микромощных цепях, не нарушая их работу.

Следующий важный параметр – размах сигнала. Так как осциллограф по условию цифровой, важно использовать всю ширину амплитудного диапазона его аналого-цифрового преобразователя, иначе будет потеряна значительная часть информации о сигнале. К тому же, увеличивая размах сигнала можно значительно повысить помехозащищённость и расстояние, на которое его можно передать.

Ещё один параметр – шум. Компоненты устройства должны минимально искажать полученный сигнал, не внося ощутимых помех и нелинейностей.

Реализовать эти условия, а именно высокое сопротивление и малую ёмкость на входе, усиление и низкий уровень шума на выходе, возможно с помощью активного щупа на основе высокочастотных широкополосных операционных усилителей.

На рынке представлено множество таких усилителей. Список некоторых из них приведён в таблице 1.

ТАБЛИЦА 1. Операционные усилители

Наименование	Частота единичного усиления, ГГц
OPA855	8
LMH6624MA	1,5
OPA847	3,9
OPA858	5,5
ADA4817	0,4

К сожалению, значимые параметры операционных усилителей не ограничиваются частотой единичного усиления, поэтому подбирать их нужно, ориентируясь на имеющуюся схему осциллографа.

Следующим этапом разработки является составление функциональной схемы будущего устройства. На ней изображают основные функциональные блоки устройства и их связи между собой.

После составления функциональной схемы её блоки начинают заменять элементами, из которых постепенно вырисовывается принципиальная схема. Пример принципиальной схемы активного щупа представлен на рис. 1.

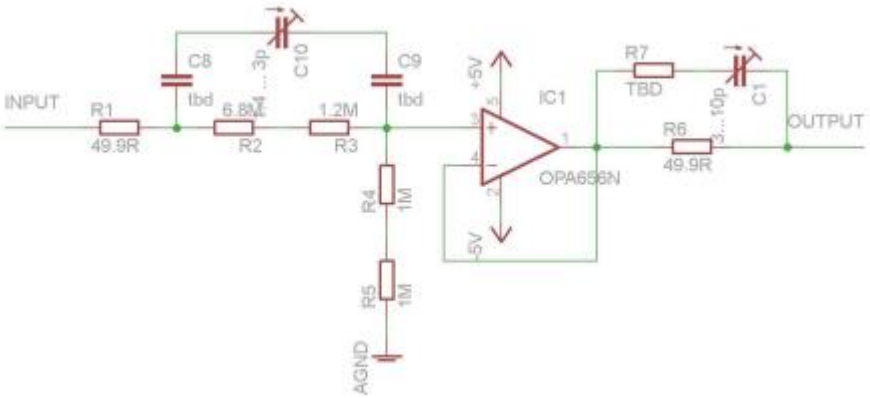


Рис. 1. Принципиальная схема активного щупа с пояснениями

В процессе создания схемы полезно пользоваться различными средами моделирования. Это позволит наглядно рассмотреть её работу и быстро рассчитать параметры элементов.

После создания принципиальной схемы можно приступать к «разводке» печатной платы. Пример разводки щупа представлен на рис. 2.

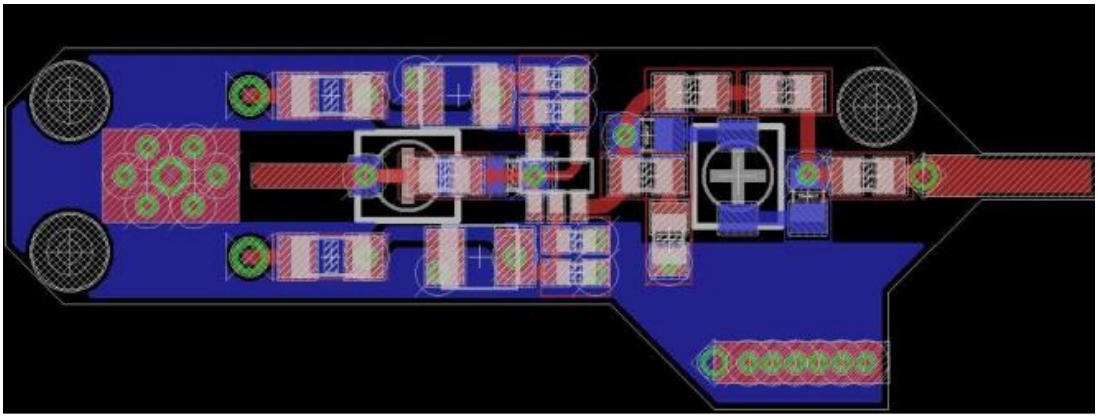


Рис. 2. Разводка активного щупа осциллографа

При работе в УВЧ диапазоне нужно учесть несколько моментов. Длины волн могут достигать десятков сантиметров, поэтому длины дорожек и расстояния между компонентами должны быть тщательно спланированы, чтобы минимизировать отражения и интерференции. По сути, важно минимизировать длины дорожек и кабелей, чтобы уменьшить потери и отражения. Острые углы и изломы также могут вызывать отражения и неустойчивость на УВЧ. Размещение компонентов должно быть сделано таким образом, чтобы минимизировать взаимное воздействие и помехи. Важно учесть материал платы и взаимное расположение слоёв на ней.

После разводки приступают к изготовлению и тестированию платы. Зачастую первые тестовые экземпляры имеют недостатки, которые необходимо выявить и устранить. Для этого понадобится высокоточное и высокочастотное оборудование. Пример тестовой платы на рис. 3.

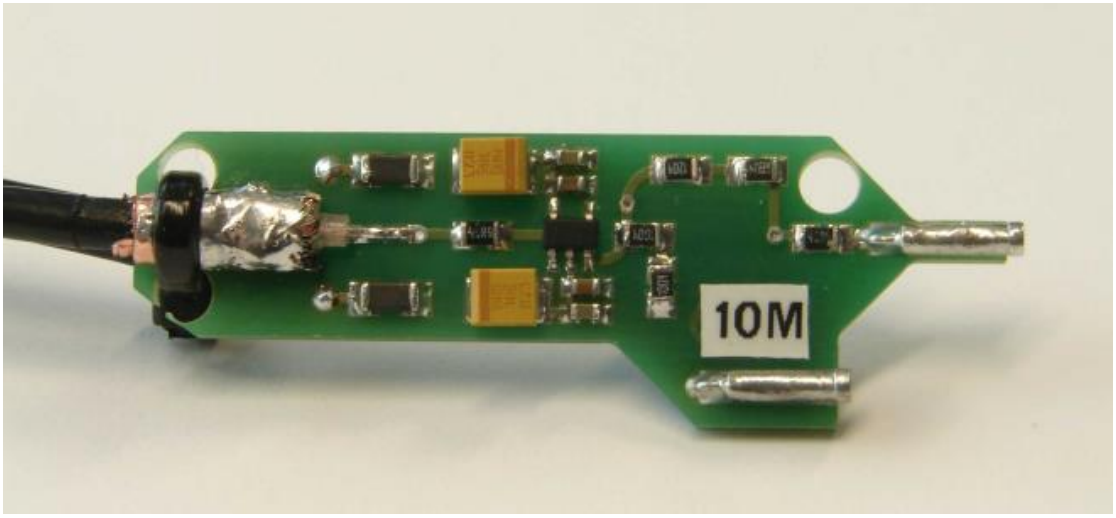


Рис. 3. Тестовая плата активного щупа осциллографа

Из всего вышеизложенного следует, что разработка даже небольших по габаритам устройств требует развитых навыков и знаний в различных областях электроники, а также материальных вложений. Таким образом, был в общих чертах сделан обзор на проблематику разработки УВЧ устройств на примере активного щупа осциллографа.

Список используемых источников:

1. Байкузов Н. А., Елин О. Г., Можжевелов Б. Н., Вишневецкий Ф., Гороховский А. В., Крылов Ю. И., Чуднов В. К. Активный щуп для осциллографа // Радио. 1988. N 12. С. 45.

2. Байкузов Н. А., Елин О. Г., Можжевелов Б. Н., Вишневецкий Ф., Гороховский А. В., Крылов Ю. И., Чуднов В. К. Активный щуп к осциллографу // Радио. 1998. N 6. С. 38.

3. ГОСТ 24375-80. Радиосвязь. Термины и определения. URL: https://docs.cntd.ru/document/1200015766

4. Texas Instruments / OPA855, 8 GHz Gain Bandwidth Product, Gain of 7 V/V Stable, Bipolar Input Amplifier /Data Sheet.

5. Analog Devices / Low Noise, 1 GHz FastFET Op Amps ADA4817-1/ADA4817-2 /Data Sheet.

Korobeynikov A., Nikitin Y.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Designing a UHF Path for Detecting and Preparing Microwave Signals for Subsequent Processing.

For many decades, the development of electronic technology has been on the path of increasing speed, reducing size and increasing computing power. This inevitably leads to the use of higher and higher frequencies. Designing a path for ultra–high frequencies is an urgent and difficult task for a novice engineer in the field of electronics.

Key words: UHF, active oscilloscope probe, development of electronic equipment.

УДК 621.372.543.2
ГРНТИ 47.45.99

ИНЖЕНЕРНЫЙ МЕТОД СИНТЕЗА УСТРОЙСТВ ЧАСТОТНОЙ СЕЛЕКЦИИ МАСШТАБИРОВАНИЕМ

Э. Ю. Седышев, Д. А. Смирнова
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Предлагаемый в статье инженерный метод синтеза фильтров СВЧ обладает рядом преимуществ, одним из которых является наглядность. Масштабирование топологии с целью получения новых частотных характеристик позволит повысить эффективность процесса синтеза фильтров. В развитие метода созданы макеты фильтров в масштабе 1:1 и 1:1,5, произведено сравнение полученных характеристик.

синтез, масштабирование, фильтр, СВЧ, микрополосковая линия

В настоящее время устройства частотной селекции являются неотъемлемыми компонентами СВЧ техники. Фильтрами называются четырехполюсники, основной функцией которых является избирательное выделение и подавление частотных составляющих сложного сигнала. Эти устройства широко применяются в приемных устройствах, в цепях согласования, являются элементами антенно-фидерного тракта (АФТ) и т. д. [1, 2].

Современные методы синтеза фильтров – оптимизационный и прямой – предполагают сложные и трудоемкие математические расчеты [2]. Таким образом, актуальной на сегодняшний день задачей является разработка простого инженерного метода синтеза устройств частотной селекции на основе изменения геометрических размеров топологии. Предлагаемый метод позволит значительно упростить процесс синтеза фильтров.

Приступая к выполнению поставленной задачи, определимся с типом устройства частотной селекции. Можно предположить, что каждый тип линии (микрополосковая, копланарная, щелевая, симметричная полосковая, несимметричная полосковая, коаксиальная, волноводная) имеет свою зависимость изменения АЧХ от изменения размеров устройства с сохранением пропорций. Очевидно, что для получения необходимых S-параметров масштабированного фильтра, изменение геометрии топологии по осям X, Y и Z будет происходить со своим коэффициентом подобия. Учитывая сделанные предположения, в качестве типа линии, на которой будет изготавливаться макет фильтра, была выбрана микрополосковая линия (МПЛ), как самая простая.

По типу расположения полос пропускания и полос заграждения был выбран полосно-пропускающий фильтр (ППФ), так как ППФ включает в себя элементы и фильтра нижних частот (ФНЧ), и фильтра верхних частот (ФВЧ). По конструктивному исполнению полосковые фильтры можно классифицировать на несколько основных типов: шпилечный, гребенчатый,

встречно-штыревой, ступенчатый, шлейфный, на связанных линиях. Структуры упомянутых типов фильтров представлены на рис. 1.

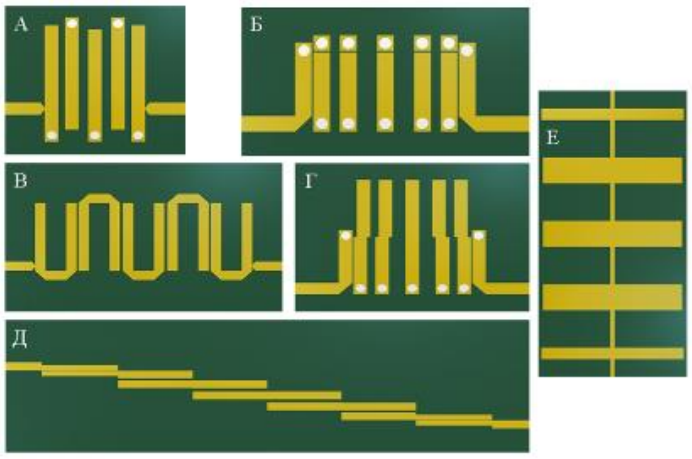


Рис. 1. Топологии основных типов полосковых фильтров СВЧ: встречно-штыревой (а), гребенчатый (б), шпилечный (в), ступенчатый (г), на связанных линиях (д), шлейфный (е)

Ранее рассматривался вопрос инженерного метода синтеза фильтров СВЧ [3, 4]. Автор создал макет шпилечного фильтра на основе фильтра-прототипа и менял его геометрические размеры. В результате исследований был сделан вывод, что при масштабировании зависимость между емкостями связей и частотой сложная, в отличии от зависимости между линейными размерами резонаторов и частотой. Автором было сделано предположение, что для поставленной задачи существуют более простые топологии фильтров. Исходя из этого, необходимо выбрать такую структуру фильтра, которая не содержит емкостных связей и является максимально симметричной для линейной зависимости между масштабом фильтра и его характеристиками. Таким критериям соответствует шлейфный фильтр, который автор [3] также использовал в ходе своей работы. Вначале можно исследовать шлейфный фильтр на резонаторах в режиме короткого замыкания (КЗ) или холостого хода (ХХ). В дальнейшем, при выявлении зависимости между характеристиками фильтра и изменением его геометрических размеров, возможно использование какой-либо структуры фильтра с емкостными связями.

В качестве первого образца был выбран шлейфный ППФ пятого порядка на параллельных полуволновых шлейфах в режиме ХХ из курсового проекта (2021/22 учебный год) по дисциплине «Компьютерное моделирование ОИС СВЧ» профиля магистерской подготовки СПбГУТ «Микроволновая техника. Объемные интегральные схемы» [5]. Принципиальная схема представлена на рис. 2.

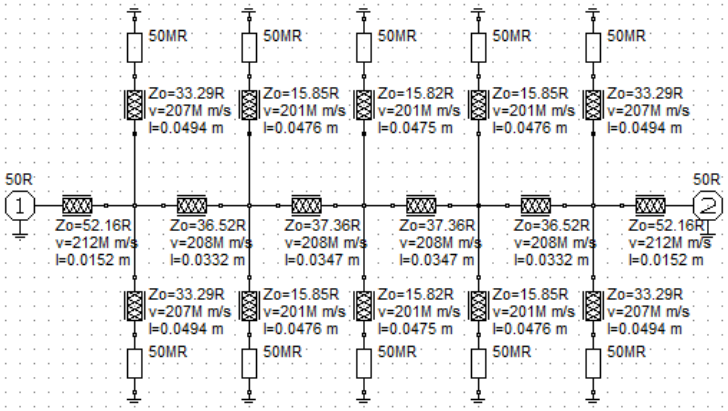


Рис. 2. Принципиальная схема шлейфного фильтра 1:1 в пакете RFSimm99

В пакете RFSimm99 была проведена эмуляция работы данного фильтра и получена его АЧХ (рис. 3). Центральная частота – 2 ГГц, полоса пропускания – 456 МГц, относительная полоса пропускания – 23 %.

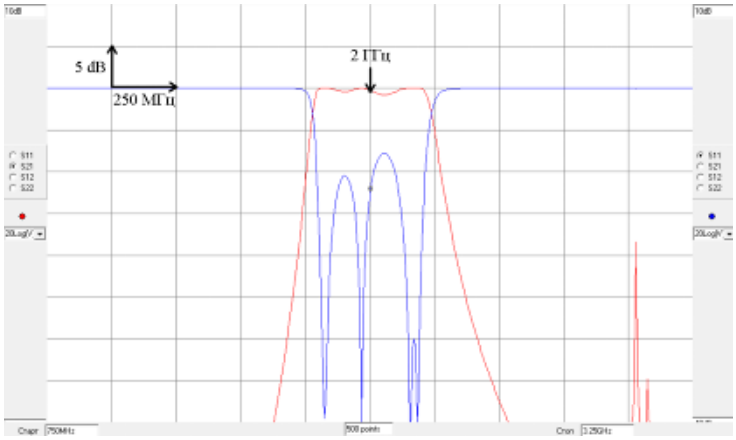


Рис. 3. АЧХ фильтра 1:1

Был изготовлен макет исходного фильтра на подложке из PET-G пластика толщиной 1 мм с диэлектрической проницаемостью ε = 2,43 и tgδ = 0.01 (рис. 4). Центральная частота макета (эксперимент) = 2,1 ГГц, полоса пропускания = 394 МГц, относительная полоса пропускания – 19 %. Из АЧХ устройства видно, что фильтр в полосе пропускания - расстроен, но в процессе работы он легко подстраивался изменением длины шлейфов.

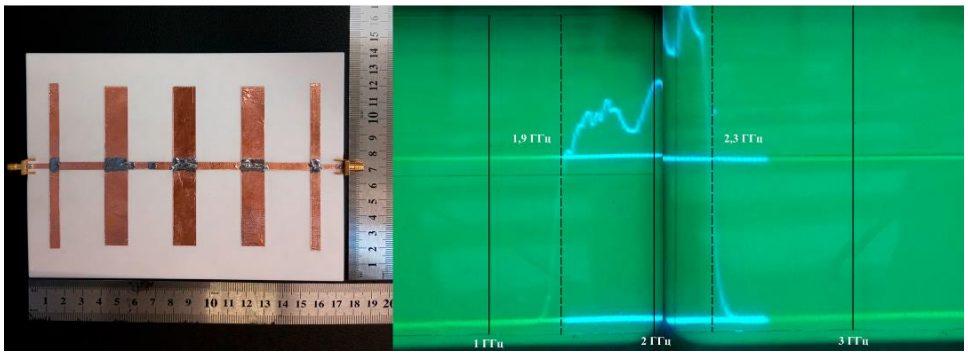


Рис. 4. Макет фильтра 1:1 и его измерения

Далее геометрические размеры фильтра-образца были уменьшены в 1,5 раза. В результате был получен фильтр, центральная частота которого увеличилась до 3,04 ГГц. На симуляции абсолютная полоса пропускания составила 706 МГц, а относительная – 23 %. Принципиальная схема и АЧХ полученного фильтра представлены на рис. 5 и 6 соответственно.

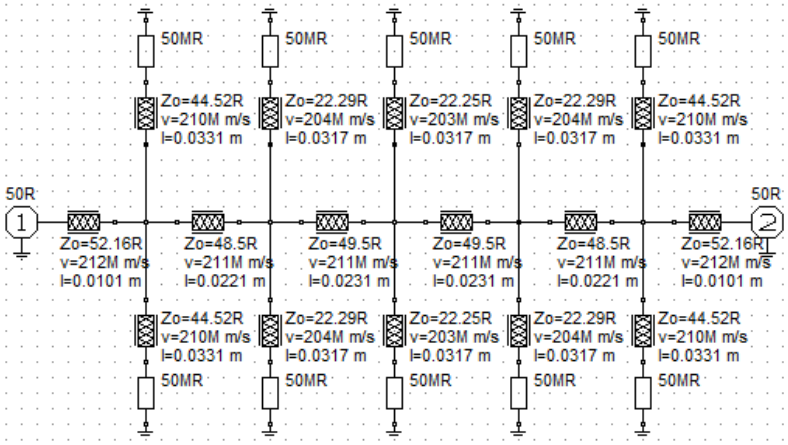


Рис. 5. Принципиальная схема шлейфного фильтра 1:1,5 в пакете RFSimm99

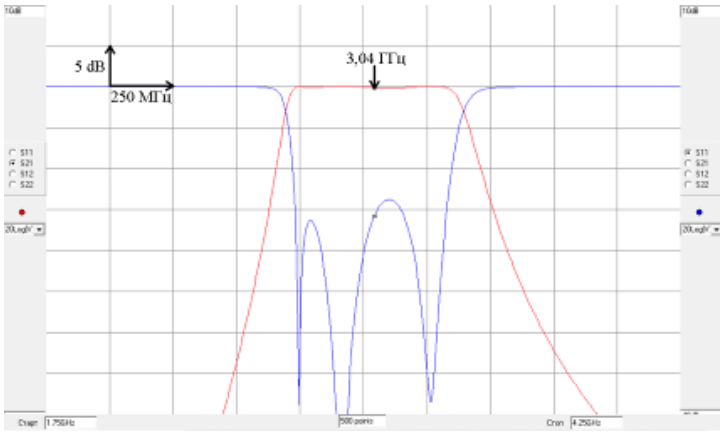


Рис. 6. АЧХ фильтра 1:1,5

Был изготовлен макет фильтра 1:1,5 (рис. 7). По результатам его измерений центральная частота составила 3,15 ГГц, полоса пропускания – 500 МГц, относительная полоса пропускания – 16 %.

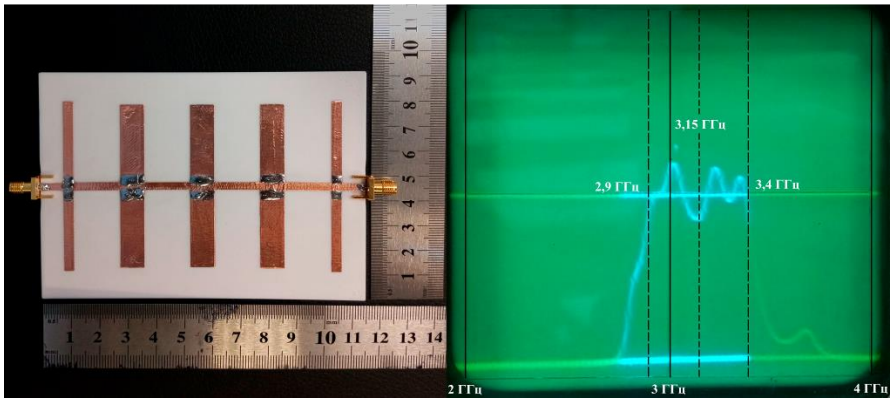


Рис. 7. Макет фильтра 1:1,5 и его измерения

Таким образом, в результате эмуляции работы устройств и экспериментальных измерений варьирование геометрических размеров фильтра-образца приводит к изменению центральной частоты, а также полосы пропускания без изменения характера характеристики. ППФ остается ППФ. Поиск точной зависимости изменений, по которой происходит изменение данных параметров, и является нашей основной задачей. На основе проведенных исследований можно сделать вывод, что *масштабирование данного типа фильтров сохраняет функционал самого фильтра*.

Подводя итоги работы, можно сказать, что метод масштабирования топологии устройств частотной селекции является простым и наглядным, и в большой мере упростит задачу проектирования фильтров конкретного типа.

Список используемых источников:

1. Маттей Д. Л., Янг Л., Джонс Е. М. Фильтры СВЧ, согласующие цепи и цепи связи: в 2 т. / под ред. Л. В. Алексеева, Ф. В. Кушнира. М. : Связь, 1971. Т. 1. 440 с.
2. Тюрнев В. В. Теория цепей СВЧ : учеб. пособие. Красноярск : ИПЦ КГТУ, 2006. 199 с.
3. Полякова А. В., Седышев Э. Ю. Масштабирование топологии как метод синтеза полосковых фильтров СВЧ // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы X Междунар. науч.-технич. и науч.-методич. конф., Санкт-Петербург, 24–25 фев. 2021 г. СПб. : СПбГУТ, 2021. Т. 2. С. 547-552.
4. Бочаров Е. И., Полякова А. В., Седышев Э. Ю. Инженерный метод синтеза полосно-пропускающих фильтров СВЧ с помощью масштабирования // Подготовка профессиональных кадров в магистратуре для цифровой экономики : материалы Всерос. науч.-технич. и науч.-методич. конф. магистрантов и их руководителей, Санкт-Петербург, 30 нояб.-02 дек. 2020 г. СПб. : СПбГУТ, 2021. С. 326-329.
5. Седышев Э. Ю. Компьютерное моделирование ОИС СВЧ: методические указания по курсовому проекту [Электронный ресурс].
6. Булатова И. А., Иванова Е. А., Крюков А. Н., Седышев Э. Ю. Шлейфные фильтры СВЧ в объемном интегральном исполнении // Электроника и микроэлектроника СВЧ. СПб. : СПбГЭТУ «ЛЭТИ», 2016. Т. 1. С. 169-174.

Sedyshev E., Smirnova D.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Engineering Method of Synthesis of Frequency Selection Devices by Scaling.

The engineering method of synthesis of microwave filters proposed in the article has a number of advantages in comparison with traditional methods. Scaling the topology in order to obtain new frequency characteristics will increase the efficiency of the filter synthesis process. Filter layouts were also created on a scale of 1:1 and 1:1.5, and the obtained characteristics were compared.

Key words: synthesis, scaling, filter, microwave, microstrip line.

Секция 1.2.
Промышленная электроника

УДК 621.389
ГРНТИ 47.41.99

РАЗРАБОТКА И ИССЛЕДОВАНИЕ Н-МОСТА ДЛЯ РЕВЕРСИВНОГО УПРАВЛЕНИЯ ДВИГАТЕЛЕМ ПОСТОЯННОГО ТОКА

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

Рассматривается вопрос проектирования и синтеза схемы Н-моста, позволяющей изменять полярность напряжения на нагрузке, а также дальнейшая возможность контроля и управления открытием и закрытием соответствующих ключей, входящих в конструкцию Н-моста. Управление схемой будет осуществляться при помощи микроконтроллера Arduino Nano, а нагрузкой в данном случае будет выступать двигатель постоянного тока, на котором, при изменении полярности напряжения, будет изменяться направление вращения, а скорость вращения будет регулироваться при помощи ШИМ-сигнала, который генерируется микроконтроллером.

Н-мост, микроконтроллер, ШИМ, двигатель постоянного тока

В современных промышленных и бытовых системах все чаще применяются электродвигатели постоянного тока, способные выполнять большой спектр задач в различных отраслях промышленности. Для эффективного управления такими двигателями используется электрическая схема, называемая Н-мостом, которая позволяет осуществлять реверсивное управление двигателем постоянного тока путем попарной коммутации транзисторов, выполняющих роль ключей, вследствие чего полярность на нагрузке будет менять свое направление.

Н-мост — это электронная схема, которая позволяет контролировать направление вращения двигателя путем изменения полярности подаваемого на него напряжения. Он состоит из четырех коммутационных элементов - обычно это транзисторы, которые соединяются в определенной конфигурации. Два коммутационных элемента образуют верхний мост, а два других - нижний мост.

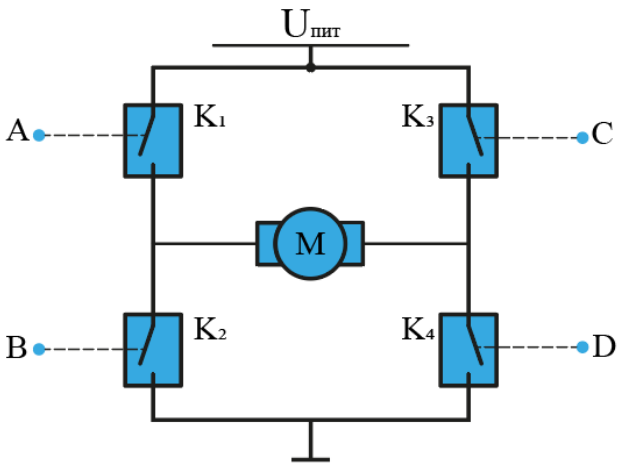


Рис. 1. Упрощенная схема Н-моста

Различные комбинации включения и выключения коммутационных элементов в Н-мосте позволяют изменять направление тока, протекающего через двигатель. При одной конфигурации ток протекает через двигатель в одном направлении, а при другой - в противоположном. Это достигается путем изменения полярности напряжения на двух выводах двигателя. Если на ключ подается сигнал «1», то он замыкается, если «0» - остается разомкнутым.

ТАБЛИЦА 1. Логика управления ключами h-моста

A	B	C	D	Результат
1	0	0	1	Мотор вращается по часовой
0	1	1	0	Мотор вращается против часовой
0	0	0	0	Свободное вращение мотора
0	1	0	1	Мотор тормозит
1	0	1	0	Мотор тормозит
1	1	0	0	Короткое замыкание
0	0	1	1	Короткое замыкание

Микроконтроллеры выполняют функцию центрального управляющего устройства, которое принимает данные о состоянии системы и генерирует соответствующие управляющие сигналы для Н-моста, а, как следствие, для двигателя постоянного тока. Также при помощи ШИМ-сигнала, генерируемого микроконтроллером, является возможным реализация регулировки скорости вращения.

Реализацию данного макета было необходимо начать с проектирования схемы Н-моста, а также всех элементов питания и включения микроконтроллера в систему управления.

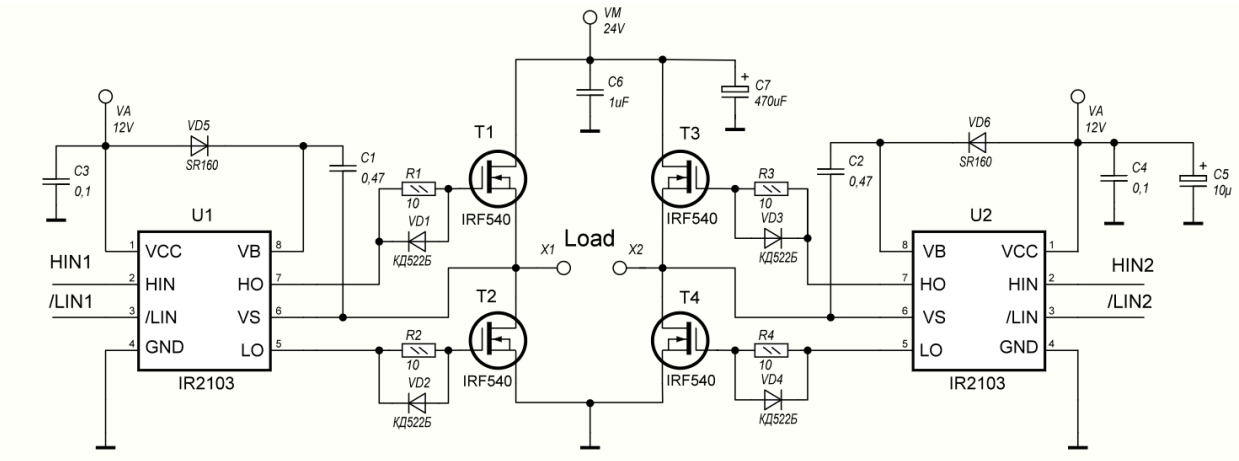


Рис. 2. Схема h-моста для макетной реализации

- HIN1, /LIN1 и HIN2, /LIN2 входы управляющих сигналов для левого и правого полумостов соответственно.
- VM 24V: Вход для общего питания всего макета.
- VA 12V: Вход питания, идущего со стабилизатора LM7812, который обеспечивает питание в 12 Вольт для работы полумостовых драйверов.
- Load: Двигатель постоянного тока, который был выбран для данной реализации.

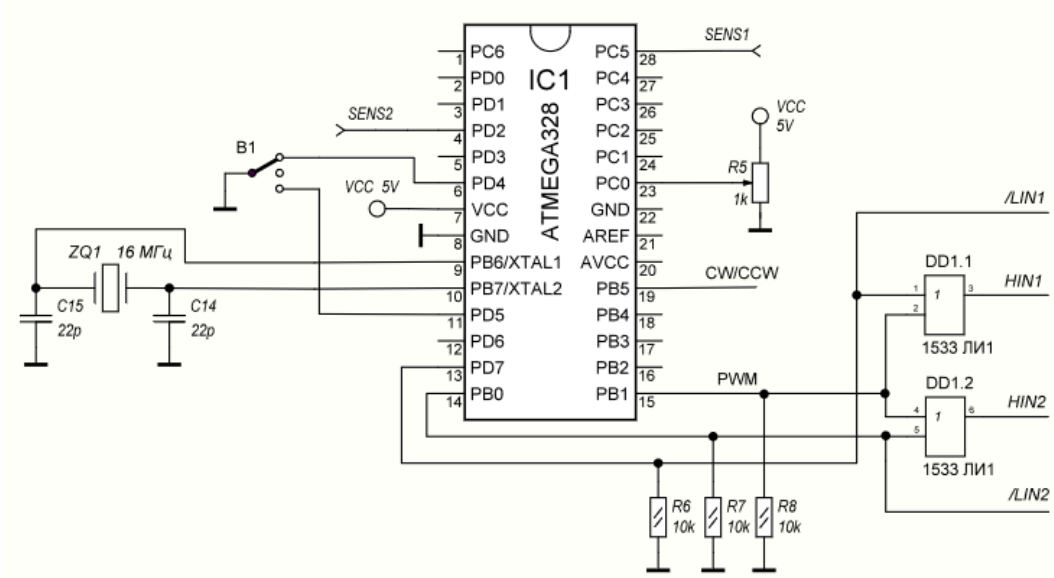


Рис. 3. Схема включения Arduino Nano в систему управления

- VCC 5V: Вход питания, идущего со стабилизатора LM7805, который обеспечивает питание в 5 Вольт для работы микроконтроллера Arduino Nano.
- Выходы HIN1, /LIN1 и HIN2, /LIN2 управляющих сигналов, в дальнейшем поступающих на входы полумостового драйвера, через логический элемент DD1 (1533 ЛИ1) для предотвращения короткого замыкания на ключах.

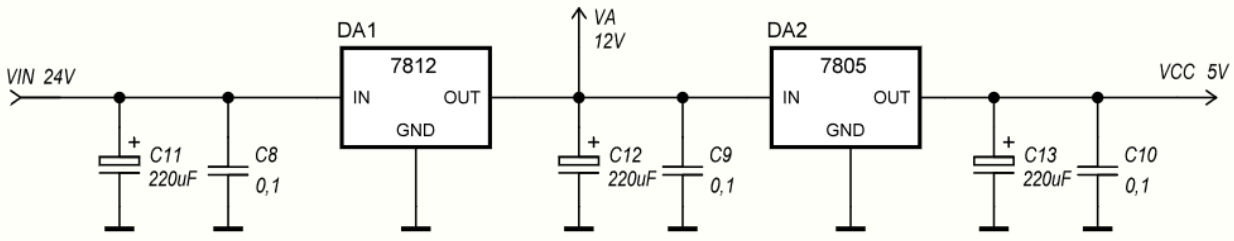


Рис. 4. Схема преобразователя входного напряжения

Задача данной схемы состоит в том, чтобы преобразовать и стабилизировать входное напряжение в 24 Вольта, чтобы обеспечить питанием другие элементы макета.

- VIN 24V: Вход общего питания.
- VA 12V: Выход сигнала, преобразованного при помощи стабилизатора напряжения DA1, который необходим для питания полумостовых драйверов.
- VCC 5V: Выход сигнала, преобразованного при помощи стабилизатора напряжения DA2, который необходим для питания микроконтроллера.

В ходе данной работы был исследован принцип работы электронной схемы Н-моста, синтезирована его принципиальная схема с подключением микроконтроллера для управления ключами Н-моста, а следовательно, направлением вращения двигателя постоянного тока.

Список используемых источников:

1. Бочаров Л. Н. Расчет электронных устройств на транзисторах : учеб. пособие / Л. Н. Бочаров, С. К. Жебряков, И. Ф. Колесников. М. : Энергия, 1978. 209 с.
2. Битюцкий И. Б. Электрические машины. Двигатель постоянного тока : учеб. пособие / И. Б. Битюцкий, И. В. Музылева. СПб. : Лань, 2018. 168 с.
3. Блум Д. Изучаем ардуино : учеб. пособие. СПб. : БХВ, 2020. 544 с.
4. Монк С. Основы работы со скетчами : учеб. пособие. СПб. : Питер, 2016. 176 с.

Erchukov I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

The design and synthesis of the H-bridge circuit, allowing to change the polarity of the voltage on the load, as well as the further possibility of monitoring and controlling the opening and closing of the corresponding keys included in the design of the H-bridge.
The circuit is controlled by the Arduino Nano microcontroller, and the load in this case will be a DC motor, which, when you change the polarity of the voltage, will change the direction of rotation, and the speed of rotation will be controlled by a PWM signal, which is generated by the microcontroller.

Key words**: **H-bridge, microcontroller, PWM, DC motor.

РАДИОТЕХНОЛОГИИ СВЯЗИ

2.1. Медиатехнологии и телерадиовещание

УДК 621.397.132
ГРНТИ 19.61.31

ИССЛЕДОВАНИЕ РАБОТЫ СПЛАЙСЕРОВ РАЗЛИЧНЫХ ПРОИЗВОДИТЕЛЕЙ В ОДНОЧАСТОТНОЙ СЕТИ СТАНДАРТА DVB-T2 В Г. САНКТ-ПЕТЕРБУРГ

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

В настоящее время на сети Российской Телевизионной и Радиовещательной Сети (РТРС) в городе Санкт-Петербурге производится вставка локальной информации или же рекламы сплайсерами двух производителей: ENENSYS и QUALITTEQ. Вследствие сложившейся в мире ситуации закупить оборудование для обслуживания сплайсеров фирмы ENENSYS не представляется возможным, так как это оборудование французского производства. В статье будет исследоваться совместная работа сплайсеров вышеупомянутых производителей в одночастотной сети стандарта DVB-T2 с целью анализа возможности импортозамещения на отечественное оборудование.

одночастотная сеть, сплайсер, DVB-T2, цифровое телевещание

Сплайсер - устройство, позволяющее врезать в транспортный поток локальную информацию, хранящуюся на рекламном сервере.

Схема вставки рекламы представлена на рис. 1.

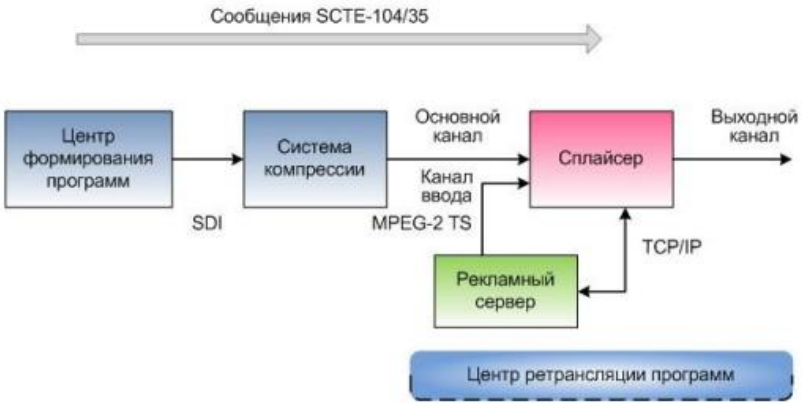


Рис. 1. Схема тракта со вставкой локальной информации

Программный сигнал центральной станции формируется в центре формирования программ (ЦФП). В англоязычной литературе используется термин Broadcast Operation Center (BOC).

Для передачи программного сигнала в систему компрессии обычно используется интерфейс HD/SD-SDI. Здесь сигналы видео и аудио подвергаются компрессии и мультиплексируются в транспортный поток MPEG-2 TS одной программы (Single Program Transport Stream – SPTS).

SPTS, в свою очередь, могут мультиплексироваться в многопрограммный транспортный поток Multi Program Transport Stream (MPTS).

Потоки SPTS или MPTS по интерфейсам DVB или IP передаются в региональные центры ретрансляции программ (ЦРП), где они подвергаются модификации путем вставки регионального контента и далее ретранслируются на свою территорию вещания в форме модифицированных потоков SPTS или MPTS.

Вставки регионального контента должны происходить в предназначенные для этого временные интервалы в расписании вещания центральной станции. В документах SCTE эти временные интервалы называются avails. При переводе на русский язык используются термины «коммерческий интервал времени», «региональное рекламное окно», «рекламный временной слот» и другие варианты. Далее в качестве аналога термина avail будет использоваться термин «слот».

На границах слота производится переключение, или сплайсинг (Splicing), между сигналами из основного канала (сигнал центральной станции) и из канала ввода (сигнал региональной станции). Точка переключения «центр/регион» называется входной точкой сплайсинга – Splice In Point, точка переключения «регион/центр» называется выходной точкой сплайсинга – Splice Out Point.

Переключение сигналов в ЦРП производится сплайсером (Splicer). Спецификации DPI (цифровой вставки программ) определяют бесшовный (seamless) – незаметный для зрителя по изображению и звуку – сплайсинг с точностью до кадра.

Для исследования работы сплайсеров различных производителей в одночастотной сети стандарта DVB-T2 в первую очередь требуется построить стенд, с помощью которого будет возможно исследовать их совместную работу.

Структурная схема стенда представлена на рис. 2:

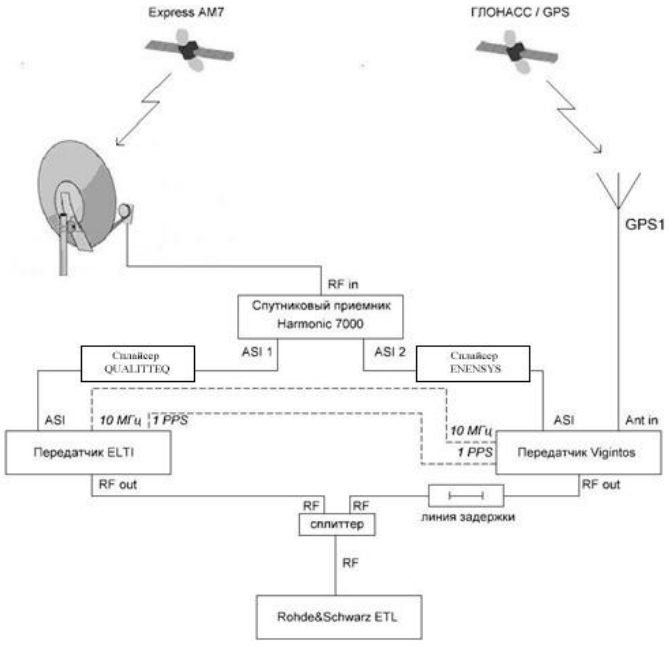


Рис. 2. Структурная схема стенда для исследования возможности функционирования сплайсеров различных производителей в одночастотной сети стандарта DVB-T2

Спутниковый приемник Harmonic 7000 принимает сигнал федерального пакета программ и транслирует сигнал T2-MI на входные интерфейсы сплайсеров QUALLITEQ и ENENSYS. Далее сигнал поступает на передатчики. Передатчики синхронизируются при помощи сигнала со спутника GPS/ГЛОНАСС, а затем сигналы выравниваются с помощью линии задержки. В качестве измерительного оборудования выступает телевизионный анализатор Rohde&Schwarz ETL.

Телевизионный анализатор ETL компании Rohde & Schwarz представляет собой мультистандартную платформу для анализа телевизионных сигналов. Он объединяет в себе функции испытательного ТВ приемника и анализатора спектра, обеспечивая достаточную точность измерений. Прибор поддерживает существующие цифровые и аналоговые телевизионные стандарты.

В ходе исследования, было обнаружено, что коэффициент MER (коэффициент ошибок модуляции) имеет крайне малое значение, равное 9 дБ, при норме в 35 дБ, что показано на рис. 3. Соответственно одночастотная сеть не строится.

Рис. 3. Результаты анализа сигнала с двух передатчиков в одночастотной сети

При этом сигналы отдельно с обоих передатчиков передавались без проблем и ошибок, задержки сигналов также находились в пределах нормы (в пределах защитного интервала):

$$\Delta t = t1 - t2 = \ 447{,}57 - 447{,}48 = 0{,}09 \text{ мс} = 90 \text{ мкс} < 224 \text{ мкс}$$

где t1- задержка на выходе с первого передатчика, t2- задержка на выходе со второго передатчика.

Соответственно, оставался последний вариант, почему одночастотная сеть рушилась - сигналы не были побитно идентичны. Для проверки этого использовалась программа DiviSuit, а также записанные транспортные потоки с обоих передатчиков.

На рис. 4 приведен раскрытый транспортный поток с первого передатчика.

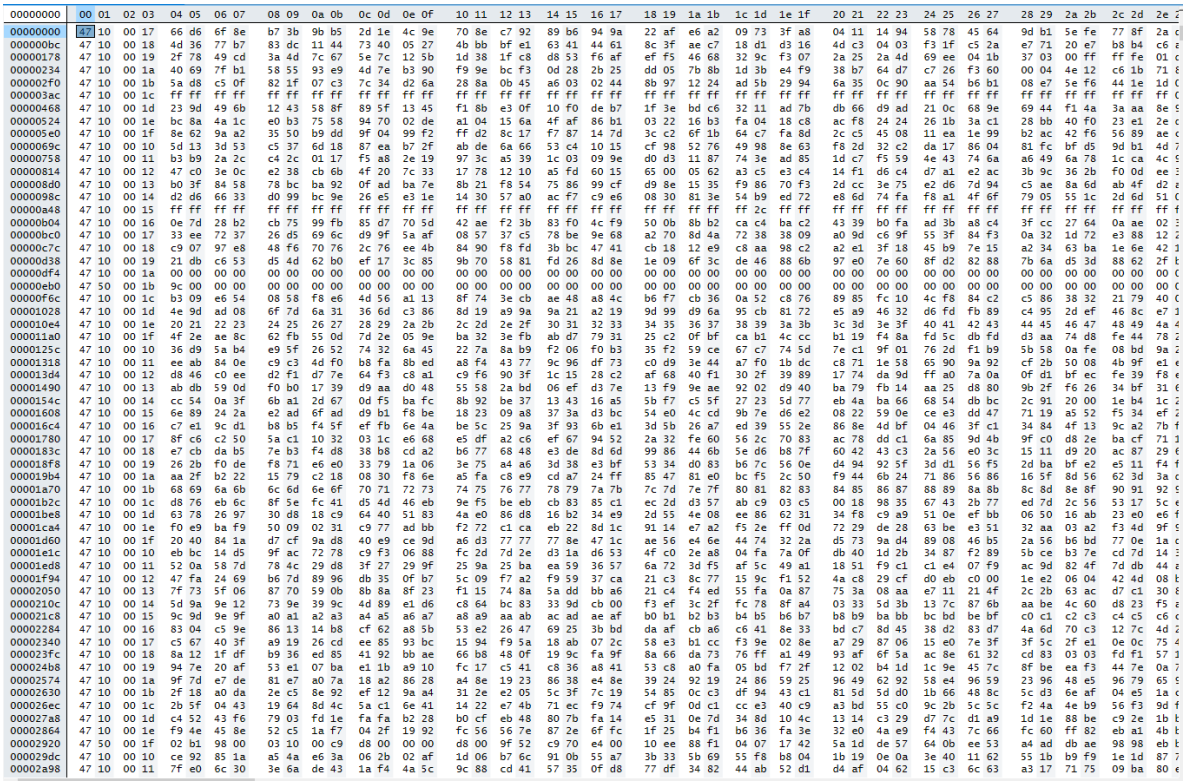


Рис. 4. Пакеты транспортного потока, полученного с первого передатчика

Требуется сравнить 2 полученных потока с выравниванием. Выравнивание нужно для того, чтобы исключить человеческий фактор при одновременном нажатии на кнопку записи потока с 2 устройств.

Результатом сравнения служат таблица 1 и рис. 5.

ТАБЛИЦА 1. Результат сравнения потоков, сформированный в виде таблицы

Тип	Блоки	Размер, байты
Совпадающие	281	124 442
Измененные	268	765 613 639
Вставленные	6	915
Удаленные	44	768 292 444

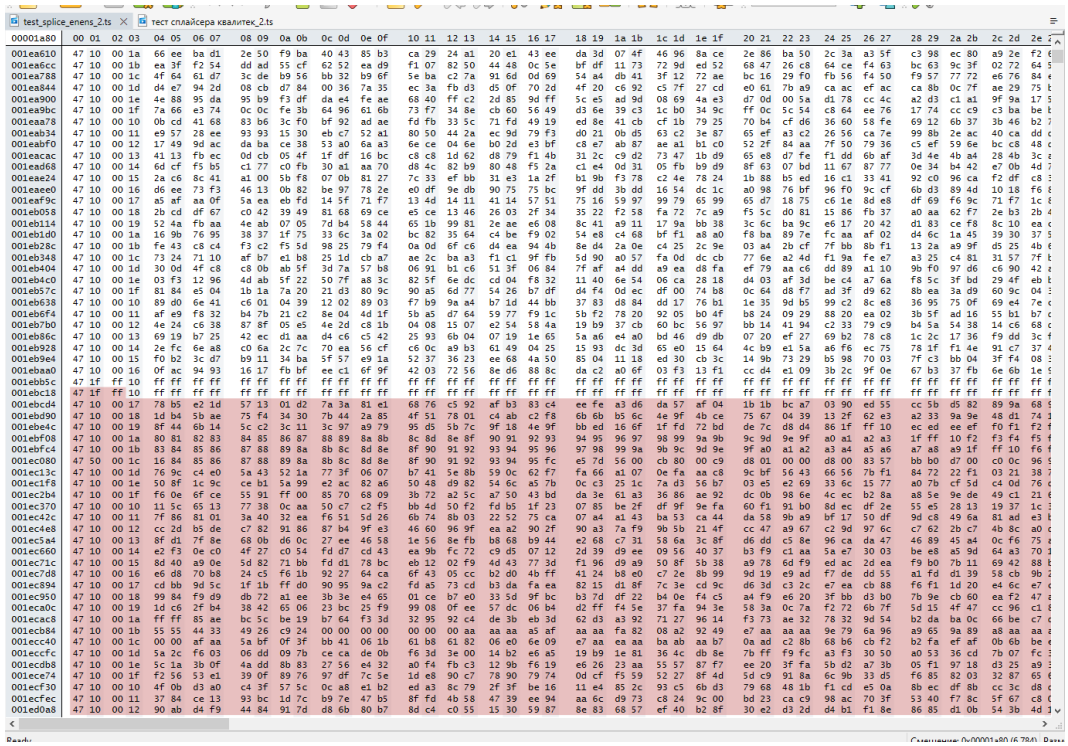


Рис. 5. Результат сравнения потоков.

По рис. 5 можем увидеть белые и красные ячейки пакетов. Белые значат, что сигналы, которые мы сравнивали побитно идентичны, а красные- побитно не идентичны. Исходя из этого, можем сделать вывод, что в какой-то момент сигналы были изменены, так как исходные сигналы были одинаковы. Произошло это на стадии вставки локальной информации в сплайсере, а объясняется тем, что пусть механика работы одна, сплайсеры начали врезку локального контента в разные кадры, вследствие разных технических характеристик. Так как для формирования одночастотной сети побитная идентичность сигналов является ключевым правилом, а в нашем случае оно не выполняется, одночастотная сеть и не строилась, в то время как каждый сигнал по отдельности принимается без проблем.

Заключение

Построение одночастотной сети стало проблематичным, несмотря на отсутствие проблем с оборудованием и соответствие характеристик сигнала нормам. Ошибка заключается в нарушении побитовой идентичности сигналов, вызванном изменением сигналов на стадии вставки локальной информации в сплайсере. Это происходит из-за различных технических характеристик сплайсеров, которые врезают локальный контент в разные кадры. Формирование одночастотной сети требует строгой побитовой идентичности сигналов, которая не выполняется в данном случае, что препятствует успешному построению сети. Различные версии программного обеспечения сплайсеров также вносят различия во врезку локальной информации, что приводит к нарушению побитовой идентичности сигналов и дальнейшему разрушению одночастотной сети. Исследования показали отсутствие возможности найти комбинацию программных обеспечений

сплайсеров разных производителей, при которой они бы врезали рекламу в один и тот же кадр, что означает, что использование сплайсеров разных производителей в одночастотной сети DVB-T2 без изменений невозможно. Единственным решением данной проблемы является использование сплайсеров одного производителя с одной версией прошивки в каждой одночастотной зоне, чтобы обеспечить согласованность и побитовую идентичность сигналов.

Список используемых источников:

1. Федеральный закон «О связи» 7 июля 2003 г. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 20.11.2023).

2. Федеральный закон «О рекламе» 13 марта 2006 г. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_58968/ (дата обращения: 20.11.2023).

3. Воробьёв М. С. Основы цифрового телевизионного вещания : учеб. пособие. Челябинск : ЮУрГУ, 2002. 74 с.

4. Электронная библиотека SCTE https://www.scte.org/standards/library/catalog/

Verbitskiy A., Verbitskiy A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Splicers in single-frequency network.

Currently, the Russian Television and Radio Broadcasting Network (RTRN) in St. Petersburg inserts local information or advertisements with splicers from two manufacturers: ENENSYS and QUALITTEQ. Due to the current situation in the world, it is not possible to purchase equipment to service ENENSYS splicers, as this equipment is French-made. The article will investigate the joint operation of the above-mentioned manufacturers' splicers in a single-frequency network of DVB-T2 standard in order to analyze the possibility of import substitution for domestic equipment.

Key words: splicer, single-frequency network, digital tv, DVB-T2.

УДК 004.946
ГРНТИ 28.17.33

ОБЛАКО ТОЧЕК И МЕТОДЫ ЕГО ПОЛУЧЕНИЯ

Н. С. Воронин, Д. А.Татаренков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире технологии сканирования и получения 3D объектов являются ключевыми для создания точных трехмерных моделей реальных объектов, которые находят свое применение в различных отраслях, включая производство, медицину, архитектуру, искусство и многие другие. Одним из способов получения объемной модели объекта является облако точек.

облако точек, 3D-сканирование, объемное изображение

Облако точек (Point Cloud) - это набор трехмерных координатных точек, которые вместе описывают поверхность или форму трехмерного объекта в пространстве (рис. 1). Каждая точка в таком облаке представляет собой точное положение в трехмерных координатах (обычно в формате (x, y, z)), которое соответствует точке на поверхности объекта. Опционально каждой точке может также соответствовать вектор, который содержит дополнительные признаки, например, её цвет в формате RGB, интенсивность полученного сенсором сигнала и т.д.

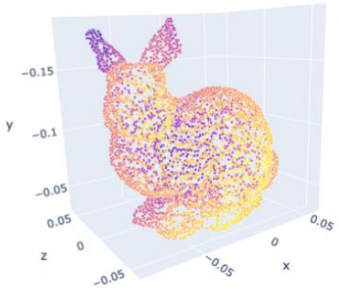


Рис. 1. Облако точек

Облака точек могут быть получены следующими методами:

- Лазерное сканирование при помощи технологии LiDAR;
- Фотограмметрия;
- Использование камер структурированного света;
- Использование время-пролетных (Time of Flight) камер;
- RGB-D камеры;
- Стереоскопические камеры;
- Kinect Fusion

1) Лазерное сканирование

LiDAR – Light Identification Detection and Ranging – это лазерные дальномеры. Данное устройство устанавливается на определенной поверхности и прибор, выпускающий лазерный луч, начинает совершать

обороты вокруг своей оси. Выпущенный световой луч отражается от поверхностей и возвращает часть света обратно [1]. Устройство принимает отраженный сигнал и определяет расстояние до объекта, измеряя время, через которое сигнал вернулся. Благодаря используемой технологии у каждой точки помимо позиции (x, y, z) будет известна ещё интенсивность. Она показывает, насколько сильным был отклик от поверхности. Данный метод предоставляет наибольшую точность в расчете расстояния до объекта, проявляет себя лучше всего на ровных поверхностях, а также отлично действует в дневное время, что говорит об отсутствии каких-либо помех от солнечных лучей.

2) Фотограмметрия

Фотограмметрия использует изображения объекта, полученные с разных ракурсов, чтобы восстановить его 3D-структуру. Это достигается путем сопоставления характерных точек на различных изображениях и анализа их геометрических отношений. Фотограмметрия может быть применена с использованием обычных цифровых камер, смартфонов и БПЛА. Для фотограмметрии обычно используют специальные конструкции со множеством камер. Камеры расположены таким образом, чтобы объект можно было запечатлеть со всех ракурсов за один подход. Затем все изображения выгружают в специальную программу, которая проверяет наложение и генерирует 3D-геометрию. Эта технология часто используется в архитектуре, археологии и создании 3D-моделей для виртуальной реальности.

3) Камеры структурированного света

Данный метод использует проекцию структурированных световых узоров на поверхность объекта. Камера регистрирует искажения узоров, и по этим данным можно восстановить 3D-форму объекта [2]. Первоначальный принцип работы данного метода заключался в том, что рядом с камерой устанавливался прожектор, который проецировал вертикальные и горизонтальные полосы на требуемый объект. Камера и прожектор были смещены относительно друг друга, из-за чего полосы, которые выпускал прожектор смещались пропорционально расстоянию до объекта. Измеряя это смещение, появлялась возможность рассчитать расстояние до объекта. С развитием технологий, глубину стали измерять при помощи ИК-проекторов, дающих псевдослучайный, т.е. вычисленный по некоторому определённому арифметическому правилу, но имеющий все свойства случайной последовательности, набор точек, по смещению которых определялась глубина в каждом пикселе.

4) Time of Flight камеры

Time of Flight камеры измеряют задержку света, то есть тот промежуток времени, который был затрачен на отправку сигнала и на подтверждение того, что сигнал был получен обратно. Измерение времени позволяет рассчитать расстояние до объекта, и, таким образом, получить облако точек. Данная технология широко применяется в смартфонах, игровых консолях,

интеллектуальных транспортных системах, в робототехнике, автоматизации производства, в системах локального позиционирования, в медицине, логистике и в других областях, где требуется определять расстояние до объекта и/или его геометрию.

5) RGB-D камеры

RGB-D камеры способны возвращать не только глубину каждого пикселя, но и его RGB значение. Используя полученные значения глубины пикселов, математическую модель камеры и RGB значения, получается создать облако точек, которое сразу содержит и информацию о цвете, что позволяет гораздо точнее обнаруживать и классифицировать различные объекты одинаковой формы или высоты.

6) Стереоскопические камеры

Эта технология основана на использовании двух камер, расположенных с некоторым расстоянием друг от друга, чтобы создать трехмерное изображение объекта. Путем сопоставления изображений, полученных каждой камерой, можно определить глубину объекта и создать 3D-модель [3]. Стереоскопическое видение часто используется в робототехнике и виртуальной реальности.

7) Kinect Fusion

Данное обновление ПО для устройства Kinect позволяет его сенсору, под управлением Windows, сканировать и создавать 3D модели объектов с высокой точностью и реалистичностью. Процесс создания модели сводится к использованию алгоритмов объединения результатов многочисленных снимков, полученных при помощи сенсора Kinect, в единый объемный объект, что позволит добиться большей детализации, чем при едином считывании изображения.

Сравнение и оценка точности двух наиболее популярных методов (LiDAR и фотограмметрия):

Для оценки точности данных методов, швейцарскими геодезистами Арминой Вебером и Томасом Лерхом был проведен эксперимент по получению облака точек гравийного карьера [4]. В данном исследовании сравнивались лазерный сканер и БПЛА, проводивший съемку объекта на различной высоте (таблица 1).

ТАБЛИЦА 1. Сравнение методов получения облака точек в ходе эксперимента

	LiDAR	БПЛА (100м)	БПЛА (150м)
Число точек	24,416,590	1,246,901	644,751
Точек/м^2	741	36	17
Время (мин)	220	20	20
Стоимость оборудования (руб)	6.9 млн.	2.5 млн.	2.5 млн.

По результатам эксперимента можно сделать вывод, что облако точек, полученное при помощи лазерного сканера имеет очень высокую плотность точек, но требует гораздо большего времени на создание объемной модели, а

также является более затратной в финансовом плане, в сравнении с БПЛА. Тем не менее, обе модели передают достаточное количество информации об объекте, что позволяет использовать полученные модели в дальнейшей работе (рис. 2).

Рис. 2. Полученные модели при помощи LiDAR (справа) и БПЛА на 100м (слева)

Облака точек предоставляют важную информацию о форме и структуре объектов и могут служить основой для создания более сложных трехмерных моделей, которые могут быть использованы в различных областях промышленности, исследований и развлечений. Методы получения облака точек предоставляют мощный инструмент для создания 3D-моделей объектов. В зависимости от конкретной задачи и доступных ресурсов можно выбрать наиболее подходящий метод сканирования. Эти технологии продолжают развиваться, и их применение будет только расширяться в будущем, улучшая методы взаимодействия с 3D-миром.

Список используемых источников:

1. Ватолин Д. Камеры глубины — тихая революция (когда роботы будут видеть) [Электронный ресурс]. URL: https://habr.com/ru/articles/458458/ (дата обращения: 16.11.2023).

2. Бучатский А. Н., Татаренков Д. А. Анализ методов 3d-сканирования, как источников вводных данных для системы распознавания лиц // Российская наука в современном мире : материалы междунар. научно-практич. конф., Москва, 21 марта 2015 г. М. : ООО «Актуальность РФ», 2015. С.178-191.

3. Поляков А. Третье измерение фотографии [Электронный ресурс]. URL: www.photo-element.ru/ps/stereo/stereo.html (дата обращения: 16.11.2023).

4. Armin Weber, Thomas Lerch «Point Clouds: Laser Scanning versus UAS Photogrammetry, Accuracy, Point Density, Time Efficiency and Costs» // GIM INTERNATIONAL, July 12, 2018 // https://www.gim-international.com/content/article/point-clouds-laser-scanning-versus-uas-photogrammetry

Voronin N., Tatarenkov D.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Point clouds and methods for obtaining it.

In the modern world, scanning and 3D object acquisition technologies are key to creating accurate 3D models of real objects, which find their application in various industries, including manufacturing, medicine, architecture, art and many others. One of the ways to obtain a three-dimensional model of an object is a point cloud

Key words: Point cloud, 3D scanning, volumetric image.

УДК 534.6.08
ГРНТИ 29.37.23

АКУСТИЧЕСКАЯ ПОДГОТОВКА СОВРЕМЕННЫХ СТУДИЙ ЗВУКОЗАПИСИ

В. П. Жиряков, С. Л. Федоров
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Важнейшей задачей при проектировании современных студий звукозаписи является акустическая подготовка помещения, обеспечивающая заданное качество записи и воспроизведения звука. В статье рассматриваются ключевые факторы, влияющие на акустические свойства помещений, а также приводятся подходы к расчету их основных акустических характеристик.

акустика помещений, реверберация, звуковой фонд, звукопоглощение

Как известно, индивидуальные акустические особенности помещения, такие как реверберация, комнатные резонансы, стоячие волны и граничные эффекты, существенно влияют на звук. В настоящее время расчет акустических параметров в малых помещениях ограничивается определением основного фонда звукопоглощения и статистическим анализом акустической ситуации с последующей корректировкой на основе измерений в готовом помещении [2].

Время реверберации представляет собой одну из основных характеристик звукового поля. Оптимальное значение времени стандартной реверберации зависит от жанра программы, объема помещения и частоты [3]. В большинстве случаев устанавливается стандартное время реверберации для частотного диапазона 125…4000 Гц. Графическое представление зависимости оптимального времени стандартной реверберации от объема помещения представлено на рис. 1.

Рис. 1. Зависимость оптимального времени стандартной реверберации на частоте 500 Гц от объема помещения

Перед тем, как приступить к реализации студии звукозаписи, разрабатывается акустический проект, который предполагает расчет требуемой частотной характеристики, времени стандартной реверберации помещения, расчет звукопоглощения, вызываемого основным фондом и расчет звукопоглощения, обеспечиваемого специальными материалами и конструкциями. Расчеты могут осуществляться посредством специального программного обеспечения.

На первом этапе определяется оптимальное значение времени стандартной реверберации, при котором акустика помещения оказывается наилучшей. Оптимальное время стандартной реверберации учитывает функциональность помещения и индивидуальные предпочтения людей, работающих в этом помещении. Типовые значения были приведены выше на рис. 1.

После определения оптимального значения времени стандартной реверберации производится расчет основного звукового фонда. Учитываются не только габариты помещения, но также предметы декора, мебель и материалы отделки, поскольку все они воздействуют на звуковые волны, отражая, поглощая и внося свои изменения [4].

На рис. 2 представлено то, как звуковые волны могут распространяться в пустом помещении и в помещении с акустическими панелями. Изображение представлено в ознакомительных целях и не является точным отражением реальных акустических процессов.

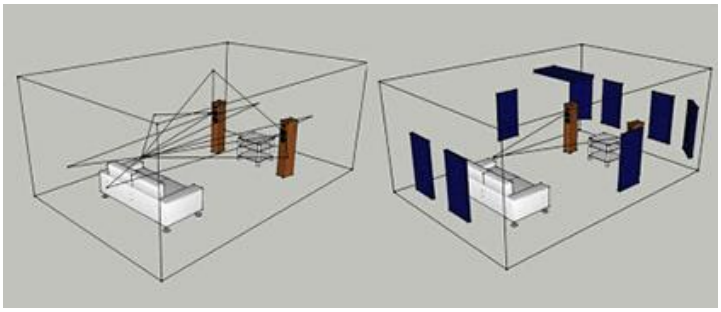


Рис. 2. Распространение звуковых волн в пустом помещении (слева) и распространение звуковых волн в комнате с использование акустических панелей (справа)

На данном этапе расчета требуется определить количество единиц звукопоглощения, вносимых материалами в помещение. Для этого коэффициент звукопоглощения материала умножается на площадь, которую он занимает [4]. Исходя из расчета основного звукового фонда, становится ясно, сколько единиц звукопоглощения необходимо добавить в помещение для достижения желаемого времени стандартной реверберации. Здесь возникает понятие «добавочное число единиц звукопоглощения».

В таблице 1 приведены примеры материалов основного звукового фонда и их коэффициенты звукопоглощения в зависимости от частоты [4].

ТАБЛИЦА 1. Зависимость коэффициентов звукопоглощения некоторых материалов основного фонда от частоты

Материал	Частота, Гц						Коэффициенты звукопоглощения
	125	250	500	1000	2000	4000	
Ковер с ворсом толщиной четверть дюйма	0,05	0,05	0,15	0,3	0,5	0,55	
Линолеум, на бетонном полу	0,02	0,02	0,03	0,03	0,04	0,04	
Деревянный паркет	0,04	0,04	0,07	0,06	0,06	0,07	
Окно	0,35	0,25	0,18	0,12	0,07	0,04	
Дверь, монолитная деревянная	0,1	0,07	0,05	0,04	0,04	0,04	
Сиденья с мягкой обивкой	0,32	0,4	0,42	0,44	0,43	0,48	
Мрамор или глазурованная плитка	0,01	0,01	0,01	0,01	0,02	0,02	

Коэффициент звукопоглощения может принимать значения в диапазоне 0 до 1, где 0 означает полное отражение звука (никакого поглощения), а 1 означает полное поглощение звука материалом (никакого отражения).

Необходимое количество единиц звукопоглощения может быть добавлено в помещение с использованием специальных звукопоглощающих материалов и конструкций, известных как абсорбенты. Эти материалы могут включать в себя разнообразные элементы, начиная от фанерных листов и заканчивая вспененным пластиком, минеральной ватой, асбеститом и т.д. Важно учитывать коэффициенты звукопоглощения этих материалов на необходимом частотном диапазоне.

Далее рассчитывается звукопоглощение, вносимое специальными абсорбентами. Если сумма единиц звукопоглощения специального фонда равна добавочному числу единиц звукопоглощения, полученному после расчета основного фонда, то задача по подбору специальных абсорбентов для помещения считается выполненной.

Сложив единицы звукопоглощения, полученные от основного фонда с звукопоглощением специального фонда получается полное звукопоглощение помещения. Полученные результаты позволяют провести расчет времени стандартной реверберации, при условии внесения в помещение специальных абсорбентов. Данное время стандартной реверберации будет соответствовать оптимальному времени стандартной реверберации в данном помещении.

Существует множество программ для акустического моделирования помещений, таких как «EASE» для больших помещений (стадионы, церкви, театры) [5], и «Ulysses» для быстрой оценки и моделирования акустических параметров. Данное программное обеспечение позволяет создать трехмерную модель помещения и разместить в нём специальные материалы. Важно отметить, что результаты звукопоглощения, полученные в процессе моделирования, могут немного отличаться от теоретических расчетов из-за ограничений моделирования. Тем не менее, экспериментальные результаты демонстрируют высокую согласованность с расчетами и моделями.

Рис. 3 иллюстрирует трехмерную модель помещения, построенного с помощью программы «EASE». На рис. 4 изображен график зависимости времени стандартной реверберации от заполняемости помещения, полученный с помощью программы «Ulysses».

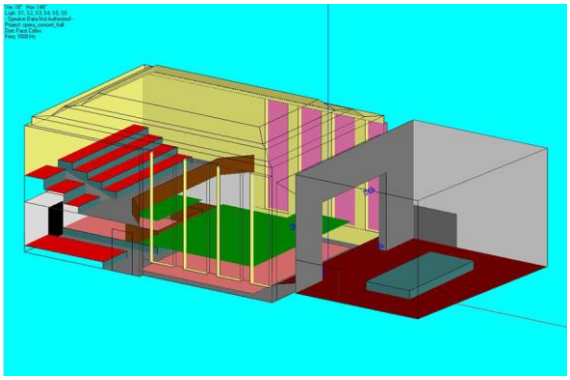


Рис. 3. Трёхмерная архитектурная модель концертного зала в программе «EASE» с указанием места расположения слушателей и акустических систем

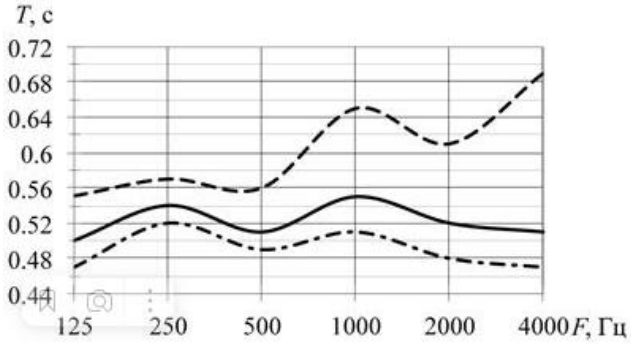


Рис. 4. Зависимость времени стандартной реверберации от заполняемости помещения исполнителями и слушателями: свободное помещение (длинный пунктир); заполненное на 2/3 (сплошная линия); полностью заполненное помещение (точка-тире)

В дальнейшем, при строительстве помещения, после проведения расчетов возникает задача правильного размещения абсорбентов. Это требует точности, чтобы обеспечить не только необходимую акустическую характеристику, но и комфортность работы и пребывания в помещении. Акустические дизайнеры сотрудничают с архитекторами и инженерами акустики для создания эффективного и удобного звукового пространства. Пример акустического дизайна студии звукозаписи приведен на рис. 5.

После завершения строительства инженеры проводят измерения акустических характеристик помещения с использованием микрофонов и анализаторов спектра. Эти данные анализируются и сравниваются с предварительными расчетами и моделированием. При необходимости вносятся коррективы с использованием дополнительных абсорбентов для достижения желаемых акустических характеристик, включая перемещение, замену или добавление материалов для оптимизации звучания помещения.

Рис. 5. Студия звукозаписи «Steve Aoki Neon Future Cave», Лас-Вегас, США

Список используемых источников:

1. Васильев И. В., Семенцов С. Г. Влияние помещения на звук [Электронный ресурс] // Молодой учёный. Международный научный журнал. 2016. N 19. С. 59–61. URL: https://moluch.ru/archive/123/33975/ (дата обращения: 13.11.2023).

2. Панфилов А. П., Тиганов Р. Е., Ведищева В. М. Оптимизация параметров акустического поля для малогабаритной студии звукозаписи [Электронный ресурс] // Вестник инженерной школы Дальневосточного федерального университета. 2022. N 1(50). С. 123–129. URL: https://doi.org/10.24866/2227-6858/2022-1/123-129 (дата обращения: 13.11.2023).

3. Исаков Ю. И. Цифровая обработка звуковых сигналов в музыкальной акустике. Электроакустическая система активного управления звуковым полем [Электронный ресурс] // Вестник музыкальной науки. 2016. N 2 (12). С 60–71. URL: https://cyberleninka.ru/article/n/tsifrovaya-obrabotka-zvukovyh-signalov-v-muzykalnoy-akustike-elektroakusticheskaya-sistema-aktivnogo-upravleniya-zvukovym-polem/viewer (дата обращения: 13.11.2023).

4. Ковалгин Ю. А., Свиньина О. А., Фадеев А. А. Расчет аппаратно-студийного комплекса телерадиовещания и аудиотехники. Часть 1. Расчет акустического оформления студий. 2013. [Электронный ресурс] URL: https://clck.ru/36Zkv2 (дата обращения: 13.11.2023).

5. Чернов К. А. Исследование акустических характеристик студии звукозаписи [Электронный ресурс] // Радиоэлектроника молодежь в XXI веке : материалы XXIII Междунар. молодежного форума. 2019. Т.3. С. 94–95. URL: https://openarchive.nure.ua/handle/document/22376 (дата обращения: 13.11.2023).

Zhiriakov V., Fedorov S.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Acoustic preparation of modern recording studios.

The most important task in the design of modern recording studios is the acoustic preparation of the room, providing a given quality of recording and sound reproduction. The article discusses the key factors affecting the acoustic properties of rooms, and also provides approaches to calculating their basic acoustic characteristics.

Key words: room acoustics, reverberation, sound foundation, sound absorption.

УДК 004.946
ГРНТИ 28.23.37

ИСПОЛЬЗОВАНИЕ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ НЕЙРОСЕТЕЙ В ПРОЦЕССЕ СОЗДАНИЯ ДИНАМИЧЕСКОГО МЕДИАКОНТЕНТА

Д. Д. Клыков, С. В. Попков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Нейронные сети, специализированные для работы с медиаконтентом, стали неотъемлемой частью этой эволюции, и они демонстрируют потенциал во множестве областей, включая генерацию изображений, аудио и видео.

нейронные сети, генерация изображений, обработка видео, обработка аудио

Современное информационное общество переживает существенные изменения в сфере создания и обработки медиаконтента. Расширение возможностей искусственного интеллекта и глубокого обучения привело к возникновению уникальных инструментов и методов, которые революционизируют создание, анализ и модификацию мультимедийных данных.

Цель настоящей статьи – это представление обзора современных нейросетей для медиагенерации и обработки медиаконтента. Рассмотрены разнообразные подходы и архитектуры, которые позволяют нейросетям создавать, улучшать и анализировать различные виды мультимедийных данных.

Медиаконтент охватывает широкий спектр форматов и типов данных, и их обработка требует уникальных решений. В данной статье был сделан упор на следующих аспектах:

1. Генерация изображений и видео: рассмотрены современные GAN-модели и другие методы, способные создавать реалистичные визуальные и аудиовизуальные контенты.
2. Синтез аудио и музыки: были рассмотрены современные TTS-модели и алгоритмы, способные генерировать аудио и музыку высокого качества.

Глава 1. Генерация видео.

GAN, или сеть генеративных антагонистов, представляет собой класс нейронных сетей, который используется для генерации данных, таких как изображения, звуки или текст, с целью создания реалистичных искусственных контентов. GAN состоит из двух основных компонентов:

1. Генератор: генератор отвечает за создание новых примеров данных. Он получает на вход случайный шум или другое начальное представление и пытается генерировать данные, которые могут быть похожи на реальные.

2. Дискриминатор: дискриминатор — это сеть, которая оценивает, насколько сгенерированные данные похожи на реальные. Он принимает как сгенерированные данные, так и реальные данные и пытается различить их.

Важной особенностью GAN является то, что генератор и дискриминатор обучаются в процессе конкуренции.

«Neural Video Generation Models» — это обобщающий термин для различных нейронных сетей, которые разработаны для генерации видеоконтента, включая последовательности изображений или видео. Эти модели используют глубокое обучение и искусственный интеллект для создания новых видео или модификации существующих.

Принцип работы Neural Video Generation Models основан на использовании нейронных сетей, которые обучаются анализировать и генерировать видеоконтент. Вот общий принцип их работы:

1. Анализ видеоданных: в начале процесса обучения или генерации нейросеть анализирует входные видеоданные. Это может быть последовательность кадров из видео, каждый кадр представлен в виде пикселей, либо предварительно обработанных признаков, извлеченных из видео.
2. Извлечение признаков: нейросеть обычно содержит слои, которые извлекают информацию и признаки из входных кадров. Это позволяет сети понимать структуру и содержание видео, включая движение объектов, цвета, текстуры и другие характеристики.
3. Генерация видеоконтента: в случае генеративных моделей, таких как GAN или VAE, сеть может использовать латентное представление для генерации нового видео, которое либо имитирует структуру и стиль входного видео, либо создает совершенно новый контент.
4. Обратное преобразование: сгенерированные признаки преобразуются обратно в видеокадры, и это создает видео, которое может быть воспроизведено.

Глава 2. Обработка звука. Распознавание и выделение.

Одной из наиболее значимых задач для нейронных сетей обработки звука является распознавание и выделение отдельных источников звука из звукового сигнала. Выделенные таким образом модели могут служить материалом для дальнейшей обработки. Такой подход используется в том числе и для удаления шумовых составляющих из звуковых сигналов.

Для выделения звуковых сигналов, и, в особенности, голоса используется многоступенчатая обработка поступающего звукового сигнала. Из сигнала, посредством анализа спектральных и динамических характеристик, выделяются первичные признаки. В спектральной области основными анализируемыми характеристиками являются:

1. Непосредственно сам частотный спектр;
2. Огибающая спектра (предварительно сглаженного);
3. Кепстр (ОБПФ от логарифма БПФ);

В качестве динамических параметров используются «дельта-параметры», представляющие собой производные по времени от основных параметров и частотно-временные зависимости, например спектрограмма.

В качестве основы для распознавания речевых сигналов используют такие лексические элементы речи, как фонемы и аллофоны. Они выделяются с помощью нейронных сетей и формируют нейронные ансамбли. Способ обучения таких нейронных может заключатся в формировании нейронных ансамблей, ядра которых соответствуют наиболее частой форме каждого лексического элементы. Формирование нейронных ансамблей представляет собой процесс обучения нейронной сети без учителя, при котором происходит статистическая обработка всех сигналов, поступающих на вход нейронной сети. При этом формируются ансамбли, соответствующие наиболее часто встречающимся сигналам. Запоминание редких сигналов происходит позже и требует подключения механизма внимания или иного контроля высшего уровня.

Для реализации нейронной сети с помощью нейронных ансамблей можно выбрать самоорганизующуюся карту признаков Кохонена. В ней для множества входных сигналов формируются нейронные ансамбли, эти сигналы представляющие. Одной из особенностей такого алгоритма является способность к статистическому усреднению, что позволяет решить проблему изменчивости речи. Легко изменяемая архитектура алгоритма позволяет быстро и эффективно адаптировать нейронную [1].

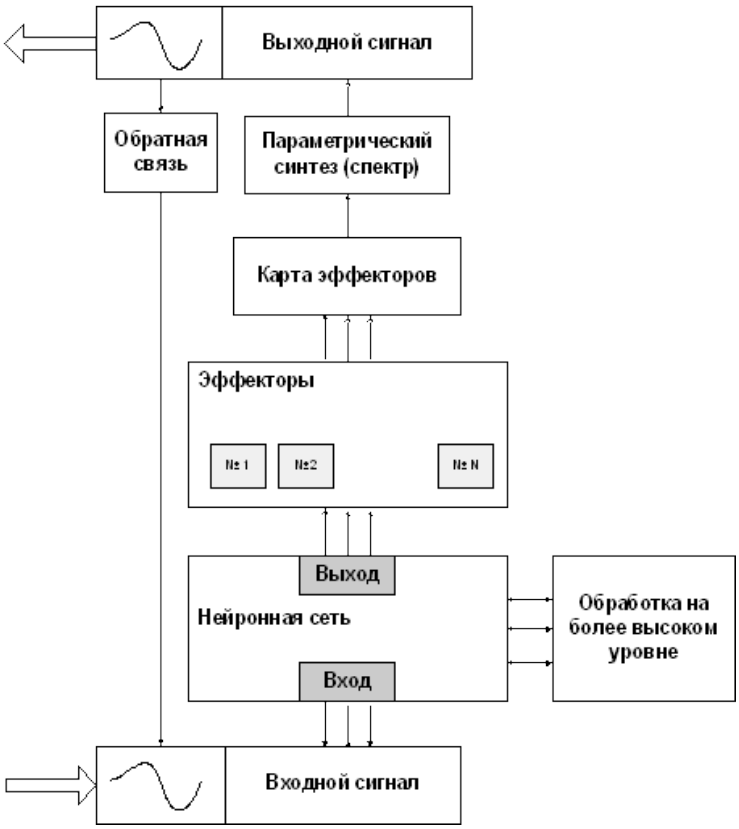


Рис. 1. Пример реализации нейронной сети обработки звука

Некоторые алгоритмы обработки звука работают не со всем спектром сигнала, а с его сжатым представлением. Дело в том, что информативность высокочастотных компонентов значительно ниже информативности низкочастотных. Поэтому, для повышения скорости и экономии ресурсов, уменьшают число входов, получающих информацию. Исходный спектр сжимается с помощью специального алгоритма, например логарифмического:

$$f_{new} = 1125 \cdot \log(0{,}0016 \cdot f + 1)$$

Вывод: таким образом, использование генеративно-сосстязательных нейросетей значительно увеличивает возможности в индустрии создания медаконтента

Список используемых источников:

1. Generative Adversarial Networks [Электронный ресурс]. URL: https://cpang4.github.io/gan/ (дата обращения: 30.10.2023).

2. Основы генеративно-состязательных сетей [Электронный ресурс]. URL: https://habr.com/ru/articles/726254/ (дата обращения: 11.11.2023).

3. Нейронная сеть Кохонена, самоорганизующиеся карты, обучение. [Электронный ресурс]. URL: https://microtechnics.ru/nejronnaya-set-kohonena-samoorganizuyushhiesya-karty-obuchenie/ (дата обращения: 14.11.2023).

4. Синтез и распознавание речи. Современные решения [Электронный ресурс]. URL: https://frolov-lib.ru/books/hi/ch05.html (дата обращения: 31.10.2023).

Klikov D, Popkov S.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Using generative adversary neural networks in the process of creation of dynamic media content.

Neural networks specialized for working with media content have become an integral part of this evolution, and they demonstrate potential in a variety of areas, including image generation, audio and video.

Key words: Neural networks, image generation, video processing, audio processing.

УДК 621.397.6
ГРНТИ 49.45.29

РАЗРАБОТКА СИСТЕМЫ IPTV

С. П. Куликов, А. И. Поляков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время в Российской Федерации наблюдается рост рынка IPTV, что делает востребованной тему разработок решений в данной области. В статье рассматривается общая структура систем IPTV и их преимущества. Дополнительно авторами статьи было предложено решение по организации системы IPTV на малом предприятии на основании конъюнктурного анализа рынка.

IPTV, VoD, NPVR, TimeShift, EPG, SMART TV, STB

Серьёзное развитие инфраструктуры сетей широкополосного доступа способствовало появлению и развитию мультисервисных сетей и как итог появлению технологии IPTV. Данная аббревиатура расшифровывается как Internet Protocol Television, то есть – «телевидение по протоколу интернета». Однако IPTV транслируется не только через сеть Интернет, для его передачи лишь используется интернет-протокол передачи данных, технология зависит не от мировой сети, а от провайдера, предоставляющего услугу. IPTV может передаваться по закрытым сетям, поддержку которых осуществляет телекоммуникационная компания. Контент IPTV хранится на сервере провайдера и передается по тому же кабелю, по которому осуществляется подключение к сети Интернет [1].

Одно из главных отличий IPTV от «классических» видов телевидения таких как кабельное, спутниковое или эфирное является интерактивность. Интерактивность заключается в возможности управления услугой и сервисами внутри неё в режиме реального времени, без обращения к оператору.

Типовые сервисы IPTV:

- Видео по запросу (Video on Demand, VoD). Пользователи могут в любой момент смотреть фильмы и получать доступ к различному контенту в сервисах, которые предоставляет провайдер.
- Запись трансляций (Network Personal Video Recorder, NPVR). Транслируемый контент пользователи могут сохранять на сервере, в памяти персонального компьютера или на флеш-карте.
- Пауза и перемотка (TimeShift). Видео можно перематывать вперед или назад, ставить на паузу, а потом продолжать просмотр с того же момента.

То есть зритель фактически становится независим от сетки вещания и уже не обязан просматривать не интересующий его контент в ожидании нужного.

Кроме того, в IPTV присутствует электронный телегид. Это подробная информация о каждой телепередаче или фильме, в которой содержатся описание телепрограммы или фильма, время начала, длительность и прочая информация о передаче.

Для получения IPTV требуется программное обеспечение, задача которого – обработка получаемых данных. В определённом классе телевизоров это реализовано при помощи технологии SMART TV, но чаще применяется отдельное специальное устройство – IPTV приставка (STB - Set Top Box). [2]

Описанная выше компоновка системы подходит только для конечного потребителя. Если систему IPTV необходимо организовать на конкретном объекте (к примеру отель, или какое-либо предприятие), требуется специализированное оборудование. Для приёма сигналов спутникового и цифрового эфирного телевидения стандартов DVB-S/S2 и DVB-T2 требуются спутниковая антенна со спутниковым приёмником и эфирная антенна с усилителем для приёма сигналов эфирного телевидения. Преобразование спутниковых и эфирных сигналов в IP-поток выполняет цифровая приёмная станция. Маршрутизацию потоков выполняет коммутатор.

На текущий момент отсутствует унифицированная схема системы IPTV для малых предприятий. Целью данной статьи является подбор наиболее оптимальной схемы построения системы IPTV и выбор подходящего оборудования, присутствующего на рынке.

Проведя сравнительный анализ, основными критериями которого были стоимость оборудования и его функциональные возможности, было выбрано следующее оборудование:

- Спутниковая антенна Супрал-СТВ 2,4;
- Спутниковый конвертер Galaxy Innovations GI-302;
- Приёмник спутникового сигнала HARMONIC PROVIEW 8105;
- Эфирная антенна Rexant RX-413;
- Усилитель для эфирной антенны SEAS 4020;
- Цифровая приёмная станция NetUp Streamer 8X;
- Коммутатор 3 уровня Eltex MES 3324;
- Источник бесперебойного питания ИДП 1-1/1-3-220 ТА;
- В качестве абонентского устройства (устройство STB) была выбрана приставка NV-730.

Спутниковая антенна Супрал СТВ 2,4 имеет компоновку офсет и предназначена для приёма сигналов спутникового телевидения стандартов DVB-S/S2 с геостационарных спутников как в Ku-диапазоне (10.95-12.75ГГц), так и в С-диапазоне (3.6-4.2ГГц) в зависимости от применяемого облучателя. Облучатель Galaxy Innovations GI-302 круговой поляризации позволяет подключить до двух независимых спутниковых приёмников.

Активная эфирная антенна Rexant RX-413 предназначена для приёма сигналов эфирного телевидения стандарта DVB-T2. Питание антенны и усиление принятого сигнала осуществляется усилителем SEAS 4020.

Спутниковый приёмник HARMONIC PROVIEW 8105 принимает и обрабатывает сигнал от спутниковой антенны, преобразует T2-MI в MPEG-TS и передаёт его на входные интерфейсы цифровой приёмной станции NetUp Streamer 8x.

Цифровая приёмная станция NetUp Streamer 8x принимает сигналы спутникового и цифрового эфирного телевидения, разделяет транспортные потоки на потоки отдельных сервисов с последующим формированием IP-потоков и их трансляцию в сеть. Дешифровку платных спутниковых каналов обеспечивает модуль условного доступа со смарт-картой. Модули условного доступа устанавливаются в слоты PCMCI цифровой приёмной станции. Данная цифровая приёмная станция обеспечивает трансляцию IPTV для 512 абонентов.

С выхода цифровой приёмной станции IP-потоки поступают на коммутатор 3 уровня Eltex MES 3324. Коммутатор имеет 24 порта Ethernet и пропускную способность до 128 Гбит в секунду

К коммутатору подключены устройства абонентские устройства NV-730.

Число абонентов можно увеличить, если подключать абонентские устройства не напрямую к центральному коммутатору (Eltex MES 3324), а к коммутаторам доступа, которые в свою очередь будут подключены к центральному коммутатору.

Унифицированная предложенная схема построения IPTV системы для малого предприятия представлена на рис. 1.

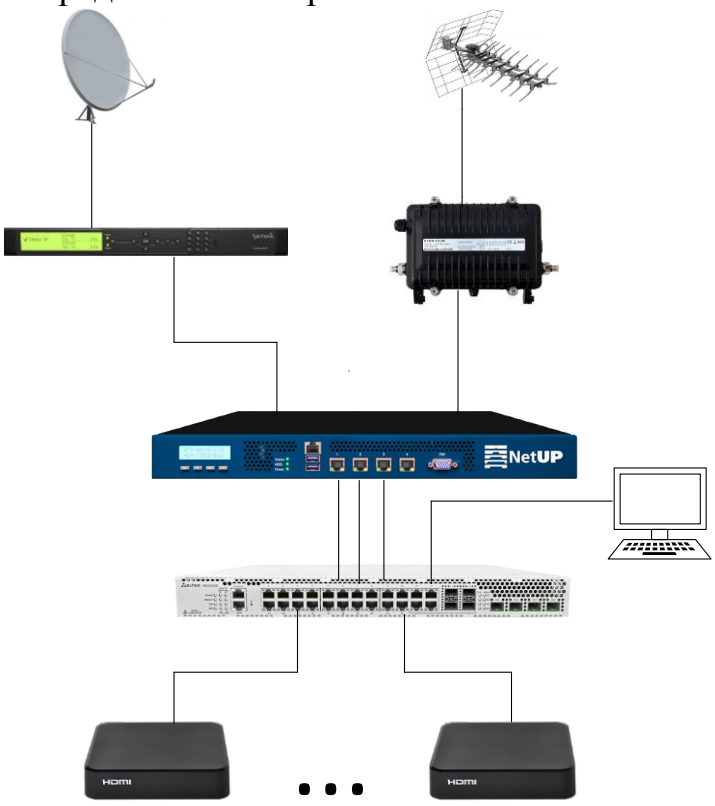


Рис. 1. Структурная схема разработанной системы IPTV

Список используемых источников:

1. HELLOWORLD.RU - документация и книги по программированию [Электронный ресурс]. URL: https://www.helloworld.ru/texts/comp/inet/ip/ip/glava_2.htm (дата обращения: 15.11.2023)
2. Барсков А. Г. ТВ в сетях IP // Сети и системы связи. 2004. N 11.

Kulikov S., Polyakov A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

IPTV system development.

Currently, the world is experiencing growth in the IPTV market, which is a popular topic for developing solutions in this area. This article discusses the general structure of IPTV and the implementation option for an IPTV system.

Key words: IP, satellite, broadcasting.

УДК 621.397.422.2
ГРНТИ 49.40.37

АНАЛИЗ ВОЗМОЖНОСТЕЙ КАМЕР SONY И CANON ДЛЯ ОСУЩЕСТВЛЕНИЯ ЦВЕТОКОРРЕКЦИИ ИЗОБРАЖЕНИЙ

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

Знание параметров видеокамер помогает выбирать наиболее подходящие устройства для конкретных целей, оценивать качество получаемого изображения, а также выявлять потенциальные ограничения и возможности видеокамер. Изучение характеристик видеокамер имеет большое значение для специалистов в сфере кино и телевидения, операторов, монтажеров, продюсеров, занимающихся производством видеоконтента, которое помогает им лучше понять возможности и ограничения разных видов видеокамер и принимать обоснованные решения при выборе аппаратуры для съемки и обработки видеоматериалов. Также будет полезно начинающим пользователям и любителям фотосъемок заняться данной деятельностью.

Цветокоррекция играет значительную роль в создании высококачественных и эстетически привлекательных изображений, поскольку она позволяет улучшить цвета, контрастность и яркость изображения, делая его более качественным.

методы цветокоррекции, камеры, изображения, гамма-кривые, метрики, Sony, Canon

В работе будут рассмотрены три камеры, широко используемые в настоящее время профессиональными фотографами и видеографами.

Sony FX-3 Cinema Line - это полнокадровая беззеркальная видеокамера, которую выпустила компания Sony в 2021 году (рис. 1). Она обеспечивает высокое качество изображения и звука, а также удобство использования и портативность [1].

Рис. 1. Видеокамера Sony FX-3 Cinema Line

Sony Alpha 7 III — это беззеркальная камера с полнокадровым сенсором (рис. 2), выпущенная в 2018 году, оснащена полнокадровым сенсором изображения, который обеспечивает превосходную детализацию и цветопередачу. Быстрый и точный автофокус позволяет камере Sony a7 III

поддерживать 693-точечную систему автофокусировки, которая может быстро и точно фокусироваться на объектах в различных условиях [2].

Рис. 2. Видеокамера Sony Alpha 7 III

Canon EOS 600D — это цифровая однообъективная зеркальная камера (DSLR), выпущенная Canon в 2011 году, представлена на рис. 3. Она оснащена 18-мегапиксельным APS-C CMOS-датчиком, 9-точечной системой автофокусировки, 3,0-дюймовым ЖК-экраном с переменным углом наклона и возможностью записи видео Full HD [3].

Рис. 3. Видеокамера Canon EOS 600D

Существует множество настроек и встроенных методов цифровой обработки, которые можно использовать для улучшения изображений, формируемых камерой. Вот некоторые из наиболее распространенных:

1. Настройка баланса белого. Баланс белого - это регулировка цветовой температуры изображения, чтобы оно выглядело естественно. Это можно сделать вручную, выбирая точку белого в изображении, или автоматически.
2. Настройка яркости и контрастности. Яркость и контрастность - это основные настройки, которые влияют на общее впечатление от изображения. Яркость регулирует общий уровень света в изображении, а контрастность регулирует разницу между светлыми и темными областями.
3. Настройка насыщенности. Насыщенность регулирует интенсивность цвета в изображении. Более высокая насыщенность означает более яркие цвета, в то время как более низкая насыщенность означает более приглушенные цвета.

4. Коррекция кривых. Кривые позволяют регулировать яркость и насыщенность отдельных цветовых каналов [4].

Изображения, полученные при работе камеры Canon с разными настройками баланса белого, представлены на рисунках ниже.

Рис. 4. Баланс белого для авторегулировки на основе освещения для естественных цветов

Рис. 5. Баланс белого для сцен вне помещения при ясном небе

Рис. 6. Баланс белого для снимков в тени

Рис. 7. Баланс белого для сцен в помещении при свете ламп накаливания

Рис. 8. Баланс белого для сцен в помещении при свете флуоресцентных ламп

Камеры Sony позволяют пользователю корректировать гамма-характеристику, рассмотрим этот процесс подробнее. S-Log2 и S-Log3 – это две гамма-кривые, которые предназначены для съемки в более широком динамическом диапазоне. S-Log3 позволяет лучше воспроизводить характеристики градации оттенков в тенях и среднем тональном диапазоне по сравнению с S-Log2 (рис. 9). Эти характеристики ближе к характеристикам отсканированной пленки [5].

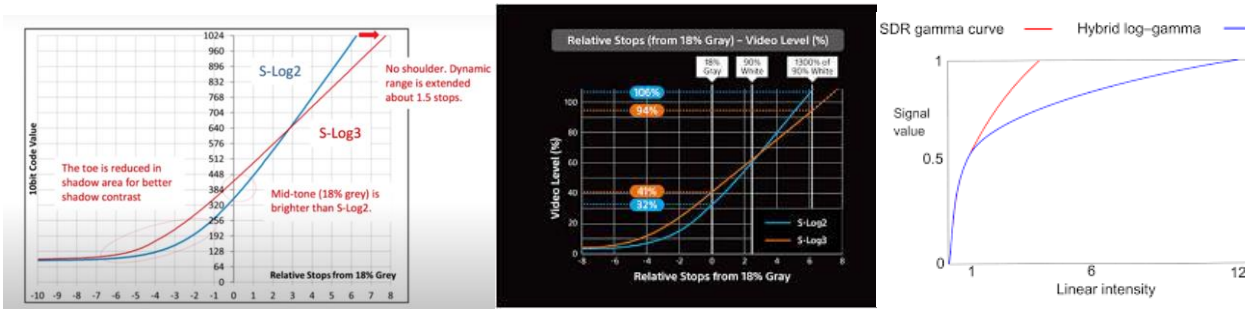


Рис. 9. Гамма-характеристики S-Log2 и S-Log3, профиль Hybrid Log-Gamma (HLG) и стандартный динамический диапазон (SDR)

При обработке кадров, снятых с использованием формата S-Log, необходимо провести обязательную цветокоррекцию, таким образом, имеется больше возможностей улучшить готовый материал.

Профили изображений Sony разработаны для упрощения процесса цветокоррекции. Они сохраняются в виде 3D LUT-файлов (таблиц преобразования) и используются для преобразования материалов, записанных в формате S-Log.

Профиль Hybrid Log-Gamma, или HLG, обеспечивает мгновенное создание контента в формате HDR (высокий динамический диапазон). Материалы, снятые с использованием этого режима, выглядят реалистично без дополнительной цветокоррекции. Поскольку HLG поддерживается всеми мониторами, такие видео могут быть воспроизведены на экранах как со стандартным (SDR), так и с высоким динамическим диапазоном (HDR).

Качество изображения оценивается как степень подобия оригиналу. Но оценка, выполняемая экспертами, носит субъективный характер. Среди объективных методов оценки качества изображения наиболее широко используются две метрики: PSNR и SSIM. PSNR (Peak Signal to Noise Ratio) — это метрика, которая измеряет, насколько близко искаженное изображение к исходному. Значение метрики вычисляется как отношение пикового сигнала исходного изображения к пиковому сигналу шума. Чем выше значение PSNR, тем лучше качество изображения. SSIM (Structural Similarity Index Measure) — это метрика, которая измеряет, насколько похожи два изображения с точки зрения человеческого зрения. Значение метрики вычисляется на основе трех характеристик изображения: яркости, контраста и структуры. Чем выше значение SSIM, тем больше два изображения похожи

с точки зрения человека [6]. В таблице 1 приведены значения метрик PSNR и SSIM для рассмотренных ранее изображений.

ТАБЛИЦА 1. Сравнительная оценка изображений с помощью метрик PSNR и SSIM и субъективной оценки качества Q

Изображение	PSNR	SSIM	Q, баллы
1	0,5452	0,3154	4
2	0,5457	0,3558	4
3	0,5482	0,4648	5
4	0,1481	0,1579	2
5	0,3845	0,2419	3

Таким образом, анализируя полученные результаты, следует отметить достаточно невысокую степень корреляции объективных и субъективных методов оценки качества для рассматриваемых изображений. Также в дальнейшем планируется рассмотрение других цветовых характеристик для изображений, в частности с использованием камер Sony.

Список используемых источников:

1. ILME-FX3. Камеры со сменной оптикой. Sony Россия [Электронный ресурс]. URL: https://www.sony.ru/interchangeable-lens-cameras/products/ilme-fx3 (дата обращения: 14.11.2023).

2. Камера Alpha 7 III с 35-миллиметровой полнокадровой матрицей ILCE-7M3/ILCE-7M3K [Электронный ресурс]. URL: https://www.sony.ru/interchangeable-lens-cameras/products/ilce-7m3-body-kit (дата обращения: 14.11.2023).

3. Инструкция по эксплуатации: CANON INC. 2011. – 30-2 Shimomaruko 3-chome, Ohta-ku, Tokyo 146-8501, Япония, Европа, Африка и Ближний Восток CANON EUROPA N.V. PO Box 2262, 1180 EG Amstelveen, Нидерланды. С. 2.

4. Цветокоррекция: что это и зачем нужна. Медиа Contented [Электронный ресурс]. URL: https://media.contented.ru/glossary/tsvetokorrektsiya/ (дата обращения: 14.11.2023).

5. S-Log, HLG, и почему их следует использовать в кино [Электронный ресурс]. URL: https://community.sony.it/t5/otkroy-dlya-sebya-sony/s-log-hlg-i-pochemu-ih-sleduet-ispolzovat-v-kino/ba-p/2678358 (дата обращения: 14.11.2023).

6. PSNR и SSIM или как работать с изображениями под C [Электронный ресурс]. URL: https://habr.com/ru/articles/126848/ (дата обращения 14.11.2023).

Mamonov M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Analysis of the capabilities of SONY and CANON cameras for image color correction

Knowing the parameters of video cameras helps to choose the most suitable devices for specific purposes, evaluate the quality of the resulting image, as well as identify potential limitations and capabilities of video cameras. Studying the characteristics of video cameras is of great importance for specialists in the field of cinema and television, operators, editors, producers involved in the production of video content, which helps them better understand the capabilities and limitations of different types of video cameras and make informed decisions when choosing equipment for shooting and processing video materials. It will also be useful for novice users and lovers of photography to engage in this activity.

Color correction plays a significant role in creating high-quality and aesthetically attractive images, because it allows you to improve the colors, contrast and brightness of the image, making it more qualitative.

Key words: color correction methods, cameras, images, gamma curves, metrics, Sony, Canon.

УДК 004.923
ГРНТИ 47.63.31

ТЕХНОЛОГИИ ПОСТРОЕНИЯ ИММЕРСИВНОГО ПРОСТРАНСТВА

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

Иммерсивные технологии — это совокупность методов, обеспечивающих погружение в виртуальный мир, который можно воспринимать через привнесенный виртуальный контент или превратив окружающий мир в виртуальную среду с помощью суперинтерактивного визуального оформления. Иммерсивные технологии позволяют увидеть недостижимые для пользователя объекты, в любой удобный момент времени. Уже сейчас погружение настолько увлекает, что невозможно отличить реальный мир от представленного. В статье рассматриваются методы создания иммерсивного пространства.

иммерсивность, VR, AR, MR

Виртуальная реальность (VR) – это искусственная среда, генерируемая компьютером, в которой имитируется реальная среда [1]. Помимо того, что виртуальная реальность сразу же получила признание в мире компьютерных игр, в настоящее время она используется во многих сферах жизни, включая архитектуру, медицину, военное дело и авиацию.

Существует три основных типа технологий виртуальной реальности. В первом случае используются шлем, наушники и пара специальных перчаток или джойстиков.

Во втором случае используются видеокамеры. Камеры отслеживают изображение участника в искусственно созданном виртуальном мире. Участник может даже перемещать объекты в этом мире, используя виртуальные технологии. И в третьем, используются трехмерные изображения. Для погружения используется экран, который имеет криволинейную форму, это позволяет максимально приблизить восприятие участника к реальному миру.

Преимущества виртуальной реальности заключаются в предоставлении различных типов данных в мгновенных формах, представление изображения с различных точек зрения, возможность представить данные недоступные в реальном мире, посещение недоступных для пользователя мест, предоставление опыта, который можно повторять и пересматривать [2].

Ограничения виртуальной реальности в том, что она создает только искусственный мир и не может взаимодействовать с объектами реального мира, при использовании в взаимодействии двух пользователей обесценивается важность человеческой связи и самое главное виртуальная реальность жестка и ей не хватает гибкости.

Другой вид реальности – дополненная (AR) – это интеграция цифровой информации с пользовательским окружением в режиме реального времени

[4]. Она добавляет графику, звук, обратную связь и запах к существующему миру. Проще говоря, это виртуальные объекты, наложенные на реальную среду в дополненной реальности.

Дополненная реальность в основном делится на четыре различные категории. Первая категория на основе маркеров. Она использует интерфейсы, такие как камера, для получения результата при обнаружении маркера считывателем. Вторая категория на основе реальности без маркеров, которая представлена на рис. 1.

Рис. 1. Дополненная реальность

Устройство использует GPS, цифровой компас, акселерометр, встроенные в устройство для предоставления данных на основе местоположения пользователя. Третья на основе проекции. Подразумевает под собой проецирование искусственного света на объекты реального мира, тем самым изменяя визуальные характеристики объекта, с которым взаимодействует. И последняя категория основана на наложении. Данный вид частично или полностью заменяет исходный вид объекта новым дополненным видом этого же объекта.

Дополненная реальность, в отличие от виртуальной реальности, более интерактивна по отношению к реальному миру, что открывает больше возможностей для применения обычными пользователями. Ограничения дополненной реальности заключаются в нескольких моментах. При её использовании разработчики производят наложение новых слоёв на реальный мир и это может привести к различию физическому несоответствию. Основная проблема в дополненной реальности — это контроль конфиденциальности.

Смешанная реальность (MR) – это сочетание лучшего в VR и AR. MR не просто накладывает, но и привязывает виртуальные объекты к объектам реального мира и позволяет пользователю взаимодействовать с комбинированными объектами [5]. Проще говоря, смешанная реальность – это тип гибридной системы, которая включает в себя как физические, так и виртуальные элементы.

Смешанная реальность выделяется высокоинтерактивным аспектом и реалистичной визуализацией проекции (рис. 2), которые добавляются к

нашему окружению. Вместо того, чтобы полагаться исключительно на пульты дистанционного управления или экраны телефонов, можно взаимодействовать с захватывающим контентом, используя естественные жесты тела и пальцев.

Недостатки смешанной реальности в основном заключаются в её требованиях. Стоимость оборудования слишком высока. Для использования требуется высокотехнологичное оборудование, и квалифицированная техническая команда, которая сможет реализовать проект.

Рис. 2. Интерактивное управление

Для погружения пользователя в иммерсивное пространство используются очки виртуальной реальности. В самом простейшем случае формируются два изображения для левого и правого глаза (рис. 3).

Рис. 3. Очки виртуальной реальности

Для формирования многоракурсного изображения (видео 360º) используются несколько камер (рис. 4). При выводе на дисплей будь то очки виртуальной реальности или просто телефон при перемещении телефона относительно осей пространства, возможно наблюдать событие и окружение, запечатлённое на видео, с разных углов.

Рис. 4. Съемка объемного видео на спортивных мероприятиях

И последняя технология, которая активно набирает популярность это иммерсивный световой дисплей (рис. 5). В данном случае может использоваться изогнутый экран или стены, на которые осуществляется проекция изображения. За счет высокого качества видеоконтента и размера видимой картинки «вылезающей» за поле зрения, происходит погружение пользователя в иммерсивное пространство.

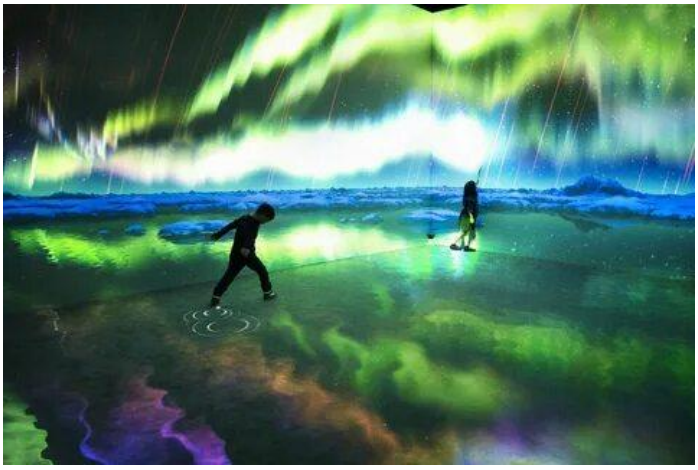


Рис. 5. Иммерсивный световой дисплей

Стандарт MPEG Immersive vide (MIV) был разработан для поддержки сжатия иммерсивного видеоконтента, в котором реальная или виртуальная 3D-сцена снимается несколькими реальными или виртуальными камерами. MIV обеспечивает хранение и распространение иммерсивного видеоконтента по существующим и будущим сетям для воспроизведения с 6 степенями свободы положения и ориентации [3]. Область применения MIV определяет синтаксис, семантику и процессы декодирования для иммерсивного видео. Он обеспечивает поддержку воспроизведения 3D-сцены в ограниченном диапазоне положений и ориентаций для просмотра.

Рассмотрев все методы формирования иммерсивных пространств можно подытожить, что AR добавляет цифровые элементы в реальный мир, VR

погружает пользователей в полностью цифровую среду, MR сочетает элементы AR и VR для создания гибридного опыта.

Технологии VR, AR и MR довольно сложны и отличаются друг от друга, но они быстро развиваются в нынешнее время и все больше привлекают внимание. Благодаря погружению в виртуальные миры пользователи могут испытывать невероятно сильные эмоции, что ещё больше подогревает интерес к данным технологиям.

Список используемых источников:

1. Jennett C., Cox A. L., Cairns P., Dhoparee S., Epps A., Tijs, T., & Walton A. Measuring and defining the experience of immersion in games. International journal of human-computer studies, 66(9), 641-661. 2008.

2. Robertson G. G., Card S. K., & Mackinlay J. Three views of virtual reality: nonimmersive virtual reality. 1993.

3. Ott M., & Pozzi F. ICT and Cultural Heritage Education: Which Added Value?. In Emerging Technologies and Information Systems for the Knowledge Society (pp. 131-138). Springer Berlin Heidelberg. 2008.

4. Логун К. А., Рощупкина И. В. Бизнес-сценарии использования технологий расширенной реальности на современных производственных предприятиях // Организатор производства. N 4. 2020. [Электронный ресурс] URL: http://cyberleninka.ru/article/n/biznes-stsenarii-ispolzovaniya-tehnologiy-rasshirennoy-realnosti-na-sovremennyh-proizvodstvennyh-predpriyatiyah (дата обращения^ 23.10.2023).

5. Hiren Kanani. What is the difference between AR, VR and MR? [+Use Cases]. 2022. [Электронный ресурс] URL: https://pluto-men.com/what-is-the-difference-between-ar-vr-and-mr/ (дата обращения 25.10.2023).

Minaev N.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

Immersive Reality technologies.

Immersive technologies are a set of methods that provide immersion in the virtual world, which can be perceived through the introduced virtual content or by turning the surrounding world into a virtual environment with the help of super—interactive visual design. Immersive technologies allow you to see objects that are inaccessible to the user, at any convenient time. Even now, immersion is so fascinating that it is impossible to distinguish the real world from the presented one.

The article discusses the methods of creating an immersive space.

Key words: immersive, VR, AR, MR.

УДК 504.064.36
ГРНТИ 81.81.17

СИСТЕМА МОНИТОРИНГ И КОНТРОЛЯ ОДНОЧАСТОТНОЙ СЕТИ В ЦЭТВ

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

Для обеспечения бесперебойной и качественной трансляции сигналов цифрового эфирного телевиденья необходим постоянный контроль за одночастотной сетью. Для этого необходимо ввести в эксплуатацию систему контроля одночастотной сети с постоянным мониторингом и удалённым доступом к ней.

телевизионная станция, зона охвата телевизионной станции, пересечение зон охвата телевизионных станций, одночастотная сеть, система контроля одночастотной сети.

Одночастотная сеть — это совокупность цифровых передатчиков, территориально расположенных для гарантированного покрытия зон обслуживания, работающих в синхронном режиме по частоте и времени.

Корректная работа одночастотной сети возможна только при выполнении определённых условий, суть которых заключается в синхронизации вещания передатчиков. Передатчики должны выдавать в эфир один и тот же сигнал в одно и то же время. Это достигается за счет использования специальной информации, вставляемой в поток данных, называемый пакетом инициализации (MIP), который вставляется с помощью специального маркера в транспортный поток MPEG-2. Чтобы синхронизовать выход в эфир телевизионного сигнала каждого передатчика используется синхронизация частотой 1 Гц (1PPS, 1 импульс в секунду) принимаемого приёмниками GPS/ГЛОНАСС. Этот сигнал синхронизации попадает в модулятор на приёмной и в шлюз T2 передающей стороне. Благодаря этому становиться возможным синхронно выдавать в эфир сигнал на всех передатчиках на одной частоте.

Рис. 1. Схема распределения MIP в одночастотной сети DVB-T2

Система контроля и мониторинга одночастотной сети должна состоять из усовершенствованного ресивера ЦЭТВ с веб-интерфейсом, встроенным осциллографом для измерения принимаемого сигнала и возможность удаленного мониторинга нескольких транспортных поток одновременно как показано на рис. 2.

Также данная система должна отслеживать следующие параметры сигнала:

1. Уровень C/N
2. Уровень Eb/N0
3. Запас устойчивости сигнала
4. Log(BER)
5. Log(PER)

Рис. 2. Веб-интерфейс системы мониторинга

Данная система необходима для:

1. Выявления нарушение в работе одночастотной сети.
2. Обнаружения ошибок в распространении, доставке или структуре сигнала.
3. Мониторинга качества вещания цифрового ТВ сигнала.
4. Мониторинг частотного диапазона с помощью осциллографа.
5. Мониторинг параметров сигнала.

На рис. 4 отражена зона охвата телевизионной станции передатчиков. В Ленинградской области в настоящий момент действуют 6 одночастотных зон цифрового эфирного телевизионного вещания (рис. 3).

Рис. 3. Одночастотные зоны DVB-T2 Ленинградской области

На рис. 4 отражена зона охвата телевизионной станции г. Санкт-Петербург. На рис. 5 отражена зона охвата телевизионной станции г. Кировск.

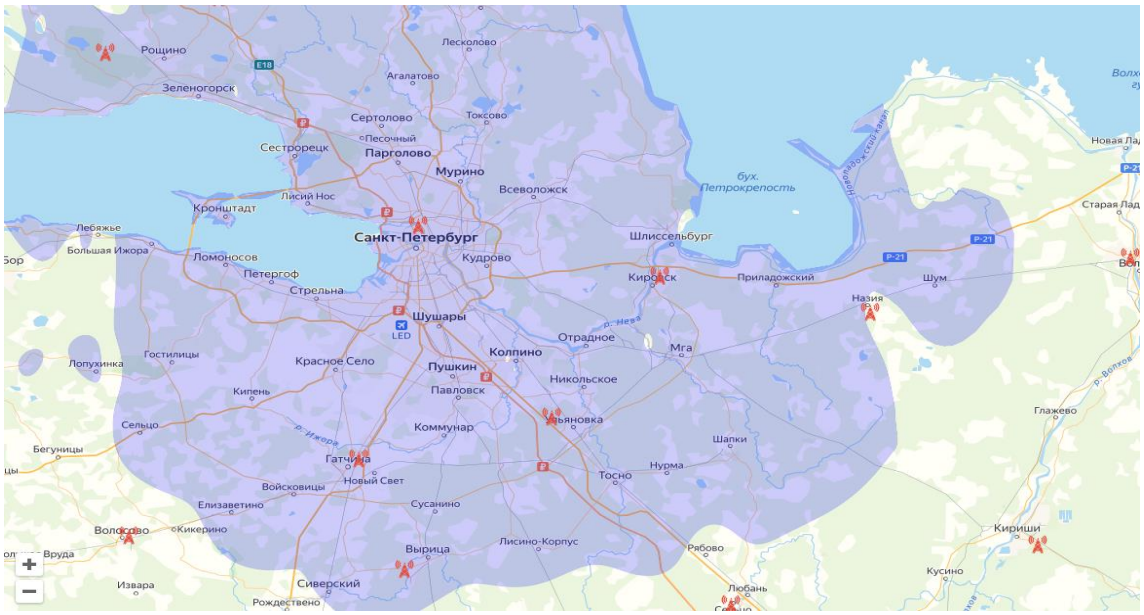


Рис. 4. Зоны охвата телевизионной станции Г. Санкт-Петербург

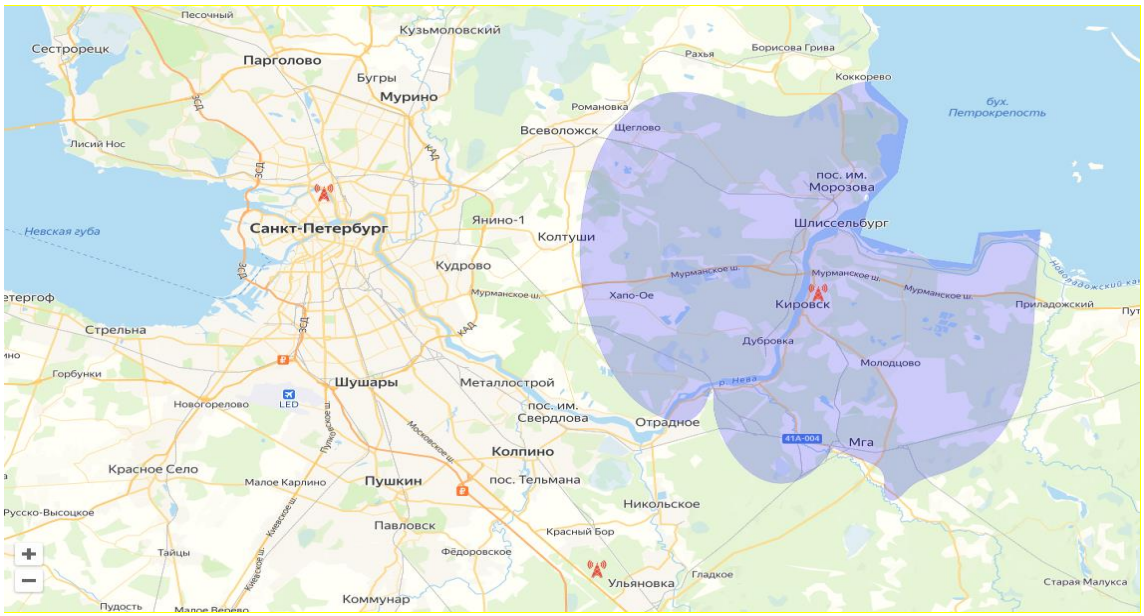


Рис. 5. Зоны охвата телевизионной станции г. Кировск

В данном случае для установки системы контроля и мониторинга одночастотной сети необходимо выбрать месторасположение, в котором сигналы на приёмы с нескольких телевизионных станций в данной сети будет равны в месте приёма.

При проведении измерений уровня сигнала, наилучшем местом при данных условиях оказался поселок Молодцово (рис. 6). В данном местоположении уровни сигналов от телепередающих станций г. Санкт-Петербурга и г. Кировск была равна 70-80 дБ. В данном местоположении необходимо установить станцию контроля одночастотной сети и мониторинга. Для данной станции необходима всенаправленная (круговая) антенна (рис. 7) расположенная на высоте 10м и выше для уверенного приёма сигнала.

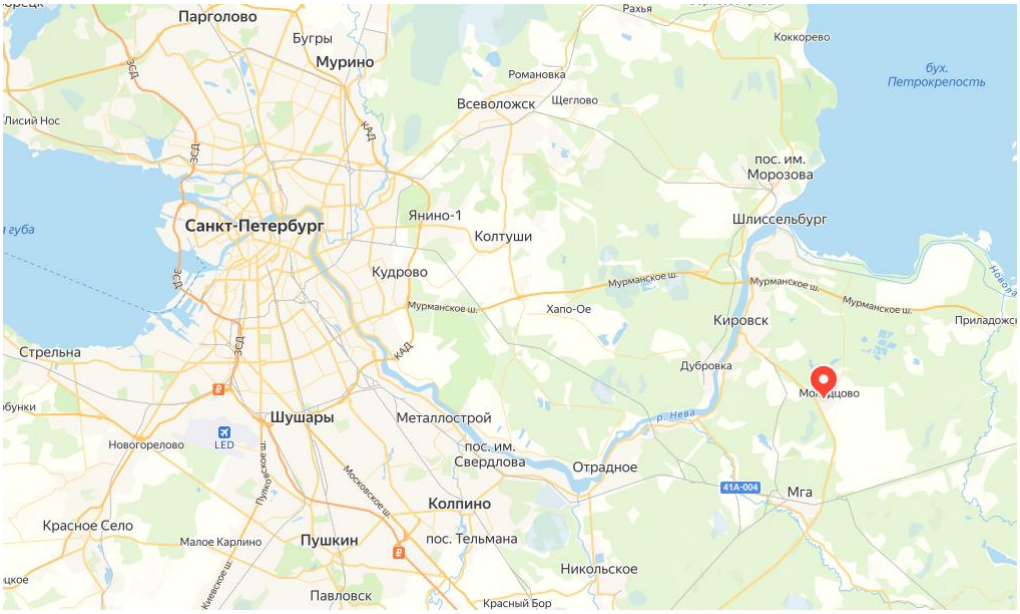


Рис. 6. Месторасположения станции контроля одночастотной сети.

Рис. 7. Всенаправленная (круговая) антенна

С помощью данной системы возможно моментально выявить неисправность работы одночастотной сети и незамедлительно начать аварийно-восстановительные работы для обеспечения бесперебойной и качественной трансляции цифрового эфирного телевиденья.

Список используемых источников:

1. Коржихин Е. О. Особенности построения одночастотных сетей в новом стандартецифрового вещания DVB-T2. [Электронный ресурс]. URL: https://tvs-mtuci.ru/attachments/article/36/Osobennosti%20postroenija%20odnochastotnyh%20setej%20v%20novom%20standarte%20cifrovogo%20veshhanija%20DVB-T2.pdf (дата обращения: 4.11.2023).

2. Рэдмонд Р. Одночастотные сети. Аспекты и практическое применение [Электронный ресурс] // GatesAir. 2011. (дата обращения: 4.11.2023).

Popov A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

System for monitoring and control of single frequency network in digital tv.

To ensure uninterrupted and high-quality transmission of digital terrestrial television signals, constant monitoring of a single-frequency network is required. To do this, it is necessary to put into operation a single-frequency network monitoring system with constant monitoring and remote access to it.

Key words: television station, coverage area of a television station, intersection of coverage areas of television stations, single-frequency network, single-frequency network control system.

Секция 2.2.
Подвижная связь и радиодоступ

УДК 621.396
ГРНТИ 32.99

АНАЛИЗ ГОРОДСКИХ СВЯЗЕЙ И ПОКРЫТИЯ С ИСПОЛЬЗОВАНИЕМ ТРАССИРОВКИ ЛУЧЕЙ

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

Несомненно, сети пятого поколения, или 5G, обещают революционные изменения в области подвижной связи. Они предоставят возможность передачи данных с гораздо большей скоростью, что позволит пользователям загружать и скачивать контент мгновенно, стримить видео высокого качества, играть в онлайн-игры без задержек и пр. При этом, 5G сети будут поддерживать большое количество одновременных подключений, что необходимо для управления растущим количеством устройств интернета вещей (IoT) - умных домов, автомобилей, городской инфраструктуры и т.д. Непрерывный рост потребностей пользователей и плотности сетей являются проблемами для существующих сетей подвижной связи, изначально не рассчитанных на работу в новых условиях. Для решения данных задач перспективные сети 5G должны обеспечить существенные прирост пропускной способности, надёжности соединения и снижение сетевых задержек. Трассировка лучей, являющееся одним из основных векторов развития сетей подвижной связи пятого поколения, требует применения моделирования и прогнозирования поведения лучей для анализа каналов связи и зон покрытия в городской среде.

сверхплотные сети, SBR, ray tracing, прямая видимость

Важным отличием сетей подвижной связи пятого поколения от существующих на сегодняшний день является их ориентированность на работу в условиях сверхплотного территориального распределения сот, вследствие перехода в диапазон миллиметровых волн. Увеличение частоты пагубно влияет на проникновение и дальность распространения волн, что приводит уплотнению сети. Обеспечение заданных параметров качества соединения в этой ситуации заметно затрудняется. Решением данной проблемы может выступать анализ пути распространение лучей радиосвязи, - Визуализация покрытия с помощью метода трассировки лучей направленных и отражающихся лучей (SBR) с различным количеством отражений, дифракций и выпущенных лучей, оптимизация связи вне прямой видимости с помощью управления лучом и Phased Array System Toolbox™.

В основе лежит моделирование в программном комплексе *Matlab* для определения направленности распространения лучей. Моделирование распространения позволяет нам оценить силу сигналов на основе системных параметров, таких как частота, свойства ландшафта и свойства создания. Теоретические и эмпирические модели оценивают потерю на пути на основе области значений и допустимы только для тех сред. В связи с чем мы можем прогнозировать распространение лучей.

В программном комплексе *Matlab* используются RayTracing объекты — это модели распространения, которые вычисляют пути распространения с использованием трехмерной геометрии среды. Предстаставление модели трассировки лучей с помощью RayTracing объекта.

Эта модель трассировки лучей:

1) Допустима в диапазоне от 100 МГц до 100 ГГц.

2) Вычисляет несколько путей распространения. Другие модели распространения вычисляют только отдельные пути распространения.

3) Поддерживает трехмерную работу как на открытом воздухе, так и внутри помещений.

4) Определяет потери на пути и сдвиг фазы каждого луча с помощью электромагнитного анализа, включая отслеживание горизонтальной и вертикальной поляризаций сигнала на пути распространения. Расчеты потерь на пути включают потери в свободном пространстве, потери на отражение и дифракционные потери. Для каждого отражения и дифракции модель вычисляет потери в горизонтальной и вертикальной поляризациях с использованием уравнения Френеля, Единой теории дифракции (UTD), геометрического угла и комплексной диэлектрической проницаемости материалов интерфейса на указанной частоте.

Также используется модель распространения SBR использует анализ трассировки лучей для расчета путей распространения и соответствующих им потерь на пути. Потери на трассе рассчитываются на основе потерь в свободном пространстве, потерь на отражение и дифракцию из-за взаимодействия с материалами, а также потерь на поляризацию антенны.

При моделировании задавались место передатчика для моделирования сценария малой соты в густонаселенной городской среде. Площадка передатчика представляет собой базовую станцию, расположенную на столбе и обслуживающую окружающую территорию. Передатчик использует изотропную антенну по умолчанию и работает на несущей частоте 28 ГГц с уровнем мощности 5 Вт, также использовался путь с одним отражением.

Результат показывает распространение сигнала по пути с одним отражением, в том числе характеристики распространения, включая полученную мощность, изменение фазы, расстояние и углы отправления и прихода, щелкнув нанесенный путь, показано на рис. 1.

Рис. 1. Имитация модели распространения сигнала с 1 отражением

Полученная мощность при идеальном отражении: -70,4 дБм., но если учитывать погодные условия и материалы зданий то потери будут увеличены почти на 10 дб. Полученная мощность будет составлять -80 дБм.

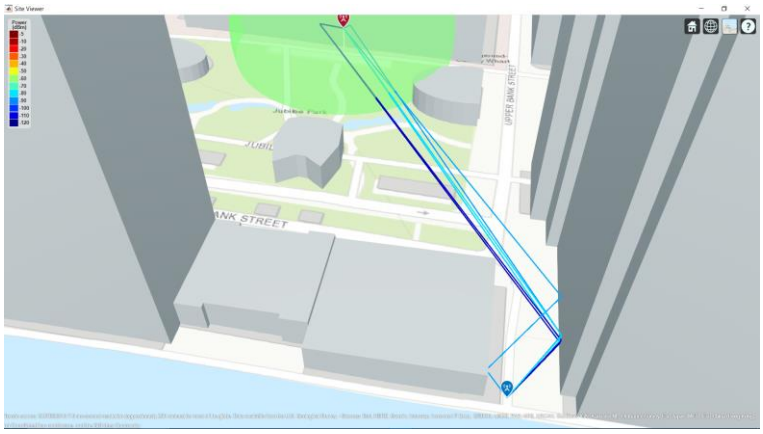


Рис. 2. Имитация модели распространения сигнала с 2 отражениями и 1 дифракцией

Результатом является принимаемая мощность с путями с двумя отражениями и одной дифракцией: -79,8 дБм, результат отображен на рис. 2.

Для достижения оптимального качества связи. В этом разделе используется Phased Array System Toolbox™ для оптимального управления лучом, чтобы максимизировать полученную мощность для линии связи, не находящейся в прямой видимости.

Для моделирования будет применяться специальная антенна из отчета МСЭ-R M.2412 для оценки радиотехнологий 5G.

Рис. 3. Имитация модели распространения сигнала с энергией антенны, направленной вдоль пути распространения

Результатом моделирования мы получили угол отклонения для пути с одним отражением и применили этот угол, чтобы направить антенну в оптимальном направлении для достижения более высокой принимаемой мощности. Азимут угла отклонения компенсируется физическим азимутом угла антенны, чтобы преобразовать его в азимут вектора управления, определенный в местной системе координат фазированной антенной решетки.

Тем самым новая полученная мощность увеличивается более чем на 20 дБ. Увеличение принимаемой мощности соответствует пиковой направленности антенны. Полученная мощность с управлением лучом: -57,5 дБм, показано рис. 3.

Основываясь на результатах моделирования можно сказать о возможности использование анализа трассировки лучей для прогнозирования мощности сигнала для линий связи вне прямой видимости, где существуют отраженные и дифрагированные на краях пути распространения.

1) Реалистичные материалов оказывает значительное влияние на расчетные потери на трассе и получаемую мощность.
2) Анализ с большим количеством отражений и дифракций приводит к увеличению времени вычислений, но выявляет дополнительные области распространения сигнала.
3) Использование направленной антенны с управлением лучом значительно увеличивает принимаемую мощность для приемников, даже если они находятся вне прямой видимости.

Список используемых источников:

1. Фокин Г. А. Моделирование сверхплотных сетей радиодоступа 5G с диаграммообразованием // TComm: Телекоммуникации и транспорт. 2021. Т. 15. N 5. С. 4 — 21.

2. Фокин Г. А. Модели управления лучом в сетях 5G NR. Часть 2. Выравнивание лучей при ведении радиосвязи// Первая миля. 2022. N 3 (103). С. 62 — 69

3. Фокин Г. А. Модели диаграммообразования в сверхплотных сетях радиодоступа 5G. Часть 1. Оценка помех// Первая миля. 2021. N 3 (95). С. 66 — 73.

4. Баланис К., Иоанидес П. Введение в смарт-антенны. Москва: Техносфера, 2012. - 101 с.

Статья представлена научным руководителем, доктором технических наук, профессором Фокиным Г. А.

Arefev A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Analysis of urban connections and coverage using ray tracing.
Undoubtedly, the fifth generation networks, or 5G, promise revolutionary changes in the field of mobile communications. They will provide the ability to transfer data at a much higher speed, which will allow users to upload and download content instantly, stream high-quality videos, play online games without delay, etc. At the same time, 5G networks will support a large number of simultaneous connections, which is necessary to manage the growing number of Internet of Things (IoT) devices - smart homes, cars, urban infrastructure, etc. The continuous growth of user needs and network density are problems for existing mobile networks that were not originally designed to work in new conditions. To solve these problems, promising 5G networks should provide a significant increase in bandwidth, connection reliability and reduction of network delays. Ray tracing, which is one of the main vectors of the development of mobile communication networks of the fifth generation, requires the use of.

Key words: superdense networks, SBR, ray tracing, direct visibility.

УДК 654.739
ГРНТИ 49.33.29

ОБЗОР ПРИМЕНЕНИЯ ИНТЕРНЕТА ВЕЩЕЙ (IoT) В СИСТЕМЕ «УМНОЕ ПОЛЕ»

О. В. Воробьев, А. В. Дубаков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На сегодняшний день проблема обеспечения населения продовольствием очень актуальна. В статье рассмотрено одно из возможных решений – применение беспроводных технологий в агропромышленном секторе. В ходе рассмотрения представлены и описаны возможности так называемых «умных» полей, которые призваны упростить работу аграриев. В ряде экспериментов данное нововведение уже показало свою эффективность.

сельское хозяйство, умное поле, интернет вещей, датчики, сенсоры.

В современном мире технологии Интернета вещей (*Internet of Things*) проникают во многие сферы нашей жизни. Наиболее известное его применение - обустройство умных домов и внедрение в автомобили. Однако активная цифровизация привела к тому, что данная технология уже сегодня используются в агропромышленном комплексе.

Население планеты постоянно растет. Если в 2008 г. оно составляло 6,5 млрд чел., в 2011 – 7 млрд, то, согласно прогнозу, к 2050 г. оно достигнет 9 млрд. На основании прогнозов сельскохозяйственное производство к 2050 г. должно увеличиться на 60 – 70 %. Следовательно, без инновационного развития технологии выращивания сельскохозяйственных культур невозможно обеспечить растущее население планеты продуктами питания [1].

«Умное сельское хозяйство» – это концепция, которая основана на использовании фермерами различных инновационных решений, позволяющих максимально автоматизировать сельскохозяйственную деятельность, повысить урожайность и улучшить финансовые показатели [2]. Так как термин «сельское хозяйство» достаточно обширный, в рамках данной статьи будет рассмотрено применение IoT в земледелии, а именно, в полях.

На «умных» полях сенсоры и датчики могут внедряться на каждом из этапов сельхозпроизводства, начиная от посева семян и заканчивая сбором урожая, и во всех видах оборудования. Они собирают данные об уровне освещенности, состоянии почвы (температура, влажность, наличие удобрений), засоренности посевов, распространении и распознании вредителей и болезней растений, уровне урожайности, качестве воздуха и погодных условиях. Информация будет направляться фермеру, который будет принимать решения и передавать команды сельскохозяйственным роботам в полях. Группировки роботов, оснащенные собственными

датчиками и навигационным оборудованием, будут курсировать по полям и реагировать на поступающие им сигналы о необходимости прополки, полива или сбора урожая. Кроме того, с воздуха за полями будут следить дроны, генерируя карты, которые будут служить руководством к действию для роботов и помогать фермерам планировать дальнейшие сельскохозяйственные работы.

«Умное поле» позволяет:

1) обеспечить стабильный рост производства продукции растениеводства за счет внедрения цифровых технологий сбора, обработки и использования данных о состоянии почв, растений и окружающей среды [3];

2) обеспечить высокий уровень урожайности, путем тщательного мониторинга всех этапов созревания растений;

3) своевременно выявить «заболевания» и предотвратить дальнейшее заражений посевов;

4) в долгосрочной перспективе выявлять более благоприятные районы для посевов тех или иных видов сельскохозяйственных культур.

Система «умное» поле работает по следующему принципу (графическое представление изображено на рис. 1). На поле сельскохозяйственного назначения размещаются сенсорные узлы, оснащенные бортовыми сенсорами [4]. Узлы в сети на поле обмениваются информацией между собой с использованием *ZigBee*. Именно эта технология лучше зарекомендовала себя, нежели *Wi-Fi* и *Bluetooth*, поскольку компоненты имеют низкую стоимость и высокую энергоэффективность. Необходимо учитывать, что поле зачастую имеет большую площадь (несколько десятков гектаров), поэтому для корректной работы *ZigBee* нужно использовать ретрансляторы. Узел-шлюз также размещается вместе с другими узлами, чтобы обеспечить соединение между сенсорной сетью и внешним миром по *GSM* с помощью SIM-карты. Для возможности контроля за всеми датчиками в шлюз внедрена система управления (рис. 2). Удаленный пользователь с помощью мобильного устройства и специального приложения может следить за состоянием поля и контролировать датчики, которые поддерживают жизнедеятельность посевов.

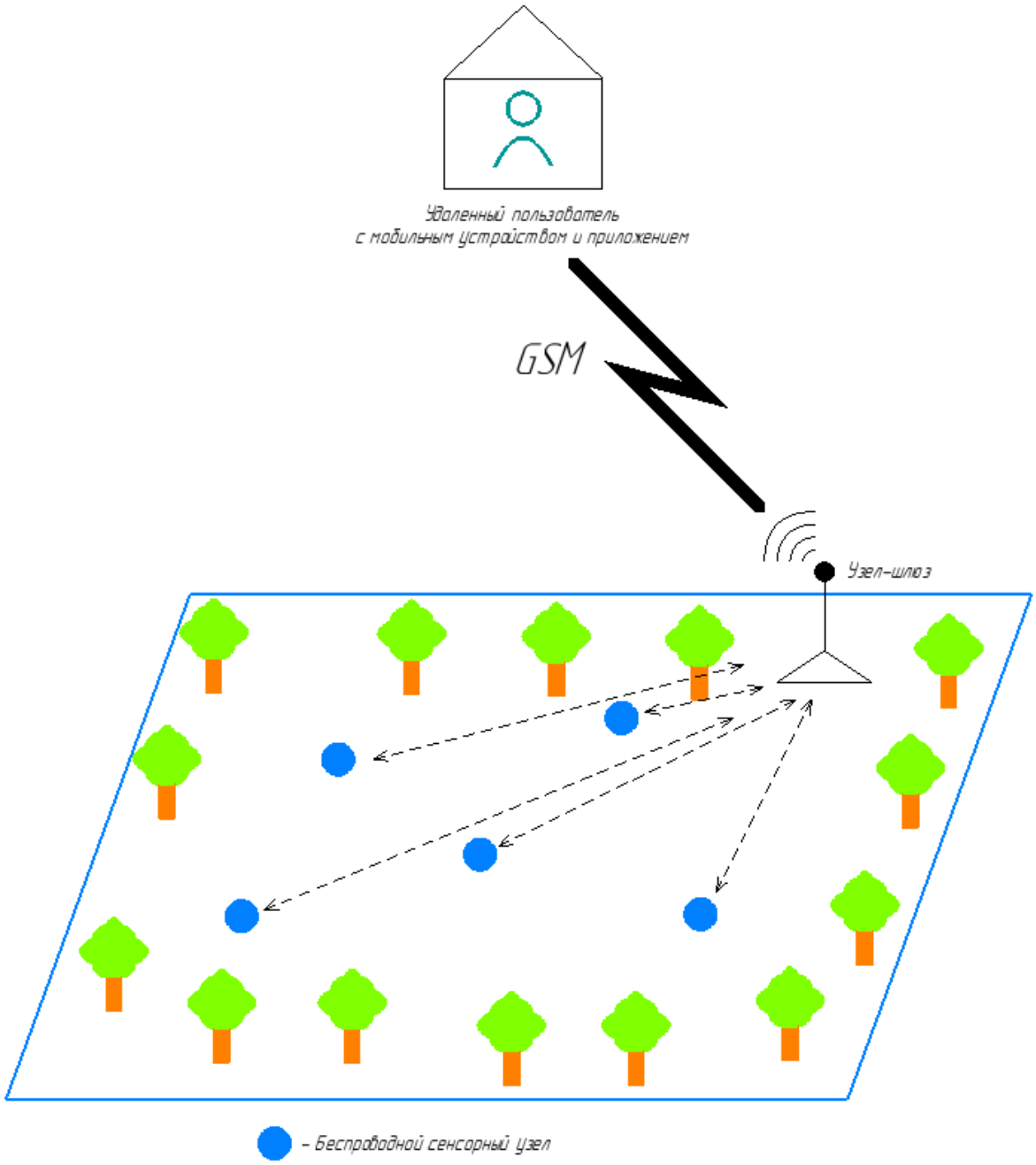


Рис. 1. Система «умное» поле

Рис. 2. Узел-шлюз

Интеллектуальная интегрированная система «Умное поле» способна обеспечивать высокую точность параметров постоянного мониторинга посевов, комплексную автоматизацию и роботизацию всех технологических этапов агропроизводства для минимизации потерь, оптимизацию

ресурсопользования, рост производительности труда, достижение потенциальной продуктивности сельскохозяйственных культур и экономическую эффективность сельскохозяйственного производства. С учетом развития беспроводных технологий в сфере АПК появляется возможность отслеживать состояние растений не только на этапе выращивания, но и при транспортировании и хранении.

Список используемых источников:

1. Нагоев З. В. и др. Разработка интеллектуальной интегрированной системы «Умное поле» // Известия Южного федерального университета. Технические науки. 2022. N 1 (225). С. 81-91.

2. Ващенко В. Р., Федоренко С. А., Ефанова Н. В. Обзор Iot-платформ для сельского хозяйства // Цифровизация экономики: направления, методы, инструменты. 2019. С. 99-101.

3. Кадыров С. В. Цифровые технологии в сельском хозяйстве. Умное сельское хозяйство // 100-летие кафедры растениеводства, кормопроизводства и агротехнологий: итоги и перспективы инновационного развития. 2019. С. 29-36.

4. Тарханова О. Ю. Применение беспроводных сенсорных сетей в прецизионном сельском хозяйстве // Проблемы информатики. 2017. N 4 (37). С. 16-46.

Vorobiev O., Dubakov A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Overview of the use of the Internet of Things (IoT) in the "smart field" system.

The problem of providing the population of foodstuff is very relevant at present. The article considers one of the possible solutions – the use of wireless technologies in the agro-industrial sector. During the review of sources, the possibilities of the so-called smart fields are presented and described. Smart fields are designed to simplify the work of farmers. In a number of experiments this innovation has already shown efficiency.

Key words: agricultural industry, smart field, Internet of Things, sensors.

УДК 621.396.2
ГРНТИ 49.03.05

БЕСПРОВОДНАЯ СВЯЗЬ 6G: ПЕРСПЕКТИВЫ И ПОТЕНЦИАЛЬНЫЕ ТЕХНОЛОГИИ

О. В. Воробьев, Д. С. Рябиков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С быстрым развитием интеллектуальных терминалов и появлением новых приложений (например, интерактивных сервисов и сервисов реального времени) резко возрос трафик беспроводных данных, и существующие сети сотовой связи (даже готовящиеся к запуску 5G) не могут полностью соответствовать быстро растущим техническим требованиям. Ожидается, что для решения предстоящих задач мобильные сети шестого поколения (6G) будут соответствовать высоким техническим стандартам, используя новый спектр и энергоэффективные технологии передачи данных. В данной статье описываются потенциальные требования и представляется обзор последних исследований перспективных технологий, развивающихся в рамках 6G, которые в последнее время привлекают большое внимание.

перспективные методы перехода на 6G

Для того чтобы в будущем обеспечить удовлетворительное качество услуг для "Индустрии 4.0", персонализированных медицинских сервисов, виртуального присутствия и других перспективных приложений, 6G должна еще больше повысить свою масштабируемость, гибкость и эффективность за счет использования новых технологий. Как и появление множества новых технологий при переходе к 5G, новые требования 6G будут влиять на основные технологические тенденции в процессе его эволюции. Успех 6G будет зависеть от прорыва в новых технологических концепциях. В этом разделе мы рассмотрим ряд последних исследований, связанных с разработкой 6G, включая технологии многодиапазонной сверхскоростной передачи, сверхгибкие интегрированные сети, многорежимную совместную передачу данных в нескольких областях, а также интеллектуальные подходы на основе машинного обучения и больших данных.

Многодиапазонная сверхскоростная передача данных

В последние годы отмечается шквал исследований, связанных с использованием нескольких высокочастотных диапазонов для сверхскоростной передачи данных, которые рекомендуются в качестве перспективных решений для 6G. В частности, консорциум DARPA, IBM и Intel сосредоточился на исследованиях по использованию частот 140 ГГц, 220 ГГц и 340 ГГц. В начале 2014 года Akyildiz и др. представили подробный обзор терагерцового диапазона в диапазоне 0,1-10 ТГц для поддержки высокоскоростной связи со скоростью терабит в секунду [4]. Еще одним преимуществом связи в терагерцовом диапазоне является возможность одновременной поддержки приложений макро- и микромасштаба, таких как терабитные беспроводные локальные сети (WLAN) и наносенсорные сети.

Более того, еще одной тенденцией развития 6G может стать динамическое использование различных частот, особенно нелицензируемых диапазонов, для получения преимуществ архитектуры совместного использования. Например, как предсказано в [1], оптическая связь в помещениях (частотный диапазон видимого света) является перспективной высокоскоростной технологией, которая заменит традиционную WLAN, поскольку люди проводят большую часть времени в помещениях (более 80%). Кроме того, для дальнейшего совершенствования мы можем комбинировать оптоволоконную технологию с беспроводной передачей данных. Сосуществование нескольких высокочастотных диапазонов и динамическое использование различных частот может быть реализовано с помощью передовых технологий программно-определяемого радио (SDR) и программно-определяемых сетей (SDN).

Супергибкая интегрированная сеть

В последнее время много усилий уделяется проектированию сверхгибких интегрированных сетей. В частности, в работе [3] авторы предложили масштабируемую архитектуру гетерогенной сети для поддержки связи в ТГц-диапазоне, где был предложен новый протокол управления доступом к среде (MAC), облегчающий многодиапазонную передачу. В работе [5] представлена потенциальная архитектура космическо-земной интегрированной сети (STIN), объединяющей космическую сеть, Интернет и мобильную беспроводную сеть. В целом STIN представляет собой крупномасштабную гетерогенную сеть с высокой гибкостью, сложной структурой и динамической топологией. Совместное использование преимуществ спутниковых систем, сетей воздушного и наземного сегментов позволит этой многомерной сети получить много преимуществ для будущей беспроводной связи 6G. В частности, как показано в [6], с увеличением количества и типов воздушных транспортных средств, таких как воздушные шары, дирижабли и беспилотные летательные аппараты (БПЛА), можно строить динамические сети с использованием летающих базовых станций (БС), которые улучшают традиционную статическую структуру. Например, в последние годы появилось множество различных проектов с использованием FBS, таких как например, проект Google Loon, проект Facebook Aquila, проект ABSOL. проект Facebook Aquila, проект ABSOLUTE, и проект Matternet [6].

Совместная многомодовая многодоменная передача

В [4] предложена конструкция физического уровня с адаптацией к расстоянию для связи в диапазонах ммВолн и ТГц, где каждый сверхширокий диапазон ГГц (даже ТГц) разделен на более узкие, но все еще широкополосные подокна, позволяющие осуществлять параллельную многократную широкополосную передачу. В каждом диапазоне для повышения эффективности могут быть использованы новые технологии с несколькими антеннами, например, технология PM-MIMO. В частности, как показано в [4], новый класс PM-MIMO, а именно UM-MIMO, является

перспективным решением для увеличения дальности связи и повышения достижимой емкости сетей ТГц-диапазона. Кроме того, для дальнейшего совершенствования конструкции PM-MIMO можно динамически комбинировать и адаптировать такие многорежимные антенные технологии, как формирование лучей (BF) и пространственное мультиплексирование (SMX), что позволяет эффективно снизить влияние высокого затухания в диапазонах ммВолн и ТГц, а SMX – увеличить пропускную способность на одного пользователя. Одновременное использование их комбинации в этих параллельных широких полосах частот может дать вышеперечисленные преимущества BF и SMX. Кроме того, для достижения выигрыша в разнесении, унаследованного от MIMO, в некоторых конкретных приложениях используются методы пространственного разнесения, такие как некоторые классические пространственно-временные блочные коды (STBC).

Помимо многомодовых технологий, перспективными для будущих сетей 6G являются также технологии совместной многодоменной передачи. Например, мультиплексирование с разделением режимов на основе орбитального углового момента (OAM-MDM) – это новое решение физического уровня для беспроводной связи на короткие расстояния в пределах прямой видимости, которое позволяет использовать все доступные DoF для передачи информации по беспроводным каналам, включая фазу, состояние поляризации и другие пространственные DoF [7]. В отличие от этого, для инновационного использования DoF нескольких антенн (пространственная область) и нескольких несущих (частотная область) в [8] была предложена методика многодоменной индексной модуляции (MD-IM), в основе которой лежит обобщенный принцип включения/выключения ключа, применяемый к любому из доступных доменов ресурсов сигнала для модуляции информационных битов по индексам ресурсов передачи, включая индексы поднесущих, передающей/приемной антенн, типов кода, матриц дисперсии, мощностей сигналов, матриц прекодирования и т.д. В целом OAM-MDM и MD-IM создают совершенно новые измерения для передачи данных. Основное преимущество технологий OAM-MDM и MD-IM заключается в том, что они могут быть гибко сконфигурированы для удовлетворения различных требований к производительности для поддержки широкого спектра приложений, что соответствует основному требованию при проектировании сетей 6G. Еще одним достижением является то, что вышеупомянутые многорежимные и многодоменные методы могут быть круговым и проникающим образом объединены для создания более эффективных и гибких конструкций.

Машинное обучение и интеллектуальная передача больших данных

Еще одна тенденция, прогнозируемая для 6G, – интеллектуальные сети и технологии, позволяющие обеспечить полное погружение пользователей в процесс передачи данных. Для решения этой исследовательской задачи необходимо создать инновации 6G, используя и комбинируя технологии из других областей. В последние годы были сделаны прорывы в области

искусственного интеллекта и технологий машинного обучения, таких как алгоритмы нейронных сетей глубокого обучения (DNN) [9]. При машинном обучении оптимальное решение (например, оптимальный режим передачи) вместо утомительных вычислений можно получить путем классификации или обучения нейронных сетей, причем классификаторы и DNN могут быть обучены на автономных наборах данных. Эти методы, основанные на машинном обучении, являются наилучшими кандидатами для улучшения проектирования и оптимизации беспроводных систем связи. В частности, ключевые вопросы синхронизации, оценки канала, эквализации, обнаружения MIMO-сигналов, итеративного декодирования и многопользовательского обнаружения в беспроводных системах связи схожи с теоретическими основами машинного обучения. теоретические основы машинного обучения.

Вышеупомянутые привлекательные характеристики методов машинного обучения и больших данных вызвали шквал исследований в области создания интеллектуальных систем беспроводной связи. В частности, в [1] машинное обучение рассматривалось как ключевой подход для реализации 6G с точки зрения пользователя. В [9] авторы обобщили методы машинного обучения для оптимизации массового MIMO, проектирования гетерогенных сетей и связи "устройство-устройство". В [10] для оптимизации физического уровня была предложена новая архитектура мобильной сети, позволяющая анализировать большие данные. В работах [2, 9, 10] отмечается, что методы машинного обучения и анализа больших данных не только обеспечат высокую производительность систем, но и коренным образом изменят дизайн и конфигурацию будущих сетей 6G (например, обработку данных на физическом уровне и MAC-протокол). Более того, машинное обучение и аналитика больших данных не являются независимыми и несвязанными элементами в проектировании будущих сетей 6G. Как отмечается в [2], совместное использование этих технологий позволит сделать мобильные сети более перспективными с точки зрения самоадаптации, самоанализа и прогнозирования. способности.

Заключение

Были представлены видения мобильных сетей 6G, способных удовлетворить растущие потребности IoE. Вначале описана концепция 6G с точки зрения использования временных, частотных и пространственных ресурсов. Затем рассмотрены некоторые перспективные современные подходы, которые могут приблизить эту концепцию к реальности. Отмечены основные характеристики сетей 6G такие как гибкость и универсальность, проектирование сетей 6G – это действительно междисциплинарная область науки. Ожидается, что новые исследования в области 6G окажут влияние и на такие области, как медицинская визуализация, полупроводники,

Список используемых источников:

1. David K. and Berndt H. 6G Vision and Requirement // IEEE Vehic. Teh. Mag., V. 13, N 3, Sept. 2018, pp. 72–80.

2. M. G. Kibria et al., Big Data Analytics, Machine Learning, and Artificial Intelligence in Next-Generation Wireless Networks // IEEE Access, V. 6, 2018, pp. 32,328–38.

3. A. S. Cacciapuoti et al. Beyond 5G: THz-Based Medium Access Protocol for Mobile Heterogeneous Networks // IEEE Commun. Mag., V. 56, N 6, June 2018, pp. 110–15.

4. I. F. Akyildiz et al. Combating the Distance Problem in the Millimeter Wave and Terahertz Frequency Bands // IEEE Commun. Mag., V. 56, N 6, June 2018, pp. 102–08.

5. H. Yao et al. The Space-Terrestrial Integrated Network: An Overview // IEEE Commun. Mag. V. 56, N 9, Sept. 2018, pp. 178–85.

6. S. Sekander et al. Multi-Tier Drone Architecture for 5G/ B5G Cellular Networks: Challenges, Trends, and Prospects // IEEE Commun. Mag., V. 56, N 3, Mar. 2018, pp. 96–103.

7. Y. Ren et al. Line-of-Sight Millimeter-Wave Communications Using Orbital Angular Momentum Multiplexing Combined With Conventional Spatial Multiplexing // IEEE Trans. Wireless Commun. V. 16, N 5, May 2017. pp. 3151–61.

8. P. Yang et al. Multidomain Index Modulation for Vehicular and Railway Communications: A Survey of Novel Techniques // IEEE Vehic. Tech. Mag., V. 13, N 3, Sept. 2018, pp. 124–34.

9. C. Jiang et al., “Machine Learning Paradigms for Next-Generation Wireless Networks,” IEEE Wireless Commun., V. 24, N 2, Apr. 2017, pp. 98–105.

10. S. Han et al. Big Data Enabled Mobile Network Design for 5G and Beyond // IEEE Commun. Mag., V. 55, N 9, Sept. 2017, pp. 150–57.

Ryabikov D., Vorobyov O.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

6g wireless communication: prospects and potential technologies.

With the fast development of smart terminals and emerging new applications (e.g., real-time and interactive services), wireless data traffic has drastically increased, and current cellular networks (even the forthcoming 5G) cannot completely match the quickly rising technical requirements. To meet the coming challenges, the sixth generation (6G) mobile network is expected to cast the high technical standard of new spectrum and energy-efficient transmission techniques. This article, sketch the potential requirements and present an overview of the latest research on the promising techniques evolving to 6G, which have recently attracted considerable attention.

Key words: 5G, 6G, WLAN, MIMO.

УДК 654.026
ГРНТИ 47.47.29

АЛГОРИТМ МНОГОПАРАМЕТРИЧЕСКОЙ АДАПТАЦИИ ДЕКАМЕТРОВОЙ РАДИОЛИНИИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Д. Д. Гайлит, А. Г. Чернышов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье представлен алгоритм совместного управления скоростью передачи и мощностью передачи декаметровой радиолинии специального назначения. Его реализация происходит при одновременном использовании частотной адаптации и частотного разнесения. Данное решение позволяет получать значительный энергетический выигрыш.

частотное разнесение, частотная адаптация, декаметровая радиолиния

Современная разработка радиолиний специального назначения играет важную роль в сфере связи и передачи данных. Декаметровая радиолиния обладает особыми характеристиками, которые требуют особого подхода при ее адаптации и настройке. При работе в сложных условиях требуется разработка оптимального алгоритма много параметрической адаптации для обеспечения стабильной и надежной передачи данных.

Представленные в известных источниках алгоритмы не учитывают разнесенного приема. Вариант алгоритма совместного управления скоростью и мощностью излучения передатчика можно записать в виде:

$$\{V,P\}=\begin{cases} V_{min},P_{1max},P_{2max} \text{ при } \mu_1(t)<\mu_{1,2},\ \mu_2(t)\le\mu_{2,2};\\ V_l,P_{1max},P_{2max} \text{ при } \mu_{1,2}<\mu_1(t)\le\mu_{1,m-1},\ \mu_{2,2}(t)<\mu_2(t)\le\mu_{2,m-1};\\ V_{max},P_{1max},P_{2max} \text{ при } \mu_1(t)=\mu_{1,m},\ \mu_2(t)=\mu_{2,m};\\ V_{max},P_{1,i},P_{2max} \text{ при } \mu_{1,m}<\mu_1(t)\le\mu_{1,n-1},\ \mu_2(t)=\mu_{2,m};\\ V_{max},P_{1max},P_{2max} \text{ при } \mu_1(t)\ge\mu_{1,n},\ \mu_2(t)=\mu_{2,m};\\ V_{max},P_{1max},P_{2,j} \text{ при } \mu_1(t)\ge\mu_{1,m},\ \mu_{1,m}<\mu_2(t)\,\mu_{2,n-1};\\ V_{max},P_{1max},P_{2min} \text{ при } \mu_1(t)=\mu_{1,m},\ \mu_2(t)\ge\mu_{2,n};\\ V_{max},P_{1,i},P_{2,j} \text{ при } \mu_{1,m}<\mu_1(t)\le\mu_{1,n-1},\ \mu_{2,m}<\mu_2(t)\le\mu_{2,n-1};\\ V_{max},P_{1,i},P_{2min} \text{ при } \mu_{1,m}<\mu_1(t)\le\mu_{1,n-1},\ \mu_2(t)\ge\mu_{2,n};\\ V_{max},P_{1min},P_{2,j} \text{ при } \mu_1(t)\ge\mu_{1,n},\ \mu_{2,m}<\mu_2(t)\le\mu_{1,n-1};\\ V_{max},P_{1min},P_{2min} \text{ при } \mu_1(t)\ge\mu_{1,n},\ \mu_2(t)\ge\mu_{2,n}; \end{cases}$$

Алгоритм автоматического регулирования скорости передачи и мощности излучения передатчика с учетом этих особенностей представлен на рис. 1 [1]. Действие алгоритма начинается с блока 1, в котором осуществляется ввод исходных данных. С блока 2 начинается вхождение в связь. В блоке 3 происходит настройка на фиксированную частоту при первом вхождении в связь или перестройка на пригодную для связи

фиксированную частоту при перерывах связи. В блоке 4 происходит вычисление вероятности связи с требуемой достоверностью в каждой из ветвей частотного разнесения $p_{чр1}$ и $p_{чр2}$. В блоке 5 вычисляется значение вероятности связи с требуемой достоверностью в декаметровой радиолинии при совместном учете частотного разнесения и частотной адаптации $p_{чр+ча}$ по методике, предложенной в п. 2.6.

В блоке 6 происходит сравнение полученной вероятности связи с заданно. В случае невыполнения требований происходит возвращение к блоку 2. Если требования выполняются, начинается ведение связи (Блок 7). В блоке 8 определяется значение коэффициента передачи $\mu_1(t)$, $\mu_2(t)$ (в первой и во второй ветви разнесения). В блоке 9 происходит сравнение коэффициентов передачи в текущий момент времени $\mu_1(t)$, $\mu_2(t)$ и в момент времени $\mu_1(t-1)$, $\mu_2(t-1)$. На основании сравнения в блоке 10 принимается решение о необходимости управления. В случае, если в управлении нет необходимости, происходит возврат к блоку 5. В блоке 11, исходя из сравнения коэффициентов передачи и текущих значений скорости и мощности, выбирается управляемый ресурс: скорость или мощность.

При увеличении коэффициента передачи (улучшении качества канала) сначала увеличиваем скорость передачи, затем снижаем мощность. В противном случае сначала увеличиваем мощность, а затем снижаем скорость.

В случае выбора управления скоростью в блоке 12 принимается решение об увеличении или снижении скорости. В блоке 13 производится сравнение текущей скорости с максимальной. Если текущая скорость меньше максимальной, то происходит переход к блоку 14, где определяется значение скорости V_l, в противном случае происходит переход к блоку 19 (начинается управление мощностью). В блоке 15 вырабатывается команда на увеличение скорости. При принятии решения о снижении скорости в блоке 16 сравнивается текущая скорость с минимальной. Если текущая скорость больше минимальной, то в блоке 17 выбирается значение V_l, в противном случае происходит возвращение к блоку 5. В блоке 18 вырабатывается команда на снижение мощности. После выработки команд происходит переход к блоку 41.

В случае выбора управления мощностью на основании значений коэффициентов передачи в блоке 19 принимается решение о том, чем мы будем управлять: мощностью в первой ветви разнесения, мощностью во второй ветви разнесения или в обеих ветвях вместе [1].

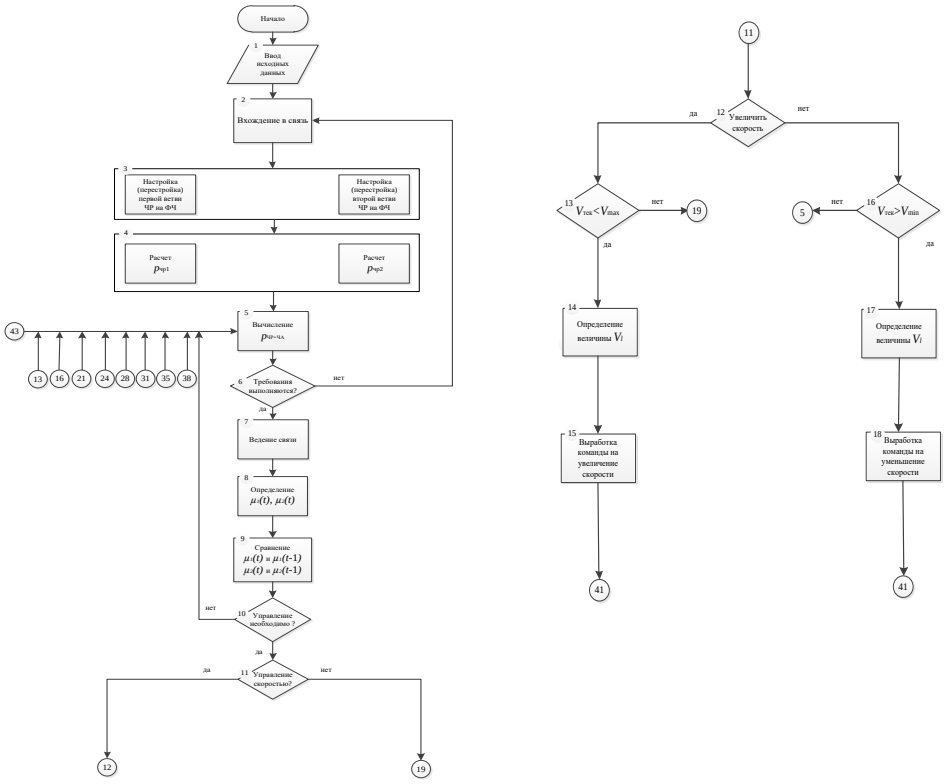


Рис. 1. Алгоритм АРСМ в декаметровой радиолинии при совместном использовании ЧР и ЧА

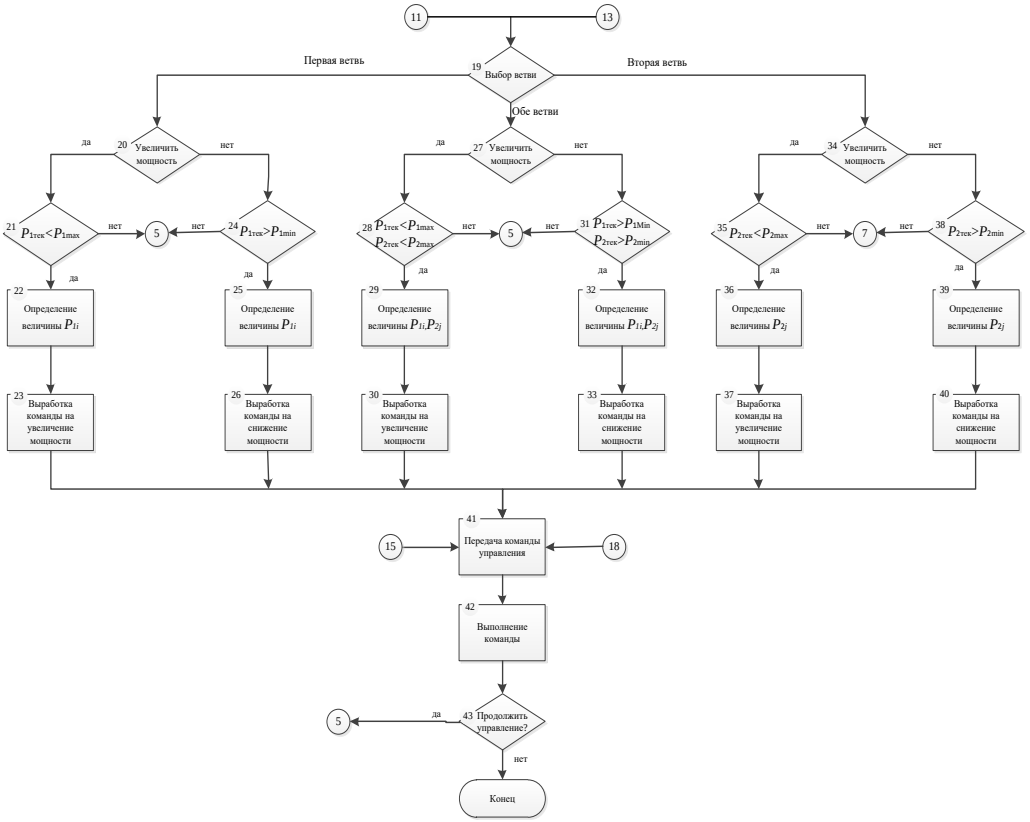


Рис. 1. (продолжение). Алгоритм АРСМ в декаметровой радиолинии при совместном использовании ЧР и ЧА

При управлении мощностью излучения первой ветви частотного разнесения в блоке 20 принимается решение об увеличении или снижении мощности. В случае увеличения мощности в блоке 21 производится сравнение текущей мощности с максимальной. Если текущая мощность меньше максимальной, то происходит переход к блоку 22, где определяется значение $P_{l,\ i}$, в противном случае происходит возвращение к блоку 5. В блоке 23 формируется команда на увеличение мощности в первой ветви разнесения. В случае принятия решения о снижении мощности в блоке 24 сравнивается текущая мощность с минимальной. Если текущая мощность больше минимальной, то в блоке 25 определяется значение $P_{l,\ i}$, если равна, то происходит возвращение к блоку 5. В блоке 26 вырабатывается команда на снижение мощности в первой ветви разнесения. После этого осуществляется передача команды управления (блок 41). Аналогичные процессы происходят при управлении мощностью излучения во второй ветви частотного разнесения, а при выборе сразу двух ветвей данные вычисления производятся, учитывая качество передачи первой и второй ветви одновременно.

Благодаря совместному управлению скоростью передачи и мощностью излучения возможно добиться значительного снижения энергетических затрат – в 1.4 раза за счет сокращения продолжительности передачи сообщения нормированного объема и уменьшения средней излучаемой мощности [2].

Список используемых источников:

1. Онышко А. Г., Постюшков В. П., Чухванцев В.Я. Оптимальное управление энергетическими ресурсами в одноинтервальных радиолиниях. Краткий текст лекций. Л. : ВАС, 1984. 48 с.
2. Постюшков В. П., Чернышов А.Г. Методика расчета вероятности связи с требуемой достоверностью при совместном использовании частотно-разнесенного приема и частотной адаптации // Системы связи. Анализ. Синтез. Управление. Вып. 22. С. 53–55.

Gailit D., Chernyshov A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Multi-parameter adaptation algorithm.

This article presents an algorithm for joint control of the transmission rate and transmission power of a decameter radio link for special purposes. It's implemented with the simultaneous use of frequency adaptation and frequency diversity. This solution allows to get significant energy gains.

Key words: frequency diversity, frequency adaptation, decameter radio link.

УДК 62-519
ГРНТИ 49.43.29

ТРЕБОВАНИЯ К СШП РАДИОЛИНИИ УПРАВЛЕНИЯ БЛА БЛИЖНЕГО ДЕЙСТВИЯ

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

Беспилотные летательные аппараты в настоящее время имеют широкий круг применений, решая задачи гражданской и военной авиации. В связи с этим имеет смысл повысить эффективность использования систем беспилотных летательных аппаратов. Для этого существует необходимость улучшения радиолинии управления беспилотным летательным аппаратом. Использование сверхширокополосной радиолинии дает возможность решения поставленной задачи.

беспилотный летательный аппарат (БЛА), радиолиния управления БЛА, СШП радиолиния, БЛА ближнего действия, требования к радиолинии управления БЛА

На сегодняшний день сфера применения беспилотных летательных аппаратов (БЛА) стремительно растет. С развитием технологий и возрастанием функциональности БЛА возникают все более высокие требования к радиолинии управления БЛА. В данной статье будет рассмотрено текущее состояние систем связи БЛА в России, недостатки существующих линий связи, актуальность задачи разработки сверхширокополосной (СШП) радиолинии для управления БЛА ближнего действия и основные требования к такой линии связи.

Наземный пункт дистанционного управления (НПДУ) предназначен для осуществления наблюдения, мониторинга, управления БЛА и его целевым оборудованием (ЦО) [1]. Для выполнения поставленных задач требуется наличие устойчивой радиосвязи между БЛА и НПДУ, из чего следует, что радиолиния должна отвечать высоким требованиям, обеспечивающим устойчивое управление БЛА.

Большая часть БЛА используют открытые частоты в диапазонах 800-900 МГц и 2400 МГц. Как следствие возникает перегрузка и некорректное использование частотного ресурса, что связанно с нехваткой частот.

В настоящее время системы связи для БЛА в России имеют ряд ограничений, которые делают их неподходящими для определенных видов задач.

Среди основных недостатков существующей линии связи для БЛА можно выделить следующие:

1) Ограниченная пропускная способность:

Многие существующие системы связи имеют ограниченную пропускную способность, что ограничивает передачу большого объема данных в реальном времени, что критично для многих задач, таких как передача видео высокого разрешения.

2) Преднамеренные и непреднамеренные помехи:

Существующие системы могут подвергаться помехам различного вида, что может привести к потере связи или ошибкам в управлении БЛА.

Для эффективного управления БЛА требуется надежная, высокоскоростная и устойчивая связь. Сверхширокополосная радиолиния управления предоставляет оптимальные решения для преодоления недостатков существующих систем связи, и, следовательно, разработка такой линии связи является актуальной задачей.

Система СШП-связи характеризуется полосой пропускания, превышающей или равной 500 МГц. В Соединенных Штатах Федеральная комиссия по связи (FCC) разрешает СШП-связь в диапазоне от 3,1 до 10,6 ГГц. В Европе Комитет по электронным коммуникациям разрешает передачу данных в диапазоне от 3,1 до 9 ГГц с несанкционированным диапазоном от 4,8 до 6 ГГц [2].

Сверхширокополосная линия связи для управления БЛА ближнего действия должна удовлетворять следующим требованиям:

1) Высокая пропускная способность

Линия связи должна обеспечивать высокую пропускную способность не менее 1 Гбит/с для передачи видео и данных в реальном времени.

2) Надежность

Система должна быть надежной и устойчивой к преднамеренным и непреднамеренным помехам, что критично для безопасности и надежности управления БЛА.

3) Низкая задержка

Минимизация задержки не более 10 мс в передаче данных необходима для реакции в реальном времени и точного управления БЛА.

4) Совместимость с существующими технологиями

Линия связи должна быть совместима с существующими системами управления БЛА и инфраструктурой.

5) Энергоэффективность

Минимизация энергопотребления обеспечивает возможность установки систем связи на микро-БЛА [3].

В таблице 1 представлены сравнительные характеристики радиолиний управления БЛА, функционирующих на различных частотах: 800-900 МГц, 2400 МГц и СШП частоты 3-10 ГГц.

ТАБЛИЦА 1. Сравнительные характеристики радиолиний управления БЛА

Частоты	800-900 МГц	2400 МГц	3-10 ГГц
Пропускная способность	200 Мбит/с	1 Гбит/с	10 Гбит/с
Задержка	20 мс	10 мс	5 мс
Помехозащищенность	Средняя	Высокая	Очень высокая
Дальность связи	до 50 км	до 50 км	до 10 км
Надежность	Средняя	Высокая	Очень высокая

Анализируя приведенную выше таблицу, можно сделать следующие выводы:

1. Пропускная способность радиолинии увеличивается с увеличением полосы частот. СШП радиолиния обеспечивает наиболее высокую пропускную способность.
2. Задержка в радиолиниях также уменьшается с увеличением частоты. СШП частоты имеют наименьшую задержку.
3. Дальность связи в диапазонах 800-900 МГц и 2400 МГц, выше, чем в диапазоне частот СШП, что делает их более предпочтительными для управления БЛА дальнего действия.
4. Помехозащищенность радиолинии управления БЛА наиболее высокая в СШП диапазоне, что позволяет снизить вероятность влияния внешних помех на устойчивость связи между НПДУ и БЛА.
5. Надежность управления БЛА значительно выше при использовании СШП радиолинии, что делает ее выбор наиболее целесообразным при решении критически важных задач.

В апреле 2023 года в Минцифры прошло заседание Государственной комиссии по радиочастотам (ГКРЧ), где ГКРЧ приняла решение о распределении частот 5030-5091 МГц для управления БЛА [4], также в перспективе планируется обсуждение про выделение других диапазонов частот.

Из сказанного ранее вытекает, что разработка сверхширокополосной радиолинии управления для беспилотных летательных аппаратов ближнего действия является актуальной задачей, обусловленной ростом функционала БЛА. Осуществление с практической точки зрения в отечественном исполнении также имеет потенциал в связи с выделением необходимых диапазонов СШП частот.

Список используемых источников:

1. Моисеев В. С. Прикладная теория управления беспилотными летательными аппаратами. Казань: ГБУ «Республиканский центр мониторинга качества образования» 768 с. ISBN 978-5-906158-53-6

2. Vladan Koncar. Smart Textiles and Their Applications, 2016. ISBN: 9780081005743

3. Рэндал У. Биард, Тимоти У. МакЛэйн. Малые беспилотные летательные аппараты: теория и практика. М. : ТЕХНОСФЕРА, 2015. 312 с. ISBN 978-5-94836-393-6

4. Государственная комиссия по радиочастотам при министерстве связи Российской Федерации (ГКРЧ России). Таблица распределения полос частот между радиослужбами Росссийской Федерации в диапазоне частот от 3 кГц до 400 ГГц. Постановление от 14 сентября 2023 года №1503.

Dobraya O.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Requirements for the uwb short-range uav control radio line.Unmanned aerial vehicles currently have a wide range of applications, solving problems of civil and military aviation. In this regard, it makes sense to increase the efficiency of the use of unmanned aerial vehicle

systems. To do this, there is a need to improve the radio control line of an unmanned aerial vehicle. The use of an ultra-wideband radio line makes it possible to solve the task.

Key words: unmanned aerial vehicle (UAV), UAV control radio line, UWB radio line, short-range UAV, requirements for the UAV control radio line.

УДК 629.058
ГРНТИ 47.49.31

СПУТНИКОВЫЕ ОРБИТЫ В СЕТЯХ 5G NTN

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

Надежность связи всегда играла важную роль в жизни человечества. С появлением спутниковой связи абоненты получили возможность обмениваться информацией даже из самых удаленных уголков мира. С развитием технологий спутниковая связь становиться доступной и вездесущей. В этой статье рассматриваются типы орбит используемые в спутниковом сегменте 5G NTN, также дается понятие 5G NTN и рассматривается архитектура спутникового сегмента.

5G, NTN, спутниковая связь, подвижная связь, спутниковые орбиты

23 февраля 2023 года компания Samsung Electronics объявила о создании системы 5G NTN (Fifth-Generation Non-Terrestrial Networks)[4]. Что является показателем скорого начала использования данной технологии. Согласно определению партнерского проекта 3GPP под неназемными сетями понимают сети или сегменты сетей связи, использующие бортовые или спутниковые радиоэлектронные средства для создания ретрансляционного узла с радиопередающим оборудованием или базовой станции мобильной сети связи [1–3].

Благодаря широкому спектру услуг и малой подверженности космических/бортовых аппаратов к физическим атакам и стихийным бедствиям неназемные сети будут способствовать внедрению услуг 5G в местах, которые не могут быть покрыты наземными системами 5G, а также в местах с плохим обслуживанием (например, в пригороде или в сельской местности) для улучшения качества предоставляемых услуг наземными сетями экономически эффективным способом. Стоит отметить повышение надежности сервиса 5G благодаря непрерывности обслуживания устройств M2M/IoT, а также пассажиров на борту транспорта дальнего следования (самолетов, судов, высокоскоростных поездов, автобусов). 5G NTN будет обеспечивать масштабируемость сети 5G, предоставляя эффективные ресурсы multicast/broadcast для доставки данных к узлам сети или даже к пользовательскому терминалу.

Преимущества связаны с неназемными сетями, работающими в одиночку или с интегрированными наземными и неназемными сетями. Они будут влиять на покрытие, пропускную способность, предоставляемую пользователям, пропускную способность системы, надежность сервиса, энергопотребление, плотность подключения.

5G NTN может быть использован в следующих направлениях: транспорт, общественная безопасность, средства массовой информации и

развлечения, электронное здравоохранение, энергетика, сельское хозяйство, финансы, автомобилестроение. [2]

Согласно техническому отчету партнерского проекта 3GPP TR 22.822 [3] и 3GPP TR 38.821 [1] для спутников связи выделяют несколько видов орбит рис 1.

Геостационарные (GEO, Geostationary Orbit) спутники расположенные точно в плоскости экватора на высоте 35 786 км, эти спутники вращаются с той же скоростью, что и Земля, благодаря этому спутник расположен неподвижно относительно Земли. Для создания непрерывного покрытия зоны диаметром от 200 км до 3500 км достаточно одного геостационарного спутника.

Спутники на негеостационарной орбите (NGSO, Non-Geostationary Orbit) находятся в постоянном движении относительно Земли. Для непрерывного обслуживания требуется спутниковая группировка (несколько спутников). Чем ниже высота, тем больше количество спутников.

Различают два вида негеостационарных орбит:

- Низкая околоземная орбита (LEO, Low Earth Orbit). Высота полета спутника на такой орбите от 300 км до 2000 км, наклонение от 0 до более чем 90 градусов. Низкая околоземная орбита расположена над МКС и космическим мусором, а также под первым поясом Ван Аллена (радиационным поясом). Диаметр зоны обслуживания колеблется от 100 км до 1000 км в зависимости от радиопередающего оборудования и высоты полета.
- Средняя околоземная орбита (MEO, Medium Earth Orbit). Высота полета спутника на такой орбите от 7000 км до 25000 км. Наклонение орбиты от 0 до более чем 90 градусов. Орбита расположена над радиационными поясами. Диаметр зоны обслуживания колеблется от 100 км до 1000 км в зависимости от радиопередающего оборудования и высоты полета.

Спутники с высокой эллиптической орбитой (HEO, Highly Elliptical Orbit) с диапазоном рабочих высот (орбита таких спутников рассчитана на эксплуатацию космического аппарата, когда он находится ближе к своему апогею - самой высокой части орбиты) от 7000 км до более чем 45 000 км. Наклонение выбирается для полной или частичной компенсации движения Земли относительно плоскости орбиты, что позволяет спутнику последовательно охватывать северные части планеты (например, Западную Европу, Северную Америку и Северную Азию). Спутники на высокой эллиптической орбите способны обслуживать зоны диаметром от 200 км до 3500 км.

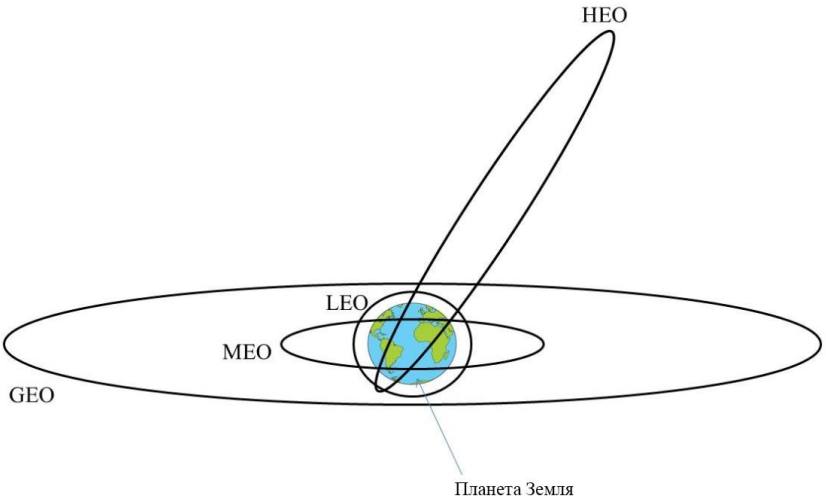


Рис. 1. Классификация орбит для спутников связи

Рассмотрим архитектуру спутникового сегмента сети 5G рис. 2,3.

Терминал NTN, который может относиться непосредственно к UE 3GPP, подключается и взаимодействует со спутником/платформой по сервисной линии (service link), которая обеспечивает радиосвязь между спутником/платформой и терминалом. Также UE может поддерживать радиосвязь с наземной сетью. Спутник/платформа может работать в прозрачном или регенеративном режиме. В прозрачном режиме выполняются такие функции как: фильтрация радиочастот, преобразование частоты и усиление сигнала. В регенеративном режиме спутник/платформа может выступать в роли базовой станции, в этом режиме межспутниковая/воздушная связь может работать в радиочастотном или оптическом диапазонах. По фидерной линии (feeder link) спутник или воздушная платформа связывается по радиоканалу с наземным шлюзом, который позволяет соединить спутниковую/воздушную сеть с наземной.

Рис 2.Структура сети с одним спутником

Рис. 3. Структура сети с двумя и более спутниками

Различают два типа сетей спутникового и воздушного доступа: для обслуживание стационарных терминалов и для обслуживания мобильных терминалов.

Сеть широкополосного доступа обслуживающая стационарные терминалы обеспечивает скорость передачи данных не менее 50 Мбит/с и даже нескольких сотен Мбит/с по нисходящей линии связи. Сервисные линии работают диапазонах частот выше 6 ГГц.

Узкополосная или широкополосная сеть доступа обслуживающая мобильные терминалы обеспечивает скорость передачи данных по нисходящей линии не менее 2 Мбит/с. Сервисные линии работают в диапазонах ниже 6 ГГц.

Появление 5G NTN в России послужит мощным драйвером для развития экономики. Благодаря вездесущности 5G NTN и возможности пользоваться спутниковой связью без специального оборудования сделают человека совершенно свободным в передвижении, что позволит осваивать новые земли и повышать уровень жизни. Но процесс внедрения будет сложным и дорогим, так как для обеспечения высокого уровня обслуживания необходимо создавать спутниковые группировки.

Список используемых источников:

1. 3GPP TR 38.821. Solutions for NR to support non-terrestrial networks (NTN). Release 16. [Электронный ресурс]. Available: https://www.3gpp.org/ (дата обращения: 15.09.2023).

2. 3GPP TR 38.811. Study on New Radio (NR) to support non terrestrial networks. Release 15. [Электронный ресурс]. Available: https://www.3gpp. org/ (дата обращения: 15.09.2023).

3. 3GPP TR 22.822. Study on using Satellite Access in 5G. Release 16.

4. https://news.samsung.com/global/samsung-electronics-introduces-standardized-5g-ntn-modem-technology-to-power-smartphone-satellite-communication (дата обращения: 15.09.2023).

Dyudin A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Satellite orbits in 5G NTN networks.

Reliability of communication has always played an important role in the life of mankind. With the advent of satellite communications, subscribers have the opportunity to exchange information even from the most remote corners of the world. With the development of technology, satellite communications are becoming available and ubiquitous. This article discusses the types of orbits used in the 5G NTN satellite segment, also gives the concept of 5G NTN and discusses the architecture of the satellite segment.

Key words: 5G, NTN, satellite communications, mobile communications, satellite orbits

УДК 654.165
ГРНТИ 49.43.01

ОЦЕНКА ПОМЕХ В СВЕРХПЛОТНОЙ СЕТИ 5G С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ МОДЕЛЕЙ МЕСТНОСТИ В MATLAB

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

В наши дни остро стоит проблема теоретического расчёта мощностей сигнала от базовых станций, особенно для перспективных сетей 5-го поколения. Такие сети позволят улучшить многие сферы деятельности, обеспечив возможность передавать большие объёмы данных. Одна из полезных процедур, требуемых для их реализации – это расчёт соотношения сигнал-шум.

SINR, MATLAB, 5G, signal-to-interference-plus-noise ratio

Современные специалисты области беспроводной радиосвязи возлагают большие надежды на реализацию и повсеместную эксплуатацию систем связи пятого поколения – *5G*. Эти системы позволят значительно улучшить многие сферы деятельности, такие как дополненная реальность, автоматизация производства, облачные системы. Многие коммерческие компании, научно-исследовательские институты, ассоциации и профсоюзы занимаются разработкой технических условий, нормативных документов и активно продвигают сети *5G*.

Для выполнения вычислений нам отлично подойдёт пакет прикладных программ *MATLAB*. Данный программный комплекс позволит нам рассчитывать зоны покрытия и определить качество сигнала в её пределах.

Для вычислений мощностей сигнала по отношению к шумам в *MATLAB* используется функция *sinr*. Но для начала стоит ознакомиться с параметром *SINR* подробнее. *SINR (Signal to Interference + Noise Ratio)* — отношение мощности полезного сигнала к сумме мощностей шума и помех, измеряется в дБ. Для удовлетворительной связи *SINR* должен принимать положительные значения [1]. Ниже представлена таблица, описывающая оценку качества сигнала.

ТАБЛИЦА 1. Оценка значений показателя SINR

Оценка	Диапазоны значений, дБ
Отлично	≥ 20
Хорошо	13… 20
Нормально	0… 13
Плохо	≤ 0

Результаты вычисления функции с описанными позднее параметрами отображают соотношения сигнал-интерференция-шум *(signal-to-interference-plus-noise ratio (SINR))* для ранее созданных базовых станций в функции *txsite*. Вычисленные результаты для каждой абонентской станции накладываются на карту, на которой они отображаются цветными областями, которые выводятся в отдельном окне site viewer. Для каждой области считается, что источником сигнала является базовая станция с наибольшей мощностью сигнала. Остальные БС, работающие на той же частоте, считаются источником интерференций и помех.

Sinr имеет множество дополнительных параметров для настройки более точного расчета. Рассмотрим некоторые их них.

Txs – передающий сайт или же базовая станция создаваемая в функции *txsite*. Используются в ситуации, когда передающих сайтов несколько штук. Эта функция поддерживает расположение антенн только в случае, когда используется географическая координатная система.

Rxs – сайты-приемники или же абонентское оборудование. Использование функции схоже с функицией *txs*.

Propmodel – Модель распространения, используемая для расчета потерь в тракте, задается в виде одной из этих опций:

Freespace – модель распространения в свободном пространстве.

Rain – Модель распространения при дожде. Используется для учета погодных условий. Данная модель учитывает распространение радиоволн в ситуации, когда пойдет дождь.

Fog – Модель распространения в тумане. Используется для учета погодных условий. Данная модель учитывает распространение радиоволн в ситуации, когда на улице туман.

Close-in – Модель распространения близкого пространства. Моделирование поведения электромагнитного излучения от точки передачи при его прохождении через городские макросоты с помощью объекта *CloseIn*. Модели распространения излучения *close-in* не имеют принудительного частотного диапазона.

Longley-rice – Модель распространения Лонгли-Райса. Данная модель не слишком известна в России, однако широко используется за рубежом. Хорошая достоверность модели Лонгли-Райса подтверждена практическими исследованиями. Модель позволяет производить вычисление медианного значения ослабления для сложных трасс в диапазоне частот от 20 МГц до 10 ГГц и предназначена для определения медианных значений ослаблений для длинных трасс в условиях пересеченной местности. Модель включает в себя два варианта расчета: «точка–точка» и «точка–область». Первый предполагает наличие цифровой карты местности и предназначен для более точных расчетов, в то время как в варианте «точка–область» оценка производится по общим параметрам подстилающей поверхности [2].

Tirem – Модель распространения *TIREM*. Эта модель рассматривает каждый путь и делает начальное решение есть ли прямая видимость (ПВ),

или трасса закрыта. Базируясь на этом решении модель использует один из двух подходов, чтобы найти потери на трассе. В режиме ПВ, программа вычисляет степень закрытия зоны Френеля и использует это, чтобы пропорционально корректировать величину дополнительных потерь на трассе (добавляет к потерям в свободном пространстве), которые вычисляются по одной из следующих двух моделей потерь в свободном пространстве. Для частот более чем 200 МГц используется модель *Longley-Reasoner*. Для частот ниже 150 МГц используется модель *Longley-Rice*. В частотах между 150 и 200 МГц, потери, рассчитанные по двум методам, пропорционально усредняются. Затухание, вычисленное этими двумя методами, корректируется степенью закрытия зон Френеля. Если открыто меньше, чем 0.5 радиуса зоны Френеля, то затухание 100 %. Если открыто больше, чем 1.5 радиуса зоны Френеля, то никакое дополнительное ослабление не вносится, а учитываются только базисные потери на трассе свободного пространства. Если открыто от 0.5 до 1.5 радиуса зоны Френеля, то вносятся дополнительные потери на трассе как линейная пропорция между 0 и 100 процентами [3].

Raytracing – Модель распространения лучей, использующая метод падающих и отраженных лучей (*SBR*). При указании в качестве входных данных модели трассировки лучей функция учитывает многолучевые помехи с помощью фазовой суммы. Значение по умолчанию зависит от системы координат, используемой входными объектами.

SignalSource – Интересующий источник сигнала, задаваемый в виде пары, разделенной запятыми, состоящей из *SignalSource* и "*strongest*", или в виде объекта сайта передатчика. Если в качестве источника сигнала указан "*strongest*", то в качестве источника сигнала, представляющего интерес для данного местоположения, выбирается передатчик с наибольшим уровнем сигнала. При вычислении *SINR* источник сигнала *SignalSource* может представлять собой массив *txsite* с равным количеством элементов *rxs*, где каждый элемент сайта передатчика определяет источник сигнала для соответствующего сайта приемника.

ReceiverNoisePower – Суммарная мощность шума приемника в дБм, указанная в % в виде числа. Значение по умолчанию равно -107, что предполагает полосу пропускания приемника 1 МГц и коэффициент шума приемника 7 дБ. Так же есть возможность вычислить это значение по формуле (1):

$$N = -174 + 10 \cdot \log(B) + F \qquad (1)$$

где,

N – шум приемника в дБм;

B – полоса пропускания приемника в Гц;

F – коэффициент шума в дБ.

ReceiverGain – коэффициент усиления приемника в дБ, заданный в виде числа. Он включает в себя коэффициент усиления антенны приемника и потери в системе.

ReceiverAntennaHeight – высота антенны приемника над уровнем земли в метрах, заданная в виде числового скаляра. Если функция вызывается с выходным аргументом, то значение по умолчанию вычисляется с использованием *rxs*. В противном случае значение по умолчанию равно 1.

Дополнительные функции, применяемые при построении графика *SINR*:

Values – Значения *SINR* для построения графика, заданные в виде числового вектора. Каждое значение отображается на карте в виде отдельного цветного контура с заливкой. Цвета контуров определяются с помощью *Colormap* и *ColorLimits*. По умолчанию используется значение [-5:20].

MaxRange – максимальная дальность построения графика *SINR* от каждой площадки передатчика, задается в виде положительного числового скаляра в метрах, представляющего собой расстояние по большому кругу. *MaxRange* определяет область интереса на карте для построения графика. Значение по умолчанию автоматически вычисляется в зависимости от типа модели распространения, как показано в таблице ниже:

ТАБЛИЦА 2. Ограничения расчетных моделей распространения радиоволн

Модель распространения	Максимальное расстояние
Атмосферная или эмпирическая	30 км
Рельеф местности	30 км или расстояние до самого удаленного здания
Трассировка лучей	500 м

Resolution – Разрешение мест расположения приемников, используемых для расчета значений *SINR*, задается как '*auto*' (значение по умолчанию) или как числовой скаляр. Разрешение определяет максимальное расстояние между точками. При значении разрешения '*auto*' значение вычисляется с использованием *MaxRange*. Числовое значение *Resolution* выражается в метрах. Уменьшение значения *Resolution* увеличивает как качество карты *SINR*, и время, необходимое для ее вычисления.

Colormap – цветовая карта для раскрашивания залитых контуров, задается в виде предопределенного имени *colormap* или массива M-на-3 триплетов *RGB* (красный, зеленый, синий), определяющих M отдельных цветов.

ColorLimits – цветовые границы для цветовой карты, заданные в виде двухэлементного вектора вида [*min max*]. Цветовые границы указывают на значения *SINR*, которые соответствуют первому и последнему цветам в цветовой карте. По умолчанию используется значение [-5;20].

ShowLegend – показывать на карте легенду цвета уровня сигнала, задается как *true* или *false*. По умолчанию используется значение *true*.

Transparency – Прозрачность карты *SINR*, задается в виде числового скаляра в диапазоне от 0 до 1, где 0 – полностью прозрачная, а 1 – непрозрачная. Значение по умолчанию равно 0,4.

Для примера использования, рассмотрим имитационную модель. В качестве координат центральной БС на картах *Global Multiresolution Terrain Elevation Data 2010 (GMTED2010)* заданы координаты существующей площадки в Адмиралтейском районе. Параметры абонентских и базовых станций были взяты на основе [4]. Результат выполненного примера на рис. 1.

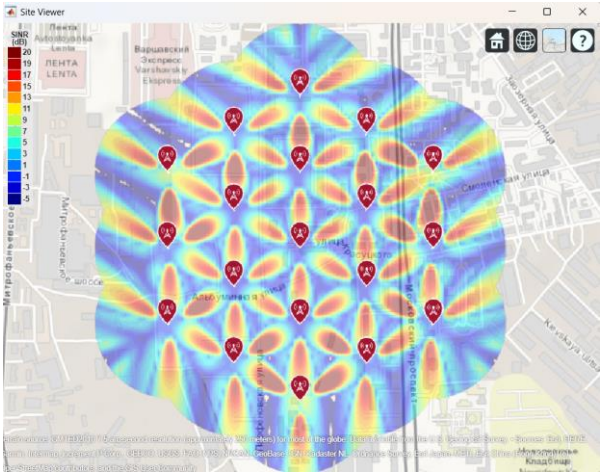


Рис. 1. Результат расчета карты SINR

Список используемых источников:

1. RSSI, SINR, RSRP, RSRQ - параметры качества сотового сигнала. [Электронный ресурс] https://www.vegatel.ru/articles/rssi-sinr-rsrp-rsrq-parametry-kachestva-sotovogo-signala (дата обращения: 20.10.2023).

2. Ломакин А. Ф., Школьный С. И. Моделирование поля DVB-T в условиях городской застройки. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/modelirovanie-polya-dvb-t-v-usloviyah-gorodskoy-zastroyki/viewer (дата обращения: 20.10.2023).

3. Модели распространения радиоволн. [Электронный ресурс] URL: https://telecomproject.tripod.com/mod.htm (дата обращения: 22.10.2023).

4. Report ITU-R M.[IMT-2020.EVAL], Guidelines for evaluation of radio interface technologies for IMT-2020, 2017. [Электронный ресурс]. URL: https://www.itu.int/md/R15-SG05-C-0057 (дата обращения: 22.10.2023).

5. Справочные материалы по программе MATLAB. [Электронный ресурс] // mathworks.com. URL: https://www.mathworks.com/help/antenna/ref/txsite.sinr.html (дата обращения: 20.10.2023)

Zanozin E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Investigation of sinr function in matlab.

Nowadays the problem of theoretical calculation of signal power from base stations, especially for prospective networks of the 5th generation, is acute. Such networks will improve many spheres of activity by providing the ability to transmit large amounts of data. One useful procedure required for their realization is the calculation of the signal-to-noise ratio.

Key words: SINR, MATLAB, 5G, signal-to-interference-plus-noise ratio.

УДК 621.396.99
ГРНТИ 49.43.29

МЕТОДЫ БОРЬБЫ С КОЛЛИЗИЯМИ В СИСТЕМЕ РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ

Е. В. Кравец, А. В. Чернышова
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассмотрены причины возникновений коллизий в системах радиочастотной идентификации на основе радиочастотных меток. Проанализированы методы борьбы с коллизиями.

RFID, радиочастотная идентификация, радиочастотная метка

Технология радиочастотной идентификации (Radio Frequency Identification — RFID) – это автоматическая технология быстрой идентификации и сбора данных об объектах с помощью цифровых радиочастотных сигналов. В системе RFID содержатся радиочастотные метки, в которых закодирован идентификационный код, который должен быть принят считывающим устройством.

Динамика развития систем радиочастотной идентификации показывает, что возрастает потребность в использовании радиомаркеров на основе поверхностных акустических волн. Рост интереса к системам радиочастотной идентификации на поверхностных акустических волнах обуславливается, с одной стороны, успехами в области технологии и конструирования акустоэлектронных устройств, с другой - прогрессом в области проектирования систем идентификации, диктующим новые, более жесткие, требования к радиомаркерам. [1]

Радиомаркеры (транспондеры, радиометки) на поверхностных акустических волнах (ПАВ) относятся к классу «только чтение», а так же обладают рядом преимуществ перед другими технологиями бесконтактной идентификации и хорошо известны: это работа по радиоканалу при отсутствии встроенных источников питания у маркеров; большая дальность действия, высокое быстродействие, малые масса и габариты, высокая радиационная стойкость, широкийдиапазон рабочих температур, практически неограниченный срок службы маркеров. [2]

Системы RFID с метками «только для чтения» могут использоваться для систем контроля и учета объектов хранения, но при применении таких систем у считывателя появляется необходимость выборочно взаимодействовать с метками, которые также расположены в зоне опроса.

Радиочастотные метки, попавшие в зону опроса считывателя, посылают одновременно модулированные сигналы, которые будут искажаться на входе считывающего устройства. Такое явление называется коллизией. Данную проблему может наглядно проиллюстрировать случай передачи сигнала опроса большому количеству уложенных на паллете

изделий, у каждого из которых собственная идентификационная ПАВ-метка с уникальным кодом. Поскольку каждая идентификационная ПАВ-метка (с каждого изделия) ответит передачей собственного ответного сигнала с глобально-уникальным кодом, обработка всего массива данных, содержащихся в этих сигналах, для точного определения и декодирования каждого ответного сигнала и надежной идентификации каждого изделия может оказаться затрудненной. [3]

В системах RFID проблема коллизий решается использованием антиколлизионных методов, которые схожи со способами конфликтных ситуаций множественного коммуникационного доступа. Данные методы позволяют отключать все облучаемые метки кроме одной – тем самым обеспечивается единовременная передача информации только от одной метки, но радиометка на ПАВ является полностью пассивной и не содержит в своем составе ни одного программируемого элемента, что делает применение антиколлизионного протокола невозможным. [4]

Наиболее общими классификационными признаками для антиколлизионных методов являются пространство, частота и время. [5]

Для радиометок на ПАВ пространственный алгоритм позволяет параллельно локализовать несколько меток что, помимо идентификации помеченных объектов, является важнейшей функцией для отслеживания этих объектов в пределах, например, склада.

Это возможно из-за изменения зоны считывания, а в случае пассивных меток из-за вариации мощности, которая излучается считывающим устройством. Главной проблемой пространственных методов является трудность достижения высокой точности определения дальности. При возрастании числа меток в зоне считывания и уменьшении расстояния между ними требования к точности определения дальности возрастают.

Метод временного разделения, при котором используется различная начальная задержка сигнала и который можно применить для частного случая, будет обеспечивать решение проблемы только при общем числе маркеров в несколько десятков, обусловлено это тем, что радиочастотные метки на ПАВ имеет уникальный код, который закладывается внутри топологии ПАВ-устройства при его изготовлении.

Использование частотного разделения потребует высокостабильных генераторов и селективных полосовых фильтров.[6]

Решение проблемы коллизий возможно и другими способами, в частности, применением технологии CDMA, реализующей корреляционное разделение откликов, активно используемой в системах передачи данных [7]. Однако, применение технологии CDMA к данной системе упирается в ту же проблему невозможности программирования метки и в конструктивные особенности метки, ограничивающие длину ее идентификационного кода. [4]

Так же возможно применить технологию FDMA, которая позволяет одновременно работать нескольким каналам передачи данных, используя различные рабочие частоты. В пассивных RFID-системах сигнал от

считывателя обычно передается на некоторых рабочих частотах для обеспечения питания и передачи команд считывателя пассивным меткам. Однако система по-прежнему позволяет получить одну идентификационную метку за один временной интервал.

На основании вышеизложенного анализа можно сделать вывод, что алгоритм разрешения коллизий меток для технологии RFID должен обладать следующими характеристиками:

— считыватель должен идентифицировать все метки, находящиеся в его зоне считывания. Поскольку считывающее устройство не может точно оценить количество меток, при проектировании жесткой системы меток и протокола борьбы с коллизиями необходимо учитывать гарантию распознавания всех меток.

— идентификация метки должна осуществляться при небольшом потреблении ресурсов, поскольку метка обладает малой мощностью. Таким образом, протокол защиты от столкновений должен загружать метку с минимально возможным временем обмена данными.

Список используемых источников:

1. Койгеров А.С. Анализ алгоритмов кодового разделения сигналов в системе радиочастотной идентификации, реализуемой на основе устройств на поверхностных акустических волнах: автореф. дис. … канд. тех. наук: 05.13.01 / Койгерова Алексея Сергеевича – Санкт-Петербург, 2011. 23 с.

2. Забузов С. А. Маркеры на поверхностных акустических волнах для систем радиочастотной идентификации // Будущее сильной России — в высоких технологиях. СПб. : Логос, 2007. С. 137–143.

3. Багдасарян А., Багдасарян С., Днепровский В., Карапетьян Г., Николаева С. Малогабаритные радиочастотные метки на ПАВ расширение функциональных возможностей // Электроника, наука, технология, бизнес. 2014. N 3 (00134). С. 70-76.

4. Чебачев В.О. О корреляционном разрешении коллизий в системах RFID на ПАВ // Электроника и микроэлектроника СВЧ. 2021. С. 315-319.

5. Шарфельд Т. Системы RFID низкой стоимости / Под ред. С. Корнеева. М. : 2006. 197 с. [Электронный ресурс]. http://www. alpha1.ru/recomend/rfid_lowcost.pdf. (дата обращения: 11.10.2023).

6. Койгеров А. С, Забузов С. А. Дмитриев В. Ф. Исследование корреляционного метода для решения задачи антиколлизии для систем радиочастотной идентификации на ПАВ // Информационно-управляющие системы. 2009. Вып. 5. С. 48-55.

7. Верзун Н. А., Воробьева Д. М., Колбанёв А. М., Колбанёв М. О. Корреляционные алгоритмы антиколлизии для RFID систем // Информационные технологии и телекоммуникации. 2018. Т. 6. N 1. С. 82–91.

Kravets E., Chernyshova A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Methods of collision control in the radio frequency identification system.

The paper considers the causes of collisions in radio frequency identification systems based on radio frequency tags. The methods of collision control are analyzed.

Key words: RFID, radio frequency identification, radio frequency tag.

УДК 654.01
ГРНТИ 49.01.11

РАЗВИТИЕ ТЕХНОЛОГИИ 5G И 6G

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

Исследования в области телекоммуникаций перешли к определению требований и вариантов использования технологий beyond-5G (B5G – технология следующего поколения после 5G) и 6G сетей (B5G/6G). Но не стоит забывать и о бизнес-модели (БМ), которая также должна быть изучена для эффективного использования возможностей B5G/6G. Вследствие чего традиционные роли в телекоммуникациях могут либо исчезнуть, либо трансформироваться, а также появятся новые. В данной статье внимание сфокусировано на телекоммуникационной экосистеме, для того чтобы можно было выделить основные изменения в БМ, связанные с 5G, и определить перспективы новой БМ для B5G/6G.

B5G/6G, бизнес-модель

Сети B5G/6G нацелены на полную реализацию потенциала виртуализации, облачных технологий, открытие новых спектральных диапазонов и использование искусственного интеллекта (ИИ) для повышения стабильности при предоставлении более специализированных и автоматизированных услуг. Эти концепции полностью изменят телекоммуникационную БМ и экосистему. Однако телекоммуникационная экосистема является сложной системой с множеством взаимосвязанных заинтересованных сторон и зависит от множества ограничений и требований. В данной статье будут найдены ответы на вопросы: Каковы основные изменения, происходящие в экосистеме 5G, с акцентом на операторов мобильной связи? Каковы основные ограничения и требования, определяющие эволюцию 5G? Каковы перспективы БМ для B5G/6G?

За последние несколько лет увеличились число мобильных операторов связи (Mobile Network Operator, MNO), в частности, появились виртуальные операторы (Mobile Virtual Network Operator, MVNO), что усилило конкуренцию на рынке и привело к снижению стоимости услуг мобильной связи и мобильного доступа в Интернет. Чтобы удержать свои позиции на этом нестабильном рынке, MNO должны использовать возможности, открывающиеся благодаря 5G/B5G, а затем 6G. MNO должны адаптировать свою архитектуру с учетом значительного воздействия 5G/B5G на отрасль телекоммуникаций, стремясь повысить энергоэффективность, зону покрытия, и пропускную способность, а также создать приватные сети. Для достижения этих целей они могут монетизировать свои долгосрочные лицензии на использование спектра путем совместного использования или сдачи в аренду части спектра другим мелким операторам связи. Они также могут полностью перестроить свою сеть за счет виртуализации и децентрализации и

инвестировать в инфраструктуру пограничных вычислений для предоставления услуг, чувствительных к задержкам. MNO также могут искать новые возможности, приобретая технологические и управленческие навыки путем сотрудничества и аутсорсинга для предоставления услуг с добавленной стоимостью на рынке B2B (Business-to-Business).

Также не стоит забывать о нормативно правовых актах и законах, регулирующих использование частотных диапазонов, которые существенно влияют на эволюцию БМ.

Экологическая точка зрения.

Цель экологической устойчивости в телекоммуникациях – это минимизация воздействия на окружающую среду. Целесообразным направлением является снижение энергопотребления в отрасли путем разработки энергоэффективных БМ, таких как использование совместного использования ресурсов. На оборудование и устройства приходится наибольшая часть воздействия сектора на окружающую среду (65%-92%, согласно исследованию, проведенному в 2022 году французским органом по регулированию телекоммуникаций). Эти устройства и оборудование могут быть изготовлены из перерабатываемых и экологически безопасных материалов. Другим вариантом, позволяющим минимизировать количество отработанных устройств, является создание обратно совместимых технологий, которые могут работать на устройствах старого поколения. Кроме того, необходимо разработать новые БМ, позволяющие перерабатывать токсичные компоненты сетевых устройств и утилизировать электронные отходы.

С рыночной и экономической точки зрения.

В течение многих лет рыночная конкуренция между операторами связи основывалась на "изобилии" (предложение наибольшего количества гигабайт с наивысшим качеством и наименьшей ценой), что ведет к более высокому потреблению (больше пропускной способности, больше устройств и т.д.). Такая парадигма должна быть изменена в сторону более бережного использования ресурсов. Этого можно достичь с помощью системы оплаты по факту использования БМ, или путем предоставления клиентам возможности настраивать свои предоплатные и постоплатные тарифные планы с индивидуальными параметрами качества обслуживания (Quality of Service, QoS) и количества объема потребленных данных. Это может помочь сдержать "эффект отскока".

Повышение энергоэффективности при одновременном снижении энергопотребления является важной задачей. Но вопреки предварительному расчету реализация мероприятий, направленных на решение этой задачи, может привести к получению значительно меньших результатов по экономии ресурсов по сравнению с приведенными ранее примерами. В таких случаях и наблюдается явление, называемое "эффектом отскока" (англ. rebound effect). Эффект заключается в увеличении потребления энергоресурсов при

повышении эффективности устройств и приборов вследствие роста их количества или изменения отношения потребителей к их использованию.

Оператор мобильной связи играет важную роль в развитии телекоммуникаций, так как для внедрения новых технологий, таких как 5G и 6G необходимо заново пересмотреть все аспекты, начиная с бизнес-модели и заканчивая техническими характеристиками. Бизнес-модель, которая использовалась в 2,3,4 G, уже не подходит для развития новых стандартов. В эпоху B5G/6G создают новые возможности БМ, которые будут бросать вызов существующим. Это малые сети, благодаря которым можно уплотнить количество сот мобильных операторов, обеспечить связь в перегруженных сетях, расширить сети в сельской местности. Это совместно использование ресурсов, которое позволит совместно использовать любой вид инфраструктуры и сетевых ресурсов с применением технологий виртуализации и облачных технологий. А также появляются перспективные направления новых БМ B5G/6G, таких как: создание платформенной экосистемы, где открывается возможность создания услуг сервитизации на основе услуг облачных вычислений. Open Source – решение с открытым исходным кодом 5G RAN и Core Network позволяет создавать специализированные сети с высокой надежностью, быстрым предоставлением услуг и расширенным покрытием.

Список используемых источников:

1. Meroua Moussaoui, Emmanuel Bertin, and Noël Crespi Divide and Conquer: A Business Model Agenda for Beyond-5G and 6G // IEEE Communications Magazine, 2023, 82 p.
2. E. Bertin, N. Crespi, and T. Magedanz, John Wiley & Sons// Shaping Future 6G Networks: Needs, Impacts, and Technologies, 2021.
3. P. Ahokangas, M. Matinmikko-Blue, and S. Yrjola, Visioning for a Future-Proof Global 6G from Business, Regulation and Technology Perspectives // IEEE Communications Magazine, 2022.
4. M. Moussaoui, E. Bertin, and N. Crespi, Telecom Business Models for Beyond 5G and 6G Networks: Towards Disaggregation? // 2022 1st Int'l. Conf. 6G Networking (6GNet), 2022, pp. 1–8.
5. P. N. Gooderham et al., The Digital Challenge for Multinational Mobile Network Operators. More Marginalization or Rejuvenation? // J. Int'l. Manag., vol. 28, no. 4, 2022, p. 100946

Makovchik D.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development of 5G and 6G technologies.

Telecommunications research has moved on to identifying requirements and use cases for beyond-5G (B5G - the next generation technology after 5G) and 6G networks (B5G/6G). But let's not forget the business model (BM), which must also be explored to effectively capitalize on B5G/6G opportunities. As a consequence, traditional roles in telecommunications may either disappear or transform, and new roles will emerge. This paper focuses on the telecom ecosystem so that the major changes in the BM associated with 5G can be highlighted and the prospects for a new BM for B5G/6G can be identified.

Key words: B5G/6G, business model.

УДК 654.01
ГРНТИ 49.01.11

ПРОЕКТИРОВАНИЕ АРХИТЕКТУРЫ 6G

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

В статье рассматривается важность архитектуры сети для нового поколения сотовых сетей и предлагаются высокоуровневые проекты архитектуры 6G. Основываясь на опыте операторов и анализе недостатков сети 5G, выявлены ключевые мотивы инноваций и принципы проектирования архитектуры 6G. Предложена новая архитектура "3 тела, 4 слоя, 5 плоскостей", а также соответствующая логическая функциональная схема на основе сервисов (Holistic Service-based Architecture, HSBA) и распределенная автономная сеть (Distributed Autonomous Network , DAN). Эти предложения являются направлением для будущих исследований в области сетевых архитектур.

6G, архитектура, HSBA, DAN, нарезка сети, TSC, 5G

Основные мотивы и факторы разработки архитектуры

Архитектура является ключевым вопросом разработки сетей сотовой связи нового поколения – 6G. Этот вопрос актуален для промышленности и научных кругов. Основные мотивы и факторы разработки архитектуры сетей 6G можно поделить на три аспекта.

Первый аспект – это новые сценарии и требования к услугам. Существуют множество сценариев, таких как иммерсивное взаимодействие, облачная расширенная реальность и голографическая связь, которые требуют высокой производительности и новых возможностей, не удовлетворяемых сетью 5G.

Второй аспект – это новые технологии и их интеграция в архитектуру 6G. Примером новой технологии является связь с учетом времени (Time Sensitive Communication, TSC), которая позволяет добиться детерминированной передачи данных. В 6G архитектура сети должна развиваться, чтобы поддерживать более широкое расширение домена, а протоколы должны быть совместимы с TSC.

Третий аспект – это вдохновение для развертывания сети 5G. Сеть 5G использует новую архитектуру, основанную на сервисах, и характеристиках сетевой нарезки (network slicing) и пограничных вычислений для поддержки различных вертикальных отраслей. Однако после развертывания сети 5G становится понятно, что требуются дальнейшие усовершенствования.

На основе возможностей 5G ожидается, что сетей 6G будет развиваться в нескольких аспектах:

1) легкий вес абонентского терминала;
2) реализация сетей доступа и опорной сети;
3) раскрытие нарезанных фрагментов опорной сети;

4) автоматическое управление жизненным циклом нарезки с помощью технологий искусственного интеллекта и машинного обучения.

В целом, разработка архитектуры сетей 6G основана на новых сценариях и требованиях к услугам, интеграции новых технологий и опыте, полученном от развертывания 5G.

Принципы проектирования архитектуры

Принципы проектирования архитектуры сети 6G основаны на опыте развертывания и эксплуатации сетей на протяжении длительного времени. Основные принципы включают дизайн, обеспечивающий совместимость, междоменное взаимодействие, распределенную автономность, нативность и минимализм.

Совместимый дизайн является одним из ключевых принципов архитектуры 6G. Он базируется на парадигмах "нативное облако", "сервис-ориентированность" и "end-to-end" на базе IP, что позволяет сделать плавный переход от 5G к 6G с обратной совместимостью. Однако в определенных областях сети может появиться революционный дизайн для расширения ее возможностей.

Междоменный дизайн предусматривает интегрированный подход к связи, преодолевающий границы уровней и доменов. Он поддерживает различные режимы доступа, управление разными типами сетей и взаимодействие внутренних доменов для обеспечения согласованного пользовательского опыта.

Распределенное проектирование – это переход от централизованного планирования к распределенной автономии. В условиях быстрого роста плотности подключений и плотности трафика, централизованный способ управления становится неэффективным. Архитектура 6G должна быть более распределенной и эластичной, чтобы гибко масштабироваться.

Нативный дизайн предусматривает использование встроенных нативных возможностей, таких как безопасность и искусственный интеллект, для оптимизации архитектуры. Применение искусственного интеллекта и связанных с ним технологий позволит создать автономную систему управления и обслуживания.

Проектирование 6G также стремится к минимализму, упрощая структуру системы и оптимизируя функции и процедуры. Это позволяет снизить сложность обслуживания системы и удовлетворить требования экологичности и низкоуглеродности.

Еще одной важной составляющей проектирования архитектуры 6G является энергоэффективность. В свете концепции безуглеродного будущего и стремления к углеродной нейтральности, необходимо систематически рассматривать вопросы энергоэффективности на всех уровнях системы, включая узлы, сервисы и сети.

Разработка архитектуры 6G будет учитывать эти принципы, чтобы достичь более совместимой, гибкой, эффективной и экологической системы связи.

Архитектура логической сети 6G

Архитектура логической сети 6G строится на принципе "3-4-5". Она включает 3 тела, 4 слоя и 5 плоскостей, которые представляют собой пространственное, логическое и сетевое функционирование. Тела включают тело сети, тело управления оркестровкой и новое тело Digital Twin (Цифровой двойник). Слои определяют функциональную структуру архитектуры, включая слои ресурсов, маршрутизации, сервисных функций и экспозиции. Плоскости представляют разделение и формирование сетевых функций в плоскостях управления пользователя, данных, вычислений и безопасности. Архитектура 3-4-5 обеспечивает все функции и сервисы 6G. Она вводит новые тела и плоскости на основе традиционных сетевых функций. В некоторых сценариях функции могут быть отменены, например, в сценарии с пониженной сложностью и стабильным развертыванием тело Digital Twin не является обязательным. Вместе с тем, служба аутентификации остается необходимой, в то время как сложная служба мобильности может быть отменена благодаря более низкой задержке и высокой пропускной способности в средне-высокочастотном диапазоне 6G, особенно в сценариях Интернета вещей.

Архитектуры HSBA и DAN

Архитектура на основе сервисов (HSBA) является основополагающей для функциональных плоскостей сети, определенных в архитектуре 3-4-5. Она применяется как к системе управления сетью, так и к биллинговой системе, и будет использоваться в сетях 6G для реализации сквозной HSBA. HSBA применяет сервис-ориентированный дизайн ко всей системе и сетевым элементам. В сети радиодоступа на основе сервисов происходит разделение функций плоскости управления и плоскости пользователя, а функции плоскости пользователя в опорной сети на основе сервисов помогают реализовать полностью облачное развертывание.

HSBA позволяет расширить возможности SBA в глубину и ширину. Сервисный фреймворк будет развиваться в сторону большей распределенности и оптимизации дизайна развязки сервисов. Интерфейс сервисов будет становиться более гибким, открытым и эффективным. Атомарные сервисы позволят гибко комбинировать и вызывать функции, а новые протоколы и технологии, такие как HTTP/3 и бессерверные технологии, будут использоваться в HSBA.

Распределенная автономная сеть (DAN) представляет собой распределенную архитектуру, основанную на взаимосвязанных интеллектуальных сотовых устройствах (SCU, Smart Cellular Unit), которая поддерживает гибкое развертывание и самодостаточность ресурсов. DAN имеет четырехслойную структуру, включая уровень ресурсов и

вычислительных мощностей, уровень маршрутизации и соединений, функциональный уровень сервисной сети и уровень воздействия.

Уровень ресурсов и вычислительных мощностей обеспечивает необходимые ресурсы для работы сети. Уровень маршрутизации и соединений отвечает за маршрутизацию информации для объединения распределенных SCU. Функциональный уровень сервисной сети включает распределенные плоскости: управления, пользователя, озера данных, вычислений и безопасности. Уровень воздействия поддерживает настройку сети и предоставляет дополнительные услуги через интерфейсы воздействия.

DAN позволяет создавать настраиваемые SCU с разными возможностями и функциями для удовлетворения различных требований. SCU также может быть спроектирован с повышенной надежностью, стабильностью и возможностью обработки большого трафика.

Дальнейшие исследования

В архитектуре 6G инновации сыграют важную роль, и исследовательское сообщество активно занимается их разработкой. В статье анализируются новые требования и предлагаются принципы проектирования и архитектура 6G, которая может стать образцом и ориентиром для дальнейшей работы. Однако 6G все еще находится в стадии формирования, и есть множество открытых вопросов, над которыми продолжается работа. Для 6G сети могут быть использованы различные технологии, такие как распределенные технологии, новые протокольные технологии, нативные вычисления, TSC, технология цифрового двойника и другие. Однако эти технологии требуют более глубокого изучения и интеграции в архитектуру 6G.

Детали архитектуры 6G нуждаются в дальнейшем исследовании и определении в организациях, занимающихся стандартами. Также остаются открытые технические вопросы, которые нужно изучить, чтобы достичь эволюции архитектуры 6G, например, вопросы разделения сетей и создания механизма межуровневых вызовов. Исследования и работы в этой области до сих пор ведутся, но с каждым днём мир всё ближе к реализации.

Список используемых источников:

1. Meroua Moussaoui, Emmanuel Bertin, and Noël Crespi Divide and Conquer: A Business Model Agenda for Beyond-5G and 6G [Электронный ресурс] // IEEE Communications Magazine, 2023, 82 p. URL: https://hal.science/hal-04084160/document (дата обращения: 17.10.2023).

2. M. A. Uusitalo et al., 6G Vision, Value, Use Cases and Technologies From European 6G Flagship Project Hexa-X. IEEE Access, vol. 9, Nov. 2021, pp. 160,004–20. [Электронный ресурс]. URL: https://research.chalmers.se/publication/527418/file/527418_Fulltext.pdf (дата обращения: 17.10.2023).

3. W. Jiang et al., The road towards 6G: A Comprehensive Survey. IEEE Open J. Commun. Society, vol. 2, Feb. 2021, pp. 334–66. [Электронный ресурс]. URL: https://arxiv.org/pdf/2102.01420.pdf (дата обращения: 17.10.2023).

4. Xiao Dong Duan et al., 6G Architecture Design: from Overall, Logical and Networking Perspective. IEEE Communications Magazine, July 2023, pp. 158-164. [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/10192290 (дата обращения: 17.10.2023).

Maksimov A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

6g architecture design.

This article discusses the importance of network architecture for the next generation of cellular networks and proposes high-level 6G architecture designs. Based on operators' experience and analysis of 5G network shortcomings, key innovation motives and 6G architecture design principles are identified. A novel "3-body, 4-layer, 5-plane" architecture is proposed, along with a corresponding service-based logical functional architecture (HSBA) and distributed autonomous network (DAN). These proposals are a direction for future research in network architectures.

Key words: 6G, architecture, HSBA, DAN, network slicing, TSC, 5G.

УДК 621.396.6
ГРНТИ 89.29.02

МОДЕЛИРОВАНИЕ СПУТНИКОВОГО КАНАЛА СВЯЗИ В СРЕДЕ MATLAB SIMULINK

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

Представлен процесс поэтапного моделирования спутникового канала связи в среде Matlab Simulink. В ходе работы смоделированы блок генерации и модуляции сигнала, линия связи земная станция - спутник, блок генерации шума, блок изменения несущей частоты, линия связи спутник - земная станция, блок демодуляции, а также блоки контроля уровня сигнала на каждом этапе моделирования. Данная модель позволяет рассчитать необходимый уровень передаваемого сигнала для прохождения канала связи, а также осуществить контроль прохождения сигнала по каналу связи. Тестирование модели показало, что модель полностью работоспособна.

Matlab Simulink, спутниковый канал связи, модель линии связи

Введение

В современном мире спутниковые системы передачи данных приобретают широкое распространение, что позволяет осуществить радиоинформационный обмен данными на огромных расстояниях между источником сообщения и получателем. Спутниковые системы передачи данных предоставляют возможность непрерывного обслуживания труднодоступных регионов и удаленных от основной инфраструктуры объектов. В таких случаях спутниковые системы связи не имеют альтернативы. Быстрые темпы роста систем связи требуют точного анализа и моделирования для безошибочного проектирования и освоения новых территорий покрытия. В данной работе представлено поэтапное моделирование канала связи для спутниковых линий передачи данных.

Моделирование

Моделирование проводится в Matlab Simulink [1]. Первым этапом моделирования линии связи является создание модуля для генерации сигнала. Первым блоком модели является блок генерации и модуляции сигнала. После прохождения этого блока поставлен спектрометр для контроля работы модели. Спектр сигнала на выходе блока генерации и модуляции представлен на рис. 1.

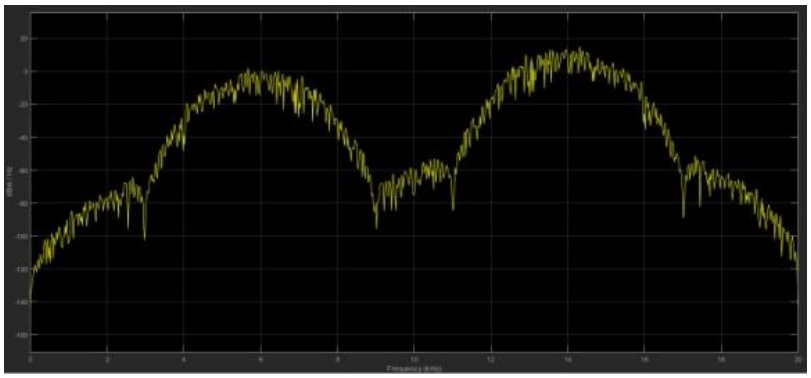


Рис. 1. Спектр сигнала после модуляции

Следующий пункт в моделировании линии спутниковой связи – моделирование линии связи вверх. Модель линии состоит из блоков усиления и ослабления, что позволяет посмотреть, как меняется сигнал по мере прохождения от земной станции до спутникового приемника [3]. Также в данной схеме представлен блок генерации шума. Рис. 2 показывает внешний вид модели линии связи.

Рис. 2. Модель линии связи земная станция – спутник

Рассмотрим подробнее блок генерации шума. Блок состоит из генератора шума и блока ослабления, который необходим для поддержания необходимого соотношения сигнал шум. Для контроля правильности моделирования на данном этапе установлен ряд спектрометров и блок измерения соотношения сигнал/шум. Полученные на блоке контроля спектрограммы представлены на рис. 3, 4 и 5.

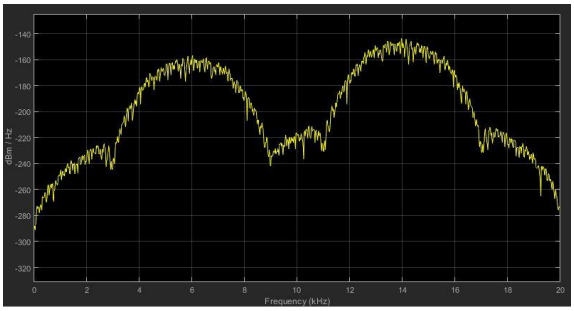


Рис. 3. Сигнал после прохождения канала связи (не зашумленный)

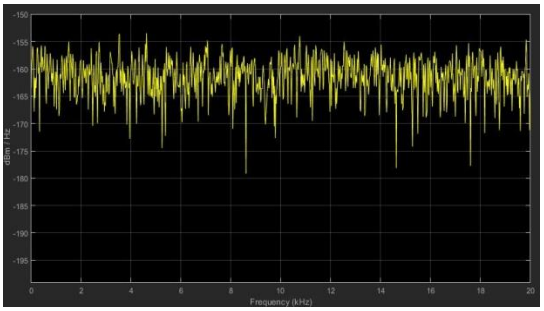


Рис. 4. Спектрограмма сгенерированного шума

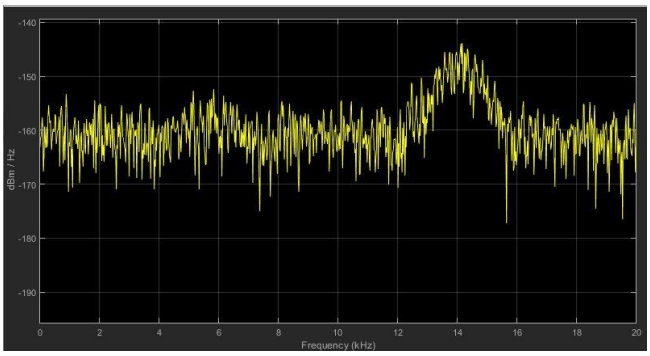


Рис. 5. Сигнал после прохождения канала связи и добавления шума

Так как на спутнике осуществляется изменение частоты сигнала с 14 ГГц на 11 ГГц, следующий блок переносит сигнал на более низкую частоту [2].

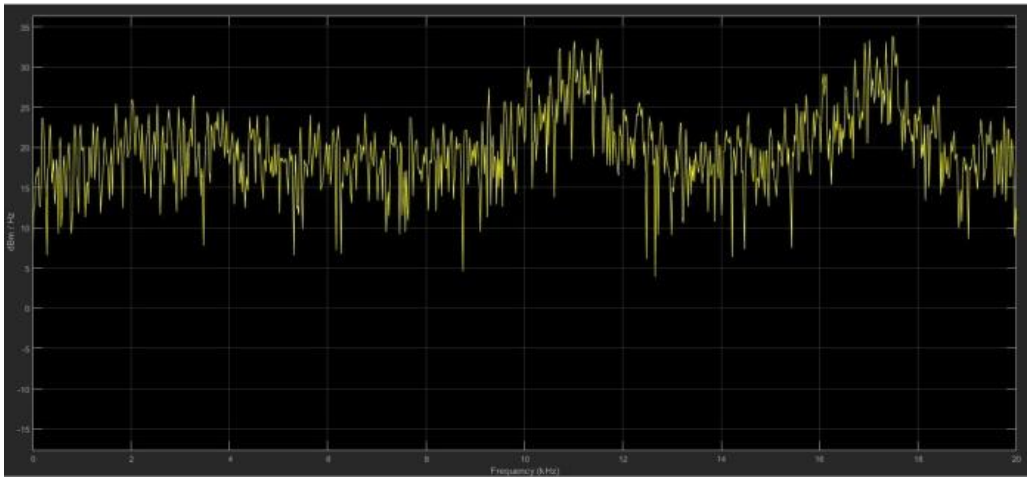


Рис. 6. Спектрограмма сигнала с измененной несущей частотой

Дальнейшим этапом моделирование следует линия связи спутник – земная станция. Непосредственно в эту линию передачи добавлен полосовой фильтр, для выделения полезного сигнала. На рис. 7 представлена спектрограмма сигнала полученного земной станцией после фильтрации. Спектрограмма на рис. 7 показывает, что фильтр работает правильно.

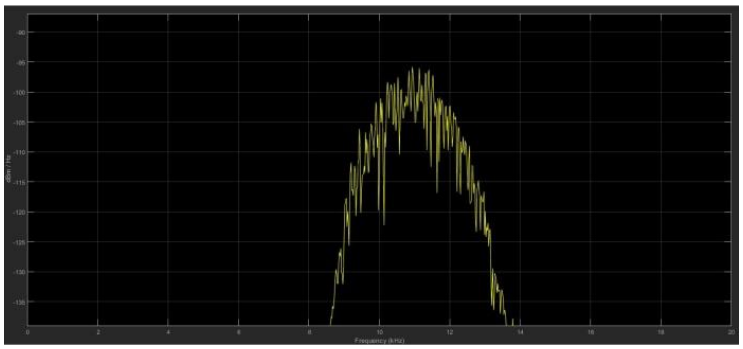


Рис. 7. Спектрограмма сигнала полученного земной станцией после фильтрации

После приема сигнала земной станцией необходимо перенести его на низкую частоту. Результат работы блока переноса представлен на рис.8. График позволяет увидеть успешный перенос сигнала на более низкую частоту.

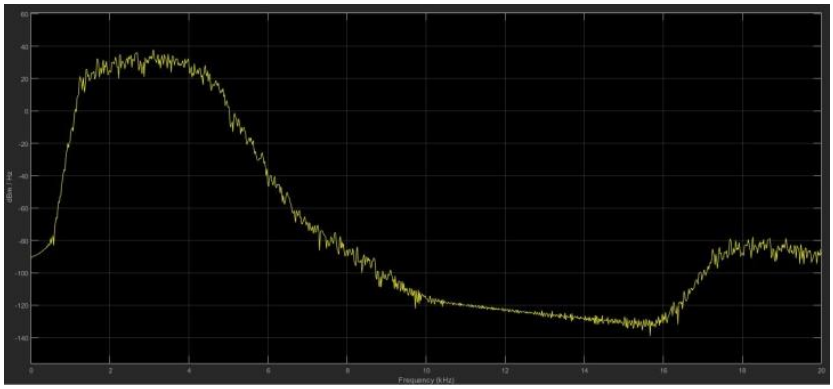


Рис. 8. Спектрограмма сигнала после переноса на низкую частоту

Финальным блоком модели является блок демодуляции. Рис. 9 показывает сгенерированный сигнал и сигнал на выходе разработанной модели. Представленные графики позволяют убедиться в правильной работе модели.

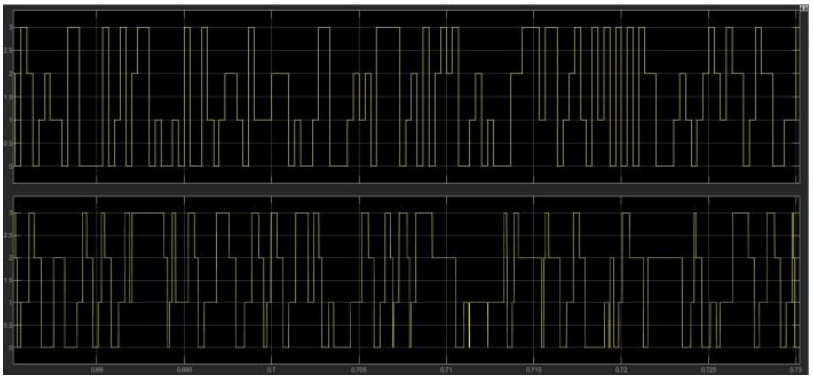


Рис. 9. Входной и выходной сигнал

Общий вид модели представлен на рис. 10.

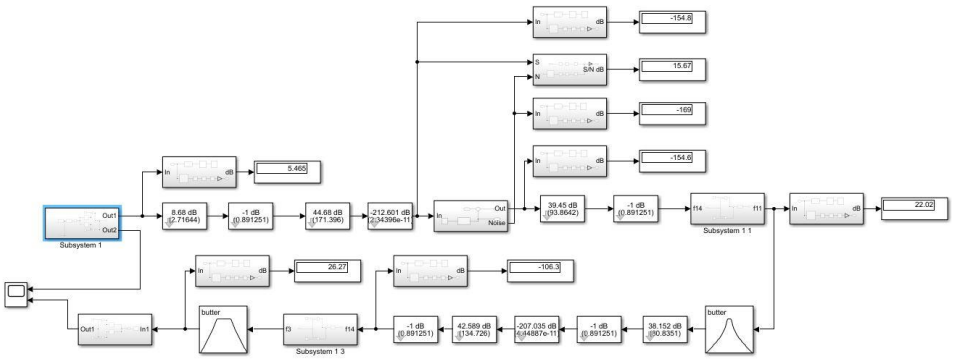


Рис. 10. Общий вид модели

Заключение

В данной работе представлено поэтапное проектирование спутникового канала связи для передачи данных в среде разработки Matlab Simulink. Данная модель позволяет рассчитать необходимый уровень передаваемого сигнала для прохождения канала связи, а также осуществить контроль прохождения сигнала по каналу связи, что подтверждается в процессе работы модели, сигнал на выходе соответствует сигналу на входе моделируемого канала связи. На основе приведенных спектрограмм можно удостовериться, что модель создана правильно, полностью работоспособна и дает возможность применения в аналитической сфере проектировки каналов спутниковой связи для передачи данных. В дальнейшем данная модель может послужить при анализе повышения энергетической эффективности линий спутниковой связи, что позволит сократить затраты на передачу данных на протяженные расстояния и обеспечить возможностью передачи данных в самые труднодоступные регионы планеты.

Список используемых источников:

1. Mathworks / [Электронный ресурс] // Mathworks : [сайт]. - https://uk.mathworks.com/products/simulink.html (дата обращения 28.10.2023).

2. Макаренко С. И. Описательная модель системы спутниковой связи Inmarsat //Системы управления, связи и безопасности. 2018. N. 4. С. 64-91.

3. Михайлов Р. Л. Описательные модели систем спутниковой связи как космического эшелона телекоммуникационных систем специального назначения. 2019.

Podlevskikh A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Modeling of a satellite communication channel in the matlab simulink environment.

The process of step-by-step modeling of a satellite communication channel in the Matlab Simulink environment is presented. In the course of the work, the signal generation and modulation unit, the Earth station-satellite communication line, the noise generation unit, the carrier frequency change unit, the satellite-Earth station communication line, the demodulation unit, as well as signal level control units at each stage of the simulation were modeled. This model allows you to calculate the required level of the transmitted signal for the passage of the communication channel, as well as to monitor the passage of the signal through the communication channel. Testing of the model showed that the model is fully functional.

Key words: Matlab Simulink, satellite communication channel, communication line model.

УДК 621.398
ГРНТИ 49.43.29

ОРГАНИЗАЦИЯ СИСТЕМЫ СВЯЗИ ДЛЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ НА ОСНОВЕ LORA С ЦЕЛЬЮ ПЕРЕДАЧИ ДАННЫХ УПРАВЛЕНИЯ НА БОЛЬШИЕ РАССТОЯНИЯ

С. И. Попович, А. Г. Чернышов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена разработке и оптимизации систем связи на базе технологии LoRa для беспилотных летательных аппаратов. Исследование представляет методы устойчивой связи на дальние расстояния, что имеет важное значение для дальнейшего развития и применения беспилотных летательных аппаратов в различных областях, включая мониторинг и связь в отдаленных и труднодоступных регионах. Расчеты проведены для нелицензируемых частотных диапазонов 868 МГц с учетом ограничений нормативно-правовой базы, использованы параметры реально применяемого оборудования, описанные в технической документации.

технология *LoRa*, беспилотный летательный аппарат, радиосвязь, дальность радиосвязи

В современном мире широкое распространение получили различные автоматизированные системы на базе беспилотных или управляемых летательных средств, использующиеся для решения широкого спектра задач: картографирование местности, разведка объектов различного назначения, мониторинг окружающей среды, наблюдение за транспортом, а также использование их в качестве средств доставки товаров различного назначения. Большинство из возникающих прикладных задач таких систем связаны с мониторингом определенной территории. Целью такого мониторинга может быть выявление посторонних лиц, контроль состояния природных и искусственных объектов.

Система связи между дроном и пунктом управления — один из важнейших аспектов беспилотных летательных аппаратов (БПЛА). Она обеспечивает передачу команд управления контроллеру полёта, передачу данных о текущем состоянии основных систем, а также данные о местоположении летательного аппарата. Все перечисленные типы сведений, обмен которыми происходит в процессе выполнения любого лётного задания, могут быть объединены в одну группу — данные телеметрии. Эти данные позволяют оператору не потерять дрон.

Помимо критически важных данных, о которых шла речь ранее, системой связи решается задача передачи информации от устройств «полезной нагрузки» БПЛА (фото/видео камеры, дальномеры и различные датчики, установленные на борту). На рис. 1 представлена общая схема системы связи беспилотника и станции управления.

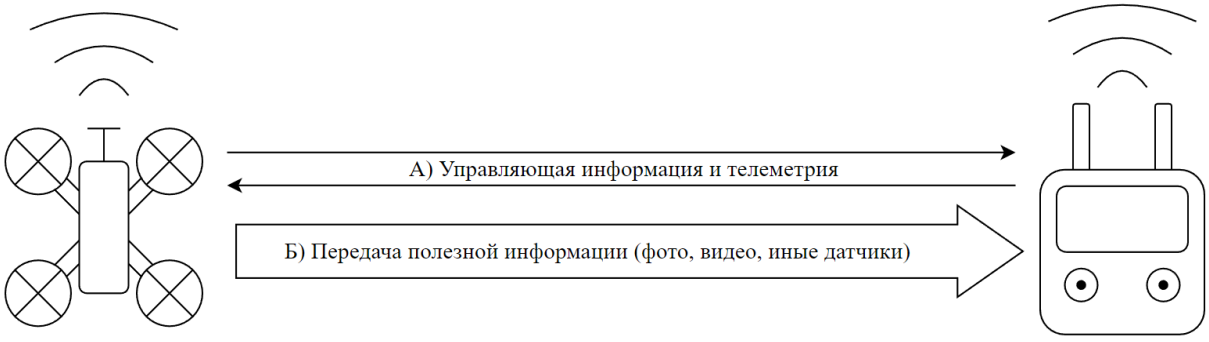


Рис. 1. Система связи БПЛА – наземная станция управления

Для сохранения БПЛА необходимо использовать наиболее помехозащищенные способы модуляции, которые способны противостоять широкому кругу радиопомех. При этом они должны обеспечивать минимальное потребление энергии, быть автономными в случае выхода аккумуляторов из строя, что позволит осуществить поиск потерянного аппарата, иметь дальность передачи сигнала равной или большей маршрута использования беспилотника.

Технология *LoRa* (*LongRange*) позволяет осуществлять передачу небольших порций данных на расстояния до 15 км на открытом пространстве и до 5 км в городской застройке на нелицензируемых частотах 864-865 МГц. LoRa использует метод модуляции спектра с расширенным спектром и вариации линейной частотной модуляции (ЛЧМ) (*Chirp Spread Spectrum*, *CSS*), который обеспечивает значительно большую дальность связи (зону покрытия), чем другие конкурирующие с ним способы.

Этот метод используется в военной и космической связи уже более десятилетий из-за его надежного характера и дальности действия. В настоящее время он используется в коммерческих целях для связи *LoRa*. Он также обеспечивает невосприимчивость к многолучевому распространению и замираниям. Расширенный спектр ЛЧМ требует низкой мощности передачи. Чирп (*Chirp*) — это сигнал, частота которого увеличивается или уменьшается со временем.

При ЛЧМ-модуляции с расширенным спектром полезный сигнал данных умножается на ЛЧМ-сигнал. Это расширяет полосу пропускания за пределы полосы пропускания исходного сигнала данных. На приемном конце полученный сигнал повторно умножается на локально сгенерированную копию сигнала ЛЧМ. Это сжимает модулированный сигнал обратно к исходной полосе пропускания, что способствует уменьшению шума и помех.

Рассмотрим способ передачи управляющей информации «прямая связь», который используется для управления большинства коммерческих БПЛА. В качестве примера для исследования был выбран модуль *LoRa* на базе *SX1276*.

ТАБЛИЦА 1. Основные характеристики SX1276

Частота, МГц	868/915
Мощность излучения, дБм	19
Чувствительность приемника, дБм	-135

Коэффициент усиления антенны, дБ	2
Высота подвеса передающей антенны, м	30
Высота подвеса приемной антенны, м	1,5
Потери в АФУ, дБ	4

Анализ проводился по эмпирической модели расчета затухания сигнала Окамура-Хата для городской застройки и сельской местности (рис. 2).

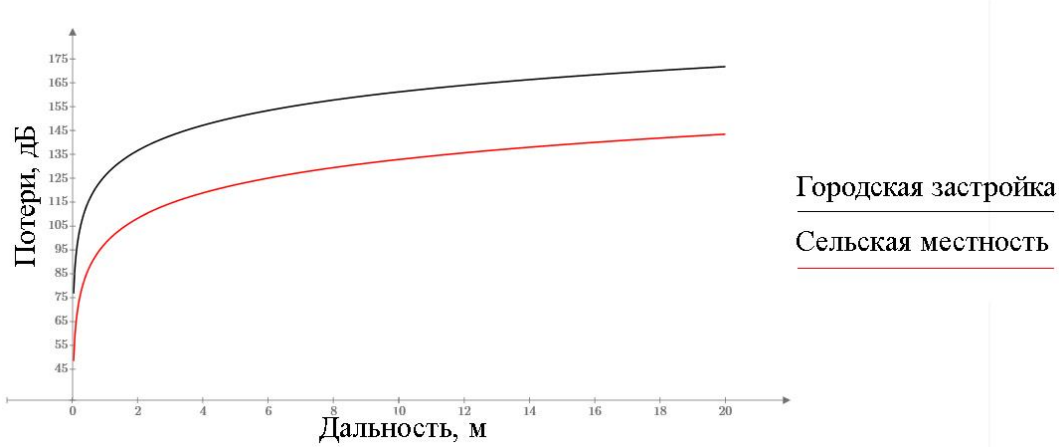


Рис. 2. Графики затухания сигнала, рассчитанного по модели Окамура-Хата

Технология *LoRa* значительно повышает чувствительность приемника и, аналогично другим методам модуляции с расширенным спектром, использует всю ширину полосы пропускания канала для передачи сигнала, что делает его устойчивым к канальным шумам и нечувствительным к смещениям, вызванным неточностями в настройке частот при использовании недорогих опорных кварцевых резонаторов. Как показал расчет по эмпирической модели Окамура-Хата – дальности в городской застройки не превышают 5 км, но на открытой местности – более 20 км (рис. 3).

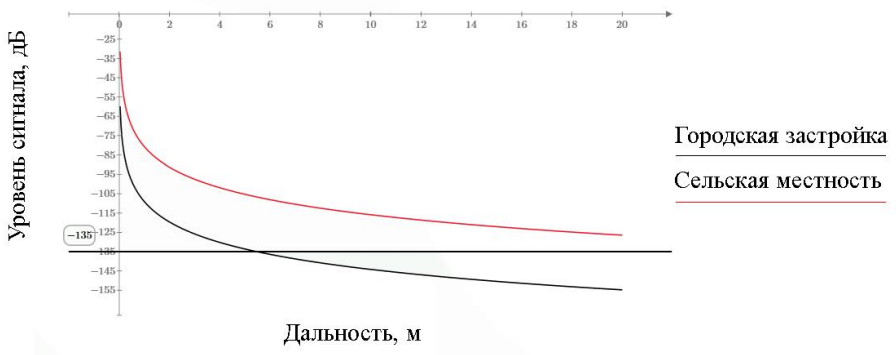


Рис. 3. Уровень сигнала по мере отдаления БПЛА от пульта управления

Немаловажный критерий – срок службы батареи. Большинству встроенных устройств необходимо обмениваться данными с другими

устройствами поблизости или далеко. Это потребляет большую мощность. Все встроенные устройства в основном работают от аккумуляторов. Таким образом, основным требованием к этим встраиваемым устройствам является срок службы батареи. *LoRa* оптимизирует расход заряда батареи в устройстве и больше всего подходит для встраиваемых устройств с батарейным питанием.

Низкое потребление батареи в сетях *LoRa* объясняется асинхронной связью узлов в сети. Узлы обмениваются данными только тогда, когда у них есть какие-либо данные для отправки, будь то энергетические или запланированные. Они используют метод *ALOHA*. В методе *ALOHA* кадр отправляется только тогда, когда есть какие-либо данные для отправки, в противном случае передача не происходит. Если кадр получен успешно, отправляется другой кадр или повторно передается тот же кадр.

Таким образом, *LoRa* обеспечивает надежную связь на большие расстояния при минимальном энергопотреблении. Это преимущество идеально сочетается с требованиями систем управления БПЛА, где надежность и продолжительность работы на передовом крае играют решающую роль. Это открывает новые горизонты для применения беспилотных летательных аппаратов, делая их более доступными и эффективными в самых разнообразных задачах.

Список используемых источников:

1. Semtech A. N. Semtech, A. N. 120022, LoRa Modulation Basics. – 2015. URL: http://www.semtech.com/images/datasheet/an1200.22pdf (дата обращения: 25.10.2023).

2. LoRaWAN Specification V1.1 [Электронный ресурс] // LoRa Alliance, 2017. URL: https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf (дата обращения: 25.10.2023).

3. Specifications of the Heltec WiFi LoRa 32. URL: https://heltec.org/project/wifi-lora-32/ (дата обращения: 25.10.2023).

3. Боев Н. М. Анализ командно-телеметрической радиолинии связи с беспилотными летательными аппаратами // Вестник СибГАУ. 2012. N 2 (42). С. 86–91.

4. Боев Н. М., Шаршавин П. В., Нигруца И.В. Построение систем связи беспилотных летательных аппаратов для передачи информации на большие расстояния // Изве-стия ЮФУ. Технические науки, 2015. 12 с.

5. Dovgal V. A. Decision-making for placing unmanned aerial vehicles to implementation of analyzing cloud computing cooperation applied to information processing // 2020 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). IEEE, 2020. С. 1-5.

6. Aden Hassan A., Karlsson Källqvist R. Evaluating LoRa Physical as a Radio Link Technology for use in a Remote-Controlled Electric Switch System for a Network Bridge Radio-Node. 2019.

7. Клочков В. Е., Андриянов Н. А. Анализ IoT и его перспектив //Актуальные проблемы физической и функциональной электроники. 2018. С. 111-112.

Popovich S., Chernyshov A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

LoRa-based communication system organization for drones to transmit control data over long distances.
The work is devoted to the development and optimization of communication systems based on LoRa technology for drones. The research presents methods of sustainable long-range communication, which is important for further development and application of drones in various fields, including monitoring and communication in remote and hard-to-reach regions. The calculations were carried out for unlicensed frequency bands of 868 MHz taking into account the limitations of the regulatory framework, the parameters of actually used equipment described in the technical documentation were used.

Key words: LoRa technology, drone, radio communication, radio communication range

УДК 621.396
ГРНТИ 81.93.29

АНАЛИЗ ОГРАНИЧЕНИЙ ПЕРЕДАЧИ ВИДЕОИНФОРМАЦИИ ДЛЯ СВЯЗИ С НАЗЕМНЫМИ РОБОТЕХНИЧЕСКИМИ КОМПЛЕКСАМИ

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

Наземные беспилотные аппараты получают все более широкое распространение в современном мире. Такие устройства используются в различных областях, от доставки товаров до служб спасения. Одной из проблем в данной области является сложность в проектировании канала для наземных беспилотных аппаратов.

беспилотные аппараты, радиосвязь, радиодоступ, дистанционное управление, каналы связи

В современном мире существуют различные наземные беспилотные аппараты. Такие роботы могут быть автономными или управляться дистанционно. Области применения таких роботов широко варьируются, в настоящее время такие устройства применяются в доставке товаров, складской логистике, горнодобывающей промышленности, а также для нужд экстренных служб [1, 2].

Наземные беспилотные аппараты актуальны в современном мире благодаря своей способности решать разнообразные задачи, включая опасные и труднодоступные для человека. Они находят применение в исследованиях, горнодобывающей промышленности, сельском хозяйстве, строительстве, поиске и спасении, а также во многих других областях. Автоматизация и оптимизация процессов, экономия ресурсов, исследования в неприступных местах, продвижение технологии и инноваций, а также использование в экстренных ситуациях делают их неотъемлемой частью современного общества и технологического прогресса.

Вне зависимости от области применения такие машины объединяет наличие радиоканала. На рис. 1 представлен универсальный «робот-пес» от *Boston Dynamics.*

Рис. 1. Прототип робопса

Радиоканал часто используется для управления роботами по нескольким ключевым причинам. Во-первых, нет необходимости прокладывать кабельные линии связи между роботом и оператором, что снижает затраты и упрощает соединение на большой дистанции . Во-вторых, радиоволны обладают способностью проникать через преграды, такие как стены и здания, что дает роботам возможность работать в разнообразных окружающих средах. Третья важная причина – радиоуправление позволяет дистанционно управлять роботами, что особенно важно в задачах, где безопасность оператора может быть под угрозой, например, при разминировании или в экстремальных условиях.

Однако, при проектировании радиоканала для наземных роботов возникают значительные сложности, которые в некоторых аспектах даже превосходят те, что возникают при разработке канала для беспилотных летательных аппаратов. Далее рассматривается причина актуальности этой проблемы и вызовы, которые стоят перед инженерами и исследователями в этой области.

В сравнении с беспилотными летательными аппаратами, наземные роботы часто имеют ограниченную высоту подвеса антенн для радиосвязи. Это связано с тем, что они должны оперировать на земной поверхности и преодолевать различные препятствия, такие как стены, деревья и неровности местности. Низкая высота антенн означает, что они подвержены большему влиянию интерференции и многим другим факторам, которые могут существенно ухудшить качество связи.

Помимо интерференции и низкой высоты подвеса антенн, проектирование радиоканала для наземных роботов сопровождается рядом других сложностей:

1. Жесткое требование к задержкам: Задержка в радиосвязи между оператором и наземным роботом должна быть минимальной, чтобы обеспечить мгновенное и точное управление роботом. Однако в реальных условиях задержка зависит от различных факторов, таких как расстояние между устройствами, качество сигнала, пропускная способность канала и другие технические аспекты;
2. Многолучевое распространение: Наземные мобильные роботы могут находиться в окружении, где сигналы многократно отражаются от близлежащих объектов, что приводит к многолучевому распространению сигнала, что требует применения технологий, позволяющих бороться с этим эффектом.
3. Энергопотребление: Мобильные роботы ограничены в электропитании от АКБ. Радиосвязь может потреблять значительное количество энергии, например, при использовании высоких частот для передачи данных. Также для передачи на большие расстояния требуется больше энергии из-за необходимости усиления мощности передатчика;

4. Область покрытия и мобильность: Роботы могут перемещаться по различным типам местности, включая: городскую застройку, здания, леса, горные районы. Поэтому необходимо разработать радиоканалы, способные обеспечить устойчивую связь в различных условиях и на различных расстояниях;

5. Взаимодействие с другими устройствами: В окружающей среде могут находиться другие источники радиосигналов, такие как Wi-Fi сети, Bluetooth устройства и многие другие. Могут возникать конфликты частот, необходимо учитывать этот аспект при проектировании радиоканала.

Необходимо учесть, что для работы с технологическим роботизированным комплексом необходимо два канала: дистанционного управления и передачи видеоинформации. Упрощенная схема изображена на рис. 2.

Рис. 2. Схема передачи данных

Особенности проектирования канала дистанционного управления: этот канал необходим для передачи команд, для него необходимы минимальные задержки, большая дальность. Так как сигнальная информация обладает небольшим объёмом, делать его высокоскоростным нет необходимости. Для передачи видеоданных необходим канал с высокой скоростью передачи данных, так как передаваемое изображение необходимо получать в высоком качестве с низкой задержкой.

Для формирования канала передачи видеоинформации были предъявлены следующие требования [3]:

1. Дальность связи: для городской застройки – 300-500 метров, для прочих типов застройки – 1500 метров.
2. Высокое качество изображения включая HD.
3. Задержка команд дистанционного управления не более 100 мс.
4. Задержка передачи и отображения информации на управляющем устройстве не более 300 мс.
5. Работа в помеховой обстановке.
6. Возможность работы нескольких беспилотных наземных аппаратов одновременно при непосредственной близости друг к другу.

Для выбора оптимальных частот и ширины полосы необходимо создать математическую модель, используя специализированные инструменты, например, MATLAB. С помощью MATLAB можно провести расчеты

каналов на разных частотах и с разной шириной полос. Таким образом, можно выбрать наилучший вариант для обеспечения максимальной дальности связи и минимизации воздействия интерференции.

Список используемых источников:

1. Добрынин Д. А. Беспилотные транспортные средства, современное состояние и перспективы // КИИ-2014 : материалы XIV национальной конф. по искусственному интеллекту с международным участием, Казань, 24-27 сент. 2014 г. Казань : НИУ ВШЭ, 2014. Т. 3. С. 265.

2. Лопота А. В., Спасский Б. А. Мобильные наземные робототехнические комплексы профессионального назначения // Робототехника и техническая кибернетика. 2020. Т. 8. N 1. С. 5-17.

3. Попов Д. С., Шмаков О. А. Особенности применения каналов управления и передачи данных в составе мобильных роботехнических комплексов наземного базирования // Extreme Robotics. 2020. Т. 1. N 1. С. 302-309. ISSN: 2658-7645.

Romanova E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Ground unmanned vehicles are becoming increasingly widespread in the modern world. Such devices are used in various fields, from the delivery of goods to rescue services. One of the problems in this area is the complexity in designing a channel for ground-based unmanned vehicles.

Key words: unmanned vehicles, radio communication, radio control, remote control, communication channels.

УДК 621.396.969
ГРНТИ 47.49.31

ОЦЕНКА ВЛИЯНИЯ ПОГРЕШНОСТИ СИНХРОНИЗАЦИИ БАЗОВЫХ СТАНЦИЙ НА ТОЧНОСТЬ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ ПОЛЬЗОВАТЕЛЬСКИХ УСТРОЙСТВ

К. Е. Рютин, Г. А. Фокин
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Дальномерный метод позиционирования пользовательских устройств требует жесткой временной и частотной синхронизации источников навигационных сигналов. В сложившихся обстоятельствах интерес представляют отечественные решения для синхронизации удаленных сетевых устройств. В данном исследовании описан лабораторный эксперимент по оценке влияния погрешности синхронизации на точность определения местоположения пользовательских устройств с использованием отечественных серверов точного времени.

4G, LTE, SDR, синхронизация, позиционирование

Введение

Данное исследование посвящено разработке подсистемы синхронизации базовых станций (*eNB*) для целей определения местоположения (ОМП) пользовательских устройств (*UE – User Equipment*) в сети *LTE* (*Long-Term Evolution*). В качестве выбранного метода позиционирования выступает разностно-дальномерный метод *Observed Time Difference Of Arrival* (*OTDOA* – наблюдаемая разность времён прихода).

Полевые испытания разработанного прототипа технологии сетевого позиционирования *LTE* показали субметровую точность ОМП при нахождении *UE* внутри периметра расположения *SDR*-макетов *eNB*, когда геометрический фактор точности (*HDOP – Horizontal Dilution Of Precision*) меньше единицы [1]. При этом достигнутая точность ОМП напрямую зависит от точности синхронизации макетов *eNB*, ведь для выбранного метода позиционирования необходима жесткая временная и частотная синхронизация источников навигационных сигналов.

Подсистема синхронизации при полевых испытаниях

В ходе проведения полевых испытаний использовалась подсистема синхронизации *eNB*, состоящая из сервера точного времени «Метроном-PTP-1U-V2» и транслятора «Метроном-Т» отечественного производства.

В данной системе выходы 1 *PPS* и 10 МГц сервера точного времени подключаются коаксиальными кабелями к соответствующим входам транслятора, а уже с него раздаются на 4 макета *eNB* [1]. При анализе на осциллографе двух каналов 1 *PPS* транслятора, начальные фазы импульсов синхронизации отстоят друг от друга примерно на 1 нс, что позволило получить вышеописанную точность ОМП, а также использовать данную

систему синхронизации в качестве эталонной системы, с которой можно сравнивать все последующие решения в данном направлении работ.

Для оценки влияния погрешности синхронизации на точность ОМП при использовании эталонной системы синхронизации выходы сигналов 1 *PPS* и 10 МГц транслятора подключались к соответствующим входам двух макетов *eNB*, далее происходили синхронизация и запуск *eNB* на передачу сигнала стандарта *LTE*. Сигналы с двух макетов *eNB* суммировались в сплиттере, выход которого был подключён ко входу приёмного канала макета *UE* (рис. 1).

После приёма и демодуляции сигнала *LTE* макетом *UE*, выполнялась оценка дистанций между макетами *eNB* и макетом *UE*. Вследствие выполнения описанных процедур был получен ожидаемый результат на графике разностей дистанций для двух макетов *eNB* (рис. 2).

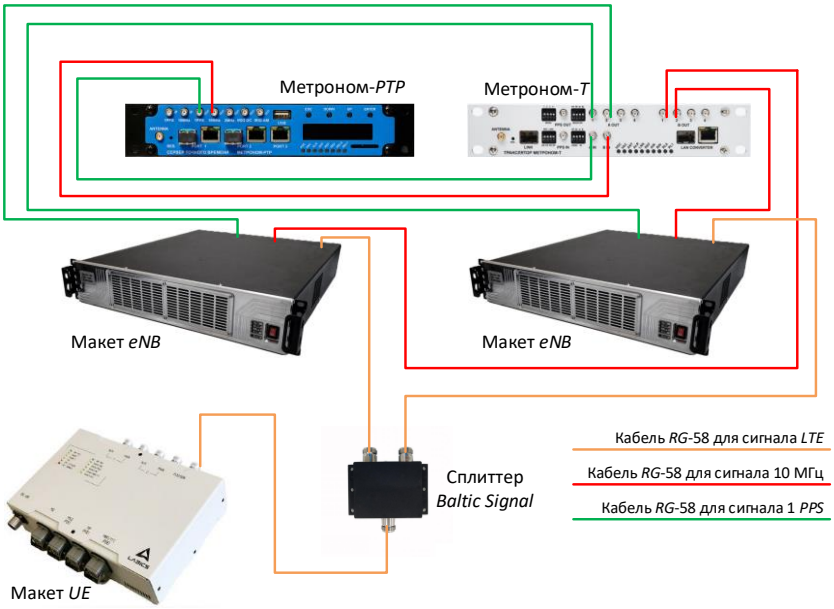


Рис. 1. Схема тестирования эталонной системы синхронизации

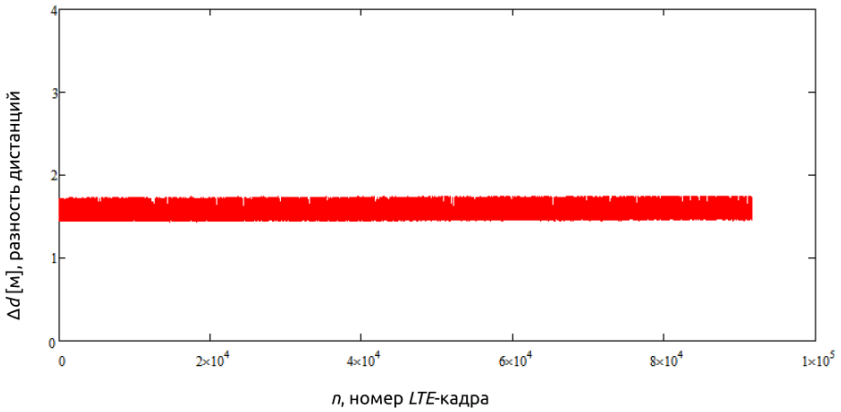


Рис. 2. Разности дистанций при использовании эталонной системы синхронизации

Анализ приведённого выше графика показывает, что вычислительная погрешность метода измерений [2] в сумме с приборной погрешностью трансивера (толщина линии) при использовании эталонной системы синхронизации постоянна и составляет примерно ±15 см, а погрешность синхронизации отсутствует, что очевидно следует из постоянства среднего значения оценок разностей дистанций на интервале наблюдения (рис. 2).
Однако, затухание в радиоканале делает невозможным стабильный приём сигналов синхронизации в контексте использования данной системы на реальной сети мобильной связи, где *eNB* отстоят друг от друга на сотни метров. Следовательно, о доступности и точности услуги позиционирования при таком подходе говорить не приходится.

Синхронизация метрономов по протоколу PTP

Далее последовала гипотеза о возможности синхронизации нескольких метрономов (по числу *eNB*) по сетевому протоколу синхронизации *PTP* (*Precision Time Protocol*) с точностью до единиц наносекунд. В такой системе один метроном, установленный на *eNB*, выступает ведущим (*Master*), а все остальные метрономы, установленные на соответствующих *eNB*, выступают в роли ведомых (*Slave*). В ходе проверки данной гипотезы с двумя метрономами, синхронизированными по протоколу *PTP*, удалось получить синхронизацию с точностью примерно 2,4 нс [3]. Однако, в ходе длительного (12,5 часов) наблюдения осциллограф зафиксировал плавный уход фазы сигнала 1 *PPS* ведомого метронома относительно фазы соответствующего сигнала ведущего в пределах 10 нс (рис. 3). Данное свойство напрямую сказывается на точность ОМП, ведь постоянный разбег фаз сигналов синхронизации можно скомпенсировать калибровкой при старте системы позиционирования, а непостоянный – нельзя.

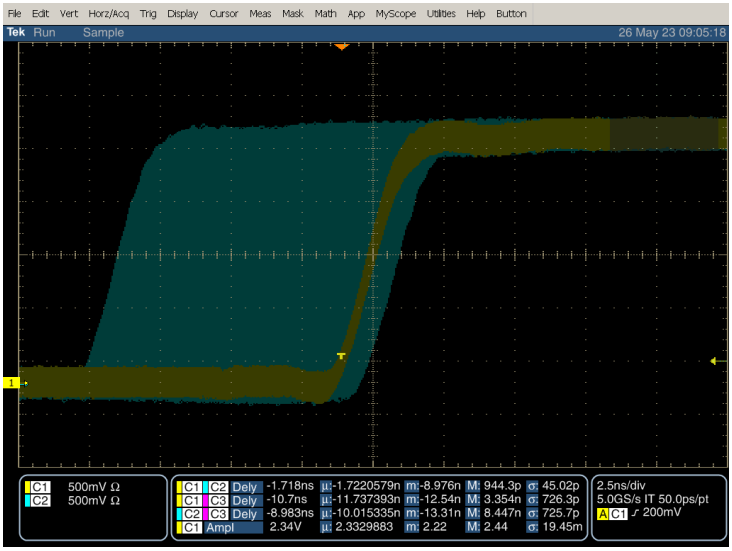


Рис. 3. Уход фазы сигнала 1 *PPS* ведомого метронома (канал 2) относительно сигнала 1 *PPS* ведущего метронома (канал 1) примерно на 10 нс

Для оценки влияния погрешности синхронизации на точность ОМП при использовании системы синхронизации метрономов по протоколу *PTP*, ведущий и ведомый метрономы соединялись между собой оптическим патчкордом, а также для контроля и настройки подключались в локальную сеть через сетевой коммутатор. Коммутация макетов *eNB* и *UE*, а также процедуры приёмопередачи сигналов *LTE* выполнялись аналогично описанию в предыдущем пункте (рис. 4). На рис. 5 представлен график разностей дистанций для двух макетов *eNB* при использовании системы синхронизации по протоколу *PTP*.

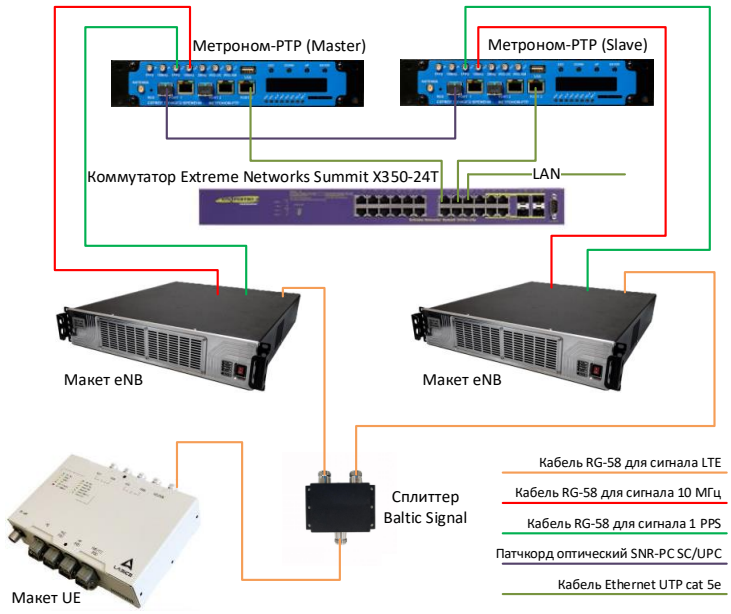


Рис. 4. Схема тестирования системы синхронизации метрономов по протоколу *PTP*

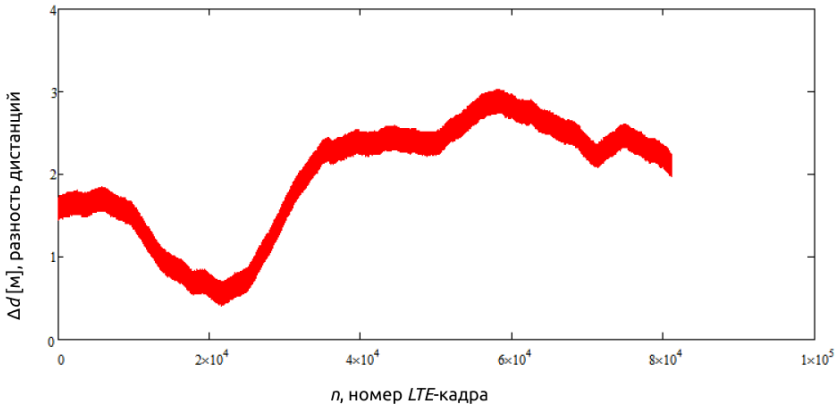


Рис. 5. Разности дистанций при использовании системы синхронизации метрономов по протоколу *PTP*

Анализ приведённого выше графика показывает, что вычислительная погрешность метода измерений [2] в сумме с приборной погрешностью трансивера (толщина линии) при использовании системы синхронизации метрономов по протоколу *PTP* равна погрешности, которая имела место для эталонной системы синхронизации (рис. 2). Однако, если применить к

данной последовательности отсчётов алгоритм скользящего среднего (или фильтр нижних частот), то можно заметить, что разности дистанций изменяются согласно некоторому неизвестному закону. Это изменение является погрешностью синхронизации, которая составляет, в данном случае, примерно ±1,25 м.

Заключение

В ходе проведения данного исследования выяснилось, что синхронизация отечественных метрономов по протоколу *PTP* даёт неудовлетворительный результат применительно к задаче ОМП с субметровой точностью, но полученной точности синхронизации вполне достаточно для задач организации связи.

Направлением будущих исследований и разработок является создание канала обратной связи, в котором *UE* будет передавать *eNB* поправки для коррекции их синхронизации.

Список используемых источников:

1. Фокин Г., Григорьев В., Рютин К., Комиссаров А., Волгушев Д. Технология сетевого позиционирования LTE. Часть 4. SDR-демонстратор в полевых условиях // Первая миля. 2023. N 4. С. 34–41;

2. Фокин Г. А., Волгушев Д. Б. Использование SDR-технологии для задач сетевого позиционирования. Процедуры приема и обработки опорных сигналов LTE [Электронный ресурс] // Вестник СибГУТИ. 2023. Т. 17, N 1. С. 52–65. https://doi.org/10.55648/1998-6920-2023-17-1-52-65. (дата обращения: 10.11.2023).

3. G. Fokin, K. Ryutin, V. Grigoriev and V. Bobrovskiy, "Software-Defined Radio Network Positioning Technology Design. Synchronization Subsystem," 2023 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO, Pskov, Russian Federation, 2023, pp. 1-6, doi: 10.1109/SYNCHROINFO57872.2023.10178428;

Ryutin K., Fokin G.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Estimation of the impact of base station synchronization error on the positioning accuracy of user equipment.

The time-difference method of positioning user equipment requires strict time and frequency synchronization of navigation signal sources. In the current situation, Russian solutions for synchronization of remote network devices are of interest. This research describes a laboratory experiment to estimate the impact of synchronization error on the accuracy of positioning of user equipment using Russian precision time servers.

Key words: 4G, LTE, SDR, synchronization, positioning.

УДК 621.372.54
ГРНТИ 47.14.17

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ПОСТРОЕНИЯ ПЕРЕСТРАИВАЕМОГО ФИЛЬТРА ДИАПАЗОНА ЧАСТОТ ОТ 30 ДО 80 МГЦ

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

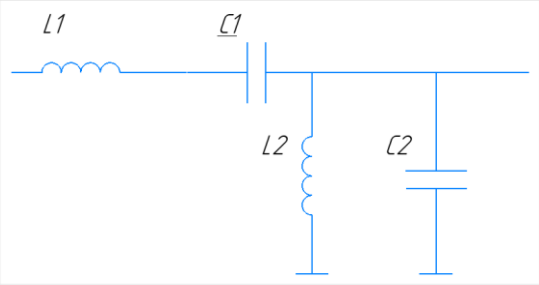
В работе рассматривается преселектор, используемый для подавления побочных каналов приема и согласования с первым усилительным каскадом УКВ диапазона и его сравнение с существующим на рынке преселектором. Устройство применимо для улучшения условий электромагнитной совместимости.

преселектор, УКВ, фильтр

Уменьшение помех приема на стационарном или подвижном объекте и присутствие разнесенного и совмещенного приема является важной составляющей радиостанции реализуемыми при помощи преселектора [1].

В настоящее время на рынке представлено только 1 устройство включающее в себя данный диапазон (Преселектор PS30-88). Преселектор PS30-88 это программно-управляемый перестраиваемый узкополосный фильтр работающий в диапазоне частот 30-88МГц. Преселектор обладает низкими вносимыми потерями, высокой электрической прочностью и высокой скоростью перестройки. Его мощность на входе 20Вт, из-за чего он применим только в мощной радиоприемной установке, что является чрезмерным в более простых усилителях, обладает большими габаритами вызванными большими катушками, и непонятной схемотнхникой, что препятствует возможности ремонта при неполадках. В этой статье представлен преселектор с мощностью на входе 0.18Вт лишенный данных ограничений.

В данной статье представлен концепт построения преселектора являющегося ВУ для частот 30-80МГц. Исходя из разумного количества



перестраиваемых контуров лучше всего составить 50 отдельных небольших полосовых фильтров Баттерворта 2-го порядка [2].

Рис. 1. Схема фильтра 2-го порядка Баттерворта

ТАБЛИЦА 1. Параметры преселектора

Параметр	Значение	Величина
Входное сопротивление	50	Ом
Выходное сопротивление	50	Ом
Мощность на входе	0.18	Вт
Неравномерность в полосе пропускания	0.5	дБ
Полоса частот каждого фильтра	2	МГц
КБВг	0.9	

На рис. 1 представлена принципиальная схема фильтров, в таблице 1 рабочие параметры преселектора.

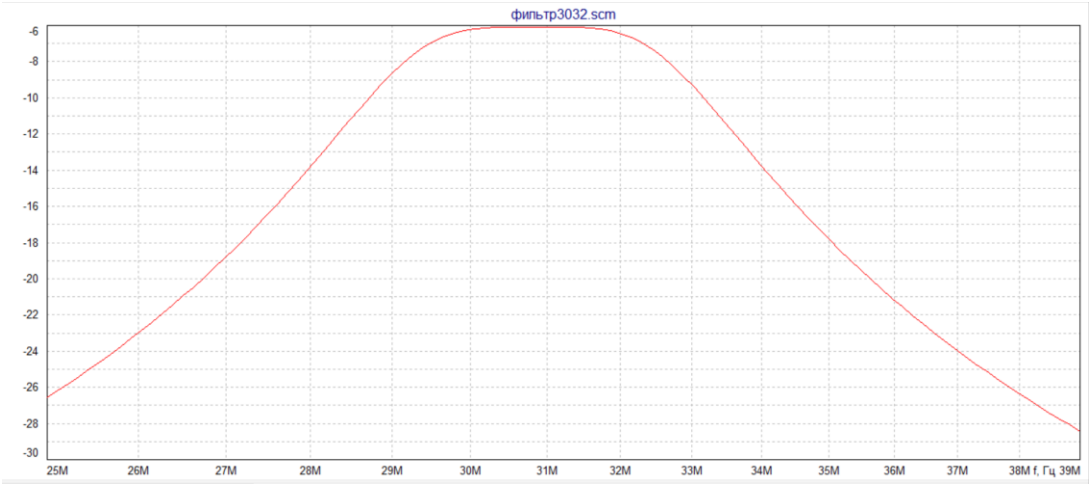


Рис. 2. АЧХ 30-32 МГц

ТАБЛИЦА 2. Номиналы фильтра 30-32МГц

Параметр	Значение	Номинал
L1	2.8	мкГн
C1	9.4	пФ
L2	24	нГн
C2	1120	пФ

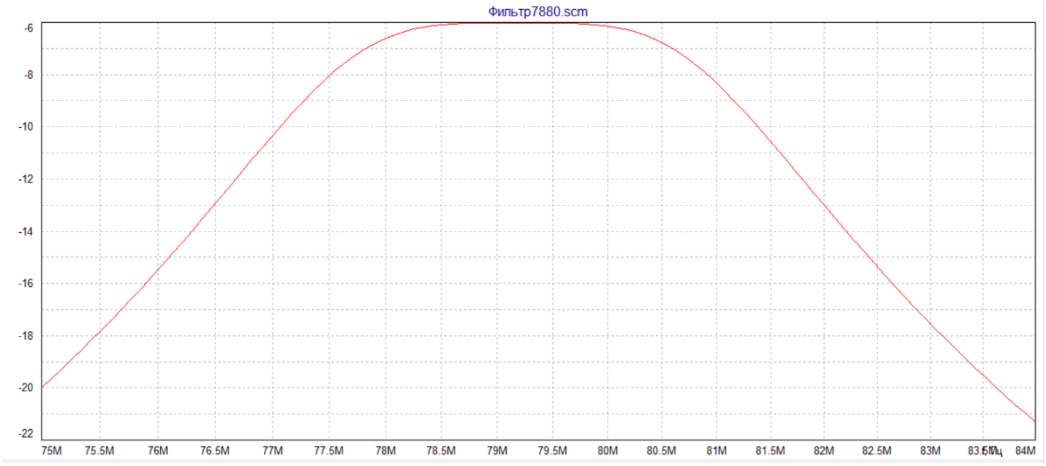


Рис. 3. АЧХ 78-80МГц

ТАБЛИЦА 3. Номиналы фильтра 78-80Мгц

Параметр	Значение	Номинал
L1	2,882	мкГн
C1	1.4	пФ
L2	3.5	нГн
C2	1155	пФ

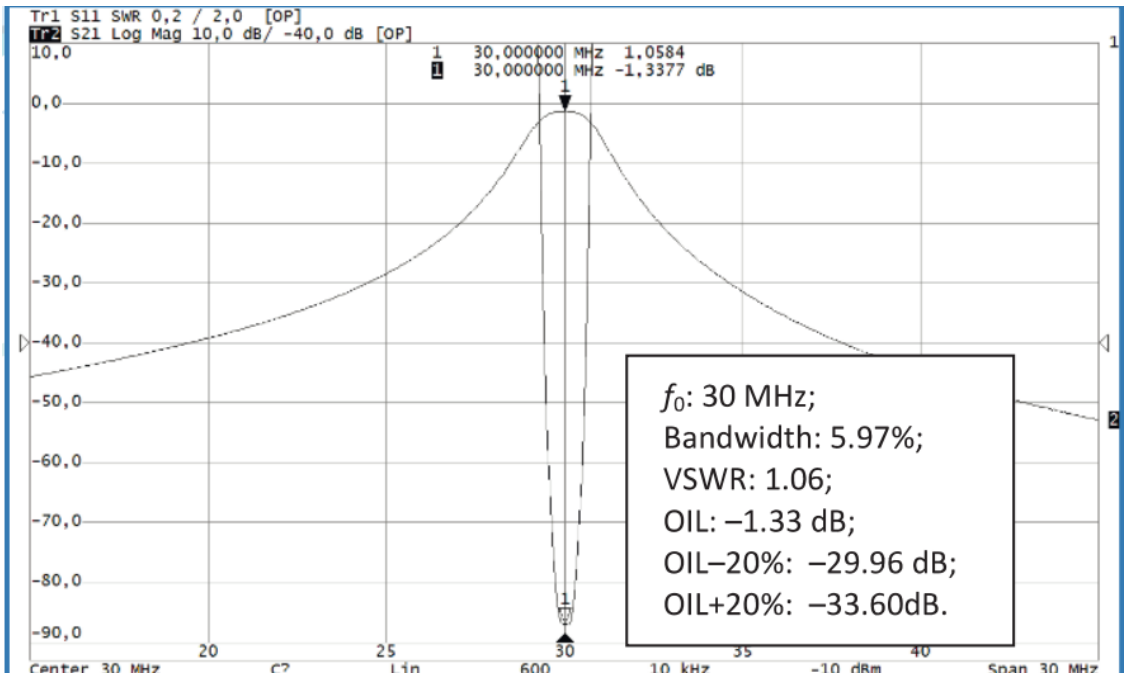


Рис. 4. АЧХ PS30-80 на частоте 30 МГц

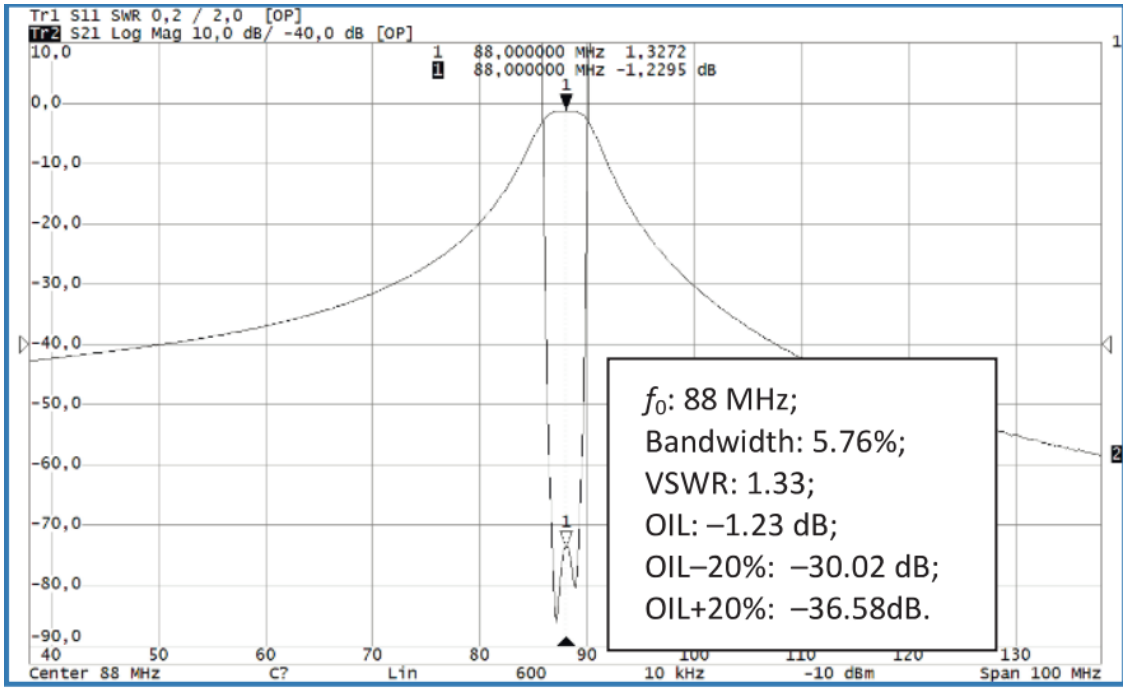


Рис. 4. АЧХ PS30-80 на частоте 88 МГц

На рис. 2 и 3 представлены АЧХ фильтров двух крайних рабочих полос частот. В таблице 2 и 3 параметры фильтров двух крайних рабочих полос часто. На рис. 4 и 5 представлены АЧХ фильтров двух крайних рабочих полос частот преселектора PS30-88 [3].

В связи с тем, что элементы C1 и L2 имеют очень малые номиналы, наилучшая реализация возможна при полосе частот равной 2МГц.Данная конфигурация обеспечивает перекрытие и исключает ситуацию с попаданием частоты на границу 2-х фильтров. Синтез представленного преселектора на порядок проще, чем преселектор PS30-88, который построен по принципу подбора сочетания элементов для фильтрации на необходимой частоте. Также размеры элементов малы, что позволяет уменьшить габариты минимум в 2 раза.

Таким образом, возможно построить фильтры для всего диапазона частот.

Список используемых источников:

1. Прасолов А. А. Приёмопередающие устройства в системах подвижной связи. Учебный курс.

2. Тюменцев А. И. Перестраиваемые полосовые фильтры // Динамика систем, механизмов и машин. 2012. N 3. С. 296-299. EDN SGNWAZ.

3. DataSheet на изделее преселектор PS30-88 [Электронный ресурс] // URL: https://uranis.pro/userfiles/File/Catalogs/10501072109010721083108610 75-108710881077108910771083107710821090108610881086 1074-22-25.pdf (дата обращения: 25.10.2023).

Smirnov D.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Study Of The Possibility Of Constructing A Tunable Filter For The Frequency Range From 30 To 80 MHz.

Study of the possibility of creating a tunable filter for the frequency range from 30 to 80 MHz. Tunable filters are used in every multi-frequency receiver and transmitter. The article discusses the option of constructing a low-power preselector with a frequency range from 30 to 80 MHz. The reason for studying the possibility of constructing a device is shown. The results are presented in the form of a comparison of the preselector under study with the Preselecor PS30-88 device, their differences and frequency response graphs.

Key words: preselector, frequency selection devices, filter VHF.

УДК 654.01
ГРНТИ 49.01.11

ОПТИМИЗАЦИЯ НАДЕЖНОСТИ ПРИ ПРОЕКТИРОВАНИИ И ВНЕДРЕНИИ СИСТЕМ 6G «АВТОМОБИЛЬНЫХ - ИНФРАСТРУКТУР» ДЛЯ УПРАВЛЕНИЯ ЧРЕЗВЫЧАЙНЫМИ СИТУАЦИЯМИ В СРЕДЕ «УМНОГО ГОРОДА»

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

Умные города и административные структуры представляют собой новую эру в транспортной мобильности, где надежные, качественные и своевременные коммуникационные системы играют ключевую роль в обеспечении безопасности, оперативности и эффективности передвижения. В свете грядущего широкомасштабного распространения спутниковых сетей 6G, эта статья рассмотрит важность мониторинга состояния транспортных средств и здоровья пассажиров, а также оптимизацию систем мониторинга транспортных средств и управления чрезвычайными ситуациями и пожарной безопасностью с целью обеспечения транспортной безопасности и качества обслуживания в умных и безопасных городах.

Интегрированный мониторинг

Профессиональный рост и развитие в сфере высоких технологий уже сейчас позволяют нам представить, насколько значимое место займут не только единая архитектура мобильных приложений, но и сами самоосознающие нейронные сети в будущих умных городах. Современные автомобили оснащены сложными системами мониторинга, включая сенсоры столкновений, которые обеспечивают безопасное и своевременное и точное обнаружение протечек и аварий.

Однако с развитием 6G возникают новые операционные вызовы, такие как обеспечение бесперебойной связи в экстремальных условиях, применение высокоскоростных смартфонов, высокую частоту, обеспечение максимальной скорости связи в экстремальных условиях и достижение максимально быстрого отклика в случае аварии. Важность разработки и реализации качественной, надежной антикризисной системы, которая остается работоспособной даже после серьезных дорожных столкновений, является актуальной задачей.

Сети самопознания

Системы связи между транспортными средствами и инфраструктурой (Vehicle-to-Infrastructure, V2I) должны автоматически обнаруживать неисправности и передавать критически важные данные в центры управления с минимальной задержкой. В этом процессе помогает концепция "самоосознающих" сетей, способных адаптироваться к различным условиям и поддерживать связь в любых обстоятельствах. Одним из ключевых аспектов обеспечения надежности является мониторинг состояния транспортных средств и здоровья пассажиров. Системы мониторинга,

включая сети сенсоров, анализируют данные о состоянии автомобиля и его пассажиров. В случае необычных ситуаций, таких как аварии, эти данные автоматически передаются в центры управления чрезвычайными ситуациями. Данный подход позволяет оперативно реагировать на чрезвычайные ситуации и обеспечивать надежное соединение, даже при сильных помехах и низком отношении сигнал/шум. Оптимизация надежности систем управления чрезвычайными ситуациями достигается благодаря интеграции мониторинга состояния транспортных средств и здоровья пассажиров. Функции самодиагностики и прогнозирования состояния помогают выявлять проблемы до того, как они станут критическими. Системы прогностики и управления состоянием здоровья не только обеспечивают безопасность путешествия, но и увеличивают срок службы компонентов, что является важным аспектом общей безопасности в умных городах.

Заключение

Развитие сетей 6G и внедрение самоосознающих сетей позволит значительно усовершенствовать системы управления чрезвычайными ситуациями и сделать "умные" города более безопасными для всех жителей и путешественников. Технические эксперты и инженеры будут играть ключевую роль в разработке и внедрении этих систем, поэтому им необходимо постоянно обновлять свои знания и навыки. Однако результат в виде безопасного и эффективного передвижения по "умным" городам стоит того, чтобы его дождаться.

Список используемых источников:

1. Reliability Optimization in the Design and Implementation of 6G Vehicle-toInfrastructure Systems for Emergency Management in a Smart City Environment // IEEE Communications Magazine. 2023. 148 p.

2. Oorni R. and Goulart A. In-Vehicle Emergency Call Services: Ecall and Beyond // IEEE Commun. Mag., V. 55, N 1, May 2017. pp. 159–65.

3. Yi H. et al. Tracing Meets Terahertz: Challenges and Opportunities // IEEE Commun. Mag., V. 60, N 10, Oct. 2022, pp. 1–7.

4. Aloqaily M., Elayan H. and Guizani M. C-healthier: ACooperative Health Intelligent Emergency Response Systemfor C-ITS // IEEE Trans. Intelligent Transportation Systems. V. 24, N 2, Feb. 2023, pp. 2111–21.

Strelnikov V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Smart cities and administrative structures represent a new era of transportation mobility in which reliable, quality and timely communication systems play a key role in ensuring safe, fast and efficient mobility given the upcoming widespread deployment of 6G satellite networks. Therefore, this paper discusses the importance of optimizing vehicle and passenger condition monitoring, tracking, and emergency and fire management systems to ensure transport safety and quality of service in smart and safe cities.

УДК 629.058
ГРНТИ 47.49.31

МОДЕЛИРОВАНИЕ ОТСЛЕЖИВАНИЯ GPS-ПРИЕМНИКА С ПОМОЩЬЮ С/А-КОДА

И. Г. Ушкова, Г. А. Фокин
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящей работе показано, как смоделировать исходную форму сигнала, содержащего код грубого приема (С/А-код), промежуточной частоты (ПЧ) системы глобального позиционирования (GPS) от нескольких спутников, добавить шум в составной сигнал, выполнить начальную синхронизацию и отследить кодовую фазу и несущую частоту доступных спутников, обнаруженных в результате операции начальной синхронизации. Отслеживание выполняется для каждого спутника независимо.

GPS, ПЧ, SNR

Все навигационные данные GPS состоят из 25 кадров, каждый из которых содержит 1500 бит. Эти навигационные данные включают в себя всю информацию об эфемеридах, часах и альманахе.

Поскольку скорость и положение каждого спутника различны, доплеровский сдвиг и доплеровская скорость, вводимые для каждого спутника, различны. Также каждый спутник находится на разном расстоянии от GPS-приемника, задержка, вносимая в каждый сигнал, для каждого спутника различна.

В GPS-приемниках алгоритмы слежения отслеживают частоту, фазу и задержку с помощью контуров частотной автоподстройки частоты (ЧАПЧ), контуров фазовой автоподстройки частоты (ФАПЧ) и контуров с автоподстройкой задержки (DLL - Delay Locked Loops) соответственно. Более широкая полоса пропускания контура обеспечивает быстрое слежение, но может привести к потере синхронизации частоты при низких значениях SNR. Более узкая полоса пропускания контура обеспечивает хорошую работу при низких значениях SNR, но медленнее отслеживает изменения фазы, частоты и задержки.

Сигнал промежуточной частоты (ПЧ) в этой работе моделируется на основе сигнала модулирующих сигналов GPS. Помимо сбора данных и отслеживания, GPS-приемник также выполняет синхронизацию битов, синхронизацию кадров и декодирование данных. На рис. 1 показаны различные блоки, используемые для работы GPS-приемника.

Смоделированная форма сигнала ПЧ содержит прецизионный код (Р-код) на синфазную составляющую и С/А-код на квадратурную составляющую, передаваемый на частоте L1 (1575,42 МГц) со спутников GPS. На основе заданного SNR для каждого спутника форма сигнала ПЧ масштабируется для соответствия мощности принимаемого сигнала. Также

необходимо смоделировать задержки для каждого спутникового сигнала независимо, а затем сложить все сигналы для получения составной формы сигнала ПЧ. К этой составной форме сигнала ПЧ добавляется фиксированное количество аддитивного белого гауссовского шума (AWGN).

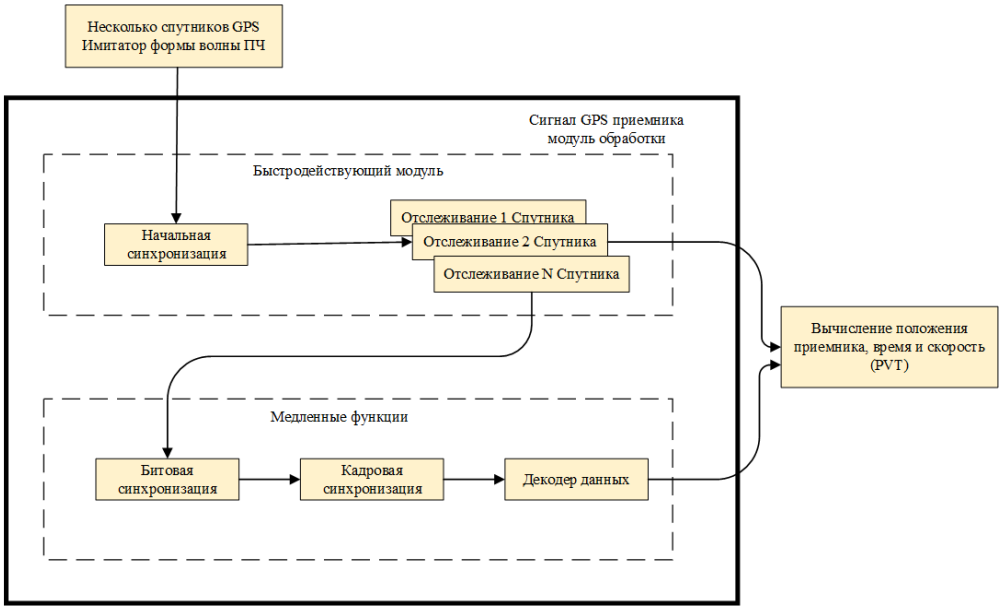


Рис. 1. Принципиальная блок-схема работы GPS-приемника

Начальные модули синхронизации и слежения обрабатывают данные с высокой скоростью (38,192 МГц) и называются быстрыми модулями [1]. Поскольку модули, выполняющие синхронизацию битов, синхронизацию кадров и декодирование данных, обрабатывают данные с низкой скоростью (50 бит в секунду), эти модули называются медленными модулями. Чтобы получить какие-либо значимые данные из этих медленных модулей, важные данные должны быть обработаны быстрыми модулями.

Моделирование исходной формы сигнала ПЧ системы GPS на частоте L1 (1575,42 МГц) от одного спутника включает в себя шаги, показанные на рис. 2. Далее масштабированные сигналы ПЧ от каждого спутника были суммированы, а затем к составному сигналу внесли постоянный белый гауссовский шум. Спектр ПЧ-сигнала показан на рис. 3. Спектр выглядит так, как будто в нем присутствует только шум, так как масштаб принимаемого сигнала равен единице мощности, спектр имеет уровень шумового сигнала единичной мощности.

При моделировании мощность каждого сигнала масштабируется в соответствии с SNR, эффективное значение SNR для каждого спутника различно. На рисунке 4 показаны суммированные сигналы с нескольких спутников. Каждый генератор сигналов на рисунке состоит из операций, представленных на рис. 2. Модуль начальной синхронизации обнаруживает все видимые спутники, оценивает грубый доплеровский сдвиг и грубое временное смещение в принимаемом сигнале от каждого спутника (рис. 5). В данном случае C/A-код преобразовали в частотную область с помощью алгоритма быстрого преобразования Фурье (БПФ) и выполнили

перемножение в частотной области с сигналом, а затем с помощью обратного БПФ (ОБПФ) вернулись во временную область. Такая синхронизация является одним из самых быстрых алгоритмов начальной синхронизации [2,3].

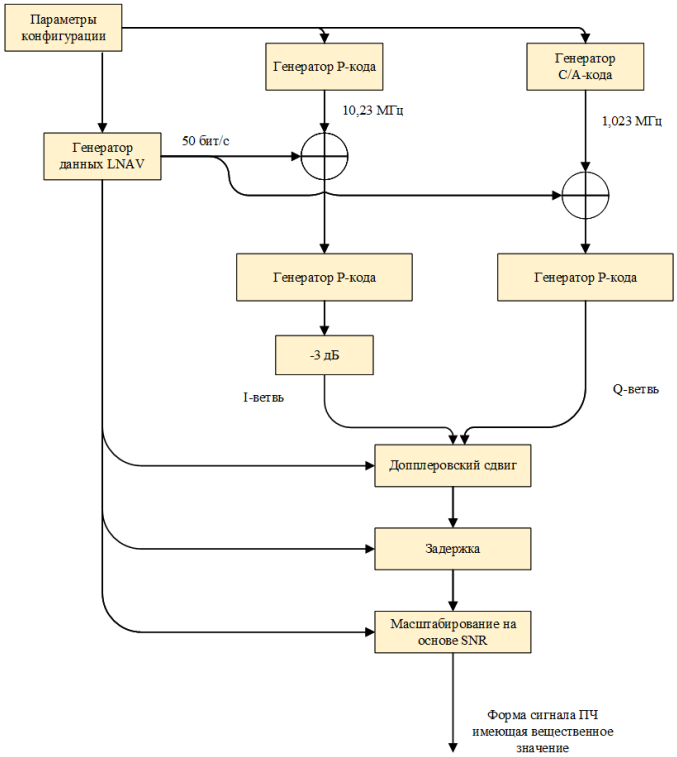


Рис. 2. Блок-схему формирования сигнала ПЧ

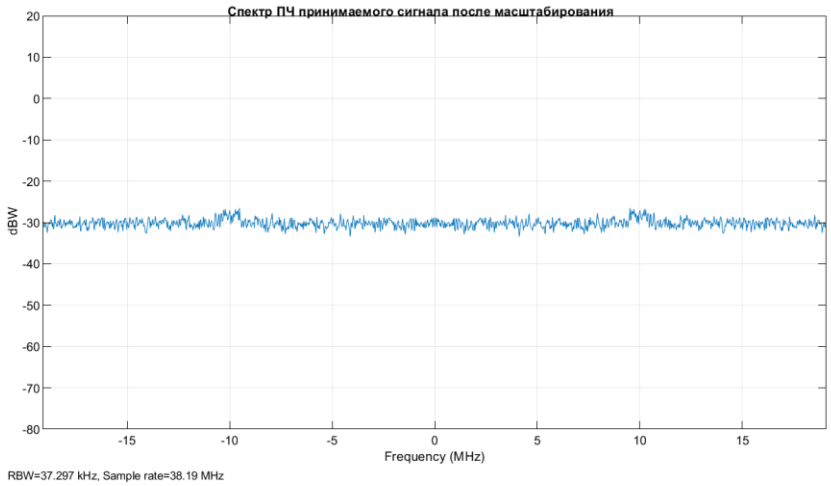


Рис. 3. Спектр ПЧ-сигнала после масштабирования

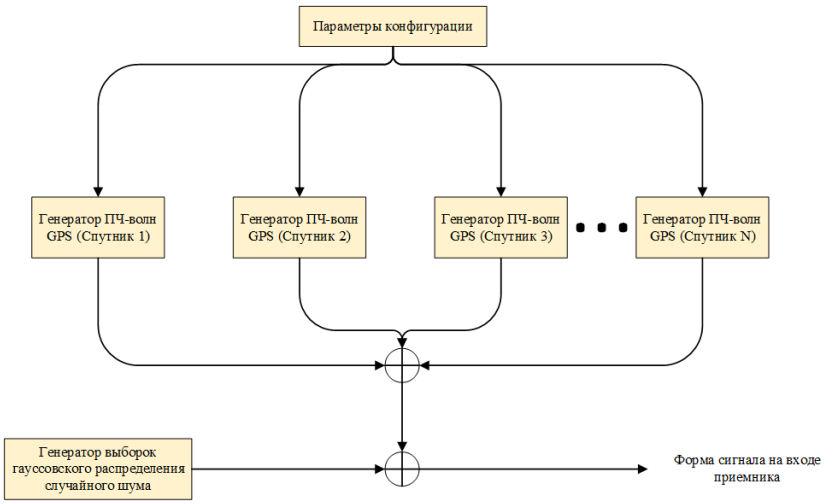


Рис. 4. Схема объединения осциллограмм с нескольких спутников

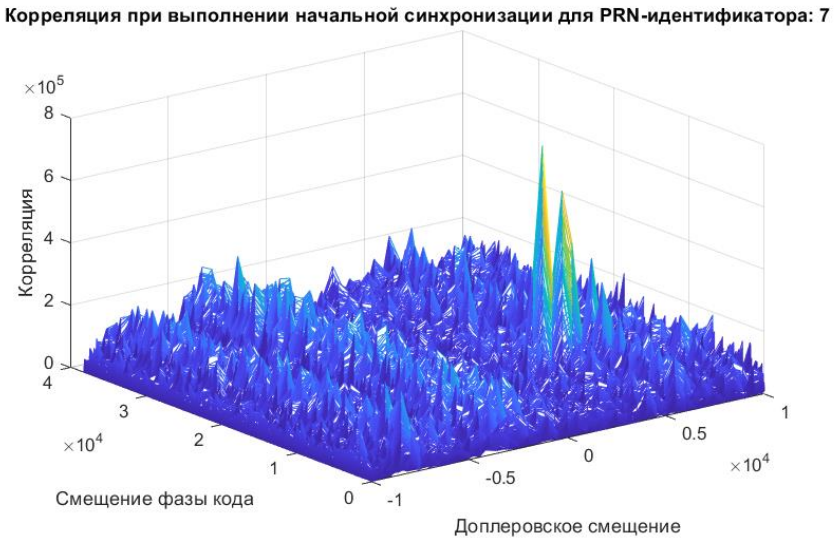


Рис. 5. Корреляция синхронизации принимаемого сигнала

На следующих графиках (рис. 6, 7) показаны результаты цикла отслеживания. Модуль слежения компенсирует доплеровский сдвиг и смещение фазы кода, остающиеся после начальной синхронизации. Происходило отслеживание трех параметров: несущей частоты, фазы несущей и кодовой задержки. Каждый из этих параметров отслеживался с помощью контуров обратной связи. Несущая частота отслеживалась с помощью FLL, фаза - с помощью ФАПЧ, а смещение кодовой фазы - с помощью DLL. Контуры слежения должны свести свести ошибки к нулю. Ошибка может быть любой физической величиной, например, частотой в FLL, или фазой в ФАПЧ, или задержкой в DLL.

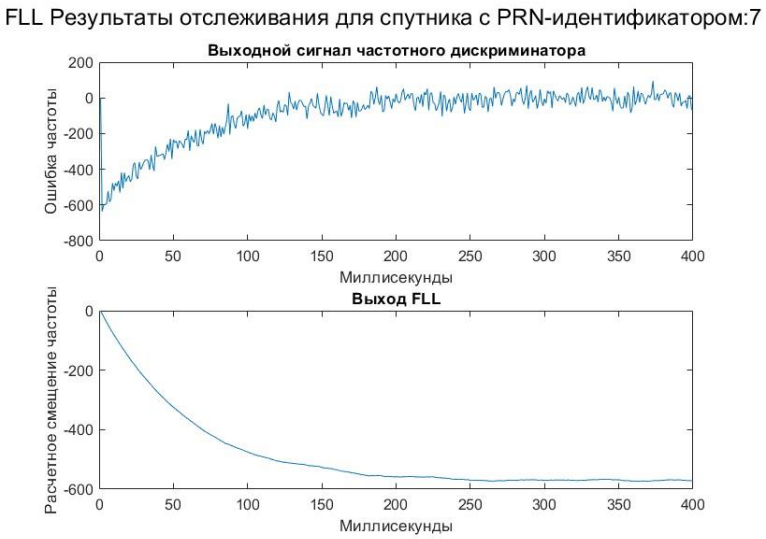


Рис. 6. Графики ошибки частоты

Ошибка обрабатывается через фильтр низких частот, называемый петлевым фильтром. По своей сути петлевой фильтр представляет собой интегратор, который накапливает выход дискриминатора, чтобы свести ошибку (выход дискриминатора) к нулю, то есть петлевой фильтр должен уменьшить шум на выходе дискриминатора. Основная роль петлевого фильтра заключается в фильрации шумов с выхода дискриминатора. Благодаря такой фильтрации любые резкие изменения ошибок будут отражаться только после достаточного времени сходимости.

При моделировании расчетная погрешность фазы показывает, что она (рис. 7) не сходится до тех пор, пока не сходится контур синхронизации частоты (рис. 6). Такое поведение ожидаемо, так как ошибка в частоте вызывает ошибку в фазе. Кроме того, выход ФАПЧ и ЧАПЧ, по-видимому, изменяется со временем из-за изменения доплеровского сдвига со временем.

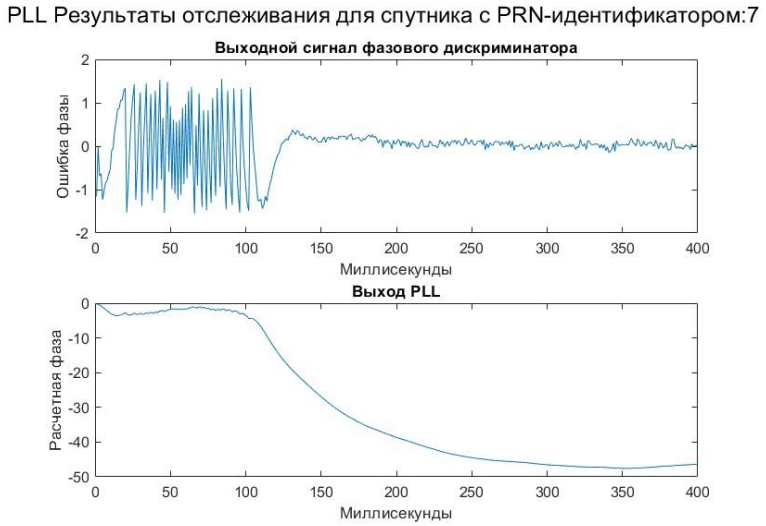


Рис. 7. Графики ошибки фазы

Список используемых источников:

1. Эллиотт Д. Каплан и. Хегарти К. Понимание GPS/GNSS: принципы и приложения. Серия технологий и приложений GNSS. Бостон : London: Artech House, 2017.

2. Фокин Г. А. Технологии сетевого позиционирования 5G. М. : Горячая линия-Телеком, 2021. 455 с. ISBN 978-5-9912-0930-4.

3. A. (Reza) Zekavat, R. Michael Buehrer Handbook of Position Location, 2012. 1195 с. ISBN 978-1-1181-8475-0.

Ushkova I., Fokin G.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Simulation of gps tracking using c/a code.

This paper shows how to simulate an initial waveform containing the coarse receive code (C/A code), intermediate frequency (IF) of a global positioning system (GPS) from multiple satellites, add noise to the composite signal, perform initial synchronization, and track the code phase and carrier frequency of the available satellites detected by the initial synchronization operation. Tracking is performed for each satellite independently.

Key words: GPS, IF, SNR.

УДК 681.3.06
ГРНТИ 50.41.25

ПРОГРАММНО АППАРАТНЫЕ СРЕДСТВА ПОВЫШЕНИЯ ТОЧНОСТИ БЕСПИЛОТНОЙ КАРТОГРАФИИ

Д. А. Хименкова, И. Н. Чернов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современные методы проведения авиационных работ с беспилотных летательных аппаратов (БПЛА) и построения геопривязанных ортофотопланов местности высокого пространственного разрешения состоят из множества задач, одной из них является выбор программных средств повышения точности картографии. В настоящем докладе приведена работа по созданию приложения для обработки данных подвижного ровера и стационарной базовой станции для точного позиционирования.

БПЛА, ортофотоплан, RTK, PPK

В настоящее время решение широкого круга инженерных и исследовательских задач, требующих определения местоположения и времени, выполняется посредством сбора данных глобальной навигационной спутниковой системы, навигационная точность которых в среднем составляет 1,5-2м. В случаях, когда требуется более точное определение местоположения, данные ГНСС необходимо корректировать. Это является важной задачей при проведении работ, требующих высокий уровень географической привязки, таких как построение геопривязанных ортофотопланов местности высокого пространственного разрешения.

Кинематика в реальном времени (*RTK*) и кинематика в постобработке (*PPK*) – это технологии коррекции наблюдений ГНСС, которые собирают данные о местоположении, выявляют ошибки и вносят поправки в данные с беспилотника. Разница между рабочими процессами *PPK* и *RTK*, которые представлены на рис. 1, заключается в том, когда происходит коррекция Кинематика в реальном времени (*RTK*) – это технология коррекции данных о местоположении в реальном времени, то есть в процессе съемки, а кинематика в постобработке (*PPK*) применяет позиционные поправки после сбора данных. С *PPK* данные могут быть загружены в облако и обработаны с помощью специализированного программного обеспечения после завершения полета. [3]

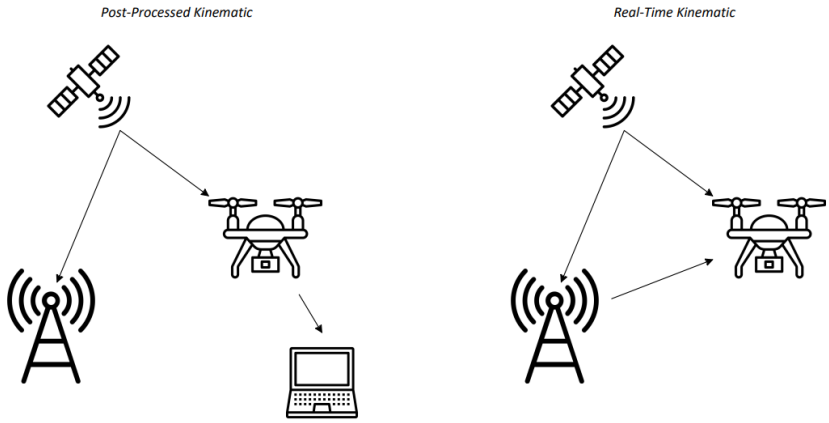
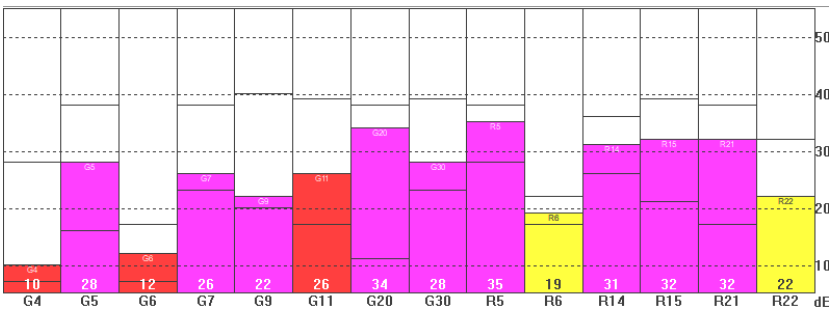


Рис. 1. Принцип работы *PPK* и *RTK* режимов

В исследовании для решения задач точной навигации и геопозиционирования используется ГНСС-модуль *u-blox NEO-m8p*, представленный на рис. 2, в качестве подвижного ровера, который поддерживает работу со всеми существующими на данный момент навигационными спутниковыми системами.

Рис. 2. ГНСС-модуль *u-blox NEO-m8p*

Для улучшения качества сбора данных в схему ровера были внесены корректировки: фильтрующий конденсатор и источник питания с минимально возможным шумом, что позволило увеличить значение *C/No* – *carrier-to-noise density ratio* – отношение принятой мощности, несущей к спектральной плотности собственного шума приемника. Значения *C/No* до и после внесения корректировок в схему приведены на рис. 3.



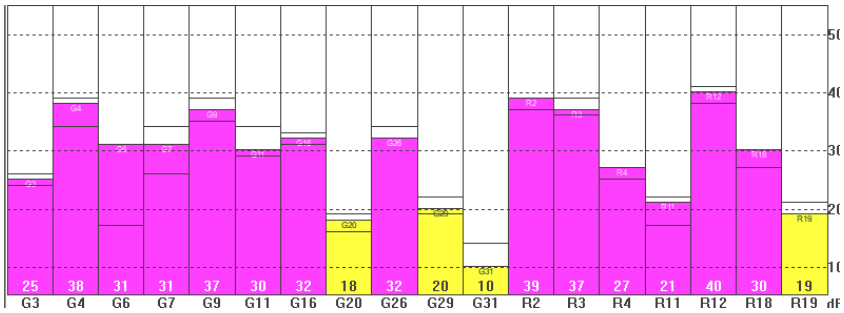


Рис. 3. Значения *C/No*

Существуют различные программные обеспечения (ПО), позволяющие выполнять обработку спутниковых данных всех существующих глобальных навигационных систем (ГЛОНАСС, *NAVSTAR GPS*, *BeiDou* и *Galileo*). Одной из таких программ является *RTKLib*. Это программный пакет с открытым исходным кодом, который поддерживает различные режимы позиционирования с ГНСС, как для обработки в реальном времени, так и для последующей обработки. [2] Данные, полученные и обработанные с использованием *RTKLib*, приведены на рис. 4. На начальных этапах для сбора данных был пройден маршрут в форме квадрата размером 40х30м.

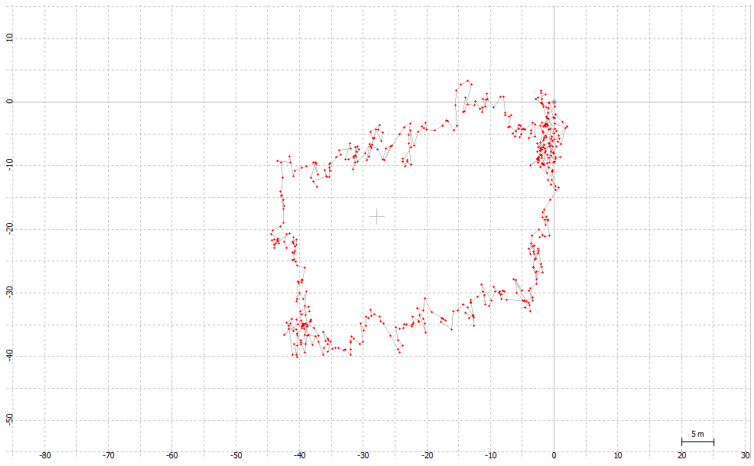


Рис. 4. Обработанные данные *RTKLib*

Еще одним примером является программное обеспечение *U-center*, которое представляет собой мощный инструмент для оценки, анализа производительности и конфигурации *u-blox* ГНСС приемников. Программа позволяет анализировать диаграммы состояния спутников и данные получаемые с них в режиме реального времени, определять динамическое и статическое поведение приемника ГНСС. [1] Данные, полученные и обработанные с использованием ПО *U-center*, приведены на рис. 5. Для сбора данных также был пройден маршрут в форме квадрата размером 40х30м, но так как *U-center* имеет внутренние поправки конечный результат получился более точным.

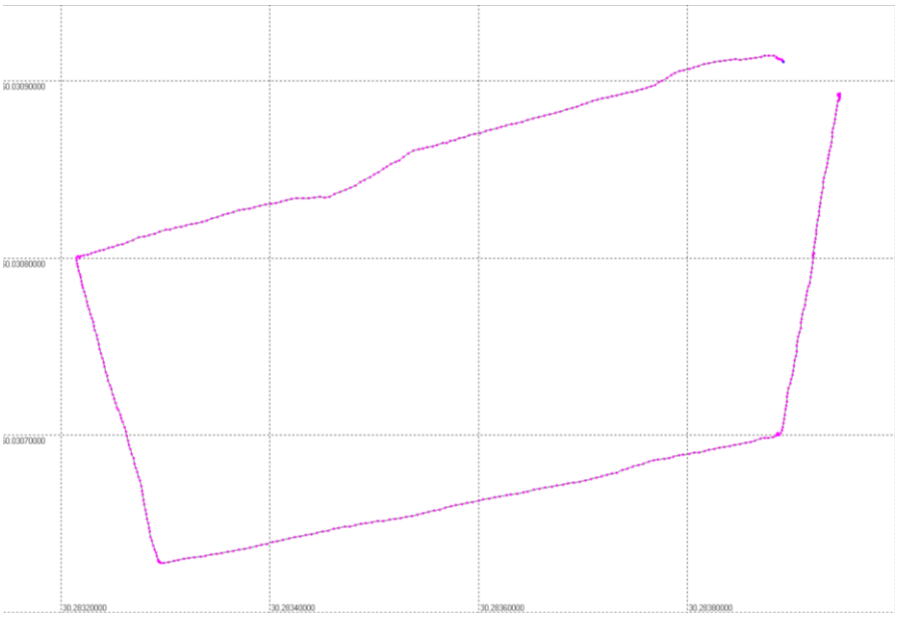


Рис. 5. Обработанные данные *U-center*

У данных программ имеется ряд недостатков: сложный пользовательский интерфейс, невозможность обработки нескольких роверов в рамках одного проекта для библиотеки *RTKLib*, использование только графического интерфейса, которые сужают круг решаемых задач. В связи с этим было принято решение о создании своего приложения, которое объединяет в себе необходимые функции существующего ПО и обеспечивает полную автоматизацию обработки принятых данных.

Разрабатываемая программа повышения точности беспилотной картографии предназначена для приёма сырых данных подвижного ровера, преобразования их в данных формата RINEX и последующей обработки с учетом поправок, поступающих от статичной базовой станции.

В силу того, что при выполнении постобработки ГНСС-измерений, как правило, доступно большее количество дополнительных исходных данных (измерения с дополнительных базовых станций, точные орбиты и пр.), а сама обработка может выполняться в прямом (Forward) и обратном (Reverse) направлении по времени, считается, что результаты измерений могут быть получены наиболее точно. [4]

Для внесения поправок в данные ровера будет использоваться один из методов системы дифференциальной коррекции глобальных навигационных спутниковых систем - кинематика в постобработке, блок-схема работы которого приведена на рис. 6.

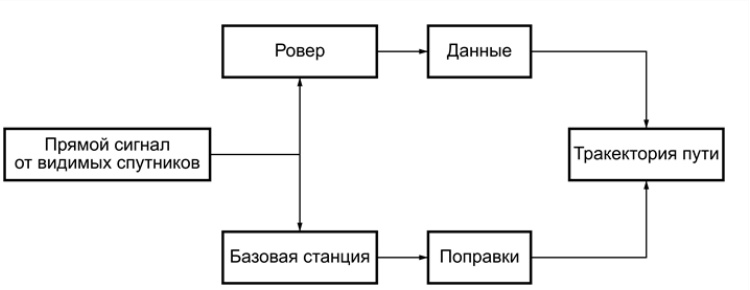


Рис. 6. Блок-схема PPK

Разработка ПО включает следующие этапы:

- Изучение особенностей существующих программ;
- Экспериментальное снятие данных с использованием готового ПО;
- Разработка программы на языке С;
- Проверка ПО с использованием ровера и базовой станции.

Разрабатываемая программа будет являться универсальным средством получения необработанных данных ГНСС с подвижного ровера, преобразования их в формат данных спутниковых навигационных приёмников (*RINEX*), что позволит производить пост-обработку полученных данных для выполнения более точных вычислений. Не менее важным фактом будет являться наличие параметризации, которая позволит выбирать определенные спутники, способы записи и передачи данных, не меняя код.

Таким образом, рассмотрены основные методы получения данных глобальной навигационной спутниковой системы, способы конвертирования их для дальнейшей обработки, проведены эксперименты по сбору данных с подвижного ровера, произведена подготовка к написанию собственного программного обеспечения.

Список используемых источников:

1. u-center GNSS evaluation software for Windows // u-blox [Электронный ресурс] URL: https://www.u-blox.com/en/product/u-center (дата обращения: 04.11.2023).

2. RTKLIB: An Open Source Program Package for GNSS Positioning // RTKLIB [Электронный ресурс] URL: https://www.rtklib.com/ (дата обращения: 04.11.2023).

3. RTK/PPK // senseFly Russia [Электронный ресурс] URL: https://sensefly.aero/rtk-ppk/ (дата обращения: 04.11.2023).

4. Atınç Pırtı / Evaluating the accuracy of post-processed kinematic (PPK) positioning technique // Geodesy and Cartography. 2021. С. 66-70.

Khimenkova D., Chernov I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Hardware and software tools to improve the accuracy of unmanned cartography.

Modern methods of aerial work from unmanned aerial vehicles (UAVs) and construction of geo-referenced orthophotos of terrain of high spatial resolution consist of many tasks, one of them is the choice of software tools to improve the accuracy of mapping. This paper presents work on a mobile rover and fixed base station data processing application for accurate positioning.

Key words: UAV, orthophoto, RTK, PPK.

УДК 621.396.677
ГРНТИ 47.45.29

ИСПОЛЬЗОВАНИЕ АЛГОРИТМОВ АДАПТИВНОГО ДИАГРАММООБРАЗОВАНИЯ В СЕТЯХ 5G

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

Адаптивное диаграммообразование является крайне важным аспектом реализации пространственного уплотнения одновременных передач (SDMA) в сетях подвижной связи пятого поколения. В сверхплотных сетях антенные решётки принимают кроме полезных сигналов множество помех, подавление которых посредством формирования нулей диаграмм направленности является задачей алгоритмов адаптивного диаграммообразования. В работе рассмотрено применение алгоритмов МНК и РМНК для вычисления весовых коэффициентов цифровых антенных решёток. Для сравнения эффективности указанных алгоритмов предложена модель в среде MATLAB.

сверхплотные сети, адаптивное диаграммообразование, алгоритмы адаптивного диаграммобразования, МНК, РМНК

Основным различием между пятым поколением мобильных сетей и нынешними является их способность функционировать в условиях очень плотного распределения сот, вызванного переходом на диапазон миллиметровых волн. Повышение частоты негативно сказывается на проникновении и дальности распространения волн, вызывая уплотнение сети и значительный рост уровня внутренних помех. В таких условиях поддержание требуемых параметров качества соединения усложняется. Одним из возможных решений этой проблемы может стать применение направленной радиосвязи - пространственного уплотнения сигнала (SDMA) посредством адаптивного формирования диаграмм направленности антенных решёток систем Massive MIMO.

Цифровые антенные решётки, также известные как SMART-антенны — это средство повышения эффективности беспроводных коммуникаций в различных аспектах. Цифровые антенные решётки позволяют повысить уровень принимаемого сигнала, подавить помехи и тем самым повысить соотношение сигнал/шум всей системы, а также предотвратить вклад устройства в ухудшение помеховой обстановки. SMART-антенны развивают идею сотовой секторизации, фактически предлагая создание для каждого абонента отдельной соты, покрытие которой задаётся множеством управляемых лучей. Формирование луча антенной решёткой осуществляется за счёт изменения задержек фаз и амплитуд сигналов на антенных элементах. Вариации диаграммы направленности создаются на основе весовых коэффициентов формирователей, получаемых в качестве результатов алгоритмов адаптивного диаграммообразования.

Алгоритмы делятся на слепые и неслепые. Слепые алгоритмы анализируют только стандартно отправляемую и принимаемую информацию

для выделения пользователя среди остальных. В неслепых формирование луча начинается со сбора информации, - каждый пользователь отправляет короткую тренировочную последовательность, которая на приёмной стороне сравнивается с оригиналом для определения параметров паттернов. Таким образом для работы неслепых алгоритмов адаптивного диаграммообразования в качестве минимального набора входных данных требуются принятая тренировочная последовательность и результат отработки предыдущей последовательности весовых коэффициентов.

Одними из основных неслепых алгоритмов адаптивного диаграммообразования являются метод наименьших квадратов и его модификация, рекурсивный метод наименьших квадратов. Алгоритм МНК представляет из себя линейный фильтр, который настраивает свои параметры, весовые коэффициенты, на каждой итерации с целью минимизации среднеквадратичной ошибки между прогнозируемым и фактическим выходным сигналом посредством применения метода наискорейшего отрицательного спуска [1]. Работа алгоритма в каждой итерации состоит из двух основных этапов - расчёта ошибки, отклонения для имеющейся конфигурации весов и расчёта новых весовых коэффициентов.

Оценка ошибки $\boldsymbol{e}(k)$ заключается в сравнении референсного сигнала-образца $\boldsymbol{d}(k)$с принятым сигналом $\boldsymbol{x}(k)$, прошедшим фильтр весовых коэффициентов $\boldsymbol{w}(k)$, из чего следует

$$\boldsymbol{e}(k) = \boldsymbol{d}(k) - \boldsymbol{w}^{H}(k)\boldsymbol{x}(k) \quad (1)$$

Коррекция весового вектора осуществляется в соответствии со следующей формулой

$$\boldsymbol{w}(k+1) = \boldsymbol{w}(k) + \mu \boldsymbol{e}^{*}(k)\boldsymbol{x}(k), \quad (2)$$

где μ — коэффициент сходимости, скалярная константа, отвечающая за скорость и стабильность алгоритма.

Высокие значения шага сходимости приводят к более быстрому, но менее точному нахождению оптимума функции и, соответственно, конечных значений весовых коэффициентов. Слишком низкие значения повышают точность, но с ней и увеличивают требуемое количество вычислений. проблема устраняется алгоритмом рекурсивного МНК путём динамического обновления размера шага градиента. Формула (2) приобретает вид

$$\boldsymbol{w}(k+1) = \boldsymbol{w}(k) + \boldsymbol{e}^{*}(k)\frac{R^{-1}(k-1)\boldsymbol{x}(k),}{\lambda - \boldsymbol{x}^{H}(k)R^{-1}(k-1)\boldsymbol{x}(k)}, \quad (3)$$

где R^{-1} — обратная автоковариационная матрица принятого сигнала $\boldsymbol{x}(k)$, λ — экспоненциальный коэффициент масштабирования.

Преимущество рекурсивного МНК заключается в отсутствии необходимости расчёта корреляционной матрицы, так как рекурсия позволяет итеративно её обновлять. Хранение информации из входных данных обеспечивает рекурсивному алгоритму большую скорость сходимости, нежели чем у простого МНК [2].

Для сравнения эффективности двух методов проведено моделирование в программном комплексе Matlab. При моделировании производилось построение диаграммы направленности линейной антенной решётки из восьми элементов с наведением главного лепестка на источник сигнала и нулей диаграммы на две помехи на равных угловых расстояниях от источника сигнала. В ходе моделирования угловые расстояния меняются, как показано на рис. 1, где SOI — источник сигнала, SNOI — помехи.

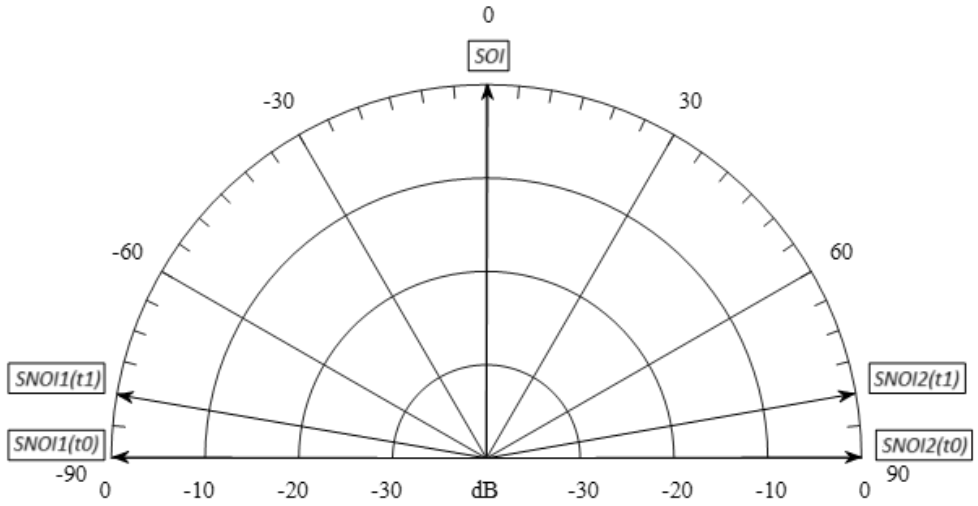


Рис. 1. Сценарий проведения измерений при исследовании эффективности работы модели при разных угловых разносах полезного сигнала и помех. Обе помехи равноудалены от источника сигнала и постепенно приближаются до пересечения с ним

Метрикой сравнения алгоритмов выбрано среднеквадратическое отклонение, представляющее собой среднее значение квадратов разностей между прогнозируемыми и фактическими значениями.

Результат моделирования представлен в таблице 1, где угловой разнос — угловое расстояние между источником сигнала и одной из помех.

ТАБЛИЦА 1. Результат моделирования для алгоритмов МНК и РМНК

Угловой разнос	СКО МНК, дБ	СКО РМНК, дБ
90°	6,29	-9,25
80°	-13,08	-22,61
70°	-11,78	-18,15

60°	-12,24	-13,64
50°	-7,36	-13,22
40°	-10,77	-14,84
30°	2,45	-12,11
20°	-10,70	-15,90
10°	-9,80	-18,73
0°	7,29	7,37

На рис. 2 данные таблицы 1 отображены на графике.

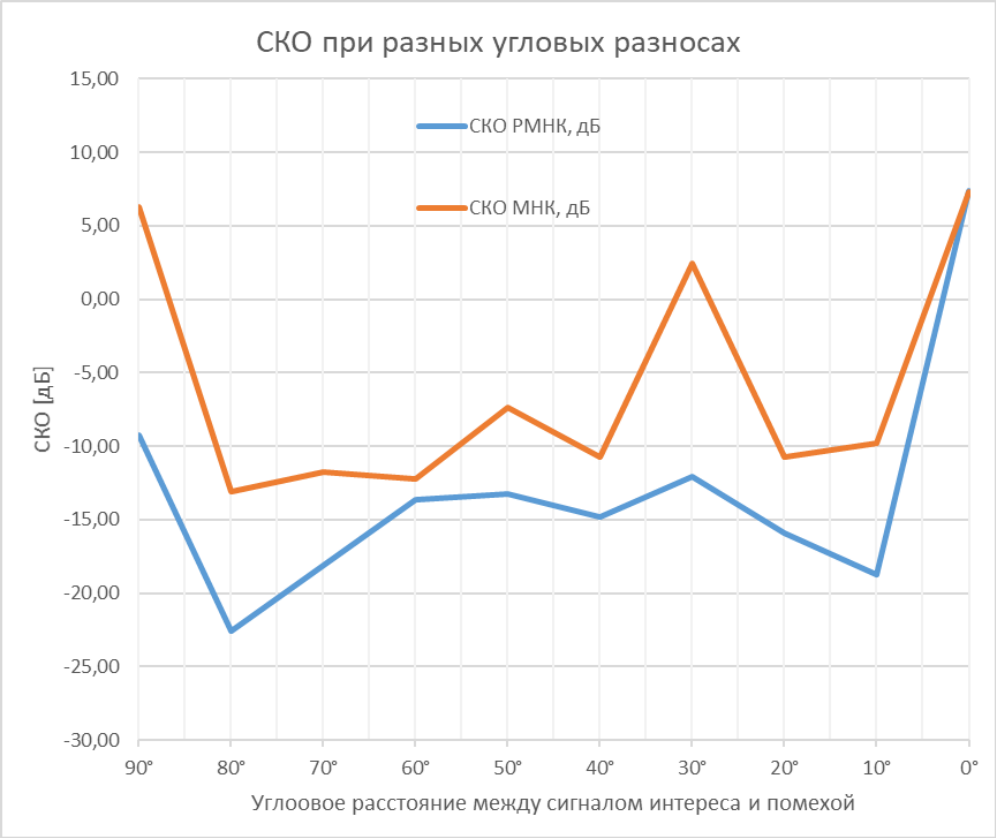


Рис. 2. Сравнение СКО двух алгоритмов

Из графика на рис. 2 можно сделать вывод о том, что алгоритм РМНК лучше, чем МНК справляется с задачей диаграммообразования, что видно по более низкому уровню СКО на протяжении всех итераций сценария. В среднем СКО РМНК на 7,14 дБ ниже. Помимо количественного преимущества РМНК не имеет пика значений СКО на отметке углового разброса 30°.

Список используемых источников:

1. Баланис К., Иоанидес П. Введение в смарт-антенны. М. : Техносфера, 2012. 117 с.
2. Gross F. Smart Antennas for Wireless Communications With MATLAB. The McGraw-Hill Companies, 2005. 238 с.

Sheremet N.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

The use of adaptive diagramming algorithms in 5G networks.

Adaptive diagramming is an extremely important aspect of realization of spatial division multiple access (SDMA) in fifth generation mobile networks. In superdense networks, antenna arrays receive a lot of interference in addition to useful signals, suppression of which by forming the zeros of directional patterns is the task of adaptive diagramming algorithms. The paper considers the application of LMS and RLS algorithms for calculating the weight coefficients of digital antenna arrays. A model in MATLAB environment is proposed to compare the efficiency of these algorithms.

Key words: superdense networks, adaptive diagramming, adaptive diagramming algorithms, LMS, RLS.

УДК 621.396.6
ГРНТИ 47.63.29

МОДЕЛИРОВАНИЕ СЕТИ IIOT В ПАКЕТЕ WOKWI

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

Представлена разработанная модель сети IIoT в симуляторе Wokwi. Произведен выбор микроконтроллера и датчиков для IIoT. Модель состоит из микроконтроллера ESP32 и 5 датчиков DHT22, расставленных в разные места и способных получать данные о влажности и температуре. Информация передается по радиоканалу Wi-Fi на сервер мониторинга. Тестирование модели показало, что модель является работоспособной и может быть реализована как аппаратная.

Wokwi, микроконтроллер, IIoT, ESP32, DHT22

Введение

Промышленный интернет вещей (IIoT) – это технология, которая позволяет объектам собирать и обмениваться данными в реальном времени, а также анализировать эти данные с помощью компьютерных систем. Она может использоваться для повышения эффективности производства, оптимизации бизнес-процессов и улучшения качества продукции. IIoT помогает автоматизировать и оптимизировать производственные процессы, повышать производительность, снижать затраты, улучшать безопасность и обеспечивать более высокое качество продукции [1].

В данной работе представлен проект, который позволит собирать данные о температуре и влажности с многих точек и передавать их по радиоканалу в центр мониторинга. Система должна обеспечивать надежную передачу данных с датчиков температуры контроллеру, при этом датчик температуры должен отличаться малой погрешностью и большим диапазоном считываемых данных. Для разработки использован бесплатный онлайн симулятор электронных схем, который позволяет моделировать микроконтроллерные проекты *Wokwi* [2]. *Wokwi* имитирует работу популярных плат для прототипирования и обучения работе с микроконтроллерами, таких как *Arduino,* ESP32 *DevKit, Raspberry Pi Pico* и ряд других.

1. Выбор оборудования

В качестве датчика температуры выберем DHT *(Digital Hygrometer and Thermometer)* датчик. Существуют две версии серии датчиков температуры DHTxx: DHT11 и DHT22. Они имеют одинаковую распиновку, но разные характеристики. DHT22 является более дорогой версией, которая имеет лучшие характеристики. Диапазон измерения температуры составляет от -40°C до +80°C с точностью ±0,5 градуса, а диапазон температур DHT11 составляет от 0°C до 50°C с точностью ±2 градуса [3]. Также датчик DHT22

имеет более широкий диапазон измерения влажности, от 0 до 100% с точностью 2-5%, в то время как диапазон измерения влажности DHT11 составляет от 20 до 80% с точностью 5%. Рабочее напряжение обоих датчиков составляет от 3 до 5 вольт, в то время как максимальный ток, используемый во время преобразования (при запросе данных), составляет 2,5 мА. Датчики DHT22 состоит из чувствительного емкостного датчика и NTC термистора, а также 8-ми битном чипе, который преобразует аналоговый 16 сигнал с датчиков, в цифровой на выходе. При производстве, компоненты входящие в модуль DHT22 имеют разные параметры и, чтобы показания были реальными, производитель калибрует каждый датчик DHT22 в калибровочной камере, а поправочный коэффициент сохраняется в памяти и вызывается при считывании данных. Преимущество данных датчиков, это небольшие размеры, низкая энергопотребление, высокая дальность передачи до 20 м, из недостатков можно отнести, задержка в передачи показаний в 2 секунды.

В качестве контроллера необходимо сделать выбор между ESP8266 и ESP32. ESP8266 дешевле, чем ESP32. Хотя у ESP8266 не так много функций, он отлично будет работать в большинстве простых проектов IoT. Однако у него есть некоторые ограничения. Когда дело доходит до использования GPIO у него просто может не хватить контактов для более сложных проектов, поэтому лучше использовать ESP32. ESP32 намного мощнее *ESP8266*, поставляется с большим количеством GPIO *(general-purpose input/output)*, с большим количеством функций, более быстрым Wi-Fi, а также поддерживает Bluetooth. Также имеет как аналоговые входы/выходы, так и цифровые [4].

Таким образом, для реализации аппаратной части нам будет необходим модуль *ESP-32*, для примера будет достаточно 5 датчиков DHT22 и *Wokwi IoT Gateway*. Данные будут пересылаться на сервер *test.mosquitto.org*.

2. Моделирование в *Wokwi*

Доступ в интернет *Wokwi* организует, используя специальный шлюз IoT *Gateway* для подключения смоделированного ESP32 к Интернету. Существует два способа использования *Wokwi IoT Gateway*: общедоступный шлюз и частный шлюз. Публичный шлюз обеспечивает прямой доступ к Интернету, при этом весь трафик отслеживается в целях безопасности, поэтому нельзя его использовать для передачи конфиденциальных данных. Частный шлюз – это приложение, которое необходимо загрузить и запустить на компьютере. Он обеспечивает *ESP32* более быстрый и надежный доступ в Интернет чем публичный шлюз. Данные передаются непосредственно из симулятора, работающего в браузере, в сеть без необходимости проходить через облако. Это означает, что трафик остается конфиденциальным, а проекты ESP32 могут получать доступ к службам, работающим на локальном компьютере или в локальной сети (например, к локальному серверу). Частный шлюз доступен только для пользователей, присоединившихся

Wokwi Club, т.е. является платным. Поэтому для моделирования выбран публичный шлюз.

Физически подключение датчиков DHT11, DHT22/AM2302 к ESP32 простое. У них довольно длинные выводы с шагом 0,1 дюйма (2,54 м), поэтому можно легко вставить их в любую макетную плату. Подаем на датчик питание 3,3 В и подключаем землю, вывод данных подключаем к цифровым выводам на ESP32.

Нередко между VCC *(Voltage Common Collector)* и линией данных устанавливают подтягивающий резистор 10 кОм, чтобы поддерживать высокий логический уровень на линии данных для правильной связи между датчиком и микроконтроллером. Так как есть готовый модуль датчика, нет необходимости добавлять какие-либо внешние подтягивающие резисторы. Модуль поставляется со встроенным подтягивающим резистором. Готовая схема проекта представлена на рис. 1.

Датчики DHT11 и DHT22/AM2302 имеют собственный однопроводный протокол, используемый для передачи данных. Этот протокол требует точной синхронизации. Однако, нам не нужно беспокоиться об этом, потому что мы собираемся использовать библиотеку DHT, которая позаботится почти обо всем.

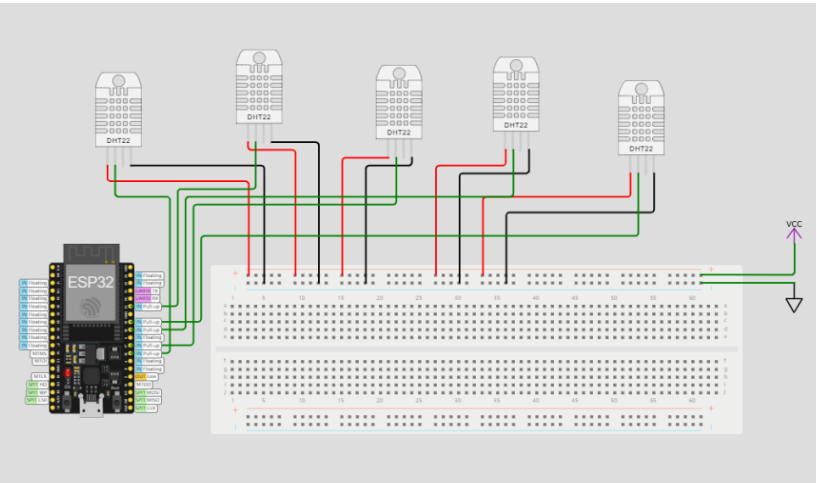


Рис. 1. Схема проекта в симуляторе *Wokwi*

Запуск разработанного программного кода начинается с подключения к MQTT *(Message Queuing Telemetry Transport)* серверу для обработки данных, после чего можно изменять показания на датчиках в симуляторе (рис. 2).

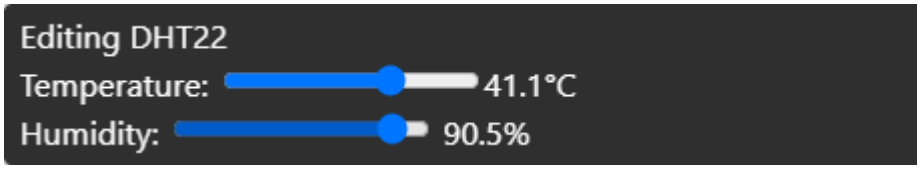


Рис. 2. Изменения показаний датчика

Результатом работы программы будет получение информации о влажности и температуры с пяти датчиков (рис. 3).

```
Connecting to Wokwi-GUEST
..Wifi connected
IP address:
10.10.0.2
MQTT connection..Connected
Temperature(1): 41.10
Humidity(1): 90.5
Temperature(2): 65.00
Humidity(2): 28.0
Temperature(3): 61.80
Humidity(3): 75.5
Temperature(4): 24.00
Humidity(4): 40.0
Temperature(5): -17.40
Humidity(5): 29.5
```

Рис. 3. Данные, полученные от датчиков

Таким образом, моделирование показывает успешную работу сети.

Заключение

В данном проекте проведено моделирование сети IIoT в пакете *Wokwi*. Данная сеть предполагает сбор информации для автоматизации систем IIoT, компонентами которой являлись микроконтроллер ESP32 и 5 датчиков DHT22. Показано, что модельная сеть является полностью работоспособной. На основе данной модели можно собрать реальную сеть с малой стоимостью и небольшими габаритами, что является важным фактором в разработках систем IIoT.

Список используемых источников:

1. Куприяновский В. П. и др. Интернет Вещей на промышленных предприятиях // International Journal of Open Information Technologies. 2016. Т. 4. N 12. С. 69-78.

2. Wokwi - Online ESP32, STM32, Arduino Simulator. [Электронный ресурс] // Wokwi. URL: https://wokwi.com/ (дата обращения 30.10.2023).

3. Mihai B. How to use the DHT22 sensor for measuring temperature and humidity with the arduino board // Acta Uiversitatis Cibiniensis–Technical Series. 2016. Т. 68. С. 22-25.

4. Берестинов А. А., Омельченко С. Д., Кулганатов А. З. Разработка беспроводного датчика температуры с совместным использованием микрокомпьютера ESP32 // Системы управления, информационные технологии и математическое моделирование. 2020. С. 75-78.

Yandiev A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

IIoT network modeling in WOKWI package.

The paper gives an overview of IIoT and presents a model of IIoT network in Wokwi simulator. The microcontroller and sensors for IIoT are selected. The model consists of an ESP32 microcontroller and 5 DHT22 sensors placed in different locations and capable of receiving humidity and temperature data. The information is transmitted via radio channel to the monitoring server. The model was also tested, which revealed the performance and feasibility of implementation in practice.

Key words: Wokwi, microcontroller, IIoT, ESP32, DHT22.

Секция 2.3.
Проектирование и технология радиоэлектронных средств

УДК 621.396.722
ГРНТИ 49.43.29

ПРИМЕНЕНИЕ СИНХРОННОГО ИНТЕРФЕЙСА ПРИ БЫСТРОМ ПРОТОТИПИРОВАНИИ ФАЗИРОВАННЫХ АНТЕННЫХ РЕШЕТОК

Н. П. Дунаев, В. А. Макаров
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В процессе реализации различных устройств, на этапе прототипирования возникает необходимость в быстрой сборке и проверке работы ключевых узлов в единой системе. Прототипирование может выполняться без второстепенных для системы узлов, например, узел преобразования и питания может быть заменен на лабораторный блок питания, вместо излучателя может быть подключен генератор сигналов с генератором шума. Интерфейсы передачи данных в готовых устройствах часто обладают достаточной сложной структурой с повышенными требованиями по электромагнитной совместимости что требует доработки или дооснасти узлов. В работе рассматривается применение интерфейса SPI как основного для межблочной передачи команд.

Фазированная антенная решетка, управление, синхронный интерфейс

В рамках работы над антенной решеткой потребовалось реализовать систему управления цифровыми фазовращателями и аттенюаторами. Обе микросхемы установлены на отладочные платы, реализованные производителем. Для переключения состояния фазовращателя необходимо передать на него 8 бит [1], на аттенюатор 6 бит [2]. Согласно документации микросхемы поддерживают параллельный и последовательный способы управления. Параллельное управление заключается в подаче напряжения на выводы микросхемы для переключения каждого бита. Переключение режимов передачи данных осуществляется перепайкой перемычки на плате фазовращателя и переключением ключа на плате аттенюатора. На каждой отладочной плате предусмотрена система преобразования и выравнивания питания (Правильно?) что позволяет подавать на них питание с напряжением пять вольт без предварительной стабилизации. На отладочной плате фазовращателя установлен малошумящий усилитель мощности, это важно учитывать при составлении СВЧ цепи.

Для управления модулями Ф/А используется SPI интерфейс, который позволяет обеспечить высокую скорость, до 100 Мб/с, в сравнении с другими базовыми интерфейсами, такими как: UART и I2C [3]. Схема подключения модулей представлена на рис. 1.

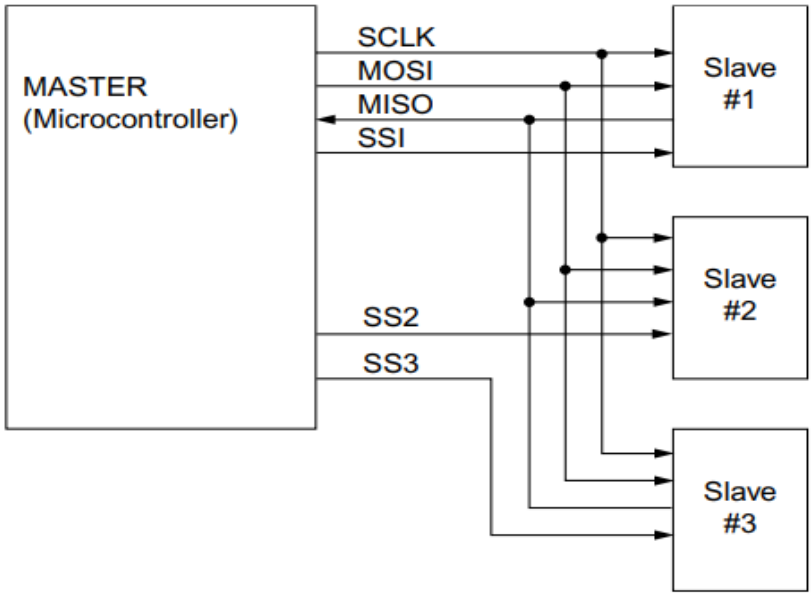


Рис. 1. SPI интерфейс

Но в отличии от других, SPI не является помехозащищенным интерфейсом, так как он использует всего две линии для передачи данных (MISO и MOSI) и одну линию для синхронизации (SCLK). Для обеспечения помехозащищенности, при подключении модулей использовались короткие провода, порядка 10 см, с целю уменьшения влияния электромагнитных помех. Также, с этой целью были дополнительно экранированы модули Ф/А и кабели.

Так как данные микросхемы не имеют выхода для последовательной записи в обе микросхемы, то к каждой микросхемы идет своя линия LE. Однако схема упрощается за счет отсутствия линий MISO, в микросхемах не предусмотрен ответ на команды или передача информации о состоянии или режимах работы. Схема подключения реализованной системы представлена на рис. 2.

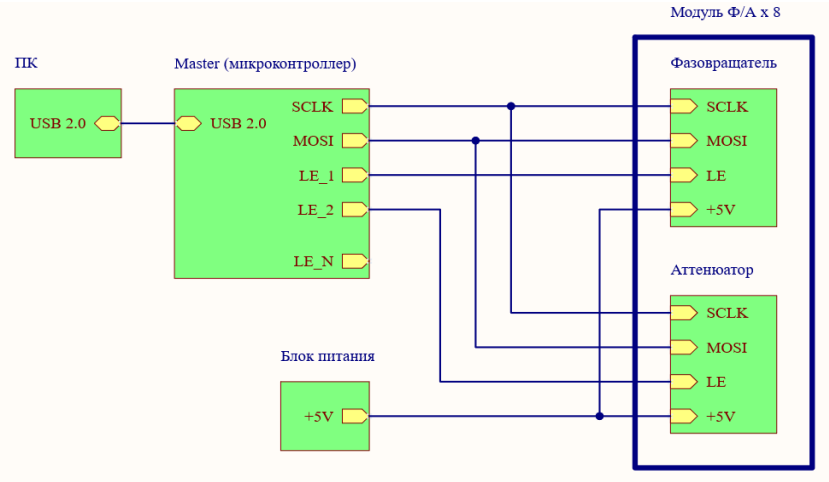


Рис. 2. Схема подключения модулей

Для расположения микросхем в пространстве была разработана крепежная рамка, помимо установки на ней отладочных плат, также предусмотрено место для разъема DB-15 (рис. 3). Применение такого разъема оправдано дешевизной, простотой установки и распайки.

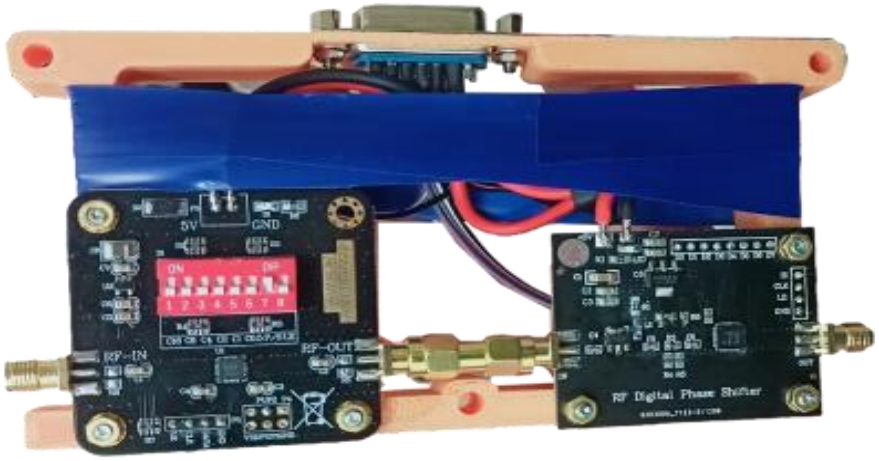


Рис. 3. Модуль фазовращателя аттенюатора

Полученный модуль фазовращателя/аттенюатора получает команды от модуля управления на основе STM32H723ZG[4]. На модуле управления установлены выводные разъемы DB-15, разводка внутри блока выполнена проводами-перемычками и, по сути, все линии находятся в воздухе.

Первые запуски системы показали, что команды передаются на модули Ф/А и они переключают свое состояние, однако при запуске полноценного алгоритма калибровки стало ясно что команды хаотичны и могут многократно повторяться. Для решения этой проблемы были реализованы экраны модуля управления и модулей Ф/А, путем покрытия корпусов алюминиевой клейкой лентой и заземлением через лабораторный блок питания.

Испытания проводились на улице во дворе университета телекоммуникаций. Питание к системе подводилось с помощью удлинителей. Результаты калибровки (рис. 4) модулей показывают, что данные снимались последовательно и согласуются с данными технической документации на микросхемы.

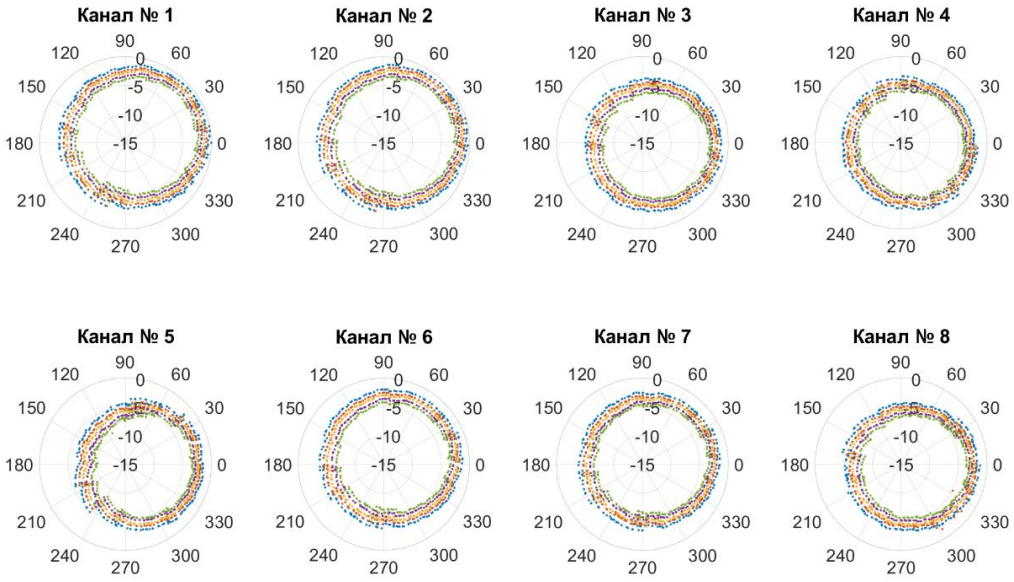


Рис. 4. Характеристики каналов

При быстром прототипировании возможно использовать интерфейсы последовательной межмикросхемной/внутриплатной связи в рамках системы и связи между блоками, но при этом важно обеспечить экранирование проводов, узлов и модулей и подобрать длинны проводов.

Список используемых источников:

1. Техническая документация на фазовращатель PE44820 [Электронный ресурс] URL: https://www.psemi.com/pdf/datasheets/pe44820ds.pdf (дата обращения: 02.09.2023).

2. Техническая документация на аттенюатор PE4302 [Электронный ресурс] URL: https://radio-hobby.org/uploads/datasheet/208/pe43/pe4302.pdf (дата обращения: 02.09.2023).

3. Frenzel L.E. Jr. Handbook of serial communications interfaces: Newnes, 2016 338 c.

4. Техническая документация на микроконтроллер STM [Электронный ресурс] URL: https://www.st.com/en/evaluation-tools/nucleo-h723zg.html (дата обращения: 02.09.2023).

Dunaev N., Makarov V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

The use of a synchronous interface for rapid prototyping of phased antenna arrays.

In the process of implementing various devices, at the prototyping stage, there is a need for quick assembly and verification of the operation of key nodes in a single system. Prototyping can be performed without secondary nodes for the system, for example, the conversion and power supply node can be replaced with a laboratory power supply unit, a signal generator with a noise generator can be connected instead of an emitter. Data transfer interfaces in ready-made devices often have a sufficiently complex structure with increased requirements for electromagnetic compatibility, which requires refinement or retrofitting of nodes. The paper considers the use of the SPI interface as the main one for interblock command transmission.

Key words: Phased array antenna, control, synchronous interface.

УДК 550.835.8
ГРНТИ 37.21.03

РАДИОМЕТР НА ОСНОВЕ СПУТНИКОВОГО КОНВЕРТОРА И SDR-RTL ПРИЕМНИКА

Н. П. Дунаев, В. А. Макаров
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье описывается радиометр на основе SDR-RTL приемника. Оцениваются технические характеристики разработанного одноканального радиометра, приводятся экспериментальные данные. Анализируются его функциональные характеристики на основе полученных в результате измерений данных.

радиометр, RTL-SDR приемник

Современные радиометры играют важную роль в различных областях науки и техники, от атмосферных исследований [1] до применений в области безопасности [2].

Для реализации радиометра были выбраны: в качестве антенны X диапазона – спутниковый конвертор, реализующий прием в миллиметровом диапазоне, перенос частоты в сантиметровый диапазон с последующим усилением, а в качестве приемника – RTL-SDR. В таблице 1 и таблице 2 приведены основные характеристики используемого оборудования.

ТАБЛИЦА 1. Основные характеристики спутникового конвертора

Частота входа	10,7 - 12,75 ГГц
Частота выхода	950 - 2150 МГц
Уровень шума	0,3 дБ
Чувствительность, δT	25-30 дБ/К

ТАБЛИЦА 2. Основные характеристики RTL-SDR приемника

Частота входа	24 МГц - 1,766 ГГц
Частота дискретизации	3,2 / 2,56 (стабильная) МГц
Разрядность АЦП	8 бит
Усиление	49,6 дБ

При исследовании данной схемы мы будем работать в верхнем Ku диапазоне и на частоте f = 12,2 ГГц. Для верхнего диапазона L.O. частота (частота локального генератора) – 10,6 ГГц. Тогда промежуточная частота:

$$f_{\text{ПЧ}} = 12{,}2 - 10{,}6 = 1{,}6 \text{ ГГц}$$

Используемая частота дискретизации $f_{sr} = 2{,}4$ МГц, это максимальная частота при которой данный SDR-RTL приемник может работать стабильно. Число отсчетов $N_{\text{отсчетов}}$ за один период наблюдения равно 2^{14}, тогда время интегрирования составит 6,8 мс.

Макетный образец, представленный на рис. 2, был собран по схеме, изображенной на рис. 1.

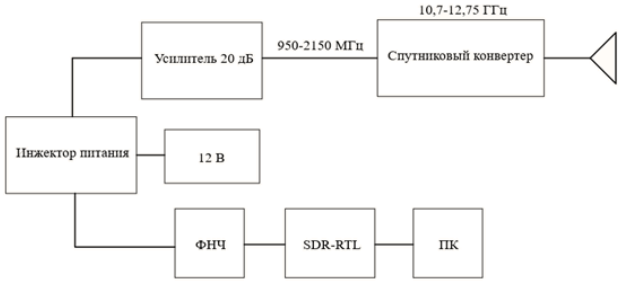


Рис. 1. Схема макета радиометра

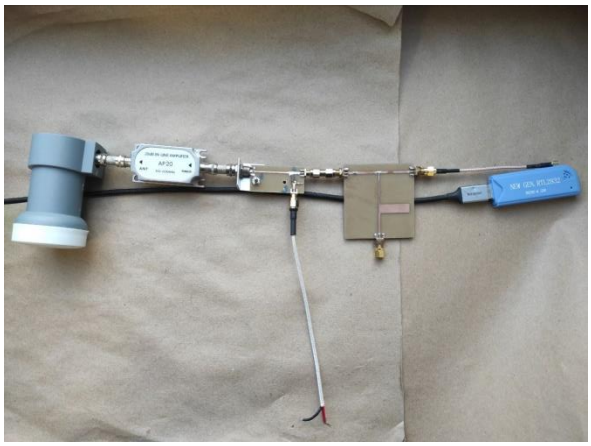


Рис. 2. Макетный образец радиометра

Для увеличения чувствительности радиометра, мы можем управлять двумя параметрами: полосой пропускания и временем интегрирования [3]. Так как полосу пропускания при использовании данного SDR-RTL приемника увеличить не представляется возможным, мы можем повысить чувствительность используя накопления. На рис. 3 приведены измерения листа алюминия и квадрата из ABS пластика, на расстоянии 1 метр от приемной антенны, при одинаковом угле зондирования.

После получения квадратур, использовалось быстрое преобразование фурье, а затем перенос полосы в ноль. Предварительно, на SDR приемник подавался монохроматический сигнал, известной амплитуды, для калибровки SDR приемника.

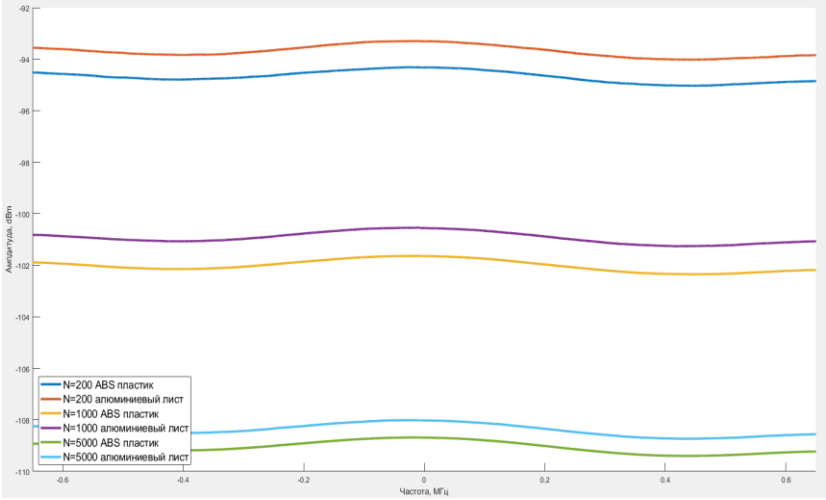


Рис. 3. Измерения при разных накоплениях

Эмиссивность алюминия меньше чем у ABS пластика, а значит и яркостная температура будет выше, что и подтверждают проведенные измерения.

На рис. 4 представлены измерения различных объектов, при числе накоплений равном 200. Данного числа накоплений достаточно чтобы отличать поверхности различных материалов, асфальт, а также небо, имеющее наименьшую яркостную температуру.

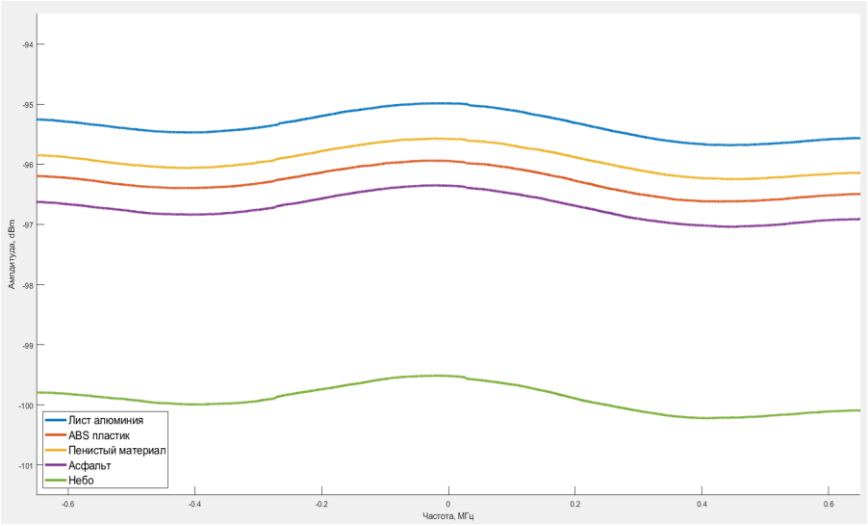


Рис. 4. Измерения различных объектов при числе накоплений 200

Использование данной радиометрической системы в качестве стационарной и не имеющей требований к скорости работы возможно. Для увеличения эффективности в дальнейшем будет использован более широкополосный SDR приемник, что позволит увеличить чувствительность и уменьшить время интегрирования.

Список используемых источников:

1. Practical handbook of remote sensing / Samantha Lavender, Andrew Lavender. Second edition. Boca Raon, FL : CRC Press, 2023. |

2. Николаев А. Г., Перцов С. В. Радиотеплолокация. Сов. Радио, 1964.

3. Микроволновая спутниковая аппаратура дистанционного зондирования Земли : учеб. пособие. СПб. : СПбГУАП. 2003. 404 с. ISBN 5-8088-0081-1

Makarov V., Dunaev N.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Radiometer based on satellite converter and SDR-RTL receiver.

The paper describes a radiometer based on SDR-RTL receiver. The technical characteristics of the developed single-channel radiometer are evaluated, experimental data are given. Its functional characteristics are analyzed on the basis of the data obtained as a result of measurements.

Key words: radiometer, RTL-SDR receiver.

УДК 621.3.049
ГРНТИ 47.13.19

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ ВОЗМОЖНОСТЕЙ ПРИМЕНЕНИЯ АДДИТИВНЫХ ТЕХНОЛОГИЙ В ПРОИЗВОДСТВЕ РАДИОЭЛЕКТРОНИКИ

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

Данная статья рассматриваем актуальные аддитивные технологии, использующие печать пластиком и проводящими чернилами, и их влияние на проектирование и производство электронных устройств. Особое внимание уделяется печати из нескольких материалов одновременно, с примерами применения в промышленности. Статья также рассматривает некоторые сложности, которые возникают в процессе создания изделий.

аддитивные технологии, 3D-печать, радиоэлектроника

Сегодня аддитивные технологии, в том числе 3D печать, обеспечивают оперативный переход от проектирования электронных устройств и прототипов к их изготовлению. Технологии позволяют создавать объекты сложной геометрии путем послойного нанесения материала, что позволяет создавать большое количество различных не только внешних, но и внутренних структур в виде пустот, которые могут быть не видимы снаружи, однако существенно облегчают конструкцию и придают ей свойства, отличающиеся от свойств однородных изделий.

При создании электронных средств особенно интересным является использование устройств, позволяющих осуществлять печать изделий из нескольких материалов одновременно. В самом простом случае такой принтер применяет два материала: пластик для создания корпуса и проводящий материал в виде чернил, или смесь пластика с графитом или медью, для создания токопроводящих путей. Используя этот подход, можно создавать полностью функциональные изделия без необходимости промежуточной сборки.

Например, в статье [1], был описан принтер Voxel8, позволяющий осуществлять печать продукции с применением пластика и проводящих чернил. Благодаря специальному программному обеспечению, конструктор, занимающийся разработкой изделия, может определить расположение проводящих путей в любой плоскости трёхмерного пространства. Такой принтер может производить как плоские печатные платы, так и сложные объекты, такие как батареи или квадрокоптеры (рис. 1). Процесс печати в данном устройстве состоит из нескольких послойно повторяющихся этапов: плавление пластиковой нити и формирование несущего каркаса, осаждение и запекание токопроводящих чернил, установка радиокомпонентов.

Рис. 1. Квадрокоптер, корпус и токопроводящие дорожки которого были напечатаны на 3D-принтере

Описанный выше принтер использует технологию FDM для создания каркаса. Это наиболее простая и распространенная технология 3D печати, но изделия, созданные таким образом, имеют довольно грубую поверхность и требуют дополнительной обработки. Более гладкая поверхность достигается с помощью методов стереолитографии или лазерного порошкового спекания. Например, в исследовании [4] разработан автоматизированный комплекс, способный послойно печатать изделия разной формы из полимерной смолы и наносить на каждом слое фрагменты токопроводящего рисунка (см. рис. 2). Так же в этом исследовании продемонстрировали как с помощью аддитивных технологий можно минимизировать устройство, если использовать объемную компоновку и корпус изделия вместо печатной платы (рис. 3).

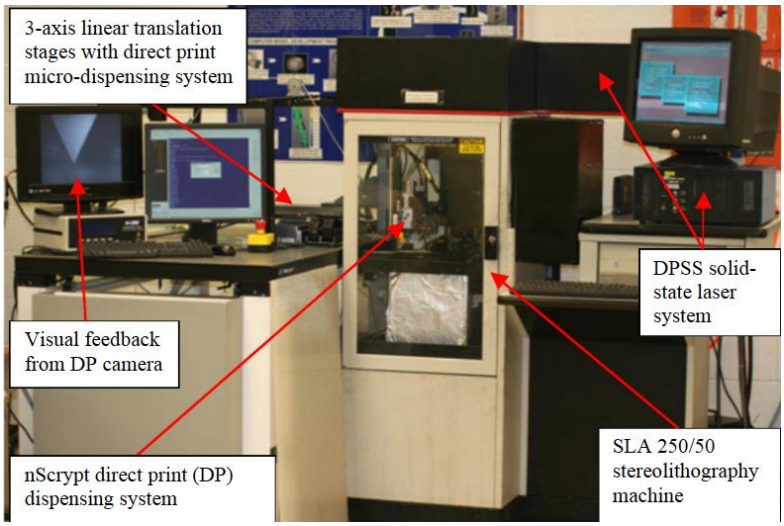


Рис. 2. Комплекс, позволяющий печатать радиоэлектронные изделия из полимерной смолы

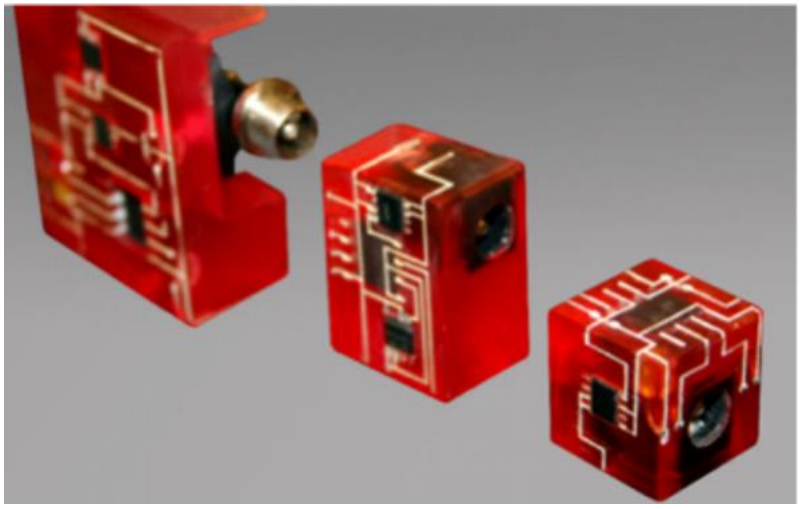


Рис. 3. Три стадии минимизации устройства с использованием 3D-печати

Примечательно, что 3D принтеры позволяют печатать токопроводящий рисунок на любой поверхности, в том числе на сферах. Например, в статье [2] для уменьшения размеров антенны исследователи применили технологию конформной печати токопроводящими чернилами (рис. 4). Вариативность поверхностей, на которых можно печатать токопроводящими материалами позволяет проектировать более компактные конструкции, так как проводящие дорожки и антенны могут быть частью корпуса изделия, что может найти свое применение в создание беспилотных летательных аппаратов или новых моделей смартфонов.

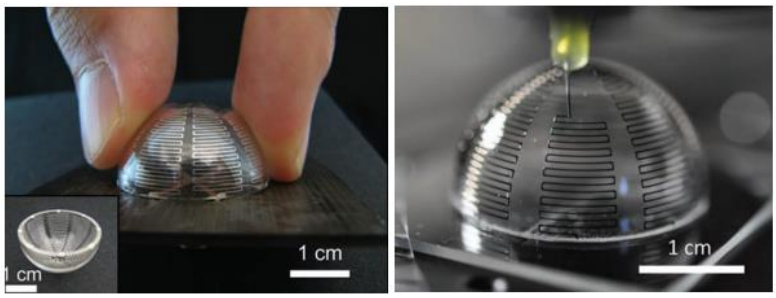


Рис. 4. Миниатюрная антенна сферической формы

Например, компания Optomec [3] предоставляет услуги нанесения токопроводящих чернил на поверхности любой формы, при этом оборудование, которое они используют позволяет осаждать материал в высоту и ширину с точностью до десятков микрон. Использование аддитивной печати в таком случае избавляет производство от создания заготовок и трафаретов для травления проводящего рисунка. Компания показала, что с помощью их технологий возможно уменьшить размер и вес смартфонов, если некоторые токопроводящие элементы, такие как антенны, наносить сразу на поверхность корпуса, что высвобождает дополнительное место на печатной плате и избавляет от шлейфов и проводов (рис. 5).

Рис. 5. Антенны, нанесенные на корпуса различных устройств без использования трафаретов и дополнительных заготовок

Нанесение токопроводящих чернил непосредственно в процессе печати изделия позволяет создавать изделия любой сложности, однако в процессе печати между слоями могут возникать зазоры, через которые возможно непредусмотренное проникновение токопроводящих частиц, что увеличивает риск возникновения коротких замыканий. Особенно эта проблема актуальна для FDM печати. Чтобы снизить риск проникновения чернил между слоями можно увеличить толщину этих слоев и расстояние между токопроводящими дорожками. Однако, если требуется высокая плотность компоновки, то перед нанесением чернил стоит покрывать пластиковый слой дополнительным защитными диэлектрическими материалом [5] (см. рис. 6). В качестве

защитного материала можно использовать тот же пластик, что и для корпуса, но наносить его с помощью стереолитографии, то есть использовать гибридный подход для печати несущей основы.

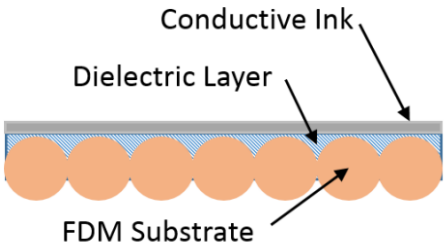


Рис. 6. Структура слоя с защитным диэлектрическим покрытием

Список используемых источников:

1. Espera Alejandro & Dizon, John Ryan & Chen, Qiyi & Advincula Rigoberto. 3D-printing and advanced manufacturing for electronics // Progress in Additive Manufacturing. 2019. DOI: 10.1007/s40964-019-00077-7.

2. Adams Jacob & Duoss Eric & Malkowski, Thomas & Motala, Michael & Ahn, Bok & Nuzzo, Ralph & Bernhard, J.T. & Lewis, Jennifer. Conformal Printing of Electrically Small Antennas on Three-Dimensional Surfaces. Advanced materials. Deerfield Beach, Fla. 2011. DOI: 10.1002/adma.201003734.

3. Are 3D-Printed Electronic Components the Real Deal? [Электронный ресурс] // All about circuits. URL: https://www.allaboutcircuits.com/news/aerosol-3d-printed-electronics-and-the-future-of-wearables-the-iot-and-more/ (дата обращения: 17.10.2023)

3. Lopes Amit & Macdonald, Eric & Wicker Ryan. Integrating Stereolithography and Direct Print Technologies for 3D Structural Electronics Fabrication // Rapid Prototyping Journal. N 18. P 129-143. 2012. DOI: 10.1108/13552541211212113.

4. Perez K.B. & Williams Christopher. Combining additive manufacturing and direct write for integrated electronics - A review // 24th International SFF Symposium - An Additive Manufacturing Conference, SFF 2013. P 962-979.

Zarubin I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Research of modern possibilities of application of additive technologies in the production of radio electronics.

This article examines current additive technologies that use printing with plastic and conductive inks, and their impact on the design and production of electronic devices. Particular attention is paid to printing from multiple materials simultaneously, with examples of industrial applications. The article also examines some of the difficulties that arise in the process of creating products.

Key words: additive technologies, 3D printing, electronics.

УДК 004.416
ГРНТИ 47.13.11

ОБЗОР САПР CADENCE ALLEGRO И АНАЛИЗ ОТЕЧЕСТВЕННЫХ АНАЛОГОВ

Д. И. Кирик, З. В. Михайлова
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлен обзор Cadence Allegro PCB Design Solution. Выявлены его особенности и недостатки. Также были профилирован российские аналоги Delta Design и Lithium ECAD.. В заключении была проведена сравнительная характеристики данных трех систем автоматизированного проектирования.

Cadence Allegro PCB Design Solution, САПР, ЕСКД, CIS, Delta Design, Lithium ECAD

Прогресс в области конструирования электронной техники определяется увеличением производительности и функциональности полупроводниковых технологий. С ростом сложности новых устройств, конфигурация выводов компонентов, уменьшение расстояний между ними, плотность их размещения, наличие современных интерфейсов компонентов становится основополагающими факторами разработки. Для реализации таких конструкторских и технологических решений необходима система автоматизированного проектирования удовлетворяющая современным требованиям разработки. Примером такой системы служит Cadence Allegro PCB Designer. Проведем обзор данного пакета программ.

Cadence Allegro PCB Design Solution - это масштабируемая среда разработки печатных плат, которая предназначена для решения актуальных технологических и методологических задач, сокращения сроков разработки и повышения надежности циклов разработки [1]. Данный пакет программ предполагает проектирование интегральных схем, проведение аналогово и цифрового моделирования, подготовку к производству многослойных печатных плат высокого уровня.

Рассмотрим основные особенности данного пакета:

- Возможность использования схемного редактора, который совместим с OrCAD, в сочетании с импортом схем, плат и библиотек из P-CAD и Altium. Встроенные отчеты в Allegro позволяют генерировать документацию в соответствии с едиными стандартами конструкторской документации (ЕСКД) непосредственно из САПР [2].
- Взаимодействие между схемным редактором и редактором печатных плат позволяет перемещать компоненты со схемы на плату в процессе размещения, выделять компоненты на схеме и видеть их на плате, а также выделять выводы или цепи на плате. Использование единой библиотеки компонентов предприятия, такой как Component Information System (CIS),

помогает сократить количество ошибок при создании компонентов, связанных с человеческим фактором.

- Система выравнивания длин сигналов обеспечивает все современные требования к трассировке скоростных интерфейсов типа PCIe, Ethernet, HDMI, DDR (T-соединения, Fly-By) и др.
- Опция Interconnect Flow Planner, позволяющая создавать сигнальные жгуты, которые предоставляют возможность автоматизированно планировать соединения и трассировку.
- Опция High Speed, расширяющая набор контролируемых электрических ограничений. Более того данная опция предполагает сохранение целостности сигналов и обеспечение точных временных характеристик.
- Интеграция с библиотеками компонентов предприятия, PDM-системами, механическими САПР, такими как Компас 3D, импорт и экспорт STEP моделей.
- Многопользовательская параллельная методология разработки для ускорения процесса и уменьшения времени планирования. С ее помощью множество разработчиков могут трудиться одновременно, имея доступ к общей базе данных независимо от удаленности.
- А также возможность обратной сверловки, смещенной трассировки, автоматического равномерного распределения трасс, учет задержки распространения в переходных отверстиях, учет разной задержки сигналов внутри микросхемы.

Основными недостатками данного пакета программ принято считать его огромную стоимость, английский язык интерфейса, трудоемкое и времязатратное обучение, необходимость дополнительных плагинов и расширений, зависимость от производителя, что может повлиять на продолжительность поддержки и доступность новых функций.

Рассмотрим отечественную альтернативу, разработанную компанией Eremex в 2015 году.

Delta Design – это первая современная отечественная система автоматизированного проектирования печатных плат, реализующая сквозной цикл проектирования [3].

Система поддерживает российские и международные стандарты. Важной особенностью является инновационная модель компонентов, что делает создание базы данных электрорадиоизделий интуитивно понятным и простым процессом. В данном САПР включен функционал схемотехнического редактора, позволяющего проектировать электрические схемы на основе выбранных стандартов проектирования и оформления. Система также поддерживает создание схем со сложной иерархической структурой, предоставляя множество инструментов для реализации даже самых сложных технических решений. Данный САПР поддерживает моделирование как аналоговых, так и цифровых процессов, происходящих в электрических схемах. Более того, существует возможность моделировать

работу программного обеспечения, которое планируется использовать для разрабатываемых устройств.

Система обеспечивает автоматизированное размещение компонентов и трассировку печатных плат, включая поддержку дифференциальных пар и контроль зазоров и длин проводников.

Комплексная 3D-визуализация позволяет разработчикам не только создавать реалистичные 3D-модели, но и отслеживать пересечения компонентов, совместимость и визуализацию корпусов радиоэлектронных устройств.

Система позволяет выпускать как конструкторскую, так и производственную документацию, обеспечивая соблюдение стандартов и возможность использования ее на автоматических производственных линиях.

Рассмотрим еще одну российскую кроссплатформенную САПР печатных плат, поддерживающую синхронизацию схемы и платы в реальном времени - Lithium ECAD [4]. Данная система предоставляет функции поиска и захвата компонентов, включая возможность импорта компонентов из редактора схемы. Более того данный САПР предполагает инструменты автоматической нумерации компонентов. проверки соответствующих правил разработки (ERC), проверки на правила проектирования печатных плат (DRC). Также присутствуют функции сквозного выделения и стека слоев, которые позволяет выделять компоненты и цепи на плате непосредственно из редактора схемы и предоставляет возможность настройки стека слоев и допустимых переходных отверстий на плате.

САПР Lithium ECAD поддерживает трехмерный просмотр модели печатной платы с компонентами, что может быть полезно для визуальной оценки конструкции.

Для передачи в производство САПР генерирует необходимые файлы в форматы Gerber 274X, NC Drill и PnP.

Далее проведем сравнительную характеристику рассмотренных программных систем. Результаты анализа представлены в Таблице №1.

В итоге, выбор между Cadence Allegro, Delta Design и Lithium ECAD зависит от ряда факторов, включая сложность проекта, бюджет, опыт пользователя и специфические требования. Каждая из этих систем предлагает уникальные преимущества и особенности, которые могут быть весьма полезны в зависимости от ситуации.

В конечном итоге, решение должно быть принято с учетом конкретных потребностей проекта и доступных ресурсов. Независимо от выбора, важно помнить, что каждая из этих САПР спроектирована для облегчения процесса электронного проектирования и повышения качества конечного продукта.

ТАБЛИЦА 1. Сравнительный анализ Cadence, Delta Design и Lithium ECAD

Критерии	Cadence Allegro	Delta Design	Lithium ECAD

Производительность и функциональность	Высокая производительность	Базовый функционал	Базовый функционал
Интерфейс и удобство использования	Сложный интерфейс, только иностранный язык	Русифицированная система	Русифицированная система
Стоимость	Дорогое решение	Доступное решение	Доступное решение
Сообщество и поддержка	Обширная база знаний, но есть риск отказа в поддержке	Менее значительные	Менее значительные
Совместимость и экосистема	Интегрируется с другими инструментами Cadence	Ограниченная экосистема	Ограниченная экосистема
Реализация совместного проектирования в реальном времени	Поддерживает	На данный момент не поддерживает	Поддерживает
Наличие отечественных и импортных баз данных	Поддерживает	Поддерживает	Поддерживает
Наличие автоматического размещения компонентов и трассировки плат	Поддерживает	Поддерживает	Поддерживает

Список используемых источников:

1. Pcbsoft.ru // Cadence Allegro [Электронный ресурс]. URL: https://www.pcbsoft.ru/cadence-allegro (дата обращения: 15.10.2023)
2. Cadence.com // Allegro PCB design [Электронный ресурс]. URL: https://www.cadence.com/en_US/home/tools/pcb-design-and-analysis (дата обращения: 06.10.2023)
3. Eremex.ru // САПР Delta Design [Электронный ресурс]. URL: https://www.eremex.ru/products/delta-design/ (дата обращения: 06.10.2023)
4. Lecad.ru // Lithium ECAD [Электронный ресурс]. URL: https://www.lecad.ru/ (дата обращения: 06.10.2023)

Kirik D., Mikhailova Z.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Review of Cadence Allegro SAR and analysis of domestic analogs.

This article presents an overview of Cadence Allegro PCB Design Solution. Its features and disadvantages are revealed. Also Russian analogs Delta Design and Lithium ECAD were profiled. In conclusion, a comparative characterization of these three computer-aided design systems was carried out.

Key words: Cadence Allegro PCB Design Solution, CAD, ECD, CIS, Delta Design, Lithium ECAD.

УДК 004.738
ГРНТИ 49.33.29

БЕСПРОВОДНАЯ СИСТЕМА ПРОТИВОПОЖАРНОЙ СИГНАЛИЗАЦИИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ZIGBEE

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

Системы пожарной безопасности являются очень важными и необходимыми в каждом доме и как любые другие системы требуют модернизации под современные нужды и возможности. В большинстве современных жилищ присутствуют системы умного дома, к которым можно интегрировать системы противопожарной сигнализации с помощью технологии ZigBee. В работе представлен анализ функциональных блоков и особенностей их схемотехнических конструкций на основе типовых решений в проектах централизованной системы противопожарной сигнализации и устройств, предотвращающих чрезвычайные ситуации объединенных беспроводной сетью.

датчик, реле, контроллер, беспроводная сеть, охранно-пожарная сигнализация, ZigBee

Актуальность:

В настоящее время применение беспроводных технологий в различных областях техники приобретают все большую популярность, в том числе все чаще встречается их использование при проектировании систем охранно-пожарной сигнализации. Элементам противопожарной системы, таким как датчики и элементы управления, не требуется высокая пропускная способность, но они нуждаются в низкой задержке и очень низком энергопотреблении для длительного срока службы батареи, особенно в случаях сложных систем. Поэтому актуальным является изучение типовых решений, применяемых в проектировании датчиков и систем управления, например, с использованием технологий ZigBee.

Цель: Планирование общей системы противопожарной сигнализации с использованием беспроводных технологий в частотном диапазоне 2,4 ГГц, с единым управлением с вторичного устройства через приложение.

С этой целью рассмотрены различные решения создания беспроводных систем противопожарной сигнализации, в том числе готовые, доступные на рынке, и способы их улучшения, проведено сравнение полученных результатов. В работе для анализа общих принципов схемных решений были выбраны следующие устройства противопожарной сигнализации и контроля безопасности: комбинированный датчик дыма и газа, датчик влажности, комбинированный датчик дыма и тепла и реле контроля тока. С целью создания беспроводной системы и улучшения рассматриваемых готовых решений был проведен анализ технологий ZigBee и LoRaWAN.

На рынке противопожарных датчиков до сих пор преобладают устройства, работающие в частотном диапазоне 433 МГц с низкой

пропускной способностью канала и невысокой емкостью, которые при объединении в одну беспроводную сеть имеют большую стоимость и высокое энергопотребление.

Один из способов улучшения характеристик беспроводных систем противопожарной сигнализации, это переход на частотный диапазон 2.4 ГГц, что позволяет уменьшить энергопотребление, увеличить емкость системы и увеличить пропускную способность беспроводного канала.

При использовании технологии ZigBee можно получить централизованную систему пожарной безопасности применимую в жилых квартирах и домах с небольшим энергопотреблением при невысокой себестоимости.

Также в качестве решения улучшения характеристик беспроводных систем можно использовать технологию LoRaWAN. Такая технология работает в частотном диапазоне 868 МГц. Протокол LoRaWAN оптимизирован для малобюджетных сенсоров с работой от батарей и включает в себя различные классы узлов. Тем самым обеспечивается компромисс между скоростью доставки информации и временем работы устройства, что особенно важно ввиду использования питания от батарей или аккумуляторов.

LoRaWAN работает на более дальних расстояниях, но имеет более высокую стоимость и меньшую пропускную способность в отличие от технологии Zigbee.

LoRaWAN использует топологию сети типа «звезда», в то время как Zigbee использует топологию ячеистой сети. Для LoRaWAN это означает, что каждый узел устройства взаимодействует с определенным шлюзом. В случае с Zigbee, каждый узел может связываться с любым другим узлом в ячеистой сети, что делает его идеальным для удаленного многозарядного переключения.

Сравнив две основных технологии, более целесообразно выбрать решение перехода на частотный диапазон 2.4 ГГц и, следовательно, использование технологии ZigBee при проектировании устройства противопожарной безопасности.

По статистике к самым распространенным причинам возгорания в жилых помещениях относятся неисправность внутриквартирных (внутридомовых) систем электрооборудования, протечка природного газа, открытый огонь с последующим задымлением и также повышенная или пониженная влажность воздуха. Последнее связано с тем, что, чем выше влажность, тем выше может быть скорость распространения огня. При пониженной влажности возможно более быстрое распространение пожара, так как горючие материалы могут быстрее загораться и гореть с большей интенсивностью. Также при низкой влажности может увеличиваться вероятность возникновения ионизации в воздухе, что усиливает электрическую активность и это, в свою очередь, может вызвать возникновение и распространение пожара.

Предлагается создать единую централизованную систему из датчиков газа, дыма, контроля влажности, тепла и реле контроля тока модернизированного интегрированной технологией ZigBee. Можно использовать готовые устройства с встроенной технологией ZigBee, в том числе комбинированные датчики.

Если рассматривать среднестатистическое жилое помещение средней площади потребуется: один комбинированный датчик дым-газ в кухонное помещение, датчик влажности в каждую комнату (кроме санузлов), несколько комбинированных датчиков дым-тепло в комнаты в количестве, зависимом от высоты потолков и длины помещения и одно реле контроля тока. Устройства с датчиками должны также включать звуковые и световые оповещатели.

Для подключения проектируемого датчика через беспроводную сеть, построенной на технологии ZigBee, необходимо, чтобы в конструкции присутствовали такие функциональные узлы схемы, как координатор, роутер, конечное устройство. Конечным устройством являются устройства, состоящие из выбранных датчиков и приемопередатчиков. Роутер передает данные сети без изменений. Роутеры могут быть как беспроводными, так и объединенные в проводную сеть по Ethernet.

Также есть возможность объединения пожарных оповещателей и роутеров для сокращения количества устройств сети, что упрощает монтаж, уменьшает стоимость системы и энергопотребление. Конечное устройство передает данные через ряд роутеров на координатор, который осуществляет контроль работоспособности всей сети.

Обработка данных происходит на приемно-контрольном модуле (ПКМ), который включает в себя координатор. ПКМ отображает на встроенном LCD-дисплее тревожные сообщения (пожар, несанкционированное проникновение в помещение и т.д.), а также информацию о том, в каком помещении сработал соответствующий датчик.

Кроме отображения на дисплее, данные передаются на смартфон для последующей обработки программным обеспечением автоматизированного рабочего места оператора. Структурная схема Беспроводной системы противопожарной сигнализации представлена на рис.1.

С помощью использования беспроводной сети все устройства связаны между собой. Система будет работать таким образом: во время возникновения опасности (при срабатывании одного датчика) все подключенные к системе оповещатели дают извещательный сигнал, который можно отключить с помощью предустановленного программного обеспечения с мобильного устройства. Также с помощью данного ПО можно будет отследить, какой именно датчик сработал.

Также в случае возникновения опасности неисправности электрооборудования, например, при превышении тока установленного значения, через время задержки будет срабатывать реле. При снижении тока реле через время, равное 5 с, происходит переключение контактов в

положение 10–11. В трехфазной сети реле измеряет ток в нулевом проводе с помощью выносного датчика тока.

При возникновении короткого замыкания в линии замыкается цепь питания катушки независимого расцепителя, который срабатывает и отключает автоматический выключатель. Реле контроля тока требует интеграции технологии ZigBee и имеет возможность для этого с помощью простого схемотехнического решения. Такое решение позволит предотвратить одну из самых частых причин возникновения пожара, а при помощи использования беспроводной технологии позволит контролировать эту систему дистанционно.

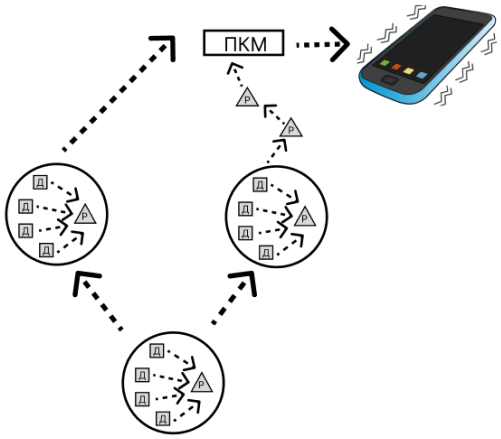


Рис. 1 Структурная схема БСПС

Заключение:

В докладе представлена типовая схема беспроводной системы пожарной безопасности с использованием технологии ZigBee, проанализирована её работа и функционал. На основе проведенного анализа ведется разработка проекта системы датчиков и реле контроля тока, которую можно будет использовать в качестве дистанционного контроля пожарной безопасности помещения через приложение на мобильном устройстве. Конструкция позволит изменять количество датчиков, оптимизируя работу системы в зависимости от площади и параметров помещения, и подключать устройство к беспроводной сети. В дальнейшем планируется модернизировать схемотехническое решение реле контроля тока за счет подключения встроенной технологии ZigBee, провести испытания работы единой беспроводной системы противопожарной сигнализации, получить результаты и сравнить с готовыми решениями, представленными на рынке, рассмотреть способы реализации данной системы в производственных масштабах.

Список используемых источников:

1. Самойлов Д. О., Семенов В. Д., Упаев А. Б., Федотов В. А. Беспроводная система охранно-пожарной сигнализации с использованием технологий ZigBee и GSM [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/besprovodnaya-sistema-ohranno-pozharnoy-signalizatsii-s-ispolzovaniem-tehnologiy-zigbee-i-gsm/viewer. (дата обращения: 15.10.2023).

2. Соколов М., Воробьев О., Реализация беспроводных сетей на основе технологии ZigBee стандарта 802. 15. 4 // Компоненты и технологии. N 2. 2005. С. 160-162.

3. Suneel Mudunuru V. Narasimha Nayak, G. Madhusudhana Rao, K. Sreenivasa Ravi REAL TIME SECURITY CONTROL SYSTEM FOR SMOKE AND FIRE DETECTION USING ZigBee [Электронный ресурс]. URL:https://www.researchgate.net/publication/357339701_REAL_TIME_SECURITY_CONTROL_SYSTEM_FOR_SMOKE_AND_FIRE_DETECTION_USING_ZigBee. (дата обращения: 15.10.2023).

4. Приказ МЧС России от 31.07.2020 N 582 Об утверждении свода правил Системы противопожарной защиты. Системы пожарной сигнализации и автоматизация систем противопожарной защиты. Нормы и правила проектирования (вместе с СП 484.1311500.2020. Свод правил. Системы противопожарной защиты. Системы пожарной сигнализации и автоматизация систем противопожарной защиты. Нормы и правила проектирования).

Pugach M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

Wireless fire alarm system based on ZigBee technology.

Fire safety systems are very important and necessary in every home and as any other system need to be develop for modern needs and capabilities. Most modern dwellings have smart home systems, to which fire alarm systems can be integrated using ZigBee technology. The report presents an analysis of functional blocks and features of their circuit designs on the basis of typical solutions in the projects of centralized fire alarm systems and devices preventing emergencies integrated wireless network.

Key words: Sensor, relay, controller, wireless network, fire alarm system, ZigBee.

УДК 621.396.677
ГРНТИ 47.45.29

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ МЕТОДОВ ИЗГОТОВЛЕНИЯ ЗЕРКАЛЬНЫХ АНТЕНН С ПРИМЕНЕНИЕМ АДДИТИВНЫХ ТЕХНОЛОГИЙ

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

С развитием аддитивных технологий появилась возможность изготавливать изделия сложной формы с меньшими ресурсными затратами. На сегодняшний день имеется обширный спектр используемых материалов, различающихся по степени прочности, тангенса угла потерь и качеству образуемой структуры. Одним из главных преимуществ таких антенн является взаимозаменяемость деталей. Если одна из деталей ломается, можно в короткие сроки изготовить необходимую часть.

зеркальная антенна, аддитивные технологии, рефлектор, CAD-система.

Аддитивные технологии (Additive Manufacturing) — метод создания трехмерных объектов, деталей или вещей путем послойного добавления материала: пластика, металла, бетона и, возможно, в будущем — человеческой ткани. Такие трехмерные или 3D-объекты создаются с помощью 3D-принтеров.

В настоящее время на рынке имеются разнообразные аддитивные системы, производящие модели по различным технологиям с использованием разных материалов. Но, все без исключений работают по аналогичному, послойному принципу построения физической модели, который состоит в следующем:

- считывание трёхмерной геометрии из 3D CAD-систем (рис. 1.а);
- разбиение трёхмерной модели на горизонтальные сечения (слои) с помощью специальных программ, предоставляемых с оборудованием или используемой как приложение (рис. 1.б);
- построение сечений детали слой за слоем снизу-вверх, до тех пор, пока не будет получен физический прототип модели. Слои располагаются снизу-вверх, один над другим, физически связываются между собой. Построение прототипа продолжается до тех пор, пока поступают данные о сечениях CAD-модели (рис. 1,в).

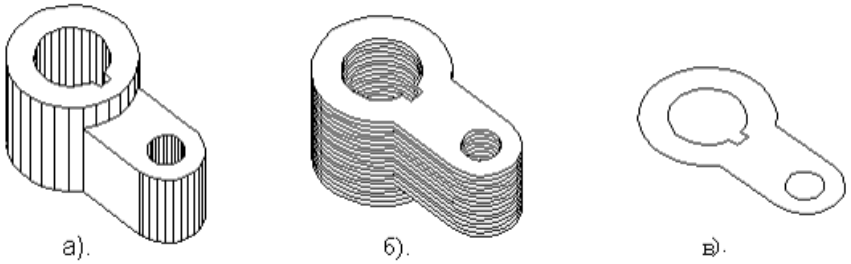


Рис. 1. Принцип построения физической модели

На настоящий период предлагается обширный спектр используемых материалов, различающихся по степени прочности и качеству образуемой структуры. В зависимости от процесса, в АТ используются следующие основные материалы: полистирол, термопластик, бумага, акрил, поликарбонат, нейлон, ABS, синтетические смолы, металлические сплавы в форме порошка [1].

Зеркальные антенны не являются исключением и их части можно изготавливать с помощью аддитивных технологий.

Наиболее активно развивается сейчас SLS-технология – метод послойного селективного лазерного плавления металлических порошков, который дает возможность безотходного изготовления деталей или заготовок непосредственно по данным из 3D CAD-систем практически любой сложности из широкого спектра металлов. Принцип работы этой технологии заключается в выборочном плавлении тонкого слоя металлического порошка лучом лазера в соответствии с геометрией сечения детали, соответствующей каждому слою порошка. Селективное лазерное спекание изначально появилось, как усовершенствованный метод отверждения жидкого фотополимера. Здесь строительным (модельным) материалом являются сыпучие, порошкообразные материалы, а лазер является не источником света, как в SLA-машинах, а источником тепла, посредством которого производится сплавление частичек порошка. В качестве модельных материалов используется большое количество как полимерных, так и металлических порошков. Современные SLS-принтеры способны работать с керамической глиной, металлическим порошком, цементом и сложными полимерами.

Самыми дешевыми по-прежнему остаются FDM-принтеры – устройства, создающие трехмерные объекты путем послойного наплавления филамента (технология "струйной печати"). Эта технология предполагает нанесение модельного материала или связующего состава с помощью струйных головок. Наиболее распространенными принтерами данного типа остаются аппараты, печатающие расплавленной пластиковой нитью. Они могут оснащаться одной или несколькими печатными головками, внутри которых находится нагревательный элемент. Большинство аддитивных принтеров, печатающих пластиковой нитью, способны создавать только одноцветные фигуры, однако в последнее время на рынке трехмерной печати появились машины, использующие одновременно несколько видов филамента. Данное новшество позволяет создать цветные объекты [2].

Мы будем использовать самый простой – это печать на 3д – принтере.

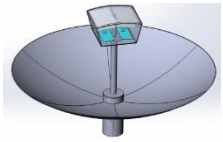


Рис. 2 Исследуемый рефлектор

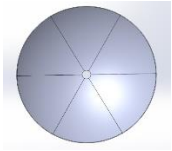


Рис. 3 Поделенный рефлектор

Для упрощения изготовления разобьём рефлектор на 6 равных частей (рис. 3). Каждая из отдельных частей с легкостью может быть напечатана даже на небольшом принтере, что упрощает и удешевляет производство.

В ходе исследования была выбрана конструкция пригодная для 3D печати. В качестве примера разработана конструкция, в которой рефлектор поделен на 6 равнозначных частей. После печати лепестки антенны необходимо металлизировать. Секторный способ компоновки параболоида позволяет компактно сворачивать конструкцию, что актуально не только для носимой техники, но и для транспортировки антенн с большой апертурой на возимой транспортной базе. Так как требования к чистоте поверхности в рассматриваемом диапазонах L и C ниже, чем к более высокочастотным диапазонам Ku и Ka, то можно утверждать, что разработанная конструкция показала возможность изготовления зеркальных антенн с применением аддитивных технологий. А развитие технологии печати металлом позволит упростить технология изготовления и увеличит качество нанесения покрытия.

Список используемых источников:

1. Богомолов А. Ф., Букреев Н. В., Важенцев Г. Н. и др., Космическая складная антенн / Под ред. Пистолькорса А. А. М. : Радио и связь, 1981, вып. 29, С. 10 - 20.

2. Библиотека Казанского национального исследовательского технологического университета [Электронный ресурс] Режим доступа: https://studfile.net/preview/16471531/page:2/ (дата обращения: 21.11.2023).

Staritsyn N.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Research of modern methods of manufacturing parabolic antennas using additive technologies.

With the development of additive technologies, it became possible to manufacture products of complex shape with less resource costs. To date, there is an extensive range of materials used, differing in the degree of strength, the tangent of the loss angle and the quality of the structure formed. One of the main advantages of such antennas is the interchangeability of parts. If one of the parts breaks, it is possible to produce the necessary part in a short time.

Key words: Parabolic antenna, additive technologies, reflector, CAD system.

УДК 621.389
ГРНТИ 47.47.29

ИССЛЕДОВАНИЕ СИСТЕМЫ «УМНЫЙ ДОМ», ПОСТРОЕННОЙ НА ОСНОВЕ ГИБРИДНЫХ ТЕХНОЛОГИЙ ПЕРЕДАЧИ ДАННЫХ

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

В данной работе рассматривается система умного дома, построенная с использованием гибридных технологий передачи данных, а именно проводной и беспроводной. В такой системе удовлетворяются все потребности пользователя. Для реализации данной системы были использованы устройства, работающие по протоколу ModBus, а также устройства с протоколом ZigBee. Современные проблемы, существующие в настоящее время в системах умного дома, такие как скорость, расширяемость и бесперебойность работы, решаются с помощью гибридных технологий передачи данных.

Умный дом, IoT, технологии передачи данных, Modbus, ZigBee

Умный дом — это система, объединяющая бытовые устройства и инженерные системы дома в единую информационно-техническую среду, которая позволяет полностью или частично автоматизировать выполнение различных бытовых задач. Как любая другая IoT-система, он состоит из набора базовых узлов (датчиков, исполнительных устройств и контроллеров), передающих информацию о своем состоянии и команды для выполнения каких-либо действий друг другу. Главной проблемой в системах умного дома на данный момент является большое количество стандартов передачи данных (проводных и беспроводных), зачастую не совместимых друг с другом. Из-за этого пользователю еще на этапе проектирования системы приходится отдавать свое предпочтение определенному стандарту без возможности дальнейшего масштабирования системы и интеграции новых устройств.

На данный момент в «классических» решениях умного дома интеграторы чаще всего применяют проводные стандарты передачи данных, такие как KNX, Modbus, CAN, 1-Wire и т.д. Основными проблемами данного подхода являются:

−невозможность установки системы умного дома после завершения ремонта;

−необходимость прокладки новых кабельных трасс для дальнейшего расширения системы;

−необходимость закладывания в проект ремонта избыточного места для установки щитового оборудования и прокладки кабельных трасс;

−невозможность подключения к уже существующей системе дополнительных устройств, работающих на ином протоколе.

Помимо «классических» проводных вариантов реализации системы активно набирают популярность решения, построенные на базе беспроводных протоколов, например, Wi-Fi, ZigBee, Z-wave, Bluetooth и т.д. Данные варианты реализации умного дома не требуют прокладки дополнительных кабельных трасс, легко масштабируются, не занимают место в электрическом щите дома, имеют возможность интеграции в уже завершенный ремонт и т.д. Несмотря на все преимущества, данный вариант обладает рядом недостатков, которые не позволяют использовать его в полной мере как альтернативу профессиональным проводным решениям. Среди недостатков беспроводных систем можно выделить:

−ненадежность беспроводного соединения;

−отсутствие некоторых типов устройств (например, модулей управления вентиляционными системами и системами увлажнения);

−большое количество устройств низкого качества из-за отсутствия обязательной сертификации;

−отсутствие совместимости устройств от разных производителей;

−работа большинства устройств только через облачные платформы в рамках одной экосистемы;

−отсутствие нативной поддержки устройствами контроллеров, отличных от оригинальных контроллеров определенного производителя.

Наиболее часто данным проблемам подвержены устройства, работающие на базе стандартов Wi-Fi и ZigBee.

Одним из вариантов решения данного ряда проблем в реализации системы умного дома является использование гибридного подхода в вопросе выбора базовых стандартов для проектирования системы. В качестве примера реализации данного подхода рассмотрена система умного дома на базе программируемого контроллера Wiren Board [2], поддерживающего работу как с проводными, так и с беспроводными стандартами связи. В умном доме реализованы следующие системы:

−система управления освещением (23 зон освещения);

−система климат-контроля (7 батарей водяного отопления, 3 кондиционера, система приточно-вытяжной вентиляция, система увлажнение воздуха, 15 климатических сенсоров);

−система защиты от затоплений;

−моторизованные шторы;

−система голосового управления.

Выбор гибридной реализации системы умного дома был обоснован особенностью размещения и габаритов электрических щитов в дизайн-проекте, из-за которой было невозможно в полной мере реализовать управление всем освещением при помощи классических проводных модулей, устанавливаемых в щит, так как для их монтажа недостаточно свободного места. Также важным аргументов в пользу такого варианта реализации стало пожелание заказчика учесть возможность дальнейшего расширения системы умного дома при помощи беспроводных модулей.

В результате согласований вариантов реализации принято решение добавить в контроллер Wiren Board специальные модули расширения ZigBee.

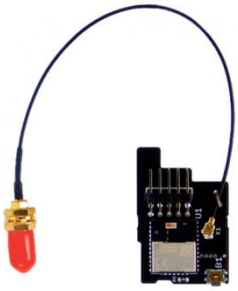


Рис. 1. Модуль расширения ZigBee

Выбор протокола ZigBee [3] был обусловлен низким энергопотреблением и поддержкой mesh-технологии, позволяющей каждому устройству принимать на себя роль коммутатора, для обеспечения высокой степени отказоустойчивости, а также возможностью добавления новых устройств для интеграции в систему умного дома.

После сборки щита, подключения всех устройств по протоколу ModBus, а также установки модулей расширения ZigBee, все устройства были объединены в единую систему.

Рис. 2. Готовый щит умного дома с установленными модулями расширения

После отладки системы, а также проверки работоспособности всех устройств работы были закончены. Исходя из полученных данных, а также продолжительной проверки в формате реального использования системы

(более 6 месяцев) пользователем, можно сделать вывод, что использование гибридных систем в рамках проектирования умного дома является не менее надежным и более функциональном, по сравнению с «классическими» проводными системами.

Список используемых источников:

1. Разбор проекта умного дома. [Электронный ресурс] // Home-Paradise. URL: https://www.home-paradise.ru (дата обращения: 09.05.2023).
2. Модульный программируемый котроллер для автоматизации и мониторинга. [Электронный ресурс] // Wiren Board. URL: https://wirenboard.com/ru/product/wiren-board-7/ (дата обращения: 09.05.2023).
3. ZigBee Specifications. [Электронный ресурс] // ZigBee. URL: https://www.zigbee.org/spec_download/download_request.asp (дата обращения: 09.05.2023).

Tarasov V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Research of the ”Smart Home" system based on hybrid data transmission technologies.

This paper examines a smart home system built using hybrid data transmission technologies, namely wired and wireless. Using such a system will satisfy all the user's needs. To implement this system, devices that operate using the ModBus protocol, as well as devices with the ZigBee protocol, were used. Modern problems that currently exist in smart home systems, such as speed, expandability and uninterrupted operation, are solved by using hybrid data transmission technologies.

Key words: Smart home, IoT, data transmission technologies, Modbus, ZigBee.

Секция 2.4
Радиотехнические системы и антенны

УДК 004.932.72'1
ГРНТИ 28.23.15

РАЗРАБОТКА АЛГОРИТМА АДАПТАЦИИ СТАТИСТИЧЕСКОГО НАБОРА ДАННЫХ ДЛЯ НЕЙРОННОЙ СЕТИ, АНАЛИЗИРУЮЩЕЙ ВНЕШТАТНЫЕ СИТУАЦИИ НА ПРОМЫШЛЕННЫХ ОБЪЕКТАХ

Д. А. Агаян, И. Н. Чернов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Разнообразность данных для обучения нейронной сети – важное условие для качественного решения задач искусственным интеллектом. Однако, из-за конфиденциальности требуемой информации, возникновения риска жизни человека или потребности во времени, сбор данных не всегда возможен. В результате хорошей альтернативой могут стать синтетические данные, полученные путём цифровой обработки изображений.

В данной статье объясняется, что такое синтетические данные, когда их лучше всего применять, какие существуют инструменты генерации и какими способами можно задействовать синтетические данные.

обучение нейронной сети, обработка изображений, dataset

Организация обучения нейронной сети осуществляется с формирования данных для обучения и валидации. Независимо от размера и сложности, нейронные сети являются очень требовательными к объему и разнообразию обучающих данных, которые часто называются «*dataset*». Для максимально качественного результата обучения требуется обеспечить должную подготовку набора данных, но к сожалению это не всегда возможно, как альтернативу, следует рассмотреть синтетический метод генерации данных.

Синтетические данные – это искусственные данные, имитирующие наблюдения реального мира, которые используются для подготовки нейронной сети. Работа с синтетическими данными актуальна, когда получение реальных данных невозможно из-за сложности или дороговизны.

Выделим основные преимущества синтетического набора данных:

1) Эффективность использования ресурсов. Генерация синтетических данных может быть намного дешевле, чем сбор данных событий реального мира. Также процесс синтеза может занять считанные дни, а для анализа реальных данных иногда требуются недели, месяцы или даже годы.

2) Исследование редких данных. Не исключено, что данные могут быть редкими или их сбор связан с опасностью. Пример редких данных – это природные явления или антропогенные опасности. Прототипом таких данных могут быть крупные землетрясения, военные действия, террористические акты.

3) Исключение проблем конфиденциальности. При необходимости передачи сторонним лицам уязвимых данных требуется учитывать вопросы конфиденциальности. Генерация синтетических данных устраняет любые

следы деанонимизации засекреченных данных, позволяя создать новый валидный dataset.

4) Простота разметки и контроля. Синтез данных упрощает разметку объектов на изображении, примером может быть сгенерированное изображение парка, на котором автоматически размещаются модели деревьев, людей и животных.

Существует два типа синтетических данных: частичные и полные. Частичный тип – включает в себя синтетические данные и реальные данные из наблюдений и измерений. Примером является сгенерированное изображение огня, вставленное в реальную фотографию комнаты (рис. 1).

Рис. 1. Пример частично синтезированных данных

Полный тип – состоит исключительно из синтетических данных. Например, сгенерированное изображение огня в смоделированном окружении (рис. 2).

Рис. 2. Пример полностью синтезированных данных

В то же время, модели нейронных сетей, обученные исключительно на синтетических данных, в некоторых случаях могут не гарантировать наилучшего качества и надёжности. Например, ПО для систем обнаружения экстренных ситуаций лучше обучать и на синтетических, и на реальных данных. Иные модели нейронных сетей, применение которых связано с меньшей потенциальной угрозой, можно обучать на одних синтетических данных.

За исключение синтезированных данных, также существуют аугментированные и рандомизированные данные.

Аугментированные данные – процесс добавления к dataset слегка изменённых копий существующих элементов. Применение аугментирования данных дополнит dataset почти такими же изображениями, но с небольшими отличиями в цветности, контрастности или яркости (рис. 3, рис. 4).

Рис. 3. Dataset оригинального изображения

Рис. 4. Dataset аугментированного изображения

Рандомизированные данные – процесс сдвигания элементов изображения внутри dataset. Таким образом, исходное изображение становится другим, без существенного изменения или добавления новых параметров (рис. 5).

Рис. 5. Dataset рандомизированного изображения

Таким образом, реализация данных методов позволит улучшить исходный dataset, модифицировав классические способы подготовки данных для обучения нейронной сети, что в первую очередь позволит уменьшить количество ошибок, которые могут допускаться различными датчиками или сенсорами, тем самым позволив увеличить правильность обнаружения искомых объектов в различных ситуациях.

Список используемых источников:

1. Как организовать разметку данных для машинного обучения: методики и инструменты. [Электронный ресурс]. Habr. URL: https://habr.com/ru/articles/572508/ (дата обращения: 12.11.2023).

2. Synthetic Data Generation: Definition, Types, Techniques, and Tools. [Электронный ресурс] Turing URL: https://www.turing.com/kb/synthetic-data-generation-techniques (дата обращения: 12.11.2023).

Agayan D., Chernov I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development of an algorithm for adapting a statistical data set for a neural network analyzing emergency situations at industrial facilities.

Traditional methods of pre-emergency detection are based on sensors or detectors. Application of such sensors does not always give information about the exact place of detection of abnormal situation and often requires a large amount of time for triggering.

This problem can be solved by applying a detection system based on neural convolutional networks. The key to the successful use of neural networks lies in the proper training process and the composition of the training data set.

Key words: Neural network training, image processing, dataset.

УДК 621.396.99
ГРНТИ 49.33.29

АНАЛИЗ ХАРАКТЕРИСТИК ПЕРЕДАЮЩИХ АНТЕНН ОНЧ ДИАПАЗОНА

М. А. Баранов, К. О. Коровин
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время антенны ОНЧ диапазона широко применяются для связи с морскими судами на больших расстояниях. В данной работе рассматриваются характеристики передающих антенн различных конструкций, их преимущества и недостатки.

Анализ характеристик вертикальных антенн

Диапазон ОНЧ соответствует частотам 3-30кГц, часть этого диапазона (10-30кГц) используется для дальней связи. Первый в мире ОНЧ-передатчик, «Голиаф», был построен в Германии в 1943 году, после войны перевезён в СССР, в 1949—1952 годах восстановлен в Нижегородской области. Передающие антенные системы, используемые для этого диапазона, представляют собой огромные сооружения; вертикальные излучатели с очень обширной верхней загрузкой, необходимые, так как электрическая высота антенн мала по сравнению с длиной волны. Для антенны высотой 300-450 метров электрическая высота составляет всего от десяти до сорока пяти тысячных длины волны.

Вертикальный проводник является единственным практически применяемым ненаправленным излучателем на сверхдлинных волнах и, как таковой, он может быть использован в сложных направленных антеннах, составляемых из нескольких ненаправленных элементов.

Применение горизонтальных излучателей при высокой проводимости подстилающей поверхности (земли) на длинных волнах малоэффективно. Положительный эффект от возможности использования длинных (с длиной более 0.25λ) излучателей нивелируется большим поглощением излучения в земле. Кроме того, максимум излучения направлен преимущественно вверх, что не соответствует эффективному возбуждению ионосферных волн. Таким образом, наиболее эффективной передающей антенной для длинных волн является лишь антенна, состоящая из одного или нескольких вертикальных проводов.

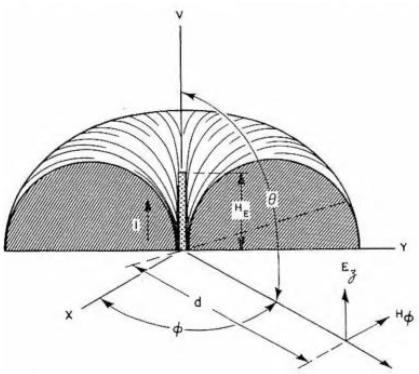


Рис. 1. Модель вертикальной антенны диапазона ОНЧ [1]

Наиболее важными характеристиками антенны являются: вмещаемая мощность 1000-2000кВт, рабочая полоса частот (несколько сот герц), КПД излучения (до 90%). Рассмотрим указанные характеристики для наиболее интересных вариантов конструкций. Основными вариантами передающих антенн, используемых в зарубежных радиостанциях являются следующие: одиночная антенна зонтичного типа с высотой мачты 350-450м (Aguada, USA), многозонтичная антенна с высотами мачт до 350м (Rhauderfehn, Germany), многомачтовая антенна высотами мачт до 380м и развитой верхней нагрузкой типа «звезда» (Cutler, USA, Harold E. Holt, Australia), антенны долинного типа (Jim Creek, USA).

Конструкции антенны представляют собой варианты вертикального диполя, имеющего длину $L \ll \lambda$, т.е. являются электрически малыми антеннами. Оценки эффективности излучения электрически малых антенн проводились как в нашей стране, так и за рубежом. Электрически малой, согласно Вилеру[2], считается антенна, для которой ka <0.5, где к- волновое число, а – радиус сферы, в которую можно вписать антенну. Было показано, что уменьшение размера антенны напрямую ограничивает radiation power factor (RPF), равный отношению излученной мощности к реактивной мощности, т.е. эффективность излучения ограничена размерами антенны. Вилер также показал, что PRF обратно пропорционален добротности Q, таким образом, уменьшение предельного Q антенны соответствует изменению верхнего предела RPF. Согласно Вилеру, нижний предел добротности электрически малой антенны $Q = \frac{1}{(ka)^3}$. В 1948 году в работе Чу [3], был приведен теоретический предел добротности малой антенны как физической системы. Согласно Чу, Q не может быть меньше, чем

$$Q_{M1} = \left[\frac{1}{(ka)^3} + \frac{1}{ka}\right],$$

Таким образом, для антенны заданных размеров в ОНЧ диапазоне задача состоит в приближении к теоретическому пределу добротности. Рассмотрим характеристики существующих антенных систем.

Сравнение характеристик существующих антенных систем

1. Антенна долинного типа (Jim Creek)

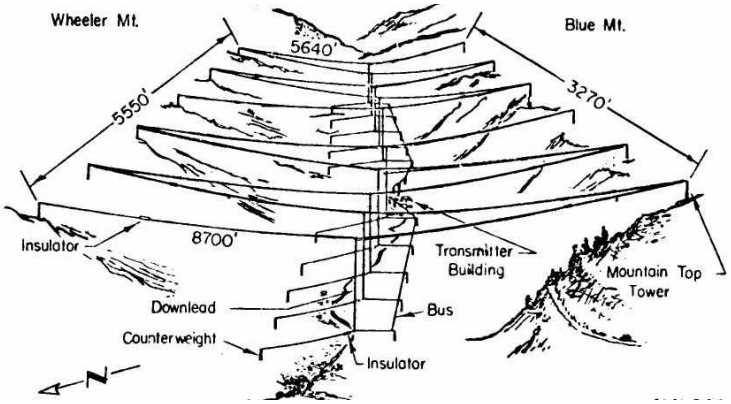


Рис. 2. Антенна долинного типа

Преимуществом таких антенн является использование рельефа местности, что позволяет применять невысокие мачты. Высоты мачт по обеим сторонам ущелья составляют от 20 до 61 метра. Между мачтами зигзагом на изоляторах растянуты 10 проводников, изготовленных из троса диаметром 2.54см. Суммарная длина проводников равна 48 км, при этом периметр образованного ими антенного полотна равен 7.1 км, а его площадь - 2.7 кв.км. Высота подвеса антенного полотна относительно нижнего уровня ущелья составляет около 795 метров. Рабочая ширина полосы пропускания - от 4 до 105 Гц, КПД: от 6-8 до 25%, в т.ч. на рабочей частоте 24.8 кГц - 20%; эффективная высота: от 105 до 116 м, собственная емкость - 78 нФ; сопротивление излучения - от 0.04 до 0.21 ом. Таким образом, основным недостатком является малый КПД излучения.

2. Одиночная антенна зонтичного типа (Aguada)

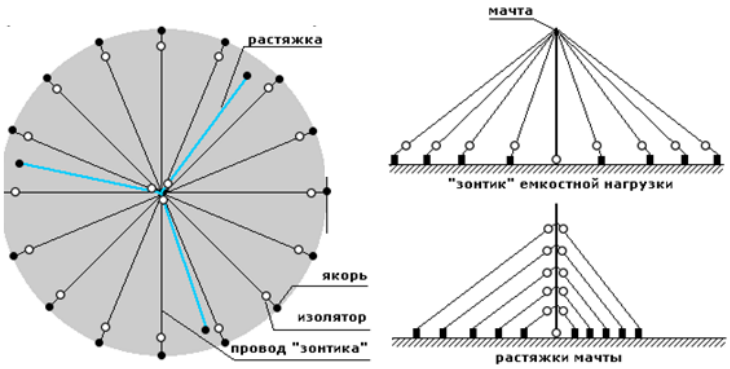


Рис. 3. Антенна зонтичного типа

Одиночные зонтичные антенны обладают достаточно большой вмещаемой мощностью, но сравнительно узкой полосой пропускания. Данный недостаток может быть компенсирован построением многозонтичных систем (Rhauderfehn).

3. Антенна типа «звезда»

Антенна типа «звезда» также называется схемой Trideco и впервые была разработана компанией DECO Electronics для радиостанции Cutler и затем многократно повторена на станции Harold E Holt (Австралия) и на ряде

других станций в Европе. Антенна является совокупностью из 6-ти однотипных антенн, каждая из которых имеет вертикальный излучатель из провода с верхней емкостной нагрузкой в виде ромба, образованного восемью проводами, растянутым между центральной и двумя рядами периферийных мачт.

Рис. 4. Антенна типа звезда (Harold E. Holt) [4]

Для радиостанции Harold E. Holt при токе антенны 1800 А полная мощность передатчика составляет 2000 кВт, сопротивление излучения от 0.142 до 0.329 Ом, эффективная высота: 184 - 194 м; излучаемая мощность: 462/1065 кВт, КПД - до 50%;

Таким образом, можно сделать вывод, что основными характеристиками ОНЧ антенн являются мощность, входное сопротивление, полоса пропускания антенны, ограничения мощности антенны, диаграммы направленности антенны. Эти характеристики будут влиять как на размер, так и на строение проектируемой антенны.

Список используемых источников:

1. Watt A. D. VLF Radio Engineering. 1967.

2. Wheeler H. A. Fundamental Limitations of Small Antennas. Proc. IRE, Vol. 35, December 1947a, pp. 1479–1484.

3. Chu L. J. Physical Limitations of Omni-Directional Antennas. J. Appl. Phys., Vol. 19, December 1948, pp. 1163–1175.

4. Hui Xie, Xiangyu Xu, Huaning Wu, Ning Wang, "Multiobjective Particle Swarm Optimization to Design the Top Load of a Very Low Frequency Thirteen-Tower Umbrella Antenna", International Journal of RF and Microwave Computer-Aided Engineering, vol. 2023

Baranov M., Korovin K.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Analysis of characteristics of transmitting antennas of the VLF band

Currently, UHF antennas are widely used for communication with ships over long distances. This paper discusses the characteristics of transmitting antennas of various designs, their advantages and disadvantages.

Key words: VLF antenna characteristics.

УДК 621.3
ГРНТИ 47.14.07

РАЗРАБОТКА АППАРАТНОЙ ПЛАТФОРМЫ ДЛЯ ОБРАБОТКИ ВИДЕОИЗОБРАЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

А. Г. Васильев, И. Н. Чернов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В России с каждым годом растет потребность в интеллектуальных камерах видеонаблюдения с распознаванием лиц, обнаружением дыма и открытого огня, утечек воды и другие. В связи с этим имеет смысл разработка аппаратной платформы, на которой можно реализовать желаемый функционал и иметь запас по производительности для будущих задач.

SoC, искусственный интеллект, ОЗУ, ПЗУ, мезонинная плата, LDO

К середине августа 2023 года в России насчитывается более 550 тысяч городских камер, часть из которых обладает возможностью распознавания лиц и определением событий [1], подробная статистика представлена на рис. 1.

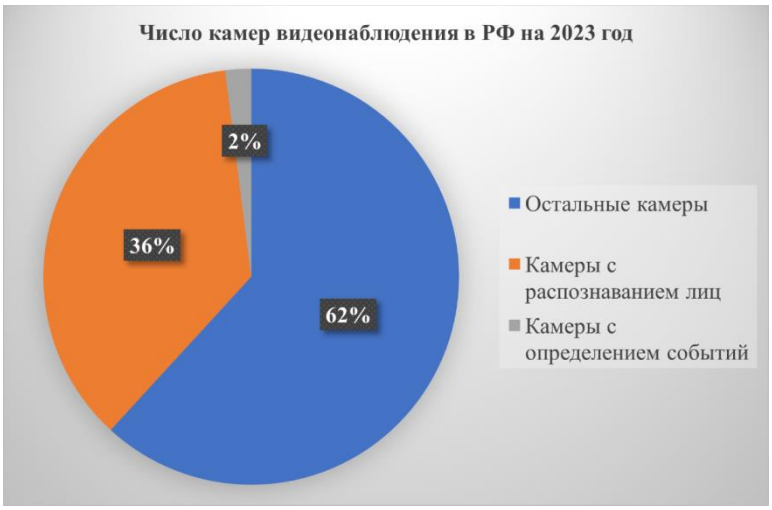


Рис. 1. Информация МВД РФ о количестве камер видеонаблюдения

Это означает, что рынок видеонаблюдения в России будет только расти.

Зачастую обработка видеоизображения происходит либо на удаленном сервере, либо в микрокомпьютере, встроенном с саму видеокамеру. В работе рассматривается вычислительный модуль, встроенный в камеру, поскольку он не требует дополнительного помещения для установки серверов и вся система получается масштабируемой.

Для создания платформы необходимо определится с *System on Chip* (далее *SoC*). В настоящее время в продаже есть как сами *SoC*, так и готовые микрокомпьютеры на их базе. Их перечень приведен на рис. 2.

Производитель	Модель	Производительные ядра	Энергоэффективные ядра	Нейронный сопроцессор	Графический процессор	Видеокодеки	Видеовход	Оперативная память	переферия
RockChip	RK3588	Quad Cortex-A76 2,6 ГГц	Quad Cortex-A55 1,8 ГГц	6 TOPS NPU	Mali-G610	H.265, VP9, AVS2, H.264 AVC/MVC	2x MIPI DC, 4x двухполосных MIPI CSI	LPDDR4 LPDDR4x LPDDR5	PCIe 3.0 X4, 2x 1 Gbit, 2x SATA 3.0, 3x USB 3.1, 2x USB 2.0
	RK3588S	Quad Cortex-A76 2,6 ГГц	Quad Cortex-A55 1,8 ГГц	6 TOPS NPU	Mali-G610	H.265, VP9, AVS2, H.264 AVC/MVC	2x MIPI DC, 4x двухполосных MIPI CSI	LPDDR4 LPDDR4x LPDDR5	1x 1 Gbit, 2x SATA 3.0, 2x USB 3.1, 2x USB 2.0
	RK3399 PRO	Dual Cortex-A72 1,8 ГГц	Quad Cortex-A52 1,42 ГГц	2.4 TOPS NPU	Mali-T860MP3	H.265, VP9, H.264 MVC/VP7	2x четырёхполосные MIPI CSI	DDR3 DDR3L LPDDR3 LPDDR3	PCIe 2.1 X4, 1x 1 Gbit, 1x USB 3.0, 2x USB 2.0
	RK3399	Dual Cortex-A72 1,8 ГГц	Quad Cortex-A52 1,5 ГГц	-	Mali-T860MP4	H.265, VP9, H.264 MVC/VP8	2x четырёхполосные MIPI CSI	DDR3 DDR3L LPDDR3 LPDDR4	PCIe 2.1 X4, 1x 1 Gbit, 1x USB 3.0, 2x USB 2.0
Broadcom	BCM2711	Quad Cortex-A72 1,5 ГГц	-	-	VideoCore VI	H.265, H.264	2x четырёхполосные MIPI CSI	LPDDR4	PCIe 2.1 X4, 1x 1 Gbit, 1x USB 3.0, 2x USB 2.0
	BCM2712	Quad Cortex-A76 2,4 ГГц	-	-	VideoCore V3D VII	H.265, H.264	2x четырёхполосные MIPI CSI	LPDDR4x	PCIe 2.0 X1, 1x 1 Gbit, 2x USB 3.0, 2x USB 2.0
Amlogic	S928X	Single Cortex-A76 2,2 ГГц	Quad Cortex-A55 1,8 ГГц	3.2 TOPS NNA	Mali-G57 MC2	H.265, VP9, H.264 AVC/VP8, AV1, AVS3	-	DDR4 LPDDR4 LPDDR4x	PCIe 2.0 X4, 1x 1 Gbit, 1x USB 3.0, 2x USB 2.0
	A311D	Quad Cortex-A73 2,2 ГГц	Dual Cortex-A53 1,8 ГГц	5 TOPS NPU	Arm Mali-G52MP4	H.265, H.264	-	LPDDR4 LPDDR4x LPDDR5	1x 1 Gbit, 3x USB 2.0

Nvidia	Jetson TX2	Dual Denver 2 2ГГц	Quad Cortex-A57 2 ГГц	5.32 TOPS NPU	NVIDIA Pascal	H.265, H.264	3x четырёхполосные MIPI CSI	LPDDR4	PCIe 2.0 X4, 2x 1 Gbit, 1x USB 3.0, 2x USB 2.0
МЦСТ	R-2000	Octa-core SPARC-v9 2 ГГц	-	-	-	-	-	DDR4 REG ECC	Подключается через контроллер КПИ-2
Байкал элетроникс	BE-M1000	Octa-core Corte-A57 1,5 ГГц	-	-	Mali-T628	H.265, H.264, VP8, VC1, AVS	-	DDR4 DDR3 ECC	1 x PCIe Gen 3.0 X8, 2x 1 Gbit, 2x 10GBASE2 x USB 3.0, 4x USB 2.0, 2x SATA 3.0
Элвис	Скиф	Quad Cortex-A53 1,2 ГГц	-	-	PowerVR Series8XE GE8300	HEVC, H.264	2x MIPI DPHYRx 1	DDR3 LPDDR3 DDR4 LPDDR4	1 x PCIe Gen 3.0 X8, 2x 1 Gbit, 2x USB 3.0,

Рис. 2. Перечень SoC и микрокомпьютеров

Оптимальным по соотношению производительность – количество интерфейсов является *SoC RK3588*. Он имеет 4 производительных и 4 энергоэффективных ядра, а также нейронный сопроцессор.

RK3588 поддерживает ПЗУ стандарта *eMMC* 5.1, но стоит проверить ограничения по совместимости конкретных моделей и модельных рядов в документации к *SoC*. Из доступных в РФ постоянных запоминающих устройств (далее ПЗУ) присутствует множество моделей, как от именитых *Kingston*, так и до менее известных Rayson. Из доступных и недорогих моделей было выбрано ПЗУ *Samsung KLM8G1GETF-B041*, версия на 8 ГБ.

Выбранная *SoC* поддерживает такие стандарты памяти, как *LPDDR4*, *LPDDR4X*, *LPDDR5*. Была выбрано оперативно запоминающее устройство (далее ОЗУ) Micron *MT62F1G32D4DS-031*, поскольку для этой *SoC*.

С выбором преобразователей питания сложнее. У *RK3588* большое количество модулей, у которых разные требования по питанию. Но *RockChip* позаботилась об этом и выпустила специализированные микросхемы питания для таких *SoC*. В данном случае подходит *RK806-1*. У этой микросхемы присутствует несколько *DC-DC* преобразователей и пару *low-dropout linear regulator* (далее *LDO*) преобразователей, что почти полностью покрывает потребности *SoC* в питания. Дополнительные преобразователи питания нужны только для двух групп ядер процессора — *BIG0* и *BIG1*, а также для нейронного сопроцессора — *NPU*. Для них был подобран преобразователь *LTM4622*. Также стоит учесть, что для *SoC* важна правильная последовательность включения питания. На рис. 3 представлена часть диаграммы последовательности включения питания для *RK3588*.

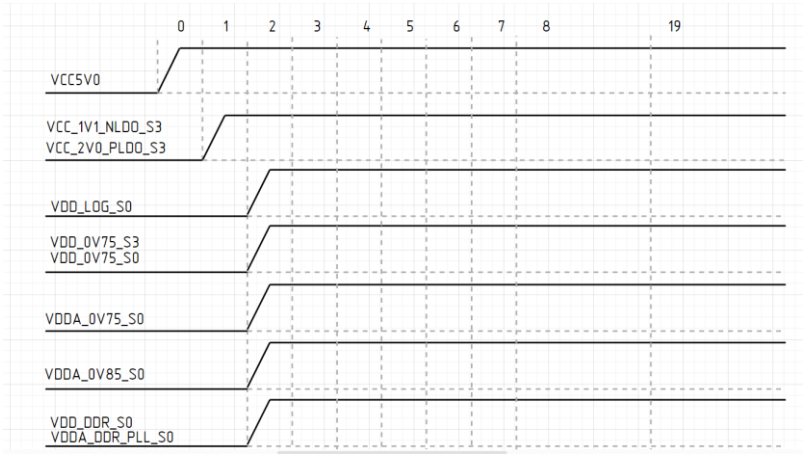


Рис. 3. Последовательность включения питаний

После того, как основные компоненты аппаратной платформы определены, составляется блок-схема. Блок-схема планируемой аппаратной платформы представлена на рис. 4.

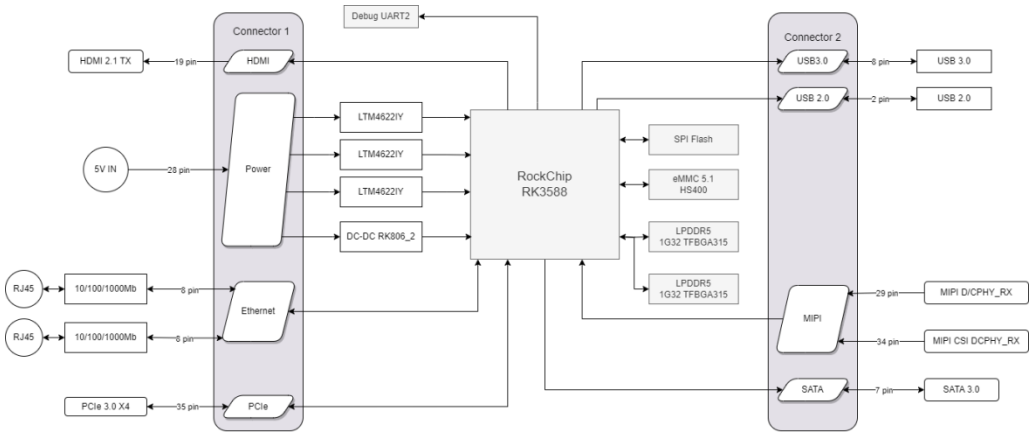


Рис. 4. Блок-схема аппаратной платформы

Следующим этапом является создание принципиальной электрической схемы. Этот этап находится в стадии разработки. На рис. 5 показаны части электрической схемы планируемого изделия.

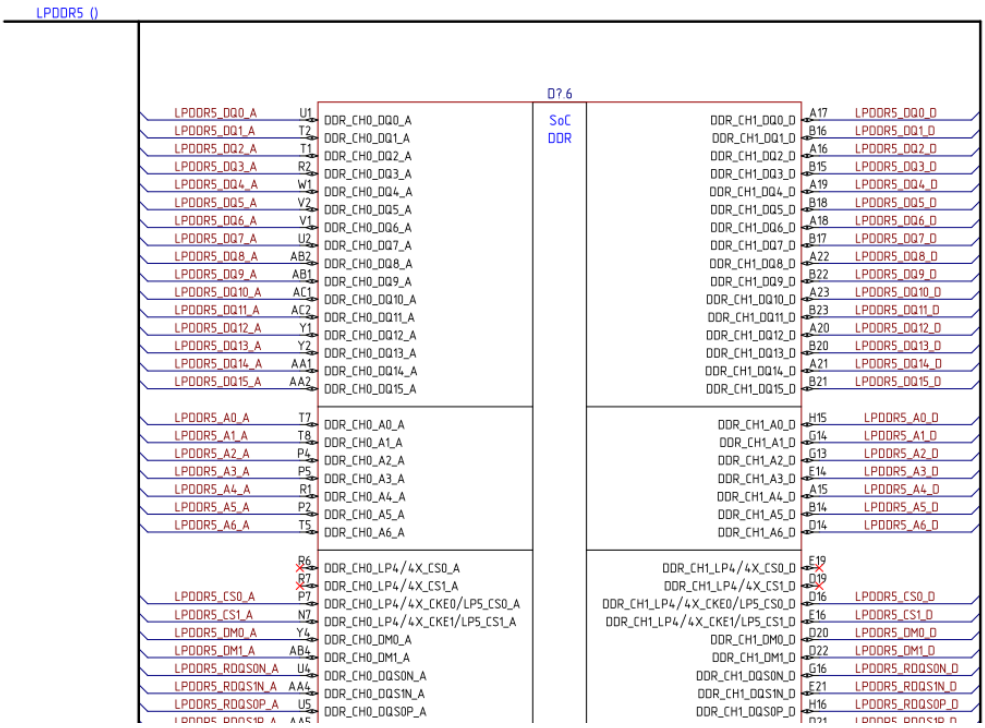


Рис. 5. Часть схемы аппаратной платформы

Поскольку производство будет происходить в России, стоит учитывать технологические возможности местных фабрик. На рис. 6 представлены возможности одного из производств – компании Резонит.

Платы повышенной сложности

Проводник/зазор (внешние слои)	**менее 0,125/0,125 мм** (≥ 0,10 мм)
Проводник/зазор (внутренние слои)	**менее 0,125/0,125 мм** (≥ 0,10 мм)
Минимальное отверстие	**менее 0,30 мм** (≥ 0,20 мм)
Минимальный поясок монтажной контактной площадки	**менее 0,20 мм** (≥ 0,15 мм)
Минимальный поясок площадки переходного отверстия	**менее 0,15 мм** (≥ 0,10 мм)

Коэффициент = 1.5 к стоимости подготовки и дм^2.

Рис. 6. Возможности производства компании Резонит

Пятый класс точности довольно дорогостоящий, поэтому целесообразно *SoC*, ОЗУ, ПЗУ и систему питания разместить на небольшой мезонинной плате. Мезонинная плата будет соединяться с основной платой, которая гораздо менее требовательна к классу точности и может размещать на себе остальную компонентную базу. При дальнейшей разработке также будет произведен анализ целостности сигналов и моделирование печатной платы, что позволит убедиться в отсутствии ошибок при трассировке печатной платы.

Таким образом, создаваемая аппаратная платформа обеспечит возможность строить на её базе разнообразные интеллектуальные системы с необходимым количеством интерфейсов, в том числе системы для обработки видеоизображения с использованием искусственного интеллекта.

Список используемых источников:

1. Объем рынка видеонаблюдения в России на 2023 год [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/ (дата обращения: 13.11.2023).
2. Analog Devices [Электронный ресурс]. URL https://www.analog.com/en/index.html. (дата обращения: 13.11.2023).
3. RockChip [Электронный ресурс]. URL: https://www.rock-chips.com/a/en/. (дата обращения: 13.11.2023).

Vasilev A., Chernov I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

In Russia, the need for smart video surveillance cameras with facial recognition, smoke and open fire detection, water leaks, and others is growing every year. In this regard, it makes sense to develop a hardware platform on which you can implement the desired functionality and have a performance reserve for future tasks.

Key words: SoC, AI, RAM, ROM, mezzanine board, LDO

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 заключается в разработке алгоритма, который позволит управлять амплитудно-фазовым распределением тока в антенных элементах АФАР таким образом, чтобы создавать несколько максимумов в диаграмме направленности в углах, соответствующих углам прихода полезных сигналов. Для достижения этой цели используется алгоритм оптимизации роя частиц с дополнительными ограничения на отношение сигнал/помеха.

Программа разработана с использованием языка программирования *Python* и включает в себя существующие библиотеки оптимизации. Процесс разработки программы включает в себя следующие этапы:

1. Создание модели диаграммы направленности для неадаптивной семиэлементной антенной решетки.
2. Реализация кода для определения оптимального вектора весовых коэффициентов для двух известных углов прихода помехи и сигнала.
3. Расширение модели для адаптивной антенной решетки путем внедрения отлаженного алгоритма оптимизации и учета дополнительного угла прихода сигнала.

Программа была проверена для разных углов прихода сигнала и помехи. Полученные результаты включают графические представления и значения отношения сигнал/помеха, которые были сравнены между диаграммой направленности адаптивной антенны и исходной диаграммой. Результаты анализа представлены на рисунках. На рис. 1 показана ДН семиэлементной антенной решетки.

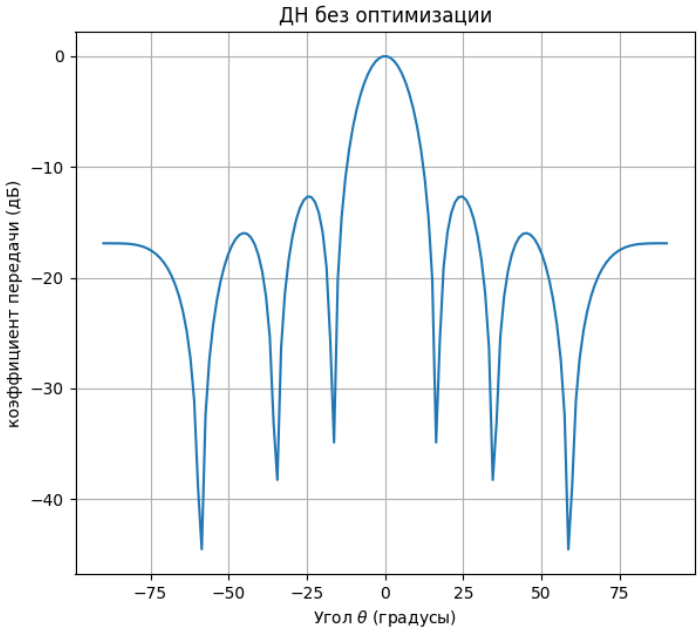


Рис. 2 стандартная ДН

На рис. 2 представлены оптимизированные ДН при заданных углах прихода сигнала (Θ_{s1}, Θ_{s2}) и помехи Θ_p, и требуемом отношении сигнал-помеха равным 6дб.

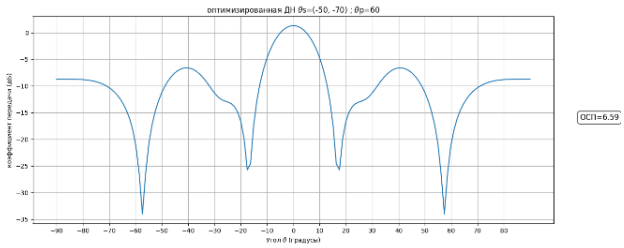


Рис. 3. (а)

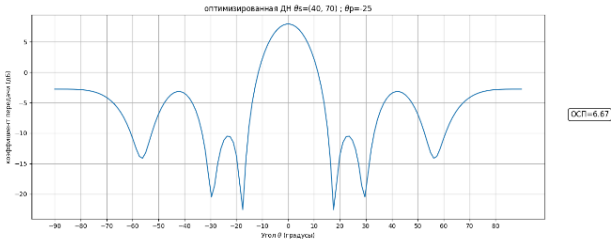


Рис. 4. (б)

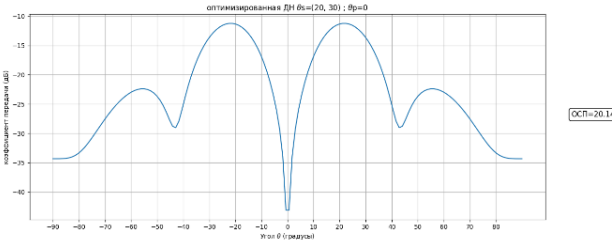


Рис. 5. (в)

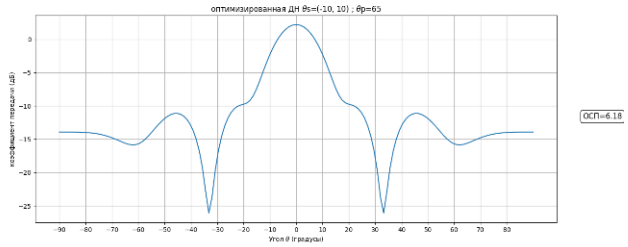


Рис. 6. (г)

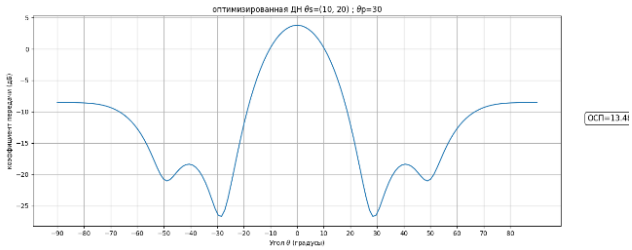


Рис. 7. (д)

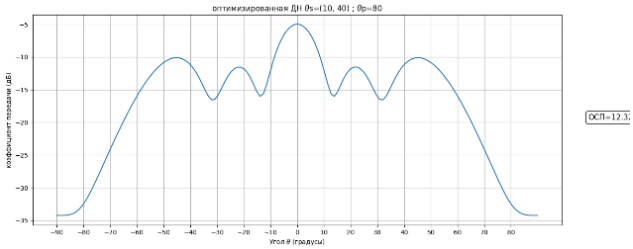


Рис. 8. (е)

(а) - Θ_{s1}=-50, Θ_{s2}=-70, Θ_p=60; (б) - Θ_{s1}=-40, Θ_{s2}=70, Θ_p=-25; (в) - Θ_{s1}=20, Θ_{s2}=30, Θ_p=0; (г) - Θ_{s1}=-10, Θ_{s2}=10, Θ_p=65; (д) - Θ_{s1}=10, Θ_{s2}=20, Θ_p=30; (е) - Θ_{s1}=10, Θ_{s2}=40, Θ_p=80;

Вывод: Представленный алгоритм адаптивного управления амплитудно-фазовым распределением тока в антенных элементах АФАР, основанный на методе оптимизации роя частиц, успешно позволяет достигать желаемых значений отношения сигнал/помеха. Программа может предоставить оптимальные векторы весовых коэффициентов как для приемных, так и для передающих антенных решеток на основе принципа взаимности.

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 : учеб. пособие. М. : Высшее образование, 2009.

Lavrov M.

The Bonch-Bruevich 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 cannel parameters, python.

УДК 629.783
ГРНТИ 89.29.55

ПРИМЕНЕНИЕ АЛГОРИТМОВ ФОРМИРОВАНИЯ ЛУЧА ДЛЯ АДАПТАЦИИ ДИАГРАММООБРАЗОВАНИЯ В СПУТНИКОВЫХ КООПЕРАТИВНЫХ СИСТЕМАХ

А. Н. Ликонцев, Д. А. Нев
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются возможные пути решения проблем, возникающих при использовании спутниковых систем и предлагается применение алгоритмов определения угла прихода сигнала для адаптивного управления диаграммой направленности. В качестве метод формирования луча используется Beamscan. Рассмотрена теоретическая возможность его использования. Результатом работы является ответ на вопрос целесообразности применения алгоритма в спутниковых системах.

спутниковые системы, формирование луча, адаптивное диаграммообразование

Спутниковые системы являются неотъемлемой частью нашей современной жизни. Они играют ключевую роль в таких сферах, как связь, навигация и метеорология. В телекоммуникационной отрасли спутниковые кооперативные системы обеспечивают связь на большие расстояния и в труднодоступных местах.

Однако, с ростом количества спутниковых систем и увеличением потока информации, возникают проблемы с обеспечением высокоскоростной связи. Одним из способов решения этой проблемы может стать применение алгоритмов определения угла прихода сигнала для адаптивной диаграммы направленности. В статье рассматривается возможность использования и реализации данного метода, его достоинства и недостатки.

Данные методы позволяют увеличить разрешение стандартных диаграмм направленности, что существенно улучшает качество сигнала и повышает пропускную способность системы. Основная идея заключается в использовании вместо одной антенны, группы антенн, работающей в режиме координации. Каждая такая антенна имеет свою диаграмму направленности, и путем комбинирования данных от всех антенн получается более точная диаграмма направленности по сравнению с использованием отдельной антенны. Перед алгоритмами поставлена задача определения угла прихода сигнала — угла между направлением, из которого приходит сигнал, и направлением на приемник. Он является обязательным параметром для определения местоположения и направления сигнала источника движения [1]. В спутниковых кооперативных системах прием сигнала можно определить с помощью антенн, установленных на спутниках. Однако, точность определения угла входного сигнала может быть ограничена различными факторами, такими как шум и ограничения на размеры антенн.

В дальнейших исследованиях в качестве алгоритма разрешения сигналов будет использоваться стандартный метод формирования луча (метод *Beamscan*) – метод обработки с вводом относительных временных задержек и суммированием – метод Бартлетта.

Его суть заключается в сканировании лучом интересующей области и вычислении выходной мощности для каждого угла сканирования луча [2]. Он идентифицирует максимумы как оценки *Direction of Arrival* (DOA). С увеличением угла обзора θ рассчитывается вектор отклика антенной решетки $a(\theta)$, и отдаваемая мощность формирователя диаграммы направленности антенны измеряется по формуле:

$$P_{CBF}(\theta) = \frac{\overrightarrow{a(\theta)}^H R_{xx} \overrightarrow{a(\theta)}}{\overrightarrow{a^H(\theta)} * \overrightarrow{a(\theta)}}, \quad (1)$$

где R_{xx} – автоковариационная матрица принятого сигнала, H – Эрмитово сопряжение, а $\overrightarrow{a(\theta)}$ – вектор отклика антенной решетки.

Т.к. $P_{CBF}(\theta)$ - пространственный спектр, то оценкой алгоритма является угол θ, который соответствует максимальному значению спектра выходной мощности.

Существенным преимуществом алгоритма является относительно простая вычислительная сложность. Однако, одним из слабых мест алгоритма *Beamscan* является неспособность распознавать близко расположенные источники. То есть, когда два сигнала поступают из направлений, разделенных расстоянием, меньшим ширины луча, *Beamscan* не определяет направления сигналов. Следовательно, выбор метода оценки DOA зависит от конкретных прикладных требований и количества источников. При применении *Beamscan* в спутниковой системе невозможность различения близко расположенных сигналов не является существенным недостатком, т.к. оценка угла будет проводиться на абонентском терминале, а расстояние между космическими аппаратами достаточно большое.

В случае, когда абонентская станция находится в зоне обслуживания 2х или более спутников, выбор обслуживающего будет производиться путем сравнения уровней сигнала, если уровни одинаковые, (рис. 1), сравниваться будет качество сигнала.

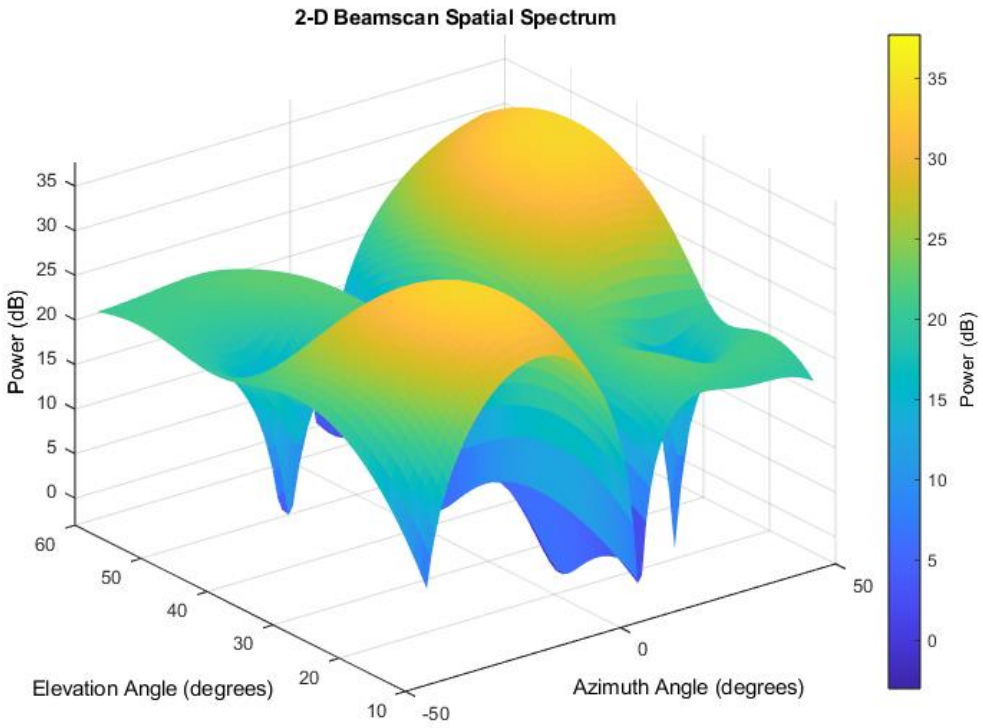


Рис. 1. Пример пространственного спектра алгоритма *Beamscan* для 2х источников сигнала с одинаковым уровнем

Адаптивное диаграммообразование позволяет управлять направленностью антенны в зависимости от угла прихода сигнала. Он основан на использовании массивных антенн, которые могут иметь различные отклонения входящего сигнала. Когда сигнал поступает на массивные антенны, каждая антенна принимает сигнал с различной фазой и амплитудой. Используя эту информацию, можно создать диаграмму направленности, которая направляет сигналы, исходящие из определенных направлений, и запрещает сигналы, исходящие из других направлений. Пример использования адаптивном диаграммы направленности представлен на рис. 2.

Применение алгоритмов для адаптивных диаграмм направленности в спутниковых системах имеет ряд преимуществ.

Во-первых, это позволяет увеличить пропускную способность и скорость передачи данных. С помощью более точных диаграмм направленности можно более эффективно использовать доступные спутниковые ресурсы, что особенно важно в условиях повышенного спроса на широкополосную связь.

Во-вторых, *Beamscan* позволяет снизить помехи и искажения сигнала. Благодаря более узким диаграммам направленности, сигнал можно лучше сфокусировать на определенных участках пространства и минимизировать влияние внешних источников помех.

Кроме того, применение алгоритмов позволяет повысить надежность и устойчивость спутниковой системы. В случае, когда одна из антенн выходит

из строя, остальные антенны могут компенсировать этот сбой и продолжить работу системы без перебоев.

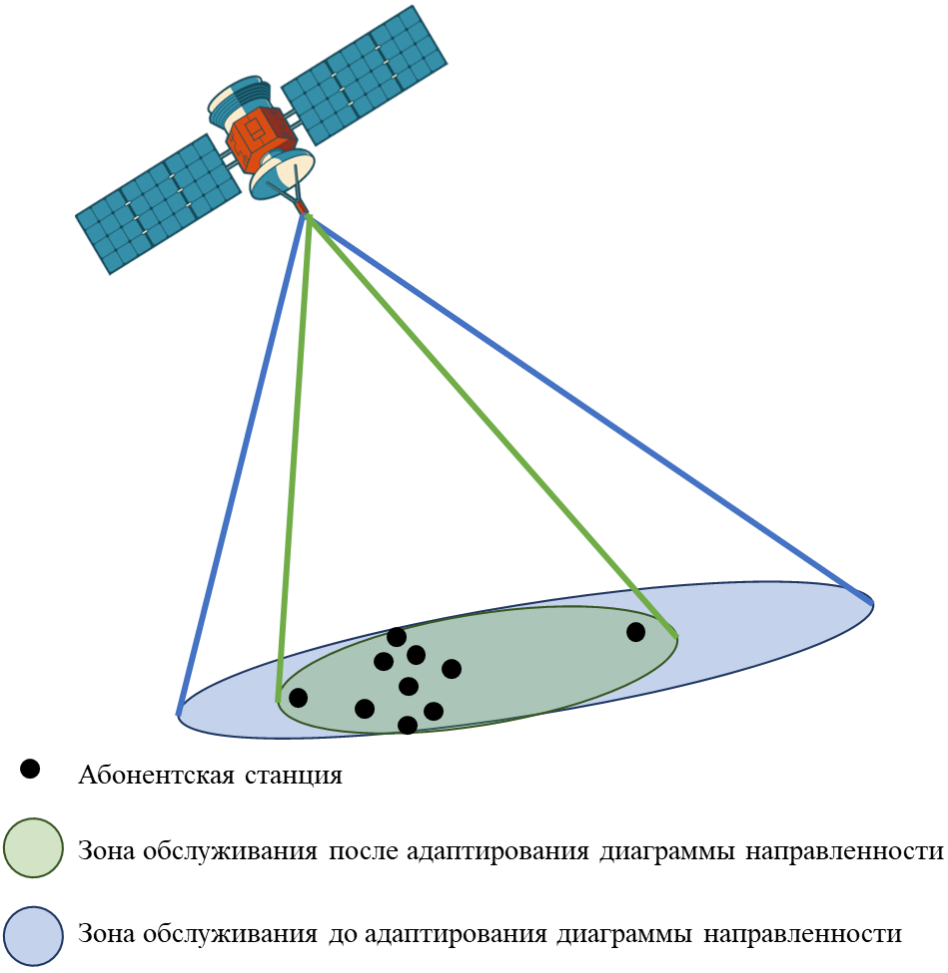


Рис. 2. Сравнение зон обслуживания спутника до и после адаптирования диаграммы направленности

Однако, применение алгоритма адаптивного формирования луча в системах спутниковых антенн связано с рядом проблем, включая:

1. Требование очень точного контроля уровня сигнала отдельных элементов, что требует продвинутых алгоритмов и вычислительной мощности, что трудно достичь в космосе;
2. Сложности в стабилизации лучей спутниковой системе;
3. Необходимость выбора конфигурации, состава и алгоритма управления адаптивной цифровой антенной решетки [3][4].

Несмотря на это, использование алгоритмов формирования луча для адаптивных диаграмм направленности в спутниковых системах может стать эффективным способом улучшения качества и производительности системы. Они позволят увеличить пропускную способность, снизить помехи и повысить надежность спутниковой связи. Внедрение этих алгоритмов может быть полезно как в спутниковых системах, так и в области связи, навигации и радиоэлектронной борьбе (РЭБ). Дальнейшие исследования в этой области

могут привести к еще более эффективным и оптимизированным алгоритмам разрешения для адаптивных диаграмм направленности в спутниковых системах.

Применение алгоритмов формирования луча в спутниковых системах позволит увеличить энергетическую и спектральную эффективность, за счёт уменьшения зоны обслуживания в тех локациях, где абонентская нагрузка отсутствует. Также уменьшение зон обслуживания благоприятно скажется на шумовой обстановке снизив нагрузку с абонентских терминалов, работающих на других спутниковых системах.

Список используемых источников:

1. Петров В. П. Алгоритмы оценки пространственного спектра в адаптивных цифровых антенных решётках // Вестник СибГУТИ. 2014. N 4 (28). С. 60-70.

2. Bellofiore S. Smart Antenna Systems for mobile platforms. Arizona State University, 2002.

3. Новицкий Ю. Г. Расчет алгоритмов определения угла прихода спутникового сигнала для адаптивного управления диаграммой направленности // Радиотехника. 2009. Т. 64, N 2. С. 26-31.

4. Ширяев И. В. Адаптивное управление диаграммой направленности спутниковых систем связи с использованием алгоритма Beamscan // Информационные технологии и машиностроение. 2013. Т. 9. N 1. С. 51-56.

Likontsev A., Nev D.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Application of beamforming algorithms for the adaptation of diagraming in satellite cooperative systems.

The article discusses possible ways to solve problems that arise when using satellite systems and suggests the use of algorithms for determining the angle of arrival of a signal for adaptive control of the directional pattern. Beamscan is used as a beamforming method. The theoretical possibility of its use is considered. The result of the work is an answer to the question of the feasibility of using the algorithm in satellite systems.

Key words: satellite systems, beam formation, adaptive diagram formation.

УДК 004.932.4
ГРНТИ 47.51.39

РАЗРАБОТКА УНИВЕРСАЛЬНОГО МОДУЛЯ ГАММА-КОРРЕКЦИИ НА ПЛИС

А. В. Максимова, И. Н. Чернов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Одним из способов повышения визуального качества изображений является гамма-коррекция. В работе рассматривается создание гамма-корректора неравномерно освещенных изображений на ПЛИС, написанного на языке SystemVerilog. Универсальность модуля позволяет использовать его в различных разработках без привязки к конкретным производителям ПЛИС.

гамма-коррекция, степенные преобразования, яркость, ПЛИС, SystemVerilog

Большую часть информации люди получают через зрительные образы. Достаточно часто изображения объектов, полученные в результате фотосъемки, не соответствуют той картине, которую видит человек. Причиной этому может быть плохое освещение или отсутствие настройки камеры. Задача улучшения изображения сводится к получению оптимальных яркости и контрастности.

Для решения этой задачи производится пространственная обработка, заключающаяся в том, что все операции выполняются непосредственно над значениями пикселей данного изображения. К наиболее используемым видам пространственной обработки для преобразования яркости изображений относятся степенные преобразования, называемые гамма-коррекцией.

Степенные преобразования имеют вид:

$$s = cr^{\gamma} \quad (1)$$

где r и s переменные, обозначающие значения яркостей входного и обработанного изображений соответственно.

При изменении параметра γ получим семейство кривых возможного преобразования, что видно на рис. 1.

При $\gamma < 1$ узкий диапазон малых входных значений преобразуется в широкий диапазон выходных значений, т.е. изображение становится темнее. При $\gamma > 1$ изображение осветляется.

Необходимость осветления или затемнения изображения определяется по среднему значению яркости всех пикселей.

Если пиксели изображения масштабируются в диапазоне 0..255:

$$\gamma = \frac{\log 128}{\log mean} \quad (2)$$

где $mean$ - среднее значение пикселей изображения. Если они масштабируются в диапазоне 0..1:

$$\gamma = \frac{\log 0{,}5}{\log mean} \quad (3)$$

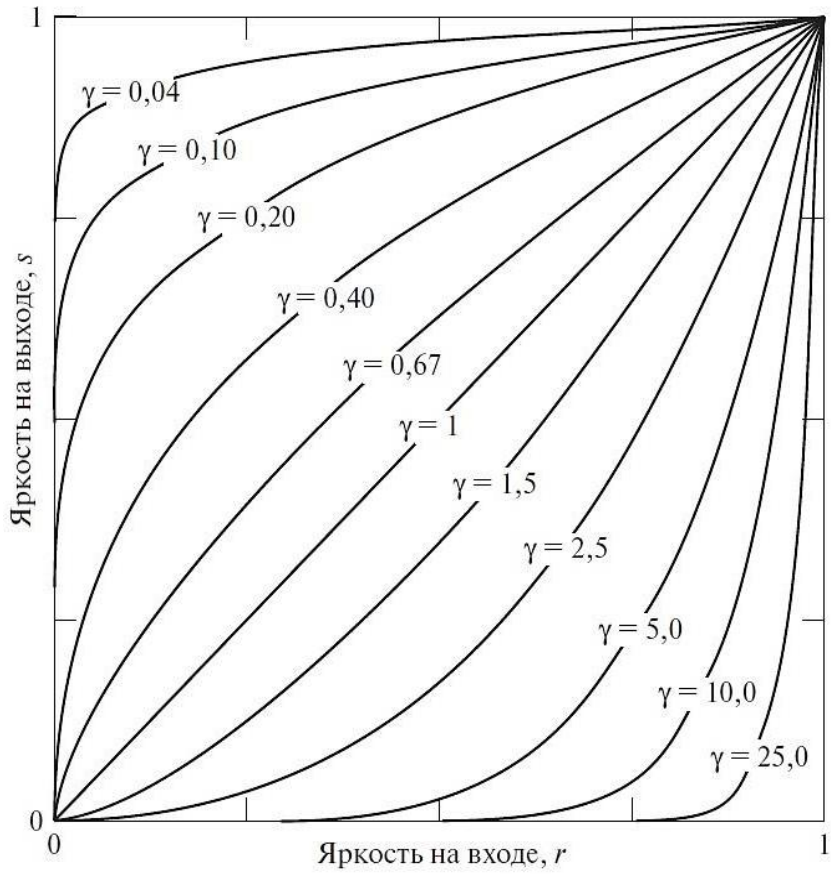


Рис. 1. Графики уравнения (1) для различных значений γ

Контрастность изображения определяется максимальным отношением яркостей:

$$k = \frac{Y_{max}}{Y_{min}}$$

где Y_{max} и Y_{min} – максимальное и минимальное значение яркости изображения соответственно.

Высококонтрастные изображения с точки зрения визуального восприятия выглядят лучше. Поэтому при обработке изображения необходимо учитывать этот параметр.

При анализе алгоритма гамма-коррекции, использующего для расчета коэффициента γ уравнение (2), в среде Matlab было определено, что уравнение не является оптимальным. Был сделан вывод, что (исходное изображение на рис. 2 является неравномерно освещенным. Несмотря на то, что человек находится в тени, большая часть изображения светлая за счет неба и водоема. Среднее значение яркости этого изображения превышает 128, и в соответствии с расчетом по формуле (2) γ < 1, изображение еще сильнее затемняется.

Для изображений, имеющих среднее значение яркости соответствующее визуальному восприятию (т.е. *mean* < 128 для темных изображений и *mean* >128 – для светлых), формула для расчета коэффициента γ является справедливой.

Одной из задач разработки универсального модуля гамма-коррекции на ПЛИС было обеспечить правильную гамма-коррекцию неравномерно освещенных изображений.

Рис. 2. Моделирование алгоритма гамма-коррекции в среде Matlab при расчете γ по формуле (2) (исходное и обработанное изображения)

Для решения этой задачи при помощи моделирования был экспериментально выведен следующий алгоритм. Показатель степени γ также зависит от среднего значения яркости изображения. Однако это среднее значение рассчитывается не как среднее арифметическое, а учитывает среднее значение всех темных и светлых пикселей. Деление на темные и светлые пиксели происходит путем сравнения значения яркости пикселя со средним значением всего диапазона, а именно со 128. По количеству темных и светлых пикселей определяется, является ли изображение условно темным или условно светлым. Результирующее среднее:

$$mean = \frac{\bar{Y}_{\text{светл.}} + \bar{Y}_{\text{темн.}}}{2}$$

Коэффициент γ рассчитывается как:

$$\gamma = \begin{cases} \dfrac{mean}{256}, \text{при условии что изображение темное } (N_{\text{светл.}} < N_{\text{темн.}}) \\ \dfrac{256}{mean}, \text{при условии что изображение светлое } (N_{\text{светл.}} > N_{\text{темн.}}) \end{cases} \quad (3)$$

На рис. 3 показаны результаты обработки уже представленного изображения по формуле (3). Можно заметить, что несущая основную информацию часть изображения (силуэт и лицо человека), после коррекции стала выглядеть лучше относительно рис. 2.

Рис. 3. Моделирование алгоритма гамма-коррекции в среде Matlab при расчете γ по формуле (3) (исходное и обработанное изображения)

Также важная задача разработки модуля заключается в адаптации алгоритма для ПЛИС. Расчет среднего значения яркости и степенной функции требуют больших вычислительных мощностей.

Рис. 4. Блок-схема разрабатываемого алгоритма

Основой разрабатываемого алгоритма гамма-коррекции, представленного блок-схемой на рисунке 4, является вычисление показателя

степени γ для конкретного кадра. Для этого используются блоки арифметических операций сложения и умножения. Для того чтобы избавиться от вычисления степени, составляются таблицы соответствия входных и выходных значений, в которых значение на выходе заранее просчитано с учетом значения γ. Данное решение позволит сократить количество необходимых операций и, соответственно, время, занимаемое на обработку видеоизображения. Коррекция видеоизображения происходит со второго кадра.

На данном этапе работы лишь обозначены основные ориентиры. Дальнейшая разработка предполагает написание модуля на языке *SystemVerilog*, тестирование и отладку проекта.

Список используемых источников:

1. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М. : Техносфера, 2012. 1104 с.

2. Фисенко В. Т., Фисенко, Т. Ю. Компьютерная обработка и распознавание изображений : учеб. пособие. СПб. : СПбГУ ИТМО, 2008. 192 с.

3. Щеглов Д. Ю. Исследование алгоритма «гамма-коррекции» для повышения визуального качества изображения // Теория и практика современной науки. 2017. N 7(25). С. 173-177.

Chernov I., Maksimova A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development of universal gamma correction module on FPGA.

One of the ways to improve visual quality of images is gamma correction. The paper deals with the creation of gamma-corrector of unevenly illuminated images on FPGA written in SystemVerilog language. The versatility of the module allows to use it in various developments without binding to specific FPGA manufacturers.

Key words: gamma correction, step transformations, brightness, FPGA, SystemVerilog.

УДК 004.932.4
ГРНТИ 47.14.03

РАЗРАБОТКА УНИВЕРСАЛЬНОГО МОДУЛЯ ОБРАБОТКИ ВИДЕОПОТОКА НА ПЛИС

В. В. Оноприенко, И. Н. Чернов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современных системах обработки видеопотока на ПЛИС используются различные алгоритмы: улучшения качества, повышения чёткости, резкости или размытие, также могут производится дополнительные преобразования с выделением контура. Эти алгоритмы могут быть реализованы с помощью матричных фильтров. В данной статье рассмотрена разработка универсального модуля обработки изображения для ПЛИС, с использованием интерфейса передачи видео Avalon – St, для настроек модуля используется интерфейс – AXI4 slave.

ПЛИС, Матричные фильтры, Свёртка, Avalon St, SystemVerilog, AXI4

Один из возможных вариантов обработки видеопотока матричные фильтры. Матричный фильтр – это фильтр обработки изображения, при котором каждый пиксель изображения рассматривается вместе с соседними. Фильтр применяется к пикселю и его окрестности путём операции дискретной свёртки [1]. Заданное ядро (матрица коэффициентов N*M) умножается на матрицу пикселей области изображения равную размеру ядра матрицы, результаты складываются. Матрица пикселей выделенной области изображения N*M сдвигается, повторяя описанное выше взвешенное суммирование при каждом сдвиге. Результатом является кадр с определённой коэффициентами ядра зависимостью пикселя от его окружения.

$$H(x,y) = \sum_{i=0}^{N_i-1} \sum_{j=0}^{M_j-1} I(x-i, y-j) f(i,j)$$

Где $H(x,y)$ – изображение после обработки
$I(x,y)$ – исходное изображение
$f(i,j)$ – Матрица коэффициентов

Матрица коэффициентов должна быть нормализована – сумма значений всех коэффициентов должна быть равна 1. Это требуется для предотвращения искажений цвета.

При реализации матричных фильтров возникает неопределённая ситуация, когда несколько элементов маски находятся вне изображения.

Существует несколько способов учесть это обстоятельство:

1. простейший способ состоит в ограничении перемещения центра окна по изображению, т. е. не выходить за края изображения. Но это уменьшит исходное изображение, что недопустимо для стандартного видеотракта;

2. расширить изображение путём добавления строк и столбцов с установленными заранее значениями;

3. расширить изображение симметрично границе, повторив строки и столбцы изображения.

Матричные фильтры универсальны, они могут использоваться для повышения резкости или чёткости, размытия или выделения контура изображения, в зависимости от используемой маски.

Рассмотрим примеры использования различных масок:

Простейший прямоугольный сглаживающий фильтр [2] радиуса r задаётся при помощи матрицы размера $(2\mathrm{r}+1) \times (2\mathrm{r}+1)$, все значения которой равны $\frac{1}{(2r+1)^2}$, а сумма значений равна единице. Пример маски фильтра 3×3:

$$M_1^{low} = \frac{1}{9}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Данный фильтр может быть применён для подавления шумов. При условии, что математическое ожидание шума равно нулю, шумы соседних пикселей при суммировании будут компенсировать друг друга. От выбора размеров матрицы будет зависеть соотношение между чёткость и шумоподавлением, при увеличении размеров окна будет происходить размытие мелких, но значимых деталей изображения. Для уменьшения размытия может использоваться фильтр меньшего размера или фильтры шумоподавления, имеющий повышенную значимостью обрабатываемого (центрального) пикселя:

$$M_2^{low} = \frac{1}{10}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

На рис. 1. Сравниваются исследуемые выше алгоритмы фильтрации.

Рис. 1. Изображение после фильтра размытия с матрицей 3x3 (левая картинка) и фильтра шумоподавления (правая картинка)

Если сглаживающие фильтры снижают общую контрастность изображения, размывая его, то фильтры, повышающие контрастность [2], производят обратный эффект и, по существу, являются фильтрами высоких пространственных частот. Например, коэффициенты повышающего контрастность фильтра равны:

$$M_1^{contr} = \begin{pmatrix} 0 & -1 & 0 \\ -1 & 5 & -1 \\ 0 & -1 & 0 \end{pmatrix} M_2^{contr} = \begin{pmatrix} -1 & -1 & -1 \\ -1 & 9 & -1 \\ -1 & -1 & -1 \end{pmatrix}$$

Пример фильтра M_2^{contr} в сравнение с оригинальной картинкой рассмотрен на рис. 2. Эффект повышения контраста достигается за счёт того, что фильтр подчёркивает разницу между интенсивностями соседних пикселей, удаляя эти интенсивности друг от друга. Этот эффект будет тем сильней, чем больше значение центрального коэффициента ядра. Минусом фильтрации данного типа являются заметные светлые и менее заметные тёмные ореолы вокруг границ.

Рис. 2. Оригинальное изображение (левая картинка) и изображение после фильтра повышения контрастности (правая картинка)

Разностные фильтры [2] – это линейные фильтры, задаваемые дискретными аппроксимациями дифференциальных операторов (по методу конечных разностей). Данные фильтры используются для задачи поиска границы на изображении.

Одним из самых простых дифференциальных операторов является взятие производной по x-координате $\frac{d}{dx}$, который определен для непрерывных функций. Распространёнными вариантами аналогичных операторов для дискретных изображений являются фильтры Прюита (Prewitt) и Собеля (Sobel):

$$M_1^{prewitt} = \begin{pmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{pmatrix} \quad M_1^{sobel} = \begin{pmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{pmatrix}$$

В отличие от сглаживающих и контрасто повышающих фильтров, не меняющих среднюю интенсивность изображения, в результате применения разностных операторов получается, как правило, изображение со средним значением пикселя близким к нулю. Вертикальным перепадам (границам) исходного изображения соответствуют пиксели с большими по модулю значениями на результирующем изображении. Поэтому разностные фильтры называют также фильтрами выделения границы объектов.

Аналогично вышеприведённым фильтрам, по методу конечных разностей можно составить фильтры для других дифференциальных операторов. В частности, важный для многих приложений дифференциальный оператор Лапласа (лапласиан) $\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$ можно приблизить для дискретных изображений фильтром с матрицей (один из возможных вариантов):

$$M_\Delta = \begin{pmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Примеры рассмотренных разностных фильтров приведены на рис. 3.

Рис. 3. изображение после фильтра оператора Собеля (правая картинка) и Лапласа (правая картинка)

Рассмотренные маски для исследуемых в данной статье фильтров могут использованы в разрабатываемом модуле обработки изображения для ПЛИС.

Разработка ведётся на HDL языке SystemVerilog, из-за его расширенных возможностей для моделирования. На рис. 4. показана схема разрабатываемого модуля для матрицы 3 на 3. Данные видео по интерфейсу avalon streaming sink [3] приходят на crs_av_st_input, где происходит декодирование контрольного пакета и изменение входной латентности из 1 в 0, после данные передаются в 2 универсальных fifo, глубиной в строку (crs_lib_fifo_sync) - (First in, First out) представляемое собой циклический буфер, где хранятся данные, которые были помещены в очередь. Данные с

crs_av_st_input и crs_lib_fifo_sync передаются в модуль, выполняющий свёртку Convolution matrix, из данного модуля данные переходят в crs_av_st_output, где происходит возращение контрольного пакета в поток и изменение латентности из 0 в 1. С помощью модуля SAXI4_cntrl по интерфейсу AXI4 [4] происходит перестройка коэффициентов ядра.

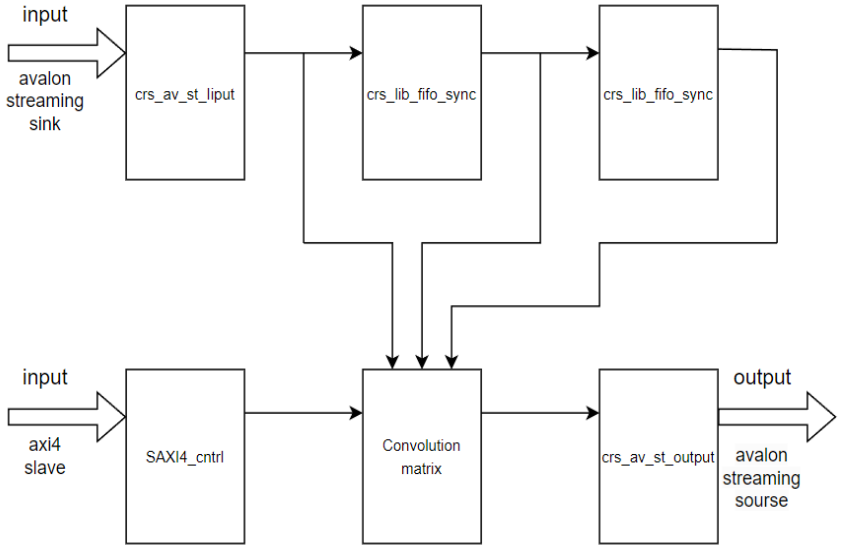


Рис. 4. RTL разрабатываемого модуля

В дальнейшем функционал модуля будет дополнен: возможностью параллельной передачи пикселей по интерфейсу Avalon St и алгоритмом округления вычислений после свёртки.

Список используемых источников:

1. Напалков В. В. Уравнения свертки в многомерных пространствах. М. : Наука, 1982. 240 с.

2. Соловьев Н. А. Цифровая обработка информации в задачах и примерах : учеб. пособие / Н. А. Соловьев, Н. А.Тишина, Л. А. Юркевская. Оренбург : ОГУ, 2016. 122 с.

3. Video and Image Processing Suite User Guide. Intel, Ink. 2021.02.12

4. AMBA AXI Protocol Specification Version: 2.0 Specification 2003-2010

Onoprienko V., Chernov I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development of a universal video stream processing module on FPGA.

In modern video stream processing systems on FPGAs, various algorithms are used: improving quality, increasing clarity, sharpness or blurring, additional transformations with contour selection can also be performed. These algorithms can be implemented using matrix filters. This article discusses the development of a universal image processing module for FPGAs, using the Avalon – St video transmission interface, the AXI4 slave interface is used to configure the module.

Key words: **FPGA, *Matrix filter, Convolution, Avalon St, SystemVerilog, AXI4.***

УДК 004.921
ГРНТИ 47.14.03

РАЗРАБОТКА УНИВЕРСАЛЬНОГО ГЕНЕРАТОРА ТЕСТОВЫХ ИЗОБРАЖЕНИЙ НА ПРОГРАМИРУЕМОЙ ЛОГИЧЕСКОЙ ИНТЕГРАЛЬНОЙ СХЕМЕ

И. Н. Чернов, Ф. П. Швецов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

При разработке систем обработки видеоизображений требуется точная отладка и настройка параметров модуля, для этого используются заранее известные тестовые изображения. В настоящем докладе приведена работа по созданию модуля генератора различных тестовых изображений с использованием шины Avalon-ST и языка описания аппаратуры System Verilog для программируемой логической интегральной схемы.

ПЛИС, видеосигнал, System Verilog, Avalon-ST, Тестовые изображения

Модуль для генерации тестовых изображений представляет инструмент, который создает визуальные объекты с целью использования их для тестирования алгоритмов обработки изображений, компьютерного зрения или других задач, требующих искусственных данных.

В данной работе рассматривается создание модуля, способного генерировать различные сигналы видеоизображения с использованием шины Avalon-ST от фирмы Intel [1].

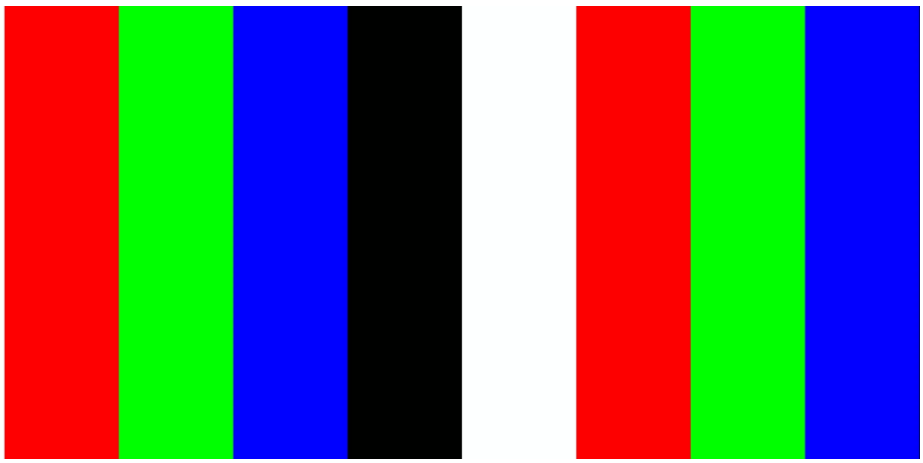


Рис. 1. Пример тестового изображения цветных полос

Тестовые изображения позволяют разработчику увидеть недостатки в исполнении алгоритмов на этапе отладки модуля или проверить монитор на корректность цветопередачи. На рис. 1 представлено изображение, которое позволяет определить искажает ли алгоритм обработки цветопередачу сигнала, а также провести коррекцию монитора по цветовой гамме.

RGB сигнал состоит из трех составляющих, красного, зеленого и синего, каждая из трех составляющих имеет яркость в диапазоне 0-255, таким образом, путем вычета или прибавлении к каждой составляющей некоторой

константы можно получить плавный переход из одного цвета в другой, как это продемонстрировано на рис. 2.

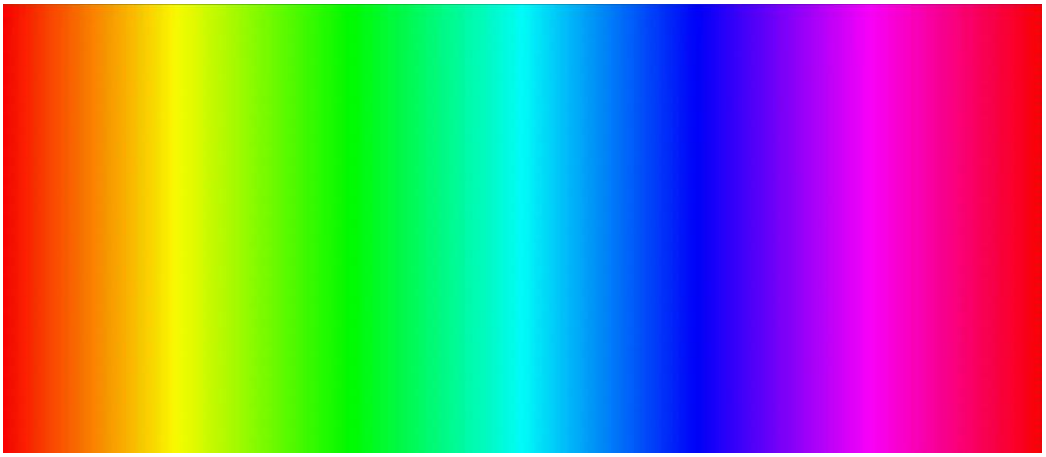


Рис. 2. Пример тестового изображения “Градиент”

Градиент, представленный на рис. 2, позволяет определить корректность цветопередачи, а также увидеть отдельные пиксели, выбивающиеся из общей цветовой гаммы.

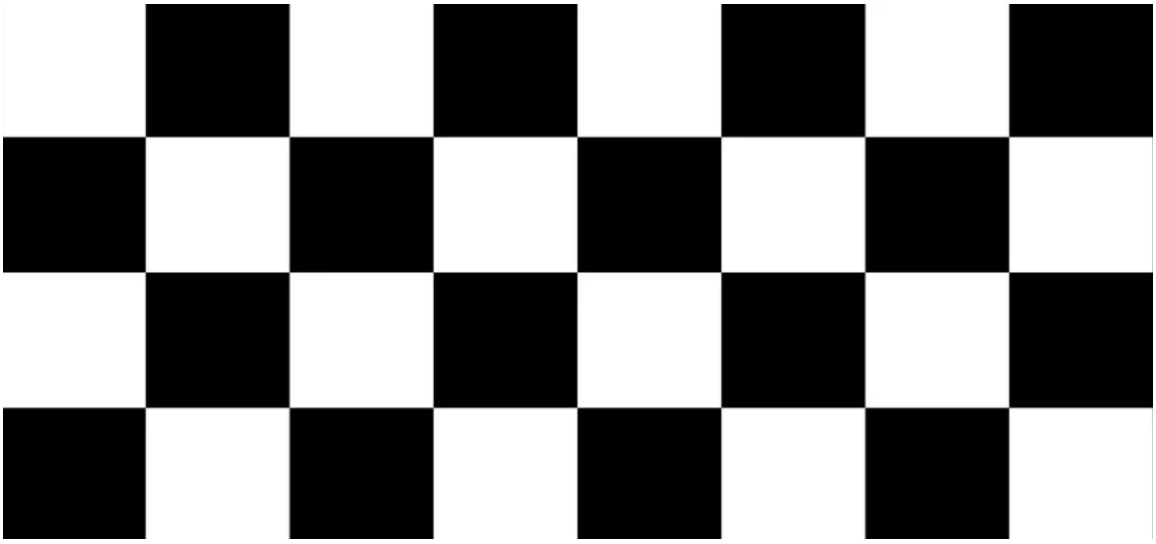


Рис. 3. Пример тестового изображения “Шахматная доска”

Подавая на тестируемый модуль изображение на рис. 3, можно увидеть искажения в виде шумов на стыках черных и белых квадратов.

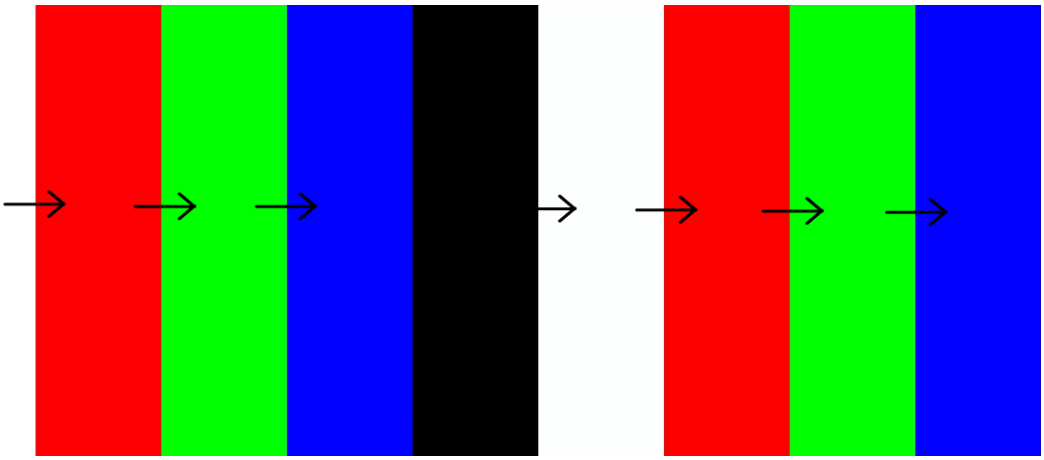


Рис. 4. Тестовое видеоизображение цветных полос со сдвигом

Видеоизображение на рис. 4, имеет известную частоту смены кадров и используется для тестирования алгоритмов, с целью обнаружение нежелательной потери кадров.

Приведённые изображения на рисунках 1,2 и 4 также могут быть представлены в черно-белом формате [2].

Использование тестовых изображение позволяет значительно ускорить процесс отладки и настройки алгоритмов видеообработки или машинного зрения, за счет визуализации заранее известных входных данных и зрительного определения несоответствий с поставленной задачей.

Разрабатываемый модуль приведенный на рис. 5, предназначен для генерации сигналов тестовых изображений в формате Avalon-ST на ПЛИС с использованием языка проектирования System Verilog. Использование этого модуля позволяет отказаться от платных аналогов, требующих лицензию Intel и не имеющих такой функционал выбора изображений.

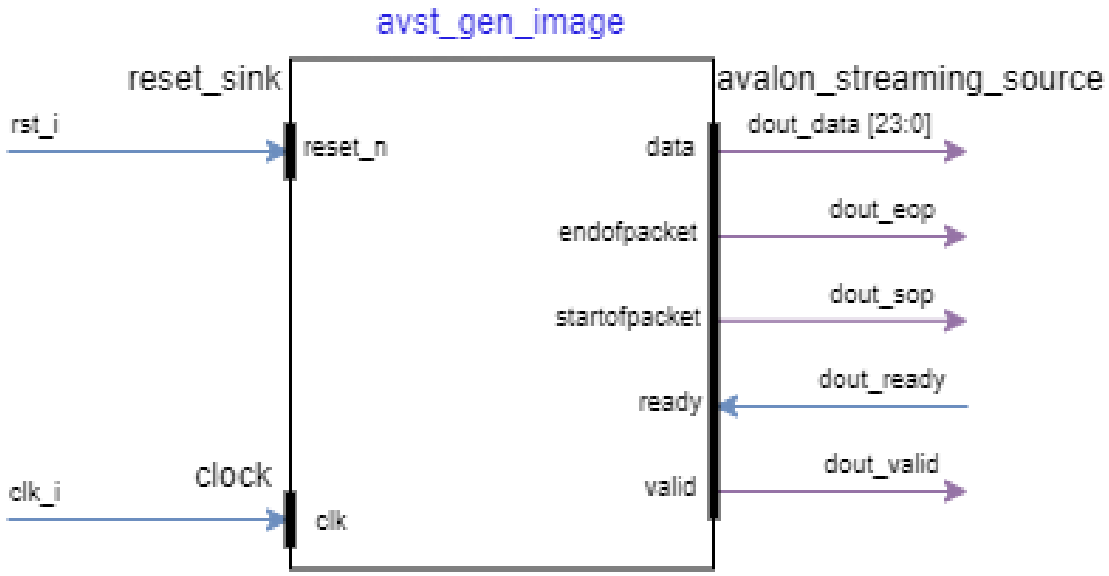


Рис. 5. Разрабатываемый модуль с сигналами Avalon-ST

Разработка модуля состоит из следующих этапов:

- Изучение разновидностей тестовых изображений и выбор самых эффективных;
- Рассмотрение существующих модулей генерации тестовых сигналов;
- Разработка модуля на языке System Verilog для ПЛИС;
- Написание testbench для проверки корректности работы модуля, отладка общих и критических ситуаций;
- Проверка модуля с использованием монитора и отладочной платы и конечная отладка

Использование современного языка описания аппаратуры позволяет использовать различные тестовые конструкции, облегчающие моделирование и отладку работы модуля.

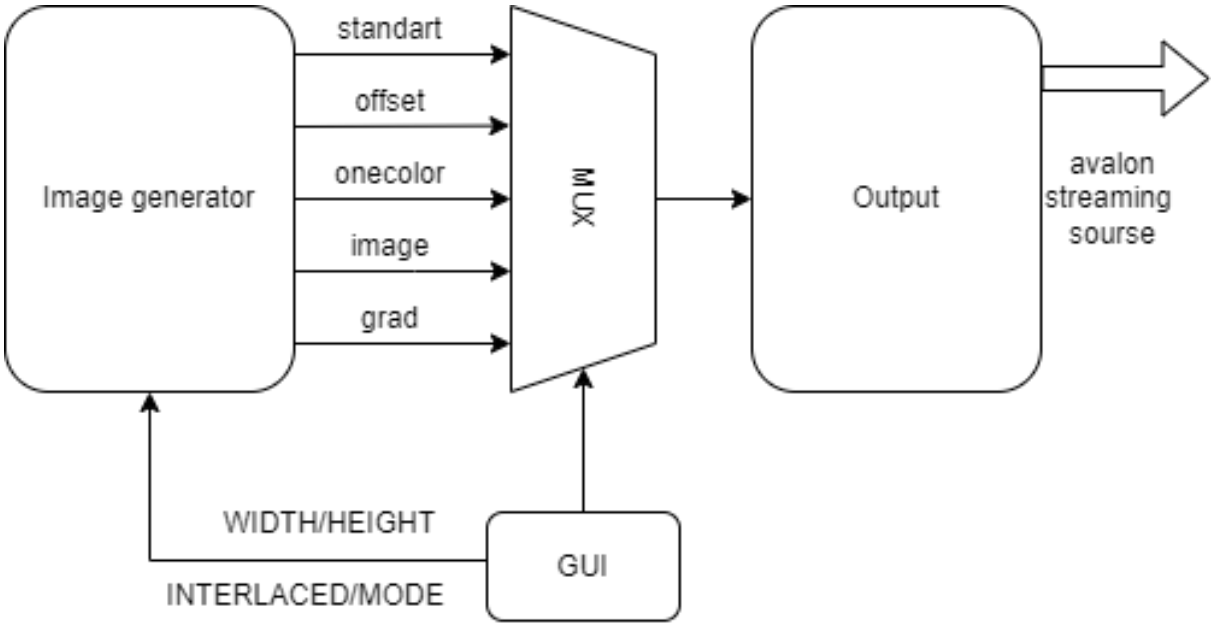


Рис. 6. Функциональная схема разработанного модуля

Разработанный модуль является универсальным за счет своей архитектуры, которая исключает использование IP блоков других производителей ПЛИС, что позволяет применять его в платах различных производителей. Важным фактом является наличие параметризации модуля, которая позволяет менять разрешение выходных данных, режим тестового изображения, а также изменять сигнал из цветного пространства в черно-белое. Для этого не требуется менять код, достаточно изменить параметры в графическом интерфейсе САПР, как показано на рис. 6, через которую будет производится сборка проекта.

В ходе разработки модуля было получено пять различных типов изображений:

- Цветные полосы
- Цветные полосы со сдвигом
- Градиент

- “Шахматная доска”
- Одноцветное изображение

Пользователем может быть изменен режим работы модуля, таким образом изображение на выход будут поступать только черно-белые.

Таким образом, при дальнейшем развитии будет сделано управление модулем за счет протокола Avalon-MM, это позволит менять изображение мгновенно, а не за счет перекомпиляции проекта.

Список используемых источников:

1. Video and Image Processing Suite User Guide. Intel, Ink. 2021.02.12
2. Цифровая фотография и калибровка [Электронный ресурс]. URL: http://www.colordigits.ru/testimg.htm. (дата обращения: 10.11.2023).

Chernov I., Shvetsov F.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development of a universal generator of test images on a programmable logic integrated circuit.

When developing video image processing systems, precise debugging and adjustment of module parameters are required, for this purpose, pre-known test images are used. This report describes the work on creating a module for generating various test images in the Avalon-ST standard using the System Verilog hardware description language for a programmable logic integrated circuit.

Key words: FPGA, Video signal, SystemVerilog, Avalon-ST, Test images.

Секция 2.6.
Экология формирования информационного пространства

УДК 621.317.421
ГРНТИ 87.15.03

ИЗМЕРЕНИЕ ЭЛЕКТРОМАГНИТНЫХ ПОЛЕЙ ПРОМЫШЛЕННОЙ ЧАСТОТЫ В ГОРОДЕ РЖЕВ ТВЕРСКОЙ ОБЛАСТИ

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

Электромагнитное поле является постоянным фоновым излучением всей планеты Земля. От уровня излучения зависит самочувствие всех живых организмов. В данной публикации рассматривается уровень электромагнитного излучения города Ржева.

электромагнитный фон, излучение, магнитная индукция, напряжение

Все живые существа, в том числе и человек находятся в зоне непрерывного воздействия электромагнитного поля Земли. Это воздействие является фоновым, оно не оказывает негативного воздействия на здоровье живых организмов, а его уровень считается нормальным.[1] Но человеческие технологии тоже могут либо создавать электромагнитное излучение, либо его изолировать.

Пространства современных населенных территорий пронизаны электромагнитными излучениями разных диапазонов, вызванными работой технических средств и устройств. Концентрация электромагнетизма в окружающей среде постоянно увеличивается, принимая вид общего электромагнитного загрязнения. Всемирная Организация здравоохранения (ВОЗ) в 1995 году ввела термин «глобальное электромагнитное загрязнение окружающей среды», а затем включила эту проблему в перечень приоритетных для человечества. [2]

Влияние на организм человека электромагнитных полей (ЭМП) определенной силы нельзя отрицать и этому посвящено много исследований. Ведь и в самом человеке заложены принципы функционирования органов и систем, основанные на электрических явлениях. Головной мозг, центральная и периферическая нервная система – вот первые объекты, которые могут подвергнуться воздействию внешних полей, не говоря о нежелательных эффектах в других частях организма и об изменениях, происходящих на клеточном уровне. Как установили специалисты в области научной гигиены, электромагнитное поле достаточной интенсивности может изменять картину высшей нервной деятельности человеческого мозга. Исследователи выявили отклонения в сигналах электроэнцефалограммы: десинхронизацию и изменение частоты основных ритмов. [3]

Электромагнитное воздействие оказывает влияние не только на людей и другие живые организмы, но и на растительный мир. Известны факты, что растения, произрастающие вблизи высоковольтных подземных кабелей, испытывают дезориентацию в пространстве. Стволы деревьев не тянутся вверх, как это должно происходить с нормальными растениями, а изгибаются

в сторону и даже вниз причудливым образом. Также зафиксированы случаи, когда вблизи GSM базовых станций сотовой связи деревья сохнут, а мощные передатчики телекоммуникационной системы Wi-Fi подавляют рост и уничтожают растительность в зоне с радиусом 100–150 метров.[3]

Для прогнозирования уровня влияния на население электромагнитного излучения используются инструментальные методы измерения излучения и последующее картографирование территории, на которой проходили измерения.

Данная статья является изложением результатов инициативного исследования пространственного распределения электрических и магнитных полей промышленной частоты (50 гц) в г. Ржев.

Измерения электрического напряжения и магнитной индукции выполнялись при помощи прибора Gigahertz Solutions ME 3830 B M/E Analyser. Данный прибор позволяет измерять для промышленной частоты 50 гц напряженность электрического поля в диапазоне от 1 до 2000 в/м и интенсивность магнитных полей (магнитную индукцию) в пределах от 1 до 2000 нТл. Прибор имеет однокоординатный датчик магнитного поля, поэтому в каждой точке путем вращения прибора вокруг горизонтальной и вертикальной оси находилось положение, при котором ось датчика совпадала с ориентацией полного вектора магнитного поля, и величина магнитной индукции достигала максимума для данной точки. Измерения проводились на высоте 1,5 метра от поверхности земли.

Измерения были выполнены в августе 2023 г. более чем в 300 точках, расположенных в жилых кварталах, вдоль улиц и дорог, на территориях учебных заведений, больниц, в парках и т.д. Вблизи высоковольтных линий электропередачи измерения проводились в местах наибольшего провисания проводов. Территория исследования ограничивается: в северной части города: Ленинградским шоссе, Лесной улицей; в восточной: Свободным переулком; в южной части: Зубцовским шоссе, Вокзальной улицей, Привокзальной улицей; в западной части: Полевым переулком, улицей Тертия Филлипова.

Статистическая обработка результатов была проведена на основе общепринятых формул, с использованием программного продукта Excel.

Результаты и их интерпретация

Электрические поля

Напряжение в городе Ржев, согласно измерениям, не превышает предельно допустимого уровня (1000 в/м на территории зон жилой застройки согласно СанПиН 1.2.3685-21). Максимальный уровень напряжения равен 74 в/м на улице Калинина под линией электропередач, рядом с домом 11/22, уровень магнитной индукции равен 72 нТл. В большинстве точек значения не превышают 10 в/м.

Магнитные поля

Индукция магнитного поля на территории жилой застройки не должно превышать 10000 нТл согласно СанПиН 1.2.3685-21. Максимальный уровень

индукции 502 нТл на Трудовой улице рядом с домом 33/15, уровень напряжения в этой точке равен 2 в/м. В большинстве точек значения не превышают 100 нТл.

Заключение

В городе Ржев не замечено нарушений СанПиН 1.2.3685-21 по уровню напряжения и магнитной индукции. Также аномально высоких значений не обнаружено. Таким образом, можно сделать вывод о том, что в городе Ржев электромагнитная обстановка на территориях жилой застройки не превышает допустимых значений и не оказывает негативного влияния на население.

Список используемых источников:

1. Александров Ю. А., Остапенко А. А, Гентош А. В. Исследование уровня электромагнитных излучений от некоторых технических устройств // Вестник Приазовского государственного университета. 2014. N 28.

2. Слукин В. М. Техногенные электромагнитные излучения как фактор экологии населенных пространств // Академический вестник УралНИИпроект РААСН. 2010. N 4.

3. Макитрюк С. Б. Влияние электромагнитного излучения на организм человека // Молодежь, наука, космос : материалы студенческой научно-практич. конф. электроэнергетического факультета, Ставрополь, 11–14 апр. 2022 г. Ставрополь : Типография «АГРУС», 2022. С. 219-225. EDN LJMCGE.

4. Стурман В. И., Логиновская А. Н. Картографирование электромагнитных полей промышленной частоты // Вестник Удмуртского университета. 2019. N 4.

Belotserkovsky M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Measurement of electromagnetic fields of industrial frequency in the city of Rzhev, Tver region.

The electromagnetic field is the constant background radiation of the entire planet Earth. The well-being of all living organisms depends on the level of radiation. This publication examines the level of electromagnetic radiation of the city of Rzhev.

Key words: Electromagnetic background, radiation, magnetic induction, voltage.

УДК 504.4.054
ГРНТИ 34.47.51

ЭКОТОКСИКОЛОГИЧЕСКОЕ СОСТОЯНИЕ ПОВЕРХНОСТНЫХ ВОД РЕКИ ЧЕРНАЯ И КАРПОВКА

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

Экотоксикологическое состояние водных объектов оказывает значительное воздействие на здоровье биологических систем и качество водных ресурсов. В данной статье представлен анализ экотоксикологического состояния выбранных водных объектов в разные времена года с использованием методов биотестирования на пресноводных организмах.

Водные объекты, такие как реки, озёра и моря, являются важными компонентами нашей окружающей среды и играют решающую роль в поддержании биоразнообразия и обеспечении человеческих потребностей в воде. Однако современные экосистемы водных объектов подвергаются разнообразным антропогенным воздействиям, которые могут оказывать негативное воздействие на их экотоксикологическое состояние. [1,2]

Целью исследования является выявление сезонных изменений в экотоксикологическом состоянии водных объектов Санкт-Петербурга. Полученные результаты представляют интерес для понимания долгосрочных последствий экотоксикологических изменений в водных экосистемах и обеспечения их устойчивости.

Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации (тема № 122041100143-5).

Объекты и методы исследования

Река Карповка – один из рукавов Невы, разделяющий Петроградский и Аптекарский острова. Длина — 3 км, ширина — 20 метров. Свое начало река берет в Большой Невке, устье реки находится в Малой Невке.

Река Чёрная – приток Большой Невки. Длина реки составляет 8,1 км, ширина до 20 метров (в нижнем течении). Исток – пересечение Байконурской улицы и Богатырского проспекта, устье – Большая Невка.

Для оценки экотоксикологического состояния водных объектов, используются различные методы, включая биотестирование с использованием живых организмов. Один из распространенных методов – использование организмов, таких как дафнии, водоросли, и рыб, чтобы выявить токсичные воздействия водных сред. Эти организмы реагируют на наличие токсинов и загрязнителей, что позволяет оценить степень токсичности воды и определить уровень воздействия на экосистему. [2, 3]

Отбор проб проводился весной, летом и осенью, по межгосударственному стандарту 17.1.5.05-85 «Охрана природы. Гидросфера.

Общие требования к отбору проб поверхностных и морских вод, льда и атмосферных осадков». [4]

Анализ выполнялся по методике ФР.1.39.2015.19242 «Методика определения токсичности проб природных, питьевых, хозяйственно питьевых, хозяйственно-бытовых сточных, очищенных сточных, сточных, талых, технологических вод экспресс-методом с применением прибора серии «биотестер», с использованием одноклеточных пресноводных тест-объектов инфузорий - Paramecium caudatum. [5]

Полученные результаты

Органолептическое исследование проб не выявило сильных отклонений от нормы: все пробы воды слабомутные, имеют небольшой оттенок желтого. У всех проб, кроме весенних отсутствовал запах, у весенних образцов был слабый железистый запах.

При проведении лабораторных исследований были получены результаты, приведенные в таблицах 1-3.

ТАБЛИЦА. 1 – Показатели токсичности проб в весенний период

№ пробы	№ пов-ти	Показания прибора	Ср.знач. показаний	Индекс токсичности, Т	Ср.знач. Т	Группа токсичности
Контроль	1	165 197 177	174,0			
	2	174 158 171				
	3	177 180 167				
Черная речка (метро)	1	93 90 107	96,7	0,44	0,52	II
	2	75 78 76	76,3	0,56		
	3	73 75 84	77,3	0,56		
Карповка	1	98 77 94	89,7	0,48	0,47	II
		95 94 91	93,3	0,46		
		93 96 82	90,3	0,48		

ТАБЛИЦА. 2 – Показатели токсичности проб в летний период

№ пробы	№ пов-ти	Показания прибора	Ср.знач. показаний	Индекс токсичности, Т	Ср.знач. Т	Группа токсичности
Контроль	1	247 239 274	231,2			
	2	231 220 210				
	3	265 197 198				
Черная речка (метро)	1	152 127 123	134,0	0,42	0,41	II
	2	152 166 128	148,7	0,36		
	3	119 123 130	124,0	0,46		
Карповка	1	148 104 121	124,3	0,46	0,47	II

ТАБЛИЦА. 3 – Показатели токсичности проб в весенний период

№ пробы	№ пов-ти	Показания прибора	Ср.знач. показаний	Индекс токсичности, Т	Ср.знач. Т	Группа токсичности
Контроль	1	294 296 268	266,6			
	2	274 275 235				
	3	260 233 264				
Черная речка	1	375 329 354	352,7	-0,32	|0,35|	I
	2	380 389 319	362,7	-0,36		

(метро)	3	366 363 363	364,0	-0,37		
Карповка	1	337 306 319	320,7	-0,20	|0,26|	I
	2	302 339 385	342,0	-0,28		
	3	359 335 342	345,3	-0,30		

Анализ результатов биотестового анализа токсичности поверхностных вод рек Чёрная и Карповка с использованием одноклеточных позволил сделать следующие выводы:

1. В весенний период токсичность больше, чем в остальное время года. Скорее всего это связано с техногенными нагрузками от близлежащих объектов инфраструктуры, использованием реагентов на автомобильных дорогах, а также с выбросами от автотранспорта. [6]

2. Весенне-летного сезона достаточно для того, чтобы снизить показатели токсичности. Это заметно при сравнительной характеристике таблицы 1 и 3. Это может быть связано с биологической активностью экосистем, которые могут поглощать, перерабатывать и сорбировать загрязняющие вещества. [3]

3. Современное экотоксикологическое состояние поверхностных вод Санкт-Петербурга требует проведения регулярных наблюдений за изменением токсичности и инвентаризации источников загрязнения.

Список используемых источников:

1. Давыдов Л. К., Дмитриева А. А., Конкина Н. Г. Общая гидрология. Л. : Гидрометеоиздат, 1973. 463 с.

2. Фрумин Г. Т. Экологическая токсикология (экотоксикология). Курс лекций. СПб. : РГГМУ, 2013. 179 с.

3. Бакаева Е. Н., Тарадайко М. Н. Экотоксичность поверхностных вод бассейна реки Северский Донец (Ростовская область) по результатам набора биотестов [Электронный ресурс] // Известия вузов. Северо-Кавказский регион. Серия: Естественные науки. 2016. N 4 (192). URL: https://cyberleninka.ru/article/n/ekotoksichnost-poverhnostnyh-vod-basseyna-reki-severskiy-donets-rostovskaya-oblast-po-rezultatam-nabora-biotestov (дата обращения: 24.10.2023).

4. ГОСТ 17.1.5.05-85 «Охрана природы. Гидросфера. Общие требования к отбору проб поверхностных и морских вод, льда и атмосферных осадков».

5. ФР.1.39.2015.19242 «Методика определения токсичности проб природных, питьевых, хозяйственно питьевых, хозяйственно-бытовых сточных, очищенных сточных, сточных, талых, технологических вод экспресс-методом с применением прибора серии «биотестер».

6. Мостепан Е. В. Исследование влияния ливневых вод с автомобильных дорог с разной интенсивностью движения на загрязнение водных объектов // Вестник ХНАДУ. 2011. N 52.

Bober A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Ecotoxicological state of surface waters of the chernaya and karpovka rivers.

The ecotoxicological state of water bodies has a significant impact on the health of biological systems and the quality of water resources. This article presents an analysis of the ecotoxicological state of selected water bodies in different seasons using biotesting methods on freshwater organisms.

Key words: surface water, toxicology, test organisms, biotests.

УДК 504.06
ГРНТИ 87.53.13

ИССЛЕДОВАНИЕ ДЕГРАДАЦИИ НЕФТЕПРОДУКТОВ В ПОЧВЕННОМ ПРОФИЛЕ НА ПРИМЕРЕ ПОДЗОЛИСТЫХ И ДЕРНОВО-ПОДЗОЛИСТЫХ ПОЧВАХ ЛЕНИНГРАДСКОЙ ОБЛАСТИ

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

В настоящее время загрязнение почвы нефтепродуктами является одной из актуальных проблем, которая приводит к серьезным экологическим последствиям. Деградация нефтепродуктов в почвенном профиле является важным аспектом данной проблемы. Зная как почвы определенных типов взаимодействуют с загрязнением углеводородами, можно создать точечные стратегии по сохранению экосистем.

Без использования углеводородов, таких как нефть, трудно представить, как бы функционировало общество сегодня. Нефть необычна тем, что она используется для создания множества полезных продуктов, включая пластмассы, бытовую химию и косметику, текстиль и продукты питания. Ошибочно мнение, что нефть используется исключительно для производства топлива. Фармацевтические препараты, включая антибиотики, антисептики и седативные средства, создаются на основе фенола, содержащегося в нефти. [1]

Целью работы является получение информации об деградации нефтепродуктов в различных типах почв, в естественных условиях и ее остаточная концентрация

Объекты и методы исследования

В данной работе для эксперимента были взяты образцы почв многолетних опытов, расположенных на территории Ленинградской области. Почвы различались по типу биогеоценоза, в котором они сформировались, и по гранулометрическому составу.

Участок 1 сосняк лишайниково-зеленомошный на подзоле иллювиально-железистом песчаном, территория учебной базы СПбГАУ, д.Гобжицы, Лужского р-на, Ленинградской обл.

Участок 2 разнотравно-злаковая залежь на дерново-подзолистой суглинистой почве, опытное поле СПбГАУ, г. Пушкин

Почва № 1 – подзолистая, песчаная.

Почва № 2 – дерново-подзолистая, суглинистая.

Почвы с поверхности были загрязнены нефтью в дозах 10 л/м2. Исходный уровень содержания нефтепродуктов был примерно одинаков и составил для дерново-подзолистой почвы 30500 мг/кг (3,05% от массы почвы), для подзолистой почвы 32000 мг/кг (3,20%). Опыт по загрязнению почв нефтью был заложен в 2004 г.

Осенью 2023 г. были выкопаны траншеи глубиной 60 см и длиной 100 м для проведения исследований по изучению процессов миграции нефти по

профилю почв. Почвенные образцы отбирали послойно с глубин: 0(6)-10 см, 10-20 см, 20-30 см, 30-40 см, 40-50 см, 50-60 см.

Отбор проб проходил ГОСТ 17.4.4.02-2017 "Межгосударственный стандарт. Охрана природы. Почвы. Методы отбора и подготовки проб для химического, бактериологического, гельминтологического анализа". [2]

Подготовка проб и измерения проводились с требованиями ПНД Ф 16.1:2.2.22-98 «методика выполнения измерений массовой доли нефтепродуктов в минеральных, органогенных, органо-минеральных почвах и донных отложениях методом ик-спектрометрии». Методика была выбрана как самая популярная среди подобных исследований. [3,4,5,6]

Полученные результаты

При органолептическом исследовании проб, были сделаны следующие выводы:

1. В почвенном разрезе дерново-подзолистой почвы не было заметно нефтяных “языков”, только небольшие органические вкрапления, которые не факт, что следы углеводорода, а не остатков органики. Характерный запах нефти и ее частицы, начали встречаться на глубине 10-20 см.

2. В песчаном подзоле на пробах с слоев 30-40 см появлялись предположения о наличии больших доз нефтепродукта. У данных проб был характерный запах нефти, частички почвы были окрашены в черный смолистый цвет.

Данные полученные при проведении измерений приведены в таблице 1.

ТАБЛИЦА 1. Концентрации нефтепродуктов в почвенном профиле

Дерново-подзолистая			Песчаный подзол		
Профиль	Глубина, см	Концентрация, мг/кг	Профиль	Глубина, см	Концентрация
AY	0-10	2730+-599	E	6-10	10645+-1072
	10-20	210+-49	BF	10-20	5900+-1597
BI	20-30	109+35		20-30	5179+-3907
	30-40	117+-22	BC	30-40	2286+-2152
	40-50	56+-4		40-50	102+-18
	50-60	78+-12		50-60	120+-6

Учитывая первоначальные данные по привнесенным нефтепродуктам 30500 мг/кг для дерново-подзолистой почвы и 32000 мг/кг для песчаного подзола, можно рассчитать примерный процент остаточного содержания нефтепродуктов за 19 лет.

Исходный уровень содержания нефтепродуктов был примерно одинаков и составил:

Для дерново-подзолисто почвы 30500 мг/кг

Для подзолистой почвы 32000 мг/кг

Процент остаточного содержания = (Остаточное значение / Исходное значение) * 100

Для дерново-подзолистой почвы: Процент остаточного содержания = (2940 / 30500) * 100 ≈ 9%

Для песчаного подзола: Процент остаточного содержания = (24010 / 32000) * 100 ≈ 75%

При расчете остаточного значения в дерново-подзолистой почве, в учет шли только показатели глубины до 20 см. Связано это с тем, что показатели глубже 20 см немного отличаются по фоновым значениям. Для этой почвы фоновые значения могут находится в промежутке от 100 до 200 мг/кг. [4,5,7]

На основе данных из таблицы 1, были построены графики (Рис.1), которые отражают уменьшение концентрации нефтепродуктов с глубиной отбора проб в разных типах почвы.

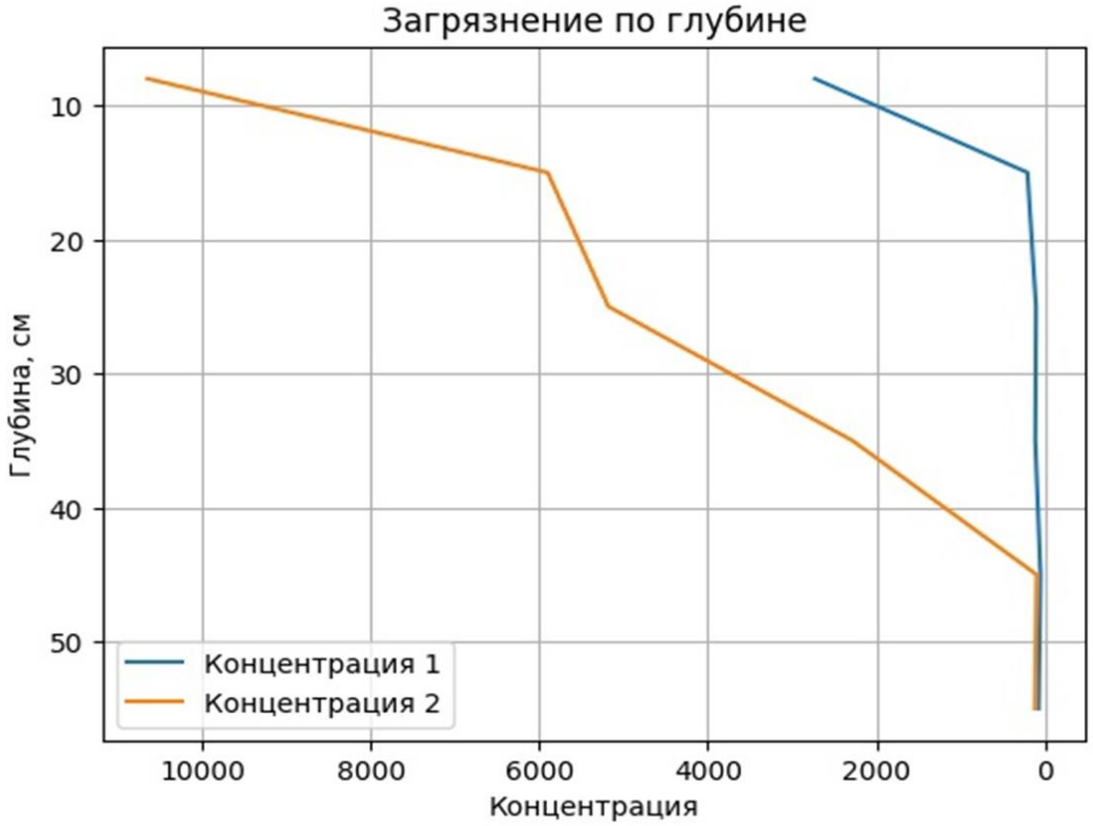


Рис. 1. График сравнение профиля миграции нефтепродуктов в песчано-подзолистой (концентрация 1) и дерново-подзолистой (концентрация 2) почве

Исходя из полученных данных, можно сделать следующие выводы:

Результаты проведенного определения содержания нефтепродуктов в почвенном профиле показывают, что при исходном уровне загрязнения почв нефтепродуктами от 30500 до 32000 мг/кг для дерново-подзолистой почвы их

остаточное содержание за 18 лет не превышало 9% от исходного уровня, а для песчано-подзолистой составило около 75%, соответственно.

В результате выполненных работ были получены данные по деградации нефтепродуктов и их остаточная концентрация на многолетних опытах. При этом установлено, что для песчано-подзолистой почвы уровень загрязнения остается высоким до глубин 30-40 см, в то время как дерново-подзолистая почва за счет своей биологической активности смогла эффективно и достаточно полно переработать нефть и большую часть продуктов ее трансформации. Остаточные концентрации нефтепродуктов в ней оказались на уровне фоновых значений.

Список используемых источников:

1. Зайлалова В. Р. Химия нефти и газа : учеб. пособие. Уфа : Уфимский государственный нефтяной технический университет. 2014.

2. ГОСТ 17.4.4.02-2017 «Межгосударственный стандарт. Охрана природы. Почвы. Методы отбора и подготовки проб для химического, бактериологического, гельминтологического анализа».

3. ПНД Ф 16.1:2.2.22-98 «методика выполнения измерений массовой доли нефтепродуктов в минеральных, органогенных, органо-минеральных почвах и донных отложениях методом ик-спектрометрии».

4. Околелова А. А., Капля В. Н., Лапченков А. Г. Оценка содержания нефтепродуктов в почвах // Региональные геосистемы. 2019. №1. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/otsenka-soderzhaniya-nefteproduktov-v-pochvah (дата обращения: 23.10.2023).

5. Маячкина Н. В., Чугунова М. В. Особенности биотестирования почв с целью их экотоксикологической оценки // Вестник Нижегородского университета им. Н.И. Лобачевского. 2009. N 1.

6. Тудакова А. А. Миграция нефти и нефтепродуктов в почвенном профиле // Студенческий. 2022. N 22-7(192). С. 14-16. EDN TZFWQK.

7. Почвоведение. Почва и почвообразование : учебник. М. : Высш. шк., 1988. 400 с.

Bober A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Study of degradation of petroleum products in the soil profile on the example of podzolic and sod-podzolic soils of the leningrad region.

Nowadays, soil contamination with oil products is one of the urgent problems, which leads to serious environmental consequences. Degradation of petroleum products in the soil profile is an important aspect of this problem. Knowing how soils of certain types interact with hydrocarbon pollution, it is possible to create point strategies for preserving ecosystems.

Key words: degradation of oil products, soil profile, podzolic soil, sod-podzolic soil, infrared spectrometry method, concentration.

УДК 504.05.054
ГРНТИ 87.17.15

ИССЛЕДОВАНИЕ ЗАВИСИМОСТИ ВЕЛИЧИНЫ ВЫБРОСА ОКСИДОВ АЗОТА ОТ КАЛОРИЙНОСТИ ТОПЛИВА

А. А. Борисова, А. Г. Казанцева
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

В данной научной статье на примере котельных рассматривается зависимость величины выброса оксидов азота от калорийности используемого топлива. Исследование проводилось расчетным методом на основе методики «Определения выбросов загрязняющих веществ в атмосферу при сжигании топлива в котлах производительностью менее 30 тонн пара в час или менее 20 Гкал в час».

выбросы, калорийность газа, оксиды азота, низшая теплота сгорания

Одним из главных загрязнителей воздушного бассейна являются выбросы оксида азота, которые поступают в атмосферный воздух при сжигании любого вида топлива. В периоды отопительного сезона котельные становятся одним из основных источников этого вещества.

Количество выбросов оксидов азота, поступающих в атмосферный воздух при работе котельных на газу, на прямую зависит от характеристик природного газа. Одной из основных характеристик газа, как топлива является его калорийность, которая определяет энергетическую ценность. Чем выше калорийность газа, тем больше энергии выделяется при его сгорании, что способствует повышению эффективности использования газа и снижению затрат на производство энергии.

Для определения общего количества выбрасываемых в атмосферу оксидов азота NO_x от котельных использовалась формула 1[1]:

$$M_{NO_x} = B_p * Q_i^r * K_{NO_2}^{\text{г}} * \beta_{\text{к}} * \beta_t * \beta_\alpha * (1 - \beta_r) * (1 - \beta_{\text{б}}) * k_{\text{п}} \quad (1)$$

где B_p - расчетный расход топлива, м^3/с (тыс. м^3/год), принятый за зимний период 2022 год (ООО «Петербург-Теплоэнерго») по городу Санкт-Петербург [3]; Q_i^r - низшая теплота сгорания топлива, МДж/м^3 взята на основе характеристик природного газа различных месторождений [2]; $K_{NO_2}^{\text{г}}$ - удельный выброс оксидов азота при сжигании газа, г/МДж рассчитан по формуле 2; $\beta_{\text{к}}$ - безразмерный коэффициент, учитывающий принципиальную конструкцию горелки принят в соответствии с методикой [1] (в данном случае - для дутьевых горелок напорного типа); β_t - безразмерный коэффициент, учитывающий температуру воздуха, указан согласно основным характеристикам; β_α - безразмерный коэффициент, учитывающий влияние избытка воздуха на образование оксидов азота, установлен на основе методики [1] (как в общем случае); β_r - безразмерный коэффициент, учитывающий влияние рециркуляции дымовых газов через горелки на образование оксидов азота и $\beta_{\text{б}}$ - безразмерный коэффициент, учитывающий

ступенчатый ввод воздуха в топочную камеру, принятые согласно методическому письму НИИ Атмосфера [4]; $k_{\text{п}}$ - коэффициент пересчета указан в соответствии с методикой [1].

Данные, используемые для расчета выбросов оксидов азота представлены в таблице 1.

ТАБЛИЦА 1. Расчетные характеристики для определения общего количества выбрасываемых в атмосферу оксидов азота NO_x

B_p, м^3/с (тыс. м^3/год)	$\beta_{\text{к}}$	β_t	β_α	β_r	$\beta_{\text{б}}$	$k_{\text{п}}$
43,861 (939820,8)	1	1,44	1,225	0,50596	0,44	1 (0,001)

Удельный выброс оксидов азота при сжигании газа ($K^{\text{г}}_{NO_2}$) рассчитывается по формуле 2 согласно методике (для водогрейных котлов) [1]:

$$K^{\text{г}}_{NO_2} = 0{,}0113 * \sqrt{Q_{\text{т}}} + 0{,}03 \quad (2)$$

где $Q_{\text{т}}$ - фактическая тепловая мощность котла по введенному в топку теплу, МВт, определяемая по формуле 3[1]:

$$Q_{\text{т}} = B_p * Q_i^r \quad (3)$$

Информация по низшей теплоте сгорания (Q_i^r) приведена в таблице 2.

Исходя из формулы 1 был произведен расчет выбросов оксидов азота при разной калорийности газа. Количество образованных выбросов представлено в таблице 2.

ТАБЛИЦА 2. Расчетные характеристики природного газа различных месторождений

Газопровод	Низшая теплота сгорания	Максимальный разовый выброс (г/с)	Валовый выброс (т/год)
Брянск-Москва	37,31	389,0329	1145574,649
Бухара-Урал	36,17	371,6971	1093481,216
Газли-Каган-Ташкент	36,26	373,0564	1097564,415
Газли-Каган	36,59	378,054	1112579,467
Гоголева-Полтава	30,98	296,1204	866815,3637
Дашава-Киев	35,88	367,3284	1080358,797
Джаркак-Ташкент	36,68	379,4207	1116686,268
Игрим-Пунга-Серов-Нижний Тагил	36,47	376,2342	1107111,582
Карабулак-Грозный	45,85	526,7813	1560542,037
Карадаг-Тбилиси-Ереван	37,09	385,6673	1135458,713
Коробки-Жирное-Камышин	41,45	454,1112	1341412,496
Коробки-Лог-Волгоград	35,84	366,7272	1078552,956
Кумертау-Ишимбай-Магнитогорск	36,8	381,2456	1122169,841
Лижво-Кологривовка-Вольск	37,01	384,4459	1131787,611
Оренбург-Совхозное	38,02	399,9591	1178424,773
Первомайск-Сторожевка	28,3	259,3427	756822,4693
Промысловка-Астрахань	35,04	354,7697	1042648,379

Рудки-Минск-Вильнюс, Рудки-Самбор	35,51	361,7791	1063693,244
Саратов-Горький	36,13	371,0935	1091668,09
Саратов-Москва	34,16	341,7665	1003624,118
Саушино-Лог-Волгоград	35,13	356,1084	1046667,389
Серпухов-Санкт-Петербург	37,43	390,8726	1151105,023
Средняя Азия-Центр	37,56	392,8689	1157106,271
Ставрополь-Невинномысск-Грозный	35,63	363,5758	1069088,825
Ставрополь-Москва:			
1-я нитка	36,09	370,4903	1089855,966
2-я нитка	36,55	377,4471	1110755,841
3-я нитка	37,01	384,4459	1131787,611
Угерско-Стрый,Угерско-Гнездичи, Угерско-Львов	35,5	361,6295	1063244,023
Урицк-Сторожевка	36,47	376,2342	1107111,582
Хаджи-Абад-Фергана	38,35	405,071	1193798,19
Щеблинка-Острогожск, Щебелинка-Днепропетровск, Щеблинка-Харьков	37,31	389,0329	1145574,649
Щеблинка-Брянск-Москва	37,87	397,6425	1171458,84
Смесь из Западной Сибири	36,84	381,8545	1123999,688
Якутск-Усть-Вилюй	34,37	344,8552	1012891,606

В соответствии с полученными расчетами была установлена линейная зависимость между выбросами и теплотой сгорания, представленная на рис. 1 и 2.

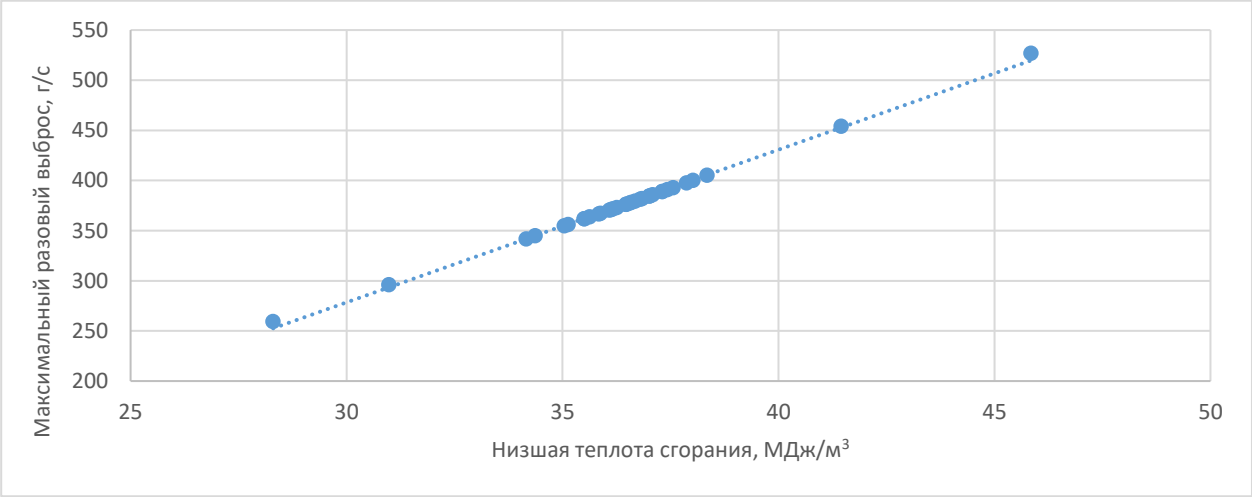


Рис. 1. Зависимость максимального разового выброса от низшей теплоты сгорания

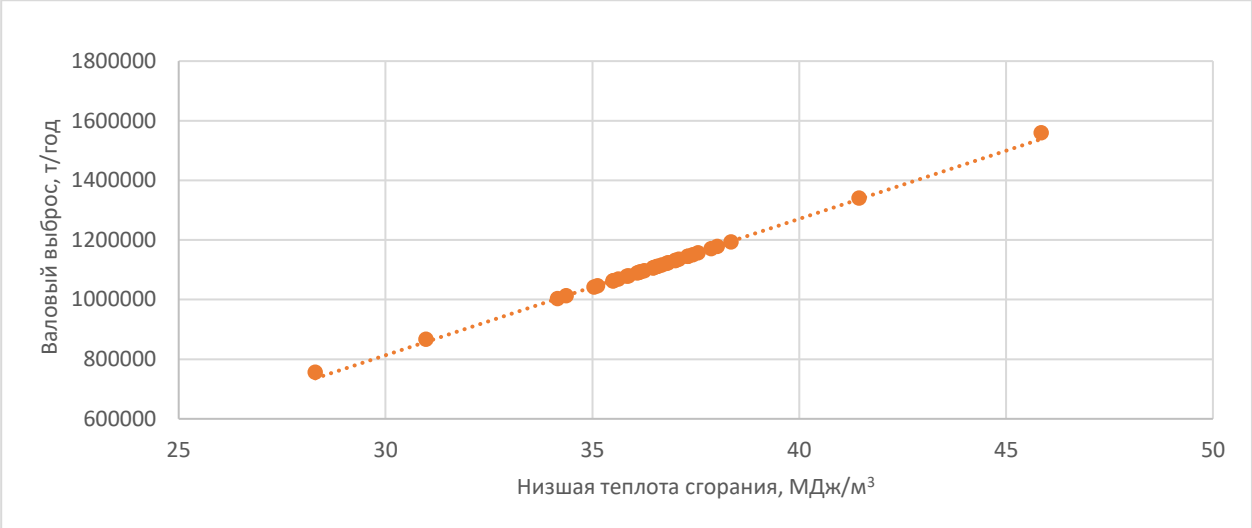


Рис. 2. Зависимость валового выброса от низшей теплоты сгорания

Таким образом, было установлено, что увеличение низшей теплоты сгорания приводит к повышению выбросов оксидов азота. В зависимости от низшей теплоты сгорания максимальный разовый выброс варьируется от 259,3427 до 526,7813 г/с, а валовый – от 756822,5 до 1560542,04 т/год.

Список используемых источников:

1. Методика «Определения выбросов загрязняющих веществ в атмосферу при сжигании топлива в котлах производительностью менее 30 тонн пара в час или менее 20 Гкал в час».

2. Актуализированная схема теплоснабжения Санкт-Петербурга на 2023 год, утвержденная приказом Минэнерго России от 04.08.2022 №762. Схема теплоснабжения Том 2 (Разделы 6, 7, 8, 9, 10, 11, 12) с. 59-60.

3. Расчетные характеристики природного газа различных месторождений // [Электронный ресурс] – URL: https://dkm.ru/for-developers/documentation/files/from-snipes/9.pdf (дата обращения: 15.10.2023).

4. Методическое письмо НИИ Атмосфера N 335/33-07 от 17 мая 2000г. «О проведении рас четов выбросов вредных веществ в атмосферу по «Методике определения выбросов загрязняющих веществ в атмосферу при сжигании топлива в котлах производительностью менее 30 тонн пара в час или менее 20 Гкал в час» (М., 1999).

Borisova A, Kazantseva A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Study of the dependence of the value of nitrogen oxide emissions on the calority of fuel.
The article considers the dependence of the amount of nitrogen oxide emissions on the caloric content of the used fuel on the example of boiler plants. The study was conducted by calculation method based on the methodology of "Pollutants emissions determination into the atmosphere while burning fuel in boilers with a capacity of less than 30 tons of water vapor per hour or less than 20 Gcal per hour."

Key words: emissions, calorie of water vapor, nitrogen oxides, the lowest heat of combustion.

УДК 628.477
ГРНТИ 87.53.13

УСЛОВИЯ И РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТА ПО БИОДЕГРАДАЦИИ ПОЛИМЕРНЫХ ОТХОДОВ В ЕСТЕСТВЕННЫХ УСЛОВИЯХ

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

Цель статьи заключается в рассмотрении рациональности использования полигонов для захоронения полимерных отходов. Так же было проанализировано устройство полигонов, благодаря которому стали известны возможные воздействия полимерных отходов на окружающую среду, в частности на почву, атмосферный воздух и воды. Произведен эксперимент, заключающийся в исследовании изменения весовых характеристик образцов полимеров - полиэтиленовых пакетов, которые наиболее распространены в бытовой жизни человека. В результате эксперимента была выявлена низкая скорость деструкции полимеров в естественной среде, был предложен альтернативный вариант обращения с полимерными отходами и так же произведен эксперимент по деструкции полимера в перекиси водорода с воздействием ультрафиолета.

полимерные отходы, полиэтилен, полигоны, загрязнения почвы, загрязнения воды, ультрафиолет, пероксид водорода

В 2021 г. на территории Российской Федерации образовалось 8448,6 млн т отходов производства и потребления, 7,164 млн.тонн - полимерные материалы, что на 21,5% выше уровня 2020 г. Общая масса захороненных отходов в 2021 г. составила 981,5 млн т. За период 2012—2021 гг. произошло увеличение этого показателя на 17,9%, при снижении до 354,6 млн т в период 2013—2015 гг. Данные 2021 г. неизбежно на восстановление тренда на увеличение объема захороненных отходов после прекращения в 2020 г [1]. Полимерные отходы российских ТКО составляют примерно 12% от общего объема, в 2021 г. на территории Российской Федерации было образовано 48 362,8 тыс. т ТКО. На переработку направляется всего лишь 20-25 процентов всех пластмассовых отходов. Остальное отправляется на полигоны[2].

А значит, что большая часть полимерных материалов попадает в почву и оказывает влияние на нее. Такие виды отходов могут разлагаться очень долгое время и сохранять свое существование в почве, при этом изменяя ее свойства и структуру. Основное воздействие происходит как раз на полигонах ТКО.

Полигон - это сложный, современный и обширный инженерно-технический комплекс сооружений, направленный на захоронение ТКО и на уменьшение попадания и воздействия отравляющих веществ на окружающую среду от отходов различного происхождения. Полигон должен соответствовать нормам объектов размещения отходов. Строительство

полигона начинается с выбора участка. Исследуют участок на состав подстилающего слоя, лучший участок является с глиной и суглинками. Исключаются участки с водоемами - реками, озерами и даже с родниками, с затапливаемыми территориями, с грунтовыми водами залегающими выше 2 метров до почвенного слоя, с геологическими разломами. Расположение участка должно быть не менее 15 км до аэропорта, так как полигон является частым местом скопления птиц, которые затрудняют работу аэропорта, а от населенного пункта не менее 500 метров[3]. Под полигоны могут использоваться карьеры, овраги. Полигоны защищаются специальной лесной полосой не менее 20 метров шириной и к ним должна проходить асфальтная дорога для беспрепятственного подъезда, которая оснащена контрольно-пропускным пунктом со шлагбаумом на въезде-выезде с полигона для контроля. Территория полигона должна быть огорожена забором для предотвращения незаконного проникновения. Расчетное время использование полигона не менее 20-25 лет[3].

Работа полигона происходит круглогодично по двухсменному графику с выполнением таких задач, как: прием отходов, их сдивгание и выравнивание, увеличение плотности отходов и в конечном итоге- изоляция. Специальный автомобильный транспорт осуществляет доставку, затем его взвешивают на автомобильных весах, чтобы узнать количество прибывающих отходов, затем машины выгружают хвосты и проходят дезинфекцию и мойку. После идет работа с отходом. Площадь полигона поделена на секторы, которые используются поочередно до пяти лет каждый. На них происходит складирование хвостов. Часто используют уплотнительные машины для отхода из-за потребности в полной реализации объема сектора. Складирование отходов происходит несколькими способами - способом «надвига» и методом «сталкивания» [4]. Для первого метода характерна укладка хвоста снизу вверх. Делают слой отходов равный половине метра и создают наклонный вал из уплотненных слоев высотой 2 метра, на который надвигают следующий вал, а потом это все изолируется слоем грунта равным четверти метра. Метод «сталкивания» идет обратным способом укладки - сверху вниз и высота склонов не должна превышать 2,3 метра[4]. Для того, чтобы поверхность полигона оставалась ровной, используют тяжелую технику, бульдозеры и катки, приминающие слои отходов и слои изоляции, которые защищают полигон от привлечения вредителей - грызунов, птиц, мух. Иногда могут проводить специальные мероприятия, направленные на уничтожение грызунов - возбудителей болезней и дезинфекцию.

В больших количествах и под действием сторонних и природных факторов полимерные отходы начинают изменять свои физико-механические свойства, что и происходит на территориях полигонов. Могут становиться уплотненными, хрупкими и сыпучими, а с появлением осадков выделяют фильтрат, который уходит вглубь почв. В фильтрат могут входить различные опасные вещества, это зависит от состава полимерных отходов на полигоне. Например, при разложении поливинилхлорида выделяется хлористый

водород, галогенированные и ароматические углеводороды, влияющие на растворимость тяжелых металлов [5]. При захоронении полимеров протекают реакции с испусканием тепла, что является причиной горения, при котором выделяются диоксины, стирол и прочие опасные вещества, выделяющиеся в атмосферу.

Разложение полимерных синтетических материалов в условиях безвоздушной среды грозит образованием биогаза - смеси токсичных газов[6]. Именно от полимеров происходит выделение толуола, винилхлорида, бензола, ксилола. Из-за смешения полимерных материлов с другими отходами выделяются взрывоопасные и высокотоксиные газы в которую входят сероводород, метан, диоксид углерода, окиси углерода.

Для того, чтобы выяснить целесообразность использования полигонов для захоронения полимерных отходов в климатических условиях средней полосы России, был проведен эксперимент. Для эксперимента были взяты полиэтиленовые пакеты различных торговых сетей и пакеты для мусора. Выбор был сделан в связи с тем, что это одни из самых популярных полимерных продуктов, которые человек использует почти каждый день своей жизни. Образцы были помещены в условия, схожие с условиями полигона. Их поместили в компостную яму в Ленинградской области в поселке Большая Ижора. Эксперимент проводился в течение почти полугода - с 20 ноября 2021 года по 10 мая 2022 года при температурах от $+18^0$C до -23^0C.

В условиях компостирования весовые характеристики не показали показали большие изменения в измерениях, результаты представлены в таблице 1.

Фирма	№	Шифр воздействия	До воздействия, г	После воздействия, г	Процентное изменение веса после воздействия относительно исходной массы
«Окей», Polymateria	1	Контрольный	0,1286	-	-
	2	В компосте	0,3376	0,3386	-0,29
«Академия Комфорта»	5	Контрольный	0,0646	-	
	6	КС	0,1999	0,2024	-1,25
«Prisma»	9	Контрольный	0,1221	-	
	10	КС	0,5909	0,6074	-2,79

ТАБЛИЦА 1 Изменение весовых характеристик полиолефионовых образцов в условиях естественного старения

«Prisma»	9	Контрольный	0,1221	-	
	10	КС	0,5909	0,6074	-2,79
«OZON»	13	Контрольный	0,8540	-	
	14	КС	0,8100	0,7919	2,23
«Магнит»	16	Контрольный	0,3415	-	
	17	КС	0,3205	0,2935	8,42
Окей вторичный	19	Контрольный	0,5989	-	-
	20	КС	0,5950	0,6066	-1,94
«Фрекен Бок»	22	Контрольный	0,1986	-	-
	23	КС	0,2033	0,1969	3,14

Только образец полиэтилена высокого давления пакет-майка розничной торговой сети «Магнит» показал наиболее заметное снижение веса, которое составило 8,42%. Так же снижение веса было замечено у следующих образцов:

- Мусорный мешок, бренд «Фрекен Бок» биоразлагаемый;
- Пакет маркетплейса «OZON»;

Наибольшее значение при компостировании в весе прибавил образец пакета-майки розничной торговой сети «Prisma», что составляет - 2,79%. Помимо этого образца увеличение массы зафиксировано у следующих полимерных упаковок:

- Пакет майка биоразлагаемый, бренд «Окей»-« Polymateria»;
- Мусорный мешок, бренд «Академия комфорта»;
- Пакет-майка, розничная торговая сеть «Окей» из вторсырья.

Изменение весовых характеристик образцов не превысило и 10%, а значит активного процесса разложения в условиях естественной среды схожей с условиями полигона не выявлено, что говорит о нецелесообразности использования полигонов. Помимо медленной деструкции полимеров происходит серьезное воздействие на окружающую среду, в результате чего могут загрязнятся почвы, подземные и поверхностные воды. В качестве альтернативного решения деструкции полимерных отходов будет предложено воздействие пероксида водорода совместно с ультрафиолетовым излучением. Так же был проведен опыт воздействия этого способа. Для ультрафиолетового облучения образцов использовался бактерицидный рециркулятор Плон 1.0 с модернизированным

металлическим корпусом и снабженный лампой мощностью 15 Вт (длинна волны - 254 нм). Образцы были помещены в раствор пероксида водорода и обрабатывались ультрафиолетовым излучением. В результате опыта весовые характеристики были непоказательны в виду непродолжительности эксперимента, в следствии чего специалистами Института высокомолекулярных соединений РАН на разрывной машине 2166 Р-5 были определены механические характеристики обработанных и контрольных образцов (σ_p – разрывное напряжение; Е– модуль упругости, или модуль Юнга; Ɛ– относительное удлинение при разрыве). Итоговые единицы такие как, разрывное напряжение, модуль упругости, относительное удлинение при разрыве, представленные в таблице 2, в которой зафиксированы изменения механических характеристик полиэтиленовых пленок по сравнению с контрольным образцом, который не подвергался каким-либо дополнительным воздействиям, выраженные в процентах, показали хорошие результаты у трех образцов, которые говорят о стремительной деструкции полимеров под воздействием данных факторов.

ТАБЛИЦА 2 Изменение механических характеристик полиэтиленовых пленок по сравнению с контрольным образцом

Метод интенсификации деструкции полимерной пленки	Изменение механических характеристик пленочных материалов[1], %								
	Полиэтилен низкого давления			Полиэтилен высокого давления			Полиэтилен «Polymateria»		
	Разрывное напряжение (σ_p)	Модуль упругости (Е)	Относи-тельное удлинение при разрыве (Ɛ)	Разрывное напряжение (σ_p)	Модуль упругости (Е)	Относи-тельное удлинение при разрыве (Ɛ)	Разрывное напряжение (σ_p)	Модуль упругости (Е)	Относи-тельное удлинение при разрыве (Ɛ)
УФ-облучение +обработка пероксидом водорода	+13	+15	+79	-38	-17	+236	+26	+14	+64

В образцах полиэтилена низкого давления и полиэтилена «Polymateria» происходит увеличение прочности при разрыве и рост модуля упругости, что

может говорить о возрастании степени кристалличности исследованных полимеров. Но при этом происходит увеличение относительного удлинения при разрыве. У полиэтилена высокого давления эти изменения несут отрицательный характер, кроме же относительного удлинения при разрыве, которое возрастает в разы.

Список используемых источников:

1. Государственный доклад «О состоянии и об охране окружающей среды РФ» в 2021г. [Электронный ресурс] https://www.mnr.gov.ru/docs/gosudarstvennye_doklady/o_sostoyanii_i_ob_okhrane_okruzhayushchey_sredy_rossiyskoy_federatsii/ (дата обращения 28.12.2022).

2. Кацевман М. Верните целлофан [Электронный ресурс] // Российская газета. N 206 (7964). URL: https://rg.ru/2019/09/15/problemu-pererabotki-plastmassovyh-othodov-peregreli-radi-imidzha.html (дата обращения: 28.12.2022).

3. Баловнев В. И., Данилов Р. Г., Кустарев Г. В. и др. Компакторы. Уплотнители твердых бытовых и промышленных отходов. Устройство, основы расчета : учеб. пособие. М. : МАДИ, 2014. 100 с.

4. Твердые бытовые отходы. Справочник. М. : Акад. коммун. хоз-ва, 2001. 319 с.

5. Гарин В. М., Клёнова И. А. Экология для технических вузов. М. : Феникс, 2003. 384 с.

6. Лобачев Г. К., Желтобрюхов В. Ф. и др. Вторичные ресурсы: проблемы, перспективы, технология, экономика : учеб. пособ. Волгоград, 1999. 180 с.

Vinogradova N.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Conditions and results of an experiment on the biodegration of polymer waste in natural condition.

The purpose of the article is to consider the rationality of using landfills for the disposal of polymer waste. The design of landfills was also analyzed, thanks to which the possible effects of polymer waste on the environment, in particular on soil, air and water, became known. An experiment was carried out to study changes in the weight characteristics of polymer samples - plastic bags, which are most common in human everyday life.As a result of the experiment, a low rate of destruction of polymers in the natural environment was revealed, an alternative option for handling polymer waste was proposed, and an experiment was also carried out on the destruction of the polymer in hydrogen peroxide under exposure to ultraviolet radiation.

Key words: polymer waste, polyethylene, landfills, soil pollution, water pollution, ultraviolet radiation, hydrogen peroxide.

УДК 504.06
ГРНТИ 87.55.37

АНАЛИЗ ШУМОВОГО ЗАГРЯЗНЕНИЯ ТЕРРИТОРИИ МУНИЦИПАЛЬНОГО ОКРУГА ГАГАРИНСКОЕ МОСКОВСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА С ПРИМЕНЕНИЕМ ГИС-ТЕХНОЛОГИЙ

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

В данной научной статье рассмотрена проблема шумового загрязнения в муниципальном округе Гагаринское Московского района Санкт-Петербурга. В связи с ростом автомобилизации в мегаполисах России шум транспорта считается одной из самых ощущаемых экологических проблем. Жители Санкт-Петербурга испытывают дискомфорт от шумового загрязнения, повышенный шумовой фон негативно влияет на здоровье человека. Анализ шумового загрязнения муниципального округа Гагаринское особенно важен ввиду того, что в настоящее время население не обеспечено информацией о воздействующем шуме на территории Московского района Санкт-Петербурга. Результаты измерений были обработаны с помощью географической информационной системы ArcGIS и сопутствующего программного обеспечения ArcMap, точки измерений в районе исследования были нанесены на карту, где отображены координатные ссылки и фактические измерения, а также была построена карта интерполяции методом OBP, для наглядного представления шумового загрязнения муниципального округа Гагаринское. В результате анализа были выявлены ключевые участки с повышенными значениями уровня шума.

шум, шумовое загрязнение, картографирование шума, геоинформационные системы, ГИС, интерполяция, муниципальный округ Гагаринское.

Шумовое загрязнение в Санкт-Петербурге является одной из наиболее важных экологических проблем, с которой сталкиваются местные жители. Основными источниками шума являются автодороги, железные дороги, аэропорты, транспортный поток, строительство и индустриальная деятельность. Уровень шума в Санкт-Петербурге превышает нормы, что может приводить к ряду проблем для здоровья человека, таких как бессонница, повышенное напряжение, усталость и другие негативные эффекты на организм. Контроль шума особенно необходим в больших городах, но в настоящее время в Санкт-Петербурге нет постоянного мониторинга шума.

В настоящее время основным источником шумового загрязнения является транспорт. Автомобильный транспорт является одним из главных источников шумового загрязнения в городской среде.

Шум от движущихся автомобилей может достигать до 90 дБ, что опасно для здоровья человека, вызывая проблемы со сном, повышение кровяного давления, стресс и другое [1].

По оценкам экспертов Роспотребнадзора, около 1 миллиона человек, проживающих в Санкт-Петербурге, живут в неблагоприятных шумовых

условиях. Большая часть этого воздействия обусловлена шумом от транспорта, автомобильных и железных дорог и аэропорта Пулково - воздушных ворот Санкт-Петербурга. Так, в районах, прилегающих к кольцевым автодорогам, аэропортам, железной дороге и основным магистралям города, а также в промышленных зонах уровни шума превышают норму в среднем на 10-15 дБ [2].

Кроме того, шум может вызывать не только физические проблемы, но и социальные проблемы, такие как ухудшение качества жизни, повышенный уровень стресса и конфликты между жителями.

Для того чтобы разобраться в этом вопросе более подробно, было проведено социологическое исследование влияния шума на жителей Московского района Санкт-Петербурга. Опрос проводился среди местных жителей, проживающих именно на территории муниципального округа Гагаринское, респонденты были опрошены прямо на улице.

В ходе исследования было опрошено 50 человек, проанализировав ответы респондентов на 3 вопроса, можно сделать определенные выводы (рис. 1).

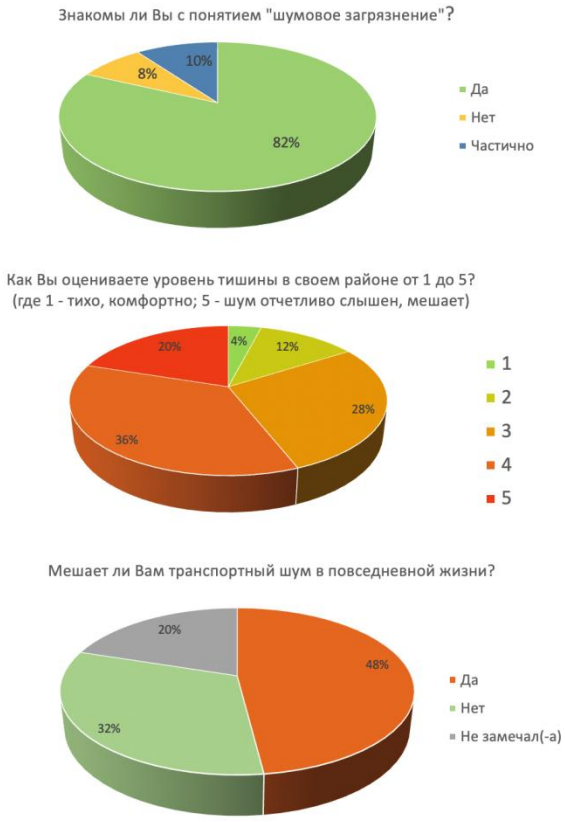


Рис. 1. Диаграммы составленные на основании ответов на социологический опрос

На представленных диаграммах можно увидеть, что местные жители неплохо осведомлены о таком явлении как шумовое загрязнение (82%). Как мы можем наблюдать больше половины респондентов оценивают уровень тишины в своем районе как довольно шумный. Около половины опрошенных людей испытывают дискомфорт от транспорта в повседневной жизни. Так как большую часть времени люди проводят чаще всего в своем районе, где

они проживают, такая ситуация никак не может быть нормой. Недовольство или же терпимое отношение к уровню шума не самый лучший исход. Он может иметь определённые последствия, которые отразятся достаточно быстро, либо могут возникнут от кумулятивного эффекта.

На территории Муниципального округа Гагаринское проходит железная дорога, вдоль Витебского проспекта, которая конечно является источником шума, однако наибольший уровень шумового загрязнения исходит все-таки от автомобильных дорог. Благодаря проведенным замерам и построенным на их основании картам, можно увидеть, что всё шумовое загрязнение района приходится на транспорт.

Для измерений значений уровня звука использовался шумомер DT-8851, и дополнительно проводились замеры шумомером ШИ-01В для расчета шумозащитного экрана.

Измерения обрабатывались с помощью географической информационной системы ArcGIS и сопутствующего программного обеспечения ArcMap, точки измерений были нанесены на карту с привязкой к координатам в пределах исследуемой территории и фактическим значением (дБА). Всего было взято около 500 точек в каждой из которых были проведены замеры уровня шума, однако в дальнейшем измерения проводились дополнительно.

Карта с ключевыми точками фактических измерений шума представлена на рисунке 2.

Из полученных замеров уровня шума и построенной карты, видно, что наибольший показатель уровня шума находится на территории КАДа (76,7 дБА), менее шумные, однако также превышающие допустимый уровень шума, который согласно СП 51.13330.2011 равен 55 дБА, расположены на улице Типанова (ул. Типанова 25 к.1), на пересечении Московского шоссе и Дунайского проспекта, по адресу Бассейная улица 89, а так же на пересечении Витебского проспекта и Благодатной улицы

Что обуславливается прохождением железнодорожной сети вдоль Витебского проспекта и трамвайными путями вдоль Благодатной улицы, и строительством новой дорожной развязки на пересечении Московского шоссе и Дунайского проспекта.

Наименьшие показатели уровня шума зафиксированы во всех районных «дворах», соответственно можно сделать вывод, что 90% шумового загрязнения поступает от дорог, и соответственно, от транспорта.

Для более наглядного представления о шумовом загрязнении муниципального округа Гагаринское была создана карта интерполяции растра, с цветовым зонированием (рис. 3).

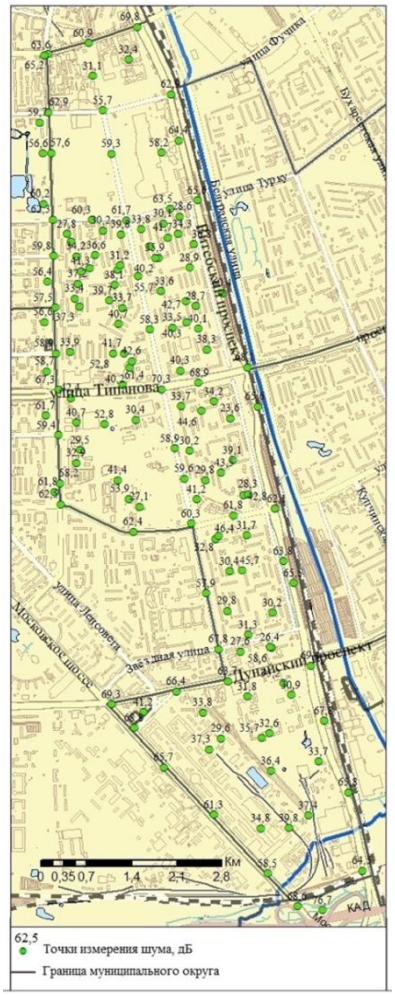


Рис. 2. Карта расположения ключевых точек замеров уровня шума с фактическими значениями в дБА значениями в дБА

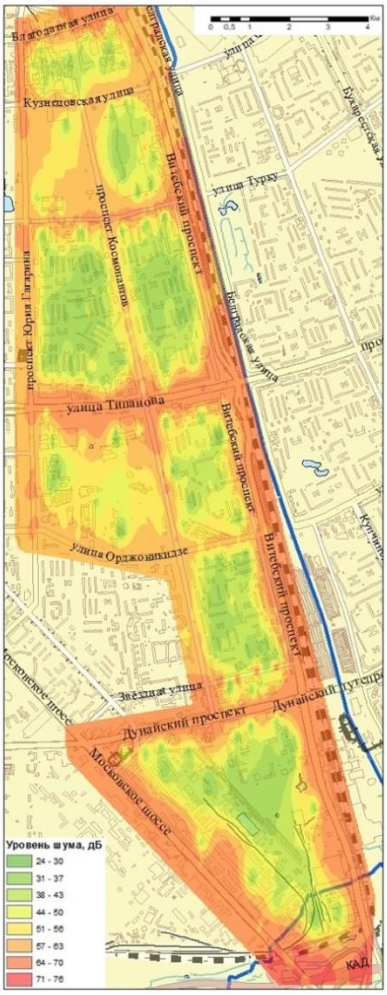


Рис. 3. Карта с наложением интерполяции растра методом ОВР

В целом, средний уровень шумового загрязнения на исследуемой территории является приемлемым и не несет опасности здоровья населения, но исходя из полученных замеров на участке по адресу улица Типанова 25к.1 показатель уровня звука превышает максимальный уровень шума, который согласно СанПиН 1.2.3685-21 равен 70 дБА. Для данной точки проводится расчет шумозащитного экрана.

Шумозащитный экран на улице Типанова 25 к.1 оказался целесообразным. Визуализация которого представлена на рис. 4.

Рис. 4. Визуализация шумозащитного экрана

Список используемых источников:

1. МР 2.1.10.0059-12 «Оценка риска здоровью населения от воздействия транспортного шума»: утвержден Главным государственным санитарным врачом Российской Федерации Г. Г.Онищенко 23 марта 2012 г.
2. Роль молодых учёных и исследователей в решении актуальных задач АПК: материалы международной научно-практической конференции молодых ученых и обучающихся. - Ч. П / СПбГАУ. - СПб., 2020. URL: https://spbgau.ru/files/nid/8990/rol_molodyh_uchenyh_i_issledovateley_chast_2_2020.pdf (дата обращения: 07.05.2023)
3. Федеральный закон от 30.03.1999 № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения»: принят Государственной Думой, 1999.
4. Федеральный закон от 10.01.2002 № 7-ФЗ «Об охране окружающей среды» (с изм. и доп. вступ. в силу от 01.03.2023): принят Государственной Думой, 2002.
5. СанПиН 2.1.2.2645-10 «Санитарно-эпидемиологические требования к условиям проживания в жилых зданиях и помещениях»: постановление Главного государственного санитарного врача РФ от 10 июня 2010.
6. СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека»: Государственная система санитарно-эпидемиологического нормирования Российской Федерации. М: Минздрав России, 2021.

Gubasheva A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Analysis of noise pollution of the territory of the gagarinskoye municipal district of the moscow district of st. Petersburg using gis technologies.

This scientific article examines the problem of noise pollution in the Gagarinskoye municipal district of the Moscow district of St. Petersburg. Due to the growth of motorization in the megacities of Russia, the noise of transport is considered one of the most felt environmental problems. Residents of St. Petersburg experience discomfort from noise pollution, increased background noise negatively affects human health. The analysis of noise pollution of the Gagarinskoye municipal district is especially important due to the fact that at present the population is not provided with information about the noise affecting the territory of the Moskovsky district of St. Petersburg. The measurement results were processed using the ArcGIS geographic information system and the accompanying ArcMap software, the measurement points in the study area were mapped, where coordinate references and actual measurements were displayed, and an IAD interpolation map was built to visually represent the noise pollution of the Gagarinskoye municipal District. As a result of the analysis, key areas with increased noise levels were identified.

Key words: noise, noise pollution, noise mapping, geoinformation systems, GIS, interpolation.

УДК 666.94
ГРНТИ 87.17.37

ОПРЕДЕЛЕНИЕ ОСНОВ НОРМИРОВАНИЯ ВЫБРОСОВ В ЦЕМЕНТНОЙ ПРОМЫШЛЕННОСТИ ПРИ ИСПОЛЬЗОВАНИИ АЛЬТЕРНАТИВНЫХ ВИДОВ ТОПЛИВА

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

Рассмотрены основные принципы нормирования промышленных выбросов в цементной промышленности при применении альтернативных видов топлива. На основании выполненного анализа предложен перечень загрязняющих веществ, подлежащий нормированию в выбросах предприятий данной отрасли.

цементная промышленность, альтернативное топливо, нормирование выбросов, загрязняющие вещества, атмосферный воздух

С целью снижения себестоимости выпускаемой продукции без ухудшения её качества, повышения энергоэффективности производства и улучшения экологической обстановки в регионах месторасположения предприятий цементной промышленности, практикуется применение помимо основного вида топлива – природного газа, применение также альтернативных видов твердого топлива.

Одна из главных задач экологической политики предприятий цементной отрасли в России на долгосрочный период – применение принципа нормирования допустимого воздействия на атмосферный воздух на основе показателей наилучших доступных технологий, в том числе при применении альтернативных видов топлива.

Основные возможные к применению в цементной промышленности виды альтернативного топлива описаны в Справочнике по наилучшим доступным технологиям ИТС 6-2022 «Производство цемента» и представлены на рис. 1 [2]:

Рис. 1. Основные возможные к применению виды альтернативного топлива

Применение альтернативного вида топлива необходимо для создания дополнительной теплотворной способности цементной печи и повышения производительности предприятия в целом. Следует отметить, что альтернативные виды топлива применяются в смеси с основным видом топлива, снижая процент его потребления.

В данной статье рассматриваются наиболее встречающиеся в цементной отрасли виды применяемых топлив, а именно:

1. твердое топливо из текстильного корда отработанных покрышек;
2. твердое биотопливо (осадок коммунально-бытовых и смешанных сточных вод и избыточный ил);
3. твердое топливо из бытовых отходов;
4. твердое топливо из пластиков вторичных.

Основными выбрасываемыми в атмосферный воздух загрязняющими веществами предприятий цементной промышленности, именуемые в дальнейшем также – маркерные вещества, являются [2]:

- Оксиды азота NO_x (сумма азота оксида (NO) и азота диоксида (NO_2), в пересчете на NO_2);
- Серы диоксид SO_2;
- Углерода оксид CO;
- Взвешенные вещества (пыль неорганическая).

В соответствии со Справочником НДТ ИТС 6-2022, также определены основные маркерные вещества, выбрасываемые в атмосферный воздух при применении альтернативных видов топлива, дополняющие вышеуказанный перечень, а именно [2]:

- Хлористый водород HCl;
- Фтористый водород HF;
- Металлы: Ртуть Hg; Кадмий Cd, Таллий Tl, Свинец Pb, Медь Cu

Согласно международным кадастрам и руководствам по выбросам, список загрязняющих веществ, которые считаются актуальными при применении альтернативных видов топлива, может включать в себя также следующие вещества [2]:

- общий органический углерод (COT), включая летучие органические соединения (ЛОС);
- полихлородибензодиоксины и полихлородибензофураны (ПХДД и ПХДФ);
- аммиак (NH3);
- полихлордифенилы (PCB);
- полициклические ароматические углеводороды (ПАУ);
- бензол;
- гексахлорбензол (HCB);
- циановодород (HCN);
- антрацен;
- нафталин.

Для определения четкого перечня загрязняющих веществ, подлежащих нормированию, необходимо также руководствоваться требованиями российского природоохранного законодательства, в частности – Распоряжением Правительства №1316-р от 08.07.2015 (в ред. 2019 г.) «Об утверждении перечня загрязняющих веществ, в отношении которых применяются меры государственного регулирования в области охраны окружающей среды».

С учетом того, что в рассматриваемых в данной статье альтернативных видах топлива так или иначе содержатся полимерные материалы, такие как пластики, в рамках данной работы был выполнен анализ научных работ по изучению выделяемых в результате горения пластиков загрязняющих веществ. Так, согласно изученным научным статьям [3, 4, 5], наиболее часто встречающимися загрязняющими веществами, выделяющимися в результате данного процесса, являются: Ацетилен; Хлорводород; Хлорметан; Хлорэтан; Бензол; Толуол; Стирол.

Таким образом, в ходе данной работы был сформирован сводный перечень нормируемых загрязняющих веществ, выбрасываемых в атмосферный воздух предприятиями цементной промышленности при использовании АТ различных видов – представлен в таблице 1.

ТАБЛИЦА 1. Перечень загрязняющих веществ, выбрасываемых в атмосферный воздух предприятиями цементной промышленности при применении альтернативных видов топлива

Наименование загрязняющего вещества	**Код**
Азота диоксид (Двуокись азота; пероксид азота)	0301
Азот (II) оксид (Азот монооксид)	0304
Углерод (Пигмент черный)	0328
Сера диоксид	0330
Углерода оксид (Углерод окись; углерод моноокись; угарный газ)	0337
Взвешенные вещества	2902
Пыль неорганическая, содержащая двуокись кремния, в %: - 70-20 (шамот, цемент, пыль цементного производства - глина, глинистый сланец, доменный шлак, песок, клинкер, зола кремнезем и другие)	2908
Пыль неорганическая, содержащая двуокись кремния, в %: - менее 20 (доломит, пыль цементного производства - известняк, мел, огарки, сырьевая смесь, пыль вращающихся печей, боксит и другие)	2909
Аммиак (Азота гидрид)	0303
Гидрохлорид/по молекуле HCl/ (Водород хлорид)	0316
Фтористые газообразные соединения/в пересчете на фтор/: - гидрофторид (Водород фторид; фтороводород)	0342
Смесь предельных углеводородов C_1H_4 – C_5H_{12}	0415
Пентилены (амилены – смесь изомеров)	0501

Наименование загрязняющего вещества	Код
Бензол (Циклогексатриен; фенилгидрид)	0602
Диметилбензол (смесь о-, м-, п- изомеров) (Метилтолуол) Ксилол	0616
Этенилбензол (Винилбензол; фенилэтилен) Стирол	0620
Метилбензол (Фенилметан,Толуол)	0621
Алканы С12-С19 (в пересчете на С)(Углеводороды С12-С19)	2754
Диоксины/в пересчете на 2,3,7,8-тетрахлордибензо-1,4-диоксин/ (Диоксин, тетрадиоксин, 2,3,7,8-ТХДД)	3620
Нафталин (Нафтален; нафтен)	0708
Бенз(а)пирен	0703
Свинец	0184
Кадмий Кадмий оксид/в пересчете на кадмий/	0133
Медь Медь оксид/в пересчете на медь/(Медь окись; тенорит)	0146
Ртуть	0183
Таллий карбонат/в пересчете на таллий/(Карбонат таллия(I), углекислый таллий)	0191
ПХБ (Полихлорированные бифенилы)	

На основании данного перечня, сформированного исходя из требований соответствия предприятий цементной промышленности наилучшим доступным технологиям и требованиям российского природоохранного законодательства, необходимо проведение инструментальных исследований для подтверждения наличия данных веществ в выбросах в значительном для нормирования количестве, что также выполняется в рамках данной научно-исследовательской работы.

Список используемых источников:

1. Распоряжение Правительства РФ № 1316-р от 08.07.2015 г. в ред. 2019 г. «Об утверждении перечня загрязняющих веществ, в отношении которых применяются меры государственного регулирования в области охраны окружающей среды».

2. Справочник по наилучшим доступным технологиям «ИТС 6-2022. Производство цемента».

3. Кетов А. А., Красновских М. П. Исследование продуктов термической деструкции пенополистирола самозатухающего и полистирола, полученного полимеризацией в массе с полихлорированными углеводородами // Вестник Пермского университета. Химия. 2013. Вып. 2.

4. Басалаева Л. В., Лобуренко А. П., Пономаренко А. Н., Пресняк И. С. Методика оценки токсичности продуктов горения отходов полимерных материалов как источника токсических веществ в эколого-гигиенических исследованиях // Актуальные проблемы транспортной медицины. 2008. N 1.

5. Басалаева Л. В., Копа М. Р., Шафран Л. М. Сравнительные санитарно-гигиенические исследования газообразных продуктов // Актуальные проблемы транспортной медицины. 2009. N 4 (18).

Zagrebaeva N. M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Determination of the basis of emission regulation in the cement industry when using alternative fuels.
This article, the basic principles of rationing industrial emissions in the cement industry when using alternative fuels are considered. Based on the analysis performed, a list of pollutants is proposed to be standardized in the emissions of enterprises of this industry.

Key words: Cement industry, alternative fuel, emissions rationing, pollutants, atmospheric air.

УДК 504.3.054
ГРНТИ 87.17.15

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ТЕМПЕРАТУРЫ НА ВЕЛИЧИНУ ВЫБРОСА

А. Г. Казанцева, И. Ю. Цветкова
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье анализируется влияние температуры выброса загрязняющих веществ в атмосферу на концентрацию этих веществ в атмосферном воздухе. Исследование проводилось расчетным методом. В качестве объекта исследования выступают выбросы производства минеральной ваты. Были сделаны выводы о рассеивании выбросов в атмосферном воздухе на основании расчётов динамической вязкости выброса.

температура выбросов, концентрация загрязняющих веществ, вязкость, водяной пар

С 2019 года в Российской Федерации введено требование по снижению выбросов в периоды неблагоприятных метеорологических условий (НМУ) [1]. Предприятия обязаны сокращать выбросы при наступлении периодов НМУ. Часто снижение выбросов достигается путем прекращения работы некоторых источников, поэтому в ряде случаев, приходится сокращать или останавливать производство, что приводит к увеличению издержек.

Исследования авторов, проведенные ранее, показали, что увеличение температуры выбросов может вполне успешно может применяться в качестве мероприятия в периоды НМУ. В качестве объекта исследования было выбрано производство минеральной ваты, организация выбросов которого позволяет регулировать температуру в широком диапазоне.

Выбросы, поступающие в атмосферу, имеют следующий состав: азот диоксид, углерод оксид, сера диоксид, аммиак, пыль неорганическая, содержащая двуокись кремния, в %: - 70-20, зола углей, сероводород, формальдегид, фенол, а также пары воды, которые не являются загрязняющим веществом.

В качестве исходных данных были взяты 2 протокола с результатами измерений концентраций загрязняющих веществ в выбросах от производства, проведенных на предприятии по производству минеральной ваты в Хабаровском края в декабре 2021 года и феврале 2022 года аккредитованной лабораторией.

На основании исходных данных, в соответствии с формулами 1-3, приведенными в приказе Минприроды России от 19 ноября 2021 года № 871 «Порядок проведения инвентаризации стационарных источников и выбросов загрязняющих веществ в атмосферный воздух» [2], было рассчитано количество загрязняющих веществ, поступающих в атмосферный воздух (г/с).

Результаты расчетов приведены в таблице 1, 2.

ТАБЛИЦА 1. Результаты расчётов разового значения мощности выброса ЗВ по протоколу №1, г/с

$T_г$, °С Наим.в-ва	Усредненные значения, мг/м^3	50	68	100	150	200
0301. Азот диоксид	16,4	0,66656	0,63138	0,57721	0,50898	0,45518
0337. Углерод оксид	12,5	0,50805	0,48123	0,43995	0,38794	0,34694
0330. Сера диоксид	28,6	1,16242	1,10106	1,00660	0,88762	0,79379
0303. Аммиак	3,3	0,13413	0,12705	0,11615	0,10242	0,09159
2908. Пыль неорг., содерж. двуокись кремния, в %: - 70-20	25,1	1,02017	0,96632	0,88341	0,77899	0,69665
3714. Зола углей	0,7	0,02845	0,02695	0,02464	0,02172	0,01943
0333. Сероводород	0,06	0,00244	0,00231	0,00211	0,00186	0,00167
1325. Формальдегид	2,0	0,08129	0,07700	0,07039	0,06207	0,05551
1071. Фенол	4,5	0,18290	0,17324	0,15838	0,13966	0,12490

ТАБЛИЦА 2. Результаты расчётов разового значения мощности выброса ЗВ по протоколу №2, г/с

$T_г$, °С Наим.в-ва	Усредненные значения, мг/м^3	50	66	100	150	200
0301. Азот диоксид	16,4	0,67003	0,63841	0,58021	0,51163	0,45755
0337. Углерод оксид	12,5	0,51069	0,48659	0,44224	0,38996	0,34874
0330. Сера диоксид	28,6	1,16847	1,11332	1,01184	0,89223	0,79792
0303. Аммиак	3,2	0,13074	0,12457	0,11321	0,09983	0,08928
2908. Пыль неорг., содерж. двуокись кремния, в %: - 70-20	25,1	1,02547	0,97707	0,88801	0,78304	0,70027
3714. Зола углей	0,7	0,02860	0,02725	0,02477	0,02184	0,01953
0333. Сероводород	0,06	0,00245	0,00234	0,00212	0,00187	0,00167
1325. Формальдегид	2,1	0,08580	0,08175	0,07430	0,06551	0,05859
1071. Фенол	4,4	0,17976	0,17128	0,15567	0,13727	0,12276

Для оценки результатов в специализированной программе «ЭКОцентр–РРВА», в соответствии с Приказом № 273 были проведены расчеты рассеивания, которые показали, что увеличение температуры выброса снижает концентрацию загрязняющих веществ в расчетных точках, что

позволяет использовать эти мероприятия в периоды НМУ. Однако, при увеличении температуры изменятся и свойства газовоздушной смеси, что может изменить способность газа к рассеиванию в окружающей среде.

Изменение температуры выброса загрязняющего вещества может существенно влиять на динамическую вязкость газовоздушной смеси. Динамическая вязкость характеризует сопротивление газа смещению одного слоя относительно другого. Единицей измерения динамической вязкости в Международной системе единиц (СИ) является паскаль-секунда (Па·с).

Динамическая вязкость газа связана с его плотностью ρ, средней длиной свободного пути $\bar{\lambda}$, и средней скоростью молекул $\bar{v}$ соотношением (1):

$$\mu = \frac{\bar{\lambda} * \bar{v} * \rho}{3} \quad (1)$$

Средняя длина свободного пробега $\bar{\lambda}$ рассчитывается по формуле (2):

$$\bar{\lambda} = \frac{k * T}{\sqrt{2} * \pi * d^2 * p} \quad (2)$$

Где k - постоянная Больцмана, Дж/К; Т - температура, К; d - средний диаметр молекулы, м; Р – давление, Па.

Средняя скорость частиц $\bar{v}$ рассчитывается по формуле (3):

$$\bar{v} = \sqrt{\frac{8 * k * T}{\pi * m}} \quad (3)$$

Где k - постоянная Больцмана, Дж/К; Т - температура, К; m - масса молекулы, кг [3].

При увеличении температуры молекулы газа приобретают большую кинетическую энергию и начинают двигаться быстрее. Также возрастает средняя длина свободного пробега молекулы, а, следовательно, и вязкость газа возрастает.

Основным компонентом газа являются пары воды, концентрация которых составляет 94,115 – 102,236 г/м^3, концентрация прочих компонентов суммарно не превышает 1 г/м^3. В таблице 3 представлены результаты расчётов средней скорости частиц, средней длины пробега и вязкости водяного пара по формулам (1), (2), (3).

ТАБЛИЦА 3. Результаты расчётов средней скорости частиц, средней длины пробега и вязкости выброса по двум протоколам

	Первый протокол					Второй протокол				
	5 0°C	6 8°C	1 00°C	1 50°C	2 00°C	5 0°C	6 6°C	1 00°C	1 50°C	2 00°C

, м/с	6 15,4	6 32,3	6 61,3	7 04,2	7 44,7	6 15,4	6 30,5	6 61,3	7 04,2	7 44,7
, м	0 ,00018	0 ,00019	0 ,00021	0 ,00024	0 ,00027	0 ,00019	0 ,0002	0 ,00021	0 ,00024	0 ,00027
, Па* с	0 ,0037	0 ,004	0 ,0046	0 ,0055	0 ,0065	0 ,0037	0 ,004	0 ,0046	0 ,0056	0 ,0066

На основании полученных данных были построены графики зависимости динамического коэффициента вязкости газа от температуры выброса (рис.1), на которых чётко прослеживается линейная зависимость.

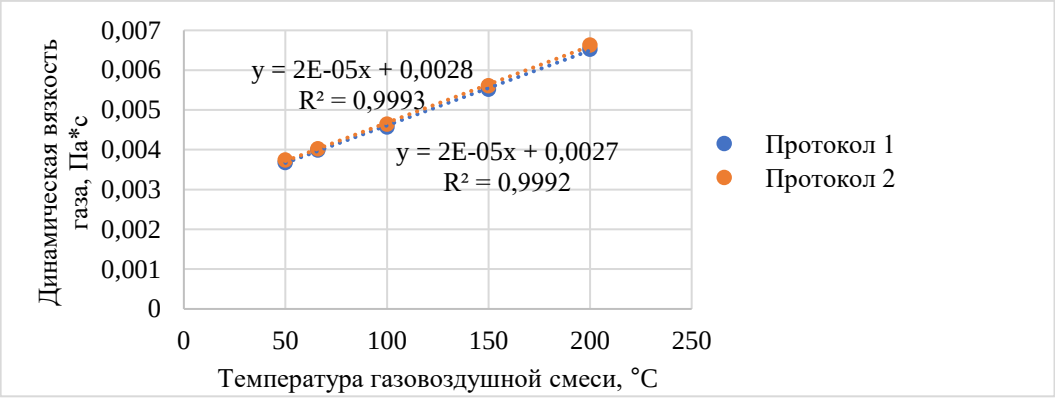


Рис.1 График зависимости динамического коэффициента вязкости от температуры выброса

Динамическая вязкость атмосферного воздуха при стандартных условиях составляет около 0,000018 Па*с, что примерно в 200 раз меньше динамической вязкости выброса. Рост температуры увеличит эту разницу до 400 раз. Такая большая разница затруднит смешивание выброса с атмосферным воздухом, что не даст рассеяться загрязняющим веществам.

Список используемых источников:

1. Приказ Минприроды России от 28 ноября 2019 года № 811 «Требования к мероприятиям по уменьшению выбросов загрязняющих веществ в атмосферный воздух в периоды неблагоприятных метеорологических условий».

2. Приказ Минприроды России от 19 ноября 2021 года № 871 «Порядок проведения инвентаризации стационарных источников и выбросов загрязняющих веществ в атмосферный воздух, корректировки ее данных, документирования и хранения данных, полученных в результате проведения таких инвентаризации и корректировки».

3. Клинских А. Ф., Меремьянин А. В., Стадная Н. П. Методические указания к работам лабораторного практикума по курсу общей физики. Молекулярная физика. Воронеж : Издательский дом ВГУ, 2016. 65 с.

Kazantseva A., Tsvetkova I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

The study of the temperature influence on amount of the emission.
The article analyzes the influence of the temperature of the pollutants release into the atmosphere on the concentration of these substances in the atmospheric air. The study was conducted by a calculated method. The object of the study is emissions from the production of mineral wool. Conclusions about the dispersion of emissions in atmospheric air were made based on the calculations of the dynamic viscosity of the emission.

Key words: emission temperature, concentration of pollutants, viscosity, water vapor.

УДК 504.3.054
ГРНТИ 87.17.15

ИССЛЕДОВАНИЕ МЕТОДА ОЦЕНКИ ВРЕДНОСТИ ПРИРОДНОЙ ПЫЛИ СЛОЖНОГО КОМПОНЕНТНОГО СОСТАВА

А. Г. Казанцева, М. В. Чурынина
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе исследован метод оценки вредности компонентов пыли на примере каменного сырья. Сырье включает в себя компоненты 2 и 3 классов опасности, которые поступают в атмосферный воздух вместе с пылью. В работе проведены расчеты критерия вредности для каменного сырья природного происхождения и расчетный эксперимент по необходимости нормирования веществ 2 и 3 классов опасности как отдельных компонентов.

кремний, алюминий, железо, пыль

Установление нормативов выбросов пыли является необходимой мерой для обеспечения безопасности и здоровья работников, а так же охраны окружающей среды. Основным компонентом выбросов пыли является диоксид кремния, который вызывает пылевой пневмосклероз [1]. Содержание свободного кремния в выбросах способно повысить фиброгенность, поэтому выделяют 3 норматива пыли по его содержанию: пыль неорганическая с содержанием SiO_2 более 70% (код 2907); с содержанием SiO_2 более 20-70% (код 2908); с содержанием SiO_2 менее 20% (код 2909). Обычно остальные компоненты, которые содержатся в выбросах помимо кремния, либо оказывают похожее воздействие, либо усиливают фиброгенность.

Однако, существуют компоненты, влияние которых, несмотря на похожее воздействие, несет существенный вред другим органам и системам. Например, алюминий оказывает влияние на обмен веществ, а железо – влияние на кровеносную систему, поэтому часто возникает вопрос о необходимости нормировать примеси как отдельный компонент [1].

Методика по расчету, нормированию и контролю выбросов загрязняющих веществ в атмосферный воздух [2] рекомендует производить оценку вредности многокомпонентной пыли и отдельных ее компонентов путем расчета оценочного критерия R_i (формула 1). Малоопасные компоненты пыли в силу их невысокой токсичности или незначительного содержания предлагается нормировать как пыль неорганическую с нормируемым содержанием диоксида кремния. Особо токсичные или превалирующие по массе компоненты должны учитываться и нормироваться отдельно [2].

$$R_i = \frac{X_i * K_i * \text{ПДК}_{\text{по}SiO_2}}{\text{ГН}_i} \quad (1)$$

где X_i – содержание i-го вещества в суммарном выбросе твердых веществ от данного источника, доли; K_i – стехиометрический коэффициент, учитывающий соотношение молекулярных масс нормируемого и фактически присутствующего в выбросе вещества, определяется по формуле 2:

$$K_i = \frac{n * M_c}{m * M_i} \quad (2)$$

где M_c – молекулярная (атомная) масса вещества, г/моль; M_i – молекулярная (атомная) масса i-го компонента, г/моль; n и m– количество молекул (атомов) в уравнениях пересчета химических формул; $ГН_i$ – гигиенический норматив (ОБУВ или ПДК) содержания компонента в атмосферном воздухе, мг/м^3; $ПДК_{noSiO2}$ – ПДК$_{с.с.}$ неорганической пыли с нормированным содержанием диоксида кремния, по одному из кодов – 2907, 2908, 2909, мг/м^3.

В качестве предмета исследования была выбрана пыль от каменного сырья. В качестве сырья рассматривались 13 видов каменных материалов: Чупинский микроклин, Нарын-Кунтинский микроклин, Талды-Курганский шпат, Карельский пегматит, Плагиоклазы, гранит месторождения «Митрофановка», ортофир месторождения «Курагино» Красноярского края, риолиты Приморья, Нефелин, аляскитанкаванский, Макванетский каолин, Белгородский мел и сподумен. Состав каменного сырья приведен в таблице 1 [3].

ТАБЛИЦА 1. Химический состав горных пород и минералов, применяемых в производстве керамики и стекла, масс.%

Материал	Среднее содержание в материале, %					
	SiO_2	TiO_2	Al_2O_3	Fe_2O_3	CaO	MgO
Чупинский микроклин	65,95	-	16,35	0,105	0,43	0,08
Нарын-Кутинский микроклин	65,27	-	19,8	0,05	0,32	0,05
Талды-Курганский шпат	67,23	0,01	18,42	0,19	0,45	0,21
Карельский пегматит	72,3	-	16,05	0,25	1,3	0,055
Плагиоклазы	62,85	-	23,5	0,085	4,1	0,01
Гранит месторождения "Митрофановка"	76,8	0,08	12,33	1,05	1,5	0,14
Ортофир месторождения "Курагино" Красноярского края	67,7	0,3	14,6	4,4	1,12	0,8
Риолиты Приморья	77	0,055	12,35	0,3	0,45	0,55
Нефелит	45,2	-	32,3	0,9	0,2	-
Аляскитанкаванский, концентрат	76,1	-	12,7	0,19	1,28	0,52
Макванетскийкволин	58,2	0,6	28,3	1,4	0,78	0,72
Белгородский мел	1,64	-	0,6	0,17	54,4	0,12
Сподумен	64,4	-	27,7	0,5	0,1	6,05

Оценка необходимости отдельного учета и нормирования компонентов пыли в зависимости от рассчитанного коэффициента R_i и класса опасности компонентов приведена в таблице 4 П.1 Приложения 4 в [2]. Результаты расчетов для каждого компонента сырья представлены в таблице 2.

ТАБЛИЦА 2. Результаты расчетов коэффициентов R_i и K_i

Материал			Чупинский микроклин	Нарын-Кутинский микроклин	Талды-Курганский шпат	Карельский пегматит	Плагиоклазы	Гранит "Митрофановка"
Компоненты	ГН	K_i	Коэффициент R_i					
SiO_2	0,02	2,14	7,066	6,993	7,203	3,873	6,734	4,114
TiO_2	5	1,67	-	-	0,0000033	-	-	0,000013
Al_2O_3	0,01	1,89	3,088	3,74	3,479	1,516	4,439	1,165
Fe_2O_3	0,04	1,43	0,004	0,002	0,007	0,004	0,003	0,019
CaO	0,3	1,40	0,002	0,001	0,002	0,003	0,019	0,004
MgO	0,05	1,67	0,003	0,002	0,007	0,001	0,0003	0,002

Материал	Ортофир "Курагино"	Риолиты Приморья	Нефелит	Аляскитанканакавский, концентрат	Макванетскийкволин	Белгородский мел (2909)	Сподумен
Компоненты	Коэффициент R_i						
SiO_2	7,254	4,125	4,843	4,077	6,236	0,264	6,9
TiO_2	0,0001	0,00001	-	-	0,0002	-	-
Al_2O_3	2,758	1,166	6,101	1,199	5,346	0,17	5,232
Fe_2O_3	0,157	0,005	0,032	0,003	0,05	0,009	0,018
CaO	0,006	0,001	0,001	0,003	0,004	0,381	0,001
MgO	0,027	0,009	-	0,009	0,024	0,006	0,202

Код пыли для расчета оценочного критерия R_i присваивался, исходя из состава каменного сырья. Из него видно, что пыль для разных материалов нормируется разными способами. Для большинства минералов пыль нормируется по коду 2908 – пыль неорганическая с содержанием диоксида кремния 20-70%; пыль Белгородского мела нормируется по коду 2909 – пыль неорганическая с содержанием диоксида кремния менее 20%; Карельский пегматит, гранит месторождения «Митрофановка», риолиты Приморья, аляскит анкаванский – по коду 2907 – пыль неорганическая с содержанием диоксида кремния более 70%.

Исходя из анализа результатов, для нормирования выбросов были выбраны следующие вещества: диоксид кремния и оксид алюминия. По рассчитанному критерию R_i отдельное нормирование оксида железа, относящегося к 3 классу опасности, не требуется.

Был проведен расчетный эксперимент, который показал, в каких случаях необходимо нормировать вещества 2 и 3 классов опасности как отдельные компоненты. Путем подбора было определено среднее содержание оксида алюминия в каменном сырье, при котором учет и нормирование данного компонента будет производиться суммарно с диоксидом кремния. Затем этим же путем было определено среднее содержание оксида железа в каменном сырье, при котором учет и нормирование данного компонента будет производиться отдельно от диоксида кремния. Результаты представлены в таблице 3.

ТАБЛИЦА 3. Результаты расчетного эксперимента

Материал	Al_2O_3		Fe_2O_3	
	Содержание, %	R_i	Содержание, %	R_i
Чупинский микроклин	0,5	0,094	28	1
Нарын-Кутинский микроклин	0,5	0,094	28	1
Талды-Курганский шпат	0,5	0094	28	1
Карельский пегматит	1,05	0,099	56	1
Плагиоклазы	0,5	0,094	28	1
Гранит месторождения "Митрофановка"	1,05	0,099	56	1
Ортофир месторождения "Курагино" Красноярского края	0,5	0,094	28	1
Риолиты Приморья	1,05	0,099	56	1
Нефелит	0,5	0,094	28	1
Аляскитанкаванский, концентрат	1,05	0,099	56	1
Макванетскийкволин	0,5	0,094	28	1
Белгородский мел	0,35	0,999	18,67	1,0002
Сподумен	0,5	0,094	28	1

Таким образом, для суммарного нормирования оксида алюминия с диоксидом кремния, содержание Al_2O_3 в составе сырья, пыль которого

нормируется по коду 2908, должно быть менее 0,5%, по коду 2909 – менее 0,35% и по коду 2907 – менее 1,05%.

Для отдельного нормирования оксида железа, содержание Fe_2O_3 в составе сырья, пыль которого нормируется по коду 2908, должно быть более 28%, по коду 2909 – более 18,67% и по коду 2907 – более 56%.

Содержание алюминия в почвообразующих породах достигает 23,5%, а железа всего лишь 9,4% [4]. Расчеты показали, что нормирование железа как отдельного компонента у пыли природного происхождения нецелесообразно, при этом в связи с высоким содержанием алюминия в природном сырье, этот компонент необходимо нормировать отдельно от смеси.

Список используемых источников:

1. Вредные химические вещества. Том 1: Элементы I-VIII групп периодической системы и их неорганические соединения. Радиоактивные вещества /под ред. В. В. Уйба и др. СПб. : ЛА «Профессионал», 2015. 1336 с.

2. Методическое пособие по расчету, нормированию и контролю выбросов загрязняющих веществ в атмосферный воздух. СПб. : ОАО «НИИ Атмосфера», 2012. 224 с.

3. Новый справочник химика и технолога. Сырье и продукты промышленности органических и неорганических веществ. СПб. : НПО «Профессионал», 2002. 988 с.

4. Самофалова И. А. Химический состав почв и почвообразующих пород Пермь. ФГОУ ВПО «Пермская ГСХА», 2009.

Kazantseva A., Churynina M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Study of the method of assessing the harmfulness of natural dust with the complex component composition.

The article presents the results of the study of the method of assessing the harmfulness of dust components on the example of stone raw materials. Raw materials include components of hazard classes 2 and 3, which enter the atmospheric air together with dust. Calculations of the hazard criterion for natural stone raw materials and a computational experiment on the necessity of rationing substances of hazard classes 2 and 3 as separate components are executed in the work.

Key words: silicium, aluminum, ferrum, dust.

УДК 504.53.052
ГРНТИ 34.35.51

ОПРЕДЕЛЕНИЕ ТОКСИЧНОСТИ ПОЧВ В ПАРКЕ АЛЕКСАНДРИНО МЕТОДОМ БИОТЕСТИРОВАНИЯ

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

Проведено исследование почвенного покрова методом биотестирования в парке Александрино Кировского района Санкт-Петербурга. Установлена степень токсичности для пробных площадок. Основными причинами загрязнения почвенного покрова являются наличие рядом крупных автомагистралей, несанкционированное разведение костров, а также образование стихийных свалок.

степень токсичности, Кировский район Санкт-Петербурга, почвенный покров.

Парк Александрино находится в Санкт-Петербурге и является одним из крупнейших объектов рекреации Кировского района [1]. Однако в последние годы жители жалуются на неблагоприятное экологическое состояние парка.

В рамках дипломной работы по оценке экологического состояния парка Александрино были проведены исследования воздушной, водной и почвенной среды; растительного покрова и животного мира. В рамках статьи рассматривается исследование почвенного покрова методом биотестирования.

В качестве тест культуры использовались семена высших растений пшеницы (Triticum vulgare L). Процедура биотестирования проводилась в лаборатории методов реабилитации техногенных ландшафтов НИЦЭБ РАН.

Определение токсичности почв основано на изменении всхожести семян (N_1), длины корня (N_2) и длине колеоптиля (первого листа) (N_3) проростков растений по сравнению с контрольной пробой, которая не подвергалась техногенному воздействию (таблица 1).

ТАБЛИЦА 1. Критерии степени токсичности техногенно–загрязненных почв

Степень токсичности	Степень изменения всхожести семян по сравнению с контролем, N_1, %	Степень изменения длины корня и колеоптиля по сравнению с контролем, N_2, %
V – практически не токсичные	$0 < N_1 \leq 20$	$0 < N_2 \leq 20$
IV – малотоксичные	$0 < N_1 \leq 20$	$20 < N_2 \leq 50$
III – умеренно токсичные	$20 < N_1 \leq 70$	$50 < N_2 \leq 70$
II – опасно токсичные	$70 < N_1 < 100$	$70 < N_2 < 100$
I – высоко опасно токсичные	$N_1 = 100$	$N_2 = 100$

Отбор проб почв на территории парка Александрино производился в июле 2023 года. Для каждой пробы закладывалась пробная площадка размером не менее 10 на 10 м. С каждой пробной площадки на глубине 0–20 см отбирались пять точечных проб методом «конверта», то есть четыре точечные пробы по краям и одна посередине площадки [2]. С каждой точечной пробы отбиралось 0,5 кг почвы, которые были очищены от корней растений и упакованы в полиэтиленовые пакеты. Таким образом, было отобрано 2,5 кг почвы с каждой пробной площадки. Всего было отобрано 6 проб в различных ландшафтных условиях (рис. 1): 1 и 3 площадки – в 10 м от автомобильной дороги; 2 и 4 – в глубине лесного массива; 5 – в долине реки, около места, где устраивают пикники; 6 – на берегу пруда р. Новая. Также была отобрана контрольная проба (К), которая не подвергалась техногенному воздействию и имела схожий тип почвы.

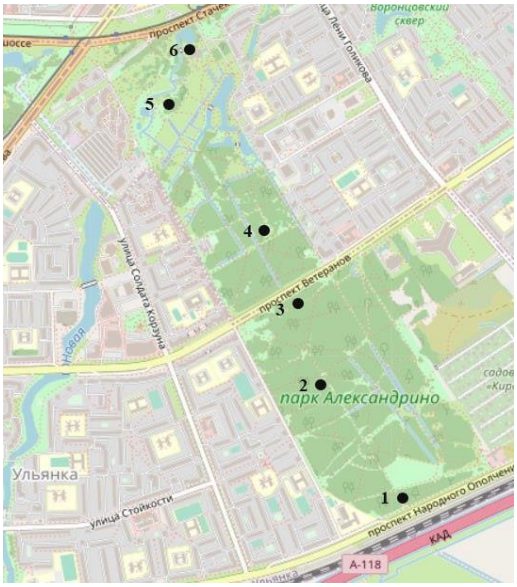


Рис. 1. Карта-схема участков отбора почвенных проб в парке

В течение недели точечные пробы почвы с каждой пробной площадки высушивались естественным путем, а затем, перемешиваясь, соединялись в объединенную пробу массой более 1 кг.

Высушенные объединенные пробы растирались в фарфоровой ступке и просеивались через сито с отверстиями диаметром 1–2 мм.

Далее, в чашки Петри диаметром 10 см вносились пробы почв слоем около 1 см по три повторности для контрольной и каждой проверяемой пробы. В каждой чашке поверхность почвы выравнивалась и увлажнялась дистиллированной водой. Семена пшеницы, после сортировки на предмет повреждений, равномерно высаживались в чашку Петри по 20 семян на глубину 2 мм. Затем чашки закрывались крышками. Учет результатов проводился на четвертый день [3].

Таким образом, в эксперименте участвовало 18 чашек Петри для проверяемых проб и 3 чашки для контрольной. Всего было высажено 420 семян пшеницы.

В день измерения растения извлекались из субстрата, и корни промывались в воде. Подсчитывалось количество проросших растений. Линейкой измерялась длина корня и колеоптиля. Далее, рассчитывались средние значения для каждой пробы, в том числе всхожесть – доля проросших растений.

Степень изменения всхожести, длины корня и колеоптиля (N_i, %) производятся по формуле (1):

$$N_i = \frac{\bar{М}т - \bar{М}к}{\bar{М}к} * 100\,, \qquad (1)$$

где: N_i – критерий определения токсичности (по всхожести, по длине корня или колеоптиля);

$\bar{М}к$ – среднее значение из трех параллельных определений в контрольном ряду;

$\bar{М}т$ – среднее значение из трех параллельных определений в испытуемом ряду.

Ошибка среднего арифметического (S) рассчитывается как среднеквадратичное отклонение всех средних результатов измерений. На основе значений ошибки проводят расчет показателя достоверности (t), который позволяет оценить значимость различий между контрольной и проверяемыми пробами. В данном случае коэффициент Стьюдента (t_{St}) равен 2,57. Если $t \geq t_{St}$, то выявленные различия достоверны, а не случайны. Если $t < t_{St}$, то выявленные различия недостоверны.

Результаты биотестирования представлены в таблицах 2–4.

ТАБЛИЦА 2. Результаты биотестирования почв по всхожести семян

№ пробы почв	Всхожесть				
	Среднее арифметическое значение показателя в параллельных измерениях, %	Критерий существенности разности, t	Ошибка среднего арифметического, S	Разница значения показателя с контрольным вариантом, % N_1	Степень токсичности
К	95,0	-	1,5	-	-
1	55,0	3,49	11,36	42,11	III (умеренно токсичные)
2	86,67	2,07	3,75	8,77	IV (малотоксичные)
3	43,33	4,37	11,74	54,39	III (умеренно токсичные)
4	93,33	0,41	3,75	1,76	V (практически не токсичные)

5	30,00	8,57	7,43	68,42	III (умеренно токсичные)
6	48,33	4,48	10,30	49,13	III (умеренно токсичные)

ТАБЛИЦА 3. Результаты биотестирования почв по длине корня

№ пробы почв	Длина корня				
	Среднее арифметическое значение показателя в параллельных измерениях, %	Критерий существенности разности, t	Ошибка среднего арифметического, S	Разница значения показателя с контрольным вариантом, % N_1	Степень токсичности
К	30,1	-	2	-	-
1	11,47	5,95	2,41	61,89	III (умеренно токсичные)
2	18,48	4,46	1,67	38,6	IV (малотоксичные)
3	11,27	3,90	4,39	62,56	III (умеренно токсичные)
4	20,42	2,85	2,75	32,16	IV (малотоксичные)
5	4,92	10,64	1,26	83,65	II (опасно токсичные)
6	12,73	3,89	3,99	57,71	III (умеренно токсичные)

ТАБЛИЦА 4. Результатов биотестирования почв по длине колеоптиля

№ пробы почв	Длина колеоптиля				
	Среднее арифметическое значение показателя в параллельных измерениях, %	Критерий существенности разности, t	Ошибка среднего арифметического, S	Разница значения показателя с контрольным вариантом, % N_1	Степень токсичности
К	21,6	-	1,6	-	-
1	6,88	7,50	1,14	68,15	III (умеренно токсичные)
2	14,85	3,54	1,04	31,25	IV (малотоксичные)
3	7,68	4,92	2,33	64,4	III (умеренно токсичные)
4	15,83	2,80	1,29	26,71	IV (малотоксичные)

5	3,55	10,20	0,75	83,56	II (опасно токсичные)
6	7,63	6,25	1,56	64,68	III (умеренно токсичные)

В результате, малотоксичными оказались территории, которые расположены в глубине лесного массива (пробные площадки №2 и №4). Области парка рядом с автомобильными дорогами (№1, №3) имеют умеренную степень токсичности, потому что расположены на открытом участке, где происходит осаждение и накопление в почву аэрозольных частиц, летящих от автотранспорта. Имеет умеренную степень токсичности береговая часть пруда (№6), на которую оказывает влияние проспект Стачек, расположенный неподалеку. Опасно токсичной оказалась парковая зона в долине реки Новая (№5), потому что на этой территории разводят открытый огонь с использованием мангалов и устраивают пикники, что приводит к образованию несанкционированных свалок.

Таким образом, применение метода биотестирования показало, что большая часть парка имеет малотоксичную и умеренную степень токсичности.

Список используемых источников:

1. Генеральный план Санкт-Петербурга. [Электронный ресурс]. URL: https://portal.kgainfo.spb.ru/GenPlan/Map/ (дата обращения: 01.10.2023).

2. ГОСТ Р 58595–2019. Почвы. Отбор проб. Введ. 01.01.2020. М. : Стандартинформ, 2019.

3. Методика выполнения измерений всхожести семян и длины корней проростков высших растений для определения токсичности техногенно–загрязненных почв: ФР.1.39.2006.02264. М. : Акварос, 2009. 19 с.

Konopleva A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Determination of soil toxicity in Alexandrino Park using biotesting.

A study of the soil cover by the method of biotesting was carried out in the Alexandrino Park of the Kirovsky district of St. Petersburg. The degree of toxicity for the test sites has been established. The main causes of soil pollution are the presence of major highways nearby, unauthorized bonfires, as well as the formation of spontaneous landfills.

Key words: degree of* toxicity, *Kirovsky district of St. Petersburg, soil cover.

УДК 57.033
ГРНТИ 87.26.25

РАКОВЫЕ ОЗЕРА ВЫБОРГСКОГО РАЙОНА ЛЕНИНГРАДСКОЙ ОБЛАСТИ В ИСТОРИЧЕСКОЙ ПЕРСПЕКТИВЕ СЕГОДНЯ И ЗАВТРА

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

В данной научной статье рассмотрен вопрос об антропогенной эвтрофикации, ее скоростях и последствиях на примере Раковых озер Ленинградской области Выборгского района. Актуальность данной проблемы обусловлена не только сокращением запасов водных ресурсов из-за заболачивания водоемов, но и устойчивостью сформированных уникальных озерных экосистем. В результате обзора и анализа литературных источников с использованием картографического метода и теоретического моделирования представлены результаты прогноза сокращения площади зеркала Ракового озера, отраженные в графиках изменения площадей, а также возможной проблемы, связанной с миграцией птиц.

эвтрофикация, площадь зеркала, Раковые озера, заказник, миграция птиц, Выборгский район

Процесс эвтрофикации – это повышение биологической продуктивности водных объектов в результате накопления в воде биогенных элементов [1].

Это естественный процесс, протекающих во всех водоемах, и в природных условиях он занимает 100-1000 лет, но его скорость может увеличиваться в несколько раз при воздействии человека. Антропогенное влияние может проявляться в разнообразных формах (рис. 1).

Рис. 1. Виды эвтрофикации

Определение типа трофности озера, являющегося сложной экосистемой, важно для оценки его состояния и планирования мероприятий по его

использованию и восстановлению. Выделяют 3 типа продукционных свойств водного объекта: эвтрофный, мезотрофный и олиготрофный (рис. 2) [2].

Рис. 2. Уровни трофности

В Выборгском районе большая часть водоемов обладает мезотрофным уровнем, в то время как Раковые озера относятся к эвтрофному уровню. С начала 1976 года эти озера включены в состав одноименного природного заказника, что гарантирует отсутствие промышленной и сельскохозяйственной деятельности в этом районе, способной оказывать влияние на состояние озер [3]. Анализ истории Карельского перешейка показывает, что до прорыва Лосевской протоки в 1857 году, река Вуокса текла на северо-восток от Лосево и образовывала озеро Балахновское. После прорыва протоки в 1857 году, Вуокса стала течь через Суходольское озеро и реку Бурная, направляясь в Ладогу. Этот процесс привел к снижению уровня озера Вуокса на 2-3 метра и обмелению района, включая Раковые озера [4], из-за чего и был запущен процесс заболачивания.

Используя части карт Ф.Ф. Шуберта (1853-1863гг.) и OpenStreetMap был составлен рис. 3, на котором отражено изменение площади зеркала с 1853 по 2023 гг.

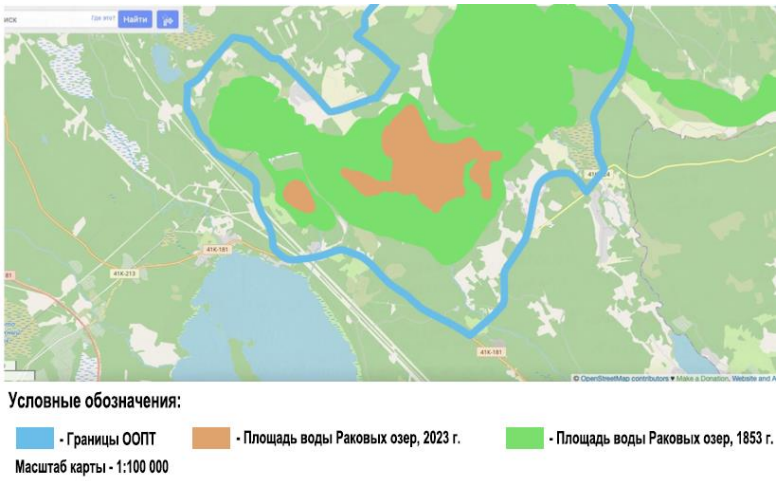


Рис. 3. Изменение площади зеркала Раковых озер с 1853 по 2023 гг.

Была составлена тенденция изменения площади в процентах по двум временным срезам 1853 и 2023 гг. (рис. 4).

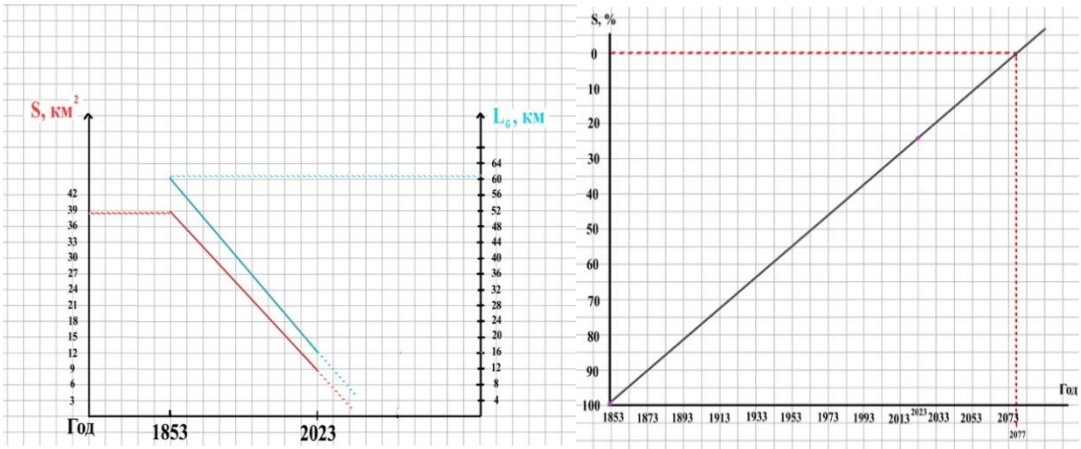


Рис. 4. Графики изменения площади Большого Ракового озера в м^2, %

Принимая во внимание, что за двадцатилетний период площадь уменьшалась на 3-4 м^2, то скорость сокращения водного зеркала - 0,17 м^2/год. При текущей скорости, если она сохранится, можно предположить, что озеро полностью исчезнет в течение следующих 50-60 лет.

В соответствии с результатами анализа сезонных миграций птиц, представленными в работе "Сезонные миграции птиц», была составлена карта миграционного пути через Карельский перешеек [5].

На этой карте видно, что перелетные птицы активно используют Раковые озера как место остановки в своем миграционном маршруте как весной, так и осенью (рис. 5).

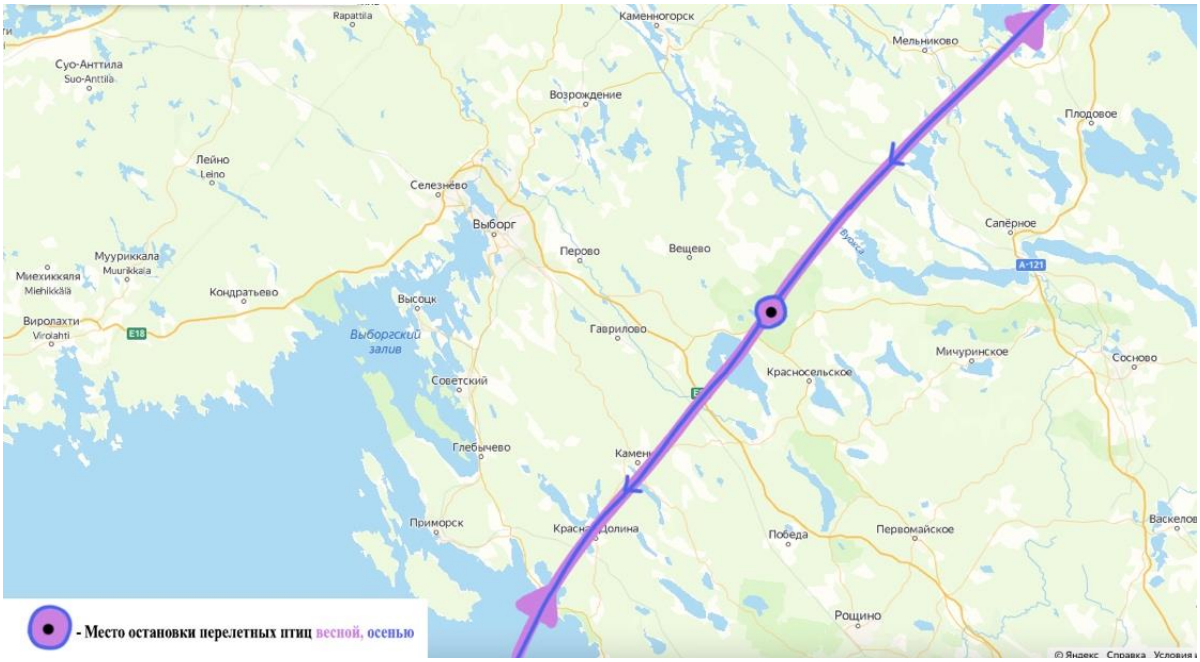


Рис. 5. Миграционный путь и место остановки на Раковых озерах перелетных птиц через Карельский перешеек

Маршрут, который птицы используют более 100 лет, находится на достаточном расстоянии от городов Выборг и Санкт-Петербург, что существенно снижает уровень возможных воздействий и беспокойства.

Присутствие Раковых озер на Карельском перешейке, образованных в результате естественного обмеления и зарастания озер, играет важнейшую роль в обеспечении территорией для различных видов птиц, особенно перелетных. Этот природный заказник создает идеальные условия для существования, а также предоставляет необходимые ресурсы в периоды миграций, способствуя выживанию пернатых обитателей. Также важным фактором является наличие подходящих мест для гнездования, таких как камышовые заросли и мелководье [6].

Изменения в природном водном режиме озерно-речной системы оказали воздействие на структуру Раковых озер, превратив их в безопасное и удобное пристанище для перелетных птиц. Однако сегодня возникает угроза исчезновения этой ключевой стоянки для птиц, что требует дальнейших исследований и внимания в сфере охраны природы.

Список используемых источников:

1. Использование и охрана вод: ГОСТ 17.1.01-77.: постановление Государственного комитета стандартов Совета Министров СССР от 16 сентября 1977 г. № 2237 // МежГосстандарт, 1986. 31 с.

2. Науменко М. А. Эвтрофированис озёр и водохранилищ : учеб. пособие. СПб. : РГГМУ, 2007. 100 с.

3. Особо охраняемые природные территории ЛО [Электронный ресурс] / Раковые озера URL: https://ooptlo.ru/rakovyie-ozera.html (дата обращения 29.10.23)

4. Озерецковский Н. Я. Путешествие по озерам Ладожскому и Онежскому. Петрозаводск : Карелия, 1989. 53 с.

5. Промптов А. Н. Сезонные миграции птиц. М. – Л. : Академия наук, 1941. 1383 с.

6. Мальчевский А. С. и др. Птицы Ленинградской области // Русский орнитологический журнал. 2021. Т. 30, N 2100. С. 3713-3797. – EDN WYYXKF

Kocherezhkina U.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Cancer lakes of the vyborg district of the leningrad region in the historical perspective of today and tomorrow.

This scientific article examines the issue of anthropogenic eutrophication, its rates and consequences using the example of Rakovyye ozera of the Leningrad Region, Vyborg District. The relevance of this problem is due not only to the reduction in water resources, but also to the formation of unique lake ecosystems. As a result of a review and analysis of literature sources using analysis, cartographic method and theoretical modeling, the results of the forecast of a decrease in the lake surface area, reflected in graphs of area changes, as well as a possible problem associated with bird migration are presented.

Key words: eutrophication, water surface area, Rakovyye ozera, nature reserve, bird migration, Vyborg district.

УДК 504.055:504.064
ГРНТИ 87.55.33

СРАВНЕНИЕ ИЗМЕРИТЕЛЬНЫХ ВОЗМОЖНОСТЕЙ ПРИБОРОВ И НОВЫЕ РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ ПРОБЛЕМ ЭЛЕКТРОМАГНИТНОГО ЗАГРЯЗНЕНИЯ

А. Н. Логиновская, В. И. Стурман
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Изложены основные результаты исследований кафедры экологической безопасности телекоммуникаций СПбГУТ в области электромагнитной экологии в 2023 г. – сопоставления результатов измерений двумя приборами, и работ съемочно-картографического характера в г. Астрахань и Великий Новгород.

картографирование электромагнитных полей, мониторинг электромагнитных полей, Астрахань, Великий Новгород

В целях исследования электромагнитных полей промышленной частоты на кафедре экологической безопасности телекоммуникаций СПбГУТ в настоящее время используются приборы двух типов: Gigahertz Solutions ME 3830 B M/E Analyser, и ВЕ-50и. В целях оценки сопоставимости результатов, полученных разными приборами, выполнена серия одновременных измерений в одних и тех же точках пространства. Результаты представлены в таблице 1.

ТАБЛИЦА 1. Результаты одновременных измерений напряженности электрического поля (Е) и магнитной индукции (М) двумя приборами

Место измерения	Gigahertz Solutions ME 3830 B M/E Analyser		ВЕ-50и	
	Е, в/м	М, нТл	Е, в/м	М, нТл
СПбГУТ, ауд. 401/1	9	5	11	4
СПбГУТ, к. 1, 4 этаж, сред. рекреация, у электрощитка	3,3	230	3	250
СПбГУТ, к. 1, 4 этаж, сред. рекреация, у серверного. шкафа	4,5	1300	6	1400
Парковка у СПбГУТ	3	4	4,5	4
Южные ворота территории СПбГУТ	4	9	5,2	4,3
Остановка «Университет телекоммуникаций»	2	4	3,6	3,5
Пр. Большевиков, 21, у маг. «Пятерочка»	2	9	4	3,5
Перекресток пр. Большевиков и ул. Дыбенко	9	120	9,8	4,3
У входа в д/с 103, аномалия, Н=1,8 м	4	620	2,8	451
У входа в д/с 103, аномалия, у земли	5	1260	3,15	1440
У ст. метро Ул. Дыбенко	2	20	3,6	3,1
Средние величины	4,35	325,5	5,15	324,3
Разница в %%	18,4	0,6		
Коэффициенты корреляции	0,88	0,99		

Как видно из приведенной таблицы, несмотря на существенные расхождения

в отдельных случаях, в целом результаты сопоставления укладываются в общепринятые требования к воспроизводимости результатов измерений и могут быть оценены как позитивные, не создающие препятствий для дальнейших исследований с использованием данных приборов.

Новые исследования были выполнены в 2023 г. в гг. Астрахань и Великий Новгород, с использованием прибора Gigahertz Solutions ME 3830 B M/E Analyser. Методика измерений была аналогичной использованной ранее: на высоте 1,8 м от поверхности земли, а при уточнении особенностей распределения аномальных значений - и на других уровнях, по возможности в условиях однородного характера использования территории и застройки. Исследования в двух указанных городах, расположенных в разных природных условиях, принесли результаты, наглядно отражающие их влияние на уровни электромагнитных полей и их пространственное распределение. Известно [1], что магнитная индукция определяется нагрузкой на системы электроснабжения.

В обоих городах значимые величины напряженности электрических полей (более 1-3 в/м) были отмечены только вблизи высоковольтных линий. Превышений действующих нормативов ПДУ согласно СанПиН 1.2.3685-21 [2] ни по напряженности магнитных полей, ни по магнитной индукции, в обоих городах не выявлено.

Магнитные поля промышленной частоты в Астрахани характеризуются широким распространением значений, превышающих ориентировочный безопасный уровень согласно зарубежных оценок – 0,2-0,4 нТл [3]. Повышенными значениями магнитной индукции характеризуются рынки, довольно многочисленные в центральной части Астрахани и малоэтажная историческая застройка. Непосредственно видимыми и подтверждаемыми приборными замерами источниками магнитных полей являются широко распространенные в городе провода воздушных линий электроснабжения, буквально опутывающие здания и целые улицы, и нередко опасно провисающие. Наличие или отсутствие проводов – решающий фактор пространственного распределения магнитных полей в Астрахани, намного более значимый, чем типы использования земель и застройки. Скопления проводов отсутствуют только на ряде центральных улиц, и электромагнитная обстановка там существенно лучше. В целом, из изученных нами городов Астрахань может быть оценена как наиболее проблемный в отношении электромагнитного загрязнения.

В то же время из-за близкого залегания минерализованных (следствие засушливого климата) грунтовых вод в этом городе практически отсутствуют кабели подземной прокладки. Астрахань стала первым из изученных нами городов, где не было встречено ни одной обусловленной кабелями приземной аномалии магнитного поля.

Магнитные поля промышленной частоты в Великом Новгороде характеризуются относительно невысокими показателями магнитной индукции, лишь локально превышающими величину 100 нТл.

Повышенными значениями характеризуются историческая и частная усадебная застройка, где есть несоответствие между созданной десятилетия назад электропроводкой, и нагрузками на нее от современной бытовой и иной техники. Тем не менее, значение, достигающее ориентировочного безопасного уровня 0,2-0,4 нТл [3] встречено лишь в одной точке, в единственной выявленной наземной аномалии кабельного характера. Свойственное Великому Новгороду близкое залегание грунтовых вод также не способствует подземной прокладке. В целом, электромагнитная ситуация в Великом Новгороде может быть оценена как благополучная, и в этом отношении Великий Новгород похож на другой изученный ранее [4] город-музей – г. Пушкин (Пушкинский район Санкт-Петербурга).

Список используемых источников:

1. Довбыш В. Н., Маслов М. Ю., Сподобаев Ю.М. Электромагнитная безопасность элементов энергетических систем. Самара : ООО «ИПК «Содружество», 2009. 198 с.

2. СанПиН 1.2.3685-21 "Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания». М. : 2021. 469 с.

3. National precautionary policies on magnetic fields from power lines in Belgium, France, Germany, the Netherlands and the United Kingdom. RIVM Report 2017-0118. DOI 10.21945/RIVM-2017-0118. Pp. 56.

4. Стурман В. И. Пространственное распределение электромагнитных полей промышленной частоты в городе Пушкин (Санкт-Петербург) // Известия Русского географического общества, 2019. Т. 151, Вып. 6. С. 58-68.

Sturman V., Loginovskaya A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Comparison of measuring capabilities of devices and new results of the study of electromagnetic pollution problems.

The main results of research of the Department of Environmental Safety of Telecommunications of St. Petersburg State University in the field of electromagnetic ecology in 2023 are presented – comparison of measurement results with two instruments, and survey and cartographic work in Astrakhan and Veliky Novgorod.

Key words: mapping of electromagnetic fields, monitoring of electromagnetic fields, Astrakhan, Veliky Novgorod.

УДК 504.055
ГРНТИ 87.55.37

ГЕОИНФОРМАЦИОННОЕ КАРТОГРАФИРОВАНИЕ ЭЛЕКТРОМАГНИТНЫХ ПОЛЕЙ ОСТРОВА ДЕКАБРИСТОВ САНКТ-ПЕТЕРБУРГА

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

Выполнено исследование пространственного распределения значений напряженности электрических полей и магнитной индукции промышленной частоты на территории острова Декабристов Санкт-Петербурга. Установлено, что превышений гигиенических нормативов не выявлено, однако, практически все значения магнитной индукции превышают примерный безопасный уровень 0,3-0,4 мкТл, подтвержденными Всемирной Организацией Здравоохранения. Особенно аномальные величины магнитной индукции встречаются в местах прокладки подземных кабелей. Для наглядности распределения уровней электромагнитных полей и выявления наиболее опасных участков на основе полученных результатов измерений были составлены карты интерполяции.

электромагнитные поля, промышленная частота, электрические поля, магнитные поля, напряженность электрического поля, магнитная индукция, картографирование, аномалии магнитного поля, остров Декабристов, Санкт-Петербург

Развитие промышленности и технологий в 19-20 веках привело к увеличению числа электрических устройств и оборудования, используемых в различных сферах. Однако, это развитие также привело к возникновению серьезной проблемы – электромагнитного загрязнения окружающей среды искусственными электромагнитными полями, в числе которых существенную роль играют электромагнитные поля промышленной частоты (50 Гц) в городских средах.

Предметом данного исследования является пространственное распределение фактических уровней электрических и магнитных полей промышленной частоты в пределах территории острова Декабристов в Санкт-Петербурге. Выбор острова Декабристов, как места проведения исследования, обусловлен повышенной заинтересованностью в связи с градостроительной разнородностью территории и наличием большого количества объектов электроснабжения. Кроме того, проведение подобных исследований на данной территории в открытых источниках найдено не было.

В рамках проведенного исследования был использован метод прямых инструментальных измерений в конкретных заранее привязанных в пространстве точках, с учетом особенностей исследуемой местности.

В качестве геоинформационной системы для расстановки точек измерений и дальнейшей геообработки полученных данных использовалась программа ArcMap 10.8.2. Так, в период с конца марта по апрель по

заданному маршруту были выполнены измерения показателей ЭМП в 164 точках.

Высота, на которой производились измерения, составляла 1,8 метра от поверхности земли, а для получения более точной информации о распределении аномальных значений, были проведены измерения прямо на поверхности земли. Также, согласно МР 4.3.0177-20 «Методика измерения электромагнитных полей промышленной частоты 50 Гц на селитебной территории» [1] измерения от подстанций, расположенных на исследуемой территории выполнялись на расстоянии 0,5 м от стен здания ПС-104 110 кВ Уральская и ограждения ПС 330 кВ Василеостровская.

Итак, пространственный анализ показателей электрических полей выполнялся методом интерполяции. Выявленные аномальные значения по магнитной индукции, обусловленных кабельными линиями и точки измерения у подстанций отмечались на карте отличающимися значками и при интерполировании исключались. Составленные карты пространственного распределения напряжённости электрических полей и магнитной индукции представлены на рис. 2, 3.

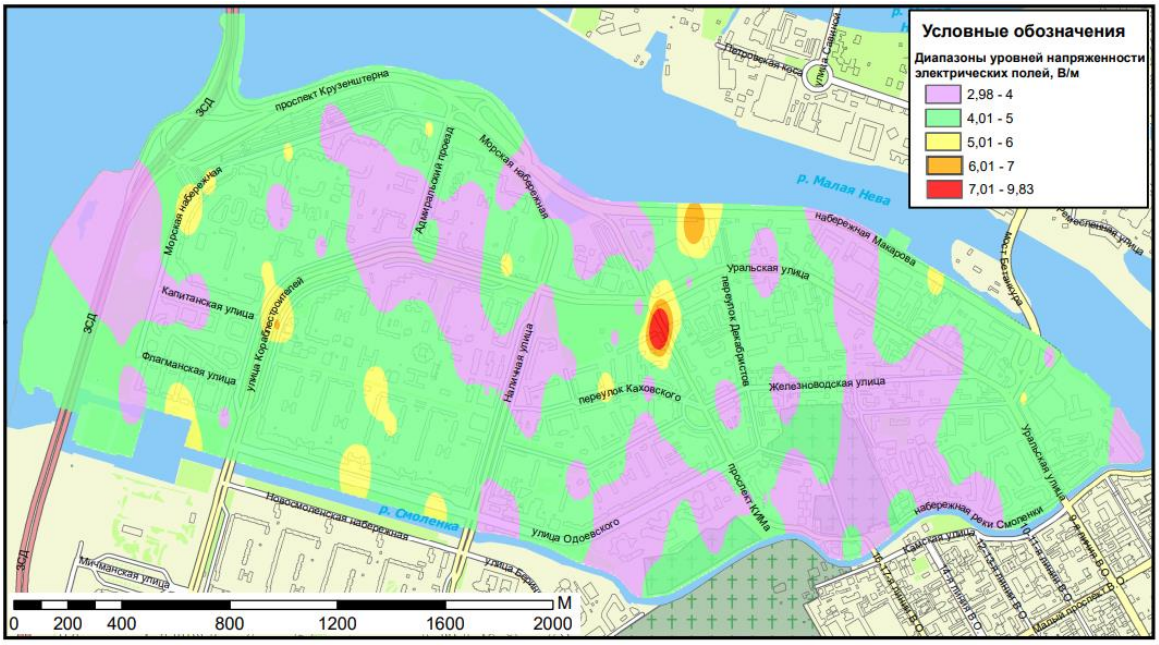


Рис. 2. Интерполяция электрических полей острова Декабристов Санкт-Петербурга

Из рис. 2 видно, что уровни напряженности электрических полей на острове Декабристов характеризуется относительно невысокими значениями и колеблются в пределах от 2 В/м до 10 В/м. Максимальные значения явно видны на набережной Макарова с значением 6,93 В/м и на проспекте КИМа с значение 9,83 В/м. Первый показатель обусловлен с рядом происходящими строительными работами, где располагаются мощные трансформаторы, строительная техника и другое электрооборудование. Второе значение обусловлено присутствием аппарата по продаже воды, для работы которых

устанавливаются электрошкафы, которые значительно генерируют электромагнитные излучения.

Так, согласно СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания» [2] ни в одной из точек измерений превышений нормативным значениям уровней напряженности электрических полей промышленной частоты на обследуемой не обнаружено. А именно, 1 кВ/м на территории зоны жилой застройки. Таким образом, ситуация с напряжённостью электрического поля на острове Декабристов Санкт-Петербурга является благополучной для населения.

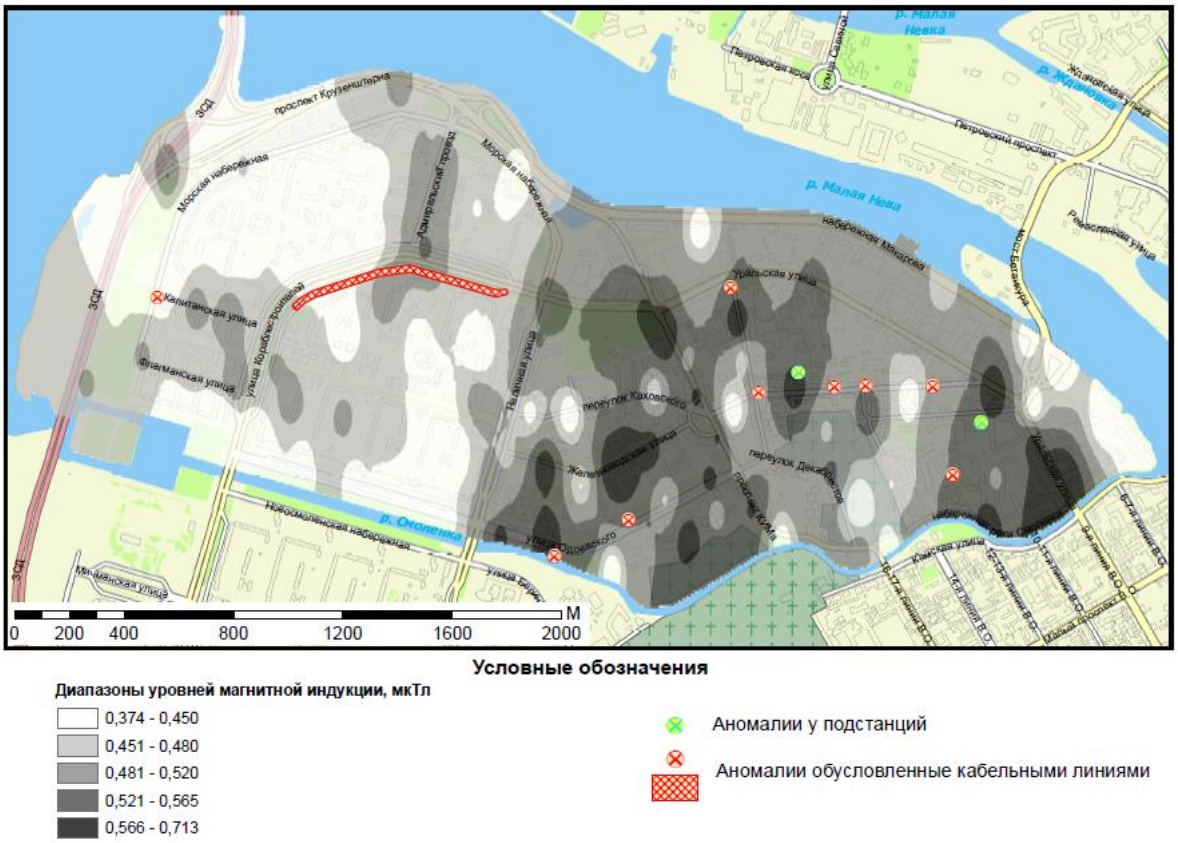


Рис. 3. Интерполяция магнитной индукции острова Декабристов Санкт-Петербурга

Как видно из рис. 3, значения магнитной индукции изменяются в пределах от 0,374 до 0,713 мкТл, за исключением аномальных значений, приуроченных к кабельным линиям и подстанциям. Отчетливо заметно, что наименьшие значения магнитной индукции приходятся на западную часть территории, которая характеризуется жилой зоной с однородной застройкой многоэтажных домов, построенных в период 70-90-х гг., а также многоэтажек последних лет. Такие низкие показатели по сравнению с другой частью территориями говорят о том, что нагрузки электросетей вполне соответствуют современной системе электропроводки. Более высокие значения магнитной индукции приходятся на восточную часть территории, где в основном расположена общественно-деловая зона с включениями объектов производственного назначения и инженерной инфраструктуры.

Значения магнитной индукции в данных зонах повышенное за счёт наличия большого количества электроприборов, технологического оборудования, электростанций, а также такие территории наиболее насыщены объектами общественного питания, торговли и т.п. Все это создает большую нагрузку на электросеть. Кроме то, в этой части острова встречаются и низкие значения, которые приурочены к историческим домам, являющимися объектами культурного наследия, а также к отдаленным метам от объектов инфраструктуры, например, сквер «Заросли» и Смоленское лютеранское кладбище.

По аномалиям, обусловленных наличием недостаточно экранированных кабелей подземной прокладки, наибольшие показатели магнитной индукции выявлены на улице Кораблестроителей. Ей соответствует КЛ 330 кВ Северная – Василеостровская (полигон на карте). Полные сведения об аномалиях приведены в таблице 1.

ТАБЛИЦА 1. Сводная результатов выявленных аномальных значений магнитной индукции (мкТл), связанных с подземными силовым кабеля и подстанциями

№ точки и место измерений	Измеренные значения, мкТл	Дополнительная информация
проспект КИМа, 4В	0,796	на асфальте 1,62
Парк на улице Одоевского	0,716	на земной поверхности 1,42
Железноводская улица, 5	0,654	на земле аналогично
Железноводская улица, 9А	2,23	на земле 5,62
Железноводская улица, 17	0,622	на земле 1,27
переулок Декабристов, напротив заправки	1,54	на земле 2,96
Железноводская улица, у скейт-парка	0,694	на земле 1,18
набережная реки Смоленки, 5-7Д	0,87	на земле аналогично
улица Кораблестроителей, 39к1	2,29	на земле 5,69
улица Кораблестроителей, 39к1	2,91	на земле 7,04
улица Кораблестроителей, 37Б	3,34	на земле 7,21
ул. Кораблестроителей, 35В	1,17	на земле 1,49
улица Кораблестроителей, 35к7	0,876	на земле 1,28
Капитанская улица, 4	0,873	на асфальте 1,43
ПС 330 кВ «Василеостровская»	0,84	на земле 1,07
ПС-104 110 кВ «Уральская»	2,04	на земле 1,59

Как видно из предоставленной таблицы 1 было выявлено 14 аномальных значения интенсивности магнитной индукции, обусловленных подземными кабелями и 2 аномалии, обнаруженных у подстанций. Так, у открытой ПС-104 110 кВ «Уральская» значение магнитной индукции - 2,04 мкТл, больше значения показателя у закрытой ПС 330 кВ «Василеостровская» почти в 2,5 раза. Это говорит о том, что ограждение территорий от таких объектов электроснабжения являются эффективным методом защиты населения от ЭМИ. Что касается аномалий связанных с прокладкой кабельных линий по всей территории острова Декабристов, то максимальное значение,

измеренное на высоте 1,8 м составил 3,34 мкТл, а на поверхности земли и вовсе 7,21 мкТл, что всего лишь 0,7 раз ниже действующих в России нормативов 10 мкТл для селитебных зон (согласно СанПиН 1.2.3685-21).

В итоге результаты измерений показателей магнитной индукции на обследуемой территории не превышают нормативных значений. Однако при сравнении с ориентировочными безопасными уровнями магнитной индукции, подтвержденными Всемирной Организацией Здравоохранения в 2007 году [3] и составляющими 0,3-0,4 мкТл, можно отметить, что показатели магнитной индукции, превышающие данные значения, имеют повсеместное распространение.

Список используемых источников:

1. МР 4.3.0177-20. 4.3. от 04.12.2020 «Методы контроля. Физические факторы. Методика измерения электромагнитных полей промышленной частоты 50 Гц на селитебной территории» // СПС Кодекс.

2. Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания: СанПиН 1.2.3685-21: постановление Главного государственного санитарного врача РФ от 28.01.2021 № 2 // Госстандарт, 2021. – 469 с.

3. WHO. Extremely low frequency fields: Environmental health criteria. Fact sheet no. 238. Geneva: WHO; 2007.

Makina M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Geoinformation mapping of electromagnetic fields of the island of the decembrists of st. Petersburg.

A study of the spatial distribution of the values of electric field intensity and magnetic induction of industrial frequency on the territory of the island of the Decembrists of St. Petersburg was executed. It was found that no excess of hygienic standards was detected, however, almost all values of magnetic induction exceed the approximate safe level of 0.3-0.4 μT, confirmed by the World Health Organization.Especially anomalous values of magnetic induction are found in places where underground cables are laid. Maps of interpolated values were compiled based on the obtained measurement results to illustrate the distribution of electromagnetic field levels and to identificate the most dangerous areas.

Key words: electromagnetic fields, industrial frequency, electric fields, magnetic fields, electric field strength, magnetic induction, mapping, magnetic field anomalies, Dekabristov Island, St. Petersburg

УДК 621.317.421
ГРНТИ 87.15.03

ИССЛЕДОВАНИЕ ШУМОВОГО ЗАГРЯЗНЕНИЯ ГОРОДСКОЙ СРЕДЫ И РЕКОМЕНДАЦИИ ПО ЕГО СНИЖЕНИЮ НА ПРИМЕРЕ ВАСИЛЬЕВСКОГО ОСТРОВА

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

В крупных городах человек постоянно подвергается воздействию шумов высоких уровней. Проведение исследований с целью измерения уровней шума в городской среде не только позволяет выявлять эти уровни, но и обеспечивает основу для разработки мероприятий, направленных на снижение и ограничение их распространения. Полученные данные для конкретных территорий в городе приобретают практическое значение, особенно в контексте проектирования новых жилых районов и борьбы с шумом в застройке.

шумовое загрязнение, акустический фон, натурные измерения уровня шума, средства защиты от шума, источники шума

Шумовое загрязнение является серьезной проблемой в современных городах. Это оказывает негативное воздействие на здоровье людей, а также может привести к различным социальным и экономическим проблемам.

Шумовое загрязнение является одной из форм физического загрязнения окружающей среды, которое выражается в повышении уровня шума сверх допустимых норм. Шумом принято называть беспорядочные акустические колебания, которые отличаются сложностью временной и спектральной структуры [2].

Многочисленные источники городского шума разбросаны по обширным территориям города, в результате чего возникает «акустический фон». Источники шума в городской среде по геометрическим параметрам разделяются на три группы: точечные, линейные и пространственные. Точечными источниками являются единичные транспортные средства, электрические трансформаторы, системы вентиляции, промышленные и энергетические установки. К линейным источникам относятся транспортные потоки на улицах и дорогах, на железной дороге, к пространственным – промышленные предприятия с многочисленными источниками шума, автовокзалы, логистические центры и т.д.

Одним из наиболее интенсивных источников акустического загрязнения окружающей среды являются транспортные потоки. По данным ряда исследователей, шумы от транспортных магистралей составляют свыше 80% всех внешних шумов города [4]. Транспортный шум на примагистральных территориях стойко держится 15-18 часов в сутки, движение затихает на 2-4 часа. Шум распространяется не только на проезжей части или в ее близи, но и вглубь жилой застройки, особенно подвержены негативному воздействию

шума прилегающие к транспортным магистралям внутренние части кварталов.

Для исследования шумового загрязнения используются инструментальные методы измерения уровня шума и последующее картографирование территории, на которой проходили измерения.

Материалы и методы

Исследования уровня звука проводились инструментальным методом с использованием портативного цифрового шумометра CEM DT-8851 (рис. 1).

Рис. 1. Шумометр CEM DT-8851

Измерения были выполнены в ноябре 2023 г. в точках, расположенных в жилых кварталах, вдоль улиц и дорог, на территориях учебных заведений, больниц, в парках и т.д. Территория исследования: Васильевский остров (г. Санкт-Петербург).

В России натурные измерения проводятся согласно ГОСТ 20444-2014 «Шум. Транспортные потоки. Методы определения шумовой характеристики». Измерение шумовых характеристик целесообразно проводить в периоды максимальной интенсивности движения транспорта в дневное время не менее трех раз: в интервале с 7.00 до 9.00 утром, с 9.00 до 19.00 днем и с 19.00 до 23.00 вечером. Измерения не проводят во время выпадения осадков и при скорости ветра более 5 м/с. Главная ось измерительного микрофона направляется в сторону транспортного потока и перпендикулярно к дороге. Прибор располагают на уровне 1,5 м высоты от уровня проезжей части. Проводящий измерения должен находится на расстоянии не менее 0,5 м от измерительного микрофона. Продолжительность измерения должна составлять не более 5 мин. Нахождение людей или посторонних предметов между прибором и транспортным потоком недопустимо.

Места для измерения уровня шума были выбраны на прямолинейных участках улиц и автомобильных дорог, на расстоянии не менее 50 м от крупных перекрестков и остановках общественного транспорта [3].

Результаты и их интерпретация

Уровни шума

Максимально допустимый уровень шума в комнатах, квартирах в дневное время по санитарным нормам— 55 дБА, в ночное — 45 дБА.

ТАБЛИЦА 1. Результаты исследования шума на территории Васильевского острова (г. Санкт-Петербург)

Адрес точки	Время измерения	Зона контроля	Источник шума	Уровень шума, дБА	Норматив, дБА	Кратность превышения
Уральская ул., 21	14-00	Жилая зона	Промышленная зона (Морской завод «Алмаз»), автотранспорт	60,3	55	1,1
Набережная реки Смоленки, 24-я линия В.О., 65 лит А	14-00	Жилая зона	Автотранспорт	57,5	55	1,05
Биржевая линия, 12	14-00	Общественно-деловые зоны	Автотранспорт	36	55	-
26-я линия В.О., 7 · 25-я линия В.О., 8 лит Б	14-00	Жилая зона	Промышленная зона, автотранспорт	41,4	55	-
Кожевенная линия, 27	14-00	Общественно-деловые зоны	Автотранспорт	45,6	55	-
Малый проспект В.О., 88	14-00	Общественно-деловые зоны	Автотранспорт, торговые центры	57	55	1,04
Парк Декабристов	14-00	Общественно-деловые зоны	Автотранспорт	47	55	-

В Василеостровском районе в 14:00 отмечается превышение норм ГОСТа по адресам:

-Уральская ул., 21 – кратность превышения составила 1,1 раз;

- Набережная реки Смоленки, 24-я линия В.О., 65 лит А –1,05 раз;

- Малый проспект В.О., 88 -1,04 раз.

Основными факторами повышенного шумового воздействия является автотранспорт, промышленная зона и торговые центры.

В остальных точках нормы были соблюдены.

Для снижения уровня шума рекомендуется применять следующие методы:

1) использование современной техники с низкими акустическими характеристиками;

2) использование акустических экранов по периметру строительной площадки, оживленной автодороги;

3) применение шумозащитных капотов и кожухов на стационарное оборудование промышленных предприятий;

4) оптимизация потоков движения по автодорогам;

5) расширение проезжей части;

6) высадка деревьев вдоль дорог [1].

Заключение

В результате оценки уровня шума на территории Васильевского острова были поучены следующие результаты:

1. в 14:00 отмечается превышение норм ГОСТа по адресам: Уральская ул., 21, Набережная реки Смоленки, 24-я линия В.О,Малый проспект В.О., 88;

2. кратность превышения нормы варьируется в пределах 1,04-1,1;

3. основными факторами повышенного шумового воздействия является автотранспорт, промышленная зона и торговые центры.

Список используемых источников:

1. Белоусов В. Н., Прутков Б. Г., Шицкова А. П. Борьба с шумом в городах. М. : Стройиздат, 2007. 45 с;

2. Васильев А. В. Шумовая безопасность урбанизированных территорий [Электронный ресурс] // Известия Самарского научного центра РАН. 2014. N 1-1. URL: https://cyberleninka.ru/article/n/shumovaya-bezopasnost-urbanizirovannyh-territoriy (дата обращения: 25.11.2023).

3. ГОСТ 20444-2014 «Шум, Транспортные потоки. Методы определения шумовой характеристики»

4. Защита населения от акустического загрязнения [Электронный ресурс]. URL: http://oplib.ru/ekologiya/view/1204595_zaschita_naseleniya_ot_akusticheskih_zagryazneniy. (дата обращения: 25.11.2023).

Nazarov I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Study of urban noise pollution and recommendations for mitigation: a case study of Vasilievsky Island.

In major cities, individuals are constantly exposed to high levels of noise. Conducting research to measure noise levels in the urban environment not only allows for the identification of these levels but also provides a foundation for developing measures aimed at reducing and limiting their spread. The obtained data for specific city areas hold practical significance, especially in the context of designing new residential neighborhoods and addressing noise issues in urban development.

Key words: noise pollution, noise sources , noise protection measures.

УДК 504.055
ГРНТИ 87.55.37

ВЛИЯНИЕ ПОЛИМЕРНЫХ ОТХОДОВ НА БИОЛОГИЧЕСКУЮ АКТИВНОСТЬ ПОЧВ

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

Полимерные отходы могут оказывать негативное влияние на биологическую активность почвы. Это связано с тем, что многие полимеры не поддаются полному биологическому разложению. В результате полимерные отходы могут накапливаться в почве годами или десятилетиями, засоряя ее и делая кислород и влагу менее доступными для растительности. В результате количество и разнообразие микроорганизмов в почве может уменьшиться, что приведет к снижению плодородности и нарушению основных функций почвенной экосистемы, таких как дыхание, удерживание воды и питательных веществ. В данной работе было исследовано влияние трех полимерных отходов на базальное дыхание почвы и разработан контактный метод определения фитотоксичности. В результате исследования были выявлены наиболее токсичные полимеры, влияющие на дыхание почвы.

полимерные отходы, почва, загрязнение пластиком, биологическая активность почв, базальное дыхание почвы, фитотоксичность, полимер

Весной 2023 года были проведены исследования для получения информации об изменениях показателей базального дыхания, а также биотестирования в процессе разложения упаковочных полимерных материалов (в т.ч. биоразлагаемых) в почве.

Дыхание почвы в настоящее время признано одним из важнейших показателей состояния почвы и почвенного микробного комплекса, а также почвенной экосистемы в целом [1,2].

Для проведения исследований были взяты 3 полимера, а именно: пакет-майка из кукурузного крахмала, пакет-майка Polymateria, жидкое стекло ПВХ. Первоначально определяется базальное дыхание образцов огородной почвы, содержащих данные материалы. Полимеры были измельчены на небольшие куски, после чего помещены в контейнеры с плодородной почвой. Каждую неделю производилось увлажнение и тщательное перемешивание почвы, чтобы приблизить лабораторные условия к естественным. Спустя 4 месяца провели первый опыт на определение базального дыхания (показатель биологической активности почвы).

Интегральным показателем биологической активности почвы является выделение углекислого газа или дыхание почвы. Метаболизм органических веществ, возвращающий углекислый газ в атмосферу, является последним звеном в глобальной пищевой цепи и происходит в почвенном покрове Земли за счет аэробной гетеротрофной микробной активности. Чем активнее микроорганизмы, тем больше вырабатывается CO_2.

Дыхание почвы в антропогенных условиях может служить количественным показателем самоочищения почвы от загрязняющих веществ и устойчивости почвы к антропогенным воздействиям. Поэтому газообмен CO_2 является важным индикатором изменений, происходящих в почве.

Для определения базального дыхания почвы в данном исследовании используются пронумерованные стеклянные боксы (банки) с плотно закрывающимися крышками. На дне боксов размещаются лабораторные стаканчики, предварительно заполненные гидроксидом натрия (NaOH - щёлочь), а также чашки Петри с влажной навеской образцов почвы.

Подготовленные боксы плотно закрываются крышками и хранятся в данном виде ровно сутки.

Суть данного метода заключается в следующем – выделяемый углекислый газ из почвы будет абсорбироваться раствором щёлочи внутри бокса [3].

Спустя сутки, поочерёдно открываются боксы, и из них достаются стаканчики с щёлочью, которые подготавливаются к титрованию. Перед началом титрования, в каждый стакан с щелочью добавляется капля фенолфталеина, он является индикатором. Подготавливается установка для титрования, стеклянные палочки и раствор кислоты H_2SO_4 (0,02%).

Приступаем к титрованию кислоты в щёлочь, при этом постоянно перемешивая щёлочь в стаканчике стеклянной палочкой. Сначала будут оттитрованы 4 холостых образца, так как в боксах этих образцов не было почвы, а находилась только щёлочь, и в них не происходил процесс выделения CO_2, соответственно базальное дыхание почвы равно нулю.

После вычисления среднего значения холостых образцов, приступаем к титрованию всех следующих образцов.

Методика заключается в следующем – бюретка наполняется 10 миллилитрами 0,02 процентного раствора серной кислоты, снизу установки под стеклянным носиком располагается стаканчик с щёлочью в который был добавлен фенолфталеин.

Далее титрование происходит до полной реакции (изменение цвета с фиолетового до прозрачного), фиксируется значение оставшейся кислоты в бюретке, границей отсчёта служит величина среднего значения холостых образцов. Для расчета количества выделяемого диоксида углерода в каждом боксе используется формула 1:

$$CO_2 = \frac{\text{остаток } H_2SO_4}{\text{К·влаж.навеска}} \times 44 \quad (1)$$

После расчета количества выделяемого диоксида углерода в каждом боксе определяется среднее количество CO_2 для всех параллельных опытов, это и является почвенным дыханием.

Общие результаты эксперимента на базальное дыхание почвы и процентное соотношение на уменьшение дыхания почвы занесены в таблицу 1.

Образец биоразлагаемого пакета уменьшает дыхание почвы на 44% по отношению к контрольному образцу, в сравнении с другими образцами, это является наилучшим результатом. Однако стоит отметить, что оптимальный показатель микробного дыхания почвы, в среднем не должен превышать 30%, так как, чем выше это значение, тем хуже для почвы.

Пакет из кукурузного крахмала показал неожиданные результаты, ведь он считается одним из самых безопасных упаковочных полимерных материалов. Данный образец абсолютно не позволяет почве дышать, он уменьшает дыхание почвы на 100%. При этом данный образец имеет лучшую деструктуризацию по визуальным и физическим свойствам, что подтверждает заявленную производителем информацию о его разложении при компостировании.

Образец ПВХ не имеет заявленных сроков разложения, но опираясь на теоретические данные из электронных и литературных источников, его срок разложения может достигать 500 лет. В проведённом опыте на дыхание почвы, ПВХ показал не самый худший результат и уменьшил дыхание на 70%, но учитывая срок его разложения, по сравнению с биоразлагаемыми образцами, где производители обещают разложение за 1 год. Чаще всего поливинилхлорид утилизируют методом пиролиза или вторичной переработки.

ТАБЛИЦА 1. Общие результаты эксперимента на базальное дыхание почвы

Варианты образцов	Среднее количество выделяемого CO_2, мг (рассчитывалось по формуле № 1)	Среднее количество выделяемого CO_2, %	Уменьшение дыхания почвы, %
Контрольный образец почвы	9,7 ± 0,2	100%	-
Образец с биоразлагаемым пакетом	5,5 ± 0,5	56%	44%
Образец с пакетом из крахмала кукурузы	0	0	100%
Образец с ПВХ	3,0 ± 0,5	30%	70%

Почвы занимают особое место в экосистемах и выполняют множество функций. Наиболее важной из них является экологическая, обеспечивающая среду обитания для человека и других организмов. Загрязнение может повлиять на структуру почвы, пористость и плотность горизонтов, что приводит к ухудшению аэрации и дренажа. В результате затрудняется прорастание семян и проникновение корней в почву, что приводит к снижению роста корней и побегов [4].

Для расчёта этих изменений существуют различные методы биотестирования, они позволяют охарактеризовать степень воздействия изучаемого фактора на биологическую экосистему и природную среду.

Среди контактных биотестов для контроля экологического состояния почвы наиболее эффективным методом считается фитотестирование с использованием высших растений в качестве тест-организмов [5]. Лабораторные фитотесты характеризуются быстротой и простотой проведения, экономичностью, воспроизводимостью и надежностью полученных результатов.

Опыт проводился по методике, разработанной в НИЦЭБ РАН.

В качестве тест-культуры использовались семена пшеницы мягкой (Triticum aestivum L). Определение степени острой фитотоксичности пробы проводилось на основании разработанной по двум показателям шкалы: по изменению всхожести семян (*N*1) и роста корней (*N*2) по сравнению с контрольным образцом.

Проведение опыта начинается с подготовления чистых чашек Петри, в них помещаются каждый исследуемый образец почвы. Следующим действием производится отбор семян пшеницы, по 20 штук на каждый образец, затем они вносятся в пронумерованные чашки Петри с образцами почвы. Когда во все образцы были внесены семена, чашки накрываются крышками, оставляются на 2-3 дня, чтобы проросли корни и побеги.

Следующим этап потребуется извлечь проросшие семена с корнями. Важно соблюдать осторожность и не торопится, потому что корни переплетаются друг с другом и их достаточно легко порвать. С использованием сито ростки промываются проточной водой и перекладываются на подготовленную поверхность (подложкой служит бумага) для измерения длинны корней.

Замеры производятся с помощью линейки, росток прикладывается к нулю, корень осторожно растягивают по измерительной шкале линейки, данные с точностью до миллиметра вносятся в таблицу 2.

ТАБЛИЦА 2. Определение фитотоксичности почвогрунтов на пшенице мягкой

№ пробы	Всхожесть		Корень		Степень токсичности почвы
	%	N_1 (см. п. 2.5)	Длина, мм	N_2 (см. п. 2.5)	
Контроль	90	-	47,62	-	
1	93	3	42,36	11	V – практически не токсичные
2	98	9	49	3	V – практически не токсичные
3	100	11	51,16	7	V – практически не токсичные

Что касается результатов биотестирования контактным методом определения, указанных в таблице 2, фитотоксичность не была установлена для всех образцов. Степень токсичности каждого образца присваивалась согласно методике выполнения измерений предоставленной в НИЦЭБ РАН.

Связанно это со сроком определения токсичных загрязнений. Ввиду небольшого срока постановки всего исследования, возможно в почву не

выделилось достаточное количество токсичных соединений, либо она не успела их саккумулировать.

Это мотивирует продолжить исследования в дальнейшем и использовать другие методы определения токсичности полимеров.

Список используемых источников:

1. Литвинец Ю. И. Технологические и энергетические расчеты при переработке полимеров экструзией. М. : Редакционно-издательский отдел УГЛТУ, 2010. 55 с.

2. Терехова В. А., Воронина Л. П., Николаева О. В., Бардина Т. В., Калмацкая О. А., Кирюшина А. П., Учанов П. В., Креславский В. Д., Васильева Г. К. Применение фитотестирования для решения задач экологического почвоведения // Использование и охрана природных ресурсов в России. 2016. 41 с.

3. Межгосударственный стандарт. Охрана природы. Почвы. Методы отбора и подготовки проб для химического, бактериологического, гельминтологического анализа: ГОСТ 17.4.4.02-2017: принят Межгосударственным советом по стандартизации, метрологии и сертификации, 30 ноября 2017 г. N 52 // Госстандарт, 2017. – 10 с.

4. Информационно-технический справочник по наилучшим доступным технологиям ИТС 9-2015 "Обезвреживание отходов термическим способом (сжигание отходов)". – Введ. 2016-07-21. Справочник НДТ – 243с.

5. Бардина Т. В., Чугунова М. В., Кулибаба В. В., Бардина В. И. Использование методов биотестирования для оценки экологического состояния почвогрунтов рекультивированного карьера. М. : Фонд научных исследований «XXI век», 2020. А11с.

Petrov M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Polymer waste can have a negative impact on the biological activity of the soil. This is due to the fact that many polymers are not amenable to complete biodegradation. As a result, polymer waste can accumulate in the soil for years or decades, clogging it and making oxygen and moisture less accessible to vegetation. As a result, the number and diversity of microorganisms in the soil may decrease, which will lead to a decrease in fertility and disruption of the basic functions of the soil ecosystem, such as respiration, water retention and nutrients. In this work, the effect of three polymer wastes on the basal respiration of the soil was investigated and a contact method for determining phytotoxicity was developed. As a result of the study, the most toxic polymers affecting soil respiration were identified.

Key words: polymer waste, soil, plastic pollution, biological activity of soils, basal respiration of soil, phytotoxicity, polymer.

УДК 004.056.5
ГРНТИ 81.93.29

НОКСОЛОГИЧЕСКИЙ ПОДХОД МОДЕЛИРОВАНИЯ РИСКОВ КИБЕРУГРОЗ В ПОЖАРНОЙ НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ ОПАСНЫХ ПРОИЗВОДСТВЕННЫХ ОБЪЕКТОВ

М. А. Тукмачева, А. В. Шестаков
Санкт-Петербургский университет государственной противопожарной службы МЧС России

Исследования проблем обеспечения безопасности опасных производственных объектов проводятся в последние несколько лет не столько в аспекте техногенной безопасности, сколько в аспекте комплексной основы происхождения и совокупного действия промышленной, экологической, социальной опасностей и кибервоздействий, описаний зон и показателей их влияния, оценки наносимого ущерба, которые составляют предмет изучения ноксологии. В государственной пожарной надзорной деятельности опасных производственных объектов такой подход ранее не использовался, поэтому предлагается применить, в первую очередь, при комплексировании моделей рисков, агрегированных на информационной инфраструктуре системы пожарной надзорной деятельности, выборе и обосновании необходимых программных средств моделирования.

ноксология, информационная инфраструктура, программное обеспечение, большие данные, чрезвычайная ситуация

В сфере техногенной безопасности в последние несколько лет достаточно активно развиваются научные положения и методология решения актуальных проблем с применением комплексирования прогнозных оценок рисков, создаваемых различными факторами и условиями чрезвычайных ситуаций, и наносимого ущерба на основе подходов ноксологии (науки об опасностях материального мира, минимизации опасностей в источниках и основы защиты от них) [1]. Имеется достаточно представительный ряд научных работ и публикаций, посвященных данной проблематике, таких авторов как С.В. Белов (Ноксология. 2020) [2], Е.А. Пряхина (Применение математических методов в ноксологии. 2021) [3], А.А. Александров, Е.В. Титов, В.А. Девисилов (Урбоэкология. 2021) [4], К.С. Дмитренко (Стохастический характер оценки рисков, как один из методов в изучении ноксологии. 2017) [5] и другие. Достаточно показательным развитием методологии ноксологии является цикл публикаций творческого коллектива авторов (Александров А.А., Девисилов В.А., Ларионов В.И., Сущев С.П.) от предмета основных профессиональных образовательных программ [6], рисков для населении и территорий техногенных аварий [7], комплексного учета природных и климатических факторов [8] и стадий развития процесса аварии [9], до комплексного анализа рисков [10].

Одним из направлений развития методов ноксологии при моделировании рисков киберугроз в государственной пожарной надзорной деятельности опасных производственных объектов, особенно для условий крупного мегаполиса (например, судостроительные объекты

"Адмиралтейские верфи", "Балтийский завод", "Северная верфь", территориально распределенные на значительной площади в Санкт-Петербурге) является комплексирование задач рисков информационной безопасности ($R_{ИБ}$) в пожарной надзорной деятельности, которые можно представить в виде концептов:

$$R_{ИБ} =< R_{ГТ}, R_{ТА}, R_{ПБ} >,$$

где $R_{ГТ}$ – риски геотектоники; $R_{ТА}$ – риски техногенной аварии;. $R_{ПБ}$ – риски пожарной безопасности.

Стек комплексной среды моделирования для такой концептуальной постановки задачи представлен на рис. 1.

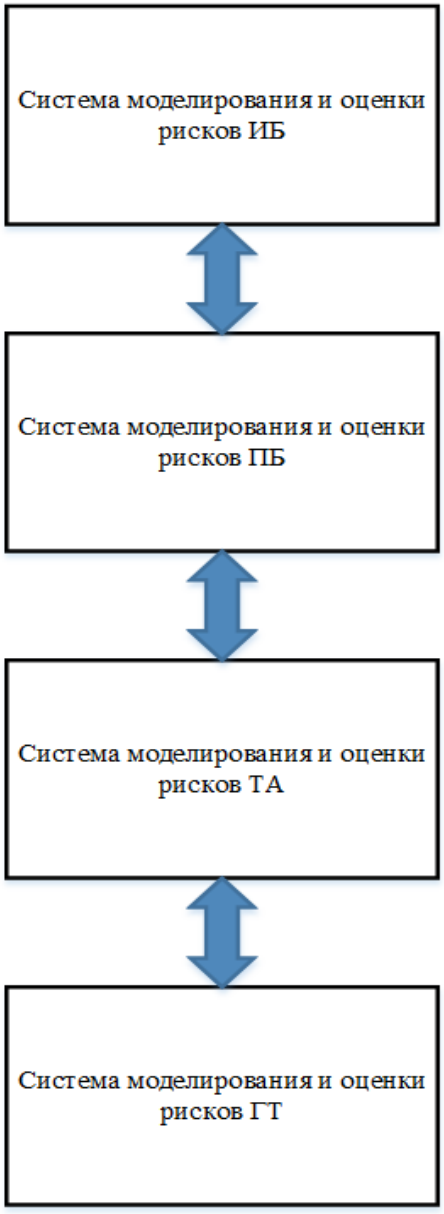


Рис. 1. Стек комплексной среды моделирования

Принятая в настоящее время методология, организация и средства моделирования и оценки рисков для $R_{ГТ}$ (геотектоники), $R_{ТА}$ (техногенной аварии) и $R_{ПБ}$ (пожарной безопасности) достаточно известны, однако достаточно новым для такого класса задач является определение методов и средств сбора и обработки больших данных при оценке $R_{ИБ}$.

Возможные к применению методы моделирования и обработки больших данных должны использовать современные программные средства такие как Arenadata, Security Vision, Скала-Р, Cassandra, Postgres Pro, Apache Hadoop, Jatoba, Квант-Гибрид, Ред БД, ProximaDB, ClickHouse, СУБД ЛИНТЕР, Tarantool, Лира-Р. Проведенный сравнительный анализ представленной линейки программных средств по обобщенным показателям качества на основе показателей ГОСТ Р ИСО/МЭК 250xx, выявил набольшую величину показателей качества существенных свойств Arenadata (отечественной аналитической распределенной СУБД).

Исследования оценочных ноксологических моделей проводятся в тесном научном взаимодействии с Геофизическим центром РАН.

Список используемых источников:

1. Ноксология : учебник / Е. Е. Барышев, А. А. Волкова, Г. В. Тягунов, Н79 В. Г. Шишкунов / под общ. ред. Е. Е. Барышева. Екатеринбург : Изд-во Урал. ун-та, 2014. 160 с.

2. Белов С. В. Ноксология : учебник и практикум для вузов / С. В. Белов, Е. Н. Симакова ; под общ. ред. С. В. Белова. М. : Издательство Юрайт, 2020. 451 с.

3. Пряхина Е. А., Чумакова А. В., Миндеева С. В. Применение математических методов в ноксологии // Молодая наука Сибири. N 2(12). 2021. С.382-390.

4. Александров А. А., Титов Е. В., Девисилов В. А. Урбоэкология. М. : Издательство МГТУ им. Н. Э. Баумана. 2021. 400 с.

5. Дмитренко К. С. Стохастический характер оценки рисков, как один из методов в изучении ноксологии // Фундаментальные исследования, методы и алгоритмы прикладной математики в технике, медицине и экономике : материалы 16-ой Междунар. науч.-практ. конф., г. Новочеркасск, 26-27 октябр. 2017г. Южно-Российский государственный политехнический университет (НПИ) имени М. И. Платова. Новочеркасск : ООО «Лик», 2017. 253 с.

6. Александров А. А., Девисилов В. А., Сущев С. П., Копытов Д. О., Смирнов А. С. Подготовка кадров в МГТУ им Н.Э. Баумана в области защиты в чрезвычайных ситуациях, анализа, оценки и прогнозирования рисков в рамках направления «Техносферная безопасность» (опыт сотрудничества университета и МЧС России, результаты и задачи // Проблемы безопасности жизнедеятельности (в сфере образования). 2016. С. 41-51.

7. Александров А. А., Ларионов В. И., Сущев С. П. Методические особенности анализа риска для населения и территорий при авариях с выбросом опасных химических веществ // Проблемы сбора, подготовки и транспорта нефти и нефтепродуктов. 2021. N 6 (134). С. 137-146.

8. Сущев С. П., Ларионов В. И., Александров А. А. Особенности методических подходов к анализу риска на пожаровзрывоопасных объектах с учетом режима ветра по многолетним метеорологическим наблюдениям // Электронный научный журнал Нефтегазовое дело. 2021. N 6. С. 95-107.

9. Ларионов В. И., Александров А. А., Сущев С. П. Методы анализа риска на ранней фазе радиационной аварии //Электронный научный журнал Нефтегазовое дело. 2021. N 6. С. 75-94.

10. Ларионов В. И., Александров А. А., Сущев С. П. Обзор методических подходов к анализу техногенных и природных рисков // Электронный научный журнал Нефтегазовое дело. 2021. N 6. С. 37-74.

Tukmacheva M., Shestakov A.

Saint Petersburg University of the State Fire Service of the Ministry of Emercom of Russia

Noxological approach to modeling the risks of cyber threats in the fire surveillance activities of hazardous production facilities.
Studies of the problems of ensuring the safety of hazardous production facilities have been conducted in the last few years not so much in the aspect of technogenic safety, as in the aspect of the complex basis of the origin and cumulative effect of industrial, environmental, social hazards and cyber-impacts, descriptions of zones and indicators of their impact, assessment of damage caused, which are the subject of the study of noxology. In the state fire supervision of hazardous production facilities, this approach has not been used before, therefore, it is proposed to apply, first of all, when integrating risk models aggregated on the information infrastructure of the fire supervision system, selecting and justifying the necessary modeling software.

Key words: noxology, information infrastructure, software, big data, emergency.

УДК 504.055
ГРНТИ 87.55.37

ГЕОИНФОРМАЦИОННОЕ КАРТОГРАФИРОВАНИЕ ЭЛЕКТРОМАГНИТНЫХ ПОЛЕЙ АДМИРАЛТЕЙСКОГО МУНИЦИПАЛЬНОГО ОКРУГА САНКТ-ПЕТЕРБУРГА

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

В данной научной статье рассмотрен вопрос пространственного распределения электрических и магнитных полей промышленной частоты (50 Гц) на территории Адмиралтейского муниципального округа Санкт-Петербурга. Изучение этой проблемы имеет большую актуальность с точки зрения влияния электромагнитных полей на экосистему. Исследования позволяют более точно определить уровень излучения и контролировать его в соответствии с международными стандартами. По результатам анализа, предельно допустимые уровни электромагнитных полей на изучаемой площади благополучны, однако, значения магнитной индукции превышают безопасные уровни зарубежных исследований. Результаты пространственного распределения электромагнитных полей Адмиралтейского муниципального округа Санкт-Петербурга представлены на картах с применением метода интерполяции и метода изолиний.

электромагнитные поля, картографирование, геоинформационная система, напряжённость электрического поля, интенсивность магнитного поля, промышленная частота, Адмиралтейский муниципальный округ

Современное общество окружено электроэнергетическими устройствами, мобильными телефонами, бытовой техникой и другими источниками электромагнитных полей, то есть физических полей, охватывающих пространство вокруг электрического заряда или тока и возникающих при изменении магнитного поля. Особенно в сложной ситуации оказываются крупные городские агломерации, ведь интенсивность электромагнитного излучения в ней выше, чем на открытом пространстве [1, 2]. Изучение электромагнитных полей в выбранном округе имеет большую важность с точки зрения их влияния на экосистему, так как Адмиралтейский муниципальный округ является центральной частью города, в котором расположено множество памятников истории и культуры, способствующих привлечению большого числа туристов, а также местных жителей.

Весной 2023 года было совершено несколько практических выходов на территорию округа для проведения замеров. В ходе измерений учитывался тот факт, что большинство зданий района относятся к исторической застройке XIX века, по большей части - из кирпича, в которой качество внутренней электропроводки часто не соответствует нагрузкам от современной бытовой техники. По результатам определения напряженности электрических полей и магнитной индукции промышленных частот 50 Гц и обработки измерений, был составлен ряд карт, отражающих

пространственное распределение этих полей в Адмиралтейском муниципальном округе Санкт-Петербурга. Расположение замеров приведено на рис. 1.

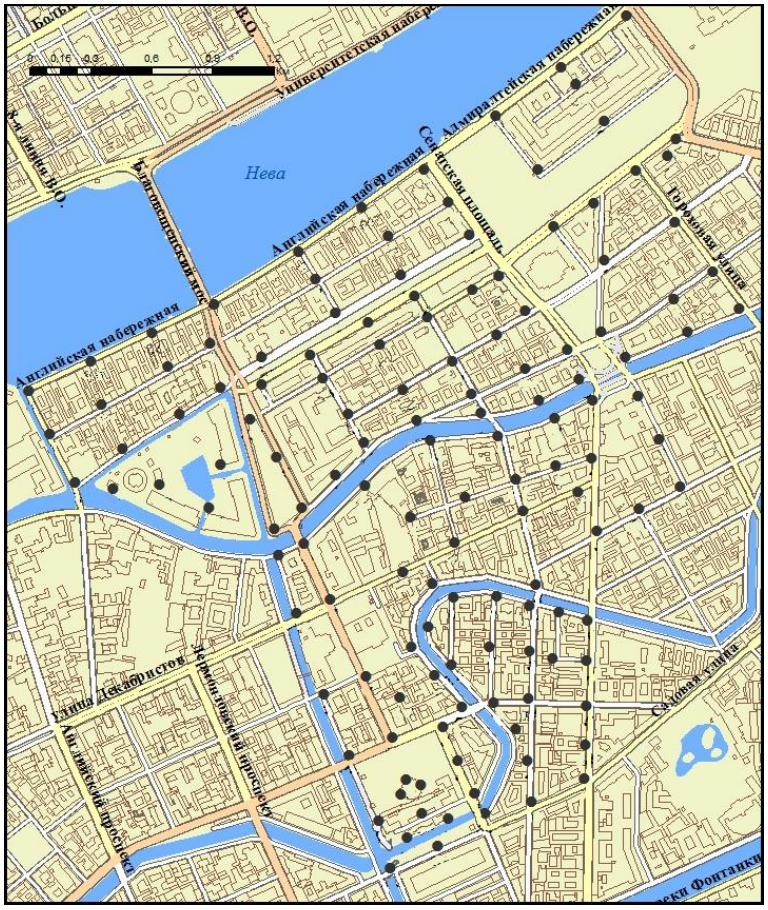


Рис. 1. Карта фактического материала

Для визуализации распространения напряжённости электрических полей, строилась карта с помощью метода интерполяции растра (рис. 2). Максимальными значениями в исследуемой области являются значения в 6-6,9 В/м. На пересечениях улиц Декабристов и Глинки, а также на стыке Почтамтской и Малой Морской, данный показатель обусловлен близким расположением энергощита в месте измерения. На остальной территории значения электрических полей распределены равномерно, с незначительными скачками вдоль фасадов зданий вблизи вывесок и объектов освещения.

На основании СанПиН 1.2.3685-21 "Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания" [3], для селитебных территорий, предельно-допустимым уровнем напряженности электрического поля промышленной частоты является значение до 1 кВ/м. Пики наблюдаемых значений примерно в 143 раза меньше, чем граница нормы. В рамках исследования пространственного распределения электрических полей в Адмиралтейском

муниципальном округе города Санкт-Петербург, превышений предельных допустимых уровней не выявлено.

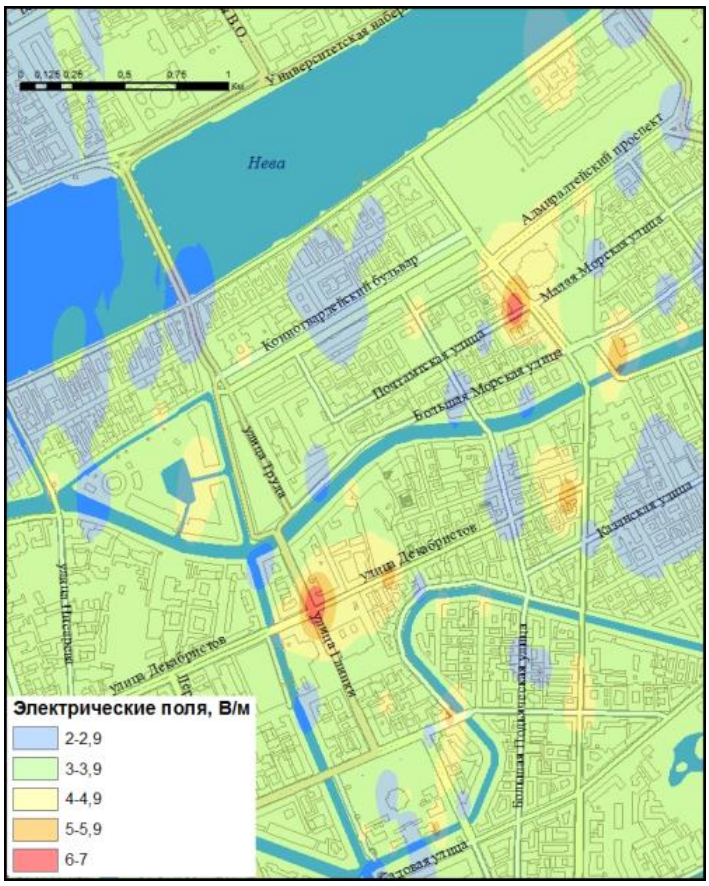


Рис. 2. Интерполяция электрических полей Адмиралтейского МО Санкт-Петербурга

Визуализация распределения магнитной индукции, также отображена на карте с помощью метода интерполяции растра (рис. 3). Уровням в 0,3-0,5 мкТл больше всего соответствуют территории скверов и рекреационных зон с малым наличием или отсутствием электрооборудования. Средние, по результатам измерений, значения в 0,5-1 мкТл обусловлены наличием сети электроснабжения бытового характера и высокой плотностью электротранспорта на узких улицах Петербурга. Пики значений наблюдаются на канале Грибоедова. Наибольшее значение, выделенное на карте красным цветом, является показателем влияния энергощита с высокой силой тока. На образование меньшей красной области повлияло наличие электрической конструкции с названием магазина, являющейся источником неоднозначного значения магнитной индукции. В других точках исследуемой территории определены значения в 1-2 мкТл. Такое влияние, как правило, оказывают кондиционерные установки, вывески магазинов и кафе, небольшие объекты освещения. В одной из точек карты значение в 2 мкТл объясняется наличием металлической решетки электроворот, поскольку конструкции, состоящие из металла, могут быть подвержены явлению электризации и быть нетипичным источником поля.

На основании того же СанПиН [3], для селитебных территорий предельно-допустимым уровнем магнитной индукции промышленной частоты является значение до 10 мкТл. Поэтому значения, даже по самым критичным точкам, в 3 раза меньше, чем граница нормы. Превышений предельных допустимых уровней не выявлено, все безопасные уровни соблюдены.

Однако, опираясь на зарубежные ПДУ [4, 5], которые говорят об опасности значений свыше 0,2 мкТл, уровень излучения в округе является повышенным. Для приведения показателя в норму, возможно, потребуется провести дополнительный мониторинг округа и произвести обновление компонентов сетей электроснабжения, поскольку установленное оборудование в этом районе, уже не соответствует современным нагрузкам. Кроме того, всему мировому экологическому сообществу, очевидно, стоит пересмотреть стандарты в области магнитной индукции, чтобы разработать общий норматив в целях единого подхода к решению насущной проблемы.

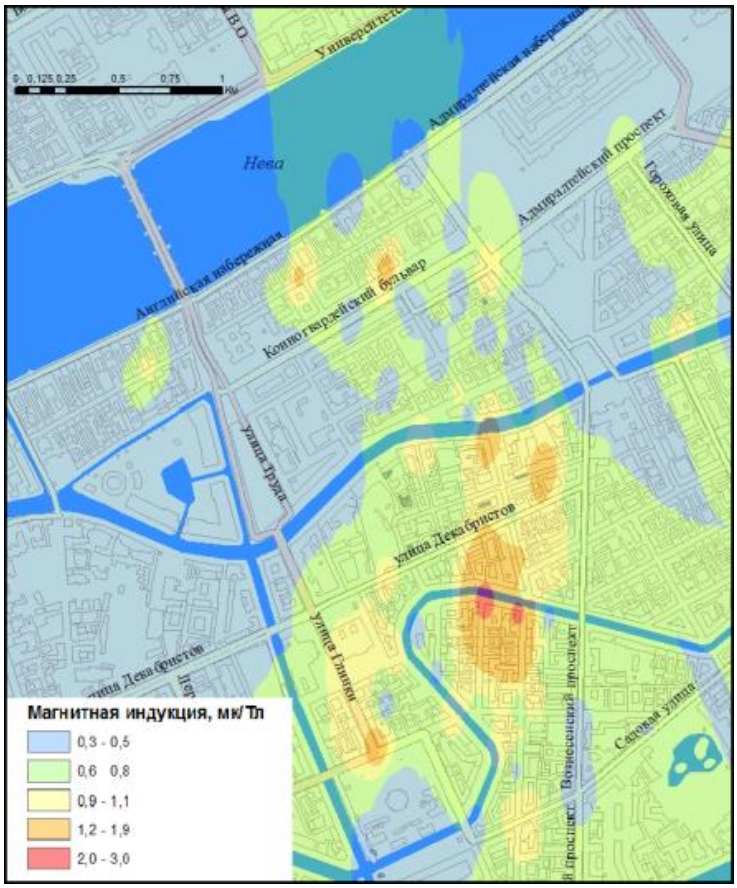


Рис. 3. Интерполяция магнитной индукции Адмиралтейского МО Санкт-Петербурга

Список используемых источников:

1. Бузов А. Л., Сподобаев Ю. М. Электромагнитная экология. Основные понятия и нормативная база. М. : Радио и связь, 1999. 78 с.

2. Калыгин В. Г. Промышленная экология: учеб. пособие. М. : Издательский центр «Академия», 2017. 368 с.

3. Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания: СанПиН 1.2.3685-21: постановление

Главного государственного санитарного врача РФ от 28.01.2021 № 2 // Госстандарт, 2021. – 469 с.

4. Opinion on Possible effects of Electromagnetic Fields (EMF), Radio Frequency Fields (RF) and Microwave Radiation on human health Expressed at the 27th CSTEE plenary meeting Brussels, 30 October 2001. // URL: https://ec.europa.eu/health/ph_risk/committees/sct/documents/out128_en.pdf (дата обращения: 22.05.2023)

5. Muller B. Electrosmog. Hausgemachtes Problem // Bild Wiss. 1996. № 4. С. 12-14.

Uporov M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Geoinformation mapping of electromagnetic fields of the admiralty municipal district of st. Petersburg.

This scientific article examines the issue of spatial distribution of electric and magnetic fields of industrial frequency (50 Hz) on the territory of the Admiralteysky Municipal District of St. Petersburg. The study of this problem is of great relevance from the point of view of the influence of electromagnetic fields on the ecosystem. Research allows us to more accurately determine the level of radiation and control it in accordance with international standards. According to the results of the analysis, the maximum permissible levels of electromagnetic fields in the study area are safe, however, the values of magnetic induction exceed the safe levels of foreign studies. The results of the spatial distribution of electromagnetic fields in the Admiralteysky Municipal District of St. Petersburg are presented on maps using the interpolation method and the isoline method.

Key words: electromagnetic fields, mapping, geographic information system, electromagnetic field strength, magnetic field, industrial frequency, Admiralteysky Municipal District.

УДК 911.2:502.72
ГРНТИ 87.31.91

ПРОЕКТ ЭКОЛОГИЧЕСКОЙ ТРОПЫ НА ТЕРРИТОРИИ ГОСУДАРСТВЕННОГО ПРИРОДНОГО ЗАКАЗНИКА РЕГИОНАЛЬНОГО ЗНАЧЕНИЯ «ШУНГЕРОВСКИЙ»

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

В данной научной статье рассмотрены основные проблемы рекреационного освоения пригородов Санкт-Петербурга, проведен анализ природно-заповедного фонда Санкт-Петербурга, рассматриваются методика организации экологических троп и развитие познавательного туризма. В качестве примера предлагается проект экологической тропы на территории государственного природного заказника регионального значения «Шунгеровский», расположенного в Петродворцовом районе Санкт-Петербурга.

экологические тропы, ООПТ, охрана природы, экологический туризм, экологическое просвещение

Одним из важных направлений экологии и природопользования является природоохранная деятельность, направленная на сохранение и восстановление природно-ресурсного потенциала.

Значимым инструментом природоохранной деятельности является организация экологических троп, которые наряду с решением задач просвещения, обучения и воспитания, способствуют и охране природы, так как локализуют посетителей природной территории на определенном маршруте, что в свою очередь снижает рекреационную нагрузку на территорию.

Основными проблемами рекреационного освоения пригородов Санкт-Петербурга являются: высокая плотность населения агломерации, большая концентрация отдыхающих на ограниченных участках территории, малая устойчивость к рекреационным нагрузкам большинства природных ландшафтов.

В связи с этим актуальность создания экологических троп на особо охраняемых природных территориях Санкт-Петербурга не вызывает сомнений.

На сегодняшний день природно-заповедный фонд Санкт-Петербурга представлен 17 особо охраняемыми природными территориями регионального значения (рис.1) общей площадью 9 212 га, что составляет 6,4 % от площади Санкт-Петербурга как субъекта Российской Федерации [1].

Для обеспечения экологического просвещения, рекреации и охраны природы на территории Санкт-Петербурга функционируют 4 экологических маршрута, расположенных в государственных природных заказниках:

«Северное побережье Невской губы», «Сестрорецкое болото», «Западный Котлин» и памятнике природы «Комаровский берег».

Рис. 1. Особо охраняемые природные территории Санкт-Петербурга
Примечание: желтым цветом обозначен государственный природный заказник «Шунгеровский»

Разработка планируемой экологической тропы основана на оценке территории по трем основным критериям: привлекательность (красота природы, своеобразие и разнообразие участков особо охраняемой природной территории), доступность (обеспечении тропы хорошими подъездными путями, возможностью прохождения различными группами населения) и информативность (размещение информационных стендов, создание визит-центра, организация видовых точек и смотровых площадок, выпуск буклетов) [2].

При проектировании экологической тропы необходимо учесть цели и задачи создания конкретной ООПТ, требования режима особой охраны, размещения уязвимых природных комплексов и объектов.

Первым шагом при создании проекта является разработка концепции, включающая в себя: актуальность создания экологической тропы на данной территории, сформулированные цели и задачи, а также обозначение целевой аудитории, а также краткая общая характеристика тропы: тематика, протяженность, сезонность, способ прохождения.

Далее, на основе рекогносцировочных исследований территории, составляется генеральный план экологической тропы.

Рекогносцировочные исследования заключаются в детальном изучении территории, на которой предусматривается создание экологической тропы. Во время рекогносцировки выявляются типичные и уникальные природные объекты, а также отмечаются «проблемные участки» где необходима инфраструктура

На генеральном плане экологической тропы отмечаются схема тропы, расположение информационных стендов, мест отдыха, видовых точек, настилов, лестниц, мостиков, туалетов, беседок и других малых архитектурных форм.

Далее, на этапе проектирования на основе проведенной инвентаризации и анализа исходных данных составляются информационные материалы для экологического просвещения.

«Шунгеровский» заказник располагает значительными ресурсами для развития экологического туризма и обустройства на данной территории экологической тропы. Рассматриваемая территория обладает богатой история освоения, а также особо ценными природными сообществами и видами животных и растений [3].

А также на территории данного заказника можно отследить и познакомится с процессами самовосстановления лесных сообществ, которые во время Великой Отечественной войны были почти полностью уничтожены.

Трасса экологической тропы (рис. 2) проходит через разнообразные природные комплексы «Шунгеровского» заказника: крупный массив сосновых лесов, ельников, смешанных и лиственных лесов, выросших за послевоенный период, и по долине реки Кикенки с лугами, ивняками и мелколиственными лесами.

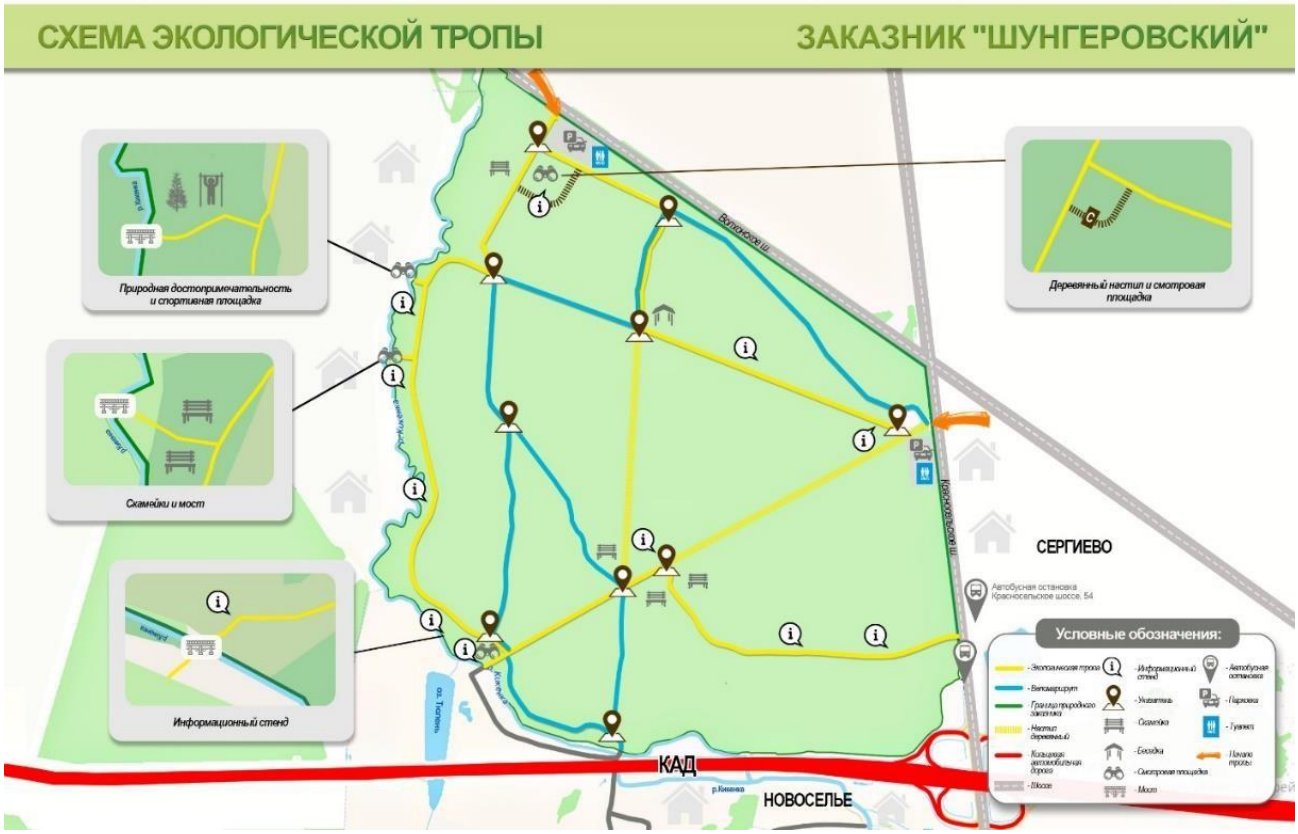


Рис. 2. Проект экологической тропы в Шунгеровском заказнике

Стоит отметить, что на территории заказника были разработаны проекты пешего и велосипедного маршрутов. Пеший экологический маршрут является полукольцевым и имеет протяжённость 6,5 км, веломаршрут – линейный, протяженностью 5,4 км. Время прохождение экологической тропы составляет 3 часа, велосипедного маршрута – 1 час.

По назначению данная экологическая тропа является познавательно-прогулочной и предназначена для посещения всех групп населения, для людей с ограниченными возможностями и пожилых лиц предусмотрены сокращения маршрута.

Маршрут не сложный для прохождения, основная часть проходит по непересеченной местности (только лишь на участке тропы вдоль реки Кикенка перепады высот составляют не более 6 м), и комфортен для посещения в бесснежный период с мая по октябрь. В зимнее время возможно использование тропы для лыжных прогулок. Экологическая тропа поделена на зоны активного (прогулочно-познавательная и спортивная зоны) и пассивного отдыха (зоны тихого созерцания природы). Также на маршруте предполагается обустройство 4 видовых точек, которые знакомят посетителей экологической тропы с уникальными или живописными местами «Шунгеровского» заказника.

Рис. 3. Пример тематического стенда, посвящённого деревьям «Шунгеровского» заказника

Всего на маршруте планируется оборудовать 11 тематических точек-остановок с различной информацией, посвящённой "Шунгеровскому" заказнику. Для каждой остановки разработаны эскизы информационных стендов (рис. 3), предложения по обустройству.

Предлагаемый проект экологической тропы позволит реализовать природоохранную функцию заказника в полной мере, так как организация экологической тропы поможет грамотно перенаправить поток посетителей, что позволит снизить рекреационную нагрузку на природные комплексы «Шунгеровского» заказника.

Список используемых источников:

1. Особо охраняемые природные территории [Электронный ресурс] // Официальный сайт государственного казенного учреждения «Дирекция особо охраняемых природных территорий Санкт-Петербурга». URL: https://oopt.spb.ru/protected_areas. (дата обращения: 24.11.2023).

2. Буторина Н. Н. Лешина Е. В., Малиновская Я. В.Б Тропа в гармонии с природой. Дальневосточный опыт. М: Издательство «Перо», 2019. 129 с.

3. Материалы комплексного экологического обследования участков территорий, обосновывающие придание этим территориям правового статуса особо охраняемой природной территории регионального значения «Шунгеровский» Отчет по государственному контракту № 12ГК от 11.03.2016. Исполнитель - ФГБУН Ботанический институт им. В.Л.Комарова Российской академии наук.

Fleishman A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

The project of an ecological trail on the territory of the state nature reserve of regional significance "shungerovsky".
In this scientific article the main problems of recreational development of the suburbs of St. Petersburg are considered, the analysis of the nature reserve fund of St. Petersburg is carried out, the methodology of the organization of ecological trails and the development of educational tourism are considered. As an example, we propose a project of an ecological trail on the territory of the state nature reserve of regional significance "Shungerovsky", located in the Petrodvorets district of St. Petersburg.

Key words: ecological trails, protected areas, nature protection, ecological tourism, environmental education.

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

Секция 3.1.
Безопасность компьютерных систем и сетей связи

УДК 004.056
ГРНТИ 81.93.29

ОПРЕДЕЛЕНИЕ ТОП-10 АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ, ФУНКЦИОНИРУЮЩИХ В СФЕРЕ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА

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

В настоящее время информационные системы играют ключевую роль в различных отраслях, включая топливно-энергетический комплекс. Они обеспечивают эффективное управление процессами, повышают производительность и предоставляют расширенные возможности по управлению потоками данных на предприятиях. Однако с развитием технологий и расширением возможностей информационных систем возникают и новые угрозы безопасности информации. В данной статье будут рассмотрены топ-10 наиболее актуальных угроз безопасности информации для информационных систем, функционирующих в сфере топливно-энергетического комплекса.

угроза безопасности информации, целенаправленная атака, автоматизированная система управления технологическим процессом

Введение

В современном мире значительную роль играет информатизация и автоматизация. Возможность автоматизации трудозатратных процессов, а также процессов, требующих обработки большого объема данных, является ключевым фактором применения информационных систем полного цикла на предприятиях топливно-энергетического комплекса. Для определения актуальных угроз безопасности информации для информационных систем, функционирующих на таких предприятиях, необходимо рассмотреть типовую топологию таких систем, объекты воздействия, входящие в данные системы, а также наиболее распространенные организационные и технические уязвимости, встречающиеся в данных системах. Стоит отметить еще один важный фактор, как правило, атаки на информационные системы топливно-энергетического комплекса носят целенаправленный характер. Особенность целенаправленных атак (APT) заключается в том, что злоумышленников интересует конкретная компания или государственная организация. Это отличает данную угрозу от массовых хакерских атак – когда одновременно атакуется большое число целей и наименее защищенные пользователи становятся жертвой. Целенаправленные атаки обычно хорошо спланированы и включают несколько этапов – от разведки и внедрения до уничтожения следов присутствия. В результате целенаправленной атаки злоумышленники закрепляются в инфраструктуре жертвы и остаются незамеченными в течение долго времени и на протяжении всего этого

времени они имеют доступ ко всей обрабатываемой информации [1]. На рис. 1 представлены фазы реализации целевой атаки.

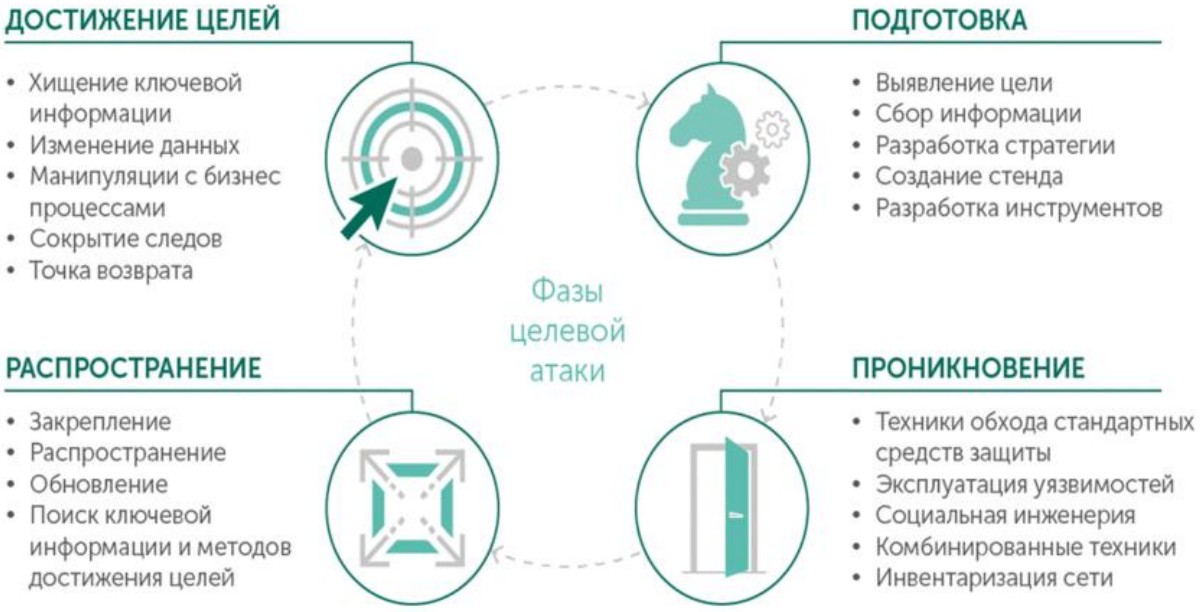


Рис. 9. Фазы развития целенаправленной атаки

Анализ типовой структуры информационной системы.

Далее рассмотрим типовую топологию информационной системы топливно-энергетического комплекса, на которой будут отражены типовые объекты воздействия (на рис. 2). В связи со спецификой, выбранной для рассмотрения сферы, большинство информационных систем представляют собой автоматизированные системы управления технологическим процессом (АСУ ТП), имеющие стандартную трехуровневую архитектуру [3]. Следовательно, к объектам воздействия будут относиться: автоматизированные рабочие места, активное сетевое оборудование, программируемые логические контроллеры и устройства нижнего уровня – датчики. Исходя из рассмотренных объектов воздействия, можно рассмотреть организационные, технические и многофакторные уязвимости, которые способствуют проведению атак:

– Наличие подключения к сетям общего пользования/сети Интернет: в случае наличия такого подключения злоумышленник может получить удаленный доступ к сети АСУ ТП. Для минимизации рисков от реализации атак на сеть, имеющую такое подключение, можно использовать диоды данных.

– Использование устаревших версий системного программного обеспечения, в связи с несовместимостью более новых версий с прикладным программным обеспечение, используемом промышленными системами.

– Слабые парольные политики учетных записей, а также применение словарных паролей, легко поддающихся перебору (атака brute force).

– Невозможность применения некоторых средств защиты информации или недостаточная настройка функционала таких средств с целью избежать нарушения работы АСУ ТП, в связи с применением специфичного ПО.

– Недостаточная информированность персонала в вопросах информационной безопасности.

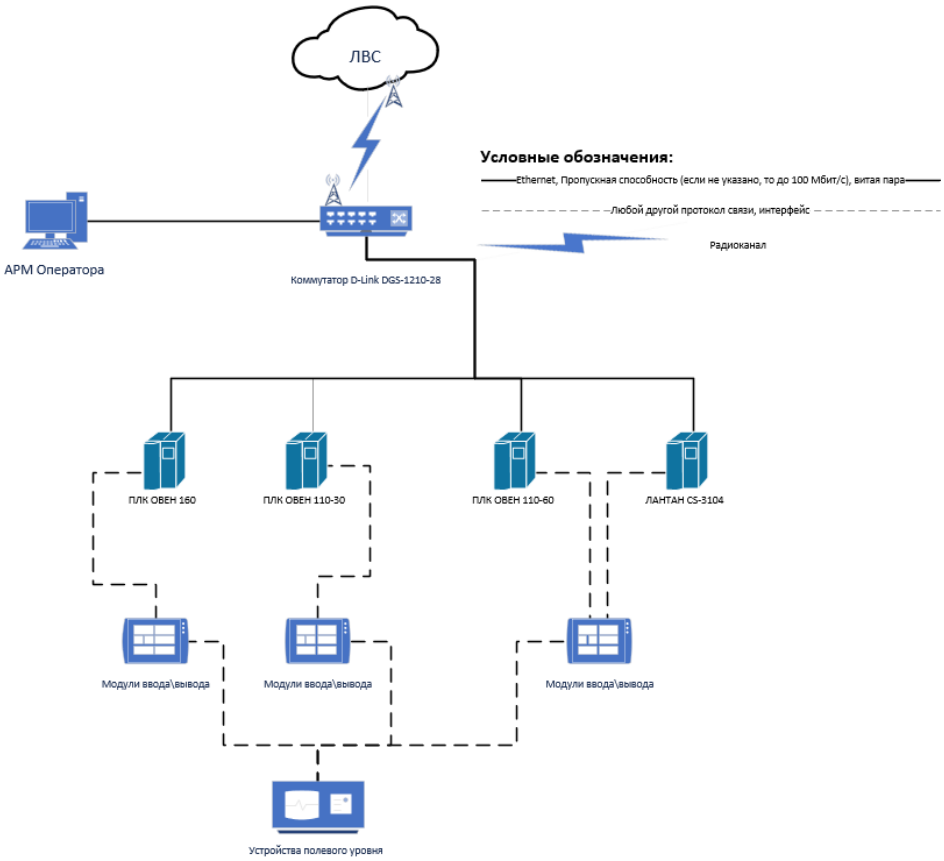


Рис. 10. Типовая схема сети АСУ ТП

Определение актуальных угроз безопасности информации

С учетом всех факторов рассмотренных ранее был проведен анализ угроз безопасности информации, представленных в банке данных угроз ФСТЭК России [4] и определен топ-10 актуальных угроз безопасности информации для информационных систем, функционирующих в сфере топливно-энергетического комплекса:

1. Угроза искажения вводимой и выводимой на периферийные устройства информации (УБИ.27).
2. Угроза использования механизмов авторизации для повышения привилегий (УБИ.31).
3. Угроза неправомерных действий в каналах связи (УБИ.69).
4. Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети (УБИ.73).
5. Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб (УБИ.98).
6. Угроза определения типов объектов защиты (УБИ.103).

7. Угроза отключения контрольных датчиков (УБИ.107).

8. Угроза отказа подсистемы обеспечения температурного режима (УБИ.180).

9. Угроза перехвата управления автоматизированной системой управления технологическими процессами (УБИ.183).

10. Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров (УБИ.204).

Реализация перечисленных выше угроз безопасности информации может привести к следующим негативным последствиям:

– Нарушение штатного режима функционирования АСУ ТП.

– Простой АСУ ТП.

– Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка ПО, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств).

– Утечка защищаемой информации.

– Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций).

– Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).

– Нарушение законодательства Российской Федерации.

– Недополучение ожидаемой (прогнозируемой) прибыли.

– Причинение ущерба жизни и здоровью людей.

– Возникновение ущерба бюджетам Российской Федерации.

– Вредные воздействия на окружающую среду.

Заключение.

Таким образом, были определены наиболее вероятные для реализации в отношении информационных систем, функционирующих в сфере топливно-энергетического комплекса, угрозы безопасности информации. Для данных угроз можно подобрать тактики и соответствующие им техники реализации, которые обеспечат корректный подбор комплекса технических и организационных мер защиты информации для митигации угроз безопасности информации и последствий их реализации.

Список используемых источников:

1. Таргетированные или целевые кибератаки «Развитая устойчивая угроза» [Электронный ресурс] // TAdviser Advanced Persistent Threat (APT). URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:APT__%D0%A2%D0%B0%D1%80%D0%B3%D0%B5%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5_%D0%B8%D0%BB%D0%B8_%D1%86%D0%B5%D0%BB%D0%B5%D0%B2%D1%8B%D0%B5_%D0%B0%D1%82%D0%B0%D0%BA%D0%B8 (дата обращения: 23.10.2023).

2. Вериго А. А., Цапко Г. П., Каташев А. С. Оценка уязвимостей автоматизированных систем управления технологическими процессами [Электронный ресурс] // Международный научно-исследовательский журнал URL: https://research-

journal.org/archive/11-53-2016-november/ocenka-uyazvimostej-avtomatizirovannyx-sistem-upravleniya-texnologicheskimi-processami (дата обращения: 22.10.2023).

3. Безопасность АСУ ТП критически важных объектов [Электронный ресурс] // Security and Safety. URL: http://lib.secuteck.ru/articles2/security-director/bezopasnost-asu-tp-kriticheski-vazhnyh-obektov (дата обращения: 23.10.2023).

4. Банк данных угроз ФСТЭК России [Электронный ресурс]. URL: https://bdu.fstec.ru/threat (дата обращения 23.10.2023).

Aleksandrova A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Determination of the TOP 10 current threats to information security for information systems operating in the field of the fuel and energy complex.

Currently, information systems play a key role in various industries, including the fuel and energy complex. They provide efficient process management, increase productivity and provide advanced capabilities for managing data flows in enterprises. However, with the development of technology and the expansion of information systems capabilities, new threats to information security arise. This article will examine the top 10 most pressing threats to information security for information systems operating in the fuel and energy complex.

Key words: threat to information security, targeted attack, automated process control system

УДК 004.056
ГРНТИ 81.93.29

МОДЕЛЬ ПРОЦЕССА РАЗРАБОТКИ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР

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

В современном мире большие компании все чаще сталкиваются с атаками на программное обеспечение для информационных инфраструктур, одним из основных пунктов для предотвращения данных атак может служить статическая проверка исходного кода на уязвимости.

информационная безопасность, информационная инфраструктура, разработка, программное обеспечение, статический анализ кода

Проблема в уязвимом программном обеспечении (ПО) может иметь серьезные последствия для пользователей и организаций, которые его используют. Найденные уязвимости могут быть использованы злоумышленниками для получения несанкционированного доступа к конфиденциальным данным, кражи личной информации, установки вредоносного ПО или причинения другого вреда. В 2021 году компания Check Point Research зафиксировала увеличение числа атак на корпоративные сети на 50% в неделю по сравнению с 2020 годом [1], результаты представлены на рис. 1. Анализ показал, что число атак в России выросло на 54% по сравнению с 2020 годом.

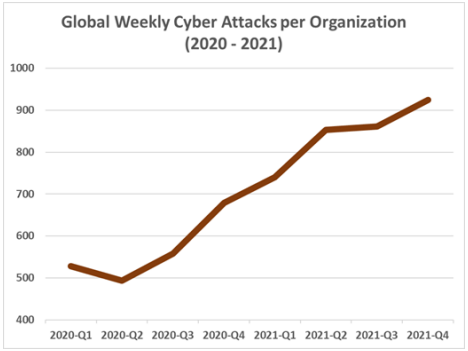


Рис. 1. Статистика роста атак на организации

Для того, чтобы понять, как защитить приложение от уязвимостей, рассмотрим жизненные циклы разработки программного обеспечения, а именно Software development lifecycle (SDLC) представляет собой несколько этапов через которые проходит любое ПО, а именно[2]:

- Анализ требований. На этом этапе анализируются и документируются требования к программному продукту, включая функциональные и нефункциональные требования.

- Планирование. На этом этапе определяются цели проекта, определяются требования к программному продукту и создается план проекта.
- Проектирование. На этом этапе разрабатывается архитектура программного продукта, определяется структура системы, выбираются технологии и платформы.
- Разработка. На этом этапе создается и тестируется код, реализующий функциональность программного продукта, используя выбранные технологии и платформы.
- Тестирование. На этом этапе проверяется работоспособность программного продукта и соответствие его требованиям.
- Развертывание. На этом этапе программный продукт выпускается и устанавливается на серверах или устройствах конечных пользователей.
- Сопровождение. На этом этапе программный продукт поддерживается и обновляется, чтобы соответствовать новым требованиям и устранять выявленные ошибки и проблемы.

В случае игнорирования или ошибочных действий в процессе выполнения вышеописанных этапов SDLC может появится уязвимость.

Стоит также определить, чем уязвимость отличается от дефекта. Дефекты (недостатки) – это ошибки, сбои и прочие проблемы реализации, проектирования или архитектуры программного обеспечения, которые могут привести к уязвимостям. Уязвимости – уже найденные кем-то ошибки, которые могут быть напрямую использованы злоумышленниками для получения доступа к системе или сети, нарушения работы сервисов [3].

В связи с ростом сложности информационных систем, возникают угрозы безопасности информации, связанные с наличием уязвимостей в программном коде, который используется в составе этих систем. Для обеспечения защиты от таких угроз обычно применяются комплексные меры, внедряемые в процессы эксплуатации и поддержки программного обеспечения. Для достижения необходимого уровня защиты информации требуется реализация мер, направленных на предотвращение возникновения и устранение уязвимостей программ на разных этапах жизненного цикла программного обеспечения, начиная с проектирования, продолжая реализацией и завершая тестированием.

Источником для определения мер по разработке безопасного ПО, можно считать методические материалы ГОСТ Р 56939-2016 [3].

Реализация мер по разработке безопасного ПО помогает достичь требований безопасности, которые предъявляются к разрабатываемому ПО, чтобы оно могло быть использовано в процессах жизненного цикла ПО, связанных с его проектированием, реализацией и тестированием. Успешная реализация этих мер приводит к формулированию перечня требований по безопасности для разрабатываемого ПО. Разработчику ПО необходимо определить требования безопасности, которые должны быть учтены при разработке ПО. Для организации работ в процессах жизненного цикла ПО и

подтверждения соответствия требованиям настоящего стандарта, документация разработчика ПО должна содержать перечень определенных требований безопасности, предъявляемых к разрабатываемому ПО.

В качестве источников для формирования требований разработчик ПО может использовать требования законов, нормативных правовых актов, отраслевых ПО. Например, могут быть определены следующие требования к ПО:

- Обеспечение идентификации и аутентификации
- Обеспечение защиты от несанкционированного доступа к информации
- Обеспечение регистрации событий
- Обработка программных ошибок и исключительных ситуаций

Необходимо также обеспечить проведение статического анализа исходного кода программы для выявления недостатков. Статический анализ следует проводить для компонентов, включенных в ПО и имеющих доступный исходный код. По результатам анализа могут быть проведены доработки программы. Для организации работ в процессах жизненного цикла ПО, документация разработчика ПО должна содержать список выявленных потенциально уязвимых конструкций в исходном коде программы. Для подтверждения соответствия требованиям стандарта, документация разработчика ПО должна также содержать следующую информацию:

- Сведения о периодичности проведения статического анализа исходного кода программы
- Наименование и идентификационные признаки инструментальных средств, используемых для проведения статического анализа исходного кода программы
- Список выявленных потенциально уязвимых конструкций в исходном коде программы, описание действий, направленных на их устранение, или обоснование невозможности или отсутствия необходимости в доработке программы.

В ответ на постоянно растущую угрозу и увеличение строк кода разработчики используют инструменты AST (Application Security Testing) [4]. AST – это процесс повышения безопасности приложений путём выявления уязвимостей в исходном коде. Изначально такое тестирование проводилось вручную. Однако рост количества строк кода и случаев применения стороннего открытого кода, который тоже нужно проверять, привели к необходимости автоматизации процесса. Исследовательский центр кибербезопасности Synopsys (CyRC) и Censuswide международная консалтинговая компания по исследованию рынка, провели опрос 1500 ИТ-специалистов, в обязанности которых входит DevSecOps [5], а также которые работают в области кибербезопасности приведенный на рис. 2.

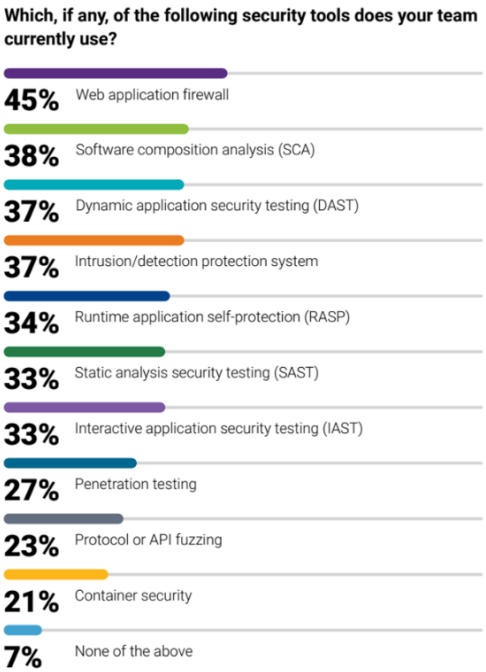


Рис. 2. Статистика использования инструментов безопасности

Как видно компании используют различные инструменты анализа кода и обеспечения безопасности ПО, однако поскольку в данной ВКР речь идет об оценки эффективности процессов DevSecOps предлагаю сосредоточиться именно на [6]: SAST, DAST и IAST:

SAST (Статическое тестирование безопасности приложений) включает анализ исходного кода приложения для обнаружения уязвимостей в системе безопасности до его развертывания. В методологии DevSecOps SAST применяется на ранних этапах жизненного цикла разработки для обнаружения уязвимостей безопасности, что уменьшает вероятность обнаружения проблем на более поздних этапах, когда исправление становится сложнее и дороже. Обычно SAST интегрируется в процесс непрерывной интеграции и доставки (CI/CD), автоматизируя процесс тестирования и предоставляя разработчикам мгновенную обратную связь по выявленным проблемам безопасности. Инструменты SAST способны обнаруживать широкий спектр уязвимостей, включая SQL-инъекции, межсайтовые скрипты, переполнение буфера и многое другое. SAST является одним из основных методов для поиска уязвимостей в исходном коде приложений. Статический анализ выполняется на этапе написания кода и позволяет обнаружить ошибки и уязвимости в ранней стадии разработки, что помогает снизить затраты на их исправление. Кроме того, этот метод применим к большинству языков программирования.

На сегодняшний день уже имеется достаточно обширной список отечественных статических анализаторов кода, которые могут выступать в роли импортозамещения иностранных решений. Несмотря на это, интегрирование данных инструментов в процесс разработки все еще

игнорируется многими компаниями, в ввиду сложной настройки анализаторов с программной точки зрения.

Список используемых источников:

1. Check point research's 2021 security report [Электронный ресурс]. URL: https://research.checkpoint.com/2021/helping-you-immunize-your-organization-against-the-cyber-pandemic-check-point-researchs-2021-security-report/ (дата обращения: 22.11.2023)

2. «Ростелеком-Солар»: SDLC Жизненный цикл разработки ПО [Электронный ресурс]. URL: https://rt-solar.ru/products/solar_appscreener/2394/ (дата обращения: 22.11.2023)

3. ГОСТ Р 56939-2016 [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200135525 (дата обращения: 22.11.2023)

4. О видах Application Security Testing [Электронный ресурс]. URL: https://vc.ru/dev/551456-kak-ne-zaputatsya-sredi-sast-dast-i-iast-ili-o-vidah-application-security-testing (дата обращения: 22.11.2023)

5. SAST, DAST, IAST, and RASP: how to choose? [Электронный ресурс]. URL: https://www.ptsecurity.com/ww-en/analytics/knowledge-base/sast-dast-iast-and-rasp-how-to-choose/ (дата обращения: 22.11.2023)

6. Dynamic Application Security Testing Market – Forecast (2023 - 2028) [Электронный ресурс]. URL: https://www.industryarc.com/Research/Dynamic-Application-Security-Testing-Market-Research-500746 (дата обращения: 22.11.2023)

Alexeychuk P.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

A model of the process of developing secure software for critical information infrastructures.

In the modern world, large companies are increasingly facing attacks on software for information infrastructures, one of the main points for preventing these attacks can be a static source code analysis for vulnerabilities.

Key words: information security, information infrastructure, development, software, static code analysis.

УДК 004.056.53
ГРНТИ 81.93.29

STUDY AND ANALYSIS OF THE AUTOMATED ADVERSARY EMULATION PLATFORM MITRE CALDERA

S. Alkattan, R. B. Petriv
The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Threats in the cyberspace are constantly evolving, and threat actors continue to improve their techniques and find many different ways evading possible defenses to gain unauthorized access to systems, in order to prevent these threats, organizations spend resources conducting penetration tests to uncover weak points. Adversary emulation aims to construct and then follow a scenario that mimics the behavior of known threats to test detection capabilities of malicious behavior within a system of an organization. The purpose of this work was to evaluate the effectiveness of the adversary emulation tool MITRE CALDERA.

adversary, tactics, techniques, APT

When talking about challenges in cybersecurity, one of the problems is determining which actor is behind the attacks, commonly known as a Cybercriminal, what their motivations are, and above all asking, how did they manage to overcome the organization's security controls?

Understanding a cyber-attack: when performing security monitoring, the first steps are to detect observed events and tie them to a chain of actions of an adversary.

Currently, cybersecurity industries have been developing new defense systems with the purpose of increasing the visibility and profiling of adversaries, one of them is the MITRE organization with its ATT&CK Framework (Adversary tactics, techniques and common knowledge) [1], which consists of a repository of information that contains techniques, tactics and procedures that cyber attackers usually use, information collected from real-world observations, thus allowing us to understand the behavior of adversaries.

MITRE ATT&CK allows defensive capabilities to improve since it has a holistic approach involving the following use cases: Adversarial simulation, Functionality tests of security solutions, Understanding a cyber-attack.

Taking into account the determining factors previously explained, the MITRE organization created an adversary emulation software with an Apache 2.0 license called CALDERA [2], which is supported on MITRE ATT&CK, whose purpose is to help organizations increase its cybersecurity defense levels by saving resources and automating adversary emulation tasks [3].

The aim of this research is to study Caldera’s capabilities and compare them with other open-source counterparts that also use the ATT&CK matrix like Atomic Red Team [5] and red team automation (RTA) [6] and even some of the commercial tools like cobalt strike [13] also uses the matrix, in terms of effectiveness in implementing cyber-attacks, analyze the effects left by this type of

attacks, and draw conclusions that may contribute to the development of protection systems against them.

It is necessary to talk about other adversary models. Among the best-known Adversarial models is Lockheed Martin's Cyber Kill Chain [8], Mandiant's attack lifecycle, it should be noted that the objective is to demonstrate the effectiveness of MITRE ATT&CK.

Lockheed Martin's model describes the activities of a cybercriminal from the beginning to the end of the attack as shown in Fig. 1.

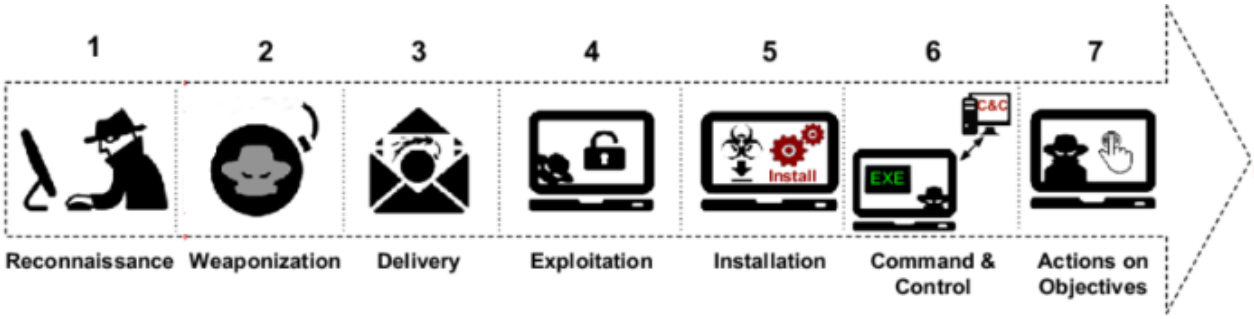


Fig. 1. Lockheed Martin's model [7]

The techniques are given to describe the attacks and are made up of 7 stages that are as follows: Reconnaissance →Weaponization →Delivery →Exploitation →Installation →Command and Control →Actions on Objectives

The Mandiant Attack life cycle_built by the FireEye [9] organization provides a Cyber-attack model that describes the life cycle of an attack from the experience seen by this organization as shown in Fig. 2, the objective of this life cycle is the early detection of adversaries.

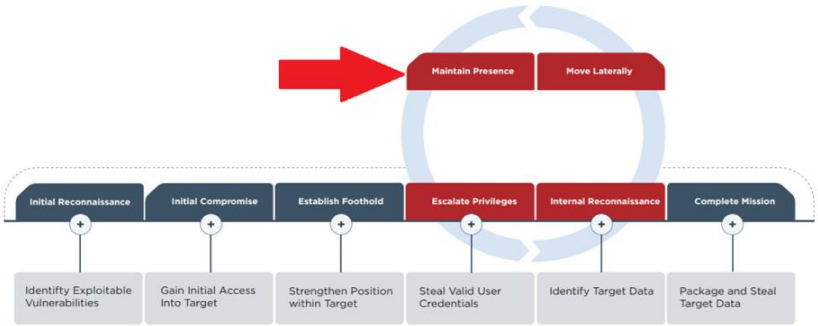


Fig. 2. The Mandiant Attack life cycle [8]

The phases are: Initial Reconnaissance →Establish Foothold →Initial Compromise →Escalate Privileges →Internal Reconnaissance →Move Laterally →Maintain Presence →Complete Mission

What is MITRE ATT&CK: The MITRE ATT&CK cybersecurity framework, a knowledge base of the tactics and techniques used by attackers, continues to gain traction as vendors, enterprises and security service providers adopt and adapt the framework to their defenses.

Unlike other security frameworks such as Lockheed Martin's Cyber Kill Chain, or the Mandiant Attack lifecycle, MITRE ATT&CK differentiates itself and

takes advantage by detailing how an adversary attack can be executed, providing greater information.

ATT&CK Model: To address ATT&CK it is known as Tactics, Techniques and Knowledge of Common Adversaries was developed by the MITRE organization also known as ATT&CK matrix as shown in Figure 3, the objective is to describe and categorize adverse behaviors based on observations of cyberattacks around the world, its strategy is based on the following items [10]:

– **Tactic**: Tactics represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical objective: the reason for performing an action

– **Technique**: Techniques represent "how" an adversary achieves a tactical objective by performing an action.

– **Sub-technique**: Sub-techniques are a more specific description of adversary behavior used to achieve an objective.

– **The procedures**: They are the specific implementation that the adversary uses for techniques or sub-techniques.

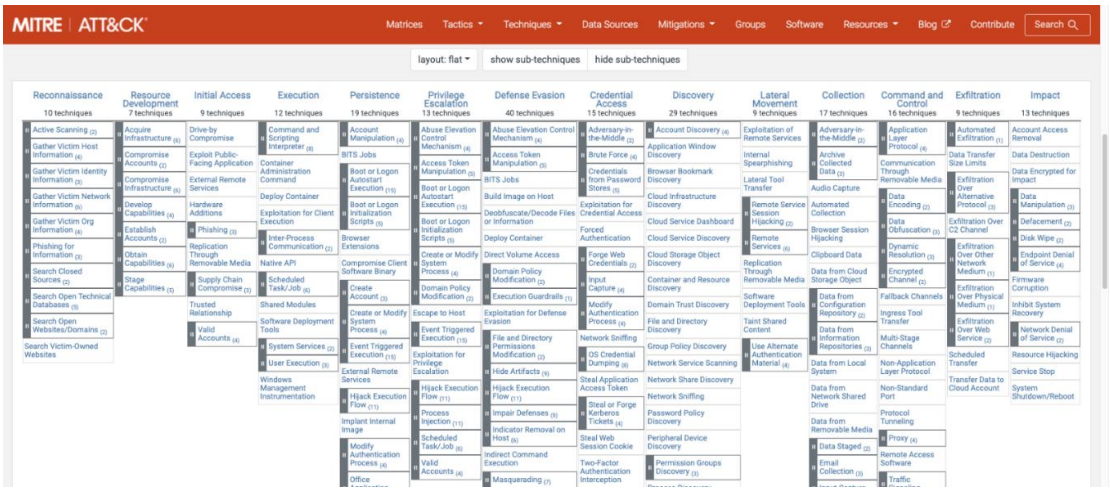


Fig. 3. ATT&CK matrix [14]

There exist many ways of testing the security aspects of a system. This can be done by performing penetration testing, where the goal is to perform a detailed assessment on a system to learn how it might be exploited and to find vulnerabilities that might be exploited.

Red team exercise an exercise [12], reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization (defending system).

Adversary emulation is a little bit different from red teaming exercises as adversary emulation aims to construct and then follow a scenario that mimics the behavior of known threats. This is done by using threat intelligence, such as which tactics, techniques, and procedures (TTP) the threat group uses. According to the computer security resource center at the National Institute of Standards and Technology (NIST), TTP is defined as the behavior of an actor. Tactics are the

highest abstraction level of what the actor wants to achieve, and techniques are at a lower abstraction level describing how the tactic is fulfilled [13]. Procedures are a detailed description of techniques, and the same technique can have many different procedures.

MITRE CALDERA is a project for investigative purposes developed by the MITRE organization [4]. Which developed software that is based on the MITRE ATT & CK cybersecurity framework, in order to easily execute autonomous attack simulation exercises with adversary emulation capabilities, focusing on post-compromise activities. It is also used to run manual red team simulations or automatic incident response.

CALDERA acts as an automated and intelligent red team, probing the target network for weaknesses and training defender.

Caldera Components:

1) The core system: This is the framework code, which consists of what is available in this repository. An asynchronous command and control (C2) server with a REST API and web interface is included;

2) Plugins: These are separate repositories that hang off the central framework, providing additional functionality. Examples include agents, GUI interfaces TTP collections, and more.

References:

1. Intelligent, Automated Red Team Emulation Andy Applebaum, Doug Miller, Blake Strom, Chris Korban, and Ross Wolf The MITRE Corporation [Electronic resource]. URL: https://clck.ru/36ezwv (online accessed 09.10.2023).

2. MITRE CALDERA GitHub repository [Electronic resource]. URL: https://github.com/mitre/caldera (online accessed 09.10.2023).

3. MITRE CALDERA official website [Electronic resource].URL: https://caldera.mitre.org/ (online accessed 15.11.2023).

4. MITRE CALDERA's documentation [Electronic resource]. ULR: https://caldera.readthedocs.io/en/latest/ (online accessed 13.10.2023).

5. Atomic Red Team GitHub repository [Electronic resource]. URL https://github.com/redcanaryco/atomic-red-team#atomic-red-team (online accessed 17.10.2023).

6. Red Team Automation (RTA) Team GitHub repository [Electronic resource]. URL: https://github.com/endgameinc/RTA (online accessed 17.10.2023).

7. Lockheed Martin's Cyber Kill Chain [Electronic resource]. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (online accessed 18.10.2023).

8. The Mandiant Attack life [Electronic resource]. URL: https://www.mandiant.com/resources/insights/targeted-attack-lifecycle?__cf_chl_tk=UAFHUd3tpEOQoabmQ2QEY6U6e.lrlSVyjBmQnWg6dGw-1698884005-0-gaNycGzNDuU (online accessed 20.10.2023).

9. Frequently Asked Questions on MITRE ATT&CK website URL:FAQ - Frequently Asked Questions | MITRE ATT&CK® (online accessed 21.10.2023).

10. "About Penetration Testing." In: IEEE Security Privacy 5.6 (Nov. 2007) [Electronic resource]. URL: https://ieeexplore.ieee.org/document/4402456 (online accessed 15.11.2023).

11. National Institute of Standards and Technology NIST, definitions [Electronic resource].

URL:https://csrc.nist.gov/glossary/term/red_team_exercise#:~:text=Definitions%3A,the%20information%20system%20and%20organization (online accessed 26.10.2023).

12. National Institute of Standards and Technology NIST, definitions [Electronic resource]. URL: https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures (online accessed 26.10.2023).

13. Cobalt strike [Electronic resource]. URL: https://attack.mitre.org/software/S0154/ (online accessed 17.10.2023).

14. MITRE ATT&CK official website [Electronic resource].URL: https://attack.mitre.org/ (online accessed 11.10.2023).

Alkattan S., Petriv R.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Threats in the cyberspace are constantly evolving, and threat actors continue to improve their techniques and find many different ways evading possible defenses to gain unauthorized access to systems, in order to prevent these threats, organizations spend resources conducting penetration tests to uncover weak points. Adversary emulation aims to construct and then follow a scenario that mimics the behavior of known threats to test detection capabilities of malicious behavior within a system of an organization. The purpose of this work was to evaluate the effectiveness of the adversary emulation tool MITRE CALDERA.

Key words: adversary, tactics, techniques, APT

УДК 004.032.26
РНТИ 28.23.37

РАЗВИТИЕ ТЕНДЕНЦИЙ В ОБЛАСТИ НЕЙРОСЕТЕЙ

Б. А. Аль-Нами, Д. Д. Коваленко, П. А. Шиян
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Эта статья представляет собой обзор ключевых моментов развития нейросетей, включая их обучение и адаптивность. Графическое представление процесса обучения нейросетей усиливает наглядность и понимание читателей относительно динамики улучшения их работы во времени.

нейронная сеть, искусственный интеллект, искусственные нейронные сети, нейронные сети и информационные технологии, особенности нейронных сетей, области применения нейронных сетей

Современные технологии нейросетей претерпевают быстрое развитие, оказывая значительное влияние на различные сферы человеческой жизни. В данной статье мы проведем анализ динамики развития нейросетей на временной оси и рассмотрим их ключевые аспекты, включая обучение и адаптивность.

Нейросети сегодня находят применение в различных областях, начиная от распознавания образов и заканчивая автоматизированным управлением производством. С их появлением начался активный процесс исследований и разработок, который с течением времени лишь усилился[1].

Первые Эксперименты: Начиная с 1950-х годов, первые исследования в области искусственных нейронных сетей были ограничены малыми вычислительными ресурсами. Основные концепции нейронных сетей, такие как перцептрон Розенблатта, возникли в этот период.

Эра Глубокого Обучения: С развитием вычислительных технологий и появлением мощных графических процессоров, идея глубокого обучения стала основополагающей, приводя к созданию глубоких нейросетей. Это период, когда нейросети стали способными решать сложные задачи в области компьютерного зрения, обработки естественного языка и многих других[2].

Трансфер Обучение и Пренебрежение Алгоритмами: Современные нейросети успешно используют техники трансфер обучения, что позволяет применять знания, полученные на одной задаче, к решению другой. Это также сопровождается переходом от ручного проектирования алгоритмов к обучению алгоритмов через данные. Эффективность этого метода стала особенно очевидной в сфере обработки естественного языка, где нейросети достигли впечатляющих результатов.

Обучение нейросетей - ключевой этап в их развитии. Сложные алгоритмы обучения позволяют нейросетям учиться на больших объемах данных и решать сложные задачи. Одной из основных методик обучения

является обратное распространение ошибки (Backpropagation), который позволяет сети корректировать свои веса и биасы для минимизации ошибки предсказания. Давайте подробнее рассмотрим процесс обучения нейросетей[3].

Обучение нейросетей происходит путем подачи на вход сети обучающих данных, которые содержат входные признаки и ожидаемые выходы. Сеть обрабатывает эти данные и генерирует прогнозы. Затем вычисляется разница между прогнозами и ожидаемыми выходами, и эта разница называется "ошибкой". Задача обучения - минимизировать эту ошибку.

Процесс обучения можно представить следующим образом:

- Инициализация: В начале обучения веса нейросети устанавливаются случайным образом.
- Прямое распространение: Данные передаются через нейросеть, и сеть генерирует прогнозы.
- Оценка ошибки: Сравниваются прогнозы с ожидаемыми выходами, и вычисляется ошибка.
- Обратное распространение ошибки (Backpropagation): Ошибка распространяется назад через сеть, и веса корректируются так, чтобы уменьшить ошибку.
- Итерации: Шаги 2-4 повторяются многократно для каждого обучающего примера.
- Оптимизация: Существует множество методов оптимизации, таких как стохастический градиентный спуск, которые помогают найти оптимальные значения весов для минимизации ошибки[4].
- Завершение обучения: Обучение завершается, когда сеть достигает уровня производительности, удовлетворяющего требованиям задачи.

Графическое Представление Обучения Нейросетей

Для наглядного представления процесса обучения нейросети, часто используют графики. На рис. 1 рассмотрим пример графика, иллюстрирующего обучение нейросети:

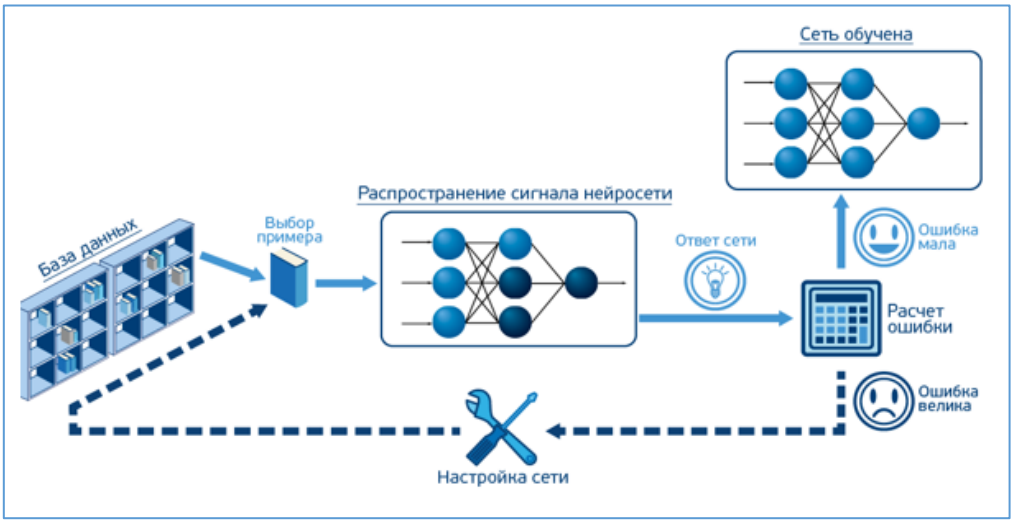


Рис. 1. Процесс обучения нейросети

С развитием технологий нейросети стали все более адаптивными к различным сценариям использования. Они могут оптимизироваться под разные архитектуры процессоров, а также адаптироваться к различным задачам, начиная от обработки текста и изображений и заканчивая управлением роботами[5].

Адаптивность нейросетей проявляется в их способности обучаться на новых данных и задачах. Это означает, что нейросети могут быть применены в различных областях, даже если изначально были обучены для решения совершенно других задач[6].

Нейросети продолжают оставаться в центре внимания исследователей и инженеров, обогащая наш опыт и понимание искусственного интеллекта. Продвинутые методы обучения и их адаптивность делают нейросети универсальным инструментом, способным решать различные сложные задачи в современном мире

Список используемых источников:

1. Тихонов А. А. Большие данные и глубокое машинное обучение в искусственных нейронных сетях // Наука и образование сегодня. 2018. N 6 (29). С. 35-38.

2. Туровский Я. А. Автоматизирование обучения нейрочипов// Актуальные направления научных исследований века: теория и практика. 2015. N 5, Ч. 2(16-2). С. 191-196.

3. Бондарев В. Ю., Сорокин А. С., Кротова Е. Л. Искусственная нейронная сеть как средство и метод статистическогй обработки данных // Вестник УрФО. Безопасность в информационной сфере. 2016. N 2 (20). С. 19-22.

4. Сердюков В. И. Использование элементов искусственного интеллекта для повышения надежности технических изделий // Вестник машиностроения. 2017. N 10. С. 29-32.

5. Рыков В.П. Модульный принцип обучения искусственных нейронных сетей на примере известных нейросетевых топологий // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2014. Т. 19. N 2. С. 583-586.

6. Туровский Я. А. Автоматизирование обучения нейрочипов// Актуальные направления научных исследований века: теория и практика. 2015. N 5. Ч. 2(16-2). С. 191-196.

Al-Nami B.A., Kovalenko D.D., Shiyan P.A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development trends in the field of neural networks.

This article provides an overview of the key aspects of the development of neural networks, including their learning and adaptability. A graphical representation of the learning process of neural networks enhances the visibility and understanding of readers regarding the dynamics of improvement of their work over time.

Key words: neural network, artificial intelligence, artificial neural networks, neural networks and information technologies, features of neural networks, areas of application of neural networks.

УДК 004.822
ГРНТИ 20.53.19

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ВЛОЖЕНИЯ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯ ПРИ ПОМОЩИ GAN-СИСТЕМ

К. А. Ахрамеева, Г. В. Жиляков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящей работе представлен результат анализа вложения текстовой информации в цветные изображения при помощи искусственного интеллекта, а также извлечение секретной информации из полученного изображения при помощи ИИ. Программа, разработанная для вложения дополнительной информации, самостоятельно определяет пиксели для осуществления вложения, при обеспечении оптимальной защиты от атак, наилучшего качества стегообъекта, вложенной информации, а также приемлемого качества для извлечения вложенной информации. Используя несколько алгоритмов, программа выдает готовое изображение с секретным сообщением. Реализация данного метода вложения при помощи искусственного интеллекта повышает качество полученного изображения, повышает устойчивость полученных изображений к примитивным методам стегоанализа, и методам стегоанализа на основе ИИ.

генеративно-состязательные сети; стеганография; машинное обучение; GAN-системы

Постоянное развитие сетевых технологий подчеркивает растущую проблему сохранения конфиденциальности сообщений, чему зачастую препятствуют постоянно растущие вычислительные возможности. В таких условиях лучшим подходом становится сокрытие самого факта существования сообщения, чем в альтернативной структуре [1-3].

Сокрытие информации представляет собой ключевой момент в обеспечении целостности данных в сети. Этот метод позволяет незаметно внедрить конфиденциальную информацию в носитель [4]. Ее полезность выходит за рамки сохранения конфиденциальности данных и включает в себя обеспечение безопасной передачи информации. Стеганография, как важнейший инструмент сокрытия информации, все чаще становится объектом научных исследований как на внутреннем, так и на международном уровне.

В 2014 году Гудфеллоу и др. [5] предложили генеративную состязательную сеть (GAN), которая дает возможность сочетания глубокого обучения и скрытия информации. Существующие модели стеганографии, основанные на глубоком обучении, можно разделить на две категории в зависимости от их направленности: 1 – на увеличение емкости, 2 – на повышение безопасности моделей стеганографии.

В данной работе рассматривается модель стеганографии с двух точек зрения: архитектуры сети и функции потерь. По сравнению с существующими моделями стеганографии, используемыми для скрытия

цветных изображений, данная кодирующая сеть, состоящая из слоев понижающей, остаточной и повышающей дискретизации, позволяет получать стеганографические изображения с низким уровнем искажения цвета и высоким визуальным качеством. В то же время в данной модели присутствует элемент стеганализа в качестве дискриминатора для повышения безопасности модели путем обучения с помощью сети кодер-декодер.

Архитектура модели стеганографии состоит из трех подсетей: кодера, декодера и дискриминатора. Сеть кодировщика-декодировщика, известная также как сеть скрытия-извлечения, используется в качестве генератора для создания стеганографических изображений и раскрытия секретных изображений с низким уровнем искажения цвета и высоким визуальным качеством. Затем стеганографические изображения, полученные с помощью указанных подсетей, используются в качестве входных данных для сети дискриминатора. При этом безопасность стеганографических изображений повышается за счет обучения по принципу состязательности. В процессе обучения искажение стеганографического изображения и реконструированного секретного изображения, а также способность противостоять обнаружению моделей стеганализа (дискриминаторов) могут использоваться в качестве измерительного показателя для оптимизации весов стеганографической модели. Общая схема модели представлена на рис. 1.

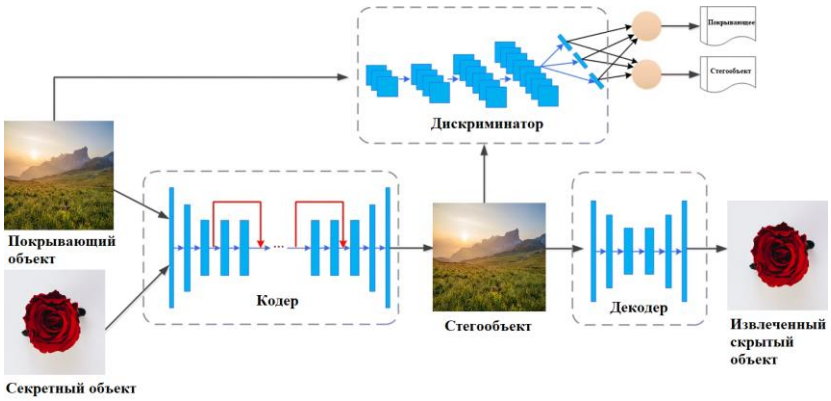


Рис. 1. Общая архитектура модели

Методы стеганографии на основе генеративно-состязательных сетей также обычно оцениваются по их способности избегать обнаружения инструментами стегоанализа. Был использован популярный инструмент стегоанализа с открытым исходным кодом под названием StegExpose [39].

Случайным образом были выбраны 1000 изображений обложек из тестового набора, создавая соответствующие стеганографические изображения, и изучены результаты с помощью StegExpose. Кривая рабочих характеристик приемника показана на рис. 2 и, стоит отметить, что инструмент StegExpose лишь немногим эффективнее случайного угадывания с площадью под ROC-кривой 0,59, даже для полезной нагрузки до 4,4 бит на пиксель. Это показывает, что модель может успешно обходить стандартные

инструменты стегоанализа, отвечая минимальным требованиям для того, чтобы быть жизнеспособным алгоритмом стеганографии.

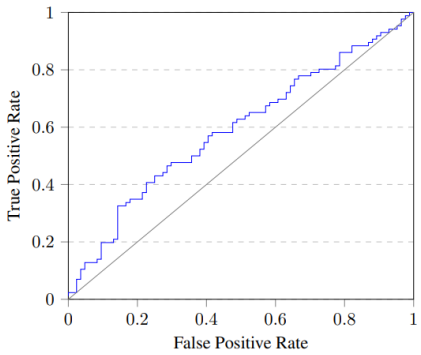


Рис. 2. ROC-кривая рабочих характеристик

Недавние исследования показали многообещающие результаты в обнаружении стеганографических изображений с использованием подходов, основанных на глубоком обучении [44]. Поэтому, можно приступить к изучению того, может ли модель обойти инструменты стегоанализа, основанные на глубоком обучении. Будет использована модель, предложенную Ye et al., для стегоанализа с небольшой модификацией, позволяющей поддерживать цветные изображения, и обучить его обнаруживать стеганографические изображения, созданные данной моделью.

Рис. 3 показывает производительность детектора для различных относительных полезных нагрузок и размеров обучающей выборки. Во-первых, стоит отметить, что производительность детектора, измеряемая площадью под рабочей характеристикой приемника (auROC), увеличивается по мере увеличения количества битов на пиксель, закодированных в изображении.

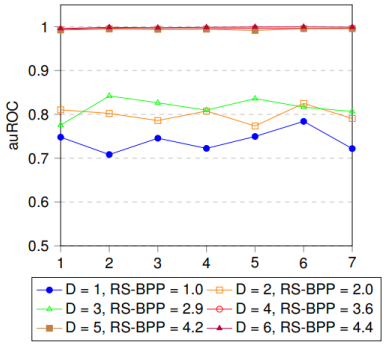


Рис. 3. На этом графике показана производительность стеганографического детектора на протянутом тестовом наборе. По оси x указано количества различных SteganoGAN экземпляров, которые использовались, а ось Y указывает площадь под кривой ROC

Кроме того, можно выделить тот факт, что нет четкой тенденции в области под кривой ROC, поскольку увеличивается количество SteganoGAN модели, используемые для обучения.

Это говорит о том, что другой стороне будет сложно построить модель, способную обнаруживать стеганографические изображения, сгенерированные SteganoGAN, не зная точных параметров модели.

Глубокое обучение для стеганографии изображений недавно изучалось в нескольких исследованиях, и все они показали многообещающие результаты. Существующие предложения варьируются от обучения нейронных сетей до интеграции и улучшения традиционных методов стеганографии для завершения сквозных сверточных нейронных сетей, которые используют состязательное обучение для создания убедительных стеганографических изображений.

Многие работы, представленные выше доказали, что глубокое обучение можно использовать для практической сквозной стеганографии изображений, и достигли скорости встраивания, конкурентоспособной по сравнению с теми, которые достигаются с помощью традиционных методов.

Список используемых источников:

1. Коржик В. И., Яковлев В. А. Основы криптографии. Учебное пособие // Санкт-Петербург, 2017.
2. Герасимович А. С., Коржик В. И., Старостин В. С. Исследования бесключевой криптосистемы Дина-Голдсмита // Труды учебных заведений связи. 2017. Т. 3. N 3. С. 43-50.
3. Korzhik V. I., Starostin V. S., Kabardov M. M., Gerasimovich A. M., Yakovlev V. A., Zhuvikin A. G. Information theoretically secure key sharing protocol executing with noiseless public channels // Математические вопросы криптографии. 2021. Т. 12. N 3. С. 125-141.
4. Petitcolas F. A., Anderson R. J., Kuhn M. G. Сокрытие информации. 1999. С. 1062–1078.
5. Goodfellow I., Pouget-Abadie J., Mehdi M., Xu B., Warde-Farely D., Ozair S., Courvile A., Bengio Y. : материалы семинаров Европейской конф. по компьютерному зрению (ECCV), 8-14 сент. 2018 г. Мюнхен : под ред. Ghahramani Z., Welling M., Cotes C., Lawrence N. D., и Weinberger K. Q. Генеративно-состязательные сети, С. 723–729.
6. Zhu J., Kaplan R., Johnson J., and Fei-Fei L. HiDDeN : Hiding data with deep networks. CoRR, abs/1807.09937, 2018.

Akhrameeva K., Zhilyakov G.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Research on the possibility of embedding information into images using GAN SYSTEMS
This paper presents the result of analysis of text information embedding into color images using artificial intelligence, as well as the extraction of secret information from the obtained image using AI. The program developed for embedding additional information independently determines the pixels to perform the embedding, while providing optimal protection against attacks, best quality of stegoobject, embedded information, and acceptable quality for extracting the embedded information. Using several algorithms, the program produces a finished image with a secret message. The implementation of this embedding method using artificial intelligence improves the quality of the obtained image, increases the robustness of the obtained images to primitive stegoanalysis methods, and AI based stegoanalysis methods.

Key words: generative-adversarial networks; steganography; machine learning; GAN systems.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИЗОЛИРОВАННОГО СЕГМЕНТА СЕТИ

Е. А. Батин, А. В. Поляничева

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

Когда дело касается изолированной сети, многие считают, что изолированность сегмента сети гарантирует реальную неуязвимость, что далеко не так. Важно знать все недостатки и возможные угрозы безопасности, которых появляется всё больше. В данном исследовании я проанализирую угрозы безопасности для изолированного сегмента сети и предложу методы борьбы с ними.

изолированная сеть, информационная безопасность, обнаружение угроз

Изолированная сеть – это сетевая инфраструктура, которая функционирует независимо от других сетей и не соединена с внешними сетями или интернетом. Это может быть выполнено физически, путем использования отдельных сетевых аппаратных устройств, или логически, через использование виртуализации или программного обеспечения для создания виртуальной изолированной сети. Изолированные сети используются, когда требуется высокий уровень безопасности или когда необходимо разделение чувствительной информации от других сетей и пользователей, например в организациях, где необходимо обеспечить защищенную и отдельную среду для хранения и обработки конфиденциальных данных.

Изолированная сеть создает физическую и логическую границу между внутренней сетью предприятия и внешними сетями. Это означает, что доступ к ресурсам внутренней сети ограничен и контролируется, часто с использованием специальных сетевых устройств, таких как файерволы или внешние шлюзы.

Изолированная сеть позволяет предприятию настроить права доступа для каждого сотрудника или группы. Это означает, что доступ к ресурсам может быть более строго контролируемым и ограниченным, что помогает предотвратить несанкционированный доступ или утечки данных. Обычная сеть может иметь менее гибкое управление доступом.

Данная сеть позволяет предприятию иметь более высокую пропускную способность, так как ресурсы могут быть выделены и оптимизированы для конкретных нужд организации. Это обеспечивает более быстрый и надежный доступ к ресурсам, чем в обычной сети, которая может быть подвержена перегрузке и замедлению из-за общего использования ресурсов. Кроме того, она облегчает управление и мониторинг сетевых ресурсов, так как предприятие имеет полный контроль над своей инфраструктурой, что позволяет более эффективно выявлять и реагировать на потенциальные сбои,

а также проводить анализ использования ресурсов и оптимизацию работы сети.

Само понятие изолированной сети наводит многих на мысль о её надежности и защищённости, что её вовсе не обязательно защищать ведь если она изолирована, значит и угрозам в ней появиться тоже не откуда. Глупо считать, что в современном мире не найдётся обходных путей и новых угроз безопасности, потому что они развиваются так же быстро, как и технологии. Изолированная сеть тоже нуждается в защите, так как уже на данный момент существует немало угроз её безопасности.

На данный момент существует несколько потенциальных угроз безопасности для изолированного сегмента сети:

1) Внутренние угрозы.

Они могут быть особенно опасными, поскольку выходят из под контроля и существуют внутри защищенной сети. К таким угрозам относятся:

1.1) Слабые пароли
1.2) Вредоносное программное обеспечение
1.3) Неправильная конфигурация
1.4) Несанкционированный доступ
1.5) Утечка данных
1.6) Неправильный управление привилегиями

2) Ошибки в конфигурации.

Неправильная конфигурация сети может привести к небезопасным областям в изолированном сегменте, которые могут быть использованы злоумышленником для проникновения в сеть. Одни из них:

2.1) Открытые порты и службы
2.2) Несанкционированные устройства
2.3) Несертифицированное программное обеспечение
2.4) Слабая шифрование или отсутствие шифрования
2.5) Неправильные настройки аутентификации

3) Физические угрозы.

Данные угрозы в изолированном сегменте сети относятся к опасностям, связанным с физическим доступом к сетевому оборудованию или физическому воздействию на него. Актуальные примеры:

3.1) Физическое повреждение оборудования
3.2) Кража оборудования
3.3) Физическое перехватывание данных
3.4) Электромагнитные помехи

4) Угрозы внутри сети.

Они относятся к потенциальным рискам и опасностям, которые могут возникнуть внутри сети или на устройствах, находящихся в пределах изолированного сегмента. К ним относятся:

4.1) Вредоносные программы
4.2) Внутренние атаки
4.3) Перехват сетевого трафика
4.4) Нехватка аутентификации и управления

Для достижения максимально возможной безопасности следует соблюдать следующие меры:

– Использование сильных и уникальных паролей для своих учетных записей, регулярное обновление программного обеспечения и операционной системы

– Должно быть установлено антивирусное программное обеспечение. Так же необходимо следить за его актуальными версиями и обновлять до новейшей.

– Если происходит подключение к изолированной сети через проводное или беспроводное соединение, следует быть осторожным с открытыми и незащищенными сетями. В данном случае следует использовать виртуальные частные сети для шифрования своих данных.

– Нужно быть осторожным при подключении внешних устройств, таких как флэш-накопители или внешние жесткие диски, их следует проверять их на наличие вредоносного программного обеспечения перед использованием их в изолированной сети.

Изолированная сеть, по своей природе, обладает более высоким уровнем безопасности по сравнению с сетью, подключенной к интернету, так как она имеет ограниченные точки входа и ограниченную связь с другими сегментами или сетями. Однако, нельзя гарантировать полноценную безопасность изолированной сети, поскольку существуют потенциальные угрозы и уязвимости, даже если она не имеет прямого подключения к интернету. Угрозы безопасности постоянно продолжают появляться и совершенствоваться, поэтому нужно знать как обезопасить себя от них.

Список используемых источников:

1. Якунин В. А., Винников В. М., Торосян А. Г. ИЗОЛИРОВАННАЯ КОМПЬЮТЕРНАЯ СЕТЬ. 2015.
2. Легкий Н. М., Шарипов С. А. ЗАЩИТА ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ ОТ ЭЛЕКТРОМАГНИТНЫХ ПОМЕХ // СОВРЕМЕННАЯ РОССИЙСКАЯ НАУКА: АКТУАЛЬНЫЕ ВОПРОСЫ, ДОСТИЖЕНИЯ И ИННОВАЦИИ. 2023. С. 25-28.
3. Олифер В. и др. Компьютерные сети. 2010.
4. Татарский Д. А., Лимонникова Е. В. Локальная компьютерная сеть предприятия // Научно-технические ведомости Севмашвтуза. 2021. N. 2. С. 46-48.
5. Шевченко С. В., Климова Е. Ю. Особенности архитектуры эволюционной модели развития корпоративных компьютерных сетей. 2006.

Batin E. Polyanicheva A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Analysis of security threats to an isolated network segment.

When it comes to an isolated network, many believe that the isolation of a network segment guarantees real invulnerability, which is far from the case. It is important to know all the shortcomings and possible security threats that are appearing more and more. In this study, I will analyze security threats for an isolated network segment and propose methods to combat them.

Key words: isolated network, information security, threat detection

УДК 004.382.4
ГРНТИ 20.53.21

РАЗРАБОТКА СИСТЕМЫ ОПРЕДЕЛЕНИЯ ОПТИМАЛЬНЫХ СРЕДСТВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОСНОВЕ АНАЛИЗА ИХ ЗАЩИЩЕННОСТИ

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

Статья посвящена актуальной проблеме обеспечения безопасности и конфиденциальности персональных данных в эпоху быстро развивающихся цифровых технологий. Автор предоставляет обзор текущих вызовов и рисков, стоящих перед организациями и государствами в области защиты данных, а также демонстрирует дорожную карту будущих исследований в данной области.

защита данных, персональные данные, кибербезопасность, анализ защищенности данных, информационная безопасность, конфиденциальность, угрозы кибербезопасности

Современный цифровой мир претерпевает революцию в обработке и хранении информации, приводя к впечатляющему росту объемов персональных данных. Эти данные, содержащие важную информацию о личности, финансовом положении, медицинских записях и других аспектах частной жизни, стали неотъемлемой частью нашей повседневности. Тем не менее, с увеличением объемов данных возрастают и риски, связанные с их безопасностью и конфиденциальностью [4, с. 21].

Защита персональных данных стала одним из наиболее важных аспектов в сфере информационной безопасности и правопорядка. Важность этой темы подчеркнута строгими законодательными требованиями, которые налагают обязанность на организации защищать данные своих клиентов и соблюдать нормы конфиденциальности. Основной нормативно-правовой акт, гарантирующий защиту персональных данных – это закон № 152-ФЗ «О персональных данных», целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну [1, с. 773].

Задача обеспечения безопасности данных далеко не всегда проста. Развивающиеся технологии и постоянно совершенствующиеся методы атак делают задачу еще более сложной. Организации должны быть в состоянии адаптироваться к новым угрозам и эффективно защищать данные своих клиентов.

Именно в этом контексте возникает актуальность темы диссертации «Разработка системы определения оптимальных средств защиты персональных данных на основе анализа их защищенности». Целью данной работы является исследование и разработка системы, которая поможет

организациям определить оптимальные методы и средства для обеспечения безопасности и конфиденциальности данных, исходя из их особенностей и потенциальных угроз.

Область защиты персональных данных сталкивается с рядом актуальных проблем и вызовов, включая:

- рост объемов данных. Быстрый рост цифровых технологий и интернета вещей привел к взрывному увеличению объемов персональных данных, что увеличивает сложность их безопасности и управления;

- угрозы кибербезопасности. Киберпреступники постоянно разрабатывают новые методы атак на информационные системы для кражи и злоупотребления данными. Это включает в себя атаки на базы данных, фишинг, вирусные программы и др.;

- управление доступом. Обеспечение правильного уровня доступа к персональным данным и их мониторинг является сложной задачей, особенно в крупных организациях. Утечки данных могут произойти из-за несанкционированного доступа к информации;

- технические сложности. С появлением новых технологий, таких как облачные вычисления, интернет вещей и искусственный интеллект, появляются новые технические вызовы в области защиты данных. Совмещение этих технологий с соблюдением стандартов безопасности становится трудной задачей;

- частные данные на рабочих устройствах. Многие работники используют личные устройства для работы, и это создает дополнительные угрозы для безопасности данных, так как граница между личными и корпоративными данными размывается;

- множество устройств и платформ. Все больше устройств и платформ используется для доступа к данным, что усложняет задачу обеспечения безопасности на всех уровнях;

- сохранение долгосрочных архивов. Многие организации сталкиваются с вопросами хранения и обеспечения безопасности персональных данных в течение долгого времени, что может потребовать решения технических и юридических задач [5, с. 357].

Эти проблемы и вызовы обусловливают необходимость развития новых и более эффективных методов и средств защиты персональных данных, а также строгого соблюдения нормативных требований. С учетом динамичного характера цифровой среды, область защиты данных будет оставаться актуальной и предоставлять множество возможностей для исследований и инноваций [3, с. 89].

Дорожная карта предстоящих исследований по теме магистерской диссертации включает в себя следующие этапы и задачи:

1. Обзор существующих методов защиты данных:

- проведение обширного обзора существующих методов и средств защиты персональных данных, включая шифрование, аутентификацию, управление доступом и др.;

- оценка из преимуществ и недостатков с точки зрения эффективности и применимости.

2. Изучение законодательных норм и стандартов:

- изучение актуального законодательства и стандартов, регулирующих область защиты персональных данных: Федеральный закон № 152-ФЗ «О персональных данных», Федеральный закон № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», Постановление Правительства РФ № 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказ ФСТЭК № 21 от 18.02.2013 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Постановление Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

- анализ требований и их сравнение с существующими методами защиты.

3. Сбор и анализ данных:

- сбор данных о характеристиках персональных данных и уровне возможных угроз;

- анализ и оценка уязвимости и рисков, связанных с этими данными;

5. Разработка системы анализа защищенности:

- разработка системы, способной оценивать текущий уровень защищенности данных на основе собранных данных и с учетом требований законодательства и стандартов;

- внедрение методики анализа, включая оценку стойкости к атакам, оценку процессов аутентификации и авторизации, анализ уровня шифрования и другие.

6. Выбор оптимальных средств и методов защиты:

- разработка алгоритмов и моделей, позволяющих определить оптимальные средства и методы защиты для конкретных типов персональных данных и уровня угроз;

- проведение анализа затрат и эффективности выбранных средств;

7. Практическое тестирование и внедрение:

- проведение практического тестирования разработанной системы в организации, использующей персональные данные;

- оценка эффективности и применимости системы в реальных условиях.

8. Оценка и доработка системы:

- анализ результатов практического тестирования и собранных отзывов;

- внесение необходимых корректировок и доработок в систему с целью повышения ее эффективности;

- документирование и публикация результатов:

Разработанная дорожная карта позволяет систематически исследовать и развивать методы и средства защиты персональных данных, что имеет большое значение в контексте растущей важности безопасности данных в современном информационном обществе.

В заключение стоит отметить, что в свете быстро растущей цифровой трансформации и повышенной концентрации внимания на защите персональных данных, тема нашего диссертационного исследования пприобретает особую актуальность и значимость. Анализ актуальных вызовов в области защиты данных позволяет нам понять, что эта проблема далеко со временем будет лишь усиливаться. Рост объемов данных, постоянное развитие технологий, а также угрозы со стороны злоумышленников делают эту тему постоянно актуальной и требующей должного внимания.

Разработка системы определения оптимальных средств защиты персональных данных на основе анализа их защищенности не только актуальна, но и обязательна для обеспечения безопасности данных в цифровой эпохе. Представленная дорожная карта будущих исследований по разработке системы определения оптимальных средств защиты персональных данных подчеркивает необходимость дальнейших усилий в этой области.

Список используемых источников:

1. Бродская Э. Г. Понятие и сущность защиты персональных данных // Экономика и социум. 2019. N 4 (59). С. 773-778.
2. Давыдова О. Б. Защита персональных данных // Вестник науки и образования. 2018. N 6 (42). С. 89-90.
3. Димова К. В., Ешенко Р. А. Разработка приложения для защиты персональных данных с учетом выбора оптимальных методов шифрования // Вестник Хабаровского государственного университета экономики и права. 2019. N 2 (100). С. 92-95.
4. Комлев Д. В. Обеспечение защиты персональных данных как элемент информационной безопасности: актуальность проблемы и способы ее решения // Междисциплинарные исследования: опыт прошлого, возможности настоящего, стратегии будущего. 2021. N 3. С. 19-27.
5. Чечуга А. О. Соблюдение уровня защищенности персональных данных // Известия ТулГУ. Технические науки. 2017. N 12-2. С. 356-360.

Bench M.

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Development of a system for determining the optimal means of personal data protection based on the analysis of their security.

The article is devoted to the topical issue of ensuring the security and privacy of personal data in the era of rapidly developing digital technologies. The author provides an overview of the current challenges and risks facing organisations and states in the field of data protection, and demonstrates a roadmap for future research in this area.

Key words: Data protection, personal data, cybersecurity, data security analysis, information security, privacy, cybersecurity threats.

УДК 004.056
ГРНТИ 81.93.29

СИСТЕМА PKI НА ОСНОВЕ БЛОКЧЕЙНА С ИСПОЛЬЗОВАНИЕМ СМАРТ-КОНТРАКТОВ

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

На сегодняшний день инфраструктура открытых ключей предоставляет надежное решение для интернет-коммуникаций. Она обеспечивает безопасный механизм аутентификации пользователей. Традиционные системы инфраструктуры открытых ключей являются централизованными, поэтому подвергаются различным угрозам безопасности и сталкиваются с некоторыми сложностями в аутентификации и авторизации. В данной работе предлагается новый подход, который включает в себя использование смарт-контрактов и децентрализованной архитектуры на базе блокчейна. Этот метод обеспечивает эффективную защиту от различных кибератак, включая распределенные атаки отказа в обслуживании и атаки человека посередине.

PKI, инфраструктура открытых ключей, смарт контракт, блокчейн, DPoS

1. Введение

В данной работе рассматривается проблема безопасности интернет-коммуникаций, связанная с традиционной инфраструктурой открытых ключей. PKI является основой для обеспечения шифрования и аутентификации серверов в интернете. Однако традиционная система PKI, основанная на централизованных удостоверяющих центрах (CA), сталкивается с серьезными угрозами безопасности. Если такие CA становятся вредоносными, то это может привести к компрометации всей системы коммуникации, создавая риск единой точки отказа. Кроме того, традиционная инфраструктура открытых ключей не обладает средствами выявления компрометированных CA, что усугубляет проблему [1]. Эти аспекты подчеркивают актуальность исследований в области кибербезопасности и необходимость разработки новых подходов к обеспечению безопасности интернет-соединений.

2. Традиционные и блокчейн PKI

Доверие к традиционным системам инфраструктуры открытых ключей полностью зависит от удостоверяющих центров третьих лиц. CA проверяет связи между открытыми ключами и субъектами, а затем предоставляет цифровые сертификаты этим субъектам. Цифровой сертификат подтверждает процесс привязки. Современные производители браузеров и операционных систем доверяют очень ограниченному числу CA. Поэтому данная архитектура PKI, основанная на CA, считается централизованной. Существующие архитектуры предпринимают множество попыток уменьшить зависимость от доверия к удостоверяющему центру.

Инфраструктуры открытых ключей на основе блокчейна представляют собой альтернативу традиционным системам PKI. Данные инфраструктуры

предоставляют среду для децентрализованной аутентификации и проверки транзакций в сети [2]. Использование различных CA для различных транзакций в децентрализованных PKI на основе блокчейна устраняет многие проблемы, вызванные устаревшими PKI. Кроме того, использование разных CA для разных транзакций повышает устойчивость сети к сбоям, и один вредоносный CA не может подорвать всю цепочку.

Примерами систем PKI на основе блокчейн являются Namecoin и Emercoin [3]. Namecoin и Emercoin требуют огромного объема памяти для хранения всей информации о блокчейне для проверки, а также необходимо хранить копию всего блокчейна на конечном устройстве пользователя. Эти проблемы хранения делают данные системы PKI на основе блокчейна непрактичными для реальных приложений. Инфраструктуры открытых ключей на основе смарт-контрактов разъединяют хранение от процесса проверки, и узлу не нужно хранить копию всего блокчейна для проверки транзакции [4]. Однако существующие PKI на основе блокчейна имеют ряд недостатков:

- Не все участники имеют равные возможности стать удостоверяющим центром.
- Сложность алгоритма консенсуса.
- Большинство существующих PKI на основе блокчейна сосредотачиваются на атаках отказа в обслуживании (DoS) и атаках «человек посередине» (MITM). Они не учитывают атаки распределенного отказа в обслуживании (DDoS), атаки 51%, атаки маршрутизации и атаки затмения.

3. Предлагаемая система

Предлагаемая система PKI состоит из следующих основных модулей: участник, смарт-контракт, подпись и аннулирование. Модуль участника содержит метод добавления атрибутов участвующего узла при его вступлении в сеть. Модуль подписи позволяет узлам подписывать и проверять ключевые пары. Модуль аннулирования позволяет узлу аннулировать свою собственную подпись, чтобы соответствующий узел мог подписать другую транзакцию.

1. Новый участник: входными данными для этого модуля является статус узла. Если узел обнаружен как новый узел в сети, то 3 атрибута: PID, ETH-адрес и ключевая пара устанавливаются для статуса нового узла для участия в транзакциях сети. Если узел уже существует в сети, модуль участника вызывает вышеупомянутые атрибуты для участия в транзакции. Атрибуты модуля участника описаны ниже:

- PID: уникальный случайный номер, который можно использовать для идентификации конкретного узла в сети.
- ETH-адрес: адрес, предоставленный средой блокчейн Ethereum, который требуется во время транзакций.
- Ключевая пара: закрытые и открытые ключи будут сгенерированы и присвоены конкретному узлу.

В данном исследовании рассматривается более легкий смарт-контракт, после развертывания сохраняется только PID соответствующего узла.

2. Смарт-контракт: входными данными для этого модуля являются PID, RID и ETH-адрес. PID и ETH-адрес выбранного узла-участника сравниваются с сохраненными PID и ETH-адресом. Если оба адреса совпадают, то RID узла-участника сравнивается с определенным порогом для этого узла. Транзакция разрешается только после успешного выполнения вышеописанных условий.

3. Проверка подписи: этот модуль позволяет узлам подписывать транзакции других узлов. Когда узел выбирается в качестве узла-подписчика, этот метод будет вызван с двумя атрибутами: PID и срок действия:

•PID: это уникальный номер, присвоенный методом участник, который обеспечивает уникальную идентификацию.

•Срок действия: после процесса проверки узел должен увеличить предопределенный счетчик на единицу, чтобы обеспечить равные возможности всем участвующим узлам в сети стать лидером транзакции. Это максимальное число, по которому один узел может быть выбран в качестве лидера транзакции.

4. Аннулирование: этот метод вызывается лидером узла после каждой транзакции. Он содержит счетчик, узел увеличивает счетчик на единицу после успешной транзакции. Если счетчик превышает максимальный предел, определенный в легкой версии смарт-контракта, процесс выборов отменяется и процесс начинается заново. RID (идентификатор аннулирования) и Signer ID (идентификатор подписчика) - два атрибута в этом модуле.

•RID: это счетчик, который увеличивает лидер узла после успешного завершения транзакции.

•Signer ID: это идентификатор узла, который собирается проверить транзакцию.

Для процесса аннулирования сертификата и обновления ключевой пары участвующий узел должен транслировать свой открытый ключ в сети в форме транзакции. Все узлы в сети хранят данные для поддержания децентрализованного доверия, поэтому содержание добытого блока может быть изменено только тогда, когда максимальное количество участвующих узлов согласны с измененным значением.

4. Структура блока

Концепция блока в контексте блокчейн технологии представляет собой важный аспект. Каждый блок, который добавляется в блокчейн, имеет определенную структуру для эффективного хранения информации и обеспечения безопасности транзакций. В данном случае, блок состоит из двух основных компонентов: заголовка блока и списка транзакций.

На рис. 1 представлена схематическая структура блока, где символ *n* обозначает количество транзакций, включенных в блок.

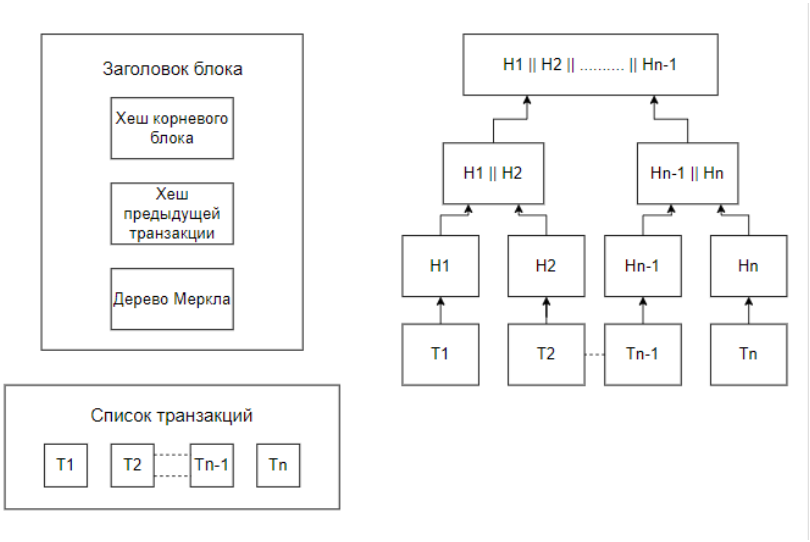


Рис. 1. Структура блока

5. Алгоритм консенсуса

В данной системе предлагается использовать алгоритм консенсуса Delegated Proof of Stake (DPoS), который является вариантом механизма PoS. DPoS повышает масштабируемость и эффективность, снижая и ограничивая количество валидаторов в сети. Он был разработан для решения проблемы «трилеммы масштабируемости» [5]. В терминологии блокчейна, увеличение количества транзакций за единицу времени означает большую масштабируемость. Однако, согласно блокчейн трилемме, большая масштабируемость может создать сложности для безопасности и децентрализации. В DPoS владельцы токенов не работают напрямую с валидностью блоков; вместо этого они выбирают делегатов для проверки транзакций от их имени. Обычно в системе DPoS выбирают от 21 до 100 делегатов. Выбранные делегаты регулярно меняются, и узлы упорядочивают их для представления своих блоков. Когда делегатов меньше, легче выделить одного валидатора и временной интервал для каждой транзакции. Если делегаты постоянно не подтверждают транзакции или блоки, это может привести к ошибочным транзакциям. В результате владельцы токенов голосуют за их отзыв и замену другим делегатом, выбранным владельцами токенов.

6. Заключение.

Представленный в данной статье подход, основанный на использовании смарт-контрактов и децентрализованной архитектуре блокчейна, открывает новые горизонты в области кибербезопасности. Этот метод не только обеспечивает высокую степень защиты от разнообразных кибератак, включая распределенные атаки отказа в обслуживании и атаки человека посередине, но и предоставляет более гибкую и эффективную систему управления ключами.

Дальнейшие исследования в этой области могут сосредоточиться на углублении в применение новых алгоритмов консенсуса, а также разработке инновационных методов защиты от более сложных кибератак.

Список используемых источников:

1. Сингх С., Хосен А.С., Юн Б. Блокчейн: атаки, вызовы и решения в области безопасности. IEEE Access 2021; 9: 13938–13959.
2. Омар И. А., Хасан Х. Р., Джайараман Р., Салах К., Омар М. Внедрение децентрализованных аукционов с использованием смарт-контрактов блокчейна. Technological Forecasting and Social Change 2021; 168: 120786.
3. Караарслан Э., Адигюзель Э. Решения DNS и PKI на основе блокчейна. Журнал стандартов связи IEEE 2018; 2(3): 52–57.
4. Кфури Э. Ф., Хури Д., АльСабех А., Гомез Х., Кричиньо Ж., Бу-Харб Э. Метод на основе блокчейна для децентрализации протокола ACME для повышения доверия в PKI. IEEE.; 2020: 461–465.
5. Кинь К., Жерве А. Обзор масштабируемости, совместимости и устойчивости блокчейна. Hochschule Luzern Imperial College London Liquidity Network 2018.

Bogomaz M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Blockchain-based PKI system using smart contracts.

Today, public key infrastructure provides a secure solution for Internet communications. It provides a secure mechanism for user authentication. Traditional public key infrastructure systems are centralized, so they are subjected to various security threats and face some difficulties in authentication and authorization. This paper proposes a new approach which involves the use of smart contracts and decentralized blockchain based architecture. This method provides an effective defense against various cyber-attacks including distributed denial of service attacks and man in the middle attacks.

Key words: PKI, public key infrastructure, smart contract, blockchain, DPoS.

УДК 004.715
ГРНТИ 81.93.29

БЕСПРОВОДНЫЕ ПРОКСИ СТАНЦИИ КАК УГРОЗА КОРПОРАТИВНОЙ WLAN

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

В данной статье проанализирована работа беспроводных локальных корпоративных сетей при подключенных к ним мобильных точках доступа. Описаны основные принципы построения и работы корпоративных WLAN-сетей. Определены основные принципы работы мобильных точек доступа. Введено понятие "беспроводная прокси-станция" для мобильных точек доступа. Определена угроза безопасности корпоративных сетей при работе в них беспроводных прокси-станций. Определены меры профилактики данной угрозы. Проанализирована проблема выявления угрозы и важность дальнейших исследований в данной области.

беспроводные локальные сети, Wi-Fi, информационная безопасность, мобильные точки доступа, прокси-станции

Введение

В настоящее время повсеместно встречается использование беспроводных локальных сетей, в частности, в современных крупных организациях, которые предпочитают технологии WLAN (Wireless Local Area Network) для удобного объединения большого количества рабочих устройств. [1] Таким образом в офисах налажена быстрая коммуникация отделов и совместная работа персонала. Корпоративная сеть может быть замкнута на территории офиса, или же иметь доступ к сети интернет. Главным преимуществом беспроводной сети является мобильность сотрудников компании, так как доступ к информации возможен из любой точки помещения, если мощность сигнала в данной точке достаточна для подключения. Несмотря на все преимущества, WLAN также обладает существенным недостатком – слабой защищенностью при недостаточной работе над администрированием сети. Тем не менее, все большее количество компаний внедряют в своих офисах подобный способ организации сети. [2]

Организация защищенных беспроводных локальных сетей

Локальная сеть внутри офиса организации предоставляет ряд возможностей, которые могут повысить эффективность работы сотрудников и обеспечить более эффективное использование информационных ресурсов. К таким возможностям относится распределение ресурсов, распределение данных и распределение программных средств. Под распределением ресурсов подразумевается общий доступ к оборудованию внутри сети, к примеру, принтерам. Распределение данных позволяет сотрудникам оперативно передавать информацию между устройствами и иметь доступ к общему хранилищу данных. А распределение программных средств

предоставляет возможность использовать программное обеспечение, которое установлено на других устройствах сети. [3]

Локальные сети позволяют сотрудникам работать с общими данными и информацией, что облегчает процесс коммуникации и совместной работы. Быстрый обмен сообщениями и доступ к общим ресурсам позволяют повысить эффективность работы и сократить затраты времени на выполнение рабочих задач. Централизованное управление сетью позволяет упростить процесс обслуживания и поддержки, а гибкая настройка и наличие средств контроля доступа повышают безопасность данных. [4]

В целом, локальная сеть внутри офиса может оказать значительное влияние на повышение производительности и эффективности работы сотрудников, уменьшение затрат времени и улучшение качества обслуживания клиентов и партнеров.

Беспроводная локальная сеть

Создание беспроводной локальной сети – это решение, которое поможет обойти недостатки проводных локальных сетей. Установка беспроводной сети в офисе организации будет проще и выгоднее по сравнению с проводной локальной сетью. Ограничения сооружения не повлияют на создание сети, а обслуживания будет требовать исключительно сетевое оборудование. Беспроводную сеть можно многократно масштабировать, что упростит создание рабочих мест для новых сотрудников. Также достоинством беспроводной сети станет мобильность сотрудников организации, так как доступ к информации у них будет из любой точки помещения, где имеется сигнал, мощности которого достаточно для подключения к сети. [5]

Для организации беспроводной локальной сети требуется наличие одной или нескольких точек доступа и адаптеров беспроводной связи для рабочих устройств, которые изначально не имеют поддержки подключения к беспроводным сетям. Точкой доступа будет являться беспроводной маршрутизатор, который подключается к серверу, который в свою очередь организует корректную работу всех устройств внутри сети, хранит и обрабатывает информацию. Для организации покрытия большей площади в случае, когда не хватает мощности одного маршрутизатора, используются точки – ретрансляторы. Они принимают сигнал с подключенных устройств и отправляют его на главную точку доступа. Еще одним типом подключения точек доступа является мост. Реализация моста заключается в физическом соединении нескольких точек доступа, когда рабочая площадь помещения распределена неравномерно, или использование ретрансляторов не имеет смысла. На дополнительных точках нужно присвоить IP-адреса в той же подсети, что находится шлюз. Далее на каждой из точек следует установить одинаковые имена беспроводной сети, одинаковые типы шифрования и ключи от сети. В результате беспроводной сетью будет покрыто все помещение. Клиенты будут менять подключение между точками по мере

перемещения по территории. Переключение будет происходить в автоматическом режиме к точке, где уровень сигнала будет выше. [6]

В целом, типовая модель корпоративной беспроводной локальной сети офиса может отличаться в зависимости от требований организации и конкретных особенностей ее инфраструктуры, но указанные компоненты являются основными и наиболее часто встречающимися в подобных сетях.

Мобильная точка доступа

Функция мобильной точки доступа (Mobile Hotspot) позволяет устройству, такому как смартфон, превращаться в Wi-Fi точку доступа для других устройств. При включенной функции мобильной ТД на устройстве, оно создает собственную беспроводную сеть Wi-Fi. Другие устройства, такие как ноутбуки, планшеты и смартфоны, могут подключаться к этой сети, при этом получая доступ к интернету через мобильную сеть устройства-точки доступа, либо же к ресурсам Wi-Fi сети, к которой параллельно подключено само устройство-точка доступа. [7]

Рис. 1. Схема работы мобильной точки доступа

Многие устройства также позволяют настроить различные параметры развернутой сети, такие как имя, тип шифрования и пароль, чтобы обеспечить её безопасность. Нужно отметить, что часто пользователи пренебрегают надежной защитой точки доступа, назначая слабый пароль, либо вовсе оставляя сеть открытой. Функция мобильной точки доступа является удобным и практичным решением для тех, кто нуждается в доступе к сети на других устройствах, не имеющих доступа к ней по умолчанию.

Трафик, создаваемый и передаваемый подключенными к мобильной точке доступа устройствами, передается через сеть устройства-точки доступа, как если бы они были подключены к целевой сети напрямую. Трафик, который генерируется каждым устройством, проходит через NAT-шлюз (Network Address Translation) устройства-точки доступа, который обеспечивает преобразование IP-адресов для пересылки трафика между устройствами в локальной сети и интернетом. [8] IP-адрес в трафике, передаваемом через мобильную точку доступа, может варьироваться в

зависимости от настроек точки доступа. По умолчанию, все подключенные устройства будут использовать один и тот же IP-адрес, полученный от устройства-точки доступа. Подключенные устройства также будут использовать MAC-адрес виртуального интерфейса устройства-точки доступа.

По вышеперечисленным особенностям работы мобильной точки доступа, можно провести аналогию с прокси-сервером, который так же выступает в роли посредника, пересылающего трафик между подключенным устройством и целевой сетью, скрывая реальный IP-адрес клиента. Для дальнейшей работы введён термин “прокси-станция”, обозначающий устройство в сети, развернувшее мобильную точку доступа Wi-Fi. [9]

Уязвимость беспроводной сети при развернутой в ней прокси-станции

В корпоративных беспроводных локальных сетях часто используются всевозможные современные методы защиты информации. Несмотря на это, злоумышленники постоянно находят обходные пути для получения доступа. Один из таких примеров заключается в особенностях устройств, работающих в режиме беспроводной прокси-станции (мобильной точки доступа). Предположим, сотрудник компании, подключенный к корпоративной WLAN, включил на своем устройстве режим точки доступа для личного пользования. Тогда сторонние устройства, которые подключаются к этой точке доступа, получают доступ к корпоративной WLAN. Выявление подобных инцидентов усложняется тем, что трафик сторонних устройств будет присутствовать в сети организации с MAC-адресом и IP-адресом легитимного устройства, работающего в режиме прокси-станции. Эта проблема может привести к серьезным последствиям для компании, таким как утечка конфиденциальных данных и вредоносные атаки на сеть. Кроме того, подключение нелегитимных устройств может снизить производительность сети и повлиять на качество работы, что приведет к финансовым и репутационным потерям, так как вызовет снижение доверия клиентов к организации. [10]

Рис. 2. Схема исследуемой модели

Меры профилактики угроз при использовании прокси-станций

Стоит отметить, что в первую очередь в подобных ситуациях виноват будет сотрудник, развернувший на своем устройстве ненадежную точку доступа Wi-Fi, тем самым сделав корпоративную сеть незащищенной. [11] В таком случае, первоначальной целью злоумышленника станет подключение к этой точке доступа.

Во избежание таких ситуаций изначально следует провести инструктаж по сетевой безопасности для всех сотрудников, имеющих доступ к сети. В инструктаж необходимо включить блоки, разъясняющие опасность создания точек доступа, памятки по созданию надежного пароля, а также советы по целесообразному использованию корпоративной сети. Большинство инцидентов, связанных с проникновением в сеть через точку доступа Wi-Fi, происходят по причине очень простого, либо вовсе отсутствующего пароля на развернутой сотрудником точке доступа, в то время как сам сотрудник может даже не подозревать, что таким образом он подвергает опасности всю корпоративную сеть. Даже если пароль назначен, злоумышленник может применить метод подбора пароля «грубой силой».

Следующим шагом необходимо ввести новые правила пользования корпоративной сетью. [12] Существует несколько вариантов вводимых изменений. Наиболее надежным и радикальным методом станет запрет на подключение к сети с личных устройств, а на корпоративной технике – отключение функции точки доступа на программном уровне. Менее радикальный метод – разрешить подключение к сети с личных устройств, но запретить создание точек доступа внутри этой сети. Такой вариант будет менее надежным, так как у сотрудников останется возможность создавать точки доступа, а контроль выполнения правил потребует дополнительных технических решений.

Все введенные правила необходимо зафиксировать во внутренних документах компании, ввести санкции за их нарушение и потребовать сотрудников ознакомиться и дать соглашение, расписаться. [13]

Проблема выявления беспроводных прокси-станций

Несмотря на все меры профилактики инцидентов, могут происходить случаи нарушения предписаний: сотрудник создает слабозащищенную точку доступа Wi-Fi внутри корпоративной сети, а злоумышленник, с легкостью подобрав к ней пароль, подключается и получает доступ к сети.

Для таких случаев требуется разработать методику обнаружения устройств внутри сети, работающих в режиме точки доступа Wi-Fi и подключенных к ним нелегитимных устройств для дальнейшего предотвращения несанкционированного доступа к целевой WLAN. Необходимо определить признаки создания мобильной точки доступа, либо подключения третьего устройства к ней, а также выявить создавшего точку доступа сотрудника. Для выполнения вышеперечисленных задач в первую очередь используется специализированное программное обеспечение для мониторинга сетевого трафика. [14] Проводится анализ сетевого трафика на предмет нестандартных запросов и ответов, анализ IP и MAC-адресов,

обнаружение нескольких подключений с одних и тех же адресов, сопоставление адресов с запросами.

Заключение

Проблема безопасности в сетях WLAN является одной из главных забот IT-специалистов в современных корпорациях. Мобильные точки доступа Wi-Fi могут быть установлены не только злоумышленниками, но и сотрудниками, которые не осознают возможные последствия своих действий. Это создает уязвимость, при которой злоумышленник может получить несанкционированный доступ к закрытой корпоративной сети, подключившись к устройству сотрудника, выступающему в качестве точки доступа Wi-Fi (прокси-станции), что может привести к нарушению конфиденциальности данных и утечке информации, а также к дополнительным расходам на обслуживание и защиту корпоративной сети.

Поэтому разработка эффективной методики обнаружения мобильных точек доступа в WLAN-сетях является необходимой мерой для защиты корпоративной сети от внешних угроз, а значит, имеет высокую актуальность и практическую значимость в настоящее время.

Для будущих исследований в данном вопросе следует вести поиск способов обнаружения прокси-станций в корпоративных WLAN-сетях. Методы должны быть применимы к корпоративным сетям и способны обеспечивать дополнительный уровень безопасности. Также возможна автоматизация данных методов, разработка специализированного программного обеспечения для облегчения и ускорения реализации.

Список используемых источников:

1. Бабков И. Н., Бударин Э. А., Кистуга А. Ю., Бударин М. Э. Разработка методики обнаружения беспроводных прокси-станций в корпоративной WLAN-сети // Экономика и качество систем связи. 2023. N 2(28).
2. Ковцур М. М., Юркин Д. В., Герлинг Е. Ю., Ахрамеева К. А. Безопасность беспроводных локальных сетей. СПб. : СПбГУТ, 2021.
3. Петрова Т. В., Ковцур М. М., Карельский П. В., Поляничева А. В. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети // Региональная информатика : материалы Юбилейной XVIII Санкт-Петербургская междунар. конф., Санкт-Петербург, 26-28 окт. 2022 г. СПб. : СПОИСУ, 2022.
4. Кистуга 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 Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 24-25 фев. 2021 г. СПб. : СПбГУТ, 2021.
5. Ковцур М. М., Кириллов Д. И., Михайлова А. В., Потемкин П. А. Исследование подходов анализа трафика беспроводных сетей с использованием библиотеки Pandas // Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей: в 4х томах. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург, 2021.
6. Юркин Д.Ю., Ворошнин Г.Е., Ковцур М.М., Мисливский Б.С. Исследование влияния атак Arpinject и Associationflood в беспроводных сетях на базе оборудования Mikrotik // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022.

7. Дрепа В.Е., Кируга А.Ю., Ковцур М.М., Кузьмина О.И., Петров В.А. Исследование метода Fingerprinting для определения местоположения беспроводного клиента IEEE 802.11 - Заметки ученого. 2022.

8. Докшин А.Д., Ковцур М.М., Прудников С.В., Таргонская А.И. Исследование подходов для аутентификации пользователей беспроводной сети с применением различных LDAP решений // Наукоемкие технологии в космических исследованиях Земли. 2021.

9. Герлинг Е.Ю., Кулишкина Е.И., Бирих Э.В., Виткова Л.А. Модели нарушителей информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности. 2017.

10. Ковцур М.М., Герлинг Е.Ю., Коновалова В.В., Кируга 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.

11. 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.

12. Герлинг Е.Ю., Зебзеев Е.А., Кируга А.Ю. Разработка метода анализа трафика беспроводной сети на базе WPA2 ENTERPRISE – В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022.

13. Дешевых Е.А., Конюхов В.М., Крылов К.Ю., Ушаков И.А. Исследование методов защиты от инсайдерских атак – В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах, 2015.

14. 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.

15. Штеренберг С.И., Красов А.В., Цветков А.Ю. Компьютерные вирусы. Ч. 1. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 2015.

16. Десницкий В.А., Сахаров Д.В., Чечулин А.А., Ушаков И.А., Захарова Т.Е. Защита информации в центрах обработки данных. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 2019.

17. Коцыняк М.А., Бударин Э.А., Карпов М.А., Муртазин И. Р., Иванов Д. А. Воздействие нарушителя на беспроводные сети передачи данных по уровням эталонной модели взаимодействия открытых систем – В сборнике: Состояние и перспективы развития современной науки по направлению "информационная безопасность. Анапа, 2020.

18. Новиков П.А., Лепешкин О.М., Шуравин А.С., Бударин Э.А. Модель сетевого мониторинга защищенности сети передачи данных – В сборнике: Неделя науки СПбПУ. Санкт-Петербург, 2020.

19. Василишин Н.С., Ушаков И.А., Котенко И.В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак – В сборнике: Информационные технологии в управлении (ИТУ-2016). Материалы 9-й конференции по проблемам управления. Председатель президиума мультиконференции В. Г. Пешехонов, 2016.

20. Steffen Schulz, Hossen A. Mustafa, Wenyuan Xu, Ahmad-Reza Sadeghi, Maria Zhdanova, Vijay Varadharajan Tetherway: A Framework for Tethering Camouflage // Conference: Wireless Network Security (WiSec) – 2012.

Budarin M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Wireless Proxy Stations as A Threat to Corporate WLAN.

This paper analyzes the operation of wireless local corporate networks with mobile access points connected to them. The basic principles of construction and operation of corporate WLAN-networks are described. The basic principles of mobile access points operation are defined. The concept of "wireless proxy station" for mobile access points is introduced. The threat to the security of corporate networks when wireless proxy stations work in them is defined. Measures of prevention of this threat are defined. The problem of threat detection and the importance of further research in this area are analyzed.

Key words: wireless local area networks, Wi-Fi, information security, mobile access points, proxy stations.

УДК 004.051
ГРНТИ 20.51.21

ПРЕДСТАВЛЕНИЕ СПОСОБОВ РЕАКТИВАНОГО ПРОГРАММИРОВАНИЯ

К. Н. Бусыгин, М. Т. Малания
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В последнее время можно чаще замечать программы, использующие графический интерфейс совместно с применением многопоточности. Такой подход заставляет задуматься о чистоте и эффективности кода. С зарождением реактивного программирования появилась возможность оптимизировать обмен данными между потоками, прибегая к определенным шаблонам проектирования.

процессоры, реактивное программирование, асинхронные потоки, объекты, графические интерфейсы

Одним из важнейших факторов, отвечающих за скорость отклика программного обеспечения, является частота процессора, на котором производится запуск программы. В прошлом увеличение частоты процессоров было одним из главных способов повышения производительности и скорости работы программ. Однако с течением времени стало все сложнее увеличивать тактовую частоту в связи с техническими ограничениями микропроцессорной базы (рис. 1) [1].

Рис. 1. Тенденция развития частоты процессора.

Альтернативным способом решения задачи была разработка многоядерного процессора, позволяющего распределить задачи на отдельные потоки. Одним из методов применения многопоточности являются комплексные многопоточные программы с графическим интерфейсом.

В предлагаемом докладе речь пойдет о проблемах разработки программного обеспечения с точки зрения реализации многопоточных объектов, которые вызывают строгую зависимость, в которой один объект будет дожидаться выполнения процесса другого объекта, что иногда приводит к длительным ожиданиям пользователя.

Также будут рассматриваться проблемы разработки с точки зрения асинхронного программирования и смысл добавления асинхронного

подмножества - реактивного шаблона проектирования [2], при котором проект обретает возможность масштабирования и упрощения управления состояниями процессов. Пример проиллюстрирован на рис. 2.

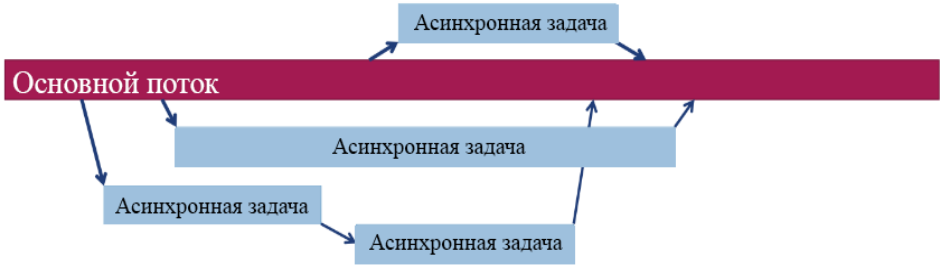


Рис. 2. Визуальный пример выполнения асинхронных задач.

Будет описан базовый метод реализации реактивного подхода на языке программирования C++ с применением шаблона проектирования “Наблюдатель”, а также показаны преимущества данного подхода по отношению к другим популярным методам разработки и вероятные минусы, с которыми может столкнуться разработчик [3]. Также будут рассмотрены подходы вталкивания и втягивания задач на реактивном примере.

В заключение можно сказать, что реактивное программирование оптимизирует работу программ, которые также становятся более элегантными и удобными для рефакторинга. Не каждой системе может потребоваться данный подход, но при этом можно с уверенностью сказать, что реактивы способны дать нашей системе возможность выдерживать нагрузки больше, чем если бы она была реализована без них.

Список используемых источников:

1. Реактивное программирование на Java: как, зачем и стоит ли? Часть 1. [Электронный ресурс]. URL: https://habr.com/en/companies/oleg-bunin/articles/543386 (дата обращения 19.10.2023).

2. Реактивное программирование на Java. Будущее, настоящее и прошлое. [Электронный ресурс]. URL: https://struchkov.dev/blog/ru/overview-of-reactive-programming (дата обращения 19.10.2023).

3. Пай П., Абрахам П. Реактивное программирование на C++ / пер. с анг. В. Ю. Винника. М. : ДМК Пресс, 2019. 324 с. С. 17 - 37. ISBN 978-5-97060-778-7.

Busygin K., Malania M.

Saint Petersburg State University of Industrial Technologies and Design

Presentation of reactive programming methods.

Recently, you can often notice programs that use a graphical interface in conjunction with the use of multithreading. This approach makes you think about the purity and efficiency of the code. With the emergence of reactive programming, it became possible to optimize data exchange between threads by resorting to certain design patterns

Key words: Processors, reactive programming, asynchronous threads, objects, graphical interface.

УДК 004.738
ГРНТИ 49.33.35

АНАЛИЗ МОДЕЛЕЙ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ

А. А. Васьков
Санкт-Петербургский государственный университет промышленных технологий и дизайна

Анализ моделей угроз информационной безопасности беспроводных сетей является важным аспектом в современной цифровой эпохе. Беспроводные сети все более распространены и становятся неотъемлемой частью нашей повседневной жизни. Однако, с ростом популярности беспроводных технологий возрастает и риск уязвимостей и атак на безопасность данных. В данной работе проводится анализ различных моделей угроз, которые могут возникнуть в беспроводных сетях. Рассматриваются такие аспекты, как подслушивание, внедрение вредоносного ПО, атаки на протоколы безопасности и другие. Кроме того, обсуждаются методы и подходы к защите от данных угроз, включая шифрование данных, аутентификацию, управление доступом и мониторинг. Целью данного анализа является обеспечение эффективной защиты информации в беспроводных сетях и предоставление рекомендаций для повышения безопасности в данной области. Результаты и выводы этого исследования могут быть полезными для специалистов в области информационной безопасности, а также для организаций и пользователей, которые используют беспроводные сети в своей деятельности.

информационная безопасность, беспроводные сети, сеть интернет

Введение:

Беспроводные сети являются неотъемлемой частью современного информационного общества, обеспечивая мобильность и гибкость в доступе к данным и ресурсам.

Обеспечение информационной безопасности в беспроводных сетях становится все более важным в свете увеличения угроз и атак на такие сети.

Основные угрозы информационной безопасности беспроводных сетей:

Подслушивание и перехват данных: злоумышленники могут использовать различные методы, такие как сниффинг и анализ трафика, для перехвата и получения конфиденциальной информации.

Внедрение вредоносного ПО: злоумышленники могут использовать беспроводные сети для распространения вредоносных программ, таких как вирусы, черви и трояны, которые могут нанести ущерб системам и данным.

Атаки на протоколы безопасности: злоумышленники могут использовать уязвимости в протоколах шифрования и аутентификации для обхода механизмов безопасности и получения несанкционированного доступа к сети.

Физические атаки: злоумышленники могут физически получить доступ к точкам доступа или сетевому оборудованию, чтобы осуществить атаки или украсть конфиденциальную информацию.

Модели угроз информационной безопасности беспроводных сетей:

Модель CIA (Confidentiality, Integrity, Availability): модель, основанная на концепциях конфиденциальности, целостности и доступности данных в беспроводных сетях, исследование и анализ каждого из этих аспектов.

Модель DAD (Denial of Access to Data): модель, фокусирующаяся на анализе угроз, связанных с отказом доступа к данным, а также оценке мер защиты от таких угроз.

Модель APT (Advanced Persistent Threats): модель, рассматривающая продвинутые угрозы, которые могут длительное время проникать и находиться в сети, исследование методов обнаружения и противодействия таким угрозам.

Модель DDoS (Distributed Denial of Service): модель, изучающая распределенные атаки отказа в обслуживании и их последствия для беспроводных сетей, а также разработку механизмов защиты.

Методы защиты и противодействия угрозам безопасности:

Шифрование данных: использование различных методов шифрования, таких как WPA2, для защиты конфиденциальности передаваемых данных в беспроводных сетях.

Аутентификация и управление доступом: применение протоколов аутентификации, таких как EAP и RADIUS, и методов контроля доступа, таких как MAC-фильтрация и аутентификация по сертификатам, для обеспечения безопасного доступа к беспроводным сетями.

Мониторинг и обнаружение инцидентов: установка систем мониторинга и обнаружения аномалий в беспроводных сетях, которые могут помочь идентифицировать потенциальные атаки или необычное поведение в сети.

Физическая безопасность: принятие мер для защиты физической инфраструктуры беспроводных сетей, таких как использование физических барьеров, видеонаблюдение и контроль доступа к точкам доступа и сетевому оборудованию.

Уязвимости беспроводных сетей:

Уязвимости протоколов: оценка уязвимостей, связанных с протоколами безопасности, таких как WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) и WPA2, и улучшение механизмов шифрования и аутентификации.

Угрозы социальной инженерии: анализ методов манипуляции и обмана пользователей для получения несанкционированного доступа к беспроводной сети, и разработка мер по повышению осведомленности пользователей и обучению по безопасности.

Физические уязвимости: изучение угроз, связанных с физическим доступом к точкам доступа и сетевому оборудованию, и разработка мер физической защиты, таких как использование замков и ограниченного доступа к оборудованию.

Модели управления рисками информационной безопасности:

Модель OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): методология, основанная на оценке операционно-критических угроз, активов и уязвимостей для разработки стратегий управления рисками.

Модель NIST (National Institute of Standards and Technology): использование стандартов и рекомендаций, разработанных Национальным институтом стандартов и технологий, для управления рисками информационной безопасности в беспроводных сетях.

Модель ISO 27001: обзор международного стандарта по управлению информационной безопасностью и его применение в контексте беспроводных сетей для разработки политик и процедур безопасности.

Анализ угроз со стороны злоумышленника:

Внутренние угрозы: исследование возможных угроз безопасности, связанных с действиями внутренних пользователей беспроводной сети, таких как несанкционированный доступ или утечка информации.

Внешние угрозы: анализ типов и методов атак со стороны внешних злоумышленников на беспроводные сети, таких как фишинг, взлом паролей, атаки перебором и DoS-атаки, и разработка мер для защиты от таких угроз.

Основные методы защиты информационной безопасности в беспроводных сетях включают шифрование данных, аутентификацию и управление доступом, мониторинг и обнаружение инцидентов, а также обеспечение физической безопасности. Шифрование данных позволяет защитить конфиденциальность передаваемых данных, аутентификация и управление доступом обеспечивают контроль доступа к сети, мониторинг и обнаружение инцидентов помогают обнаружить аномалии и потенциальные атаки, а физическая безопасность защищает сетевое оборудование и точки доступа от несанкционированного доступа.

Оценка уязвимостей беспроводных сетей позволяет идентифицировать возможные проблемы и уязвимости, связанные с протоколами безопасности, социальной инженерией и физическим доступом. Улучшение протоколов шифрования и аутентификации, повышение осведомленности пользователей и обучение по безопасности, а также применение физических мер защиты могут помочь устранить уязвимости.

Модели управления рисками информационной безопасности, такие как OCTAVE, NIST и ISO 27001, предоставляют стандарты и методологии для эффективного управления угрозами безопасности в беспроводных сетях. Они включают оценку угроз, активов и уязвимостей, разработку политик и процедур безопасности, а также стратегии управления рисками.

Анализ угроз со стороны злоумышленника позволяет понять возможные угрозы безопасности, связанные с внутренними и внешними действиями злоумышленников. Внутренние угрозы могут включать несанкционированный доступ или утечку информации со стороны внутренних пользователей, в то время как внешние угрозы могут быть связаны с фишингом, взломом паролей, атаками перебора и DoS-атаками.

В целом, обеспечение безопасности в беспроводных сетях требует комплексного подхода, включающего использование различных методов защиты, оценку уязвимостей, применение стандартов и методологий управления рисками, а также анализ угроз со стороны злоумышленника. Это поможет обеспечить надежную защиту информации и ресурсов в беспроводных сетях.

Кроме того, для обеспечения безопасности в беспроводных сетях необходимо также учитывать физические аспекты. Например, ограничение доступа к оборудованию и контроль над физическими точками доступа могут помочь предотвратить несанкционированный доступ к сети. Также важно регулярно обновлять программное обеспечение и прошивки устройств, чтобы исправить известные уязвимости.

Беспроводные сети также должны быть защищены от атак на протоколы безопасности, такие как атаки на аутентификацию и шифрование. Правильная конфигурация сети, использование сильных паролей и механизмов аутентификации, а также регулярное обновление ключей шифрования могут помочь в предотвращении таких атак.

Кроме того, важно понимать, что безопасность в беспроводных сетях - это непрерывный процесс. Угрозы постоянно развиваются, и поэтому необходимо постоянно обновлять и улучшать меры безопасности. Регулярный мониторинг сети, обнаружение и реагирование на инциденты, а также проведение аудитов и оценок уязвимостей помогут обнаружить и устранить возможные уязвимости.

Наконец, обучение пользователей также является важной составляющей безопасности в беспроводных сетях. Пользователи должны быть осведомлены о возможных угрозах и обучены правилам безопасного использования сети. Это включает в себя обучение о выборе надежных паролей, запрет на открытие подозрительных ссылок и файлов, а также использовании только доверенных сетей.

В целом, обеспечение безопасности в беспроводных сетях требует комплексного подхода, который включает в себя технические, физические и организационные меры. При соблюдении этих мер можно обеспечить надежную защиту данных и информации в беспроводных сетях.

Список используемых источников:

1. Vacca J. R. Computer and Information Security Handbook. Morgan Kaufmann. 2013.

2. Chandra M., & Gupta N. Wireless Networks: Security, Performance, and Applications. CRC Press. 2018.

3. Whitman M. E., & Mattord H. J.. Principles of Information Security. Cengage Learning. 2019.

4. Joshi J. B., & Patil A. Wireless Security: Models, Threats, and Solutions. CRC Press. 2016.

Vaskov A.

Saint Petersburg State University of Industrial Technologies and Design

Analysis of Threat Models in Wireless Network Information Security.
The analysis of threat models in wireless network information security is an important aspect in the modern digital era. Wireless networks are becoming increasingly widespread and have become an integral part of our everyday lives. However, as the popularity of wireless technologies grows, so does the risk of vulnerabilities and attacks on data security. This paper conducts an analysis of various threat models that can arise in wireless networks. Aspects such as eavesdropping, malware infiltration, attacks on security protocols, and others are considered. Additionally, methods and approaches to protect against these threats are discussed, including data encryption, authentication, access management, and monitoring. The aim of this analysis is to ensure effective information protection in wireless networks and provide recommendations for enhancing security in this field. The results and conclusions of this research can be useful for information security specialists, as well as organizations and users who utilize wireless networks in their activities.

Key words: Information security, wireless networks, internet network.

УДК 004.056.53
ГРНТИ 49.33.29

РАЗРАБОТКА ПОРТАТИВНОГО ДЕТЕКТОРА СЕТЕВЫХ АТАК

С. А. Винников, В. И. Трезоров
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире сетевых технологий при обеспечении информационной безопасности в сетях Wi-Fi важно не только противодействовать угрозам на беспроводные сети, но и фиксировать сами попытки злоумышленников атаковать. Для решения подобной задачи можно разработать простой и портативный детектор сетевых атак.

Wi-Fi, атака, детектор, scapy

На сегодняшний день технология беспроводной передачи данных Wi-Fi широко распространена практически во всем мире [1]. Это подтверждается статистикой, представленной на рис. 1. Поэтому обеспечение информационной безопасности в беспроводных сетях остается актуальным всегда.

Страна	
US	540,468,127
DE	81,542,793
GB	66,062,776
CA	60,934,443
NL	49,532,969
AU	28,449,734
JP	27,330,791
RU	23,373,956
FR	21,159,694
ES	15,170,791
PL	14,825,482
CN	13,195,649
IT	12,807,452

Рис. 11. Примерное количество Wi-Fi сетей в разных странах

При этом важно не только устранять уязвимости, вызванные ошибками в программном обеспечении, использованием устаревших методов шифрования и аутентификации или человеческим фактором, но и фиксировать попытки злоумышленников атаковать сети. Это дает

дополнительную информацию об уровне защиты сети Wi-fi, наиболее частых методах атак, а также выступает в качестве сигнала того, что хакер заинтересовался проникновением в сеть и следует насторожиться, ведь возможно атаки в скором времени продолжатся с новой силой. Для этих целей следует использовать простой детектор сетевых атак, который должен соответствовать нескольких условиям:

- Программная реализация. Программно-реализованный детектор легко клонировать и распространять на несколько компьютеров в большой сети.
- Простота и удобство использования. Возможность быстро и просто запустить сканирование, а также удобное отображение важной информации, позволит любому человеку практически без специальных навыков развернуть детектор.
- Портативность. Данное свойство поможет в быстром развертывании детектора при расширении сети или при потребности во временном сканировании участка сети с минимальной тратой ресурсов.

Для разработки программы был выбран Scapy. Это сетевой инструмент, написанный на языке Python, главной особенностью которого является возможность ручного создания кадров и пакетов. Гибкость в создании пакетов достигается с помощью широкого функционала Scapy, что позволяет задавать настройки для каждого поля пакета [2]. Поскольку Scapy воспринимает отдельные поля и значения в них, это также поможет в сканировании сети и выявлении отдельных кадров по определенным значениям в полях. Схема разрабатываемого детектора атак представлена на рис. 2. Реализован он будет на ОС Kali linux.

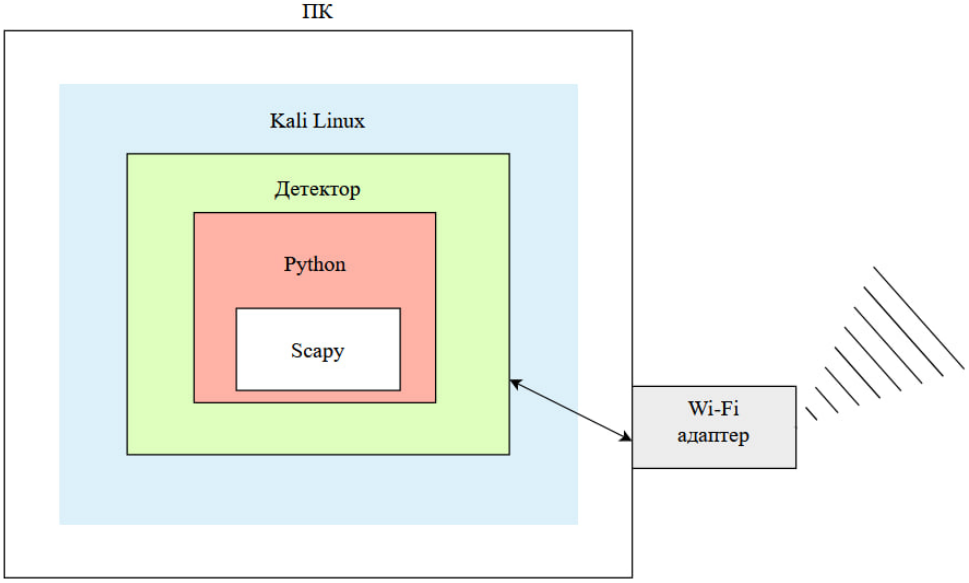


Рис. 12. Схема детектора атак

Для работы программы будут необходимы Wi-Fi адаптер, установленные язык программирования Python и Scapy. Принцип работы детектора показан на рис. 3 и реализован он с помощью нескольких функций:

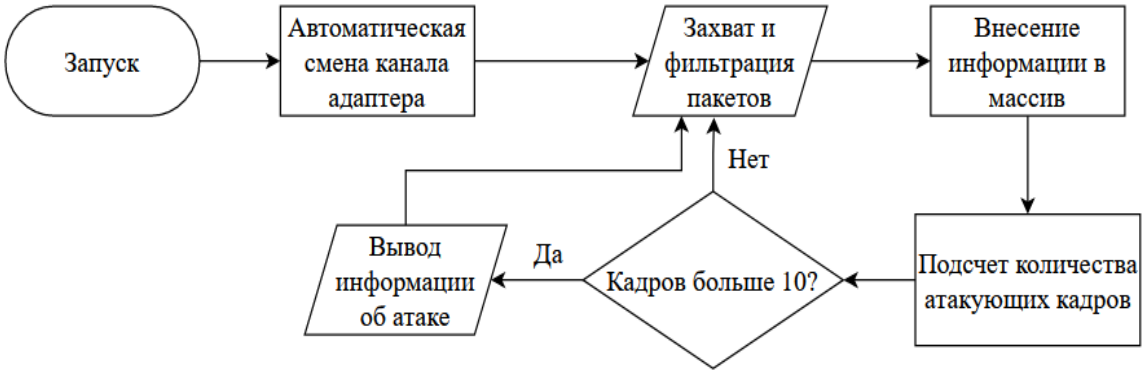


Рис. 13. Блок схема работы детектора атак

1. Функция def change_channel(iface) автоматически меняет канал сетевого адаптера, таким образом реализуется полное сканирование сети. Список каналов реализован с помощью массива, выбор через random, а сама функция представляет собой бесконечный цикл while true. Также в конце цикла прописана пауза time.sleep, иначе каналы будут меняться слишком быстро, и сканирование будет бесполезным.
2. Следующая функция def sniff_packets нужна для сканирования пакетов и фильтрации их по наличию аргумента Dot11. Таким образом в дальнейшем программа не будет работать со всеми пакетами и кадрами в сети. Затем, если подтип кадра (subtype) равняется 0x00c (кадр деаутентификации) или 0x00a (кадр диассоциации), то считываются поля target_wifi_mac и target_device_mac и вносятся в соответствующий массив, сам кадр вносится в список packet_list.
3. Функция def detect_attack проверяет длину списка packet_list, если она превышает введенное значение, то детектор выводит информацию об атаке: дата, время, предполагаемый инструмент атаки, mac адрес атакованной точки доступа и mac адрес атакуемого устройства. Пример обнаружения атаки представлен на рис. 4.
4.

```
[+] Fri, 09, Jun 2023 07:52:02  Aircrack-ng Target Wi-Fi: 54:AF:97:54:90:95 Target Device: 5E:89:4C:28:5D:EA
[+] Fri, 09, Jun 2023 07:52:03  Aircrack-ng Target Wi-Fi: 54:AF:97:54:90:95 Target Device: 5E:89:4C:28:5D:EA
[+] Fri, 09, Jun 2023 07:52:04  Aircrack-ng Target Wi-Fi: 54:AF:97:54:90:95 Target Device: 5E:89:4C:28:5D:EA
[+] Fri, 09, Jun 2023 07:52:05  Aircrack-ng Target Wi-Fi: 54:AF:97:54:90:95 Target Device: 5E:89:4C:28:5D:EA
[+] Fri, 09, Jun 2023 07:52:06  Aircrack-ng Target Wi-Fi: 54:AF:97:54:90:95 Target Device: 5E:89:4C:28:5D:EA
[+] Fri, 09, Jun 2023 07:52:07  Aircrack-ng Target Wi-Fi: 54:AF:97:54:90:95 Target Device: 5E:89:4C:28:5D:EA
[+] Fri, 09, Jun 2023 07:52:08  Aircrack-ng Target Wi-Fi: 54:AF:97:54:90:95 Target Device: 5E:89:4C:28:5D:EA
[+] Fri, 09, Jun 2023 07:52:09  Aircrack-ng Target Wi-Fi: 54:AF:97:54:90:95 Target Device: 5E:89:4C:28:5D:EA
[+] Fri, 09, Jun 2023 07:52:10  Aircrack-ng Target Wi-Fi: 54:AF:97:54:90:95 Target Device: 5E:89:4C:28:5D:EA
[+] Fri, 09, Jun 2023 07:52:11  Aircrack-ng Target Wi-Fi: 54:AF:97:54:90:95 Target Device: 5E:89:4C:28:5D:EA
```

Рис. 14. Обнаружение атаки детектором

Таким образом, был разработан простой детектор атак, который работает в фоном режиме, а также запускается одной командой «python detect_attack.py wlan0mon», что позволяет быстро и просто его развернуть.

В дальнейшем планируется улучшить детектор, добавив в него возможность обнаружения и других атак, а также собрать детектор в отдельный live-cd образ, который поместится на флешке и позволит начать сканирование на любом компьютере.

Список используемых источников:

1. Statistics: Geo-political [Электронный ресурс] // WIGLE.NET URL: https://wigle.net/stats#geostats (дата обращения: 25.10.23).

2. Welcome to Scapy’s documentation [Электронный ресурс] // Scapy URL: https://scapy.readthedocs.io/en/latest/index.html (дата обращения: 07.05.23).

3. Детектор деаутентификации (диссоциации) клиентов. Часть 2 [Электронный ресурс] // Codeby URL: https://codeby.net/threads/detektor-deautentifikacii-dissociacii-klientov-chast-2.66382/ (дата обращения: 10.05.23).

Vinnikov S., Trezorov V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development of a portable network attack detector.

In the modern world of network technologies, when ensuring information security in Wi-Fi networks, it is important not only to counteract threats to wireless networks, but also to record the very attempts of intruders to attack. To solve such a problem, a simple and portable network attack detector can be developed.

Key words: Wi-Fi, attack, detector, scapy.

УДК 004.056
ГРНТИ 49.33.29

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЦИФРОВОГО МИРА: КОМПЛЕКСНОЕ РУКОВОДСТВО ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И. Висал, С. И. Штеренберг
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В современном все более взаимосвязанном и цифровом мире нельзя недооценивать важность информационной безопасности. С развитием технология возрастают и угрозы и уязвимости, которые могут подвергнуть опасности конфиденциальные данные и цифровые активы. Это комплексное руководство глубоко исследует мир информационной безопасности, предоставляя понимание ее основ, актуальной угрозой ситуации, передовых практик и взгляд в будущее этой важной области

безопасность, информационная безопасность, угроза, цифровой мир, опасность

В эпоху, когда цифровые технологии проникают во все сферы нашей жизни, обеспечение безопасности информации не имеет альтернативы. Информационная безопасность, часто называемая InfoSec, представляет собой практику защиты данных, систем и сетей от несанкционированного доступа, раскрытия, изменения или уничтожения. Это комплексное руководство направлено на исследование глубоких аспектов информационной безопасности, предоставляя понимание её основ, развивающейся угрозной ситуации, передовых практик и взгляд в будущее этой важной области [1].

Информационная безопасность охватывает несколько ключевых принципов [2]:

– **Конфиденциальность:** гарантия, что информация доступна только для авторизованных лиц

– **Целостность:** обеспечение точности и целостности данных;

– **Доступность:** обеспечение доступности информации по требованию;

– **Аутентификация и авторизация:**проверка личности пользователей и управление их доступом;

– **Управление рисками:** оценка и управление рисками в области безопасности;

– **Политики и процедуры безопасности:** установление фреймворков для мер безопасности.

Информация представляет собой ценный актив, и её нарушение может иметь серьезные последствия, включая финансовые убытки, ущерб репутации и даже национальную безопасность.

Изучение истории информационной безопасности позволяет понять её эволюцию. В частности можно выделить следующие этапы [3]:

– Криптография в Древние времена:древние цивилизации использовали коды и шифры для обеспечения безопасной связи;

– Вторая Мировая Война и Энигма: взлом кода Энигма подчеркнул важность криптографии в разведке во время войны;

– Эра компьютерной безопасности:начальные меры безопасности компьютеров фокусировались на физическом контроле доступа;

– Эра интернета и киберугрозы: рост интернета создал новые вызовы в области безопасности.

Следует также выделить общие угрозы информационной безопасности [4]:

– Вредоносное ПО: вирусы, трояны, черви и вымогательское ПО могут нарушить работу систем и украсть данные;

– Атаки по перехвату: обманчивые тактики направлены на обман пользователей и получение от них чувствительной информации;

– Атаки DoS и DDoS: перегрузка системы или сети с целью недоступности;

– Утечки данных: несанкционированный доступ к базам данных ведёт к утечке данных;

– Внутренние угрозы: работники или партнёры могут злоупотреблять своим доступом.

Несмотря на общие угрозы в современном мире также следует определить и новые угрозы, такие как [5]:

– Атаки с использованием ИИ и машинного обучения:злоумышленники используют искусственный интеллект и машинное обучение для сложных автоматизированных атак;

– Проблемы безопасности интернета вещей:распространение устройств IoT (интернета вещей) вводит новые уязвимости;

– Блокчейн и информационная безопасность:поднимается вопрос о безопасности в контексте использования блокчейна.

Важно отметить, что ошибки человека и социальная инженерия вносят значительный вклад в нарушения, среди которых [6]:

– Социальная инженерия:злоумышленники манипулируют людьми для получения конфиденциальной информации;

– Осведомленность о фишинге:программы обучения о фишинге обучают сотрудников распознавать и реагировать на подобные атаки;

– Анализ поведения пользователей:инструменты помогают выявлять необычные паттерны активности, указывающие на нарушения безопасности.

Основы информационной безопасности [7]:

– Принципы информационной безопасности –информационная безопасность руководствуется основными принципами: конфиденциальность, целостность, доступность, аутентификация, авторизация, управление рисками и политики безопасности;

– Тройственность (CIA Triad) – подчеркивает важность конфиденциальности, целостности и доступности, обеспечивая баланс между этими принципами;

– Защита в глубину (DefenseinDepth) –защита в глубину предполагает использование нескольких мер безопасности для защиты от различных угроз и снижения рисков.

В политике и практике информационной безопасности следует выделить следующее [8]:

– Разработка политики информационной безопасности –организации должны создать фреймворк политики безопасности, провести оценку рисков и классификацию данных для разработки эффективных политик информационной безопасности;

– Управление доступом на основе ролей –управление доступом на основе ролей назначает разрешения на основе ролей пользователей, следуя принципу наименьших привилегий;

– Шифрование и защита данных –шифрование данных в пути и на хранении и внедрение планов резервного копирования и восстановления данных имеют решающее значение для защиты данных.

Следует также иметь ввиду технологии и инструменты кибербезопасности [9]:

– Брандмауэры и системы обнаружения вторжений –защищают сети от несанкционированного доступа и мониторят подозрительную активность;

– Антивирусное и анти-малварное ПО – обеспечивают защиту от известных сигнатур вредоносных программ и различных видов вредоносного ПО;

– Системы управления информацией о безопасности (SIEM) –решения SIEM собирают и анализируют данные о безопасности, помогая выявить и реагировать на инциденты безопасности в реальном времени.

– В каждом случае необходимо реагирование на инциденты и восстановление. К ним относится [10]:

– Подготовка к кибератакам–организации должны иметь план реагирования на инциденты, команду реагирования на инциденты и проводить регулярные тесты и учения;

– Обнаружение и реагирование на инциденты –обнаружение, ограничение, ликвидация инцидентов и тщательное расследование - важные шаги в реагировании на инциденты;

– Восстановление и уроки, извлеченные из инцидентов – восстановление, документирование и непрерывное усовершенствование - критические шаги после инцидентов для организаций.

Невозможно оставить без внимания и тренды в информационной безопасности [7]:

– Искусственный интеллект в кибербезопасности и машинное обучение все чаще используются для выявления угроз в реальном времени и автоматизированного реагирования на инциденты;

– Проблемы безопасности интернета вещей –рост числа устройств Интернета вещей вводит новые уязвимости, которые необходимо учитывать;

– Блокчейн и информационная безопасность –блокчейн повышает целостность данных и представляет возможности и вызовы, особенно в использовании криптовалют.

Необходимо также обратить внимание на соблюдение и правовые аспекты [7]:

– GDPR и защита данных – накладывает строгие требования по защите данных на организации, обрабатывающие персональную информацию;

– HIPAA и защита медицинской информации – устанавливает стандарты для защиты медицинских данных, требуя от медицинских организаций внедрения мер безопасности;

– Киберзащита и соблюдение – различные отрасли имеют отраслевые регуляции по кибербезопасности, чтобы обеспечить соблюдение мер безопасности, невыполнение которых влечет за собой серьезные последствия.

Важно не забывать о практиках информационной безопасности, таких как [5]**:**

– Обучение и привлечение сотрудников к проблемам безопасности – регулярные программы обучения по безопасности неотъемлемы для информирования сотрудников о существующих угрозах и безопасных практиках. Эти программы обучают персоналу распознавать и реагировать на угрозы безопасности, такие как фишинговые письма или атаки методом социальной инженерии. Они также подчеркивают важность соблюдения протоколов безопасности и лучших практик;

– Регулярные аудиты и оценки безопасности – проведение регулярных аудитов и оценок безопасности имеет важное значение для организаций. Сканирование на уязвимости и пенетрационное тестирование - это методы, которые используются для выявления и устранения уязвимостей безопасности. Сканирование на уязвимости помогает выявить слабые места в программном обеспечении, системах или сетях, а пенетрационное тестирование моделирует атаки в реальных условиях для оценки уровня безопасности организации;

– Культура совместной безопасности – стимулирование культуры совместной безопасности в организации побуждает сотрудников принимать активное участие в обеспечении безопасности. Это подразумевает общую ответственность, при которой каждый сотрудник играет роль в защите чувствительных данных и в сообщении о событиях безопасности. Крепкая безопасностная культура способствует повышению осведомленности, сотрудничеству и соблюдению протоколов безопасности.

Будущее информационной безопасности заключается в следующих аспектах:

– Эволюция ландшафта угроз – ландшафт угроз постоянно эволюционирует, поскольку киберпреступники разрабатывают более

сложные методы атак. Этот подраздел подчеркивает необходимость для организаций оставаться бдительными и адаптироваться к новым угрозам. Он отмечает, что угрозы станут все более сложными и разнообразными, требуя применения продвинутых мер безопасности и стратегий;

– Ожидаемые технологические достижения – в этом подразделе обсуждается роль предстоящих технологий в информационной безопасности. Упоминаются квантовые вычисления, кибербезопасность на основе искусственного интеллекта и вычисления на периферийных устройствах. Квантовые вычисления могут нарушить существующие методы шифрования, что потребует новых средств безопасности. Искусственный интеллект будет использоваться для выявления и реагирования на угрозы в реальном времени. Вычисления на периферийных устройствах представляют вызовы в области безопасности, так как обработка данных будет происходить на устройствах, а не на централизованных серверах;

– Роль профессионалов в области кибербезопасности – поскольку растет спрос на квалифицированных специалистов в области кибербезопасности, становится важным постоянное обучение и повышение квалификации. В этом подразделе подчеркивается значение того, чтобы специалисты в области кибербезопасности оставались в курсе новых угроз и технологий. Также акцентируется важность прохождения сертификаций и постоянного обучения для удовлетворения требований быстро меняющейся области кибербезопасности.

На основе изложенного выше следует заключить, что информационная безопасность имеет первостепенное значение в цифровой эпохе. Она охватывает фундаментальные принципы, динамичный ландшафт угроз, соблюдение и лучшие практики, а также перспективы развития новых технологий. Поскольку организации и частные лица всё больше полагаются на цифровые технологии, обеспечение безопасности данных, систем и сетей становится постоянной задачей. Будущее информационной безопасности представляет вызовы и возможности, требуя бдительности, адаптации и сотрудничества для защиты цифрового мира.

Список используемых источников:

1. Смит Д. Введение в Информационную Безопасность[Электронный ресурс] // Издательство ABC. 2020. URL: selfpub.ru/?utm_source=yandex&utm_medium=cpc&utm_campaign=izdatelstvo_poisk&utm_content=utp5&utm_term=электронные%20издательства&yclid=447823002484342783 (дата обращения: 05.10.2023).

2. Джонсон М. Ландшафт Угроз в Кибербезопасности: Тенденции и Вызовы // Журнал Кибербезопасности. 2019. N 8(2). С. 45-62.

3. Лучшие Практики по Защите Устройств Интернета Вещей [Электронный ресурс] // Агентство Кибербезопасности и Инфраструктуры (CISA). 2022. URL: //ozuz.ru/luchshie-praktiki-v-oblasti-kiberbezopasnosti-zashhita-vashih-cifrovyh-aktivov/?ysclid=lnseun2ozu499639948 (дата обращения: 06.10.2023).

4. Смит Э. Будущая Роль Профессионалов в Кибербезопасности: Вызовы и Возможности // Журнал Кибербезопасности. 2019. N 15(4). С. 321-335.

5. Андерсон Д. Влияние ИИ на Кибербезопасность // Международная Конференция по Кибербезопасности. 2021. (ICC). С.123-140.
6. Общее Регулирование по Защите Данных [Электронный ресурс] // Европейский Союз. 2018.URL: ru.wikibrief.org/wiki/General_Data_Protection_Regulation (дата обращения: 07.10.2023).
7. Закон о Переносимости и Ответственности в Области Здравоохранения [Электронный ресурс] // Министерство Здравоохранения и Социальных Служб США. 2009. URL: ranslated.turbopages.org/proxy_u/en-ru.ru.d16feef3-652cc007-03fd9364-74722d776562/https/htm.fandom.com/wiki/Health_Insurance_Portability_and_Accountability_Act (дата обращения: 08.10.2023).
8. NIST Кибербезопасности [Электронный ресурс] // Национальный Институт Стандартов и Технологий. 2018. URL: www.nist.gov/cybersecurity (дата обращения: 09.10.2023).
9. Квантовые Вычисления и Квантовая Криптография [Электронный ресурс] // Национальный Институт Стандартов и Технологий. 2020. URL: moscow-test.ru/content/kvantovye-vychisleniya-i-kvantovaya-kriptografiya?ysclid=lnsf08ar43462915551 (дата обращения: 10.10.2023).
10. Программы Сертификации в Области Кибербезопасности [Электронный ресурс] // Международная Ассоциация Профессионалов в Области Кибербезопасности.2021. URL: habr.com/ru/articles/746154/ (дата обращения: 11.10.2023).

Visal I., Shterenberg S.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Ensuring the security of the digital world: comprehensive guide to information security.
In today's increasingly interconnected and digital world, the importance of information security cannot be underestimated. With the development of technology, threats and vulnerabilities that can endanger confidential data and digital assets are increasing. This comprehensive guide deeply explores the world of information security, providing an understanding of its fundamentals, the current threat of the situation, best practices and a look into the future of this important area

Key words: security, information security, threat, digital world, danger.

УДК 004.056.53
ГРНТИ 81.93.29

К ВОПРОСУ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ УТЕЧЕКИ КОМПРОМЕТАЦИИ

Л. А. Виткова, А. Л. Зрелова

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

В статье рассматривается проблема защиты персональных данных в Российской Федерации. Особое внимание уделяется киберпреступлениям, которые за последний год привели к краже и распространению баз данных пользователей. Заметно, что требования к операторам персональных данных становятся все более строгими с целью укрепления защиты персональных данных и обеспечения неприкосновенности частной жизни. Анализ внесенных изменений в законодательство РФ о персональных данных проведен после участившихся атак на крупные компании и утечку личной информации пользователей.

кибератаки, персональные данные, анализ законодательства, утечки персональных данных

Введение

Проблема обеспечения защиты персональных данных является крайне актуальной в современном мире. В 2022 году было зарегистрировано увеличение в два раза числа кибератак на Российскую Федерацию по сравнению с предыдущим годом. В 2023 году рост составил еще в 1,5 раза. Атаки, направленные на кражу персональных данных, стали массовыми. Однако, мотивация киберпреступников изменилась. Ранее, украденные базы персональных данных продавались на теневых и «полутеневых» ресурсах, таких как форумы в Dark web. В настоящее время же, эти данные выкладываются в публичный доступ с целью нанесения репутационного и экономического ущерба бизнесу и его клиентам [1].

Анализ изменений в нормативно правовом поле ПДн

С начала сентября 2022 года вступили в силу значительные изменения в законодательство, регулирующее работу с персональными данными, вследствие непростой ситуации, которая сложилась. 152-й Федеральный закон «О персональных данных» подвергся изменениям, направленным на ужесточение требований к обработке персональных данных, касающихся не только операторов и сторонних обработчиков, но и регуляторов и органов государственной власти [2].

Согласование с Роскомнадзором теперь обязательно для всех нормативных актов Российской Федерации, связанных с передачей персональных данных за границу, обработкой особых видов данных (например, информацией о состоянии здоровья), с использованием биометрических данных и с передачей персональных данных

несовершеннолетних лиц. Также требуется согласование вопросов о предоставлении и распространении персональных данных, полученных после обезличивания.

С 1 марта 2023 года вступили в силу изменения статьи 12 ФЗ № 152 «О персональных данных», которые ужесточают требования к трансграничной передаче. Роскомнадзор получил право ограничивать или полностью запрещать передачу персональных данных в страны, которые не обеспечивают адекватную защиту.

В приказе №128 от 05.08.2022 Роскомнадзор утвердил список 89 стран, которые обеспечивают адекватную защиту прав субъектов персональных данных. В этот список включены как участники конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, так и страны, не принимающие участие в конвенции, но соответствующие ее положениям в своих нормах права и принимаемых мерах [3].

Роскомнадзор требует, чтобы операторы незамедлительно сообщали о произошедших инцидентах с передачей персональных данных. Информация должна быть предоставлена в течение 24 часов с момента обнаружения неправомерной или случайной передачи данных, а результаты внутреннего расследования должны быть представлены в течение 72 часов.

Выводы

Каждый год статистические данные экспертно-аналитических центров подтверждают, что персональные данные остаются наиболее привлекательным ресурсом для киберпреступников. Утечка таких данных сталкивает все больше пользователей с проблемами. В 2023 году все увидели еще большее количество утечек и появилось множество скомпрометированных баз данных. Это может привести к появлению нового тренда среди киберпреступников – объединению различных баз данных для создания полного личного профиля человека. Такие сведения позволят киберпреступникам осуществлять более сложные атаки и манипулировать организациями с помощью социальной инженерии. Необходима методика защиты персональных данных от утечек и компрометации, учитывающая сложившуюся обстановку в государстве и в обществе и обеспечивающая повышение осведомленности граждан об утечках их персональных данных.

Разработана методика поиска информации об утечке персональных данных граждан, в будущем планируется предложить архитектуру системы оповещения и предупреждения.

Список используемых источников:

1. Аналитика отрасли информационной безопасности. Международные новости утечек информации, ежегодные аналитические отчеты и статистика по инцидентам за прошедшие годы URL: https://www.infowatch.ru/analytics/analitika (дата обращения: 30.10.2023)

2.Федеральный закон от 14.07.2022 № 266-ФЗ "О внесении изменений в Федеральный закон "О персональных данных", отдельные законодательные акты

Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона "О банках и банковской деятельности"

3.Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций приказ от 5 августа 2022 г. № 128 «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных»

Vitkova L., Zrelova A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

On the issue of protecting personal data from leakage of compromise

The article deals with the problem of personal data protection in the Russian Federation. Particular attention is paid to cybercrimes, which over the past year have led to the theft and distribution of user databases. It is noticeable that the requirements for personal data operators are becoming more stringent in order to strengthen the protection of personal data and ensure privacy. The analysis of the changes made to the legislation of the Russian Federation on personal data was carried out after the frequent attacks on large companies and the leakage of users' personal information.

Key words: Cyber attacks, personal data, analysis of legislation, leaks of personal data.

УДК 004.056.53
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ СИСТЕМЫ МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Л. А. Виткова, Н. А. Крестьяшин, Пучков В.В.
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире количество угроз информационной безопасность неуклонно растет. Производители создали множество средств защиты информации: антивирусы, межсетевые экраны, системы предотвращения утечек информации и так далее. Однако данные решения не позволяют оценить состояние защищенности всей используемой инфраструктуры. Для решения подобной задачи существуют системы мониторинга событий информационной безопасности.

события, система мониторинга, siem, информационная безопасность

Введение

В нашем стремительном информационном веке, где данные играют ключевую роль во всех аспектах нашей жизни, обеспечение информационной безопасности стало неотъемлемой частью операций и процессов в организациях и компаниях. Системы мониторинга событий информационной безопасности, также известные как SIEM-системы (Security Information and Event Management) являются надежным инструментом для выявления и реагирования на потенциальные угрозы и киберинциденты [1,2]. В данной работе представлено исследование, направленное на анализ функциональных возможностей системы мониторинга событий информационной безопасности «Wazuh».

Анализ

Система мониторинга событий информационной безопасности – это программно-аппаратный комплекс, предназначенный для наблюдения, сбора анализа и управления событиями, происходящими в информационных системах [3,4]. Большинство SIEM-систем обладает следующими функциями:

- Сбор данных - SIEM-система собирает данные из различных источников в информационной системе, таких как журналы событий операционных систем, логи сетевого оборудования, события АСУ ТП систем, а также других источников.
- Нормализация данных - Собранные данные проходят процедуру нормализации - приведение к единому формату, который облегчает дальнейший анализ событий.
- Корреляция - SIEM-система проводит корреляцию событий для выявления связи между ними.

•Обнаружение угроз и инцидентов - SIEM-систем способна выявлять угрозы и инциденты информационной безопасности.

•Уведомления и реагирование – При обнаружении угрозы или инцидента, SIEM-система создает уведомления для офицера безопасности.

•Отчетность и анализ – SIEM-система позволяет создавать отчет о состоянии защищенности подключенных источников и оценки эффективности принятых мер по обеспечению безопасности.

Wazuh

Wazuh – SIEM-система с открытым исходным кодом, распространяемая по свободной лицензии и разрабатываемая сообществом разработчиков по всему миру [5].

Архитектура программного комплекса Wazuh представлена следующими компонентами:

•Wazuh indexer – полнотекстовый движок поиска, данный компонент предназначен для хранения событий, созданных компонентом Wazuh server;

•Wazuh server – данный компонент отвечает за получение событий от агентов и последующую обработку в соответствии с установленными правилами и декодерами. Также данный компонент предназначен для управления и настройки агентов.

•Wazuh agent – компонент, реализующий сбор данных с конечных устройств в информационной системе.

•Wazuh dashboard – пользовательский графический интерфейс, визуализирующий поток обрабатываемых событий, а также обнаруженных инцидентов.

На рис. 1 представлена структурная схема взаимодействия компонентов программного комплекса Wazuh.

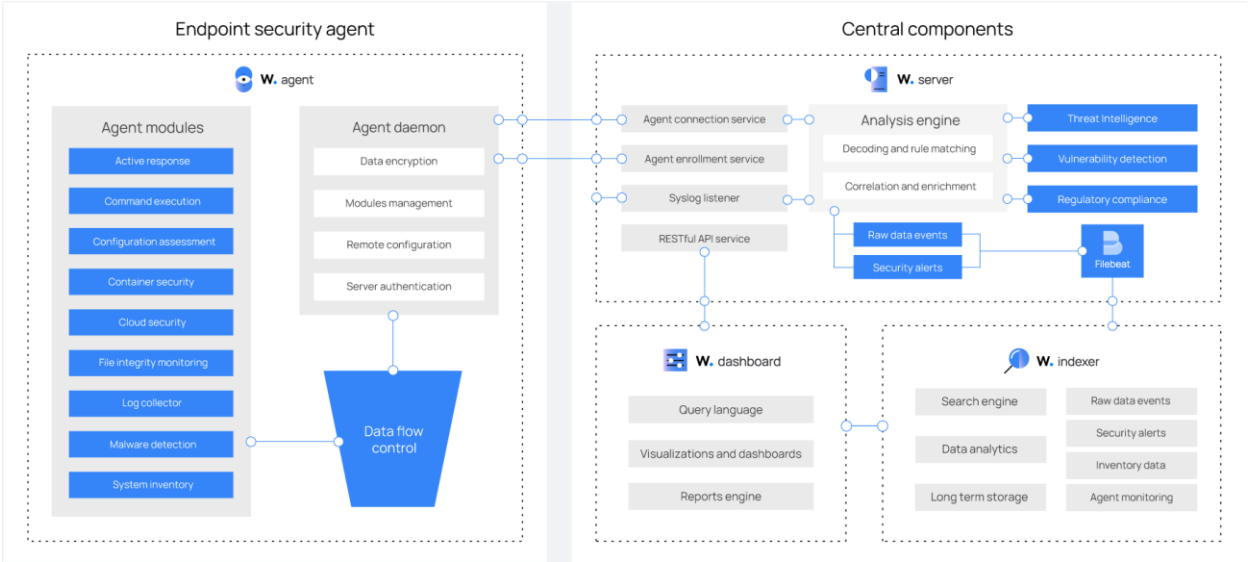


Рис. 1. Структурная схема взаимодействия компонентов программного комплекса Wazuh

Функциональные возможности

Программный комплекс Wazuh поддерживает следующие методы сбора событий информационной безопасности:

•Безагентный метод – данный способ используется для сбора с источников, на которые невозможно выполнить установку агента. В большинстве случаев такими источниками является сетевое оборудование: межсетевые экраны, коммутаторы, маршрутизаторы.

•Агентный метод – данный способ реализуется через установку на источник программы-агента.

Функциональные возможности агента, помимо сбора событий, также позволяют решать следующие задачи (рис. 2):

•Контроль целостности файлов – агент способен отслеживать вносимые в файл изменения;

•Обнаружение уязвимостей – скан операционных систем и установленного ПО для проверки наличия уязвимостей;

•Системная инвентаризация - агента регулярно выполняет сканирование сети и собирает следующую информацию: версия операционной системы, сетевые интерфейсы, запущенные процессы, установленные приложения и список открытых портов;

•Активное реагирование – агент автоматически реализует меры по устранению обнаруженных угроз: блокирование сетевого соединения, завершение процессов, а также удаление подозрительных файлов.

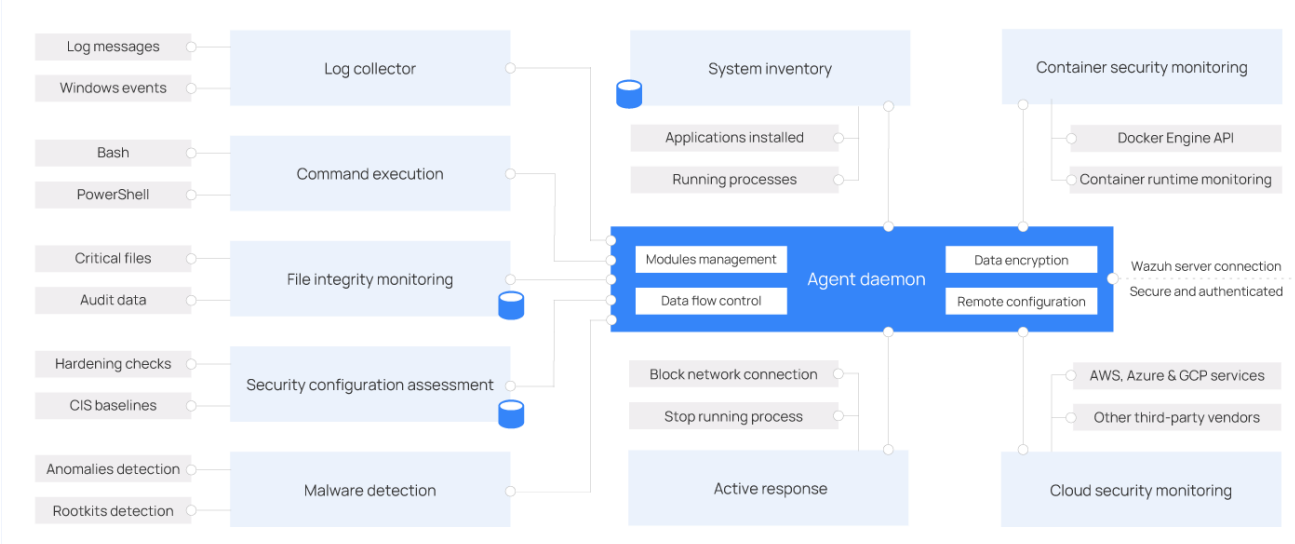


Рис. 2. Функциональные возможности компонента «Агент»

Заключение

В данной статье было представлено исследование, направленное на анализ функциональных возможностей системы мониторинга событий информационной безопасности «Wazuh». Анализ рассмотренных источников показал, что данная система обладает достаточным функционалом для разработки методики расследования киберинцидентов.

Список используемых источников:

1. Абраменко Г. Т. Обзор средств мониторинга локальных событий информационной безопасности / Г. Т. Абраменко, Л. А. Виткова, М. В. Мельник // 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. 46-49. EDN GHRPIO.
2. Штеренберг С. И. Разработка методики внедрения и выявления эффективности siem-системы / С. И. Штеренберг, Ю. С. Данилова // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 3. С. 40-45. DOI 10.46418/2079-8199_2020_3_6. EDN HTBAAS.
3. Красов А. В. Разработка методики внедрения и выявления эффективности SIEM-системы в среде доверенной зоны // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2022. N 3. С. 109-120. – DOI 10.37882/2223-2966.2022.03.18. EDN XYRYTI.
4. Дешевых Е. А. Интеграция siem-систем с системами корреляции событий безопасности, основанных на технологии больших данных / Е. А. Дешевых, И. А. Ушаков, А. А. Чечулин // Информационные технологии в управлении : материалы 9-й конф. по проблемам управления, Санкт-Петербург, 04–06 окт. 2016 г. СПб. : Концерн «Центральный научно-исследовательский институт «Электроприбор», 2016. С. 684-687. EDN XFCHVV.
5. Components // Wazuh URL: https://documentation.wazuh.com/current/getting-started/components/index.html (дата обращения: 20.10.2023).

Vitkova L., Krestyashin N., Puchkov V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Investigation of the functionality of the information security event monitoring system.

In the modern world, the number of threats to information security is steadily increasing. Manufacturers have created a variety of information security tools: antiviruses, firewalls, information leakage prevention systems, and so on. However, these solutions do not allow us to assess the security status of the entire infrastructure used. To solve such a problem, there are systems for monitoring information security events.

Key words: events, monitoring system, SIEM, information security.

УДК 004.056
ГРНТИ 81.93.29

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОБЛАСТИ МЕДИЦИНСКИХ УСТРОЙСТВ И ЭЛЕКТРОННОГО ЗДРАВООХРАНЕНИЯ

А. В. Воробьев
Санкт-Петербургский государственный университет промышленных технологий и дизайна

С развитием современных технологий в медицине возникают серьезные угрозы в области информационной безопасности. В связи с этим необходимо уделять особое внимание обеспечению информационной безопасности в медицинской сфере, чтобы минимизировать риски и обеспечить защиту чувствительных данных.

информационная безопасность, медицинские устройства, электронное здравоохранение, конфиденциальные данные

Тема информационной безопасности в области медицинских устройств и электронного здравоохранения становится все более актуальной в современном мире, где медицинские технологии и электронное здравоохранение играют ключевую роль в обеспечении качественной медицинской помощи. Использование высокотехнологичных медицинских устройств и систем электронного здравоохранения способствует улучшению диагностики, лечения и учета пациентов, однако вместе с этим возникают серьезные проблемы в области информационной безопасности. Электронные медицинские устройства, хранящие и обрабатывающие чувствительные медицинские данные, подвергаются разнообразным угрозам, таким как хищение личных данных, вредоносные атаки и нарушение конфиденциальности.

За последнее десятилетие цифровая революция привела к появлению разнообразных медицинских технологий, способных существенно улучшить диагностику, лечение и уход за пациентами, таких как цифровые медицинские карты, мониторинг состояния пациентов в реальном времени, телемедицину, а также множество медицинских устройств, начиная от портативных электрокардиографов и заканчивая имплантируемыми медицинскими устройствами.

С ростом числа электронных медицинских устройств и объема медицинских данных, цифровая безопасность становится вопросом первостепенной важности. Утечка медицинской информации может иметь серьезные последствия для конфиденциальности пациентов, и, что более важно, для их здоровья и безопасности. Например, если хакеры получат доступ к медицинским данным и изменят лекарственные назначения, это может привести к непредсказуемым последствиям и даже угрожать жизни пациентов. Компрометация электронных медицинских записей может

создать возможность для мошенничества и краж. Такие инциденты могут также повлиять на доверие общества к системам электронного здравоохранения и вызвать социальные и юридические последствия для медицинских организаций и медицинских специалистов.

Одним из ключевых аспектов информационной безопасности в сфере здравоохранения является аутентификация и авторизация пользователей. Системы электронного здравоохранения часто хранят чувствительные медицинские данные, и поэтому необходимо обеспечивать доступ к ним только уполномоченным лицам. Это может быть достигнуто с помощью современных методов биометрической идентификации, многофакторной аутентификации и других технологий. Однако, даже наличие сильных методов аутентификации не гарантирует полной безопасности, поскольку хакеры могут применять социальную инженерию или вредоносные программы.

Помимо вопросов аутентификации, важно обеспечивать целостность и конфиденциальность медицинских данных в электронных системах. Криптография и механизмы защиты данных играют решающую роль в этом вопросе. Шифрование данных может предотвратить несанкционированный доступ к медицинской информации, а также обеспечить ее целостность. Однако даже с самыми современными технологиями криптографии возможны угрозы, связанные с человеческим фактором, когда сотрудники медицинских организаций могут иметь доступ к данным и злоупотреблять им.

Также хакерским атакам подвержены медицинские устройства, нападения на которые могут иметь серьезные последствия. Например, хакеры могут взломать имплантируемые медицинские устройства, такие как кардиостимуляторы или инсулиновые помпы, и повлиять на их работу. Это может повлечь за собой ситуации, опасные для здоровья и жизни пациентов. Такие атаки также могут быть использованы для шантажа или вымогательства.

Целью данной работы является выявление и анализ угроз для медицинских устройств и электронного здравоохранения в области информационной безопасности, а также предложение рекомендаций по их устранению.

Список используемых источников:

1. Information Security Behavior in Health Information Systems: A Review of Research Trends and Antecedent Factors // MDPI - Publisher of Open Access Journals URL: https://www.mdpi.com/2227-9032/10/12/2531 (дата обращения: 12.10.2023).

2. Information Security Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities // NCBI – National Library of Medicine URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8481013 (дата обращения: 14.10.2023).

3. Обеспечение информационной безопасности в медицинских организациях // КиберЛенинка — научная электронная библиотека URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-v-meditsinskih-organizatsiyah (дата обращения: 15.10.2023).

Vorobiev A.

Saint Petersburg State University of Industrial Technologies and Design

Information security in e-health and medical devices.

With the development of modern technologies in medicine, serious threats arise in the field of information security. In this regard, it is necessary to pay attention to ensuring information security in the medical field in order to minimize risks and ensure the protection of sensitive data.

Key words: information security, medical devices, e-health, confidential data.

УДК 003.26.09
ГРНТИ 28.29.19

ОСНОВНЫЕ ВИДЫ АТАК НА СИСТЕМУ КВАНТОВОЙ КРИПТОГРАФИИ

А. А. Воронцов, С. Н. Шемякин
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича.

Создание совершенных алгоритмов распределения ключей является одним из приоритетных направлений современной криптографии. Для передачи по сетям связи больших объемов информации требуется частая смена ключей шифрования. Алгоритмы распределения ключей должны решать проблему доставки ключей шифрования участникам сети связи при условии того, что они будут недоступны для нарушителей. В настоящее время проводятся многочисленные исследования алгоритмов распределения ключей, основанных на принципах квантовой криптографии, представляющей собой одно из передовых направлений развития современных средств защиты информации.

информационная безопасность, защищенная связь, модели выбора ключей, секретность ключа, квантовая криптография

Введение

Создание совершенных алгоритмов распределения ключей является одним из приоритетных направлений современной криптографии. Для передачи по сетям связи больших объемов информации требуется частая смена ключей шифрования. Алгоритмы распределения ключей должны решать проблему доставки ключей шифрования участникам сети связи при условии того, что они будут недоступны для нарушителей [4].

Большинство классических алгоритмов распределения ключей основаны на криптографических протоколах. Эти алгоритмы обеспечивают секретность ключей с помощью математических методов. Однако, с внедрением квантовых компьютеров, данные методы защиты могут потерять свою стойкость [3].

С 80-ых годов прошлого века ведется разработка квантовых криптографических алгоритмов, которые могут быть устойчивы к взлому с помощью квантового компьютера. Эти алгоритмы полагаются на постулаты квантовой теории. Безопасность квантовой криптографии основывается на принципе неопределенности Гейзенберга. Он является одним из краеугольных камней квантовой механики и может быть сформулирован следующим образом: существует некоторый ненулевой предел для точности измерений параметров физической частицы [6]. Иными словами, этот принцип обосновывает невозможность измерения квантового состояния (поляризация и фаза) отдельной частицы, не внеся в нее искажения.

Алгоритмы квантовой криптографии находят применение главным образом в системах распределения ключевых данных. Их называют системами квантового распределения ключей – Quantum key distribution (QKD). В качестве примеров методов квантового распределения ключей алгоритмы BB84, B92, E91 и другие. При кажущейся на первый взгляд

устойчивости, подобные системы теоретически могут быть подвержены атакам злоумышленников. Наиболее распространенные типы атак нарушителя: атака «перехват-перепосылка» и атака индивидуальных измерений.

Атака «перехват-перепосылка»

В квантовой связи для кодирования информации используются особые квантовые состояния, называемые кубитами. Кубит или квантовый бит – это квантово-механическая система, имеющая только два состояния: 0 и 1. Кубит является аналогом логического бита в классической криптографии.

Квантовое состояние кубита может представляться, как линейная суперпозиция его ортонормированных базисных векторов (базисных состояний). Существует специальная нотация Дирака (нотация bra-ket), которая применяется для записи этих базовых векторов. Запись кубита осуществляется следующим образом: $[0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ и $[1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$. Состояния $\{[0\rangle;\ [1\rangle\}$ называют вычислительным базисом кубита.

Теперь определим понятия прямоугольного и диагонального базисов. Рассмотрим вектор

$$|u\rangle = cos0 * |0\rangle + sin0 * |1\rangle = |0\rangle$$

Тогда пара операндов

$$R = \{R_0 = |0\rangle\langle 0|, R_1 = I - |0\rangle\langle 0|\}$$

осуществляет измерение, то есть порождает вероятностное распределение на множестве исходов $\{0, 1\}$ в прямоугольном базисе R [1]. Здесь I – единичный элемент.

Также рассмотрим вектор

$$|u\rangle = cos\frac{\pi}{4} * |0\rangle + sin\frac{\pi}{4} * |1\rangle = |0\rangle$$

Тогда пара операндов

$$D = \{D_0 = |u\rangle\langle u|, D_1 = I - |u\rangle\langle u|\}$$

осуществляет измерение, то есть порождает вероятностное распределение на множестве исходов $\{0, 1\}$ в диагональном базисе D [1].

Термин базис здесь понимается как упорядоченный набор векторов в векторном пространстве. Прямоугольный базис R представляет собой двумерную прямоугольную систему координат, а диагональный базис D задает такую же систему координат, но повернутую на 45° относительно базиса R.

Для описания атак на любую криптосистему используются следующие обозначения:

- Алиса и Боб – легальные корреспонденты, которые обмениваются сообщениями между собой;
- Ева – нарушитель, который пытается взломать криптографическую систему.

Атака типа «перехват-перепосылка» происходит следующим образом:

1. Ева выбирает случайным образом измерительные базисы R и D.
2. Ева внедряется в канал связи и перехватывает передаваемые фотоны.

3. Ева с помощью имеющихся измерительных базисов осуществляет прием фотонов и извлекает сообщения.

4. Ева отправляет Бобу фотон в том квантовом состоянии и в том базисе, в котором она его получила.

Данная атака во многом схожа с атакой «человек посередине» в цифровых сетях связи. Базисы легальных корреспондентов, Алисы и Боба, согласованы до сеанса связи. Для этого помимо оптического квантового канала вводится также классический канал связи.

Для Боба при несовпадении базисов, вероятность получить правильный результат на приеме фотонов составляет ½.

Атака индивидуальных измерений

Еще один тип атаки называется атакой индивидуальных измерений. В ходе этой атаки злоумышленник нарушает ортогональность квантовых состояний, передаваемых по квантовому каналу связи. Для этой цели Ева использует квантовую память, в которой для хранения информации применяются особые квантовые биты [1].

Нарушитель Ева имеет в своей квантовой памяти различные квантовые состояния, обозначаемые $|A\rangle$ (ancilla). Ева перехватывает фотоны из квантового канала и позволяет каждому квантовому состоянию взаимодействовать отдельно с его собственным $|A\rangle$ из ячеек памяти. В результате передаваемое состояние и $|A\rangle$ оказываются запутанными. Состояние $|A\rangle$ изменяется в зависимости от передаваемого состояния. Изменяется также передаваемое состояние. Далее измененное состояние Алисы отправляется Бобу по квантовому каналу. После произведенных Бобом измерений, корреспонденты согласуют базисы. Посылки, где Боб производил измерения в не согласованным с Алисой базисе, отбрасываются [2].

После взаимодействия Ева удерживает все состояния для измерений. При этой атаке Ева знает правильные базисы из классического канала обратной связи и проводит измерения после согласования базисов. В этом виде атак, называемых также некогерентными, предполагается, что Ева ждет только окончания процедуры сравнения базисов и не дожидается окончания процедур коррекции ошибок и усиления секретности [3].

В этой модели векторы (квантовые состояния) $|0\rangle$ и $|1\rangle$ кодируют логические биты 0 и 1. $|A\rangle$ – квантовое состояние Евы.

На рис. 1 представлено положение векторов квантовых состояний в прямоугольном базисе после атаки индивидуальных измерений.

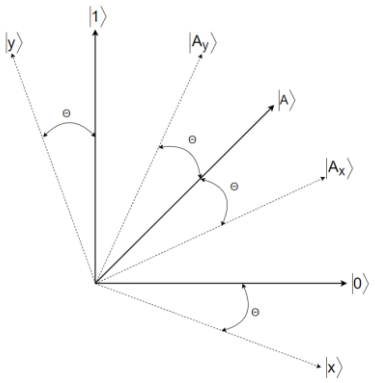


Рис. 15. Положение векторов квантовых состояний

Если передавалось квантовое состояние $|0\rangle$, то при внедрении Евы в квантовый канал происходит поворот квантовых состояний $|0\rangle$ и $|A\rangle$ на угол Θ по часовой стрелке до соответствующих квантовых состояний $|x\rangle$ и $|A_x\rangle$.

Если передавалось квантовое состояние $|1\rangle$, то при внедрении Евы в квантовый канал происходит поворот квантовых состояний $|1\rangle$ и $|A\rangle$ на угол Θ против часовой стрелке до соответствующих квантовых состояний $|y\rangle$ и $|A_y\rangle$.

Таким образом, вместо ортогональных состояний $|0\rangle$ и $|1\rangle$ на приеме Боб вынужден различать не ортогональные состояния $|x\rangle$ и $|y\rangle$ [1].

Также можно рассчитать вероятность ошибки, с которой Боб будет различать состояния $|x\rangle$ и $|y\rangle$. Согласно [1] эта вероятность равна:

$$Q_B = \frac{1}{2} - \frac{1}{2}\cos(2\theta)$$

Вероятность ошибки различения квантовых состояний для нарушителя Евы может быть получена как:

$$Q_E = \frac{1}{2} - \frac{1}{2}sin(2\theta)$$

Таким образом, можно заключить, что при атаке индивидуальных измерений Алиса-Боб и Алиса-Ева находятся в ситуации классического двоично-симметричного канала связи с искажениями [5].

Заключение

Рассмотренные в статье атаки на данный момент могут быть осуществлены лишь с помощью теоретических моделей. Для практической реализации этих атак необходимо создать устройства, способные извлекать фотоны из квантового канала, а также механизмы квантовой памяти. Однако, необходимо отметить, что система квантового распределения ключей должна быть стойкой к описанным специфическим атакам. В работе приводятся примеры лишь некоторых основных видов атак, список которых может быть впоследствии дополнен.

Список используемых источников:

1. Арбеков И. М. Элементарная квантовая криптография: Для криптографов, не знакомых с квантовой механикой : учеб. пособие. М. : Издательство Ленанд, 2022. 168 с., ил. - ISBN 978-5-9710-9745-7

2. Молотков С. Н., Тимофеев А. В., Явная атака на ключ в квантовой криптографии (протокол BB84), достигающая теоретического предела ошибки Qc ≈ 11% : Письма в ЖЭТФ, 85:10 (2007), 632–637; JETP Letters, 85:10 (2007), 524–529.

3. Белера Р. А., Деев Д. Д., Смирнов И. А., Короченцев Д. А., Черкесова Л. В. Квантовый хакинг: атаки на линии связи [Электронный ресурс] // Научное обозрение. Технические науки. 2020. N 4. С. 7-13; URL : https://science-engineering.ru/ru/article/view?id=1295 (дата обращения: 31.10.2023).

4. Коржик В. И. Основы криптографии : учеб. пособие. СПб. : СПбГУТ, 2014. 277 с. : ил. ISBN 978-5-89160-097-3

5. Молотков С. Н. О квантовомеханической границе на величину утечки информации по побочным каналам в квантовой криптографии : Письма в ЖЭТФ, 97:10 (2013), 693–699; JETP Letters, 97:10 (2013), 604–610.

6. Действительно ли надёжна квантовая криптография? // Хабр. Блог компании Toshiba. 2020. [Электронный ресурс]. URL: https://habr.com/ru/company/toshibarus/blog/444502/ (дата обращения: 31.10.2023).

Vorontsov A., Shemyakin S.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

The main types of attacks on the quantum cryptography system.

The creation of perfect algorithms for key distribution is one of the priorities of modern cryptography. To transfer large amounts of information over communication networks, frequent change of encryption keys is required. Key distribution algorithms should solve the problem of delivering encryption keys to the participants of the communication network, provided that they will be inaccessible to violators. Currently, numerous studies are being conducted on key distribution algorithms based on the principles of quantum cryptography, which is one of the leading directions in the development of modern information security tools.

Key words: Information security, secure communication, key selection models, key secrecy, quantum cryptography.

УДК 004.054
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ПУТЕЙ ОЦЕНКИ ПРОИЗВОДИТЕЛЬНОСТИ ВЕБ-СЕРВЕРОВ

А. В. Грохольский
Санкт-Петербургский государственный университет телекоммуникаций им. Проф. М. А. Бонч-Бруевича

В работе рассматриваются существующие исследования по анализу производительности веб-серверов. На основе сравнения существующих решений сформированы требования и критерии к разработке собственной методики исследования производительности веб-серверов.

веб-серверы, производительность веб-сервера, методика анализа производительности

В современном информационном обществе веб-серверы играют ключевую роль в обеспечении доступа к веб-ресурсам и обработке запросов от пользователей. Однако, учитывая постоянно изменяющиеся требования и условия, такие как количество одновременных пользователей, объем и типы передаваемых данных, пропускная способность сети и аппаратные характеристики серверов, важно иметь возможность оценивать производительность веб-серверов для оптимизации их работы. В данной работе представляется исследование существующих методик оценки производительности веб-серверов.

Вопросам производительности веб-серверов посвящены различные исследования. В работах [1-2] рассматриваются пути оптимизации веб-серверов, а также исследуется их производительность. Однако, отсутствует сравнительный анализ различных методов и инструментов тестирования производительности, отсутствует детальный анализ влияния сетевых факторов на производительность сервера. В работах [3-4] рассмотрены способы оптимизации серверных приложений, но не рассмотрены методы тестирования производительности веб-сервера, а также работы ограничиваются небольшим набор сценариев тестирования. В работе [5] рассматривается методика по оценке производительности, но не предоставляются методы тестирования самого веб-сервера.

Существуют готовые программные решения [6-11] для оценки производительности. Однако, каждая из программ имеет свои недостатки.

ТАБЛИЦА 1. Перечень некоторых групп недостатков, присущих нескольким популярным инструментам

Недостатки	Программы			
	Gatling	JMeter	Locust	Siege
Ограниченная поддержка протоколов	Да	Нет	Нет	Да
Сложность интерфейса	Да	Да	Нет	Да
Ограниченная документация	Да	Нет	Да	Нет
Требуется дополнительная конфигурация	Нет	Да	Да	Нет
Ограниченные встроенные аналитические отчеты	Нет	Нет	Да	Нет
Ограниченная масштабируемость и высокая загрузка ресурсов	Нет	Да	Нет	Да
Не поддерживает работу в распределенном режиме	Нет	Нет	Да	Нет

Наиболее часто используемый инструмент Apache JMeter позволяет создавать и запускать тестовые сценарии, имитирующие поведение реальных пользователей, чтобы оценить производительность и надежность приложения в условиях высокой нагрузки. Несмотря на высокую популярность, даже он имеет ряд недостатков. Один из существенных недостатков – чрезмерное потребление ресурсов. Для масштабного тестирования Apache JMeter требуется значительное количество аппаратных и сетевых ресурсов, необходимо создавать тестовые серверы и строить централизованные оркестраторы.

Также в некоторых готовых программных решениях имеются такие недостатки, как отсутствие поддержки новых версий PHP и MySQL [12], недостаточное покрытие возможных сценариев, отсутствие конкретных примеров или недостаток документации, что может вызвать затруднения в использовании. Учитывая эти факторы, целесообразно будет разработать методику, устраняющую все недостатки готовых решений.

В результате работы были изучены исследования, а также рассмотрены готовые программные решения по анализу производительности веб-серверов. Дальнейшим путем является задача по разработке собственной методики с учетом недостатков и особенностей уже представленных ранее методик и готовых решений.

Список используемых источников:

1. Jader O. H., Zeebaree S. R., Zebari R. R. A state of art survey for web server performance measurement and load balancing mechanisms // International Journal of Scientific & Technology Research. 2019. Т. 8. N. 12. С. 535-543.

2. Fan Q., Wang Q. Performance comparison of web servers with different architectures: A case study using high concurrency workload // 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb). IEEE, 2015. С. 37-42.

3. Тихонов А. В., Козлов В. В., Юльский А. П. Исследование нагрузочной устойчивости веб-серверов посредством DDoS-атаки // Информационные технологии в работе с одаренной молодежью. 2015. С. 465-469.

4. Дзюбин И. А., Малышев А. В. Способы оптимизации высоконагруженных приложений. // Программная инженерия: современные тенденции развития и применения. 2021. С. 12-20.

5. Ковцур М. М., Михайлова А. В., Потемкин П. А. Разработка методики по оценке тестирования производительности базы данных. // Подготовка профессиональных кадров в магистратуре для цифровой экономики : материалы Всерос. научно-методич. конф., магистрантов и их руководителей, Санкт-Петербург, 30 нояб.-02 дек. 2021 г. Сборник лучших докладов конференции. СПб. : СПбГУТ, 2022. С. 236-240.

6. GitHub – apache/Jmeter. [Электронный ресурс]. URL: https://github.com/apache/jmeter (дата обращения: 30.10.2023).

7. GitHub – JoeDog/siege. [Электронный ресурс]. URL: https://github.com/JoeDog/siege (дата обращения: 30.10.2023).

8. GitHub – gatling/gatling. [Электронный ресурс]. URL: https://github.com/gatling/gatling (дата обращения: 30.10.2023).

9. GitHub – locustio/locust. [Электронный ресурс]. URL: https://github.com/locustio/locust (дата обращения: 30.10.2023).

10. GitHub – manishas_sample/php_mysql. [Электронный ресурс]. URL: https://github.com/manishas/sample_php_mysql (дата обращения: 30.10.2023).

11. GitHub – vanilla-php/benchmark-php. [Электронный ресурс]. URL: https://github.com/vanillaphp/benchmark-php (дата обращения: 30.10.2023).

12. Груздев А. С., Ковцур М. М., Коновалова В. В. Исследование подходов оценки производительности web-сервера // Региональная информатика : материалы XVIII Юбилейной Санкт-Петербургской междунар. конф., 26–28 октября 2022 г. СПб. : СПОИСУ, 2022. С. 546.

Grokholskyi A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Exploring ways to evaluate web server performance.

The paper reviews the existing research on web server performance analysis. Based on the comparison of existing solutions, the requirements and criteria for the development of our own methodology for analyzing the performance of web servers are formed.

Key words: web servers, web server performance, productivity analysis methodology

УДК.004.056
ГРНТИ 81.93.29

ПРОБЛЕМА ВЫЯВЛЕНИЯ НЕЖЕЛАТЕЛЬНОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

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

Социальные сети стали неотъемлемой частью современного общества, предоставляя платформу для общения, обмена информацией и создания сообществ. Однако, с ростом популярности социальных сетей возрастает и проблема нежелательной информации, включая фейковые новости, ненавистный контент и манипуляции общественным мнением. Данная статья рассматривает актуальность проблемы выявления нежелательной информации в социальных сетях, проводит обзор существующих исследований и подчеркивает необходимость дальнейших усилий в области обеспечения безопасной и информационно здоровой среды для пользователей социальных сетей.

социальные сети, нежелательная информация, фейковые новости, безопасность в сети, информационная грамотность

Социальные сети в наше время стали важной частью нашей повседневной жизни. Они предоставляют возможность общения с друзьями, делиться контентом, и находя новых знакомых. Однако, с ростом популярности социальных сетей, возрастает и проблема нежелательной информации. Это включает в себя ложные новости, ненавистный контент, клевету, и многие другие виды вредоносного содержания. В данной статье мы рассмотрим проблему выявления нежелательной информации в социальных сетях, проведем обзор имеющихся исследований и подчеркнем актуальность данной проблемы.

Проблема нежелательной информации в социальных сетях имеет множество аспектов. С одной стороны, это свобода выражения и право на обсуждение разных вопросов. С другой стороны, нежелательная информация может вызвать серьезные негативные последствия, включая манипуляции общественным мнением и нарушение приватности.

Исследования в этой области обычно сосредотачиваются на методах выявления нежелательной информации, а также на разработке алгоритмов и технологий для борьбы с этим явлением. Многие социальные сети активно работают над средствами модерации, фильтрации, искусственным интеллектом и машинным обучением, чтобы выявлять и удалять нежелательный контент.

Актуальность проблемы нежелательной информации в социальных сетях подчеркивается несколькими факторами. Первый фактор - рост числа пользователей социальных сетей, что увеличивает объем информации и возможность ее распространения. Второй фактор - использование

социальных сетей для влияния на общественное мнение и даже выборы. Фейковые новости и манипуляции информацией могут иметь серьезные последствия для общества.

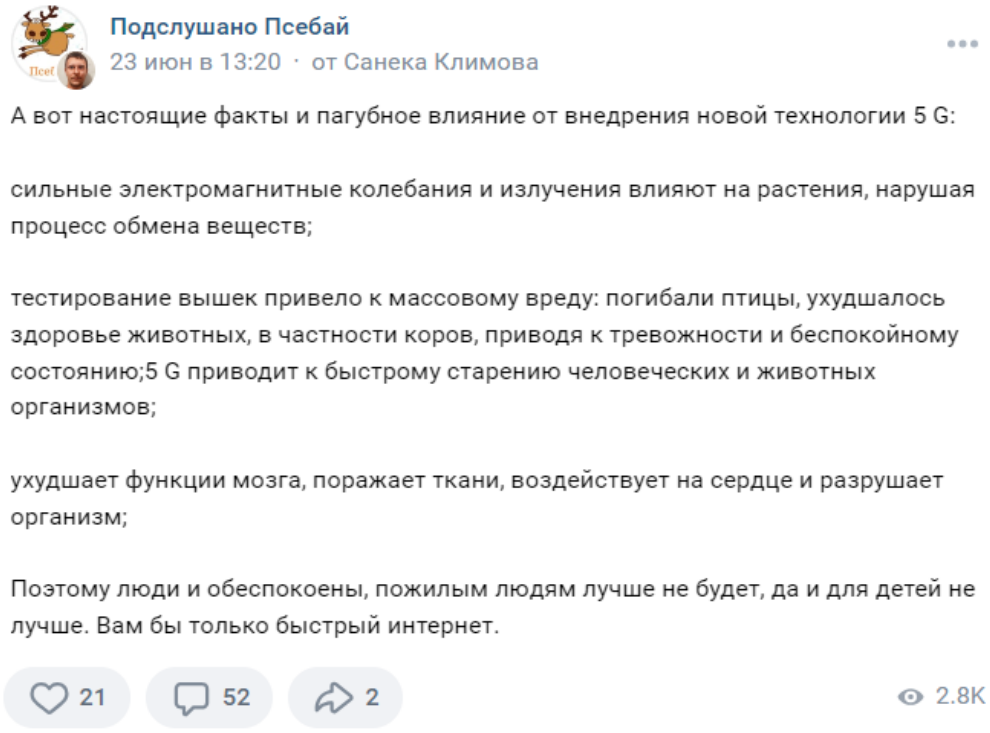


Рис. 1. Пример нежелательной информации из социальной сети «Вконтакте»

Необходимость дальнейшей работы по проблеме нежелательной информации в социальных сетях несомненна. Это включает в себя развитие более точных и эффективных методов выявления и фильтрации нежелательного контента, а также образование и информационную грамотность пользователей. В контексте социальной сети ВКонтакте, как одной из крупнейших российских социальных сетей, особенно важно сотрудничество с исследователями и общественностью для обеспечения безопасной и информационно здоровой среды для всех пользователей.

По проблеме выявления нежелательной информации в социальных сетях, можно выделить несколько слабоизученных проблемных вопросов:

Манипуляции информацией включают в себя создание и распространение фейковых новостей, а также множество других методов воздействия на общественное мнение. Существует необходимость в более глубоком понимании этих методов и разработке эффективных стратегий для их выявления.

Информационная грамотность пользователей играет важную роль в борьбе с нежелательной информацией. Однако, мало исследований посвящено эффективным методам и подходам для развития культуры информационной безопасности среди пользователей социальных сетей.

Эффективное взаимодействие между администрацией социальных сетей и пользователями играет ключевую роль в выявлении нежелательной информации. Слабоизученные аспекты включают в себя методы обратной

связи, обучение пользователей и совместные усилия в борьбе с нежелательным контентом.

На основе выявленных слабоизученных проблемных вопросов, можно сделать вывод о необходимости дальнейших исследований в области выявления и борьбы с нежелательной информацией в социальных сетях. Развитие более точных и эффективных методов выявления, образование и информационная грамотность пользователей, а также взаимодействие между администрацией социальных сетей и сообществом - это ключевые направления для будущих исследований. Эффективное решение этой проблемы обеспечит безопасность и качество использования социальных сетей, создавая более информационно здоровое и дружественное онлайн-пространство для всех пользователей.

Проблема выявления нежелательной информации в социальных сетях остается актуальной и требует дальнейших исследований и разработок. Эффективная борьба с нежелательным контентом не только обеспечит безопасность и приватность пользователей, но и поддержит долгосрочное развитие социальных сетей в цифровой эпохе. ВКонтакте и другие социальные платформы должны продолжать работать над разработкой и совершенствованием инструментов для обнаружения и фильтрации нежелательного контента. Помимо технических инноваций, важно также обучать пользователей различным аспектам информационной безопасности и критическому мышлению.

Итак, проблема нежелательной информации в социальных сетях остается сложной и многогранной. Ее решение требует усилий со стороны разработчиков, исследователей и общества в целом. Вместе мы можем создать среду, где свобода слова соседствует с уважением к мнению других и защитой от вредоносного контента. Только так мы сможем максимально использовать потенциал социальных сетей для обогащения информацией и связей, сохраняя при этом их безопасность и чистоту от нежелательных влияний.

Список используемых источников:

1. Виткова Л. А., Потехин И. Ю., Сахаров Д. В. Проблема выявления информационно-психологического воздействия в информационной инфраструктуре Российской Федерации // 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. 166-170.

2. Виткова Л. А. Обзор степени разработанности темы мониторинга и противодействия угрозам информационно-психологической безопасности в социальных сетях // Информационные технологии и телекоммуникации. 2018. Т. 6. N 3. С. 1-9.

3. Виткова Л. А., Проноза А. А., Сахаров Д. В., Чечулин А. А. Проблемы безопасности информационной сферы в условиях информационного противоборства // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VII Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 28 фев.-01 марта 2018 г. СПб. : СПбГУТ, 2018. С. 191-195.

4. Бирих Э. В., Сахаров Д. В. Модель нарушителя распределенной информационно-вычислительной сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании : V Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 10–11 марта 2016 г. СПб. : СПбГУТ, 2016. С. 235-238.

5. Гамидов Т. О., Десницкий В. А., Дудкина О. С., Сахаров Д. В. Методы и методики анализа нежелательной информации в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании : VIII Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 27–28 фев. 2019 г. СПб. : СПбГУТ, 2019. С. 317-320.

6. Проноза А. А., Виткова Л. А., Чечулин А. А., Котенко И. В., Сахаров Д. В. Методика выявления каналов распространения информации в социальных сетях // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2018. Т. 14. N 4. С. 362-377.

7. Костарев С. В., Липатников В. А., Сахаров Д. В. Модель процесса передачи результатов аудита и контроля в автоматизированной системе менеджмента предприятия интегрированной структуры // Проблемы информационной безопасности. Компьютерные системы. 2015. N 2. С. 120-125.

Gruzdev A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

The problem of identifying unwanted information on social networks.

Social networks have become an integral part of modern society, providing a platform for communication, information exchange and community creation. However, with the growing popularity of social networks, the problem of unwanted information is also increasing, including fake news, hateful content and manipulation of public opinion. This article examines the relevance of the problem of identifying unwanted information in social networks, conducts an overview of existing research and emphasizes the need for further efforts in the field of ensuring a safe and informationally healthy environment for users of social networks.

Key words: social networks, unwanted information, fake news, online security, information literacy.

УДК 004.056.57
ГРНТИ 81.93.29

ВЛИЯНИЕ СОЦИАЛЬНЫХ СЕТЕЙ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

А. Р. Гудочкина
Санкт-Петербургский государственный университет промышленных технологий и дизайна

Социальные сети оказывают большое влияние на информационную безопасность современного общества. Пользователи все чаще сталкиваются с атаками социальной инженерии или утечкой личных данных. В связи с этим необходимо осознанное и безопасное использование цифровых сетей, предусматривать все меры предосторожности и рекомендации операторов.

социальные сети, киберпреступник, злоумышленник, информационная безопасность, угрозы, интернет, платформа

Современное общество проходит этап активного развития информационных технологий, в которых социальные сети играю немало важную роль в обмене информации и в взаимодействии людей. В связи с растущей популярностью и влиянием социальных сетей, под их воздействие попадает информационная безопасность общества, компании и даже государства. Такое влияние может быть как чем-то полезным, так и угрозой.

Так, например, в социальных сетях можно прорекламировать свою компанию, найти сотрудников, но также сотрудник этой компании может попасть под атаку социальной инженерии.[1] Киберпреступник способен найти человека по его откры

Текущий документ не содержит источников.атым данным о месте работы, втереться в доверие и обманом заставить выдать личную информацию, учетные данные или отправить ему вредоносные ссылки, переходя на которые загружается вредоносное программное обеспечение.

Социальные сети могут быть полезными в поддержании социальных связей, в маркетинге, в спасательных работах и в поиске общих групп, но угрозами в случае запугивания в интернете, эксплуатации частной информации, изоляции и зависимости от них.

Причиной проблем безопасности в социальных сетях является их масштаб(атаки киберпреступников могут очень быстро распространятся), доверительный характер[1](многие люди слишком доверчиво относятся к неизвестным заявкам в друзья, особенно если есть общие подписчики), невидимость для служб безопасности(наблюдение за огромным количеством людей в социальных сетях довольно затруднительно, поскольку у них ограничены полномочия в этой сфере).

Решением информационной безопасности в социальных сетях для операторов может стать хороший механизм аутентификации (например,

двухфакторная аутентификация позволяет понижать риски захвата учетной записи), настраиваемые параметры безопасности на учетной записи (такие как «закрытый профиль», «публикации только для друзей» и так далее)[2], возможность жалоб на страницы в социальных сетях(тем самым можно помочь службе безопасности защитить не только вас, но и других пользователей), механизмы по обнаружению фишинга, кибергруминга, киберзапугивания, кликджекинга, кибersталкинга, кибершпионажа, поддельных профилей, спама, вредоносного программного обеспечения и тому подобное.

Чтобы не стать жертвой угроз информационной безопасности в социальных сетях, обычным пользователям стоит использовать надежные пароли, ограничить обмен данными о местоположении, быть избирательными к заявкам в друзья, остерегаться ссылок и сторонних приложений, установить программное обеспечение для интернет-безопасности, быть внимательнее к тому, чем они делятся в социальных сетях. [3]

В интернете есть множество разных платформ социальных сетей: платформы профессиональных сетей, платформы обмена мультимедиа, платформы социальных связей, платформы дискуссионных форумов. У каждой из них есть свои уязвимости, меры предосторожности по обеспечению информационной безопасности и киберпреступники. Ученые и исследователи нашли множество методов и решений для защиты пользователей на всех этих платформах социальных сетей, но все еще остаются нерешенные проблемы:

- Социальные сети – самое удобное место, где злоумышленник может соврать о своей личности и нанести удар по жертве, особенно на детей. Нахождение киберпреступников является довольно сложной задачей из-за огромного количества пользователей, системы социальных сетей пока что не являются настолько эффективными, чтобы с этим справляться, но включение искусственного интеллекта в системы чатов может помочь улучшить мониторинг и принятие решений. [4]
- Социальные сети получают прибыль за счет показа рекламы, которая собирает данные о пользователях, что может привести к утечке их личной информации (потому что эти данные выставляют на продажу). Для решения этой проблемы необходимо информировать пользователей о подобном использовании данных, а также принимать правовые меры по защите информации. Ограничения в браузере на стороне клиента также могут повысить уровень безопасности. [5]
- Опросы и игры в социальных сетях пользуются популярностью, но при этом могут собирать учетные данные пользователей, что делает их мишенью для злоумышленников. В этом случае пользователям необходимо проявлять осторожность при вводе персональных.
- Сокращенные URL-адреса на таких платформах, как VK, могут скрывать вредоносные сайты, создавая угрозу безопасности. Для

обнаружения и предупреждения пользователей об опасных сайтах необходимы центральные хранилища фишинговых сайтов и приоритетные решения по анализу URL.

Выше разобрана лишь пара проблем и решений социальных сетей из всех, существующих на сегодняшний день.

Влияние социальных сетей на информационную безопасность необходимо воспринимать серьезно. С активным развития информационных технологий и ростом популярности социальных сетей, она остается актуальной и представляет проблемы, которые необходимо решить. Безопасное использование социальных сетей требует образования, осознанности и сотрудничества между всеми участниками цифровой среды.

Список используемых источников:

1. Хэднеги К. Искусство обмана: Социальная инженерия в мошеннических схемах. М. : Альпина Паблишер, 2020. 430 с.
2. MacKay J. How To Protect Your Personal Information on Social Media [Электронный ресурс]. URL: https://www.aura.com/learn/how-to-protect-your-personal-information-on-social-media (дата обращения: 15.10.2023)
3. Модуль 3. Повышение защищенности при общении в сети интернет [Электронный ресурс]. URL: https://internetpolicy.kg/literacymodule/course_1/module3/glava3_1.html (дата обращения 15.10.2023)
4. Applications of Artificial Intelligence in Social Media (AI) [Электронный ресурс]. URL: https://aihints.com/artificial-intelligence-in-social-media-ai-hints/ (дата обращения: 15.10.2023)
5. Защита персональных данных в процессе использования таргетированной рекламы и прямого маркетинга: национальные и европейские требования [Электронный ресурс]. URL: https://legalitgroup.com/ru/zashchita-personalnykh-dannykh-pri-ispolzovanii-reklami/ (дата обращения: 15.10.2023)

Gudochkina A.

St. Petersburg State University of Industrial Technologies and Design

Influence of social networks on information security.

Social networks have a great impact on information security of modern society. Users are more and more often faced with social engineering attacks or leakage of personal data. In this regard, it is necessary to use digital networks consciously and safely, to provide all precautions and recommendations of operators.

Key words: social networks cybercriminal, malicious, information security, threats, internet, platform.

УДК 004.891.2
ГРНТИ 28.23.35

ПРИНЦИПЫ РАЗРАБОТКИ ЭКСПЕРТНОЙ СИСТЕМЫ ДЛЯ ПОИСКА ПРОБЛЕМ В ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЕ ПРЕДПРИЯТИЯ

С. Ю. Гусенов
Санкт-Петербургский государственный университет промышленных технологий и дизайна

Для осуществления развития бизнеса в разных ИТ сферах, промышленных предприятий, заводов и других рабочих организаций, существуют экспертные системы. Разработка экспертных систем предназначена для формирования мнения о предпочтительности выбора того или иного вида обслуживания ИТ-инфраструктуры для конкретного предприятия. В данной статье рассматриваются этапы разработки и описание экспертной системы для выбора вида обслуживания ИТ-инфраструктуры предприятия. Экспертные системы относятся к числу интеллектуальных информационных систем, предназначенных для массового использования.

экспертная система, ИТ-инфраструктура, структурированные знания, база знаний, модели представления знаний

Практически каждое предприятие, независимо от сферы деятельности и организационно-хозяйственной характеристики, имеет определенную ИТ-инфраструктуру. Ее функционирование играет важную роль в деятельности всей организации, поэтому необходимо поддерживать ее в порядке и вовремя устранять возникающие проблемы.

Таким образом, очень важно правильно выбрать вид обслуживания ИТ-инфраструктуры предприятия. Предметной областью для данной экспертной системы является обслуживание ИТ-инфраструктуры предприятия. При этом необходимо учитывать множество различным критериев и параметров деятельности предприятия. В целях упрощения подобной задачи была разработана экспертная система, которая позволяет учесть все нужные факторы и возможности предприятия, уменьшив временные затраты руководителя и сократив риски при принятии решения.

Экспертные системы – это яркое и быстро прогрессирующее направление в области искусственного интеллекта. Причиной повышенного интереса, является возможность их применения к решению задач из самых различных областей человеческой деятельности. Экспертная система выполняет функции эксперта-человека, который в процессе своей работы оперирует со знаниями, которые хранятся в базе знаний.

Перед тем, как приступить непосредственно к самому процессу создания экспертной системы, необходимо спроектировать общую схему её работы, взаимосвязь модулей, структуру базы данных и знаний с учетом специфики использования экспертной системы на предприятии.

Структура и взаимосвязь модулей экспертной системы (ЭС) приведена на рис. 1.

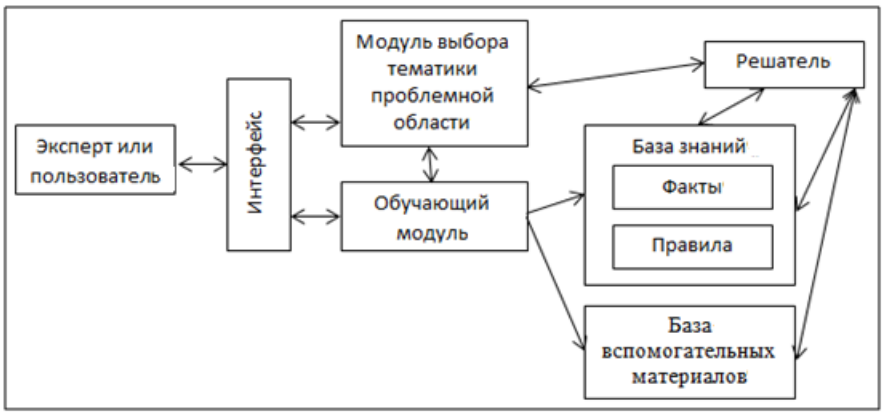


Рис. 1. Взаимосвязь модулей автоматизированной системы поддержки пользователей предприятия

ЭС состоит из следующих модулей:

- интерфейса;
- модуля выбора тематики проблемной ситуации;
- обучающего модуля;
- решателя;
- базы знаний;
- базы вспомогательных материалов.

База знаний состоит из правил анализа информации от пользователя по конкретной проблеме. ЭС анализирует ситуацию и, в зависимости от направленности ЭС, даёт рекомендации по разрешению проблемы.

База вспомогательных материалов содержит файлы подсказок и решений, предлагаемых экспертных систем в процессе работы.

Решатель, использует исходные данные из модуля выбора тематики проблемной ситуации и знания из базы знаний, основываясь на правилах взаимодействия фактов, выбирает решения, которые, будучи примененными к исходным данным, приводят к разрешению проблемной ситуации пользователя.

Обучающий модуль позволяет дополнить фактами базу знаний и текстами базу вспомогательных материалов.

Интерфейс ориентирован на организацию дружелюбного общения со всеми категориями пользователей, реализован в оконном режиме.

Экспертная система использует алгоритм прямого вывода и метод полного поиска в ширину. Выбор алгоритма обусловлен тем, что поиск решения ведется от фактов к гипотезе. Выбор метода обусловлен:

- конечностью базы знаний, что гарантирует поиск решения данным методом;
- возможностью возврата на предыдущий шаг и поиска другого решения, в случае неудачи с предложенным решением.

Разработка программных комплексов экспертных систем в данное время зачастую происходит при помощи искусственного интеллекта, который автоматически рассматривает цель, а также все аспекты создания ЭС.

Процесс разработки промышленной экспертной системы, опираясь на традиционные технологии можно разделить на шесть более или менее независимых этапов (рис. 2), практически не связанных с предметной областью.

Рис. 2. Этапы Разработки ЭС

Для начала работы пользователю необходимо выбрать тематический блок, к которому относится проблемная ситуация.

На примере блока 1 «Microsoft Outlook» (рис. 3) рассмотрим интерфейс ЭС.

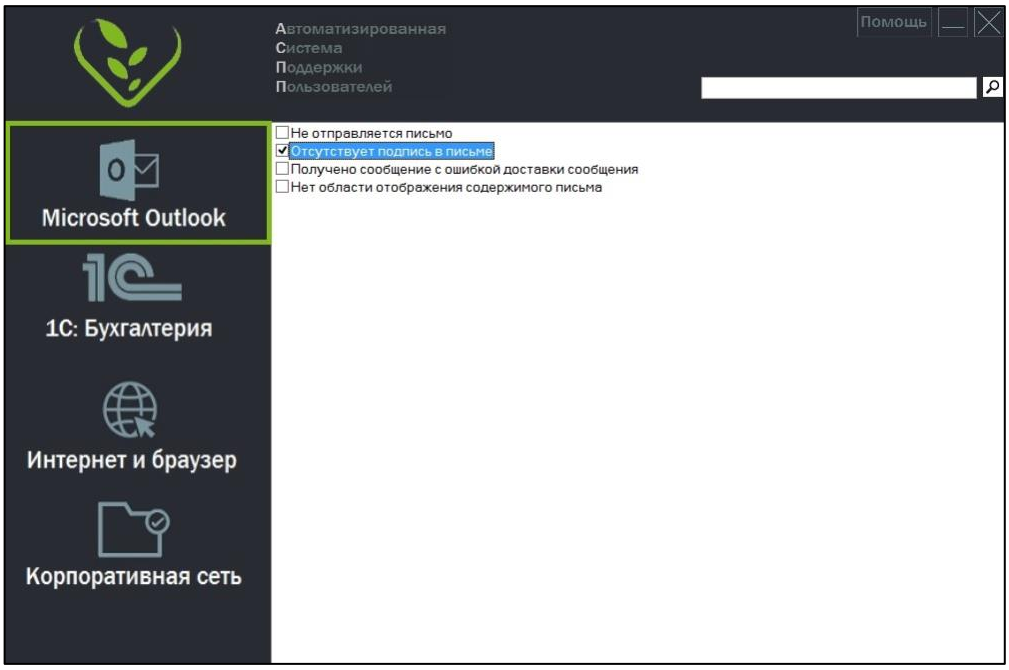


Рис. 3. Внешний вид представления вопросов по разделу Microsoft Outlook

При выборе проблемной ситуации открывается список вопросов, на которые требуется ответить, к каждому вопросу прилагается информационная поддержка, в которой наглядно продемонстрированы описание вопросов применительно к программе (рис. 4).

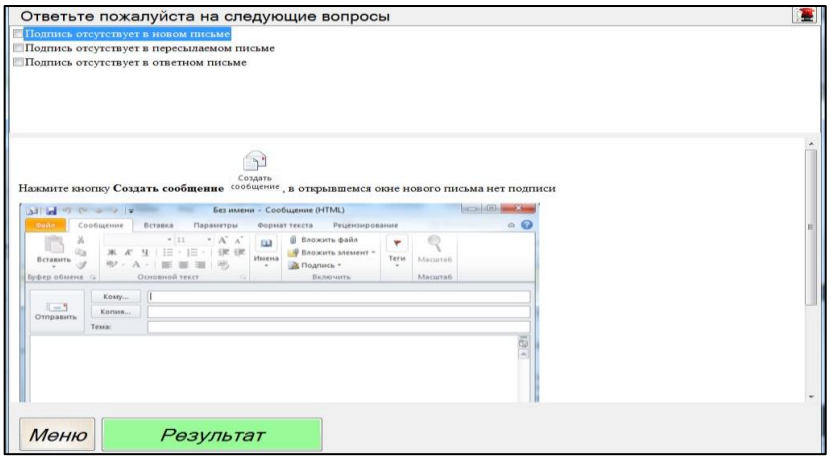


Рис. 4. Список вопросов при выборе проблемной ситуации

После ответов на вопросы и нажатия кнопки «Результат» выводится окно, в котором описано решение данной проблемной ситуации, после чего пользователь отмечает, привело ли данное решение к положительному результату (рис. 5).

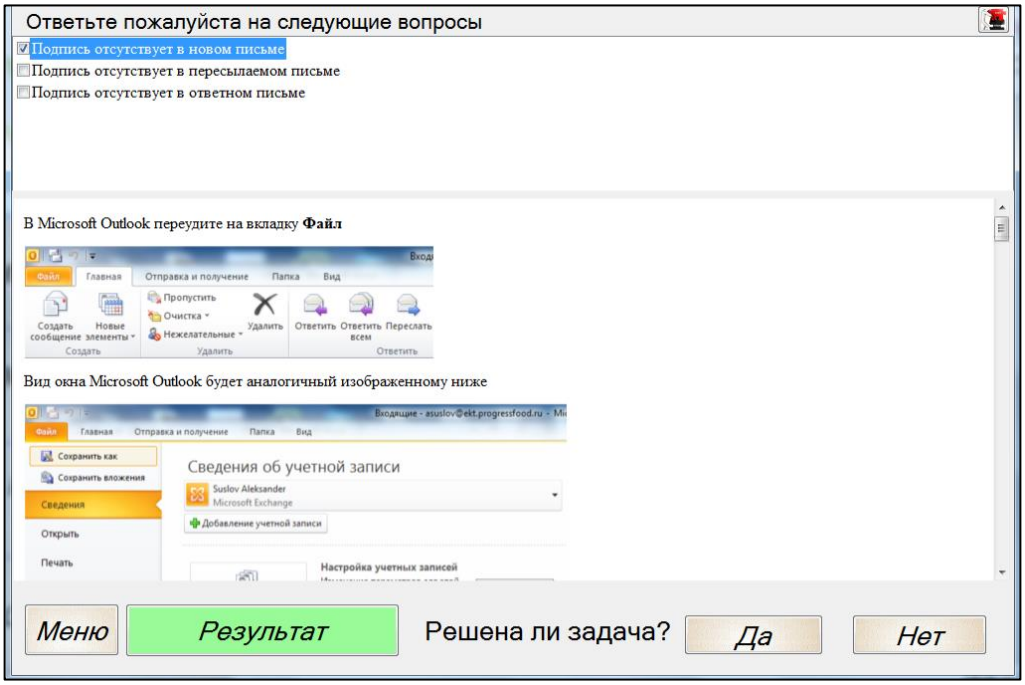


Рис. 5. Внешний вид фрагмента вывода решения

Как мы можем заметить, созданная система может быть использована при принятии решения о выборе вида обслуживания ИТ-инфраструктуры предприятия, однако не во всех случаях она способна привести адекватный ответ на поставленный вопрос. Поэтому область применения созданной системы ограничивается лишь использованием в качестве вспомогательного средства при принятии решения человеком-пользователем. Главными достоинствами экспертной системы являются возможность накапливать знания и подстраивать с минимальными временными затратами под конкретное предприятие. В связи с этим в качестве дальнейшего развития

созданной экспертной системы предполагается расширение базы знаний, уточнение отдельных правил, а также улучшения механизма вывода в целях повышения эргономичности экспертной системы.

Список используемых источников:

1. Багиров Р. ИТ-менеджмент начинается с Service Desk [Электронный ресурс]. URL: http://www.cnews.ru/reviews/in —dex.shtml?2005/06/01/178742 (дата обращения: 06.05.2019).

2. Богданов Д. О. Система обработки заявок современного ИТ-отдела [Электронный ресурс]. Режим доступа: http://elib.sfu-kras.ru/handle /2311/4211 (дата обращения: 06.05.2019).

3. ГОСТ 28397-89-2019. Языки программирования. Термины и определения. М. : Изд-во стандартов, 2018. 27 с.

4. ГОСТ Р7.0.100-2018. Библиографическая ссылка. Общие требования и правила составления. Введ. 04.06.2018. М. : Изд-во стандартов, 2018. 9 с.

5. Демьянов А. В. Автоматизация службы технической поддержки // Молодежный научно-технический вестник. 2014. N 8. С. 14–22.

6. Зубов Ю. С. Информатизация и информационная культура // Проблемы информационной культуры: сборник научных статей. 2014. С. 6–11.

7. Коптелов А. Автоматизация центра технической поддержки пользователей // Мобильные телекоммуникации. 2006. N 9. С.35–39.

8. Лорьер Ж. Л. Системы искусственного интеллекта [Электронный ресурс]. Режим доступа: http://www.padaread.com/?book=15248 (дата обращения: 05.06.2019).

Gusenov S.

Saint Petersburg State University of Industrial Technologies and Design

Principles of develoroblems in the telecommuping an expert system for finding pnications infrastructure of an enterprise.

To implement business development in various IT fields, industrial enterprises, factories and other working organizations, there are expert systems. The development of expert systems is designed to form an opinion on the preference of choosing a particular type of IT infrastructure maintenance for a particular enterprise. This article discusses the stages of development and description of an expert system for choosing the type of maintenance of an enterprise's IT infrastructure. Expert systems are among the intelligent information systems designed for mass use.

Key words: expert system, IT infrastructure, structured knowledge, knowledge base, knowledge representation models.

УДК 004.056.5
ГРНТИ 81.93.29

АНАЛИЗ ЭФФЕКТИВНОСТИ ЭТИЧНОГО ХАКИНГА В ЗАЩИТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С. С. Дмитриев, В. А. Шестакова
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В современном мире информационные технологии играют все более важную роль. Одним из видов методов в защите информации является этичный хакинг. Он имеет ряд преимуществ и недостатков. Важным вопросом для такой методологии – это эффективность. Полезность для специалистов и для организации, которая обращается к этичным хакерам, стоит на первом месте.

хакинг, безопасность, уязвимости, тестирование на проникновение, конфиденциальная информация

Поскольку программы безопасности развиваются, возникает необходимость в соответствующих специалистах. Одними из таких профессионалов являются этичные хакеры или тестировщики на проникновение. Первоначально специалистов этой области называли тех, кто обладал способностью понимать технологии и манипулировать ими. Сейчас хакеры до сих пор способны манипулируют технологиями, но роль и тип хакеров эволюционировали. Хакеры теперь разделены на категории, соответствующие их намерениям: *white, black* и *grey hat*. Начиная с простой манипуляций технологиями это явление вскоре получило возможность воздействовать и на человека, углубляясь в такие схемы атак, как простой фишинг и более широкие методы социальной инженерии [1].

Black hat - это хакеры, работающие на преступные организации, которые используют инструменты эксплуатации недостатков систем безопасности или различные виды мошенничества, связанный с вредоносными ПО или социальной инженерией. *White hat* используют те же методы, что и *black hat*, но для защиты организации от хакерских атак. Их главная задача – поиск недостатков систем безопасности. Осуществление этой цели происходит только при разрешении владельца системы, в этом их главное отличие. *Grey hat* ищут уязвимости в системе без ведома владельца, после чего сообщают об этом. Зачастую это несанкционированные вторжения, которые несут доброжелательный характер. Хакеры не используют уязвимость со злыми намерениями, а указывают на слабости системы. Их мотивы заключаются в том, чтобы прославится или получить соответствующее вознаграждение, а иногда целью является показательное выступление о небезопасности какой-либо системы [2]. Представление сообщества хакеров довольно точно описывает структура *white- black -grey hat,* представленная на рис. 1.

Рис. 1. Структура *white- black -grey hat*

Параллельно росту внедрения информационных систем, увеличилась частота утечек данных. В большинстве случаев утечки происходят из-за взлома с использованием уязвимостей системы. Для защиты необходимо придерживаться многоуровневого подхода. В него входят не только технические уязвимости, но и аспекты, связанные с человеческим фактором. Постоянное увеличение видов уязвимостей провоцирует рост количества средств предотвращения угроз безопасности и средств обнаружения. Обеспечение эффективности кибербезопасности так же важно, как и обеспечение постоянного улучшения системы. Ключевым методом является проведение тестирования на проникновения. Этим занимаются этичные хакеры или *white hat*. Название данной профессии обосновано тем, что этика и доверия – основные принципы специалистов “белого” хакинга. При сотрудничестве с людьми этой профессии организация предоставляет условия для согласованной атаки на систему. Приглашенные хакеры зачастую получают доступ к конфиденциальной информации. Безусловно в таких отношениях важно доверие и соглашение во всех этапах [3].

Этичные хакеры уже стали важной частью арсенала безопасности предприятия. *White hat* все чаще выполняют функции, выходящие за рамки тестирования на проникновение. По мере изменения угроз меняется и список способностей этичных хакеров, включая социальную инженерию, разведку по открытым источникам и использование любых потребительских технологий. Важными качествами для всех этичных хакеров являются терпение, нестандартное мышление и способность анализировать быстро меняющиеся угрозы безопасности [4].

Использование этичных хакеров является хорошей стратегией для укрепления защищенности системы вне поля отдела информационной безопасности, который сформирован в организации. Учитывая объём информации, которая может оказаться под угрозой, недостаточно одного отдела безопасности. При привлечении этичного хакера выявляются слабые места, которые могут быть упущены техническими специалистами организации.

Одним из важных аспектов в оценке эффективности этичного хакинга является то, что специалисты идти в ногу с временем в мире информационной безопасности, изучая архитектуры, устройства, протоколы, операционные системы различных производителей, приложения и программные обеспечения безопасности. Это одно из самых главных и затратных направлений этичного хакинга. Необходимо быть в курсе того, как и какие технологии применяются в различных отраслях промышленности и непрерывно развивающихся стандартах защиты информационной безопасности.

Использование таких методов, где специалисты ведут себя как злоумышленники, стирает грань между этичным и злонамеренным хакингом. Это очередной раз подчеркивает важность профессионализма такого вида деятельности. При доверительных отношениях, обе стороны находятся в выгодном положении, что способствует эффективному проведению процедуры защиты системы в короткие сроки.

Одним из важным факторов эффективности является частота проведения процедуры, что способствует выявлению новых уязвимостей и обеспечивает регулярную защиту систем. В этом аспекте важно отметить, что слишком частое проведение тестирования может повлечь за собой негативные последствия для организации в виде перегрузки системы. Так же во избежание проблем с этичными нормами хакинг должен соответствовать законодательству.

Учитывая отчет о глобальных рисках *WEF* 2019 года, предсталенный на рис. 2, в котором киберпреступность является одной из самых больших угроз для бизнеса, становится очевидным необходимость обращения к специалистам этичного хакинга. Эти угрозы не исчезнут самостоятельно, а будут только увеличиваться в количестве, поэтому, в сегодняшних условиях, соотношение рисков и затрат на тестирование склоняется в пользу использования метода этичного хакинга [5].

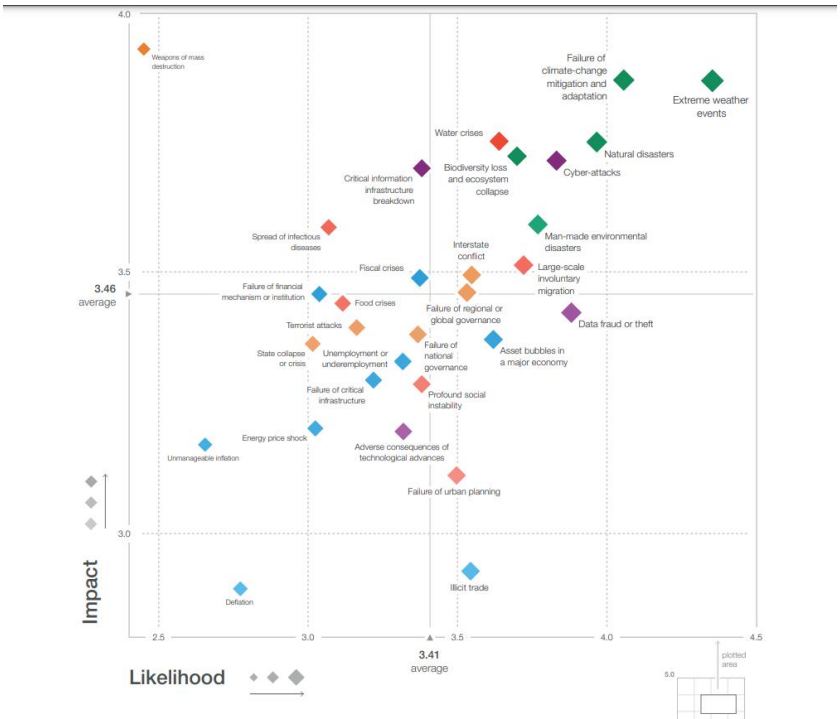


Рис. 2. Ландшафт глобальных рисков 2019 [6]

Тестирование на проникновение может быть недостаточно точным или неполным, что может повлиять на безопасность системы и угрозе появление уязвимостей. Тем не менее такой метод подразумевает рекомендации по улучшению системы и помощь в устранении обнаруженных уязвимостей. Проводятся консультации по защите потенциальных угроз, связанных с человеческим фактором и технической частью работы системы. Таким образом, этичный хакинг является эффективным методом повышения уровня безопасности в определённых условиях.

Список используемых источников:

1. Кто такой этичный хакер? [Электронный ресурс]. URL: https://habr.com/ru/articles/682454/ (дата обращения: 11.10.2023).

2. Хакеры Черные шляпы, Белые шляпы и Серые шляпы – определение и описание [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/definitions/hacker-hat-types (дата обращения: 17.10.2023).

3. Thomas G., Burmeister O., Low G. / Issue of Implied Trust in Ethical Hacking // ORBIT Journal. 2018, C. 1-8.

4. Caldwell T. Ethical hackers: putting on the white hat // Network Security. 2011. N 7. C. 10-13.

5. Nicholson S. How ethical hacking can protect organisations from a greater threat // Computer Fraud & Security. 2019. N 5. C. 15-19.

6. The Global Risks Report 2019: 14th Edition. World Economic Forum. 2019. 5 c.

Dmitriev S., Shestakova V.

Saint-Petersburg State University of Industrial Technologies and Design

Analysis of the effectiveness of ethical hacking in protecting information security.

In the modern world, information technology plays an increasingly important role. One type of information security method is ethical hacking. It has a number of advantages and disadvantages. An important issue for such a methodology is efficiency. Usefulness for professionals and for the organization that turns to ethical hackers comes first.

Key words: hacking, security, vulnerabilities, penetration testing, confidential information.

УДК 004.056.53
ГРНТИ 20.15.05

КОНТРОЛЬ ВНЕШНЕЙ ПОВЕРХНОСТИ АТАКИ: ОБЕСПЕЧЕНИЕ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

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

Контроль и мониторинг внешней поверхности атаки на основе SWOT-анализа и метода экспертной оценки позволит провести стратегическое планирование защиты инфраструктуры организации и устранить потенциальные точки входа злоумышленниками в элементы информационных систем. Для защиты инфраструктуры и ликвидации потенциальных каналов утечки необходим всеобъемлющий анализ теневых активов и полная инвентаризация всех элементов контроля.

внешняя поверхность атаки, ASM, SWOT-анализ, каналы утечки, мониторинг, управление инфраструктурой

Информация стала ценным товаром в современном мировом сообществе. Ценность информации стимулирует активный рост киберпреступлений, связанных с кражей данных. Одной из критически опасных угроз, направленных на кражу данных, являются таргетированные атаки на организации ***APT***-группировками (***advanced persistence threat***). Злоумышленники из ***APT***-объединении в своей организационной структуре содержат первоклассных менеджеров информационной безопасности уровня ***red team***, пентест-специалистов и социальных инженеров [1].

Утечка информации в масштабах организации – это событие нарушения конфиденциальности, целостности и доступности информации, которое произошло по причине непреднамеренного раскрытия критической служебной информации. Раскрытие данной информации может нанести разрушительный ущерб репутации компании, снизить лояльность и доверие клиентов, а также привести к штрафным санкциям со стороны нормативных регуляторов.

По данным Роскомнадзора, в РФ за 2023 год была зафиксирована компрометация более 200 млн записей о субъектах персональных данных, порядка 70 случаев утечек подтверждено. Согласно исследованию ГК “***InfoWatch***”, масштаб утечек в финансовой сфере вырос в 1,7 раз [3].

Злоумышленники заинтересованы базами данных, содержащими строки данных с клиентами компании, поскольку лояльность клиентов – это условие для шантажа бизнес-владельцев [1].

В настоящее время в общем доступе растет объем данных, которые публикуются без согласия владельцев, вследствие взлома баз данных или раскрытия сведений из-за уязвимости систем безопасности.

В рамках перспективного диссертационного исследования предполагается провести анализ вариантов проведения менеджмент-контроля внешней поверхности атаки, и, с опорой на фундаментальное исследование инструментов киберразведки по открытым источникам [2], подготовить стратегию плана мониторинга и превентивной защиты активов организации от атак.

Внешняя поверхность атаки

Attack Surface Management, или ASM (*пер*. внешняя поверхность атаки) – это концептуальная система менеджмента общего количества потенциальных угроз безопасности в пространственном контуре организации для оценки общего состояния безопасности инфраструктуры. Также ASM – это совокупность потенциальных слабостей и средств контроля, присутствующих во всех аппаратных, программных и сетевых компонентах, а также структурный подход, предполагающий идентификацию, определение приоритетов и минимизацию потенциальных векторов угроз в среде организации с точки зрения внешнего злоумышленника [4].

Управление внешней поверхности атаки предлагается планировать на основании переосмысленного концепта Центра интернет-безопасности (CIS) в ходе приоритизации мониторинга элементов управления инфраструктурой:

1. Инвентаризация активов предприятия:
1.1. Активы, подключенные к инфраструктуре физически, виртуально, удаленно и в облачных средах;
1.2. Анализ полного перечня активов, а также «теневые» активы;
1.3. Анализ программного обеспечения (далее – ПО) в сети;
1.4. Поддержание параметров конфигурации и мер безопасности;
1.5. Управление сетевой инфраструктурой, включая мониторинг сети.
1.6. Безопасность прикладного ПО.
2. Защита данных:
2.1. Установка средств контроля для идентификации данных;
2.2. Управление учетными записями и ролями доступа.
2.3. Управление журналами аудита;
2.4. Защита электронной почты и веб-браузера;
2.5. Резервное копирование данных.
3. Непрерывное управление уязвимостями:
3.1. Комплексный план для оценки и мониторинга уязвимостей;
3.2. Мониторинг государственных и частных отраслевых источников на предмет получения актуальной информации об угрозах и уязвимостях;
3.3. Антивирусное сканирование устройств.
4. Превентивный и оперативный контроль инцидентов:
4.1. Обучение персонала организации правилам ИБ;
4.2. Контроль поставщиков услуг;

4.3. Управление реагированием на инциденты ИБ, включая фазы обнаружения и митигации угрозы;

4.4. Регулярное тестирование на проникновение.

Каналы проникновения в инфраструктуру организации

Для проведения мониторинга поверхности атаки требуется инвентаризация потенциальных точек входа для доступа к инфраструктуре и оценка стоимости реализации обнаруженных векторов. Согласно проведенному исследованию в работе [3], каналы для проникновения в инфраструктуру организации предлагается классифицировать следующим образом:

- Облачные ресурсы:
  - облачные серверы;
  - приложения ***Software-as-a-Service (SaaS);***
  - облачные хранилища;
- Локальные ресурсы (аппаратное, программное обеспечение в периметре инфраструктуры организации и информационные потоки):
  - Датчики интернета вещей (***IoT***);
  - Искусственный интеллект;
  - Веб-сайты;
  - Поддомены;
  - Приложения;
  - ***IP***-адреса, ***DNS***-сервера;
  - Профили организации в социальных сетях;
- Сотрудники организации:
  - Мобильные устройства, используемые сотрудниками;
  - Учетные записи сотрудников в различных сервисах;
  - Таргетированная фишинг-атака на хост сотрудника;
- Теневые активы (любые активы, которые не подконтрольны системе защиты информации, но входят в инфраструктуру организации);
- Партнеры и поставщики (активы и услуги, которые приобретаются в пользование у сторонней организации).

В процессе выявления уязвимостей исследование поддоменов может отобразить конфиденциальную информацию, а серверные версии ПО могут содержать известные уязвимости, например, зарегистрированные в базах БДУ ФСТЭК.

SWOT-анализ и экспертиза потенциально уязвимых компонентов

Одним из способов стратегического планирования защиты внешней поверхности атаки является структурный ***SWOT*-анализ**. ***SWOT*** – это набор аббревиатур ***Strengths*** (*пер.* сильные стороны), ***Weaknesses*** (*пер.* слабые стороны), ***Opportunities*** (*пер.* возможности), ***Threats*** (*пер.* угрозы). Визуализация концепции представлена на рис. 1. Данный подход планирования позволяет оценить конкурентное позиционирование организации и выявить возможности и угрозы в области безопасности. SWOT-анализ отражает внешние и внутренние проблемы инфраструктуры,

сведения об активах безопасности, рисках, проблемах и вызовах, с которыми столкнется отдел информационной безопасности и бизнес в целом [1].

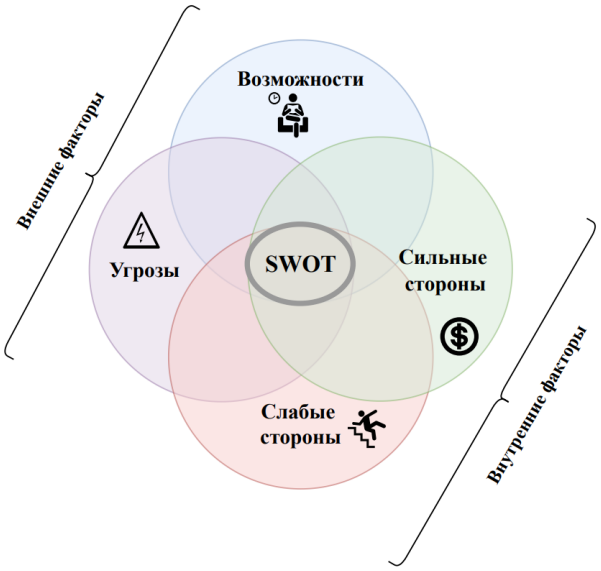


Рис. 1. Схема *SWOT*-анализа

Подробнее об элементах ***SWOT***-анализа [1]:

•Сильные стороны – это жизненный цикл системы менеджмента информационной безопасности организации, демонстрирующие устранение уязвимых точек входа в инфраструктуру.

•Слабые стороны – это способ анализа дистанции между реализацией подходов к защите поверхности атаки и желаемого результата.

•Угрозы – это наглядное отражение несоответствий между политикой безопасности, а также практически внедренными средствами защиты и менеджментом управления внешней поверхности атаки.

•Возможности (*внешняя среда*) – это перспективы совершенствования нормативного регулирования, грамотной инвентаризации активов и проведение обучения сотрудников.

Недостатком данного метода [1, 3] является его субъективность, поскольку существует перекос в сторону субъективной позиции аналитика, осуществляющего анализ защищенности поверхности атаки. Для компенсации предлагается комбинация с методом экспертного оценивания.

Метод экспертных оценок – это метод анализа архитектуры поверхности атаки, включающий комплексный анализ экспертами-аналитиками и обработки мнений экспертов, заключенных в количественно-качественной форме, с целью подготовки вердикта для принятия решений ответственными лицами.

В дальнейших работах планируется проработка экспертной реализации SWOT-аналитики и экспертной аналитики.

Заключение

Стремительный рост киберпреступности в РФ и высокая латентность преступлений в сфере компьютерных технологий, согласно исследованию, связаны с низким уровнем отклика об инцидентах среди пострадавших коммерческих организаций и трансграничностью совершенных действий [2].

В настоящее время безопасность инфраструктуры в масштабах организации во многом зависит от доступности ее сетевых активов. Отсутствие полного контроля за элементами инфраструктуры приводит к эксплуатации плохо защищенных или «забытых» активов злоумышленниками и серьезным репутационным и финансовым потерям. Больше половины атак на инфраструктуру совершаются через внешний периметр.

Благодаря качественному менеджменту внешней поверхности атаки организации получат периметральный контроль над элементами инфраструктуры и источниками данных об организации, в том числе и контроль за репутацией бренда в сети.

Список используемых источников:

1. Jarmul K. Practical Data Privacy: Enhancing Privacy and Security in Data. 2023. First Edition. United States of America : O'REILLY, 2023. 315 с.

2. Исследование инструментов кибер разведки по открытым источникам для оценки доступности информационных активов организации: вып. квалиф. раб. на соискание степ. бкл. по спец. 10.03.01 / И. Н. Дмитриева; научный руководитель А. А. Миняев; Санкт-Петербургский гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича, Кафедра ЗСС. 2023. 105 с. URL: http://lib.sut.ru/jirbis2_spbgut

3. Бацупа, А. П., Кураленко, А. И. Моделирование информационной безопасности методом стратегического планирования и экспертных оценок / А. П. Бацупа, А. И. Кураленко // Безопасность информационных технологий. Т. 21, N 3 (2014) URL: https://www.semanticscholar.org/paper/Моделирование-информационной-безопасности

4. Adarsh Nair, Greeshma M. R Mastering Information Security Compliance Management [Текст] / Adarsh Nair, Greeshma M. R — April 2023: First Edition. — Birmingham: Packt, August 2023. 193 с.

5. Саенко Н. Повышение культуры приватности в организации / Саенко Н. // Журнал DPO о персональных данных и приватности — SBER PRIVACY JOURNAL, Выпуск N 6, сентябрь 2023. С. 31-36. URL: https://www.sberbank.ru/ru/person/kibrary/personal_data

Dmitrieva I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Control of the Attack Surface Management: ensuring the protection of confidential information in the organization.

Control and monitoring of the external attack surface based on SWOT analysis and the expert assessment method will allow strategic planning of the organization's infrastructure protection and eliminate potential entry points by intruders into elements of information systems. To protect the infrastructure and eliminate potential leakage channels, a comprehensive analysis of shadow assets and a complete inventory of all control elements are necessary.

Key words: Attack Surface Management, ASM, SWOT-analyze, channels of information leakage, monitoring, infrastructure management.

УДК 62-52
ГРНТИ 50.47.29

ВЫБОР РЕГУЛЯТОРА ДЛЯ БЕЗОПАСНОГО УПРАВЛЕНИЯ КОНВЕЙЕРОМ

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

С увеличением автоматизации и использования конвейерных систем в различных отраслях становится критически важным выбор подходящего регулятора, который обеспечит безопасную и эффективную работу. В данной статье было произведен расчет конвейера, по результатам которого составлена математическая модель. Также был добавлен и настроен регулятор для безопасного управления.

математическое моделирование, безопасное управление, регулятор, перерегулирование, PID Tuner

Математическая модель (технологической или управленческой) операции – это система математических и логических правил, позволяющих с достаточной полнотой и точностью описывать наиболее существенные процессы, присущие операции, прогнозировать возможный ход и исход её по определенным исходным данным и оценивать эффективность вариантов решений и планов [1].

Компьютерное моделирование объекта обеспечивает точность исследования и быстроту получения результатов. Также использование модели позволяет минимизировать материальные затраты на проведения работ.

Модель нужна для того, чтобы понять, как устроен конкретный исследуемый объект, каковы его структура, внутренние связи, основные свойства, законы развития, саморазвития и взаимодействия с окружающей средой [2].

С помощью моделирования технологического процесса можно управлять объектом по оптимальным воздействиям с конкретно поставленными целями. Моделирование позволяет учитывать множество различных факторов, влияющих на ход технологического процесса.

Довольно часто построение модели, позволяющей получить практически значимые результаты, требует комплексного использования различных методов моделирования.

Обязательным этапом моделирования является оценка адекватности модели – соответствие сконструированного формального описания реальному объекту и сформулированным предположениям с учётом целей исследования [3]. Модель изучается всеми доступными методами в интересах достижения поставленной цели.

В качестве исследуемого конвейера был выбран реально существующий ленточный питатель-конвейер:

Q = 1800 об/с – двигатель;
L = 60 см – длина конвейера;
V = 5 см/с – скорость движения ленты [4].

Передаточная функция конвейера является передаточной функцией апериодического звена:

$$W(p) = \frac{Y(p)}{X(p)} = \frac{К_П}{T \cdot p + 1} \quad (1)$$

Где $К_п$ – коэффициент усиления конвейера; T – постоянная времени конвейера, характеризующая инерционность звена, с.

Принимая, что при увеличении скорости движения ленты от 0 до 5 см/с, его производительность также изменяется от 0 до 1800 об/с, то коэффициент усиления конвейера:

$$K_П = \frac{\Delta Q}{\Delta V} = \frac{1800}{5} = 360 \quad (2)$$

где ΔQ – изменение производительности, т/с, ΔV – изменение скорости движения ленты, м/с.

Для нахождения постоянной времени достаточно оценить влияние скорости движения и длины конвейера на переходную характеристику апериодического звена:

$$T = \frac{L}{V} = \frac{60}{5} = 12с \quad (3)$$

Таким образом, передаточная функция конвейера примет вид:

$$W(p) = \frac{360}{12 \cdot p + 1} \quad (4)$$

Однако, на производительность конвейера также влияет и время разгона электродвигателя, приводящего в движение приводной вал конвейера. Это время зависит от настроек частотного преобразователя и составляет, в среднем, 10 секунд, потому передаточное звено последовательно подключенного двигателя можно описать так:

$$W(p) = \frac{1}{10 \cdot p + 1}$$

Моделирование объекта управления (ОУ) выполнено в среде графического анализа динамических систем Simulink. Структурная схема САУ ленточным конвейером в этой программе приведена на рис. 1.

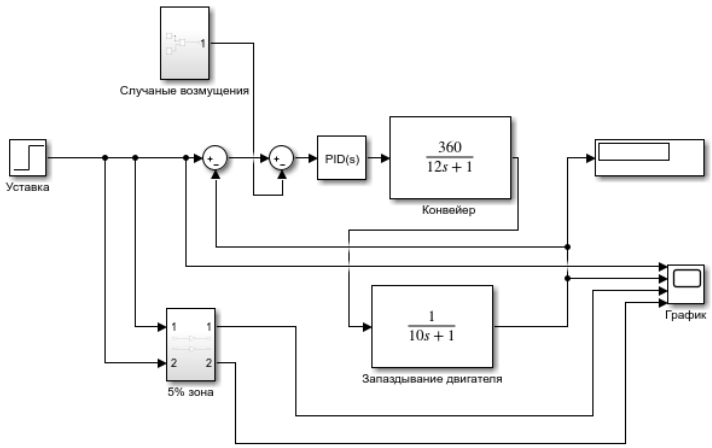


Рис. 1. Структурная схема САУ ленточным конвейером

Передаточная функция (4) объекта является комбинацией апериодического звена 1-го порядка и звена запаздывания. В блоке регулятора выбран тип ПИД, а значения коэффициентов установлены так, чтобы не оказывать влияние на переходную характеристику: П=1, И=0, Д=0.

На рис. 2 представлена переходная характеристика нескорректированной системы регулирования по задающему воздействию.

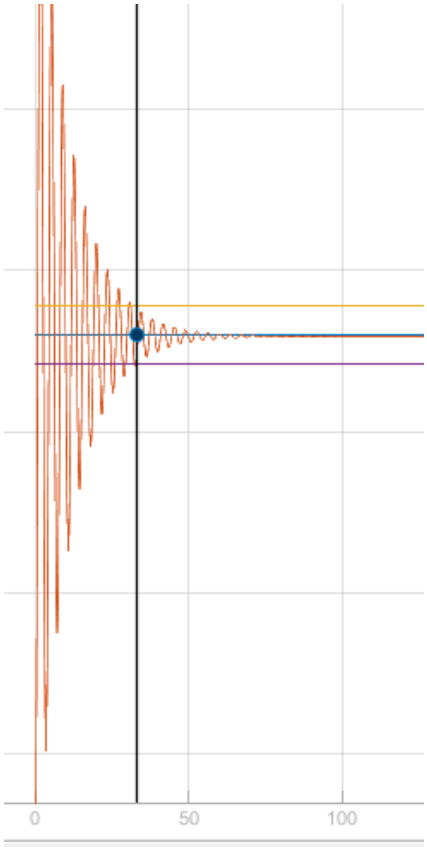


Рис. 2. Данные переходной характеристики

Регулируемая величина – производительность ленточного конвейера. По графику и значениям, снятым в определенные моменты времени, видно, что значение переходной функции вошло в 5%-ю зону через 33с и зафиксировалось на значении 1795, заметно приближаясь к заданным 1800 об/с.

Расчёт значения статической ошибки в установившемся режиме осуществлён по формуле (5).

$$e_{\text{уст}} = SP - PV = 1800 - 1795 = 5 \text{ об/с}, \quad (5)$$

где SP – задающее значение (от англ. set point); PV – значение регулируемого параметра (от англ. process value). Отсюда возникает необходимость использования регулятора.

Настройка ПИД-регулятора осуществлена с помощью программного модуля PID Tuner [5]. Данный инструмент позволяет автоматически сконфигурировать параметры регулятора объекта управления из модели Simulink. Окно PID Tuner продемонстрировано на рис. 3.

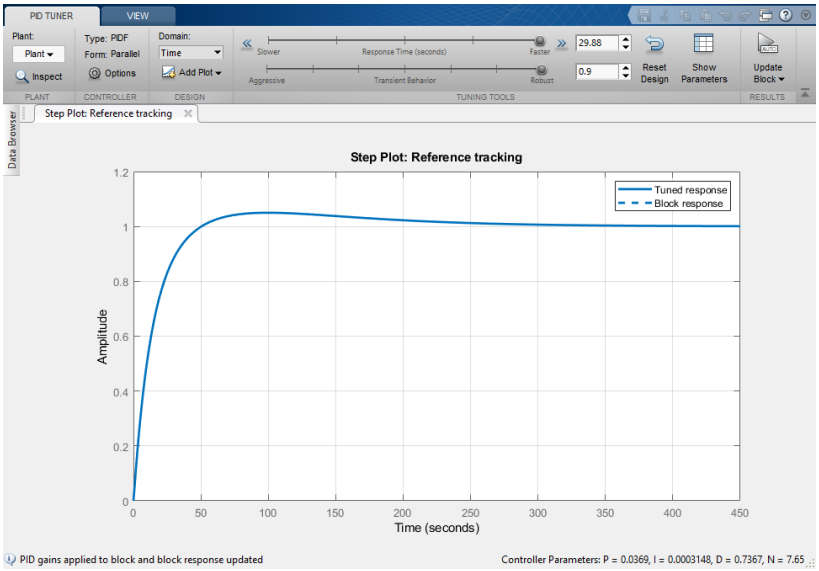


Рис. 3. Программное окно инструмента PID Tuner

Оптимальные параметры, полученные с помощью PID Tuner, позволяющие обеспечить минимальное время выхода на уставку и не превышающее 5% от задающего значения, представлены на рис. 4.

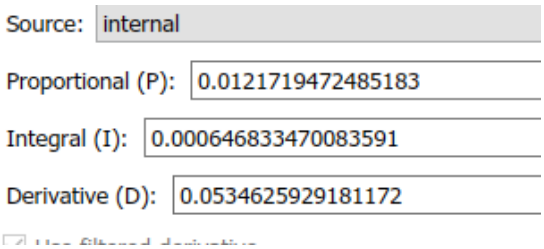


Рис. 4. Расчетные параметры ПИД-регулятора

На рис. 5 смоделирована кривая разгона ленточного конвейера с управлением по заданию и настроенным ПИД-регулятором.

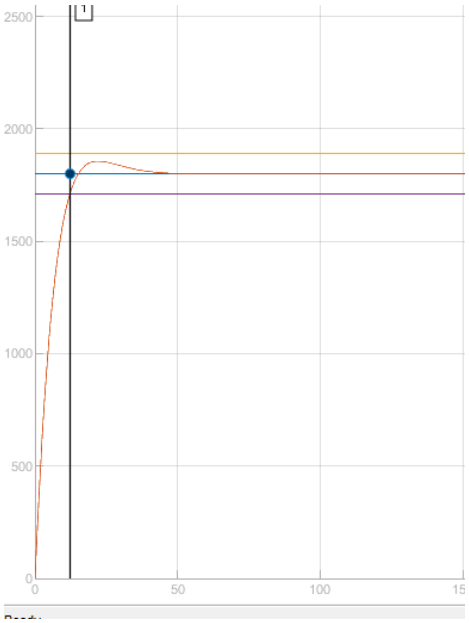


Рис. 5. Характеристика ОУ с регулированием по заданию с ПИД-регулятором

Как видно по графику, время входа в 5%-зону составило 12 секунд.

$$e_{\text{уст}} = SP - PV = |1800 - 1800| = 0 \quad (6)$$

$$\sigma = \frac{y_{\text{макс}} - y_{\text{уст}}}{y_{\text{уст}}} \cdot 100\% = \frac{1856 - 1800}{1800} \cdot 100\% = 3\% \quad (7)$$

Таким образом, полученная система автоматического регулирования конвейера обеспечивает поддержание выходного параметра на требуемом уровне.

Список используемых источников:

1. Абакумова И. В. Моделирование и оптимизация технологических процессов. Благовещенск : 2012. 114 с.

2. Штерензон В. А. Моделирование технологических процессов. Екатеринбург : Рос. гос. проф.-пед.ун-та, 2010. 66 с.

3. Мальков М. В., Олейник А. Г., Федоров А. М. Моделирование технологических процессов: методы и опыт // Труды Кольского научного центра РАН. 2010. N 1. С. 93 – 101.

4. Ленточный конвейер 460 мм или 600 мм [Электронный ресурс]. URL: https://aliexpress.ru/item/1005005139741934.html?sku_id=12000035582477216 (дата обращения: 30.10.2023).

5. Настройка ПИД-регуляторов [Электронный ресурс]. URL: https://habr.com/ru/companies/etmc_exponenta/articles/512012/ (дата обращения: 30.10.2023).

Dogadaev A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Selection of a regulator for the safety of conveyor control.

With the increasing automation and use of conveyor systems in various industries, it becomes critically important to choose a suitable regulator that will ensure safe and efficient operation. In this article, the pipeline was calculated, according to the results of which a mathematical model was compiled. A controller has also been added and configured for safe operation.

Key words: mathematical modeling, safe control, regulator, overshoot, PID Tuner.

УДК 004.056.53
ГРНТИ 81.93.29

ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ КИБЕРИММУННОГО ПОДХОДА ДЛЯ ЗАЩИТЫ ОПЕРАЦИОННЫХ СИСТЕМ

Р. М. Домбровский, Э. О. Филипов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В наше время банки данных угроз безопасности информации постоянно пополняются новыми уязвимостями для актуальных дистрибутивов операционных систем. В связи с этим классические методы защиты операционных систем могут не справляться со своевременным обнаружением и устранением потенциальных угроз. Для решения подобной задачи существует перспективный кибериммунный подход для защиты операционных систем.

кибериммунитет, кибербезопасность, операционные системы

С момента создания первого компьютера и на протяжении всего последующего времени в информационных технологиях существует проблема обеспечения кибербезопасности. Каждое цифровое устройство в нашем мире имеет свою операционную систему и в связи с этим защита операционных систем является одним из приоритетных направлений в кибербезопасности. Операционные системы очень сложны по своему устройству и в силу этой сложности даже в самых защищенных системах периодически находят уязвимости.

Для того чтобы выявить преимущества и перспективы кибериммунного подхода перед современными операционными системами, необходимо для начала рассмотреть имеющиеся операционные системы с точки зрения кибербезопасности. Сразу стоит отметить, что невозможно назвать систему доверенной если ее исходный код закрыт, ведь это сильно сужает возможности для тестирования и изучения операционной системы на устойчивость перед атаками, а также поиска уязвимостей. В связи с этим можно сразу сказать, что защищенность проприетарных систем, таких как Windows и IOS, основывается отчасти на доверии к производителю, а не на самой системе.

Если говорить о системах с открытым исходным кодом, в частности о UNIX-системах, ОС семейства Linux продолжают поддерживать целый ряд устаревших защитных механизмов и концептов. Многие администраторы считают, что для превращения Linux в высокозащищённую ОС достаточно установить пакет SELinux. Этот инструмент широко применяется для реализации замкнутой программной среды, однако использование SELinux для построения более сложных моделей управления доступом требует существенных усилий по разработке соответствующих политик, потому что отсутствуют какие-либо протестированные конфигурации и нет проверенных рекомендаций, что существенно затрудняет настройку [1].

Было предпринято множество попыток создать на базе Linux защищённую операционную систему, как за рубежом, так и на территории Российской Федерации. Наиболее успешными попытками можно считать следующие системы:

- ОС Альт был разработан на основе ALT Linux, которая имела несколько особенностей, например, раздельное хранение аутентификационных данных пользователей, однако все эти особенности не привносят существенного повышения безопасности операционной системы. Некоторые дистрибутивы на основе ОС Альт, которые реализуют мандатное управление с помощью SELinux, принято считать одним из лучших примеров реализации данного инструмента среди всех известных операционных систем. Несмотря на успех, эта система имеет ряд потенциальных уязвимостей в мандатной подсистеме управления доступом [1].
- Мобильная система Вооружённых Сил (МСВС), разработанная на основе ОС Red Hat Enterprise какое-то время считалась самой защищённой российской ОС, однако, из-за устаревшего ядра Linux, установка нового программного обеспечения была серьёзно затруднена [1].
- Операционная система специального назначения AstraLinux Смоленск - была разработана таким образом, что не требует дополнительных средств защиты информации. Высокая степень защиты операционной системы позволяют использовать её в государственных информационных системах, связанных с персональными данными, в вычислительных комплексах, в системах, работающих с государственными тайнами, в защищенных комплексах виртуализации, в компонентах критической информационной инфраструктуры. В “Смоленске” реализован механизм мандатного разграничения доступа. Данный механизм традиционно используется в СЗИ, где нужна обработка высоких уровней конфиденциальности. Данная система полностью покрывает потребности для использования на территории Российской Федерации, разработчики данной операционной системы даже запустили программу по поиску уязвимостей в защите ОС [2]. Однако AstraLinux по-прежнему является дистрибутивом Linux и нет гарантий того, что уязвимости, которые компрометируют систему, не будут обнаружены в будущем, и нам остается лишь довериться производителю.

Исходя из всего вышесказанного можно сделать вывод, что, несмотря на очевидные недостатки безопасности операционных систем семейства Linux, разработчикам удалось приблизиться к созданию устойчивой защищенной операционной системы. Тем не менее остается вероятность того, что при написании системы были допущены ошибки в силу человеческого фактора, которые в последствии могут стать проблемой. Именно поэтому предлагается вместо наращивания новых средств защиты информации на морально устаревшее ядро Linux, разработать защищённую систему, заложив устойчивость к угрозам в основу создания системы, сделав её невосприимчивой к большинству атак.

Реалии современного подхода к защите устройств в информационной безопасности таковы, что в большинстве случаев только после появления новой атаки или уязвимости разрабатываются новые решения по их устранению. В условиях бизнеса, когда в некоторых предприятиях реализуется целая инфраструктура на основе разного рода устройств, которых может быть большое количество, вышеописанный подход может быть неэффективен, потому что каждая новая атака может быть критичной для предприятия, и в связи с этим предлагается подойти к вопросу с другой стороны и создать операционную систему, опираясь на кибериммунный подход, который позволит нам, как и было сказано ранее, сделать устойчивую систему, заложив принципы безопасности в ее архитектуру [3].

Для создания кибериммунной системы в рамках данной статьи рассматриваются следующие принципы:

•Минимизация доверенной вычислительной базы. Современные популярные операционные системы изначально проектировались с упором на функциональность и удобство разработки, поэтому они создавались на монолитном ядре и содержали в себе миллионы строк кода, количество которых с каждой новой версией только растёт. Сравнение количества строк кода ядер представлен на рис. 1. Тем самым появляется проблема в контроле корректности такого объёма кода, что может привести к появлению новых уязвимостей. В связи с этим необходимо минимизировать поверхность атаки путём разработки системы на базе микроядра, которое будет содержать только критичные для работы механизмы [3].

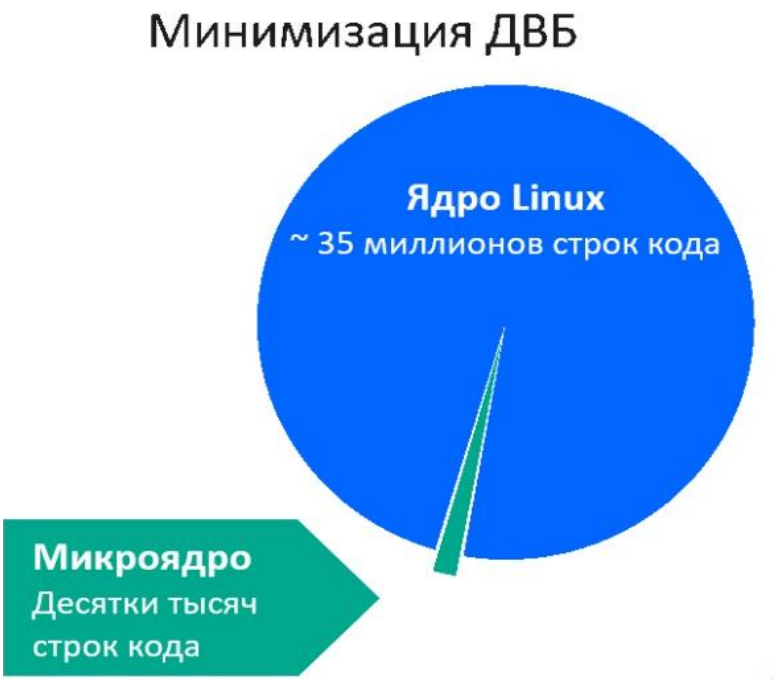


Рис. 16. Сравнение ядер

•Изоляция компонентов друг от друга. Кибериммунная система разделяется на домены безопасности в соответствии с уровнем доверия к коду, и все компоненты изолируются друг от друга с помощью этих доменов, как представлено на рисунке 2, что не позволит злоумышленнику получить доступ ко всей системе при взломе одного компонента. Благодаря этому можно использовать стороннее программное обеспечение, не опасаясь за безопасность системы. Кроме того, уменьшаются трудозатраты, необходимые для создания безопасной системы за счёт использования

сторонних разработок [3].

Рис. 17. Изоляция компонентов

•Контроль всех взаимодействий. Операционная система не сможет функционировать, если все компоненты будут изолированы друг от друга, в связи с этим необходимо контролировать все взаимодействия. Эту функцию выполняет специальный монитор безопасности. На этот модуль поступает запрос на взаимодействие, после чего принимается решение о дальнейших действиях в соответствии с политиками безопасности. Использование данного модуля позволяет исключить риск эксплуатации большого количества угроз, за счёт того, что не доверенные и не прописанные в политиках безопасности взаимодействия не будут реализованы [3].

Реализация данных принципов позволит обеспечить устойчивость операционной системы перед большинством классов атак, обеспечить прогнозируемость работы информационных систем, минимизировать риски инцидентов и связанных с ними аварий. С точки зрения бизнеса, данное решение существенно снижает стоимость разработки и поддержки безопасных IT – решений, так как даже при использовании стороннего недоверенного кода, кибериммунный подход позволяет поддерживать высокий уровень защищённости и гибкость системы, создавая политики безопасности для каждой задачи.

Примером реализации данного перспективного кибериммунного подхода является операционная система KasperskyOS, созданная специалистами компании Kaspersky. Данная система построена на базе микроядра, которое было написано с нуля разработчиками компании. Именно это ядро позволяет нам реализовать первый принцип в системе. Остальные два принципа реализуются за счёт подсистемы Kaspersky Security System, через которую проходят все межпроцессные коммуникации. Данная система работает на основе комбинации множества моделей для построения политики, которая наиболее точно соответствует поставленным целям безопасности. Разработчику не придётся писать код, реализующий политику безопасности, так как он генерируется автоматически [4].

Таким образом, несмотря на то, что предотвратить все атаки невозможно, однако вполне реально создать систему, которая будет продолжать стабильно работать в условиях атаки. Число угроз и их масштаб, а также технические возможности киберпреступников возрастают, и на это есть несколько путей решения. Можно закрывать эти угрозы, наращивая наложенную защиту (например, антивирусы). Однако не на все устройства можно установить антивирусы и другие дополнительные средства защиты. Использование кибериммунного подхода позволяет изначально разработать киберзащищённую архитектуру, минимизируя потенциальные убытки.

Список используемых источников:

1. Буренин П. В, Девянин П. Н., Лебеденко Е. В. и пр. Безопасность операционной системы специального назначения Astra Linux Special Edition : учеб. пособие для вузов. М. : Горячая линия - Телеком, 2020. 404 с.
2. Девянин П. Н., Тележников В. Ю., Третьяков С. В. Основы безопасности операционной системы Astra Linux Special Edition. М. : Горячая линия - Телеком, 2023. 147 с.
3. Как создать кибериммунную систему? [Электронный ресурс] // blog.kaspersky.kz URL: https://blog.kaspersky.kz/how-to-create-cyberimmune-system/25610/ (дата обращения: 20.10.2023)
4. Kaspersky Security System [Электронный ресурс] // os.kaspersky.ru URL: https://os.kaspersky.ru/technologies/kaspersky-security-system/ (дата обращения: 20.10.2023)

Dombrovsky R., Filipov E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Prospects for the introduction of a cyberimmune approach to protect operating systems. Currently, data banks on information security threats are constantly replenished with new vulnerabilities for current operating system distributions. In this regard, classical methods of protecting operating systems may not be able to cope with the timely detection and elimination of potential threats. To solve such a problem, there is a promising cyberimmune approach to protecting operating systems.

Key words: Cyberimmunity, cybersecurity, operating system

УДК 004.046
ГРНТИ 49.43.01

МЕТОДИКА ВЫБОРА ДОПУСТИМЫХ ЗНАЧЕНИЙ RSSI ДЛЯ СИСТЕМЫ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ Wi-Fi КЛИЕНТА МЕТОДОМ FINGERPRINTING

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

Одними из наиболее популярных систем определения местоположения беспроводных клиентов в сетях семейства IEEE 802.11 являются системы, базирующиеся на методах трилатерации и использующие метрику RSSI. В частности, метод fingerprinting предполагает применение карты радиоотпечатков – набора заранее рассчитанных метрик RSSI. В данной статье рассматривается подход к сравнению заранее рассчитанных метрик с метриками, полученными от искомого беспроводного клиента.

Wi-Fi, трилатерация, fingerprinting, IEEE 802.11, точность, location, RSSI

Система определения местоположения методом fingerprinting является одной из самых точных среди систем, использующих метрику RSSI (Received Signal Strength Indication). Главной особенностью данного метода является возможность достаточно точного учёта препятствии на пути сигнала от передатчика до приёмника. Это реализуется с помощью предварительного расчёта радиоотпечатков (метрик RSSI) по следующим формулам [1-4]:

$$RSSI = PwTr - Cbl_LTr + Ant_GTr - FSPL - Obs_Atten + Ant_GRs - Cbl_LRs, \quad (1)$$

где *RSSI* – индикатор уровня принимаемого сигнала, дБм; *PwTr* – мощность излучения передатчика, дБм; *Cbl_LTr* и *Cbl_LRs* – потери в кабелях передатчика/приёмника, дБ; *Ant_GTr* и *Ant_GRs* – усиление антенны передатчика/приёмника, дБи; *FSPL* – Free Space Path Loss (затухание сигнала в свободном пространстве), дБ; *Obs_Atten* – коэффициент затухания сигнала от преград [5], дБ.

$$FSPL = 20 \times \lg(f) + 10 \times D \times \lg(d) + p - 24, \quad (2)$$

где f – рабочая частота, МГц; D – коэффициент затухания; d – дистанция между приёмником и передатчиком, м; p – коэффициент проницаемости. Значение параметра D в формуле (2) зависит от среды передачи сигнала [6], обычно приравнивается к 2 и 2,5 для частот 2,4 и 5 ГГц соответственно; коэффициент p для воздушной среды равен 1.

Затухание сигнала в свободном пространстве (FSPL) является существенным фактором, влияющим на точность определения местоположения беспроводных клиентов. График зависимости FSPL от

частоты и дальности передачи представлен на рис. 1.

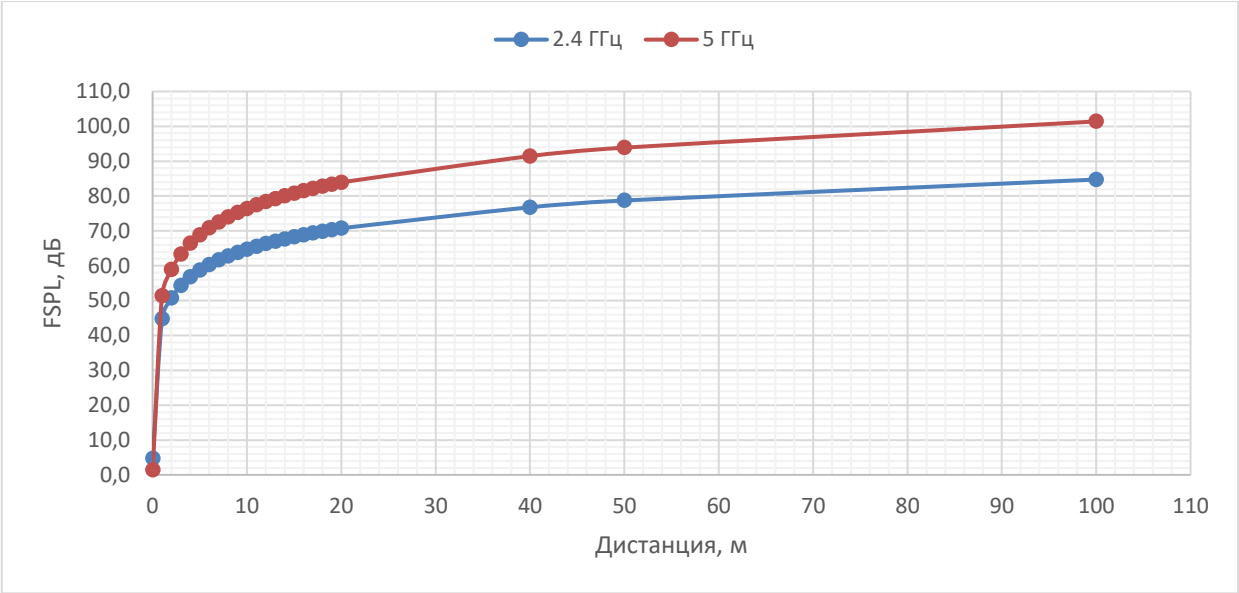


Рис. 1. Графики зависимости затухания сигнала в свободном пространстве от частоты и дальности передачи

На данных графиках видно, что FSPL изменяется по логарифмическому закону, из чего следует, что с увеличением FSPL увеличивается погрешность определения расстояния до клиента.

Позиционирование беспроводного клиента осуществляется путём сравнения заранее рассчитанных RSSI с RSSI, полученными от данного клиента, с некоторым допуском (ΔRSSI), на величину которого сравниваемые значения могут отличаться. Есть несколько подходов к выполнению данной операции: фиксированный ΔRSSI, например ±3 дБм; циклическое уменьшение дельты, пока количество полученных результатов не будет превышать некоторое заранее заданное значение, например 50. Так как FSPL имеет логарифмическую зависимость от расстояния передачи, применение фиксированного ΔRSSI либо линейно уменьшающегося ΔRSSI приведёт к выборке некорректных местоположений. Одно из решений – варьировать ΔRSSI для каждого RSSI по логарифмическому закону таким образом, чтобы погрешность системы определения местоположения не превышала заданного значения.

Ожидаемая точность позиционирования беспроводных клиентов задаётся на этапе проектирования системы определения местоположения и выражается в метрах погрешности на 1 дБм. Зависимость погрешности измерения расстояния от затухания сигнала в свободном пространстве (FSPL) представлена на рис. 2.

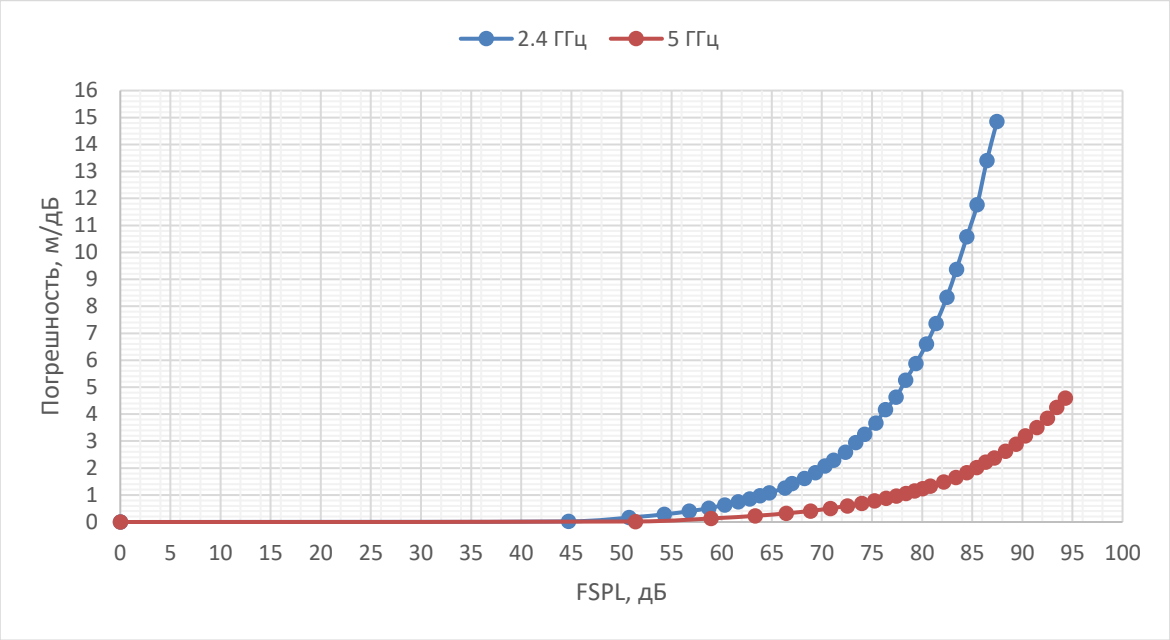


Рис. 2. График зависимости погрешности измерения расстояния от затухания сигнала в свободном пространстве (FSPL)

Исходя графиков рис. 2, погрешность в 5 метров в диапазоне частот 2,4 ГГц соответствует значению FSPL 78 дБ, что в данном случае соответствует расстоянию 50 метров от устройства до приёмника; для диапазона частот 5 ГГц FSPL равна 95 дБ, что соответствует 55 метрам. Так как сигнал с частотами диапазона 5 ГГц имеет большую силу затухания, чем сигнал из диапазона частот 2,4 ГГц, погрешность измерения расстояния для диапазона частот 5 ГГц всегда будет ниже, чем – для 2,4 ГГц.

Для вычисления ΔRSSI предлагается использовать следующие формулы:

$$d = 10^{\frac{FSPL - p - 20\times\lg(f)+24}{10\times D}}$$

$$\Delta RSSI = \begin{cases} C_{\min} \text{ при } \left(1-\frac{d}{d_{\max}}\right)\times C_{\max} \le C_{\min} \\ \left(1-\frac{d}{d_{\max}}\right)\times C_{\max} \text{ при } C_{\min} < \left(1-\frac{d}{d_{\max}}\right)\times C_{\max} \le C_{\max} \\ C_{\max} \text{ при } C_{\max} < \left(1-\frac{d}{d_{\max}}\right)\times C_{\max} \end{cases}$$

где d_{max} – максимально допустимая дистанция передачи, м; C_{min} – минимально допустимая ΔRSSI, дБм; C_{max} – максимально допустимая ΔRSSI, дБм. Значение d_{max} для диапазона частот 2,4 ГГц в данном случае равно 50 метров, для 5 ГГц – 55 метров (рис. 2). C_{min} и C_{max} предлагается приравнивать к 1 и 3 дБм соответственно. График зависимости допустимой ΔRSSI от индикатора уровня мощности принимаемого сигнала (RSSI) для погрешности позиционирования 5 метров представлен на рис. 3.

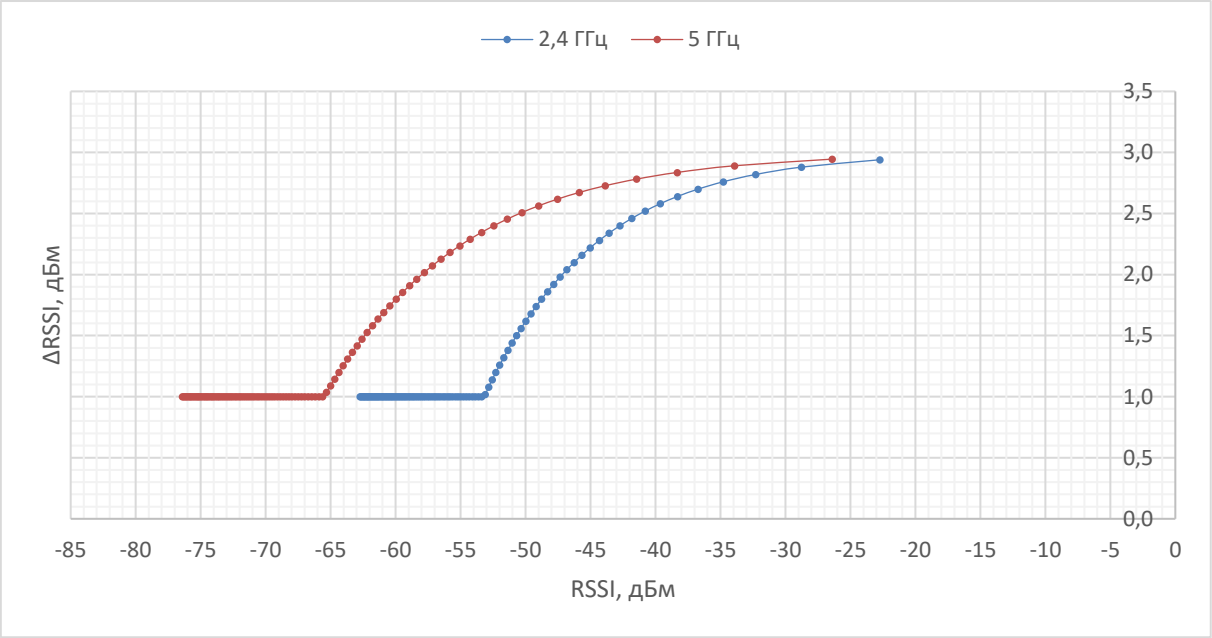


Рис. 3. График зависимости допустимой ΔRSSI от индикатора уровня мощности принимаемого сигнала (RSSI) для погрешности позиционирования 5 метров

Данный график иллюстрирует подбор допустимых значений ΔRSSI в зависимости от входящих метрик RSSI, которые, в свою очередь, логарифмически зависят от расстояния, на которых они были получены. Минимальный допуск в 1 дБм необходим для учёта интерференций и прочих непрогнозируемых факторов.

Заключение. Использование представленного подхода позволяет определить допустимое значение ΔRSSI, при котором можно гарантировать, что погрешность позиционирования беспроводного IEEE 802.11 клиента не превысит установленный лимит погрешности по дальности в наблюдаемых условиях.

Список используемых источников:

1. Дрепа В. Е. Оценка точности позиционирования беспроводного IEEE 802.11 клиента в свободном пространстве методами трилатерации с использованием метрики RSSI // Региональная информатика и информационная безопасность : материалы Юбилейной XVIII Санкт-Петербургской междунар. конф., Санкт-Петербург, 26–28 окт. 2022 г. Выпуск 11. СПб. : СПОИСУ, 2022. С. 578-582. EDN ABKCWL.

2. Eric Jacobsen. Frequency Dependence in Free Space Propagation [Электронный ресурс]. URL: https://www.dsprelated.com/showarticle/62.php (дата обращения: 05.10.23).

3. Friis H.T. A Note on a Simple Transmission Formula. May 1946. IRE Proc.: 254–256.

4. Indoor Positioning Algorithm Based on the Improved RSSI Distance Model / Guoquan Li, Enxu Geng, Zhouyang Ye, Yongjun Xu 1, Jinzhao Lin, Yu Pang. 27 August 2018.

5. Robert Wilson. Propagation losses through common building materials 2.4 GHz vs 5 GHz // E10589, Magis Network, Inc. 2002.

6. Robust Localization Algorithm Based on the RSSI Ranging Scope / Yan Huang, Jianying Zheng, Yang Xiao, Miao Peng. 21 January 2015.

Drepa V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Methodology of Selecting Acceptable RSSI Values for a Wi-Fi Client Location System Using the Fingerprinting Method.

One of the most popular systems for determining the location of wireless clients in networks of the IEEE 802.11 family are systems based on trilateration methods and using the RSSI metric. In particular, the fingerprinting method involves the use of a radio fingerprint map – a set of pre-calculated RSSI metrics. This article discusses an approach to compare pre-calculated metrics with metrics obtained from the desired wireless client.

Key words: Wi-Fi, trilateration, fingerprinting, IEEE 802.11, accuracy, location, RSSI.

УДК 004.056.57
ГРНТИ 20.51.19

КОМПЬЮТЕРНАЯ АТАКА DNS AMPLIFICATION: МЕХАНИЗМЫ, ИНСТРУМЕНТЫ И ЗАЩИТА ОТ УГРОЗЫ

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

Пользователям и организациям необходимо обращать внимание на серьезные последствия распространенных атак на отказ в обслуживании. Пока существуют информационные системы, всегда будет риск, что их атакуют, в результате чего можно столкнуться различными последствиями: отказ в доступе, потеря данных, остановка значимых процессов. В статье рассматривается атака DNS усиление: были изучены этапы проведения, возможные инструменты для реализации атаки и предложены методы защиты от нее.

DDoS атака, DNS усиление, безопасность, защита

Введение

DDoS (Distributed Denial of Service) — атаки являются серьезной угрозой для сетевой безопасности. Они позволяют злоумышленникам перегрузить сетевую инфраструктуру и вызвать отказ в обслуживании у легитимных пользователей. Одним из распространенных методов DDoS-атак является использование усиления трафика (amplification) — это метод, при котором злоумышленники используют открытые службы сетевого протокола для увеличения объема трафика, направленного на жертву. [1] Как правило в таких атаках участвуют три стороны: злоумышленник, отражатель (сервер) и цель. Злоумышленник подделывает IP-адрес жертвы, чтобы ответ от сервера вернулся ей же в увеличенном в несколько раз объеме. Суть действий злоумышленника заключается в создании наибольшего отражения из наименьших запросов. Данный тип атаки действует на 4 и 7 уровне модели OSI, некоторые из наиболее распространенных протоколов, используемых для усиления трафика, включают: DNS (Domain Name System), NTP (Network Time Protocol) и SNMP (Simple Network Management Protocol) [2].

DNS amplification

При атаке с усилением DNS киберпреступники используют повседневное функционирование Системы доменных имен (DNS), превращая ее в оружие.

Атака DNS amplification является одним из видов DDoS-атак, при которой злоумышленник использует открытые DNS-серверы для усиления своего трафика и нацеливает его на жертву. Рассмотрим этапы атаки подробнее:

Подготовка:

Злоумышленник ищет открытые DNS-серверы (открытые рекурсивные DNS-серверы), которые могут быть использованы для атаки. Для этого могут быть применены методы:

- Отправка запросов на рекурсивный DNS и анализ ответов. Если сервер отвечает на запросы с любого IP-адреса, это может указывать на открытый DNS сервер.
- Использование утилит: например, dnsrecon, которая может автоматически сканировать сеть и искать открытые DNS сервера.
- Поиск уязвимостей: злоумышленники могут искать известные уязвимости в программном обеспечении DNS серверов и использовать их для получения несанкционированного доступа.
- Мониторинг сетевого трафика: Злоумышленники могут мониторить сетевой трафик и искать DNS запросы, отправляемые на открытые DNS сервера.

После чего злоумышленник создает поддельный IP-адрес отправителя-жертвы

Начало атаки:

Злоумышленник отправляет запросы на открытые DNS-серверы, используя IP-адрес жертвы в качестве адреса назначения. UDP-пакеты отправляют запросы с типом аргумента “ANY” для получения большого количества ответов на трафик, чтобы сервер был занят. Запросы формируются таким образом, чтобы они были гораздо больше по размеру, чем предполагается, что позволяет усилить трафик [3-4].

Усиление трафика:

Открытые DNS-серверы получают запросы от злоумышленника и начинают отвечать на них. Однако, вместо отправки ответов напрямую злоумышленнику, серверы отправляют их на адрес жертвы, при этом ответы DNS-серверов гораздо больше по размеру, чем сами запросы, что приводит к усилению трафика. Схема действия атаки приведена на рис. 1.

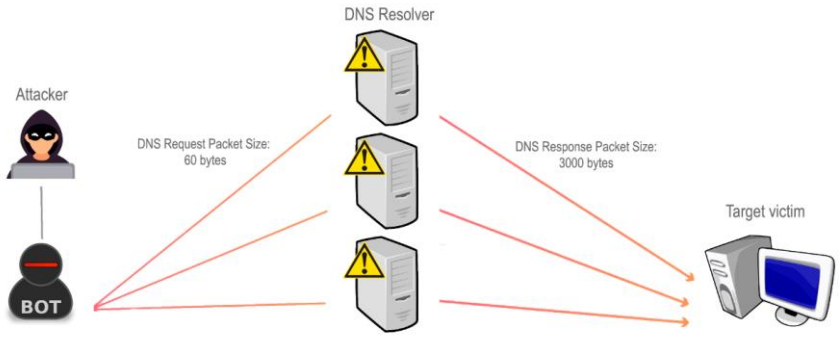


Рис. 18. Схема действий при атаке DNS усиление

Последствия для жертвы:

Жертва начинает получать огромное количество ответов от DNS-серверов, превышающие ее пропускную способность, что приводит к

перегрузке сети и серьезному снижению производительности системы. В результате, сервисы жертвы могут быть недоступными для легитимных пользователей. Также владельцы систем и сетей, подвергшихся атаке, могут столкнуться с дополнительными издержками для мониторинга, защиты и восстановления после атаки. Атаки DNS-амплификацией могут вызвать потерю данных и привести к разглашению конфиденциальной информации [5].

Злоумышленник может повторять запросы на DNS-серверы с различных IP-адресов, чтобы усложнить идентификацию его источника. Он также может использовать ботнеты или другие компрометированные устройства для увеличения объема атакующего трафика.

Инструменты для проведения DNS amplification

Стоит отметить, что проведение атак носит незаконный характер, в случае проверки сервисов необходимо получить разрешение владельцев на подобные тесты.

Для проведения атаки DNS-амплификацией злоумышленники могут использовать различные утилиты и инструменты, такие как:

- Scapy: это мощный инструмент для создания и отправки собственных сетевых пакетов. С его помощью злоумышленники могут создавать и отправлять DNS-запросы с поддельными исходными IP-адресами. [6]
- Nmap: это инструмент сканирования сети, который также может использоваться для генерации DNS-запросов с поддельными IP-адресами. [7]
- Custom Scripting: Злоумышленники могут написать собственные скрипты или программы для генерации фальшивых DNS-запросов. [8]
- DDoS-инструменты: Некоторые DDoS-инструменты и ботнеты также могут включать в себя функциональность для проведения атак DNS-амплификацией [8].

Способы защиты от DNS amplification

1. Конфигурация DNS-серверов: ограничение доступа к рекурсивным DNS-серверам только для авторизованных клиентов.
2. Мониторинг: тщательный мониторинг сети и DNS-трафика для быстрого обнаружения аномалий и атак.
3. Обновление ПО: постоянная поддержка ПО в актуальном состоянии для устранения известных уязвимостей.
4. Использование фильтрации DNS для блокировки запросов, исходящих из IP-адресов с большим количеством запросов.
5. Использование IDS/IPS: системы обнаружения вторжений и системы предотвращения вторжений помогают выявить и предотвратить атаки с DNS усилением.
6. Сетевая сегментация: организация сетевой сегментации для ограничения распространения атак на разные части сети.
7. Защита от подделки IP-адресов: методы проверки подлинности IP-адресов, такие как BCP38 (стандарт сетевой безопасности, который

позволяет предотвратить подмену источника DDOS-атак) для предотвращения использования поддельных IP-адресов.

8. Отклонение запросов типа ANY по UDP: DNS относится к протоколам с двойным стеком, соответственно в подобных ситуациях предпочтительней использовать TCP, как более безопасный относительно UDP.

Для атакуемых устройств

Защита жертвы от атаки DNS-амплификацией может быть сложной задачей, но существует несколько методов и рекомендаций, которые могут помочь уменьшить риск и смягчить последствия атаки:

1. Использование фильтров DNS: DNS фильтры для блокировки DNS-запросов с подозрительных источников.

2. Ограничение доступа к DNS-серверам только для известных и авторизованных источников. Настройка брандмауэра и правил доступа.

3. Использование CDN службы доставки контента (Content Delivery Network, CDN), которые могут распределять трафик между несколькими серверами, что позволяет снизить нагрузку на отдельные DNS серверы и предотвратить перегрузку, также CDN может фильтровать трафик, направленный на DNS серверы, и блокировать запросы, которые могут быть связаны с атаками амплификации.

4. Использование средств для мониторинга и анализа сетевого трафика, например: системы обнаружения вторжений (IDS), системы сбора и анализа журналов (Syslog), системы управления информационной безопасностью и событиями безопасности (SIEM).

5. Скрывать авторитативный DNS-сервер за облачным ресурсом, у которого большая полоса пропускания и в целом больше возможностей, чем у серверной машины.

6. Обновление и обеспечение безопасности: инфраструктура и DNS-серверы должны быть обновлены и защищены от известных уязвимостей.

Защита от атак DNS-амплификацией требует комплексного подхода, включая настройку серверов, мониторинг и реакцию на атаки, и соблюдение рекомендаций по безопасности [1].

Заключение

Атаки DNS-амплификацией представляют собой серьезную угрозу сетевой безопасности и доступности ресурсов в Интернете. Эти атаки могут использовать открытые рекурсивные DNS-серверы для увеличения объема атакующего трафика, что приводит к отказу в обслуживании и угрожает инфраструктуре сети.

Для того чтобы защититься от атак DNS-амплификацией, необходим комплексный подход, включающий настройку DNS-серверов, фильтрацию трафика, мониторинг и реакцию на атаки. Важно также соблюдать рекомендации по безопасности и использовать облачные службы для защиты от DDoS-атак.

Целью атаки DNS amplification является создание огромного объема трафика, который превышает пропускную способность жертвы и приводит к ее недоступности. Это может причинить серьезный ущерб бизнесу или организации, а также нарушить работу их онлайн-сервисов.

Список используемых источников:

1. DDoS-атаки с DNS-усилением: как это работает и как их остановить [Электронный ресурс]. URL: https://networkguru.ru/ddos-ataki-s-dns-usileniem-kak-eto-rabotaet-i-kak-ix-ostanovit/ (дата обращения: 25.10.2023)
2. DDoS-атаки: нападение и защита [Электронный ресурс]. URL: https://habr.com/ru/companies/ruvds/articles/321992/ (дата обращения: 25.10.2023)
3. Anatomy of a DDoS amplification attack [Электронный ресурс]. URL: https://www.microsoft.com/en-us/security/blog/2022/05/23/anatomy-of-ddos-amplification-attacks/ (дата обращения: 25.10.2023)
4. Everything You Need to Know About DNS Amplification Attacks [Электронный ресурс]. URL: https://www.cdnetworks.com/cloud-security-blog/dns-amplification-attacks/ (дата обращения: 25.10.2023)
5. Information security [Электронный ресурс]. URL: https://security.stackexchange.com/ (дата обращения 25.10.2023)
6. Scapy [Электронный ресурс]. URL: https://scapy.net/ (дата обращения: 26.10.2023)
7. Nmap [Электронный ресурс]. URL: https://nmap.org/ (дата обращения: 26.10.2023)
8. DNS amplification attack [Электронный ресурс]. URL: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/ (дата обращения 25.10.2023)

Dyusmetova A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Dns amplification computer attack: mechanisms, tools and threat protection. Users and organizations need to pay attention to the serious consequences of widespread denial of service attacks. As long as information systems exist, there will always be a risk that they will be attacked, as a result of which you can face various consequences: denial of access, data loss, stopping significant processes. The article discusses the DNS amplification attack: the stages of carrying out, possible tools for implementing the attack were studied and methods of protection against it were proposed.

Key words: DDoS attack, DNS enhancement, security, protection

УДК 004.056
ГРНТИ 81.93.29

МЕТОДИКА АУДИТА ПРОЦЕССА «ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ УПРАВЛЕНИИ ДОСТУПОМ»

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

Рассмотрен процесс обеспечения защиты информации при управлении доступом в финансовых организациях. Проанализированы требования к мерам защиты информации, содержащейся в автоматизированных системах финансовых организаций, а также приведены примеры сравнения требований, предъявляемых ФСТЭК России и ФСБ России. Результаты исследования позволяют финансовой организации выбрать наиболее подходящие методы и подходы к обеспечению безопасности обрабатываемых данных.

защита информации, финансовые организации, ГОСТ Р 57580.1-2017, меры защиты информации

В целях обеспечения безопасности информации в финансовых организациях, Банком России установлены требования к мерам защиты информации, содержащейся в автоматизированных системах финансовых организаций. Указанные требования, помимо прочих локальных нормативных актов, содержатся в ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» [1].

Требование соответствовать одному из трех уровней защиты информации ГОСТ Р 57580.1-2017 установлено в Положении Банка России № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» [2].

Поскольку указанные организации помимо своей профильной деятельности также обрабатывают персональные данные и являются операторами персональных данных, то они должны выполнять требования по обеспечению безопасности персональных данных, приведенные в Приказе ФСТЭК России от 18.02.2013 № 21 [3]. То же касается и информации, составляющей коммерческую тайну. Кроме того нередко финансовые организации также являются субъектами критической информационной инфраструктуры, соответственно они должны выполнять требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, приведенные в Приказе ФСТЭК России от 25.12.2017 № 239 [4]. Требования к обеспечению безопасности указанных типов информации, помимо Банка России, выдвигаются, в частности, ФСТЭК России и ФСБ России.

Большинство информационных систем финансовых организаций будут обрабатывать информацию перечисленных типов.

В связи с тем, что базовый набор мер защиты информации конечен, в данной статье будет рассмотрен процесс №1 «Обеспечение защиты информации при управлении доступом», состав мер которого установлен требованиями ГОСТ 57580.1-2017.

Указанный процесс состоит из следующих подпроцессов (Рис. 19):

- Управление учетными записями и правами субъектов логического доступа (УЗП).
- Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа (РД).
- Защита информации при осуществлении физического доступа (ФД).
- Идентификация и учет ресурсов и объектов доступа (ИУ).

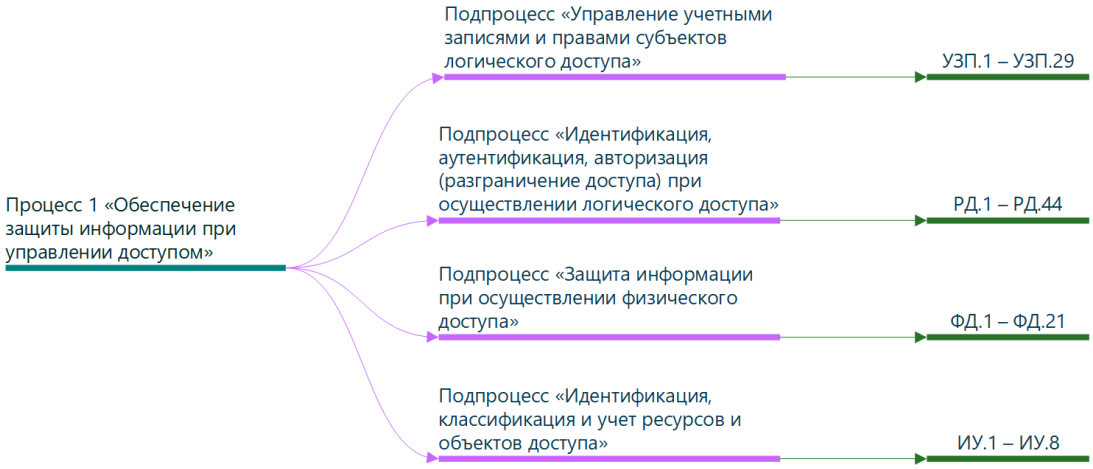


Рис. 19. Обеспечение защиты информации при управлении доступом

Требования процесса №1 из ГОСТ 57580.1-2017 можно распределить и сопоставить со схожими мерами в требованиях ФСТЭК России к обеспечению безопасности персональных данных, а также в требованиях о защите информации, содержащейся в государственных информационных системах (ТАБЛИЦА 1).

ТАБЛИЦА 1. Сравнение мер защиты информации

	Мера защиты информации по ГОСТ 57580.1-2017	Мера защиты информации по Приказу ФСТЭК России № 21 и Приказу ФСТЭК России № 17
	УЗП.1: Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями	ИАФ.1: Идентификация и аутентификация пользователей, являющихся работниками оператора
		ИАФ.6: Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
	УЗП.24:	РСБ.3:

	Мера защиты информации по ГОСТ 57580.1-2017	Мера защиты информации по Приказу ФСТЭК России № 21 и Приказу ФСТЭК России № 17
	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению логическим доступом	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
	СМЭ.4: Реализация и контроль информационного взаимодействия между сегментами контуров безопасности и иными внутренними вычислительными сетями финансовой организации в соответствии с установленными правилами и протоколами сетевого взаимодействия	УПД.3: Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
	РД.8: Сокрытие (неотображение) паролей при их вводе субъектами доступа	ИАФ.5: Защита обратной связи при вводе аутентификационной информации
	ФД.8: Оборудование входных дверей помещения механическими замками, обеспечивающими надежное закрытие помещений в нерабочее время	ЗТС.3: Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
	ФД.13: Контроль доступа к серверному и сетевому оборудованию, расположенному в запираемых серверных стоечных шкафах	
	РД.31: Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод) при разграничении логического доступа к ресурсам доступа	УПД.2: Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа

Как видно из отрывка сравнительной таблицы, многие меры пересекаются, повторяют друг друга или дополняют. Например, РД.8 и ИАФ.5 идентичны по смыслу, однако звучат по-разному, хотя обе запрещают отображение вводимых символов аутентификационных данных. Меры УЗП.24 и РСБ.3 обе относятся к логированию, однако нельзя сказать, что одна заменяет другую, поскольку УЗП.24 является дополнением и уточнением к мере РСБ.3. В таком случае, если финансовая организация выполняет требования меры УЗП.24 она соответственно выполняет и

требования меры РСБ.3, однако при этом выполнение РСБ.3 является необходимым, но недостаточным для сравнения этих мер и приравнивания их выполнения.

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. Стандартинформ, 2020.
2. Положение Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».
3. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
4. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

Dyatchenko A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Audit methodology of the process "ensuring the protection of information in access control".
The process of ensuring information security in financial organizations has been discussed. The requirements for information protection measures in automated systems of financial organizations have been analyzed, and examples of comparing the requirements of the Federal Security Service of Russia and the Federal Security Service of Russia have been provided. The research results allow financial organizations to choose the most suitable methods and approaches to ensure the security of processed data.

Key words: information protection, financial organizations, GOST R 57580.1-2017, information security measures.

УДК 004.832.34
ГРНТИ 81.93.29

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КИБЕРБЕЗОПАСНОСТИ

П. Ю. Егорова, Ю. В. Охлопкова, А. А. Шиян
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Искусственный интеллект (ИИ) стал неотъемлемой частью современной кибербезопасности. С развитием технологий он стал широко применяться для обнаружения угроз, защиты от кибератак и принятия решений. Анализ больших объёмов данных является одной из основных причин использования искусственного интеллекта в кибербезопасности. Это позволяет выявлять угрозы быстрее и принимать меры для их предотвращения.

искусственный интеллект (ИИ), кибербезопасность, информационная безопасность, угрозы, машинное обучение (МО)

Технологии искусственного интеллекта (ИИ, англ. *Artificial Intelligence, AI*) и машинного обучения (англ. *Machine Learning, ML*) сейчас широко применяются в информационных системах для увеличения производительности труда, повышения продаж, обучения, что проиллюстрировано на рис. 1. Их использование в защите от кибератак становится одним из ключевых направлений в информационной безопасности. Использование ИИ помогает автоматизировать процессы обнаружения и реагирования на кибератаки. ИИ может непрерывно мониторить сеть и обнаруживать аномальное поведение, которое может указывать на кибератаку. Кроме того, ИИ может автоматически реагировать на угрозы, блокируя доступ хакеров и предотвращая утечку данных.

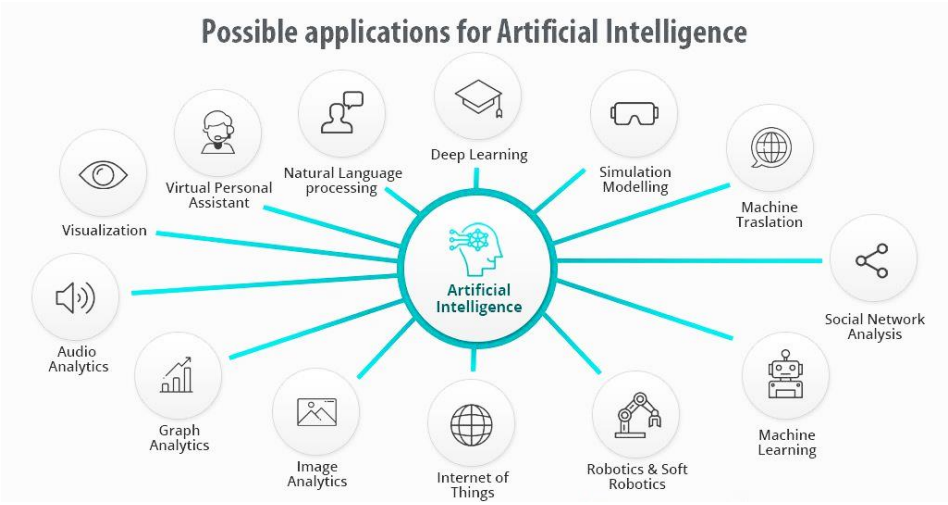


Рис. 20. Отрасли применения искусственного интеллекта

Машинное обучение – это тип искусственного интеллекта, который включает в себя разработку и использование компьютерных систем, которые

могут изучать и делать прогнозы на основе наборов данных без необходимости следовать явным инструкциям человека. Как правило, модели машинного обучения используют алгоритмы и статистические модели для обработки исторических данных в качестве входных данных, а затем используют тенденции в этих данных для прогнозирования новых выходных значений. Методы ML разработаны для того, чтобы сделать эти прогнозируемые результаты более точными без помощи программирования, специально разработанного для создания решения. Платформы машинного обучения и программные приложения анализируют данные и делают выводы на основе закономерностей, которые они обнаруживают в этих данных.

Объем мирового рынка машинного обучения оценивается в 19,20 миллиарда долларов в 2022 году и, как ожидается, вырастет до 26,03 миллиарда долларов в 2023 году до 225,91 миллиарда долларов к 2030 году. Растущее внедрение и совершенствование технологий и автоматизации, включая облачные платформы, сетевые системы, интегрированные системы памяти и встроенные в ИИ процессоры, позволяют быстро решать сложные задачи и являются основной движущей силой прогнозируемого роста рынка машинного обучения.

Виды атак на ИИ в зависимости от их цели делятся на:

1. Шпионаж – получение представления о системе и использование полученной информации для собственной выгоды или подготовки более сложных атак. К примеру, так злоумышленник может обмануть личного голосового помощника и получить личные данные пользователя, просто сымитировав его голос.

2. Саботаж – действия, направленные на введение в неисправность системы ИИ. Его можно произвести несколькими способами: затопление ИИ запросами, которые требуют больше времени вычислений, чем обычно; модификация модели путем ее переподготовки и т.д.

3. Мошенничество – обман ИИ через неправильную классификацию. Так можно обмануть систему, чтобы она ошибочно классифицировала, например, кошек и собак. У мошенника есть два способа сделать это – взаимодействуя с системой на этапе обучения или через применение моделей.

Пример мошенничества – отравление данных. Это атака, при которой ошибка закладывается на этапе обучения и злоумышленник заранее знает, как обмануть сеть. Отравление данных может произойти в следующих случаях: порча данных на краудсорсинг-платформах, например, при пометке капчей с определенными объектами; использование предобученных моделей, т.е. моделей, уже обученных на определенном наборе данных, схожих с целевыми; порча данных при обучении в облаке.

Порой для целостности данных и уменьшения рисков данной атаки производится хеширование исходных данных и хранение их в виде хеш-сумм, однако Microsoft рекомендует считать, что все данные изначально

отравлены и требуют обработки для удаления потенциально отравленных данных.

Следующий пример данного вида атак – атаки уклонения. Это атаки, возникающие на этапе применения нейронных сетей. В этом случае злоумышленник пытается создать оптическую, слуховую или смысловую иллюзию для модели. То, что может быть легко распознано и определено как поддельное для человека, может быть неразличимым для искусственного интеллекта.

В основном для атак уклонения используются «состязательные примеры». Эти примеры обладают некоторыми свойствами, ставящими под угрозу многие системы. Состязательные примеры зависят от данных, а не от архитектур, и их можно сгенерировать для большинства датасетов. Обман сети производится с помощью наложения шума на изображение. Пример данной атаки приведен на рис. 2.

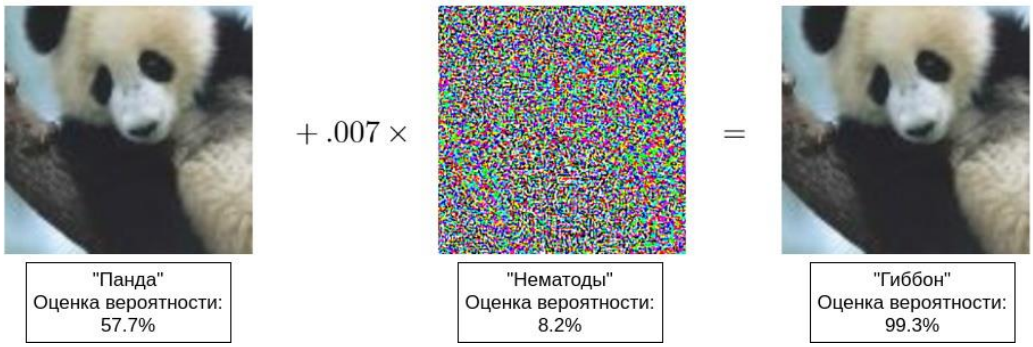


Рис. 21. Обман сети с помощью наложения шума на изображение

Для предотвращения данной атаки известно несколько техник: использование преобразования данных для изображений (метод главных компонент, пороговое преобразование, уменьшение глубины цвета, а также сжатие в JPEG); обучение модели на наборе с состязательными примерами и правильно размеченными метками.

Основные методы улучшения кибербезопасности при помощи машинного обучения и ИИ:

1. Искусственный интеллект подойдет для классификации, обработки, кластеризации и фильтрации поступающей информации, поскольку есть много информационных данных в такой сфере.

2. Машинное обучение дает возможность анализировать прошлую информацию, предоставлять оптимальные методы решения для будущего и настоящего. При помощи прошлых данных алгоритмы обеспечивают инструкциями, позволяющие найти угрозы или вредоносное ПО. AI и ML помогают нарушать работу любого, кто захочет проникнуть в систему.

3. Внедрение технологий систематизирует информацию по заданным параметрам, позволяя сопоставлять разную информацию, отслеживать любые угрозы.

4. ИИ упростит ведение аудита способов защиты информации, что даст возможность быстро узнать об эффективности внедрения ограничений. Это защищает пользователей конкретной компании.

5. AI и ML быстро находит угрозы, вредное ПО, создавая платформу безопасности для сканирования крупных информационных объемов.

На наш взгляд, чтобы использование ИИ в кибербезопасности было эффективным, необходимо учитывать несколько важных моментов.

Во-первых, обеспечение защиты данных и алгоритмов ИИ от кибератак и взломов. Существует возможность использования злоумышленниками вредоносных алгоритмов для вторжения в системы ИИ и изменения ее работы, чтобы обойти системы защиты. Поэтому необходимо усилить меры защиты систем, работающих на основе ИИ, и проводить регулярные проверки на наличие уязвимостей.

Во-вторых, обучение ИИ на различных типах кибератак и угроз, а также использование актуальные данные. ИИ не сможет эффективно обнаруживать новые типы угроз, если он не обучен на них. Поэтому необходимо использовать актуальные данные о киберугрозах, чтобы ИИ мог обнаруживать новые типы угроз.

В-третьих, необходимо учитывать этические и правовые вопросы в отношении использования ИИ в кибербезопасности. Необходимо разрабатывать этические и правовые стандарты, которые будут регулировать использование ИИ в кибербезопасности, так как некоторые решения принятые на основе ИИ могут привести к нарушению прав человека.

Таким образом, использование ИИ в кибербезопасности не может полностью заменить человеческий фактор. ИИ может помочь автоматизировать процессы обнаружения и реагирования на угрозы, но для принятия окончательного решения о безопасности все же требуется участие специалиста. Поэтому следует использовать ИИ как инструмент, который помогает человеку, а не заменяет его.

В целом, использование ИИ в кибербезопасности является важным и перспективным инструментом для борьбы с киберугрозами, при грамотном учете рисков и недостатков его использования и обеспечении мер безопасности и этичности.

Список используемых источников:

1. Применение технологий искусственного интеллекта в информационной безопасности [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-security (дата обращения 27.10.2023)

2. 30 Machine Learning Statistics + Trends in 2023[Электронный ресурс]. URL: https://youngandtheinvested.com/machine-learning-statistics/ (дата обращения 27.10.2023)

3. Fortune Business Insights [Электронный ресурс]. URL: https://www.fortunebusinessinsights.com/ (дата обращения 27.10.2023)

4. Market Research Future [Электронный ресурс]. URL: https://www.marketresearchfuture.com/ (дата обращения 21.10.2023)

5. Применение ИИ и машинного обучения в кибербезопасности [Электронный ресурс]. URL: https://is.astral.ru/news/blog/primenenie-ii-i-mashinnogo-obucheniya-v-kiberbezopasnosti/ (дата обращения 25.10.2023)
6. Как ИИ кибербезопасность усиливает: новые тренды и возможности [Электронный ресурс].URL: https://habr.com/ru/companies/neuronet/articles/645539/ (дата обращения 31.10.2023)
7. ТРЕНДЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА (ИИ) В 2023 ГОДУ [Электронный ресурс].URL: https://merehead.com/ru/blog/ai-trends-2023/ (дата обращения 4.11.2023)
8. Роль искусственного интеллекта в кибербезопасности [Электронный ресурс]. URL: https://vc.ru/dev/621020-rol-iskusstvennogo-intellekta-v-kiberbezopasnosti (дата обращения 31.10.2023)

Egorova P., Okhlopkova Yu., Shiyan A.

The Bonch-Bruevich Saint-Peterburg State University of Telecommunications

Features of the use of artificial intelligence in cybersecurity.

Artificial intelligence (AI) has become an essential part of modern cybersecurity. Due to the advancement of technology, artificial intelligence has become widely used for threat detection, protection against cyberattacks and making decisions. One of the main reasons for using artificial intelligence in cybersecurity is the ability to quickly analyze large amount of data. This allows you to identify threats faster and take action to prevent them.

Key words: artificial intelligence (AI), cybersecurity, information security, threats, machine learning (ML).

УДК 004.8
ГРНТИ 20.53

ОБЕСПЕЧЕНИЕ СОВ ПНП ДЛЯ ПРОВЕДЕНИЯ МОНИТОРИНГА РИС

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

В современном мире, где данные стали новым золотом, а их безопасность – необходимостью, роль искусственного интеллекта в сфере информационной безопасности постоянно возрастает. Уже существуют попытки атак на информационные системы с помощью вредоносного искусственного интеллекта, для предупреждения и выявления таких атак, требуется применять аналитику Больших данных в связке с СЗИ

искусственный интеллект, информационная безопасность

В данной работе внимание акцентируется на выгодном использовании как параметров IDS, так и SIEM, что положительно влияет на накопление информации о потенциальных угрозах и наращивание опыта для ассоциативной памяти. Можно утверждать, что этот подход не просто дополняет модель обработки ассоциативной памяти, а, скорее, самоорганизующаяся карта способна представить в системе YaVi всестороннее представление о вторжениях и обеспечить целостность и централизацию всей её архитектуры.

В процессе разработки методики, были достигнуты следующие результаты:

1. Разработан алгоритм обработки полученных значений. В рамках методики предложен планомерный процесс сбора данных для поддержания интеллектуальных СОВ и РИС
2. Определено пороговое значение увеличения объёма сбора информации Ксбор, что позволяет устанавливать нужное значение для переменных *N*бит (объём обрабатываемой информации в битах), что в последствии поможет ориентироваться на значение *Sn*.
3. Интегрировано устройство для диагностики каналов передачи данных, что, с целью обеспечения качества и надёжности сетевого контроля, предполагает использование диагностического устройства РИС. Это устройство улучшает точность диагностики благодаря вероятностному прогнозированию возможных сбоев в измерительных приёмниках и комплектах оконечного оборудования на определённый временной интервал, а также расчёту их коэффициента оперативной готовности с помощью многослойной нейронной сети (НС).
4. Представлен нейросетевой процессор ЦУС, в котором во время непрерывного мониторинга осуществляется коррекция ошибок в интеллектуальный СОВ.

В данной работе применяется метод МРЧ, где внутренние компоненты YaVi были организованы в таблицу так, чтобы компенсировать вносимые искажения. В результате экспериментов с устройствами в РИС, где осуществляется сбор Больших данных, выявлено, что минимально отклонение везде не превысило 2.15%. Отмечено, что эти отклонения являются максимальными, полученными на основе анализа терабайт данных без коллизий и с минимальными коллизиями. В реальности, зарегистрированные коллизии были значительно ниже 1%.

В планы по разработке карты саморганизации включено введение концепции SOM – это тип искусственной нейронной сети, основанный на обучении без учителя. В SOM нейроны располагаются в узлах сетки, обычно одно- или двумерной. В разрабатываемой методике предложено оценивать корреляционные связи событий через вычисление их сходства.

Важным аспектом методики является минимизация возможных ошибок в этом процессе. Предлагается провести статический анализ работы Больших данных в РИС по МРЧ, что поможет оценить вероятность случайной ошибки при передаче данных.

Формула будет выяснять на каких типах замен операторов, риск случайной ошибки при передаче данных уменьшается или увеличивается.

Учитывая важность последующего использования методики сбора данных, важно обеспечить чёткий порядок действий для надёжного сбора и хранения информации. Данные, полученные на каждом этапе, служат входными данными для следующего этапа. Передача данных между этапами обозначена стрелками.

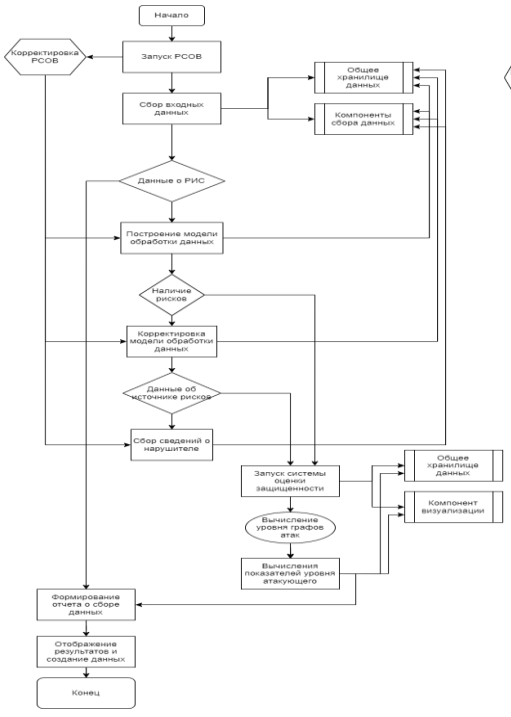


Рис. 1. Схема методики построения самоорганизующейся карты нейронной сети в статическом режиме. (этап 1)

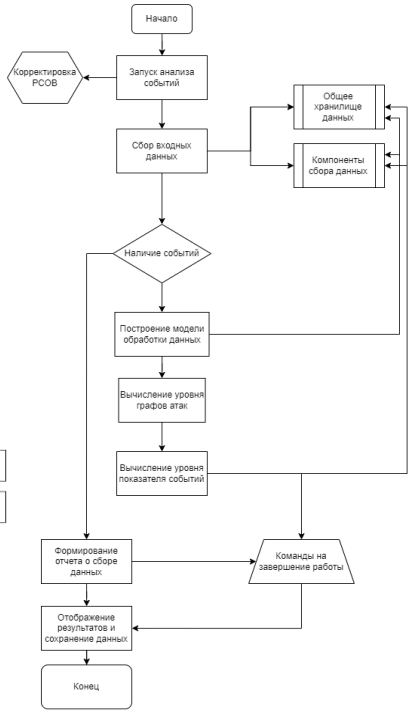


Рис. 2. Схема методики построения самоорганизующейся карты нейронной сети в динамическом режиме. (этап 1)

Методика включает в себя статический и динамический режимы функционирования всей РСОВ. Более подробно этапы функционирования методики в динамическом режиме и их последовательное выполнение изображены на рис. 2. Установлено пороговое значение увеличения сбора информации *k*сбор (коэффициент сбора данных без ошибок), что позволяет задать требуемое значение для параметров *N* бит (объём обрабатываемой информации в битах), облегчая последующее определение значения *Sn*. Значение *Sn* определяется как функция характеристик Больших данных, на примере которых заранее известно успешное количество данных, собранных в РИС.

При обработке РСОВ используется небольшой объём данных, согласно которому, при 100% заполнении данными, возможно сохранить без ошибок 40% данных при общем параметре *F* = 45%. По формуле можно соотнести значения *F* и выразить их для расчёта коэффициента *k*сбор по другой формуле.

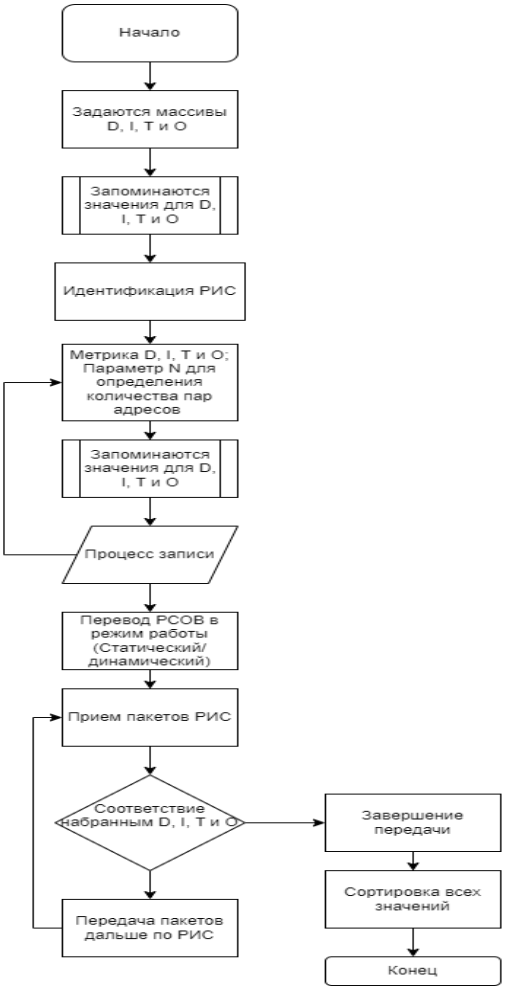


Рис. 3 Схема сбора данных на центральном узле РИС (этап 2)

Так как параметры взаимосвязаны через обмен битами в исполняемых файлах, изменение параметра *F* может зависеть от этих параметров, ведь в них присутствует значение *Sn*.

Формула будет отвечать за прогнозирование успешности обработки информации для пользователей РИС, учитывая потенциальные ошибки и угрозы вторжений. Это подразумевает, что коэффициент *k*сбор влияет на уровень защиты в модели обработки данных.

Если первый этап связан с определением рисков и ошибок при сборе данных, то второй этап направлен на распараллеливание задач в процессе их окончательной обработки, сокращая время на выявление вторжений. Реализация второго этапа описывается алгоритмом рис. 3, выполняемым на центральном узле в модели обработки потоков данных. Исходя их этого, для РСОВ формулируется плановое выполнение мониторинга при сборе данных рис. 4 для обеспечения, функционирования РИС.

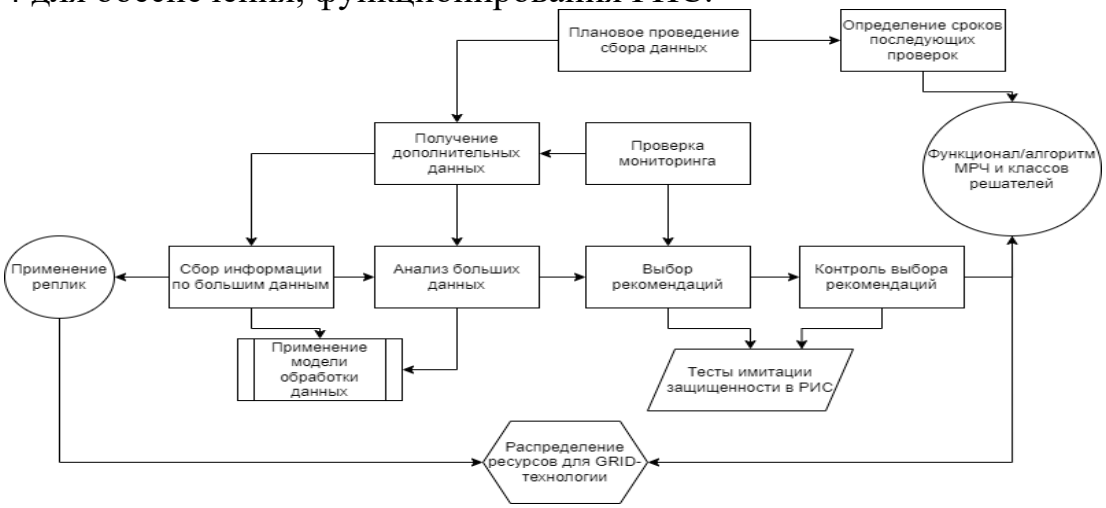


Рис. 4. Мониторинг в РИС при сборе данных (этап 2)

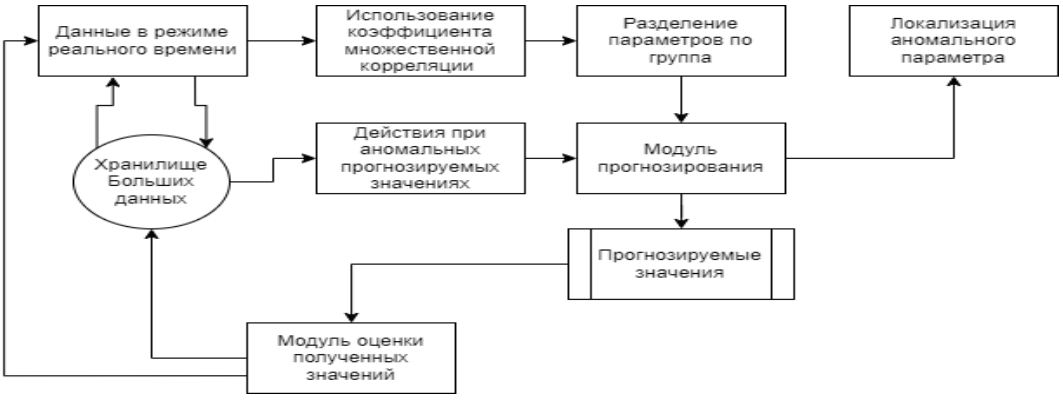


Рис. 5. Схема работы СОВ с дополнительным использованием краткосрочного прогнозирования

Для оценки своевременности выполнения методики измерим время, требуемое для прохождения её основных этапов, включая статический режим. В общем, время реализации методики будет составлено из продолжительности времени, затраченного на выполнение перечисленных выше категорий. Будут разработаны формулы.

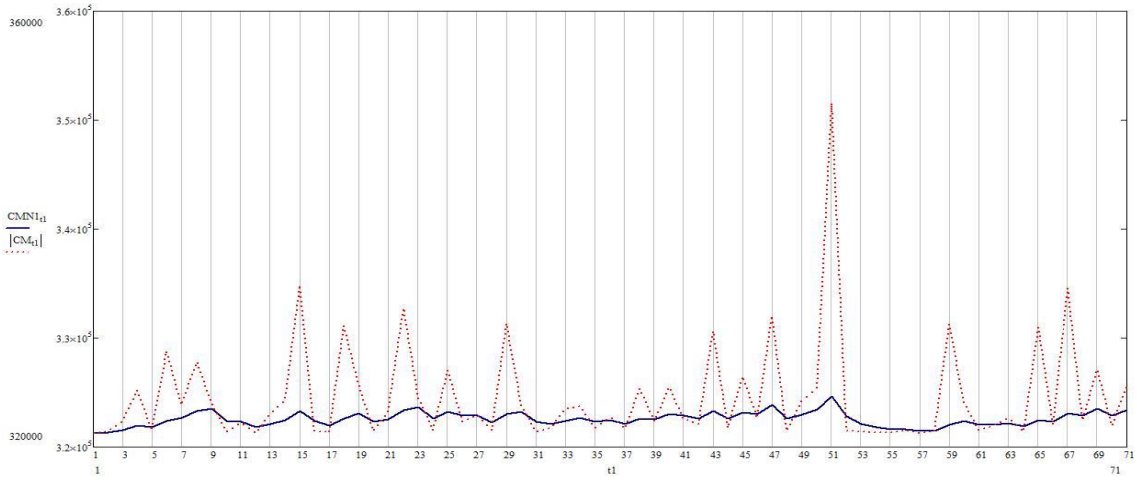


Рис. 6. Значение метрик до и после применения адаптивного алгоритма

Схема методики с интеграцией краткосрочного прогнозирования изображена на рис. 5. рис. 6 демонстрирует совмещение значений метрик до и после применения алгоритма. Пунктирной линией отмечены значения при стандартной эксплуатации РИС, сплошной линией – значения при использовании краткосрочного прогнозирования по методике.

Как можно увидеть на графике, реакция на значительное изменение метрики не является существенной, что даёт возможность установить определённое граничное значение изменения.

Список используемых источников:

1. Фостер Д. Генеративное глубокое обучение. СПб. : Питер, 2020. С. 134-145.
2. Душкин Р. Искусственный интеллект. М. : ДМК Пресс, 2019. С. 83-90.
3. Мюллер Д. П., Массарон Л. Artificial intelligence. М. : Диалектика, 2019. С. 56-75.
4. Форд М. Архитекторы интеллекта. СПб. : Питер, 2020. С. 349-420.

Emelyanenko G.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Provision of the SOV PNP for monitoring RIS.

In the modern world, where data has become the new gold, and their security is a necessity, the role of artificial intelligence in the field of information security is constantly increasing. There are already attempts to attack information systems with the help of malicious artificial intelligence, in order to prevent and detect such attacks, it is required to use Big Data analytics in conjunction with SPI..

Key words: Artificial intelligence, information security.

УДК 621.396.99
ГРНТИ 49.33.29

АНАЛИЗ ЭФФЕКТИВНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В ЗАДАЧАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М. В. Ермачкова
Санкт-Петербургский государственный университет промышленных технологий и дизайна

Технологические изменения, происходящие в современном мире, постоянно увеличивают свою скорость. В ходе цифровой трансформации экономики, государственного управления и социальной сферы происходит завершение построения информационного общества во всём мире и переход к обществу знаний, который не может обойтись без внешних и внутренних угроз.

интеллектуальные системы, информационная безопасность, кража информации, искусственный интеллект, технологии иммунных систем, автоматизация, автономное обучение

В современности нередки случаи кражи информации, в том числе конфиденциальной, что является угрозой информационной безопасности и надежности последующей деятельности как коммерческих, так и некоммерческих организаций. Одной их причин стало использование предприятиями информационных технологий, которые способны обеспечивать работу многих операционных процессов. Для защиты информации разрабатываются и внедряются высокоэффективные планы по обнаружению сбоев доступа с использованием аппаратной части и программного обеспечения.

В последнее десятилетие наблюдается активное развитие нового поколения аналитических систем, которые основаны на передовых технологиях искусственного интеллекта. Они входят в такое понятие, как “Интеллектуальные информационные системы”. Они имеют большой потенциал в сфере защиты информации благодаря возможности разработки систем, которые обучаются и способны автономно принимать решения, а также обнаружить и классифицировать потенциальные атаки или угрозы.

Интеллектуальные информационные системы, как следует из названия, обладают когнитивными способностями благодаря своим функциям обучения. Интеллектуальные информационные системы могут учиться одним из двух основных способов: под наблюдением и без надзора. При обучении под наблюдением каждая запись в обучающем наборе данных помечается своей правильной классификацией, чтобы машина узнавала, что делает запись более или менее вероятной в каждой группе. В упражнении по выявлению мошенничества каждая запись помечается как мошенническая или не мошенническая, и машина идентифицирует другие атрибуты в записи,

которые помогают различать две группы. Система ищет наилучшие отличительные признаки для описания одной группы по сравнению с другой.

Таким образом, интеллектуальная информационная система представляет собой разновидность интеллектуальной системы, содержащей комплекс программных, логико-математических, лингвистических средств для решения определённых задач, например, возможность проводить продвинутый диалог на естественном языке и осуществлять поиск информации в этом режиме.

На данный момент популярны следующие подходы технологии иммунных систем, байесовская сеть, генетические алгоритмы, нейронные сети и так далее. Задачи, которые могут быть решены интеллектуальными информационными системами:

1. Интерпретация данных: определение смысла данных и анализ множества вариантов для достижения согласованности, и корректности результатов.
2. Диагностика: соотношение объекта с определенным классом объектов или обнаружение неисправностей в системе.
3. Мониторинг: непрерывный анализ данных в режиме реального времени и оповещение о превышении допустимых значений параметров.
4. Проектирование: подготовка спецификаций для создания «объектов» с заранее определенными свойствами.
5. Прогнозирование: возможность предсказывания последствий определенных событий или явлений на основе данных параметрической динамической модели, при которой значения параметров подбирают под заданную ситуацию.
6. Планирование: поиск планов действий к конкретным объектам, которые могут выполнять те или иные функции.
7. Обучение: выявление ошибок в процессе изучения и предоставление правильных решений, на основе накопления знаний о гипотетическом «ученике» и его типичных ошибках.

Нейронные сети обладают таким свойством и это их главное преимущество перед другими алгоритмами. Они способны выявлять сложные закономерности, между входными и выходными данными, а также осуществлять обобщение. Вследствие чего осуществлять прогнозирование на основе данных, которых не было в обучающем наборе.

1. Управление: поддержание определенного режима деятельности систем в соответствии с заданными спецификациями.
2. Поддержка принятия решений: помощь специалистам в выборе нужной альтернативы из множества выборов при принятии ответственных решений.

Интеллектуальные системы используются в данных системах информационной безопасности: биометрические системы идентификации, применяемые, например, в банковской сфере как полная или частичная

замена обычных паролей для контроля и управления доступом. При помощи нейросетевых алгоритмов обработка информации биометрической идентификации проходит в 4 этапа:

1. Получение биометрических данных пользователя путем использования сенсоров (устройств для преобразования входных сигналов);
2. Извлечение информативных биометрических характеристик;
3. Создание биометрического шаблона пользователя с использованием нейронной сети;
4. Применение решающего правила, основанного на нейронной сети.

Системы обнаружения вторжений, основанные на интеллектуальных системах, помогают обнаружить, предупредить и среагировать на инциденты с применением компьютерных атак. Системы обнаружения вторжений реализуются с использованием разных методов поиска специальных индикаторов того, что передача сетевого трафика проходит в пределах какой-либо атаки на информационную систему.

Интеллектуальные системы антивирусной защиты, равно как и системы обнаружения вторжений, используют в борьбе с вирусами метод сигнатурного анализа. Антивирусная защита сообщает о «заражении» вирусами, помогает «излечиться» от вирусов и контролирует каналы проникновения вирусов. На рис.1 представлена условная схема работы системы обнаружения вторжений.

Рис.1. схема работы системы обнаружения вторжений

Список используемых источников:

1. Авдеева И. Л., Полянин А. В., Головина Т. А. Цифровизация промышленных экономических систем: проблемы и последствия современных технологий // Известия Саратовского ун-та. Нов. сер. Сер. Экономи- ка. Управление. Право. 2019.Т. 19, вып. 3. С. 238-245.

2. Шарапова Т. Н., Селиванов С. А. Анализ угроз информационной безопасности и способы ее защиты // Наукосфера. Экономические науки. 2021. N 1(1).

3. Классификация задач, решаемых ИИС. URL: https://studfile.net/preview/7411411/page:2/ (дата обращения: 13.10.2023).

4. Advantages of Al in Cyber Security. URL: https:// www.analyticssteps.com/blogs/6-advantages-ai-cyber- security (дата обращения: 13.10.2023).

5. Роль искусственного интеллекта в кибербезопасности. URL: https://vc.ru/dev/621020-rol-iskusstvennogo-intellekta-v-kiberbezopasnosti (дата обращения: 13.10.2023).

Ermachkova M.

St. Petersburg State University of Industrial Technologies and Design

Analysis of the effectiveness of intelligent systems in information security tasks.
Technological changes taking place in the modern world are constantly increasing their speed. In the course of the digital transformation of the economy, public administration and social sphere, the construction of the information society throughout the world is being completed and the transition to a knowledge society, which cannot do without external and internal threats.

Key words: intelligent systems, information security, information theft, artificial intelligence, immune system technologies, automation, autonomous learning.

УДК 004.056
ГРНТИ 49.33.35

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ НА БАЗЕ WPA3 ENTERPRISE

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

Беспроводные технологии передачи данных, в частности Wi-Fi, широко распространены и применяются повсеместно, как в частном доме с одним или несколькими подключенными устройствами, так и в крупных компаниях с сотнями устройств. Растет не только число пользователей, но и количество и разнообразие атак. Обеспечение информационной безопасности передаваемых данных является важной задачей, особенно в корпоративных сетях, где под угрозой может оказаться секретная информация компании. Стандарт WPA3, представленный в 2018 году, является новейшим решением для защиты сетей Wi-Fi. В данной статье рассматриваются новые, в сравнении с предыдущим стандартом, механизмы, применяемые в WPA3.

WPA3 Enterprise, SAE, OWE, информационная безопасность, администрирование сети.

Wi-Fi все чаще используется в офисах, на крупных промышленных предприятиях и в бизнесе. Поскольку эта технология не ограничивает мобильность сотрудников, компании все чаще отдают ей предпочтение.

В составленном аналитиками IDC отчете за 2022 год говорится о том, что рынок WLAN вырос на 31% по сравнению с предыдущим годом. Значительный рост объясняется увеличением спроса на продукцию, поддерживающую Wi-Fi 6. Так, например, лидером в сегменте точек доступа являются занимающие 82% от всего дохода решения, поддерживающие Wi-Fi 6 [1].

Особое внимание всегда уделяется безопасности передачи данных, особенно в беспроводных сетях. Это связано с тем, что среда передачи является открытой и могут передаваться как персональные данные отдельных пользователей, так и конфиденциальная информация компании.

В настоящее время стандартом безопасности сетей Wi-Fi является Wi-Fi Protected Access 3. Этот стандарт не является обязательным для устройств, сертифицированных по стандарту Wi-Fi 5, но является встроенным для Wi-Fi 6. Поэтому безопасность современных беспроводных локальных сетей должна обеспечиваться с приоритетом использования этого стандарта. [2].

WPA3 предполагает два режима работы:

1. Personal – режим, использующий общий ключ сети для подключения;
2. Enterprise – режим, использующий для аутентификации и авторизации пользователей стандарт IEEE 802.1X. В данном режиме

предусматривается личная учетная запись для каждого пользователя. Учетная запись содержит имя и пароль, а также может содержать сертификат безопасности. Вследствие того, что в данном режиме используются уникальные УЗ, его рекомендуется использовать в корпоративных сетях [3].

Использование Enterprise режима предполагает наличие в сети структуры, представленной на рис. 1, которая состоит из трех компонентов: супликант, аутентификатор и AAA сервер, в качестве которого может быть использован RADIUS-сервер.

Рис. 6. Структурная схема WPA2 Enterprise

К основным особенностям WPA3, по сравнению с предыдущим стандартом, относятся:

- Opportunistic Wireless Encryption (OWE);
- Simultaneous Authentication of Equals (SAE);
- Easy Connect (Device Provisioning Protocol, замена WPS).

OWE – это технология, заменяющая уязвимый режим предварительного доступа с общим ключом (PSK) [4].

При OWE клиент и точка доступа (ТД) используют протокол обмена ключами Диффи-Хеллмана и получают общий секрет вместо PSK [5]. Пример процесса генерации общего секрета представлен на рис. 2.

Основная идея заключается в том, что в сообщениях Assoc Req и Assoc Reg передаются открытые ключи Диффи-Хеллмана, а затем генерируется общий секрет, который используется в последующих криптографических вычислениях.

Использование OWE обеспечивает защиту от MITM-атак и защиту управляющих кадров, однако протокол не обеспечивает аутентификацию точек доступа, что делает его уязвимым для атак типа “Honeypot” и “Evil Twin AP”. [6].

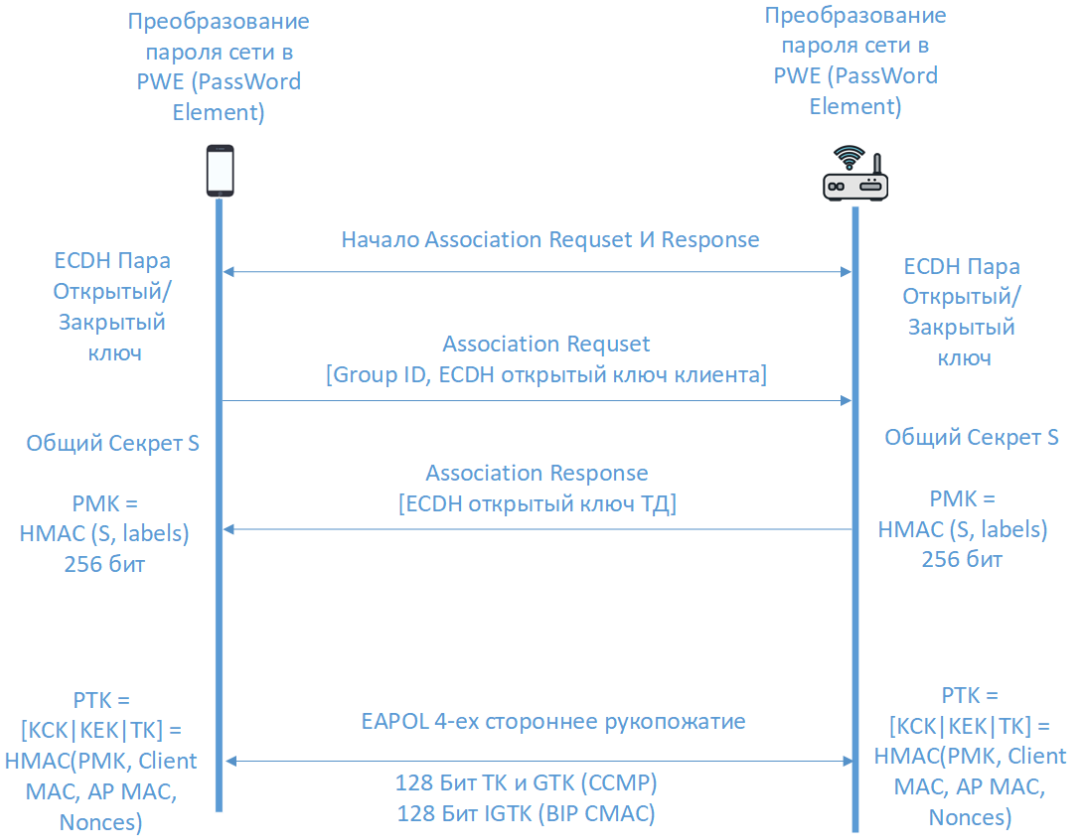


Рис. 2. Обмен сообщениям OWE

SAE (Simultaneous Authentication of Equals, SAE) – метод, основанный на протоколе Dragonfly, а именно на методе Password Authenticated Key Exchange (PAKE) и позволяет противостоять атакам по офлайн словарю на пароль сети Wi-Fi [7]. Протокол генерирует для клиентов различные ключи PMK, которые не могут быть получены даже при перехвате 4-стороннего рукопожатия.

SAE-аутентификация предназначена для ситуаций, когда аутентификация основана на паролях, которые могут быть распространены или получены потенциальным злоумышленником. С помощью SAE точка доступа в сети дополнительно аутентифицируется на основе статической пары открытого/закрытого ключей.

Ключевое отличие WPA3 от WPA2 в режиме Enterpise является опциональное усиленное 192-битное шифрование. Данный режим использует стандарт Suite B, определенный NSA (Национальным агентством безопасности) [8]. Стандарт определяет режим работы, в котором используется только определенный набор защищенных криптографических алгоритмов:

- Алгоритм шифрования – AES;
- Алгоритм обмена ключами – ECDH (эллиптическая кривая Диффи-Хеллмана);
- Алгоритм цифровой подписи – ECDSA (алгоритм цифровой подписи с эллиптической кривой);

- Алгоритмы хеширования (SHA-256 или SHA-384).

В 2018 году NSA заменило Suite B на CNSA (коммерческий пакет алгоритмов национальной безопасности – для обеспечения безопасности не менее 192 бит).

В 192-разрядном режиме WPA3-Enterprise используются следующие алгоритмы [4]:

- AES-256-GCMP – алгоритм шифрования;
- ECDH, ECDSA – получение ключей аутентификации;
- HMAC-SHA-384 – формирование KCK, KEK.

Процесс аутентификации представлен на рис. 3.

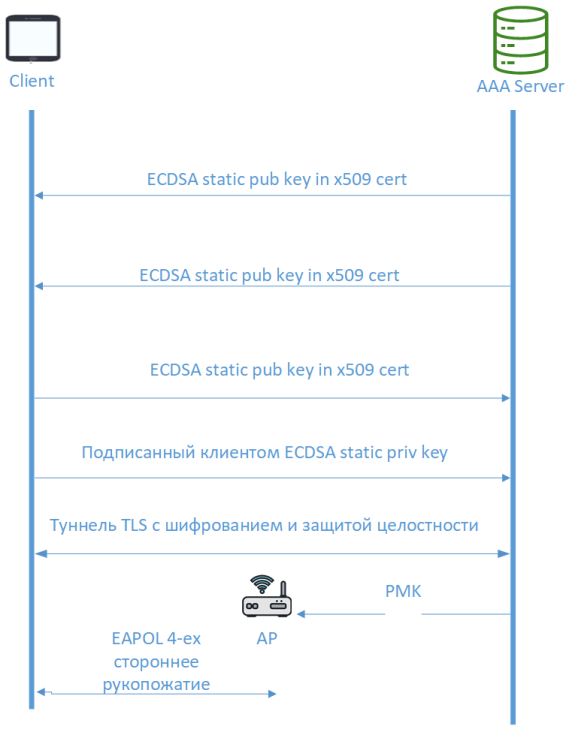


Рис. 3. Процесс аутентификации 802.1X EAP-TLS 192-бит

Таким образом, в WPA3 Enterprise, аналогично предыдущему стандарту, на этапе аутентификации 802.1X формируется PMK (Pairwise Master Key) – парный мастер ключ, который в дальнейшем участвует в вычислении парного передаточного ключа PTK на этапе 4-ех стороннего рукопожатия.

В статье рассмотрены основные особенности защиты беспроводной сети на базе WPA3. Описаны механизмы, применяемые в WPA3, а также рассмотрено ключевое отличие работы режима Enterprise в сравнении с предыдущим стандартом. Дальнейшая работа предполагает проверку возможности анализа трафика защищенного WPA3.

Список используемых источников:

1. Enterprise WLAN market growth in fourth quarter of 2022 builds on 34% growth in third quarter of 2022 2021, According to IDC [Электронный ресурс]. URL: https://www.idc.com/getdoc.jsp?containerId=prUS50475523 (дата обращения 18.10.2023).

2. Крыщенко Н. И., Миняев А. А., Ковцур М. М. Обзор методических рекомендаций по конфигурированию защищённой WLAN сети // Региональная информатика : материалы Юбилейной XVIII Санкт-Петербургской междунар. конф., Санкт-Петербург, 26-28 фев. 2022 г. СПб. : СПОИСУ, 2022. С. 554-555.

3. Kovtsur M. M., Muthanna A., Karelsky P., Kozmyan A., Voroshnin G., Al-Khafaji H. M. R. IPTV access methods with RADIUS-Server authorization // Journal of Information Technology Management. 2022. Т. 14. N 2. С. 80-89.

4. Wi-FI Alliance, WPA3™ Specification Version 3.1, 2019.

5. RFC 8110, Opportunistic Wireless Encryption, 2017.

6. Юркин Д. Ю., Ворошнин Г. Е., Ковцур М. М., Мисливский Б. С. Исследование влияния атак Arpinject и Associationflood в беспроводных сетях на базе оборудования Mikrotik // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. N 1. С. 44-48.

7. RFC 7664, Dragonfly Key Exchange, 2015.

8. National Security Agency (NSA) Suite B Cryptography [Электронный ресурс]. URL: https://www.ibm.com/docs/en/ibm-mq/9.2?topic=tls-national-security-agency-nsa-suite-b-cryptography (дата обращения 20.10.2023).

Zebzeev Y.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Research of the features of wireless network protection based on WPA3 Enterprise/
Wireless data transmission technologies, especially Wi-Fi, are widespread and used everywhere, both in a private home with one or more connected devices, and in large companies with hundreds of devices. Ensuring the information security of the transmitted data is an important task, especially in corporate networks, where the company's secret information may be at risk. The WPA3 standard, introduced in 2018, is the latest solution for protecting Wi-Fi networks. This article discusses the new mechanisms used in WPA3 in comparison with the previous standard.

Key words: WPA 3 Enterprise, SAE, OWE, information security, network administration.

УДК 004.056.53
ГРАНТИ 81.93.29

ИССЛЕДОВАНИЕ ОСНОВНЫХ ФУНКЦИЙ ПОСТРОЕНИЯ MAXPATROL SIEM

Ю. А. Иванилова, И.А. Ушаков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

На протяжении многих лет основным инструментом выявления инцидентов информационной безопасности остаются SIEM-системы. В статье описаны основные инструменты отечественной SIEM-системы MaxPatrol.

SIEM-система, MaxPatrol SIEM, инциденты информационной безопасности, события безопасности, атака

С каждым годом атаки злоумышленников становятся сложнее и запутаннее, что приводит к необходимости совершенствования способов обнаружения, анализа и реагирования на инциденты безопасности. В этом контексте системы управления информационной безопасностью (SIEM) становятся важным компонентом защиты организаций [1].

По данным исследований Positive Technologies за первые девять месяцев 2023 года, в сравнении с показателями за весь 2022 год, количество проектов по расследованию инцидентов информационной безопасности выросло на 76%.

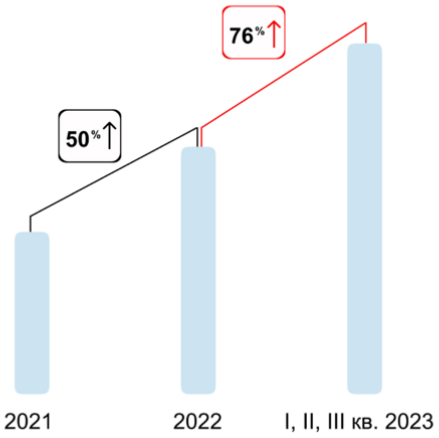


Рис. 1. Количество проектов по расследованию инцидентов в 2021-м, 2022-м и за I—III квартал 2023 года

Большинство организаций (69%), в отношении которых производились атаки – госучреждения, а также промышленные, финансовые и ИТ-компании. Значительная часть расследованных атак носили целенаправленный характер, то есть злоумышленники ставили своей целью нанести ущерб именно конкретной компании [2].

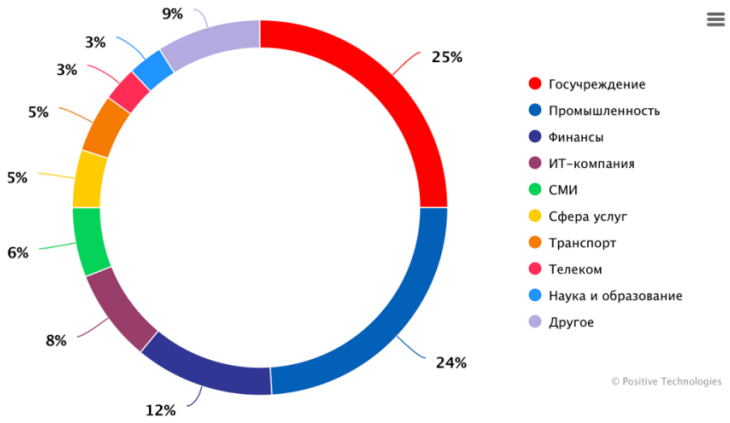


Рис. 2. Распределение организаций-жертв по отраслям

На протяжении многих лет основным инструментов для выявления инцидентов информационной безопасности является система класса SIEM. SIEM (Security information and event management) – класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности. В качестве источников информации для SIEM-решений могут выступать:

- антивирусные программы;
- системы авторизации и аутентификации;
- межсетевые экраны, брендмауэры;
- журналы сетевого оборудования, серверов и рабочих станций;
- контроллеры домена;
- системы обнаружения и предотвращения вторжений (IDS/IPS);
- DLP-системы.

SIEM-системы необходимы для сбора огромного количества событий информационной безопасности, нормализации данных и сравнения между собой по правилам корреляции.

Процесс управления инцидентами информационной безопасности можно разделить на 4 этапа: подготовка, выявление инцидента ИБ, реагирование и анализ последствий [3].

Рис. 3. Процесс управления инцидентами

MaxPatrol SIEM — инновационная система детектирования киберугроз и атак. Она обеспечивает полномасштабную экспертизу информационной безопасности и прозрачность IT-инфраструктуры. Высокая точность выявления инцидинтов достигается за счет периодического получения экспертных данных PositiveTechnologies, раскрывающих методы обнаружения актуальных типов кибератак.

Шаг 1. Подготовка.

Данный этап включает в себя установку SIEM-систем, настройку прав корреляции, прав доступа и многое другое. MaxPatrol SIEM также предлагает сервис M-Scan, который предназначен для проверки файлов на вирусы. M-Scan анализирует данные из трафика, электронной почты, облачных хранилищ. И Network Attack Discovery Sensor, который позволяет контролировать действия в сети. При попытке несанкционированного вторжения или кражи данных, система оповещает администратора в режиме онлайн.

Шаг 2. Выявление инцидента информационной безопасности.

На этом этапе осуществляется идентификация, выявление и регистрация инцидента ИБ.

SIEM-система MaxPatrol позволяют осуществлять централизованный сбор и анализ по заранее заданным правилам корреляции событий информационной безопасности. В случаях, когда правил корреляции не достаточно для точного ответа, является ли событие инцидентом ИБ, оператор переходит к анализу карточки события, алертов с хостами, файлами и другими процессами. Контекстные экшены MaxPatrol позволяют аналитику быстро перейти во внешнюю систему, например, в сервисы, анализирующие сетевой трафик, и другие репутационные сервисы.

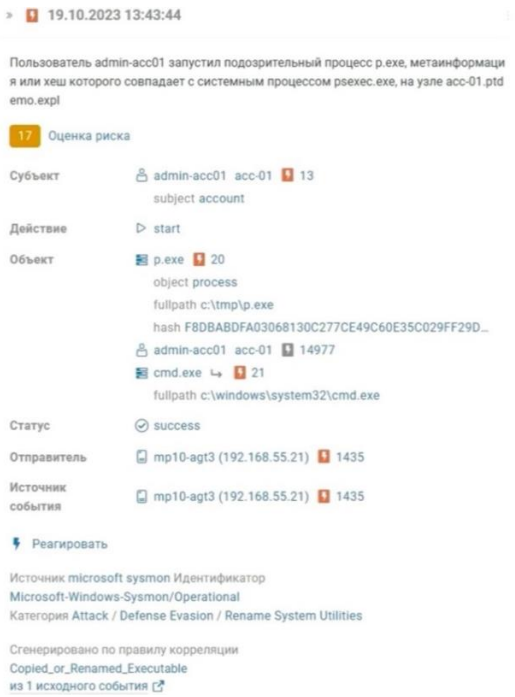


Рис. 4. Карточка события MaxPatrol SIEM

Дополнительный инструмент выявления инцидентов MaxPatrol SIEM – BAD (Behavioral Anomaly Detection) – функция, основанная на машинном обучении. BAD не зависимо от правил корреляции выявляет аномалии в поведении хоста и дает оценку события. Таким образом аналитик получает «второе мнение» в оценке безопасности.

Шаг 3. Реагирование на инцидент ИБ.

Этот шаг, как правило состоит из нескольких этапов: локализация инцидента, выявление, анализ и ликвидация последствий.

При использовании решения MaxPatrol EDR аналитики могут среагировать на инцидент напрямую из карточки события изолировав хост, остановив вредоносный процесс или удалив пакеты.

Шаг 4. Анализ последствий инцидента.

Заключительным шагам является составление и реализация рекомендаций по доработке системы защиты. Кроме того, необходимо провести анализ предпринятых действий для предотвращения повторных инцидентов ИБ и улучшения эффективности реагирования на них [1].

В случае если событие не являлось инцидентом ИБ необходимо откорректировать правило корреляции, то есть ввести в него исключения.

Управление инцидентами информационной безопасности является одним из основополагающих элементов системы защиты информации. Корректно выстроенный процесс позволяет значительно снизить вероятность повторения инцидентов ИБ, а также возникновения новых. MaxPatrol SIEM обладает мощными инструментами для обеспечения безопасности информационных систем. Ее возможности в обнаружении угроз и реагировании на них позволяют организациям эффективно бороться с современными кибератаками и обеспечивать надежную защиту своих данных.

Список используемых источников:

1. MaxPatrol Security Information and Event Management, Свидетельство о регистрации программы для ЭВМ 2016616938, 22.06.2016. Заявка № 2016614275 от 26.04.2016.
2. Итоги расследований инцидентов ИБ в 2021–2023 годах [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/outcomes-of-IS-incident-investigations-in-2021-2023-years/#id5 (дата обращения: 20.10.2023)
3. Инциденты информационной безопасности: выявление, расследование и реагирование [Электронный ресурс]. URL: https://selectel.ru/blog/security-incidents/ (дата обращения: 20.10.2023)
4. Васильева И. Н. Расследование инцидентов информационной безопасности : учеб. пособие. СПб. : СПбГЭУ, 2019. 113 с.
5. MaxPatrol Security Information and Event Management, Свидетельство о регистрации программы для ЭВМ 2016616938, 22.06.2016. Заявка № 2016614275 от 26.04.2016.
6. Филяк П. Ю. Обеспечение безопасности при работе в интернет на основе анализа с использованием сертифицированных решений MaxPatrol / Филяк П.Ю.,

Байларли Э.Э., Мухин И.Н., Ибрагимов У.Ж.У. // Информация и безопасность. 2018. Т. 21. N 4. С. 524-529.

Ivanilova J., Ushakov I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Investigation of main functions of building MaxPatrol SIEM.

For many years, SIEM systems have remained the main tool for detecting information security incidents. The article describes the main tools of the domestic SIEM system MaxPatrol.

Key words: SIEM system, MaxPatrol SIEM, information security incidents, security events, attack.

УДК 004.056
ГРНТИ 81.93.29

РАЗРАБОТКА ВИРТУАЛЬНОГО СТЕНДА ДЛЯ АНАЛИЗА МЕТРИК БЕЗОПАСНОСТИ ВИРТУАЛЬНЫХ МАШИН И КОНТЕЙНЕРОВ

Д. А. Игнатьева, А. О. Камалова, И. Е. Пестов, Е. О. Романюк
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Технологии контейнеризации пользуются популярностью в современном мире. Количество возможных атак на контейнеры тоже увеличивается. Поэтому специалисты пользуются метриками контейнеров для отслеживания информации о состоянии контейнеров.

виртуализация, метрики, Kubernetes, docker

В настоящее время контейнеры используются практически в каждой компании для тестирования и развертывания приложений. Контейнеры помогают компаниям модернизироваться и облегчают масштабирование и развертывание приложений, но в то же время контейнеры создали новые задачи, создав совершенно новую инфраструктурную экосистему [1].

Ежедневно в компаниях разворачивают тысячи контейнерных экземпляров, которыми требуется управлять. Для оркестрации контейнеров используется платформа Kubernetes [2].

Kubernetes - это платформа с открытым исходным кодом, предназначенная для автоматизации развертывания, масштабирования и управления контейнерными приложениями.

С помощью Kubernetes [3] можно управлять следующими действиями:

- контролировать потребления ресурсов по приложениям;
- равномерно распределять нагрузки приложения на инфраструктуру;
- создавать автоматические запросы балансировки нагрузки в различных экземплярах приложения;
- выполнять мониторинг потребления ресурсов и ограничений ресурсов для автоматического остановки приложений от потребления слишком большого количества ресурсов и повторного перезапуска приложений [4];
- перемещать экземпляры приложения с одного хоста на другой, если на хосте не хватает ресурсов;
- автоматически использовать дополнительные ресурсы, доступные при добавлении нового хоста в кластер.

Для того, чтобы отслеживать метрики в Kubernetes и видеть обзорные панели на основании этих метрик есть возможность настроить сервер метрик [5]. Сервер метрик - это масштабируемый, эффективный источник метрик контейнерных ресурсов для встроенных конвейеров автомасштабирования Kubernetes.

Также при использовании Kubernetes следует выполнять его мониторинг. Мониторинг предоставляет следующие преимущества:

- устранение неполадок и надежность: приложения Kubernetes часто сложны, особенно если они основаны на облаке или используют архитектуру микросервисов, это затрудняет выявление первопричины проблем. Меры мониторинга могут предложить видимость развертывания Kubernetes, чтобы можно было видеть, где могут возникнуть (или возникли) проблемы, что позволяет предотвращать и устранять проблемы.
- настройка производительности;
- управление затратами: важно следить за ресурсами, которые потребляются, чтобы убедиться, что отсутствует их перерасход.
- безопасность: важная возможность в современной вычислительной среде заключается в том, чтобы видеть, какие задания выполняются и где, это позволяет идентифицировать несанкционированные или ненужные задания, которые могут указывать на нарушение или атаку DOS. Хотя мониторинг Kubernetes не решит все проблемы безопасности, он может предоставить важную информацию для поддержания безопасности.

Для отслеживания метрик была выполнена установка minikube на операционную систему Linux (Ubuntu). Minikube - это легкая реализация Kubernetes, которая создает виртуальную машину на вашей локальной машине и развертывает простой кластер, содержащий только один узел.

Сперва была выполнена установка Docker и запущен docker.service. С помощью команды systemctl status docker выполнена проверка состояния его работы (рис. 1).

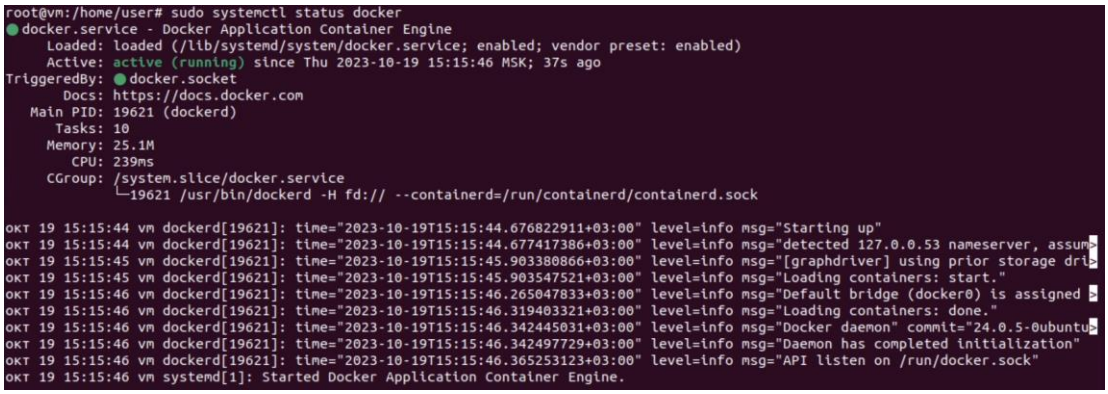


Рис. 7. Проверка статуса docker.service

После чего была выполнена установка и запущено приложение minikube (рис. 2). При запуске программы был применен параметр - force для того, чтобы разрешить minikube выполнять потенциально опасные операции.

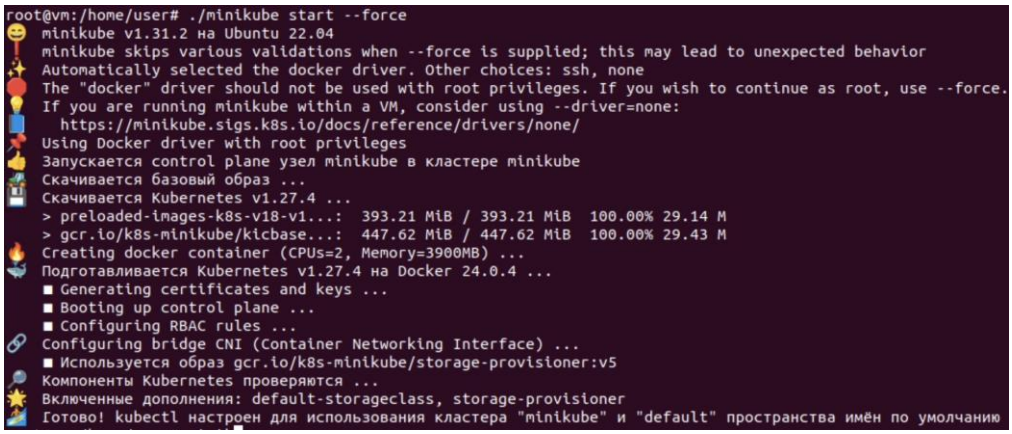


Рис. 8. Запуск minikube

Далее запущено приложение в контейнере, у которого должны отслеживаться метрики. Для примера было выбрано приложение OWASP JuiceShop – заведомо уязвимое приложение.

После установки minikube активирована обзорная панель, в котором можно наблюдать за метриками, графический интерфейс обзорной панели показан на рис. 3.

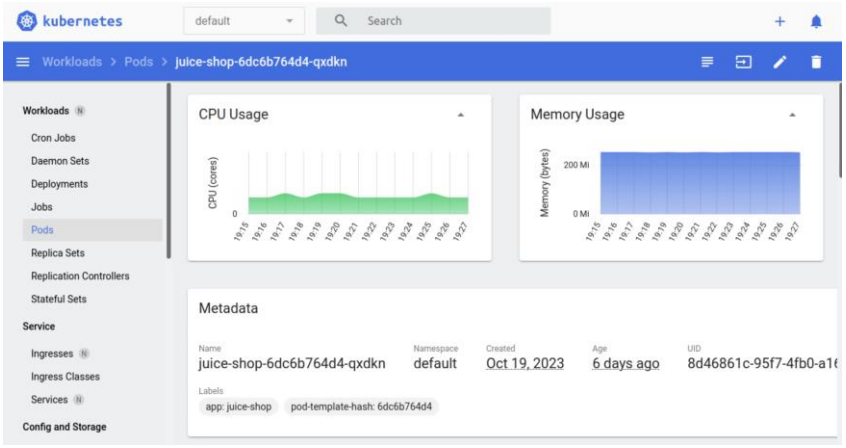


Рис. 9. Графический интерфейс обзорной панели

Для более удобного представления получаемых метрик дополнительно установлен Prometheus [6] и Grafana [7][8]. Prometheus – это программное решение с открытым исходным кодом для мониторинга для сбора и агрегирования метрик в виде временных рядов данных. Grafana — это платформа с открытым исходным кодом для визуализации, мониторинга и анализа данных. Для отслеживания метрик были выбраны эти программы, потому что они имеют открытый исходный код (open source), постоянно обновляются и поддерживаются разработчиками, а также их легко можно установить и настроить в своей системе.

Таким образом, для отслеживания метрик и для проведения сравнительного анализа метрик безопасности используется Grafana и Prometheus (рис. 4).

Рис. 10. Обзорная панель в Grafana

Список используемых источников:

1. Гурбатов Г. О., Паничев А. Д., Ушаков И. А. Обеспечение безопасности Kubernetes // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы X Междунар. науч.-технич. и науч.-методич. конф., Санкт-Петербург, 24–25 фев. 2021 г. СПб. : СПбГУТ, 2021. С. 282-286.

2. Загребаев Д. К. Мониторинг кластера анализа больших данных Apache Spark на основе Kubernetes // Достижения науки и образования. 2019. N 5(46). С. 34-42.

3. Гурбатов Г. О., Паничев А. Д., Ушаков И. А. Сравнительный анализ IAAS (Openstack) и PAAS (Openshift) // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы IX Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 26–27 фев. 2020 г. Т. 2. СПб. : СПбГУТ, 2020. С. 272-276.

4. Фомин С. П., Швидкий А. А. Анализ механизмов поддержки состояния инфраструктуры облачного сервиса // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы XII Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 28 фев. – 01 марта 2023 г. Т. 1. СПб. : СПбГУТ, 2023. С. 922-926.

5. Дедухова А. А., Швидкий А. А. Сравнительная оценка систем мониторинга компонентов облачной инфраструктуры // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы X Междунар. науч.-технич. и науч.-методич. конф., Санкт-Петербург, 24–25 фев. 2021 г. СПб. : СПбГУТ, 2021. С. 292-296.

6. Prometheus [Электронный ресурс]. URL: https://prometheus.io (дата обращения: 27.10.2023).

7. Grafana [Электронный ресурс]. URL: https://grafana.com (дата обращения 27.10.2023).

8. Яремчук С. Ставим мониторинг Prometheus + Grafana // Системный администратор. 2017. N 5(174). С. 36-44.

Ignatieva D., Kamalova A., Pestov I, Romanyuk E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development of a virtual stand for analyzing the security metrics of virtual machines and containers.

Containerization technologies take advantage of the modern world. The number of possible attacks against containers is also increasing. Therefore, experts use container metrics to record information about the state of containers.

Key words: virtualization, metrics, Kubernetes, docker.

УДК 004.056
ГРНТИ 81.93.29

ПЕРСПЕКТИВЫ РАЗВИТИЯ УСТРОЙСТВ НА БАЗЕ ТЕХНОЛОГИИ NFC

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

В настоящее время количество технологий использующих радио сигналы и созданных для беспроводной работы с устройствами весьма многочисленно, однако их количество будет лишь возрастать В данном исследовании рассмотрены основные принципы её работы и характерные особенности самой технологии NFC. После определения основных направлений применения технологии, будут подробно описано каждое из них. В заключение будет сказано о тенденции развития технологии NFC и напрвылениях её внедрения в России.

безопасность, радиосвязь, NFC, развитие NFC

Проблема быстрого обмена данными без настройки сетей или специальных устройств передачи информации остро встала в последнее время в связи с развитием общества. Появилась потребность сокращать время оплаты проездов, совершение безналичных расчётов, создание системы пропускного режима на предприятии и многого другого. Одна из технологий, позволивших решить такие задачи – это технология NFC (Near Field Communication), или как её ещё называют «технология ближнего поля» или «связь ближнего действия».

NFC представляет собой технологию беспроводной высокочастотной связи. Поскольку используется спектр частот около 13 МГц, то и дальность действия, как правило, не превышает десятка сантиметров. Существуют и более редкие системы, позволяющие совершать обмен информацией на расстоянии до 40 или даже 50 сантиметров.

Ниже будут рассмотрены самые распространённые области применения NFC:

1) Безналичная оплата картой

Безналичная оплата с помощью пластиковой карты с чипом была возможна ещё несколько десятилетий назад, однако старые карты не имели модуля ближнего поля, и, как следствие, оплата должна была происходить через физический контакт чипа и считывающего устройства.

Недостатки способа произведения транзакций:

- Механический износ контактов. Карта могла приходить в негодность после длительного использования.
- Необходимость обязательного введения ПИН-кода при любых, даже небольших покупках, что существенно замедляло процесс оплаты.

Использование новых беспроводных технологий во много ускорило и упросило процесс совершения оплаты. Однако, ряд проблем остался, а так же появились, другие. Среди них:

- Отсутствие терминалов, поддерживающих технологию ближайшего поля.
- Возможность кражи денежных средств через фальшивый терминал (накладной терминал в случае контактной карты и специальный мошеннический терминал дальнего радиуса действия для карт с технологией NFC).

2) Мобильные платежи

Если смартфон пользователя имеет модуль NFC, то установив специальное приложение и записав в него свою карту, можно совершать бесконтактные платежи. По сути, оплата таким образом мало отличается от бесконтактной оплаты картой, однако даёт ряд преимуществ. Среди них:

- Возможность подключения нескольких карт.
- Возможность использования нескольких платёжных систем.
- Безопасность. В отличии от карты, которая работает всегда, NFC модуль активен только при включении. Таким образом, если не забывать выключать его, возможность кражи средств через мошеннические терминалы становится невозможной.

3) Сопряжение устройств Bluetooth

Поскольку процесс сопряжения устройств бывает крайне сложен и длителен, была придумана технология установления доверительного соединения с помощью технологии коммуникации ближнего поля. Близкое расположение устройств позволяет так же обеспечить и высокую скорость передачи информации.

4) Метка-имплантат

Из множества идей писателей фантастов многие доступны уже сегодня. Одна их таких – подкожные чипы. Данные метки являются мало распространённым явлением среди людей. Импланты представляют из себя маленькие стеклянные цилиндры, длинной около сантиметра. Они не требуют зарядки или какой-либо смены компонентов внутри себя, а потому не требуют обслуживания. Широкое распространение они получили в животноводстве. Коровы и иные домашние животные на фермах помечаются, что позволяет следить за каждым животным и выдавать пищу и лекарства не путаясь. Так же метки используются для того, что бы потерявшееся животное можно было вернуть владельцу, считав персональную информацию фладельца.

5) Средства авторизации и идентификации

Вторая по распространённости на сегодняшний день область применения технологии NFC это устройства доступа и авторизации. Ключи для открытия ворот, электронные карты и пропуска на предприятиях или в учебных заведениях, специальные ключи авторизации доступа к защищённым компьютерным системам и многое другое – построено на базе

беспроводных технологий ближнего поля. Такие системы крайне просты для пользователей, но при этом позволяют вести учёт событий внутри системы, а так же существуют возможности защиты и создания сложных систем безопасности, которые не позволят копировать ключи карты.

На практике данное решение выглядит следующим образом:

- Пользователь включает рабочую станцию.
- При загрузке операционной системы запускается специализированное программное обеспечение, позволяющее аутентифицироваться на данной рабочей станции с помощью мобильного телефона со встроенным модулем NFC.
- При запуске специализированного ПО, инициализируется модуль NFC, подключенный к рабочей станции.
- Пользователь запускает на мобильном телефоне приложение для аутентификации через NFC, подносит его к NFC-модулю рабочей станции и вводит PIN-код.
- Приложение проверяет PIN-код, введенный пользователем, и в случае, если он введен, верно, активирует модуль NFC.
- Поле, создаваемое модулем NFC рабочей станции, обнаруживает мобильное устройство, работающее в режиме эмуляции смарт-карты, проверяет, что данное устройство находится в списке разрешенных, и аутентифицирует пользователя на рабочей станции.

6) Настройка устройств по NFC

Последняя, и самая мало распространённая область применения NFC технологии, это настройка и задание параметров устройствам. В повседневной жизни существует множество настраиваемых устройств, параметры которых необходимо задавать лишь единожды. Например, при покупке и установке такового. Это могут быть коммунальные или бытовые устройства, такие как: средства обогрева, устройства освещения, системы полива растений, или иные программно-аппаратные комплексы, работа с которыми производится мало квалифицированными сотрудниками. Среди главных преимуществ применения такой технологии будут:

- Низкая стоимость устройства. Поскольку задание настроек на устройстве возможно несколькими способами рассмотрим некоторые из них: встроенные физические компоненты управления механического воздействия – встречаются в большинстве устройств и обычно представлены в виде рычажка переключателя режимов, или реже кнопок. Механические компоненты усложняют конструкцию и приводят к необходимости создания более сложной модели расположения частей внутри готового устройства. Так же наличие дополнительных частей уже само по себе приводит к увеличению стоимости готового продукта; встроенные радио модули на базе технологии wifi или bluetooth – их стоимость намного больше, чем NFC модулей, иногда в несколько десятков раз. Некоторые платы уже содержат в себе NFC модуль и не потребуют никаких дополнительных вложений вообще.

•Простота эксплуатации. Настройка по wifi или bluetooth требует сложной системы подключения, что зачастую делает эксплуатацию невозможной ввиду низкой квалификации конечного пользователя (настройщика). Так же в случае если система подразумевает целую систему таких устройств, это приведёт к проблемам связанным с созданием единой сети продуктов, что так же невозможно на практике.

•Нулевая энергозатратность. Метка NFC не требует никакого питания, кроме поля от устройства задающего или считывающего параметры, например телефона.

Технологии бесконтактной оплаты уже созданы, и их развитие будет идти по пути увеличения защищённости, что является узким направлением. Технологии вживляемых меток не будут широко применяться в обозримом будущем из-за этических норм и правил, кроме уже имеющегося чипирования животных. Технология авторизации развивается, усложняется, однако уже который год остаётся одной из самых востребованных и перспективных. А вот технология настройки параметров устройств практически не получила распространения в России, и потому является одним из потенциально востребованных сегментов рынка.

Список используемых источников:

1. Рабинович А. С., Казарин О. В. Методика аутентификации пользователя в информационной системе с использованием технологии nfc // Вопросы кибербезопасности. 2022. N 4. С. 59-62

2. Ревазов Х. Ю., Тавасиев Д. А., Команов П. А. Основной принцип работы NFC-устройств и их безопасность // Инновационная наука. 2020. N 1. С. 23-25.

3. Козырь Н. С., Гетманова А. В. Бесконтактная технология MasterCard PayPass и перспективы ее развития в России // Финансы и кредит. 2015. N 4. С. 44-54

4. Карельский П. В., Ковцур М. М., Штеренберг С. И., Малинин Н. И. Анализ современных средств автоматизированной проверки функций безопасности коммутационного оборудования // Информационная безопасность регионов России : материалы XII Санкт-Петербургской межрегион. конф., Санкт-Петербург, 27-29 нояб. 2021 г. СПб. : СПОИСУ, 2021. С. 385-386

5. Ковцур М. М., Симанов М. С. Анализ особенностей организации авторизации пользователей в сетях коллективного доступа стандарта ieee 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VIII Междунар. науч.-технич. и науч.-методич. конф., Санкт-Петербург, 27–28 фев. 2019 г. Т. 1. СПб. : СПбГУТ, 2019. С. 537-541.

Ilin Y.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Prospects for the development of devices based on nfc technology.

Currently, the number of technologies using radio signals and created for wireless operation with devices is very numerous, but their number will only increase. This study examines the main characteristic features of technology itself and the principle of its operation. After determining the main areas of application of the technology, each of them will be described in more detail. In conclusion, it is said about the trend in the development of near-field technology and the prospects for its implementation in Russia.

Key words: Security, Radio communication, NFC.

УДК 004.056
ГРНТИ 81.93.29

УГРОЗЫ СЕТЕВОЙ БЕЗОПАСНОСТИ В СФЕРЕ ВЫСШЕГО ОБРАЗОВАНИЯ

А. А. Казанцев, А. С. Махорин
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В последние несколько лет значительно изменилось то, как работают высшие учебные заведения по всему миру. Применение средств дистанционного обучения стало уникальной возможностью для процесса дальнейшего образования. Это усилило угрозы информационной безопасности в сфере образования в целом и вузов в частности. Чтобы выявить самые большие угрозы для вузов, было проанализировано несколько отчетов по безопасности и научных статей.

кибербезопасность, онлайн-образование, кибератаки, электронное обучение

Введение

Сегодня информационные технологии широко используются вместо традиционных часов обучения. Современные технологии, такие как онлайн-платформы для обучения, приложения для видеоконференций, веб-сайты и облачные вычисления, помогают людям получать необходимые знания. Согласно последним исследованиям, рынок онлайн-образования ожидает роста на 16,4% каждый год. Как студенты, так и сотрудники университетов должны приспосабливаться к новым условиям, чтобы обеспечить непрерывность образовательного процесса.

Онлайн-образование привело к существенному увеличению кибератак. Согласно опросу, проведенному Kaspersky Lab, 41% организаций в образовательной сфере в 2022 году стали жертвами кибератак, а 36% из них потеряли конфиденциальные данные.

В условиях дистанционного обучения стало необходимым адаптировать приложения для обучения к требованиям информационной безопасности, а также обеспечивать минимальные требования безопасности домашних сетей студентов. Эти меры обеспечивают доступность, конфиденциальность и целостность передаваемой информации.

В этой статье мы рассмотрим данные исследований, отражающих угрозы кибербезопасности для высших учебных заведений на основе нескольких отчетов за период 2020-2022 годов. Наша цель - показать, что онлайн-деятельность университетов увеличила риски кибератак. Использование платформ онлайн-обучения, приложений для видеоконференций и централизованных хранилищ данных в сетях университетов, а также участие в интенсивной коммуникации по электронной почте создали новые возможности для несанкционированного доступа к сетям университетов и конфиденциальным данным. Мы проведем анализ данных исследований, чтобы дать более полное представление об этой проблеме.

1. Кибербезопасность и образование

Высшие учебные заведения (ВУЗы) становятся целью кибератак из-за хранимой ими информации. Информация, которая представляет интерес для злоумышленников, включает:

- Интеллектуальную собственность
- Личные данные студентов, включая материалы диссертации, а также результаты экзаменов
- Данные исследований также представляют собой серьезную уязвимость

Таким образом, можно сказать, что количество киберугроз в ВУЗах значительно возросло с 2020 года благодаря дистанционному обучению, которое позволило сохранить непрерывность образовательного процесса в ВУЗах. Детальный анализ угроз позволит выявить риски и разработать эффективные стратегии для защиты сетей университетов и их пользователей. Наибольшими угрозами в образовательной сфере являются вредоносные программы, DoS/DDoS атаки и фишинг [1].

1.1 Атаки вредоносных программ

Из отчета, опубликованного Microsoft Security Intelligence, следует, что образовательная сфера стала наиболее уязвимой к кибератакам в сравнении с другими отраслями, и на ее долю приходится 61% из 7,7 млн атак зафиксированных за последние 30 дней. Отчет компании Jisk, специализирующейся на анализе кибербезопасности в образовательной сфере, подтверждает первенство инфицирования вредоносными программами в данной отрасли. Вредоносная программа, которая больше всего нацелилась на образовательную - это программное обеспечение-вымогатель. Вредоносное программное обеспечение, известное также как "рансомваре", используется хакерами для ограничения доступа авторизованных пользователей, таких как студенты или сотрудники университета, путем шифрования дисков и требования оплаты для дешифровки данных.

Сети университетов предназначены для предоставления образовательных услуг студентам, но они также могут быть использованы злоумышленниками для атак на авторизованных пользователей и получения доступа к сети [2]. После вторжения злоумышленник может шифровать диски, ограничивая доступ легитимных пользователей к ресурсам. Администраторам остается только выбрать один из вариантов: выплатить требуемую сумму, чтобы получить доступ к данным, восстановить данные из резервной копии, потерять данные или взломать ключ шифрования методом перебора. Как правило, злоумышленники требуют оплату биткоинами, так как это позволяет им обойти финансовые учреждения. Однако восстановление данных из резервной копии также может быть проблематичным, так как программы-вымогатели могут искать резервные копии на дисках, чтобы зашифровать их, и в этом случае восстановление

данных не всегда возможно. Взлом ключей шифрования является очень сложным процессом, который может занимать годы.

1.2. DoS/DDoS атаки

Согласно опубликованному отчету от компании Kaspersky, количество атак типа DOS/DDoS в образовательной сфере увеличилось на 350-500% с начала 2020 года. Увеличение числа DoS/DDoS атак в основном связано с переходом на дистанционное обучение, так как большинство университетских сервисов, таких как доступ к библиотеке, расписание учебных занятий, доступ к учебным ресурсам, экзамены, оценки и поступление на учебу, частично перешли в онлайн среду, и нарушение этих сервисов может привести к серьезным проблемам в академической деятельности. Это заявление подтверждается экспертами из Kaspersky, которые утверждают, что увеличение атак DoS/DDoS в сфере образования, которое можно увидеть на рис. 1, обусловлено переходом на дистанционное обучение.

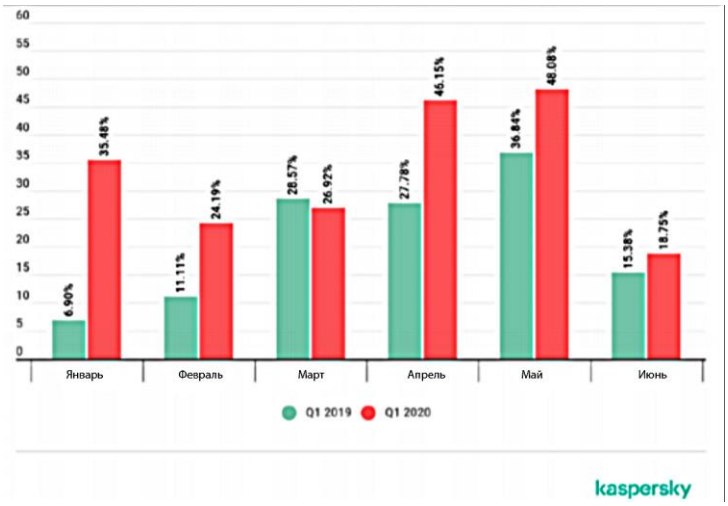


Рис. 22. Количество DDoS-атак, которые повлияли на образовательные ресурсы в 2020 году по сравнению с тем же периодом в 2019 году

В большинстве случаев целью являются:

- У каждого университета есть хотя бы один веб-сервер, который содержит информацию о студентах и сотрудниках, такую как персональные данные, академическая информация и расписание занятий. Нарушение доступа к этой информации может привести к серьезным последствиям, таким как утечка личных данных и изменение академических записей, что может серьезно повлиять на учебный процесс и вызвать проблемы для авторизованных пользователей. [3]
- Конечные устройства и сетевые устройства, такие как коммутаторы и маршрутизаторы, также могут стать целью атак DoS/DDoS. Блокировка сетевых устройств может привести к невозможности доступа к онлайн-платформам обучения, виртуальным лабораториям или другим университетским услугам, предоставляемым онлайн. В области облачных

вычислений атака DDoS может существенно снизить производительность облачных сервисов, повредив виртуальные серверы.

Атаки DoS/DDoS на ВУЗы нацелены на прерывание доступа к образовательным ресурсам, особенно во время важных мероприятий, таких как экзамены или конкурсы. Это говорит о том, что с переходом на дистанционное обучение атаки DoS/DDoS стали более актуальными, поскольку доступность университетских сервисов стала еще более важной.

1.3. Фишинговые атаки

Киберугрозы в области высшего образования включают множество угроз, однако особенно опасными являются атаки фишинга. Согласно исследованию, проведенному компанией Barracuda Networks в период с июня по сентябрь 2020 года, высшие учебные заведения стали целью более чем 3,5 миллиона атак фишинга. Более 25% всех атак фишинга были направлены именно на образовательный сектор.

Самыми распространенными векторами атак являются:

- Атаки на основе электронной почты, где злоумышленник замаскировывает электронные письма таким образом, чтобы они выглядели как законный запрос на предоставление личной и конфиденциальной информации [4]. Электронные письма, отправленные со схожими характеристиками, такие как фишинговые письма, представляют угрозу безопасности данных студентов и персонала вуза. В этих электронных письмах может содержаться зловредное ПО, которое может заразить персональные устройства пользователей и похитить их личные данные, такие как пароли, логины и банковские реквизиты.
- Приложения для видеоконференций стали новой мишенью для атак фишинга в связи с повышенным спросом на дистанционные формы обучения в период пандемии. Согласно исследованию Check Point Research, за период с конца апреля по середину июня 2020 года было зарегистрировано около 2449 доменов, связанных с платформой Zoom, из которых 32 были вредоносными, а 320 вызывали подозрение. Эти домены использовались для распространения вирусов, получения доступа к учетным записям пользователей и других видов мошенничества.
- Атаки на сетевую инфраструктуру университетов, такие как DDoS-атаки или кибершпионаж, которые могут привести к сбоям в работе сетевых сервисов и утечке конфиденциальной информации [6].

2. Известные случаи кибератак на ВУЗы России

- В 2020 году на сайт МГУ была проведена масштабная DDoS-атака, которая привела к его недоступности. В результате атаки была заблокирована система электронных анкет для поступления в вуз.
- В 2021 году на сайт СПбГУ была проведена атака типа "SQL Injection". Взломщики смогли получить доступ к базе данных студентов, которая содержала персональные данные и информацию об успеваемости.

•В 2020 году на сайт НИУ ВШЭ была проведена атака типа "Phishing". Вредоносный сайт, который был создан злоумышленниками, копировал официальный сайт вуза и собирал данные авторизации студентов.

•В 2019 году на сайт Университета ИТМО была проведена атака типа "Ransomware". Взломщики зашифровали базу данных университета и требовали выкуп в размере 150 тысяч долларов.

•В 2018 году на сайт Московского института физики и технологии была проведена атака типа "Brute-force". Взломщики попытались получить доступ к системе управления сайтом, перебирая все возможные пароли.

•В 2017 году на сайт МФТИ была проведена атака типа "Advanced Persistent Threat". Злоумышленники использовали уязвимость в системе электронной почты и получили доступ к переписке профессоров и ученых вуза.

•В 2016 году на сайт СГУ была проведена атака типа "DoS". Атака привела к временной недоступности сайта вуза, что затруднило доступ к онлайн-библиотеке и другим электронным сервисам.

3. Рекомендации

Эксперты отмечают, что проблема кибербезопасности в сфере высшего образования России связана с недостаточным вниманием к этому вопросу со стороны университетов. Многие из них не вкладывают достаточных средств и ресурсов для защиты своей сетевой инфраструктуры [7].

Кроме того, часто студенты и сотрудники университетов не соблюдают базовые меры безопасности, такие как использование надежных паролей и защита от фишинг-атак.

Для решения проблемы кибербезопасности в сфере высшего образования России необходимо создать специальные команды по кибербезопасности в университетах, проводить обучение и регулярное тестирование на безопасность, а также разрабатывать и реализовывать стратегии защиты данных.

Заключение

Анализируя несколько международных отчетов по кибербезопасности, было возможно выявить наиболее актуальные угрозы кибербезопасности в высших учебных заведениях. Личные данные студентов/сотрудников, интеллектуальная собственность и результаты исследований вызывают повышенный интерес хаккеров. Таким образом, были выявлены наиболее распространенные атаки с использованием вредоносных программ, атаки типа DoS/DDoS и фишинг. С начала пандемии интерес к высшим учебным заведениям со стороны злоумышленников только возрос. Чтобы защитить данные, эксперты рекомендуют принять меры, направленные на ограничение несанкционированного доступа к сети университета и мониторинг с целью обнаружения нелегальных попыток проникновения в режиме реального времени. Для обеспечения безопасности данных в высших учебных заведениях необходимо внедрить сложные системы. В будущем следует провести исследования в области систем управления информационной

безопасностью, посвященных высшим учебным заведениям, а также проанализировать международные стандарты безопасности, такие как ISO 27000, COBIT, NIST, для создания эффективной и экономически эффективной системы безопасности.

Список используемых источников:

1. Сазонов В. В., Носов А. О. Моделирование сети передачи данных специального назначения // Перспективные направления развития отечественных информационных технологий : материалы V межрегион. научно-практич. конф., Севастополь, 24-28 сент. 2019 г. Севастополь : Севастопольский государственный университет. Санкт-Петербургский институт информатики и автоматизации РАН, 2019. С. 212–214.

2. Переспелов А. В., Сагдеева Л. А. Сравнительный анализ существующих реализаций проектирования защищенных компьютерных сетей // Инновации. Наука. Образование. 2021. Т. 1. N 44. С. 910–915.

3. Мещеряков А. И. Проблема выбора среды моделирования для изучения сетевых технологий // Молодой исследователь Дона. 2021. N 6 (33). С. 70–76.

4. Истратова Е. Е., Аверьянов Р. В., Гаськов Н. А. Исследование программных эмуляторов сетевого оборудования // Программно-техническое обеспечение автоматизированных систем: материалы Всерос. молодежной научно-практич. конф., Барнаул, 16 дек. 2020 г. Барнаул : АлтГТУ, 2021. С. 3–7.

5. Королев И. Д., Маркин Д. И. Сравнительный анализ средств эмуляции автоматизированных систем // Информационная безопасность: вчера, сегодня, завтра : материалы IV Междунар. научно-практич. конф., Москва, 22 апр. 2021 г. М. : РГГУ, 2021. С. 111–118.

6. Васин Н. Н., Ирбахтин А. А. Моделирование защищенных каналов телекоммуникаций с использованием средств виртуализации // Инфокоммуникационные технологии. 2017. Том 15. N 1. С. 29–35.

7. Гельфанд А. М. и др. Защита для распределенных отказов в обслуживании в облачных вычислениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VIII Междунар. науч.-технич. и науч.-методич. конф., Санкт-Петербург, 27–28 фев. 2019 г. СПб. : СПбГУТ, 2019. С. 329-334.

Kazancev A., Makhorin A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Threats to network security in higher education.

In recent years, there has been a significant change in the way that higher education institutions operate worldwide. The use of distance learning has become a unique opportunity for further education, not only in times when most activities were suspended, but also for improving the educational process currently. To ensure the quality of distance learning in universities, online learning platforms, applications, video conferencing, and cloud computing tools have been introduced and widely used. However, this has intensified the threats to information security in the field of education in general, and universities in particular, as the number of cyberattacks has increased, resulting in significant financial losses, as well as business interruption, and theft of personal data or intellectual property. To identify the biggest threats to universities, several security reports and scientific articles related to the area of study were analyzed in order to identify the most common security threats. As a result of the research conducted, the main cyber threats to universities are malware attacks, DoS/DDoS attacks, and phishing attacks. Ensuring the security of university networks has been a challenging task for specialists in this field.

Key words: cybersecurity, online education, cyber-attacks, e-learning

УДК 004.056
ГРНТИ 49.33.35

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Е. К. Караханова, А. В. Светова
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются проблемы уязвимости безопасности облачной среды, описываются основные облачные модели, рассматриваются вопросы по минимизации угроз, а также предлагается стратегия по достижению высокого уровня защиты облачной инфраструктуры.

облачные вычисления, персональные данные, безопасность данных в облаке, PaaS, SaaS, IaaS

С каждым днем в сетевой инфраструктуре набирают популярность облачные вычисления (*cloud computing*), главная цель которых состоит в том, чтобы обеспечить безопасное, быстрое и удобное хранение данных, предоставляемых через Интернет. Актуальность облачных систем растет вместе с увеличением объемов информации. Так же рост интереса к технологиям облачных вычислений связан с экономическим эффектом от их использования. Однако несмотря на то, что облачные вычисления стремительно завоевывают популярность, существует множество проблем информационной безопасности, которые стали основным препятствием для внедрения облачных услуг.

Поднимая вопрос безопасности данных в облачных вычислениях, мы должны понимать, за построением безопасной инфраструктуры стоит множество методов и решений. Требования к безопасности, а также наиболее уязвимые места «облачных» сервисов зависят от моделей обслуживания (см. рис. 1), видов предоставляемых услуг, а также от зоны ответственности клиента и провайдера (см. таблицу 1).

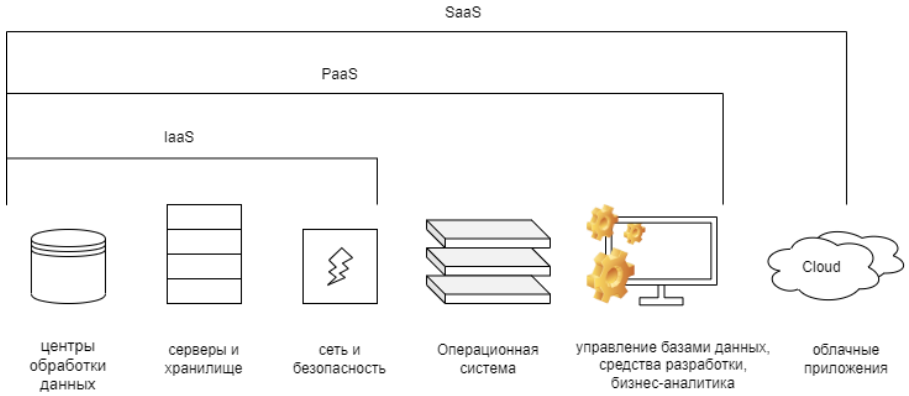


Рис. 1. Облачные модели

Программное обеспечение как сервис (*Software as a Service*, SaaS) наиболее распространённая модель для различных предприятий на рынке,

так как предоставляет клиентам доступ к приложению как к готовому интернет-сервису. Следующая модель *Platform as a Service* (PaaS) больше подходит для программистов, так как позволяет пользователям самим разрабатывать приложения. Модель дает возможность клиентам в готовой облачной платформе создавать, тестировать и развёртывать приложения, такие как простые облачные программы, а также крупные промышленные системы. Модель *Infrastructure-as-a-Service* (IaaS) позволяет получить в распоряжение полноценную виртуальную инфраструктуру и разместить в облаке все вычислительные ресурсы, включая операционную систему. Провайдер в данной модели управляет облачными службами, а также несет ответственность за вопросы администрирования серверного и сетевого оборудования. Клиент же отвечает за настройку операционной системы и приложений. Так на плечи потребителя ложится обязательство за безопасность приложений. Поэтому IaaS считается самой уязвимой моделью.

Таблица 1. Модель ответственности за безопасность облака.

Облачная модель	IaaS		PaaS		SaaS	
Ответственность	Клиент	Провайдер	Клиент	Провайдер	Клиент	Провайдер
Классификация данных и ответственность за их доставку	+	–	+	–	+	–
Защита клиента / конечных устройств	+	–	+	–	+	+
Управление индентификацией / доступом	+	–	+	+	+	+
Управление на уровне приложений	+	–	+	+	–	+
Управление сетью	+	+	–	+	–	+
Операционная система	+	–	–	+	–	+
Физическая безопасность	–	+	–	+	–	+

Наиболее часто угрозы безопасности облака относятся к данным, инфраструктуре и мощностям вычислительной машины. В зависимости от модели можно определить границы ответственности за безопасность клиента и провайдера. В большинстве случаев борьба с уязвимостями происходит преимущественно на серверной стороне, то есть это обязанность поставщика облачных услуг. Но свои обязанности есть и у клиентов. В первую очередь они должны правильно использовать настройки защиты, уметь безопасно пользоваться службами, а также заботиться о защите всех устройств и сетей конечных пользователей [2]. Существует довольно большой список угроз

безопасности облачных вычислений, самые распространённые представлены на рис. 2.

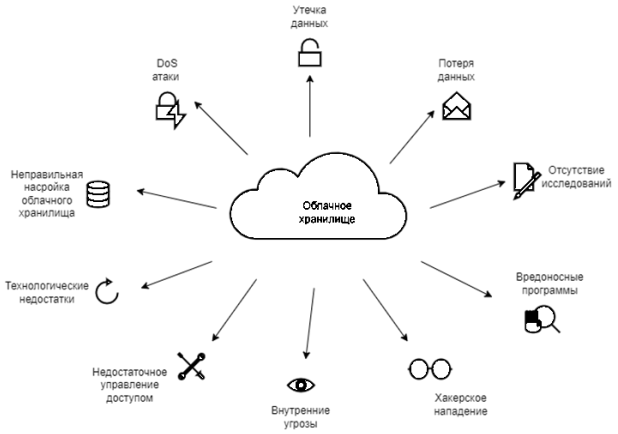


Рис. 2. Примеры угроз безопасности облака

Говоря о безопасности облака, предполагается создание архитектуры безопасности, которая реализуется добавлением к базовой архитектуре защитных средств. Представленная на рис. 3 схема иллюстрирует реализацию архитектуры облачной безопасности с выявленными уровнями, требующими защиты, а также предлагаются инструменты и процессы для обеспечения сохранности облачных ресурсов. В предложенной схеме сформирована комплексная защищенная платформа гибридной облачной инфраструктуры, которая обеспечивает возможности по контролю и управлению безопасности.

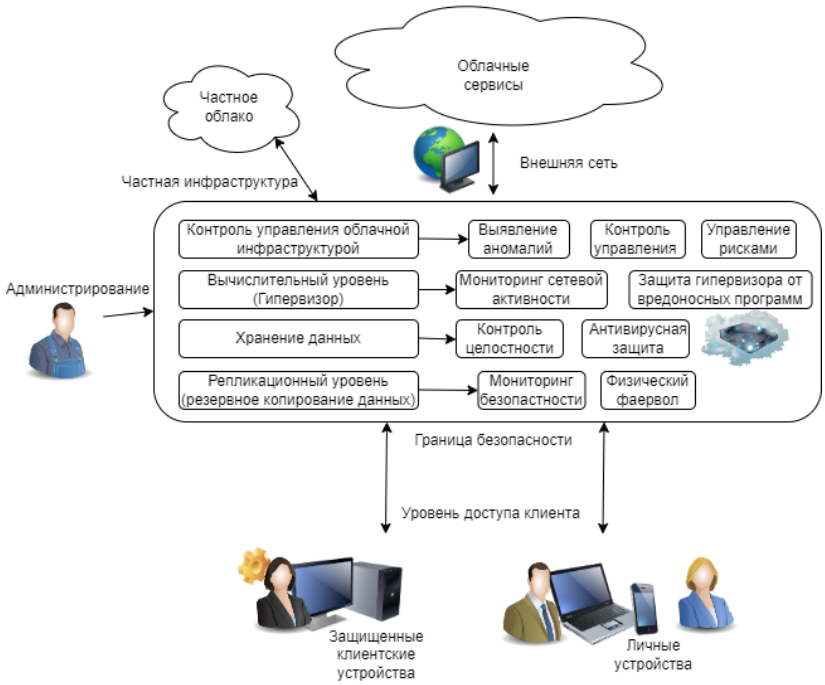


Рис. 3. Схема гибридной архитектуры безопасности облака с предложенным комплексом защитных средств.

Предлагается решение, базирующееся на политике безопасности с нулевым доверием, а также обеспечивающее контроль безопасности и

процесс реагирования на инциденты за счет организации комплекса защитных средств. Основное внимание уделено выявлению аномалий и угроз в трафике клиентов и возможности управления, контроля каждого уровня облачной инфраструктуры.

Таким образом, можно сделать вывод, что вопрос безопасности один из наиболее важных для поставщика облачных сервисов, который требует организованной работы и разработки новых методов и стратегий по реализации защиты каждого уровня облачной инфраструктуры. Так как следует помнить, что характер и направленность угроз в современном мире претерпевают изменения, следовательно, вопрос безопасности не может быть решен однократно, а требует систематической работы как со стороны провайдера, так и со стороны клиента.

Список используемых источников:

1. Пестов И. Е. Атаки на облачную инфраструктуру / И. Е. Пестов, С. А. Кошелева // Инновационные решения социальных, экономических и технологических проблем современного общества : материалы круглого стола со всерос. и междунар. участием, Москва, 15–16 дек. 2021 г. М. : ООО «КОНВЕРТ», 2021. Т. 8. С. 113-115.

2. Что такое безопасность облака? [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security (дата обращения: 22.10.2023).

3. Новые смыслы. Проблематика информационной безопасности в гибридной облачной инфраструктуре в условиях нулевого доверия [Электронный ресурс]. URL: https://ib-bank.ru/bisjournal/post/1894 (дата обращения: 22.10.2023).

4. Предотвращение угроз безопасности облачным сервисам [Электронный ресурс]. URL: https://www.it-grad.ru/blog/oblachnyj-iaassaas-servis-provajder-i-problemy-bezopasnosti-tri-shaga-na-puti-predotvrashheniya-ugroz / (дата обращения: 22.10.2023)

5. Что такое IaaS [Электронный ресурс]. URL: https://cloud.ru/ru/services/iaas (дата обращения: 22.10.2023)

Karahanova E., Svetova A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

Problems of providing information security for cloud computing.

The article observes the problems of security vulnerabilities in the cloud environment, describes the main cloud models, addresses issues of minimizing threats, and also suggests a strategy to achieve a high level of protection for the cloud infrastructure.

Key words: Cloud computing, personal data, cloud data security, PaaS, SaaS, IaaS.

УДК 004.056.7
ГРНТИ 81.93.29

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ ЭЛЕКТРОННЫХ ПОДПИСЕЙ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА И МЕТОДЫ ОБЕСПЕЧЕНИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДОКУМЕНТОВ

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

В современном информационном сообществе обеспечение безопасности персональных данных является критически важной задачей. Одной из угроз является утечка данных, особенно со стороны внутренних сотрудников, которые имеют доступ к ценной информации. Для обеспечения защиты конфиденциальных данных в государственных и коммерческих учреждениях применяют электронную цифровую подпись, которая подтверждает целостность и подлинность данных.

криптографические средства защиты информации, система электронного документооборота, информационная безопасность, персональные данные, ЭП

В настоящее время трудно представить компанию, не использующую СЭД (система электронного документооборота). СЭД – это система процессов по обработке документов в электронном виде, в функции которой входит: классический документооборот, безопасность данных, управление корпоративными процессами, электронных архив и другие [1].

С переходом на электронный документооборот появилась потребность в обеспечении документов юридической силой посредством электронной подписи (ЭП). Такая подпись сохраняет информацию, которая была в документе на момент подписания, тем самым подтверждая ее целостность.

Однако, создание ЭП невозможно без использования средств криптографической защиты информации (СКЗИ). СКЗИ – может быть как программой (КриптоПро CSP, VipNet CSP, LISSI-CSP, Signal-COM CSP), так и устройством (Рутокен CSP, Рутокен CSP 2.0, JaCarta SE), которые шифруют хеш-функцию документа и производят генерацию электронной подписи. С помощью закрытого ключа СКЗИ создает электронную подпись и прикрепляет ее к документу вместе с сертификатом проверки.

Электронная подпись является уникальным доказательством происхождения и авторства электронного документа, которое подтверждает, что он был создан и подписан конкретным лицом или организацией. Для обеспечения надежности и безопасности подписи необходимо соблюдение следующих требований:

1. Надежность - подпись должна быть защищена от возможного отказа или вмешательства со стороны посторонних лиц, чтобы исключить возможность утверждения, что документ был подписан другим человеком.

2. Целостность - если внесены изменения в подписанный документ, подпись должна быть нарушена, чтобы предотвратить подделку и сохранить целостность оригинала.

3. Авторство - электронная подпись должна быть жестко привязана к конкретному физическому или юридическому лицу, чтобы установить его идентичность и авторство.

Принцип работы достаточно прост и представлен на рис. 1.

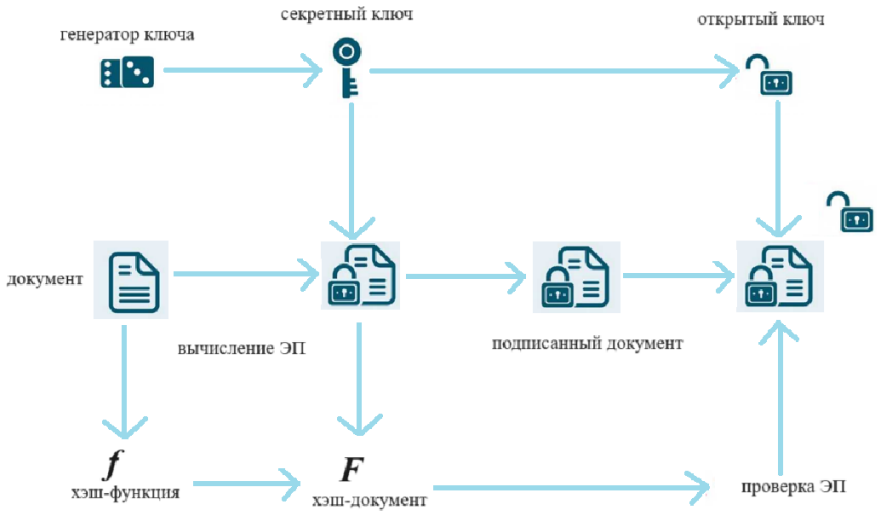


Рис. 1. Схема работы ЭП и СКЗИ

1. Автор создает исходный документ.
2. С использованием средства криптозащиты информации (СКЗИ) и закрытого ключа электронной подписи автор добавляет файл подписи, шифрует документ и объединяет все данные в один файл, который затем передается получателю.
3. Получатель получает переданный файл.
4. Получатель расшифровывает документ, используя СКЗИ и свой собственный закрытый ключ электронной подписи.
5. Получатель проверяет целостность электронной подписи, убедившись, что исходный документ не был изменен.

Поскольку процесс шифрования больших документов закрытым ключом является сложным и длительным, на практике часто используется более быстрое и простое хэш-шифрование. Сначала к тексту документа применяется хэш-функция, которая генерирует короткую последовательность символов. Затем полученный хэш шифруется закрытым ключом, создавая цифровую подпись. При передаче документа получателю передается его открытый текст вместе с цифровой подписью. Получатель лишь должен повторно хэшировать текст документа с использованием той же хэш-функции, расшифровать цифровую подпись открытым ключом и при помощи СКЗИ и сравнить полученные результаты. Если они совпадают, то документ был подписан отправителем и не был изменен, дополнен или подменен в процессе передачи. Чтобы гарантировать авторство, отправитель

должен иметь установленную пару ключей. На практике для этой цели используются удостоверяющие центры (УД), которые выдают сертификаты на пары ключей и обеспечивают их уникальность.

Несмотря на большие преимущества внедрения такой системы, СЭД также порождает большие риски в обеспечении защиты конфиденциальной информации.

В настоящее время есть несколько способов взлома или подделки подписи. Из них самый привлекательный для криптоаналитика - это угадывание закрытого ключа по открытому ключу. Если злоумышленник сможет это сделать, то ему будут доступны все возможности, которые есть у настоящего владельца подписи, включая управление его имуществом. Однако обычно такой взлом невозможен, так как подбор закрытого ключа по открытому является трудоёмкой задачей, для решения которой нужны большие вычислительные ресурсы и время. При генерации пары ключей широко применяются факторизация и дискретное логарифмирование, что сильно затрудняет возможность взлома.

Еще одной уязвимостью является хэш-функция. Здесь возможны несколько видов атак. Если алгоритм хэширования не надежен, то злоумышленник может подобрать свой документ, хэш-функция которого будет совпадать с исходным документом. Или он может создать два документа, дающих одинаковый хэш, и затем использовать один из них вместо другого. Эти ситуации называются коллизиями хэш-функций. Однако, взломщикам хэш-функций тоже не просто: подставной документ должен быть читаемым текстом, а не бесполезным набором битов. Кроме того на сегодняшний день разработаны достаточно надежные алгоритмы хэширования [2].

В России получение электронной подписи регулируется законом № 63-ФЗ "Об электронной подписи". Чтобы получить такую подпись, необходимо получить сертификат от удостоверяющего центра (УЦ). Для этого требуется предоставить соответствующие документы и заплатить определенную сумму, после чего можно забрать свой сертификат и eToken с закрытым ключом [3].

Однако в процессе получения сертификатов могут возникать различные махинации. Все удостоверяющие центры являются коммерческими организациями, они обязательно аккредитованы Министерством цифрового развития и имеют лицензию от ФСБ. Но иногда, ради прибыли, УЦ могут нарушать установленные правила выдачи сертификатов. Например, сегодня возможно получить электронную подпись на чужое лицо, используя утечки персональных данных или некомпетентность УЦ. Это может привести к серьезным последствиям, вплоть до переоформления имущества или создания фиктивных организаций для получения кредитов. Подделка подписей в России не требует особых знаний криптографии, достаточно только знать особенности сертификации электронной подписи.

Усиление электронной подписи с помощью криптографии можно достичь путем применения различных методов и алгоритмов [4].

1. Усиление безопасности с помощью современных алгоритмов электронной подписи: выбор наиболее устойчивых к взлому алгоритмов подписи, таких как RSA или ECDSA.

2. Защита данных: использование длинных ключей для усиления безопасности современных алгоритмов электронной подписи.

3. Усиление хэш-функций: внедрение хэш-функций с большей длиной хэша, таких как SHA-256 или SHA-512.

4. Подход, основанный на двухфакторной аутентификации: дополнительное применение пароля или биометрических данных.

5. Использование аппаратных средств хранения ключей: эксплуатация аппаратных устройств, таких как USB-токены или смарт-карты, для хранения приватных ключей.

Становится очевидно, что усиление ЭП с помощью криптографии является постоянным процессом, так как появляются новые угрозы и методы взлома. Поэтому регулярное обновление и совершенствование применяемых методов и алгоритмов является необходимостью для дальнейшего развития обеспечения безопасности информации.

Алгоритм достаточно устойчив и почти не имеет слабых мест. Однако, как и во многих случаях, самое слабое место этого метода - человеческий фактор, оставляющий большой простор для действий злоумышленников.

Список используемых источников:

1. Анацкая А. Г. Защита электронного документооборота : учеб. пособие. Омск : СибАДИ, 2019. 87 с.

2. Трубникова Е. А. Применение хэш-функции в создании электронной цифровой подписи [Электронный ресурс] // Юный ученый. 2020. N 7 (37). С. 19-22. URL: hhtps://moluch.ru/young/archive/37/2117/ (дата обращения: 26.10.2023).

3. Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 04.08.2023) «Об электронной подписи» // Собрание законодательства РФ № 15, 11.04.2011, ст.2036

4. Келдыш Н. В. Анализ существующих методов решения информационных задач, используемых при разработке систем электронного документооборота [Электронный ресурс] // Науковедение. 2012. N. 3(12). URL:http://naukovedenie.ru/sbornik12/12-61.pdf (дата обращения: 26.10.2023).

Kirilova D.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Identification of vulnerabilities of electronic digital signatures in electronic document management systems and methods of ensuring cryptographic protection of documents.

In the modern information community, ensuring the security of personal data is a critically important task. One of the threats is data leakage, especially from internal employees who have access to valuable information. To ensure the protection of confidential data, government and commercial institutions use an electronic digital signature that confirms the integrity and authenticity of the data.

Key words: cryptographic means of information protection, electronic document management system, information security, personal data, electronic digital signature.

УДК 004.056.5
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ И РЕАЛИЗАЦИЯ МЕТОДА ШИФРОВАНИЯ ДАННЫХ ПО ГОСТ ДЛЯ ОС ASTRA LINUX

А. А. Ковалева, И. О. Курманов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящей статье рассматривается вопрос исследования и внедрения методов шифрования данных с использованием стандартов ГОСТ в операционной системе Astra Linux. Акцент делается на важности обеспечения безопасности данных в современном информационном мире, особенно в чувствительных областях, таких как государственная безопасность и коммерческая информация. Также рассматриваются основные принципы и задачи шифрования данных, необходимость использования стандартов ГОСТ для обеспечения соблюдения российских законодательных требований и обязательств по защите информации. Описываются методы и алгоритмы, используемые в стандартах ГОСТ для шифрования данных, их преимущества и особенности. Рассматривается процесс интеграции и настройки этих методов в операционной системе Astra Linux. Анализируются результаты исследования и представляем выводы о применимости и эффективности шифрования данных по стандартам ГОСТ в Astra Linux.

Astra Linux, информационная безопасность, шифрование

1. Введение

В нашей современной цифровой эре, где большие объемы информации обрабатываются и передаются каждую секунду, безопасность данных становится вопросом первостепенной важности. Операционная система Astra Linux, разработанная в России, обеспечивает высокий уровень безопасности для своих пользователей, включая государственные структуры и коммерческие предприятия. Однако, обеспечение информационной безопасности данных требует не только организационных мероприятий, но и технических, в частности – надежных методов шифрования.

В настоящей статье приоритет отдается исследованию и внедрению методов шифрования данных, основанных на стандартах ГОСТ, в операционной системе Astra Linux. Проводится рассмотрение не только технических аспектов данного процесса, но и юридические аспекты соблюдения законодательных требований Российской Федерации.

2. Основы шифрования данных

Конфиденциальность, целостность и доступность данных являются ключевыми аспектами безопасности информации. Шифрование данных играет важную роль в обеспечении конфиденциальности, предотвращении несанкционированного доступа и обеспечении целостности данных. Операционная система Astra Linux, используемая в чувствительных секторах, таких как государственные структуры и финансовые организации, призвана обеспечивать высокий уровень защиты данных.

Конфиденциальность – один из фундаментальных аспектов информационной безопасности. Она гарантирует, что данные могут быть доступны только тем лицам, которые имеют на это право. В контексте операционной системы Astra Linux, это означает, что конфиденциальные данные, такие как государственные секреты, финансовая информация и другие чувствительные сведения, должны быть надежно защищены от несанкционированного доступа. Шифрование данных является ключевым методом обеспечения конфиденциальности, так как оно позволяет представлять информацию в непонятном для злоумышленника виде.

Целостность данных – второй важный аспект информационной безопасности. Он гарантирует, что данные не были изменены, повреждены или подделаны в процессе их передачи или хранения. В контексте Astra Linux, это означает, что любые изменения или повреждения данных должны быть обнаружены и предотвращены. Шифрование данных также помогает в обеспечении целостности, так как изменение зашифрованных данных без ключа расшифрования практически невозможно.

Доступность данных – третий аспект информационной безопасности, гарантирующий доступность данных в нужном времени и месте. Операционная система Astra Linux должна обеспечивать надежный доступ к данным для легитимных пользователей и процессов, но при этом предотвращать несанкционированный доступ. Шифрование данных может быть настроено так, чтобы обеспечить безопасный доступ к данным только авторизованным пользователям и при выполнении определенных условий.

Аутентификация – сервис, с помощью которого доказывается, что участники являются требуемыми, т.е. обеспечивается доказательство идентификации. Это может достигаться с помощью паролей, смарт-карт, биометрических токенов. В случае передачи единственного сообщения аутентификация должна гарантировать, что получателем сообщения является тот, кто нужно, и сообщение получено из заявленного источника. В случае установления соединения имеют место два аспекта. Во-первых, при инициализации соединения сервис должен гарантировать, что оба участника являются требуемыми. Во-вторых, сервис должен гарантировать, что на соединение не воздействуют таким образом, что третья сторона сможет маскироваться под одну из легальных сторон уже после установления соединения.[1]

Важность данных в операционной системе Astra Linux, особенно в чувствительных секторах, таких как государственные структуры и финансовые организации, подчеркивает необходимость эффективных методов шифрования данных для обеспечения конфиденциальности, целостности и доступности информации. В следующих разделах статьи будет более подробно рассмотрено, каким образом стандарты ГОСТ и его методы шифрования способствуют этой цели в операционной системе Astra Linux.

2. Стандарт ГОСТ и его роль в России

Стандарты ГОСТ (Государственные стандарты) в России представляют собой фундаментальные нормативные документы, разработанные для обеспечения информационной безопасности, включая шифрование данных. Эти стандарты разрабатываются с учетом особенностей российской законодательной среды и имеют решающее значение для обеспечения безопасности данных в различных секторах.

Основная роль стандартов ГОСТ заключается в обеспечении соблюдения законодательных требований Российской Федерации в области защиты информации. Множество организаций, включая государственные органы, критически важные инфраструктуры и финансовые учреждения, обязаны соблюдать эти стандарты при обработке, передаче и хранении конфиденциальных данных. Это обеспечивает минимизацию рисков и поддерживает национальные интересы в области информационной безопасности.

Стандарты ГОСТ также способствуют унификации и стандартизации процессов шифрования данных в России. Это позволяет обеспечивать совместимость различных систем и приложений, работающих с зашифрованными данными, что особенно важно в контексте безопасности. Соблюдение этих стандартов также облегчает проверку и аудит безопасности систем, что способствует поддержанию высокого уровня защиты данных.

Важно отметить, что стандарты ГОСТ в области шифрования данных представляют собой уникальные решения, адаптированные к российской информационной среде. Они учитывают особенности регулирования и реализации информационной безопасности в России. В следующих разделах статьи мы более подробно рассмотрим методы и алгоритмы шифрования, предлагаемые этими стандартами, и их внедрение в операционной системе Astra Linux.

3. Методы и алгоритмы шифрования ГОСТ

Стандарт ГОСТ предоставляет разнообразные методы и алгоритмы шифрования, которые играют ключевую роль в обеспечении безопасности данных. Эти методы и алгоритмы разработаны с учетом специфических потребностей и требований российской информационной среды. Более подробно рассмотрим некоторые из них.

- ГОСТ 28147 – симметричный алгоритм шифрования, который широко используется для защиты данных в России. Он предоставляет надежное шифрование и был адаптирован к российским стандартам. [4]
- ГОСТ Р 34.11-94 – используется для хэширования данных и обеспечивает целостность информации. Он является важной частью систем обеспечения целостности данных в российских организациях. [3]
- ГОСТ Р 34.10-2012 представляет собой алгоритмы для электронной цифровой подписи (ЭЦП), который является важным элементом аутентификации и цифровой безопасности в России. [2]

Преимущество ГОСТ-шифрования заключается в его специфичности для российской среды и соответствии российским законодательным

требованиям. Эти алгоритмы обеспечивают высокий уровень защиты данных и могут быть успешно интегрированы в операционную систему Astra Linux. В следующем разделе статьи мы рассмотрим процесс интеграции методов шифрования ГОСТ в Astra Linux более подробно.

4. Интеграция методов шифрования в Astra Linux

Процесс интеграции методов шифрования ГОСТ в операционную систему Astra Linux включает в себя настройку и настройку алгоритмов, обеспечивающих безопасность данных. Важно, чтобы данные алгоритмы были правильно настроены и интегрированы, чтобы обеспечить максимальный уровень защиты информации.

Первым шагом при интеграции методов шифрования ГОСТ в Astra Linux является выбор алгоритмов, которые наилучшим образом соответствуют потребностям системы и требованиям безопасности. Определение, какие алгоритмы лучше всего подходят, зависит от конкретных задач и сценариев использования.

Правильная настройка параметров шифрования, таких как длина ключа и режимы работы, является критически важной. Это влияет на безопасность и производительность системы. Настройки должны соответствовать рекомендациям и требованиям безопасности ГОСТ.

Методы шифрования ГОСТ должны быть интегрированы в ядро операционной системы, чтобы обеспечить их доступность на низком уровне системы. Это обеспечивает защиту данных даже до начала загрузки операционной системы.

После интеграции в ядро, необходимо настроить прикладные программы и сервисы, чтобы они использовали методы шифрования ГОСТ при обработке данных. Это включает в себя настройку серверов, клиентов, и других компонентов системы.

После завершения интеграции, важно провести тестирование системы на предмет безопасности. Это включает в себя проведение аудита безопасности и проверку системы на уязвимости. Только после успешного завершения тестов можно считать систему готовой к работе.

Уязвимость компоненты для интеграции различных методов аутентификации в операционной системе Astra Linux связана с применением нестойких криптографических хеш-функций для хранения unix-паролей. [5] Эксплуатация уязвимости может позволить нарушителю получить несанкционированный доступ к системе. Процесс интеграции методов шифрования ГОСТ в операционную систему Astra Linux представляет собой важный шаг в устранении подобных уязвимостей и обеспечении безопасности данных.

Интеграция методов шифрования ГОСТ в Astra Linux требует комплексного подхода и учета множества факторов, чтобы обеспечить максимальный уровень защиты данных. В следующем разделе статьи мы рассмотрим результаты исследования и анализа, а также подведем итоги этого процесса.

5. Заключение

В данной статье мы рассмотрели важность обеспечения безопасности данных и возможности интеграции ГОСТ-шифрования в операционную систему Astra Linux. ГОСТ-шифрование представляет собой надежный метод защиты информации, который соответствует российским стандартам безопасности данных. Интеграция ГОСТ-шифрования в программу анализа публикационной активности обеспечивает конфиденциальность и безопасность данных в современном мире информационных технологий.

Список используемых источников:

1. Межсетевые экраны. Лекция 2: Конфиденциальность, целостность, доступность. Национальный исследовательский университет «ИНТУИТ» [Электронный ресурс]. URL: https://intuit.ru/studies/courses/4088/1286/lecture/24236/ (дата обращения: 11.10.2023).

2. ГОСТ Р 34.10-2012. Информационные технологии. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М. : Стандартинформ, 2012.

3. ГОСТ Р 34.11-2012. Информационные технологии. Криптографическая защита информации. Функция хэширования. М. : Стандартинформ, 2012.

4. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М. : ИПК Издательство стандартов, 1990.

5. BDU: 2019-01001. Банк данных угроз информационной безопасности. ФСТЭК России [Электронный ресурс]. URL: https://bdu.fstec.ru/vul/2019-01001 (дата обращения: 13.10.2023).

Kovaleva A., Kurmanov I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Research and Implementation of Data Encryption Method According to GOST for Astra Linux OS.

This article discusses the issue of research and implementation of data encryption methods using GOST standards in the Astra Linux operating system. Emphasis is placed on the importance of data security in today's information world, especially in sensitive areas such as government security and commercial information. It also discusses the basic principles and objectives of data encryption, the need to use GOST standards to ensure compliance with Russian legal requirements and obligations to protect information. The methods and algorithms used in GOST standards for data encryption, their advantages and features are described. The process of integrating and configuring these methods in the Astra Linux operating system is discussed. We analyze the results of the study and present conclusions about the applicability and effectiveness of data encryption according to GOST standards in Astra Linux.

Key words: Astra Linux, information security, encryption.

УДК 004.056
ГРНТИ 81.93.29

УСОВЕРШЕНСТВОВАННЫЙ ВАРИАНТ КОРПОРАТИВНОГО HONEYPOT-РЕШЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ

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

В данной статье предлагается решение, представляющее собой вариант зонда, который может применяться в случаях, когда появляются признаки атаки. Решение позволяет специалисту по информационной безопасности действовать на опережение, производя мониторинг подозрительной сетевой активности с экрана на рабочем месте.

корпоративные сети, Honeypot, информационная безопасность, злоумышленник, виртуальная станция

1. Введение

Корпоративные сети являются неотъемлемой частью инфраструктуры современных компаний. Внутри такой сети циркулируют информационные потоки, содержащие важную информацию, в том числе конфиденциальную, обеспечение безопасности которой является первостепенной проблемой, стоящей перед любой организацией. Защита информации в корпоративных сетях обеспечивается путем использования комплекса мер и инструментов по предотвращению утечек корпоративных данных, персональных данных сотрудников и клиентов, отражению атак на ресурсы компании и другие [1].

С каждым днем появляются новые угрозы, разрабатываются вредоносные программы, увеличивается количество кибератак. Для своевременного реагирования и обеспечения безопасности необходимо постоянное совершенствование мер защиты, разработка новых методов противодействия. Их эффективность во многом зависит от того, насколько исследованы действия злоумышленников, проанализированы инциденты безопасности. Именно на решение таких задач и получения необходимой информации нацелены корпоративные приманки.

2. Совершенствование варианта honeypot-решения

С момента активного развития технологии Honeypot было разработано большое количество предлагаемых решений, среди которых есть как те, что нацелены на решение конкретных узконаправленных задач, так и те, что представляют собой полноценные системы, с различными инструментами и настройками. Идеального и универсального Honeypot-решения не существует, в каждом конкретном случае надо выбирать программу исходя из намечаемых целей [2]. Таким образом, при принятии решения об установке ловушки в корпоративной сети, поднимается вопрос о выборе конкретного инструмента, о расходах на настройку и поддержание ловушки в рабочем состоянии, о наличии кадров, имеющих необходимую

квалификацию и опыт [3]. Поэтому наиболее выгодным выбором для корпоративных сетей будет использование продуктов с предустановленными Honeypot, не требующими детальной настройки.

Одним из таких решений является продукт T-pot. Он объединяет в себе инструменты и сервисы для анализа данных, что позволяет повысить надежность защиты корпоративной сети. В T-Pot используется Docker - программа, позволяющая запускать программное обеспечение в виртуальных операционных системах в экземплярах, называемых контейнерами [4]. Эти контейнеры легко управляются и настраиваются на хост-машине, и на одной машине может работать множество контейнеров Docker. В T-Pot каждая приманка и инструменты работают в отдельных контейнерах, что обеспечивает модульность, а также более высокую безопасность по сравнению с запуском программного обеспечения непосредственно на машине.

В качестве усовершенствования управления решением T-pot используется дистрибутив для создания межсетевого экрана PfSense. Он состоит из множества базовых функций и может быть расширен с помощью пакетной системы, включая установку "в одно касание" [5]. В настоящее время pfSense является полноценной заменой коммерческих пакетов межсетевого экранирования/маршрутизации, включая многие функции, присутствующие в коммерческих продуктах (Cisco Pix, SonicWall, WatchGuard). В список функций, в частности, входят: межсетевой экран, маршрутизация, разграничение QoS, NAT, резервирование, балансировка нагрузки, VPN, отчеты и мониторинг, информация в реальном времени.

3. Реализация решения

В настоящее время для обеспечения безопасности корпоративных сетей все чаще тестируются решения на виртуальных аппаратных платформах, предполагающих более оперативное взаимодействие сотрудников безопасности с изучаемыми данными приманок в режиме реального времени. В данной работе в качестве продукта виртуализации применяется Virtualbox. На рис. 1 производится установка T-pot на виртуальную машину.

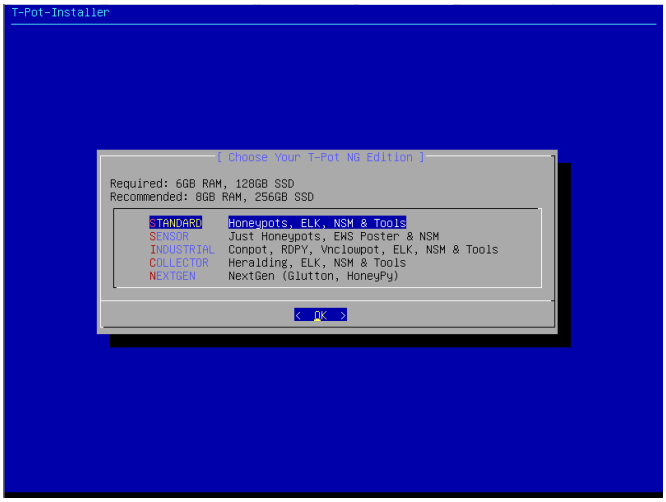


Рис. 1. Инсталляция T-pot

Изначально управление системой осуществляется командами в терминале, поэтому дополнительно устанавливается графическая оболочка xfce. Это позволит в дальнейшем осуществлять настройки и мониторинг с одного рабочего места. На рис. 2 представлена панель инструментов T-pot.

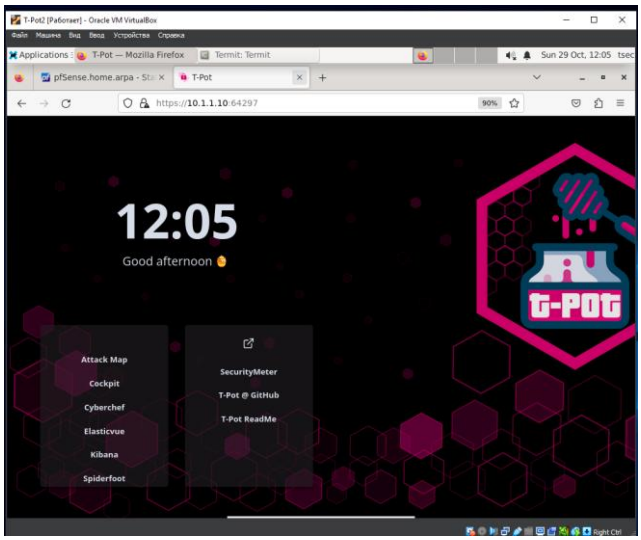


Рис. 2. Панель инструментов

Подключение межсетевого экрана pfsense осуществляется путем настройки внутреннего и внешнего интерфейсов. На рис. 3 представлено меню настройки pfsense.

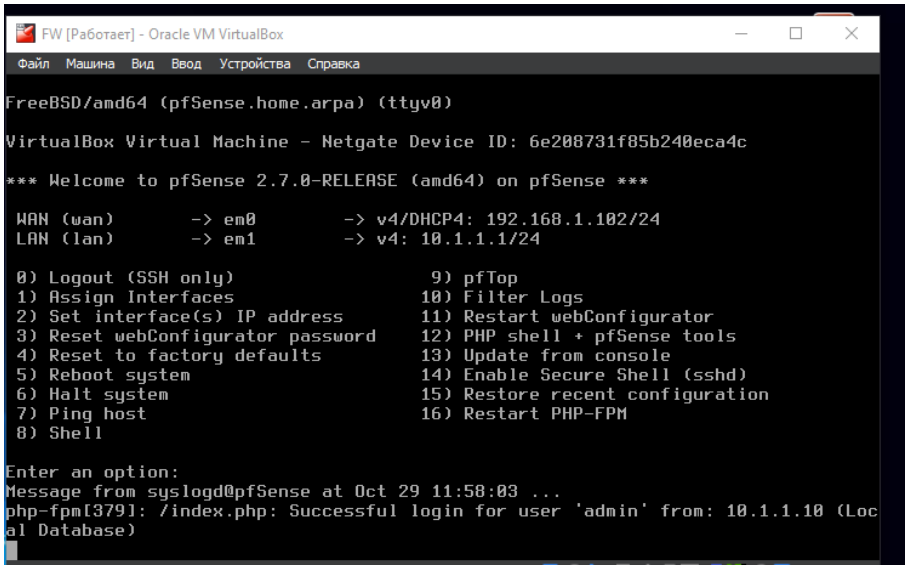


Рис. 3. Меню настройки

В результате с одной машины производится управление и мониторинг приманки и межсетевого экрана. На рис. 4 продемонстрирован веб-интерфейс межсетевого экрана.

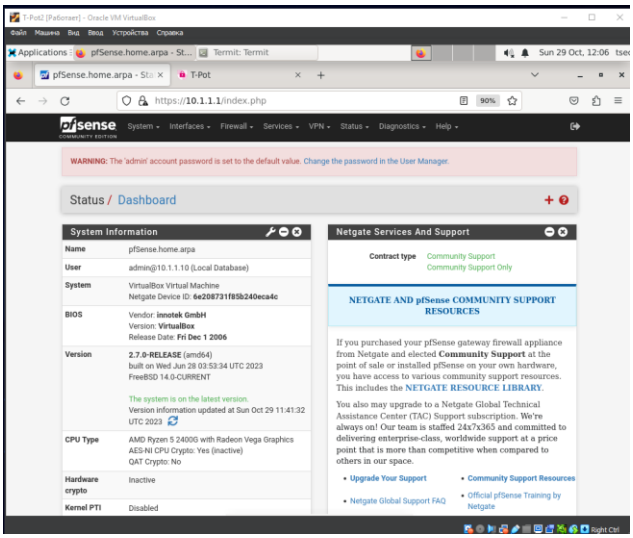


Рис. 4. Веб-интерфейс pfsense

4. Заключение

Усовершенствованный вариант корпоративного honeypot-решения позволяет использовать виртуальные аппаратные платформы для развертывания. Таким образом, решение является мультисистемным и может быть использовано с различными конфигурациями платформ и оборудования. Централизированное управление обеспечивает постоянный мониторинг трафика корпоративной сети.

Список используемых источников:

1. Как установить honeypot в вашей сети [Электронный ресурс] // Heritage-offshore. URL: https://heritage-offshore.com/net-admin/kak-ustanovit-honeypot-v-vashej-seti/ (дата обращения: 29.10.2023).
2. Защита корпоративной информации [Электронный ресурс] // Группа компаний Интегрус. URL: https://integrus.ru/blog/it-decisions/zashhita-korporativnoj-informatsii.html (дата обращения 29.10.2023).
3. 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. N 3. С. 86–97
4. Anton Kukoba. Honeypots as a Method of Malware Detection [Электронный ресурс] // Apriorit. 2018. URL: https://www.apriorit.com/dev-blog/568-honeypots-for-malware-detection (дата обращения 29.10.2023)
5. Что такое honeypot? [Электронный ресурс] // Kaspersky. URL: https://www.kaspersky.ru/resource-center/threats/what-is-a-honeypot (дата обращения 29.10.2023)

Kolomiycev R.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

An improved version of the corporate honeypot solution to ensure corporate network security.

This paper proposes a solution that is a variant of a probe that can be applied when signs of an attack appear. The solution allows an information security professional to be proactive by monitoring suspicious network activity from a workplace screen.

Key words: corporate networks, Honeypot, information security, intruder, virtual station.

УДК 004.056.7
ГРНТИ 81.93.29

ВНЕДРЕНИЕ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В МОДУЛЬ, ОТВЕЧАЮЩИЙ ЗА КОРПОРАТИВНУЮ БЕЗОПАСНОСТЬ ОПЕРАЦИОННОЙ СИСТЕМЫ LINUX, С ЦЕЛЬЮ ПРОВЕРКИ ЦЕЛОСТНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ В ПРОЦЕССЕ ЕЕ РАБОТЫ

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

В условиях современного информационного общества, где безопасность данных становится ключевым аспектом, статья рассматривает проблему утечек конфиденциальной информации, особенно среди внутренних сотрудников. В фокусе внимания предлагается применение цифрового водяного знака для обеспечения целостности данных и защиты операционных систем Linux. Акцент делается на внедрении цифрового водяного знака в модуль корпоративной безопасности, с целью проверки и подтверждения целостности операционной системы в процессе ее работы. Одной из угроз является утечка данных, особенно со стороны внутренних сотрудников, которые имеют доступ к ценной информации.

ЦВЗ, компоновка, ОС Linux, внедрение, вложение, эффективность, целостность

Цифровой водяной знак представляет собой уникальный метод защиты данных, предназначенный для подтверждения целостности и подлинности информации. В его основе лежит уникальный код, внедренный в данные, что обеспечивает возможность верификации подлинности информации и ее изменений. Роль цифрового водяного знака заключается в гарантировании, что данные остаются неприкосновенными в процессе их передачи, хранения и обработки.

Поддерживая целостность данных, цифровой водяной знак обеспечивает дополнительный уровень защиты от несанкционированных вмешательств и утечек информации. Его использование в операционных системах Linux становится важным элементом стратегии безопасности, обеспечивая не только защиту данных, но и поддерживая доверие к целостности операционной системы в целом.

Операционные системы Linux, благодаря своей открытой структуре и командному интерфейсу, предоставляют пользователям уникальные возможности, но в то же время, они подвержены различным угрозам. Важные аспекты безопасности включают в себя контроль доступа, защиту файловой системы, и реализацию средств обнаружения вторжений.Угрозы, с которыми сталкиваются операционные системы Linux:

Операционные системы Linux подвергаются разнообразным угрозам, включая вредоносное программное обеспечение, атаки на уровне ядра, перехват трафика, и сетевые атаки. Кроме того, внутренние угрозы со

стороны авторизованных пользователей могут стать источником утечек данных или системных нарушений.

Эффективные стратегии безопасности для операционных систем Linux требуют не только внимания к традиционным методам, таким как шифрование и аутентификация, но и использование современных технологий, включая цифровые водяные знаки, для обеспечения целостности данных и предотвращения угроз. В следующих разделах статьи мы рассмотрим, как цифровые водяные знаки могут стать важным инструментом в обеспечении безопасности операционных систем Linux. Критическость корпоративной безопасности:

Корпоративная безопасность представляет собой неотъемлемый элемент успешного функционирования бизнеса в современной цифровой среде. Сложившаяся сложность киберугроз, внутренних и внешних, ставит под угрозу конфиденциальность, целостность и доступность бизнес-данных. Несоблюдение стандартов безопасности может привести к серьезным последствиям, таким как утечка важной информации, потеря доверия клиентов и репутационные убытки.

Роль цифрового водяного знака в укреплении безопасности операционных систем Linux:

Цифровой водяной знак становится ключевым инструментом в арсенале мер безопасности, особенно в контексте операционных систем Linux. Внедрение цифрового водяного знака в модуль корпоративной безопасности призвано усилить существующие уровни защиты, обеспечивая дополнительный слой безопасности для критически важных данных и операций.

Цифровой водяной знак дает возможность не только проверить подлинность данных, но и обнаружить любые изменения в целостности операционной системы. Это особенно важно в условиях, где внутренние угрозы могут быть не менее значимыми, чем внешние. Путем внедрения цифрового водяного знака в корпоративную безопасность операционных систем Linux бизнес может обеспечить себе дополнительные гарантии безопасности, минимизируя риски несанкционированного доступа и поддельных манипуляций с данными.

Процесс внедрения цифрового водяного знака в модуль корпоративной безопасности Linux. Разработка Модуля Безопасности:

- Создание нового модуля безопасности для Linux, который будет интегрирован в ядро операционной системы.
- Определение интерфейсов и хуков для взаимодействия с ядром.

Разработка Цифрового Водяного Знака:

- Создание программы для встраивания цифрового водяного знака в исполняемые файлы.
- Реализация замены эквивалентных функций в исполняемом файле для внедрения цифрового водяного знака.

Интеграция Модуля в Ядро Linux:

•Разработка инструкций для загрузки и выгрузки модуля в ядро Linux.

•Тестирование модуля в изолированной среде для обеспечения совместимости и стабильности.

Встраивание Цифрового Водяного Знака:

•Внедрение цифрового водяного знака в код безопасностного модуля, используя ранее разработанный инструмент.

Тестирование и Отладка:

•Проведение тестов для проверки работоспособности модуля и правильности встраивания цифрового водяного знака.

•Отладка и исправление возможных ошибок.

Оценка Производительности и Безопасности:

•Оценка воздействия модуля на производительность системы.

•Проверка стойкости модуля к потенциальным атакам и попыткам обхода безопасности.

Документация и Внедрение:

•Создание подробной документации по использованию, установке и настройке нового модуля безопасности.

•Внедрение модуля в производственную среду, соблюдая необходимые процедуры и политики безопасности.

Мониторинг и Обновление:

•Установка механизмов мониторинга для отслеживания активности модуля и возможных инцидентов безопасности.

•Регулярное обновление модуля для устранения выявленных уязвимостей и обеспечения соответствия современным стандартам безопасности.

Этот процесс предполагает внедрение цифрового водяного знака с использованием созданного вами модуля безопасности в операционной системе Linux, обеспечивая тем самым дополнительный уровень защиты и целостности данных.

В завершение данной статьи о внедрении цифрового водяного знака в модуль корпоративной безопасности операционной системы Linux, мы подчеркиваем не только важность, но и необходимость дополнительных шагов в обеспечении целостности данных. Разработка и внедрение нового модуля безопасности, с уникальной способностью встраивания цифрового водяного знака на основе замены эквивалентных функций, открывает перед нами перспективы в области современных методов защиты.

Этот новейший метод проверки целостности не только усиливает безопасность операционных систем Linux, но и предоставляет возможность эффективного противодействия внутренним и внешним угрозам. Подчеркивается важность внимательного мониторинга и регулярного обновления данного модуля, чтобы поддерживать его высокую степень эффективности в постоянно меняющейся кибербезопасной среде.

Далее предстоит обширная работа в сфере дальнейших исследований и разработок, направленных на оптимизацию и совершенствование этого нового метода проверки целостности данных. Внимание к деталям, анализ результатов и оперативное внедрение обновлений станут ключевыми элементами успешной реализации этого инновационного подхода к обеспечению безопасности операционных систем Linux.

Список используемых источников:

1. Коржик В. И. Цифровая стеганография и цифровые водяные знаки: в 2 ч. СПб. : СПбГУТ, 2016 - 2017. ISBN 978-5-89160-125-3.

2. Коржик В. И., Анфиногенов С. О., Кочкарев А. И. Цифровая стеганография и цифровые водяные знаки. СПб. : СПбГУТ, 2017. 197 с.

2. Штеренберг С. И. Разработка методики построения доверенной среды на основе скрытого программного агента. Часть 3. Принцип действия программного агента и проверка его работоспособности // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. N 4. С. 34-40. – DOI 10.46418/2079-8199_2021_4_5. – EDN KWGAUD.

3. Красов А. В. Исследование применимости известных методов внедрения цифровых водяных знаков к исполняемым файлам Unix-подобных систем / А. В. Красов, В. И. Борисов // Известия высших учебных заведений. Технология легкой промышленности. 2022. Т. 56, N 2. С. 38-42. – DOI 10.46418/0021-3489_2022_56_02_07. – EDN NSRRTA.

4. Красов А. В. Метод защиты авторских прав и целостности программного обеспечения на основе внедрения ЦВЗ в исполняемый код / А. В. Красов // Перспективы науки. 2022. N 4(151). С. 16-25. – EDN OHFBUV

Konkov V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Embedding a digital watermark in the module responsible for the corporate security of the Linux operating system, in order to verify the integrity of the operating system during its operation.

In today's information society, where data security is becoming a key aspect, the article examines the problem of leaks of confidential information, especially among internal employees. The focus is on the use of digital watermarking to ensure data integrity and protect Linux operating systems. Emphasis is placed on the implementation of a digital watermark in the corporate security module, in order to verify and confirm the integrity of the operating system in the process of its work. One of the threats is data breaches, especially from internal employees who have access to valuable information.

Key words: CEH; layout; Linux OS; introduction; attachment; Efficiency, Integrity.

УДК 004.738
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ТЕХНОЛОГИЙ IOT В СЕЛЬСКОМ ХОЗЯЙСТВЕ

И. Д. Коршунов
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В наше время технологии интернета вещей активно внедряются в сельское хозяйство, переворачивая традиционные методы управления фермой. В данной статье рассмотрено, как сенсоры, искусственный интеллект и другие инновации влияют на производственные процессы, повышая эффективность сельскохозяйственной деятельности. Исследованы перспективы развития этих технологий и их воздействие на будущее сельского хозяйства.

интернет вещей, IoT, сельское хозяйство, автоматизация, цифровизация

Интернет вещей (Internet of things, IoT) представляет собой концепцию, в которой физические объекты оборудованы технологиями связи для сбора и обмена данными в режиме реального времени. Эти объекты могут взаимодействовать между собой и внешними системами, создавая цифровую среду, где улучшается мониторинг, управление и оптимизация различных процессов.

Сельское хозяйство, как фундаментальная отрасль, сталкивается с растущими вызовами в современном мире, такими как увеличение мирового населения, изменения климата и необходимость повышения производительности.

Применение технологий IoT в сельском хозяйстве приобретает стратегическое значение в решении этих проблем. Автоматизация процессов, мониторинг роста растений, управление животноводством и оптимизация использования воды – все это становится возможным благодаря сенсорам, сетевым устройствам и аналитическим платформам, объединенным в единую систему IoT.

Технологии интернета вещей предоставляют сельским хозяйствам точные данные в режиме реального времени, позволяя принимать информированные решения. Это не только увеличивает производительность и качество сельскохозяйственных продуктов, но также предотвращает избыточное использование ресурсов.

В сельском хозяйстве используются различные устройства и технологические решения IoT:

- Системы мониторинга за растениями:

Использование сенсоров и специальных датчиков для отслеживания состояния растений, почвы и атмосферных условий. Такие данные позволяют оптимизировать полив, следить за уровнем удобрений и предупреждать о возможных болезнях.

- Умное животноводство:

Внедрение IoT в животноводство для мониторинга здоровья животных. Смарт-бирки и датчики помогают следить за физиологическими параметрами, предупреждают о заболеваниях, отслеживают местоположение стада и позволяют оптимизировать условия содержания.

- Автоматизация сельскохозяйственных машин:

Использование беспилотных летательных аппаратов помогает эффективно отслеживать проблемные зоны и следить за состоянием полей. Применение автономных тракторов и комбайнов позволяет осуществлять более точную и быструю сборку урожая.

- Большие данные и аналитика:

Анализ обширных объемов данных, собранных с сенсоров и устройств IoT, для создания точных прогнозов и оптимизации стратегии управления ресурсами.

В нашей стране уже существует множество успешных компаний, которые предоставляют свои услуги и продукты сельскохозяйственному бизнесу. К примеру, компания DigiFarm Software [1] предоставляет системы управления стадом, а также бирки и различные чипы для крупного рогатого скота, которые представлены на рис. 1. Их системы управления процессами предприятия позволяют руководителям эффективно распределять обязанности работников, вести контроль исполнения задач, а также оптимизировать затраты. Для рядовых сотрудников система предоставляет необходимую информацию о животном, формирует рабочие списки на исполнение и экономит время на рутинных операциях.

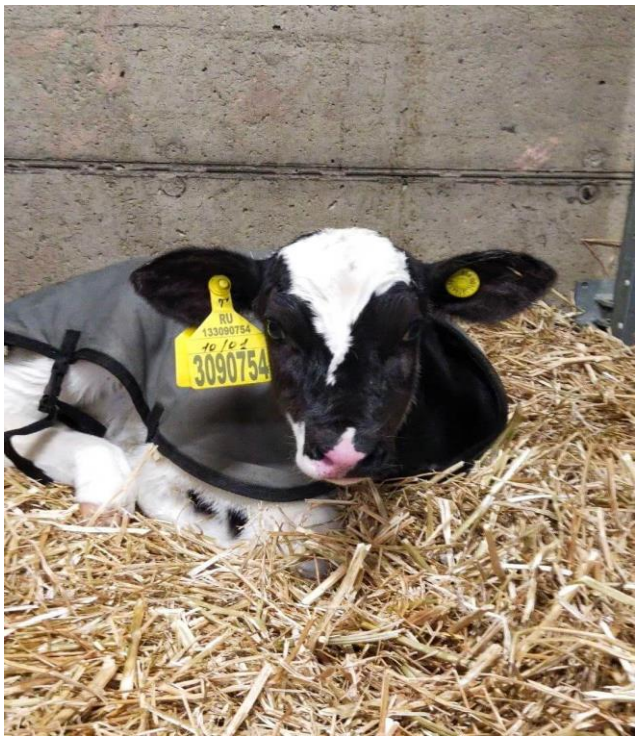


Рис. 1. Прикрепленные бирка и чип

Развитие технологий интернета вещей играет решающую роль в формировании будущего сельского хозяйства. Взглянем на перспективы развития этих технологий и их воздействие на отрасль:

1. Искусственный интеллект и машинное обучение:

Прогресс в области искусственного интеллекта и машинного обучения создает возможности для создания прогностических моделей. Эти модели будут способны предсказывать заболевания растений, оптимизировать условия выращивания и предоставлять ценные рекомендации.

2. Полная автоматизация сельскохозяйственной техники:

Развитие автономных сельскохозяйственных машин обеспечит эффективные инструменты для обработки полей, посева и уборки. Это поможет снизить необходимость человеческого труда, уменьшая затраты и повышая точность выполнения задач.

Таким образом, внедрение умных технологий в сельское хозяйство становится настоящим прорывом. Сенсоры, искусственный интеллект и другие инновации помогают фермерам лучше управлять полями, снижать расходы и улучшать качество продукции. Эти изменения создают перспективы для более умного, эффективного и экологически чистого сельского хозяйства в будущем.

Список используемых источников:

1. DigiFarm Software [Электронный ресурс]. URL: https://dfsoft.ru/ (дата обращения: 12.10.2023).

2. IoT в сельском хозяйстве: точное земледелие, умные теплицы и другие инновационные решения [Электронный ресурс]. URL: https://www.euromobile.ru/m2m-resheniya/iot-v-selskom-khozyaystve-tochnoe-zemledelie-umnye-teplitsy-i-drugie-innovatsionnye-resheniya/ (дата обращения: 12.10.2023).

3. Геомир, современные технологии для агробизнеса [Электронный ресурс]. URL: https://www.geomir.ru/ (дата обращения: 12.10.2023).

4. Gurtam, решения для спутникового мониторинга и IoT [Электронный ресурс]. URL: https://gurtam.com/ru (дата обращения: 12.10.2023).

Korshunov I.

Saint Petersburg State University of Industrial Technologies and Design

Research of iot technology in agriculture.

Nowadays, Internet of Things technologies are being actively introduced into agriculture, overturning traditional methods of farm management. This article examines how sensors, artificial intelligence and other innovations affect production processes, increasing the efficiency of agricultural activities. The prospects for the development of these technologies and their impact on the future of agriculture are investigated.

Key words: Internet of Things, IoT, agriculture, automation, digitalization.

УДК 004.056.53
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ПРИНЦИПОВ АУТЕНТИФИКАЦИИ ПОСРЕДСТВОМ OPENLDAP В ОПЕРАЦИОННЫХ СИСТЕМАХ LINUX

В. А. Кравцова, Д. И. Сухомлинов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Облегченный протокол доступа к каталогам (LDAP) — это протокол приложений с открытым исходным кодом, который позволяет приложениям получать доступ и проверять подлинность определенной пользовательской информации в службах каталогов. В статье рассматривается структура построения LDAP, вариант установки, а также возможные угрозы безопасности.

Аутентификация, LDAP, OPENLDAP, домен, Active Directory, Linux, Kerberos

Введение

Доменная аутентификация является одним из самых быстрых и удобных методов для развертывания инфраструктуры большой организации. Одним из классических способов было использование службы каталогов Active Directory [1], которая позволяла быстро объединить разные элементы сети. Однако, использование данного метода является неподходящим в рамках перехода на импортозамещающую продукцию, а также, эксплуатация уязвимости Kerberos Relay в Microsoft Active Directory, использующая особенности протокола доменной аутентификации Kerberos, чтобы повысить права на любом доменном компьютере (от непривилегированной учетной записи до системных прав) и закрепиться в системе, является серьезным аспектом угрозы информационной безопасности. Поэтому актуальным является исследование методов аутентификации в операционных семействах Linux.

Целью данной статьи является исследование принципов аутентификации посредством OpenLDAP в операционных системах Linux.

Основная часть

Каталоги LDAP представляют собой иерархические базы данных, содержащие информацию о людях и объектах (например, файлы PAM или SAM рабочих станций). Внутри каждого каталога данные хранятся в древовидной структуре, причем каждый уровень дерева представляет собой отдельный домен (рис. 1).

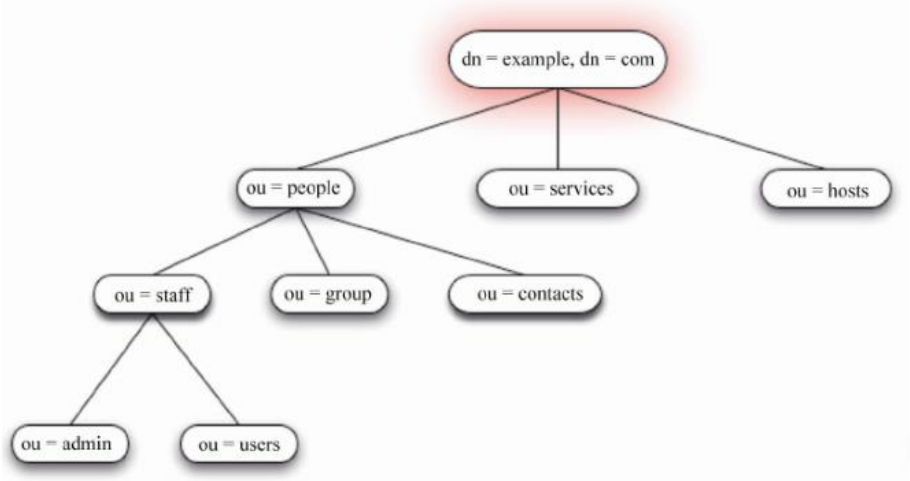


Рис. 1. Структура LDAP

Эта структура напоминает структуру DNS-серверов; домен верхнего уровня (TLD) — .com или .ca, а полное доменное имя (FQDN) — ldap. example.com. Все подкаталоги также имеют эту структуру. LDAP предназначен для предоставления служб каталогов другим открытым системам. Это означает, что LDAP по своей сути является открытой системой приема и возврата запросов [2]. Разница между каталогами и обычными базами данных заключается в том, что данные в каталоге обычно организованы так, чтобы обеспечить быстрый поиск результатов для быстрого выполнения запросов.

Наличие слишком большого количества учетных записей пользователей на нескольких хостах может привести к несогласованности в отслеживании учетных записей. LDAP может использоваться для создания централизованной системы аутентификации и обеспечения повышения стабильности данных. Наиболее используемый метод распространения данных учетных записей пользователей и другой информации через сеть осуществлялся через сетевую информационную службу (NIS). NIS-сервер опрашивается клиентами для получения этой информации, однако передает все данные в незашифрованном виде, что делает его небезопасным для использования. Защищенный канал передачи между сервером LDAP и клиентами, организованный с использованием Secure Socket Layer (SSL), делает его популярнее в эпоху интереса к области информационной безопасности. LDAP позволяет применять сложные списки контроля доступа к базам данных, в которых хранится значимая информация. Это позволяет осуществлять тонкую настройку разрешений [3].

Поскольку LDAP облегчает подключение к базам данных, хранящим конфиденциальные учетные данные, этот протокол можно использовать для аутентификации пользователей.

На высоком уровне процесс аутентификации происходит в 4 этапа после ввода имени пользователя и пароля.

1. Запрос Bind отправляется от клиента LDAP на сервер LDAP для инициирования процесса аутентификации;

2. Сообщение о результате привязки отправляется обратно клиенту LDAP для подтверждения начала процесса аутентификации;

3. Протокол LDAP используется для подтверждения существования всех учетных данных в каталоге LDAP и допустимой комбинации каждой записи;

4. После аутентификации учетных данных пользователя на сервер LDAP отправляется операция отмены привязки для разрыва соединения;

5. Доступ пользователя либо разрешается, либо запрещается.

Установка сервера OpenLDAP и клиентских компонентов

Выполнение данной настройки является несложным процессом. На сервере, выступающем в роли сервера OpenLDAP, сначала необходимо установить компоненты OpenLDAP. Затем настроить компоненты сервера, например, скопировав файл конфигурации шаблона, включенный в установку. Следующим этапом выполняется настройка порта, и запуск. Установка стандартных объектных классов LDAP, создание пользователя диспетчера каталогов LDAP, структуры каталогов. И завершающим этапом является создание пользователей и групп. Таким образом, можно сделать вывод, что настройка OpenLDAP является быстрым и удобным способом обеспечения аутентификации пользователей в инфраструктуре.

Несмотря на быстроту создания домена, служба каталогов Linux также уязвима для атак. LDAP-инъекция — основная атака на службы каталогов Linux. В книге «Предотвращение веб-атак с помощью Apache» упоминается, что: «LDAP-инъекция — это метод атаки, используемый для использования веб-сайтами, создающими операторы LDAP на основе пользовательских данных» [4].

LDAP-инъекция работает почти так же, как SQL-инъекция. Это своего рода эксплойт безопасности, при котором злоумышленник добавляет код языка структурированных запросов в веб-форму. Оба типа атак в основном происходят из-за слабой или отсутствующей проверки входных данных, которая не отклоняет ненормальные входные управляющие символы LDAP перед включением в запрос ненадежных пользовательских данных.

Основная причина того, что внедрение LDAP и подобные эксплойты работают, заключается в том, что безопасности не уделяется должного внимания во время процедуры разработки приложения. Еще одна атака, которой могут подвергнуться службы каталогов Linux, — это атака Syn Flood. Атака SYN Flood использует особенности реализации протокола управления передачей. Это так называемое трехстороннее рукопожатие. Сначала клиент обычно запрашивает соединение, отправляя серверу сообщение синхронизации. Затем сервер подтверждает запрос, отправляя Syn-Ack обратно клиенту. Наконец, клиент отвечает серверу подтверждением, и между ними устанавливается соединение. В данной атаке используется огромное количество запросов на соединение, что перегружает сервер.

Заключение

В заключение данной статьи хотелось бы отметить важность перехода на импортозамещающие способы аутентификации пользователей. Дальнейшим вектором развития данной тематики является обеспечение безопасности при использовании данных доменных каталогов.

Список используемых источников:

1. Мызникова Т. А. Основы информационной безопасности : учеб. пособие. Омск : ОмГУПС, 2017. 82 с. ISBN 978-5-949-41160-5. [Электронный ресурс] URL: https://e.lanbook.com/book/129192 (дата обращения: 11.10.2023).
2. Прохорова О. В. Информационная безопасность и защита информации. СПб. : Лань, 2023. 124 с. ISBN 978-5-507-46010-6. [Электронный ресурс] URL: https://e.lanbook.com/book/293009 (дата обращения: 15.09.2023).
3. Грекул В. И. Проектирование информационных систем : учеб. пособие. М. : ИНТУИТ, 2016. 570 с. [Электронный ресурс] URL: https://e.lanbook.com/book/100391 (дата обращения: 27.09.2023).
4. C. Obimbo and B. Ferriman, "Vulnerabilities of LDAP As An Authentication Service," Journal of Information Security, Vol. 2 N. 4, 2011, pp. 151-157.

Kravtsova V., Sukhomlinov D.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Studying the principles of authentication using OPENLDAP in Linux operating systems
Lightweight Directory Access Protocol (LDAP) is an open-source application protocol that allows applications to access and authenticate certain user information in directory services. The article discusses the structure of LDAP, installation option, and possible security threats.

Key words: Authentication, LDAP, OPENLDAP, domain, Active Directory, Linux, Kerberos.

УДК 004.056.53
ГРНТИ 81.93.29

ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ DKIM, DMARK, SPF В ДОМЕНАХ ЭЛЕКТРОННОЙ ПОЧТЫ

В. А. Кравцова, Д. И. Сухомлинов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Передача данных посредством электронной почты может быть небезопасна не только в связи с человеческими ошибками, такими как неверное указание получателя письма при передаче конфиденциальной информации, но также и в связи с фишинговыми письмами. Именно поэтому для обеспечения высокого уровня информационной безопасности организации необходимо использовать методики защиты, такие как DKIM, DMARK, SPF.

аутентификация, DKIM, DMARK, SPF, фишинг, электронная почта, почтовый домен

Введение

Во многих отчетах и анализах безопасности постоянно подчеркивается, что служба электронной почты является причиной или отправной точкой многочисленных инцидентов безопасности. Небезопасность службы электронной почты приводит к постоянному росту финансового мошенничества, вызванного компрометацией учетных записей пользователей. Использование более совершенных протоколов аутентификации, таких как DMARC, значительно снижает риск возникновения этих угроз.

Целью данной статьи является изучение эффективности протоколов DMARC, SPF, DKIM посредством.

Для достижения данной цели будут рассмотрены принципы работы данных протоколов, проанализированы возможные риски при их использовании.

Основная часть

Sender Policy Framework (SPF) — это протокол аутентификации электронной почты и часть кибербезопасности электронной почты, используемая для предотвращения и минимизации фишинговых атак [1]. Данный протокол построен на основе проверки хоста на наличие разрешения на использование данного домена, так как построенная инфраструктура электронной почты на данный момент позволяет пользователю самостоятельно выбрать доменное имя DNS. Данный протокол основан на записях DNS (тип TXT RR), в которых указывается, каким хостам разрешено использовать данное доменное имя, а также на какой промежуток времени. Время играет важную роль в данном способе аутентификации так как предполагается, что при изменении информации и не соответствию

указанному промежутку времени доменное имя будет считаться нелегитимным.

DKIM: Идентифицированная почта DomainKeys (DKIM) позволяет получателю электронной почты проверять целостность сообщения; отправитель электронной почты может включить цифровую подпись в заголовок электронного письма, подписанный его закрытым ключом. Получатель электронной почты может проверить подпись, получив соответствующий открытый ключ отправителя (записи TXT) из DNS [2]. DKIM является более надежным, в отличие от SPF, так как формируемый селектор всегда случаен, зависит от нескольких аспектов в момент отправки сообщения и находится в основной зоне сообщения, поэтому не может быть удаляем, в отличие от SPF, который встраивается в конверт сообщения и может быть откинут при модификациях во время передачи по сети.

Хотя SPF и DKIM обеспечивают подлинность отправителя электронной почты, они не сообщают, какие действия должен предпринять получатель в случае неудачной проверки. DMARC — это технический стандарт, защищающий отправителей и получателей электронной почты от спама, спуфинга и фишинга [3]. DMARC публикует политику, которая определяет методы аутентификации электронной почты и предоставляет получающим почтовым серверам инструкции по их обеспечению. Владелец доменного имени может опубликовать свою запись DMARC как запись TXT в поддомене с именем «_dmarc»; запись DMARC для a.com должна быть опубликована по адресу _dmarc.a.com. Владелец домена может настроить политику DMARC, используя комбинацию тегов и значений в записи DMARC.

Главными являются три тега: rua, ruf, ri, которые соответственно определяют отчеты по всем полученным письмам; по конкретному письму, вызвавшему сбой и по времени между отправкой уведомления после сбоя. Отчеты отправляются получателям в сжатом формате.

Анализ 20 государственных вебресурсов при использовании Hardenize, производства Hardenize team показал, что лишь 65 процентов доменов использует SPF, и лишь 45 процентов протокол глубокого анализа DMARC (рис. 1).

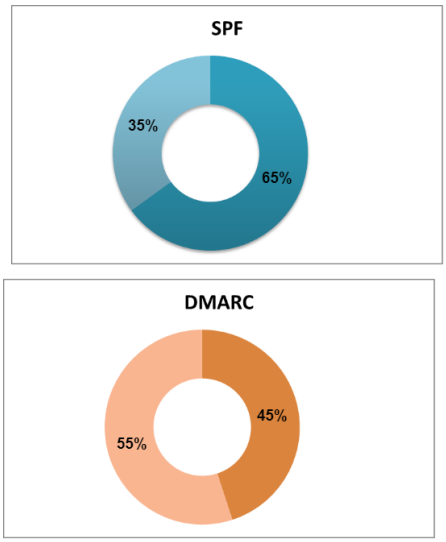


Рис.1. Использование SPF и DMARC

Заключение

SPF, DKIM и DMARC помогают аутентифицировать отправителей электронной почты, проверяя, пришли ли электронные письма из домена, из которого они утверждают. Эти три метода аутентификации важны для предотвращения спама, фишинговых атак и других угроз безопасности электронной почты. SPF и DKIM могут быть использованы без DMARC, однако данный протокол основывается лишь на данных от двух предыдущих. Новым этапом средств защиты электронной почты является BIMI — это механизм, который помогает получателю электронной почты визуально отличать легитимные и фишинговые электронные письма. Поскольку Google официально поддержал BIMI в июле 2021 года, этот подход начинает распространяться по всему миру.

Список используемых источников:

1. Kitterman S. RFC 7208: Sender policy framework (SPF) for authorizing use of domains in email, version 1. 2014.
2. Crocker D., Hansen T., Kucherawy M. (ed.). RFC 6376: Domainkeys identified mail (DKIM) signatures. 2011.
3. Kucherawy M., Zwicky E. (ed.). RFC 7489: Domain-based message authentication, reporting, and conformance (DMARC). 2015.

Kravtsova V., Sukhomlinov D.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Effectiveness of using DKIM, DMARC, SPF in email domains.

Data transmission via email can be insecure not only due to human errors, such as incorrectly specifying the recipient of an email when transmitting confidential information, but also due to phishing emails. That is why, to ensure a high level of information security, an organization needs to use security techniques such as DKIM, DMARK, SPF.

Key words: Authentication, DKIM, DMARC, SPF, phishing, email, mail domain.

УДК 004.056
ГРНТИ 81.93.29

РАЗРАБОТКА КОНЦЕПЦИИ МЕССЕНДЖЕРА НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ МЕТОДОВ СТЕГАНОГРАФИИ

А. В. Красов, М. Д. Масютин, Я. В. Черник
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С каждым днем информационная безопасность становится все более важным аспектом взаимодействия пользователей в сети интернет. Передача конфиденциальных данных всегда сопряжена с риском. Для решения этой проблемы можно использовать различные методы стеганографии, которые затруднят доступ третьих лиц к истинной передаваемой информации. В данном материале будет проведен обзор предстоящих исследований для диссертационной работы на тему разработки мессенджера с использованием методов сетевой стеганографии.

стеганография, сети и интернет, скрытая передача информации, сетевая безопасность, мессенджеры, LACK, RSTEG

В современном мире особо остро поставлена проблема защиты информации. Сейчас сложно найти данные в каналах связи, которые не закодирована тем или иным образом. Но, несмотря на возрастающие усилия по созданию различных технологий защиты данных их уязвимость не только не уменьшается, но и постоянно возрастает.

Одним из путей решения части вопросов связанных с безопасной передачей данных является сокрытие факта их передачи. Данное действие лежит в основе науки, называемой стеганографией. Стеганография (τεγανός — скрытый + γράφω — пишу, дословно «скрытопись») — это междисциплинарная наука и искусство передавать сокрытые данные, внутри других, не сокрытых данных. Скрываемые данные обычно называют стегосообщением, а данные, внутри которых находится стегосообщение называют контейнером. В ходе работы будут использоваться виды стеганографии, называемые цифровой и сетевой стеганографией.

Цифровая стеганография — это метод классической стеганографии, который заключается в скрытии дополнительной информации в цифровых объектах, таких как видео, изображения, аудио и текстуры. Это достигается путем внесения незначительных изменений в эти объекты, которые обычно находятся ниже порога восприятия человека.

Особенностью цифровой стеганографии является то, что цифровые объекты уже содержат некоторый уровень шума и искажений, таких как шум квантования и артефакты воспроизведения. При внедрении скрытой информации в эти объекты, добавление дополнительного шума и искажений становится еще менее заметным.

В результате, скрытая информация остается незаметной для большинства людей, при этом цифровые объекты остаются визуально и

звуко неизменными. Это делает цифровую стеганографию эффективным инструментом для скрытой передачи информации в цифровой форме.

Сетевая стеганография – это один из видов стеганографии, где носителем скрытой информации является сетевой протокол. Передача данных в таком случае производится путем модификации заголовка протокола или его полезной нагрузки, изменением структуры передачи данных или гибридным методом.

Методы сетевой стеганографии разделяются на 3 группы [1]:

1. Метод изменения данных в полях заголовка или полезной нагрузки;
2. Метод изменения структуры передачи пакета, например, последовательности его передачи;
3. Гибридные методы, при которых изменяется и содержимое пакета, и методы его передачи.

Каждый из этих методов делится на несколько групп: например, методы модификации пакетов включают три различных метода:

1. Методы изменения данных в полях заголовков протоколов: они основаны на изменении полей заголовков IP, Transmission Control Protocol (TCP), SCTP и т. д.
2. Методы модификации полезной нагрузки пакета: в этом случае используются различные алгоритмы водяных знаков, речевые кодеки и другие стеганографические техники для сокрытия данных.
3. Гибридные методы.

Методы модификации структуры передачи пакетов включают в себя три способа:

1. Методы, при которых изменяется порядок следования пакетов.
2. Методы, изменяющие задержку между пакетами.
3. Методы, суть которых заключается в преднамеренной потере пакетов путем пропуска порядковых номеров у отправителя.

Смешанные (гибридные) методы стеганографии используют два подхода: методы потери аудиопакетов (LACK) [2] и повторной передачи пакетов (RSTEG) [1]. Метод RSTEG основан на механизме повторной отправки пакетов, суть которого заключается в следующем: когда отправитель посылает пакет, получатель не отвечает флагом подтверждения, из-за чего должен сработать механизм повторной отправки пакетов, и пакет со стеганограммой внутри будет отправлен повторно, но из-за отсутствия флага подтверждение не осуществляется. В следующий раз, когда этот механизм срабатывает, происходит отправка оригинального пакета без стегавложения, в ответ на который приходит пакет с подтверждением успешного получения. Стеганография потерянных аудиопакетов (LACK) - метод стеганографии с преднамеренной задержкой аудиопакетов [2]. Принцип работы данного метода заключается в следующем: отправитель выбирает один из пакетов, в полезную нагрузку которого встраивается стеганограмма, после чего происходит его задержка. При получении такой

пакет отбрасывается, однако, человек, принимающий сообщение, может перехватить его и расшифровать.

Основной идеей метода модификации полей является добавление в них стеганограммы [3, 4]. Данное действие становится возможным в виду некоторых условий, когда при определенных значениях данный параметр не будет участвовать в передаче пакета. Например, поле “ID” пакета протокола IP задается адресантом, которое, в свою очередь, используется только во время фрагментации. В таком случае, если отсутствует необходимость, для модификации становится доступным поле “Flags”, содержащее поле “DoNotFragmentBit”, которое становится пригодным для стегавложения. Самыми часто распространёнными протоколами являются IPv4 и IPv6 для сетевого уровня и TCP и UDP для транспортного.

В рамках будущей работы основной целью является разработка мессенджера, возможности которого позволяют передавать скрытую информацию для обеспечения дополнительной конфиденциальности. Из приведенного выше материала можно сделать вывод, что основные вложения могут происходить в:

1. Мультимедиа файлы;
2. Части пакетов данных.

На основе этого поставлены следующие задачи:

1. Анализ методов и реализаций вложения информации в мультимедийные файлы;
2. Собственная реализация методов вложения информации в мультимедийные файлы;
3. Анализ реализаций и собственная реализация метода LACK;
4. Анализ реализаций и собственная реализация метода RSTEG;
5. Анализ реализаций и собственная реализация механизма вложения информации в различные поля заголовков пакетов (механизм создания “персональных” пакетов);
6. Разработка тестового мессенджера с вышеперечисленными возможностями.

Идея работы данного мессенджера заключается в том, что приложение будет рассчитано на работу в рамках узкого круга лиц. Благодаря этому можно будет миновать шаг маскировки используемых средств создания стегаконтейнера для обычных пользователей. При запуске и авторизации пользователя в приложении, ему будет предлагаться выбор собеседника, либо же добавление его в контакты. В настоящий момент предполагается, что диалог двух пользователей возможен только при нахождении обоих в сети. При заходе в диалог, будет предлагаться выбор используемого метода создания стегаконтейнера, который потребуется подтвердить обеим сторонам. Далее действия будут зависеть от выбора пользователя:

1. Обмен мультимедиа файлами с вложенной в них информацией;
2. Тестовый звонок с преднамеренной потерей пакетов (метод LACK);

3. Текстовый диалог пользователей с вложением информации в заголовки пакетов.

После получения стегаконтейнера на принимающей стороне будет происходить обратная процедура для получения исходной информации. Как прообраз такого мессенджера можно использовать Invisible Chat – специального бота в мессенджере Discord. Это приложение позволяет пользователям обмениваться сообщениями, которые скрыты в изображениях. При отправке сообщения Invisible Chat автоматически встраивает его в выбранное изображение, делая его незаметным для посторонних наблюдателей. Получатель может извлечь скрытое сообщение, используя тот же ключ шифрования, что и отправитель. Для реализации метода генерации пакетов потребуется создать программу подобную Scapy.

Разработка мессенджера, который позволяет обмениваться скрытой информацией является перспективным направлением, так как использование стеганографии обеспечивает дополнительный уровень безопасности и конфиденциальности, ведь скрытая информация не вызывает подозрений у третьих лиц.

Список используемых источников:

1. Мазурчик В., Щипиорски К. Стеганография потоков VoIP // На пути к значимым интернет-системам. Конфедеративные международные конференции OTM, CoopIS, DOA, GADA, IS и ODBASE. Материалы, часть II. Монтеррей, 9-14 нояб. 2008 г. С. 1001-1018.

2. Мазурчик В., Сага П., Щипиорски К. Ретрансляционная стеганография и ее обнаружение // Программные вычисления. 2011. С. 505-515.

3. Роуланд Ч. Скрытые каналы в наборе протоколов TCP/IP. Центрально-европейский журнал компьютерных наук. 1997. С. 45-66.

4. Кауич Е., Гомес Р., Ватанабе Р. Сокрытие данных в идентификационных и смещенных IP-полях. Компьютерные науки и инженерия. 2005. С. 118-125.

Krasov A., Masyutin M., Chernik Y.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development of a messenger concept based on the use of steganography methods.
Every day, information security is becoming an increasingly important aspect of user interaction on the Internet. Transmission of confidential data is always associated with risk. To solve this problem, various steganography techniques can be used to make it difficult for third parties to access the true transmitted information. This paper will review the upcoming research for a thesis paper on the topic of developing a messenger using network steganography techniques.

Key words: steganography, networks and the internet, covert information transfer, network security, messengers, LACK, RSTEG.

УДК 004.056.52
ГРНТИ 49.33.29

РАЗРАБОТКА КОНЦЕПЦИИ РЕШЕНИЯ ДЛЯ РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ WLAN НА ОСНОВЕ LBS

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

Ограничение прав доступа пользователя беспроводной сети на основе его местоположения может позволить предотвратить несанкционированный доступ к ресурсам организации и защитить конфиденциальную информацию. Кроме того, использование данных о местоположении даёт возможность оптимизировать использование ресурсов сети, например, предоставляя ограниченный доступ для гостей, что уменьшает нагрузку на сеть и повышает ее производительность для сотрудников.

беспроводные сети, LBS, RADIUS, разграничение доступа, определение местоположения

Защита корпоративных данных становится все более важной задачей в современном мире информационных технологий, с каждым днём растёт количество возможных угроз кибербезопасности. LBS (Location-Based Services) – это технология, использующая информацию о местоположении пользователя или устройства для предоставления определенных услуг [1]. Использование LBS не является прямым решением для борьбы с угрозами, но оно может помочь в предотвращении инцидентов информационной безопасности. Применение LBS для контроля доступа к корпоративным системам и ресурсам по географическим параметрам означает, что доступ к конфиденциальной информации может быть разрешен только в определенных географических областях, и любые попытки доступа из других мест будут заблокированы или записаны в журналы системы безопасности. Разграничение прав доступа на основе LBS также может использоваться для обнаружения и предотвращения утечек данных, связанных с потерей или кражей устройств. При активации определенного местоположения, удаленного или незарегистрированного, могут приниматься меры безопасности, например, удаленно стирать данные на устройстве или заблокировать его.

В ходе данной работы была разработана концепция решения для разграничения прав доступа пользователей беспроводной сети на основе данных о местоположении, представленная на рис. 1.

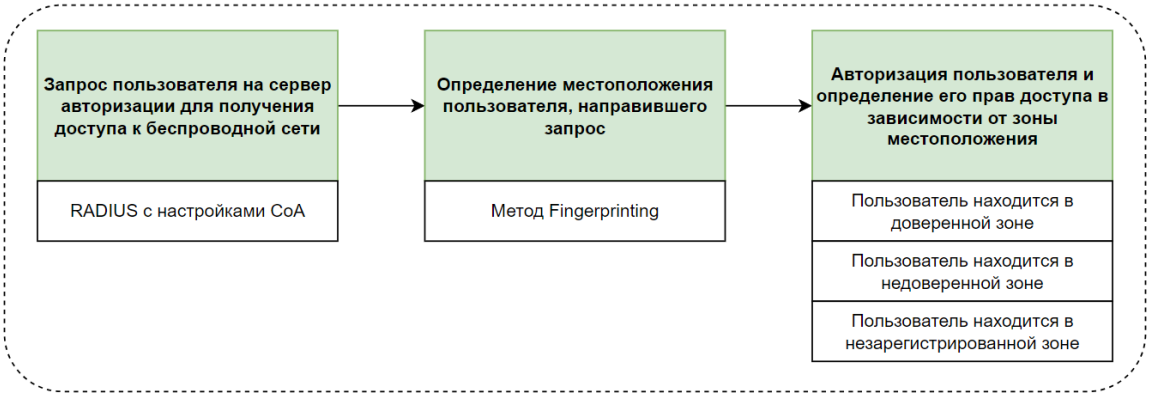


Рис. 1. Концепция решения для разграничения прав доступа пользователей WLAN на основе LBS

Чтобы применить механизм разграничения прав доступа клиента беспроводной сети, в разработанной концепции применяется сервер RADIUS (Remote Authentication Dial-In User Service) с настройками Change of Authorization (CoA). RADIUS - это протокол для аутентификации, авторизации и учета пользователей сети. Технология CoA позволяет динамически изменять параметры аутентификации и авторизации уже установленного сеанса связи.

Чтобы определить местоположение клиента, используется метод позиционирования по радиоотпечатку, то есть Fingerprinting, основанный на измерении расстояния по уровню мощности принимаемого сигнала (Received Signal Strength, RSS) [2]. Такой подход состоит из двух этапов. На первом этапе происходит измерение RSS на сенсорах, расположенных заранее в разных точках карты. Эти измерения называются радиоотпечатками. Каждой точке на карте соответствует своё значение радиоотпечатка, такая карта называется радиокартой. На втором этапе происходит определение местоположения устройства клиента в реальном времени по сопоставлению уровня мощности его сигнала с составленной на первом этапе радиокартой [3, 4].

На основе данных о местоположении клиента беспроводной сети принимается решение о предоставлении или ограничении прав доступа. Например, если пользователь находится в определенной географической области, доступ может быть предоставлен, а если пользователь находится за пределами разрешенной зоны, доступ будет ограничен или запрещен.

В разработанной концепции предусмотрены различные сценарии использования. Например, можно установить разные права доступа на основе местоположения, чтобы ограничить доступ к конфиденциальной информации только внутри офиса или специфических зон безопасности. Это может помочь предотвратить утечку данных в результате несанкционированного доступа из внешних или незарегистрированных зон.

В качестве технических мер предполагается использовать сетевые решения, такие как точки доступа Wi-Fi с возможностью сбора и анализа данных об уровне сигнала от устройств сети.

В разработанной концепции, после изменения местоположения пользователя, возможно генерирование запроса от сервера RADIUS для изменения прав доступа данного пользователя. В результате этого запроса сервер RADIUS может обновить параметры аутентификации и авторизации для данного пользователя в режиме реального времени. Например, доступ может быть предоставлен, изменен или ограничен в зависимости от конкретных политик безопасности и требований организации [5].

Использование RADIUS с функцией CoA позволяет гибко управлять правами доступа пользователей, основываясь на их местоположении. Это может быть полезно для оптимизации сетевой безопасности и эффективности, особенно в ситуациях, когда пользователи перемещаются внутри сети или имеют различные уровни доступа в зависимости от географической зоны.

Таким образом, разработанная в ходе данной работы концепция для разграничения прав доступа пользователей беспроводной сети на основе данных о местоположении способна помочь защитить корпоративные данные. Однако важно отметить, что LBS не является единственным или исчерпывающим решением для защиты данных. Обеспечение полной безопасности требует комплексного подхода, включающего в себя как технические решения, так и обучение сотрудников в области кибербезопасности.

Список используемых источников:

1. Кузьмина О. И., Миняев А. А., Сахаров Д. В. Исследование стандарта IEEE 802.11mc и его применимости в рамках обеспечения информационной безопасности беспроводной сети предприятия // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы XII Междунар. науч.-технич. и науч.-методич. конф., Санкт-Петербург, 28 фев. – 01 марта 2023 г. Санкт-Петербург: СПбГУТ, 2023. Т. 1. С. 727-731.

2. Дрепа В. Е., Кузьмина О. И., Миняев А. А. Разработка модели системы определения местоположения беспроводных клиентов сетей семейства IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы XI Междунар. науч.-технич. и науч.-методич. конф., Санкт-Петербург, 15–16 фев. 2022 г. Санкт-Петербург: СПбГУТ, 2022. Т. 1. С. 428-433.

3. Дрепа В. Е., Киструга А. Ю., Ковцур М. М. Точность определения местоположения WI-FI клиента в свободном пространстве при использовании индикатора уровня принимаемого сигнала // Региональная информатика : материалы Юбилейной XVIII Санкт-Петербургской междунар. конф., Санкт-Петербург, 26-28 окт. 2022 г. СПб. : СПОИСУ, 2022. С. 549-550.

4. Дрепа В. Е., Киструга А. Ю., Ковцур М. М., Кузьмина О. И., Петров В. А. Исследование метода fingerprinting для определения местоположения беспроводного клиента IEEE 802.11 / // Заметки ученого. 2022. N 3-2. С. 137-141.

5. Kovtsur M., Minyaev A., Khramtsov D., Abramenko G. Investigation of attacks and methods of protection of wireless networks during authorization using the IEEE 802.1X protocol // ACM International Conference Proceeding Series. 5, The Premier Conference on Smart Next Generation Networking Technologies. Сер. "ICFNDS 2021 - 5th International Conference on Future Networks and Distributed Systems: The Premier Conference on Smart Next Generation Networking Technologies" 2021. PP. 555-561.

Kuzmina O.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Conceptualization of a solution to control the access rights of WLAN users based on LBS. Controlling a wireless network user's access rights based on location can prevent unauthorized access to enterprise resources and protect confidential information. In addition, the use of location data provides an opportunity to optimize network resource utilization, such as providing limited access for guests, which reduces network load and improves network performance for employees.

Key words: wireless networks, LBS, RADIUS, access control, positioning.

УДК 004.032.26
ГРНТИ 28.23.37

НЕЙРОСЕТИ ДЛЯ АНАЛИЗА ТОНАЛЬНОСТИ ТЕКСТА

И. О. Курманов, А. М. Лешукова, Т. С. Петрова
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире, который становится все более зависимым от информационных технологий, анализ тональности текста приобретает огромное значение. Нейросети, обученные распознавать и классифицировать эмоциональный окрас текстов, играют важную роль в таких областях, как социальные медиа, маркетинг, финансы и многие другие. В данной статье будут рассмотрены сферы применения, существующие архитектуры, а также проанализировано на практике, какие архитектуры больше подходят для анализа тональности текста.

набор данных, тональность текста, информационные технологии, информация, полносвязные нейронные сети, рекуррентные нейронные сети

С развитием интернета и повышением активности пользователей в социальных медиа, объем текстовых данных стремительно увеличивается. В этом контексте, задача анализа тональности текста становится критически важной. Это позволяет определить, как пользователи относятся к различным продуктам, событиям или явлениям. Данная информация неоценима для бизнеса, помогая им адаптировать свои стратегии, и для государственных органов, чтобы мониторить общественное мнение. Актуальность этой темы подтверждается тем, что многие компании инвестируют значительные средства в разработку нейросетей для анализа тональности текста.

Прежде чем преступить к анализу нейронных сетей, нужно ответить на два вопроса: что такое тональность текста и почему анализ тональности текста так важен.

Тональность текста относится к эмоциональному оттенку или настроению, которое передается в тексте. Это может быть положительное, отрицательное или нейтральное настроение, а также спектр эмоций внутри этих общих категорий [1].

Анализ тональности текста направлен на определение и классификацию этого эмоционального оттенка. Например, текст, который выражает радость, счастье и удовлетворение, будет классифицирован как текст с положительной тональностью. Текст, в котором выражается гнев, разочарование и негодование, будет иметь отрицательную тональность. Текст, который не выражает ярко выраженных эмоций или является информативным без эмоциональной окраски, будет иметь нейтральную тональность.

Интернет, социальные медиа и мобильные устройства делают текстовую информацию легкодоступной. Люди выражают свое мнение о всем - от фильмов и продуктов до политических событий и брендов - в текстовой

форме. Анализ тональности позволяет нам понять, какие слова и фразы сопровождают определенные эмоции, будь то радость, разочарование или гнев.

Существует несколько различных архитектур нейросетей, которые могут использоваться для анализа тональности текста. Два основных типа, которые будут рассмотрены в этой статье: полносвязные нейронные сети и рекуррентные нейронные сети.

Полносвязные нейронные сети: Это классический тип нейросетей, где каждый нейрон в одном слое связан с каждым нейроном в следующем слое. Они отлично подходят для анализа тональности, так как могут выявлять сложные нелинейные зависимости в тексте. Полносвязные нейронные сети могут просто учиться на больших объемах текстовых данных и делать классификацию [2].

Рекуррентные нейронные сети (RNN): Эти сети разработаны для анализа последовательных данных, таких как текст. Они способны учитывать контекст предыдущих слов и фраз, что делает их эффективными для анализа тональности текста. RNN могут анализировать не только отдельные слова, но и их последовательности, что придает им способность улавливать смысл в тексте [3].

Обе архитектуры имеют свои преимущества и недостатки, и выбор между ними зависит от конкретной задачи и доступных данных.

Самое важное в работе нейронных сетей – это этап обучения. Машинное обучение производится с использованием набора данных (data set). Data set – это набор данных, который используется при обучении разных нейронных сетей. Причем качество обучения напрямую зависит от объема используемой информации: чем ее больше, тем точнее будет работать искусственный интеллект. Для каждой цели используется конкретный набор данных, он выбирается из уже существующих или составляется самостоятельно, если задача имеет узконаправленный характер [4].

Самыми популярными наборами данных для анализа тональности текста являются: IMDb, Amazon Customer Reviews (Amazon Product Reviews), Sentiment140, RuSentiment. Также ннекоторые компании создают собственные наборы данных, используя тексты из своих социальных медиа-платформ для анализа реакции пользователей.

Анализ тональности текста может быть выполнена на разных языках. Но на английском языке данная область более развита, и существует множество доступных ресурсов и моделей для анализа тональности. Некоторые из наиболее популярных англоязычных библиотек и моделей включают в себя "VADER" (Valence Aware Dictionary and sEntiment Reasoner), а также модели от Google и Facebook.

В то время как на русском языке ресурсы ограничены, но существует ряд библиотек и моделей, таких как "pymorphy2" для морфологического анализа и "Sentiment" для анализа тональности. Кроме того, нейросети, такие

как BERT, могут быть дообучены на русскоязычных данных для анализа тональности.

В рамках написания данной статьи было проведено сравнение двух способов анализа тональности текста, используемых для анализа тональности текста. Первый с использованием полносвязной нейронной сети, а второй с использованием рекуррентных сетей. При реализации нейросетей использовались библиотеки: TensorFlow, Keras и платформа: Google Colaboratory.

Первым объектом исследования является полносвязная нейронная сеть прямого распространения — это сеть, в которой каждый нейрон связан со всеми остальными нейронами, находящимися в соседних слоях, и в которой все связи направлены строго от входных нейронов к выходным.

Особенностью данной сети является то, что она может работать только данными одинаковой длинны, а длина отзывов в наборе данных разная. Поэтому определяем желанную длину отзыва, в нашем случае - 200. А затем с помощью функции pad_sequences обрезаем отзыв, если он больше, чем нужно или дополняем символами заполнителями (0), если меньше.

В данном способе создается модель типа Sequential, в которую будут добавлены полносвязные слои типа Danse. На первом слое 128 нейронов, на втором 64, на выходном слое 1 нейрон. На выходном слое достаточно одного нейрона так, как в данном случае у нас задача бинарной классификации. Если на выходе 0 – отзыв отрицательный, 1 значит положительный.

Обучение происходит в течение 20 эпох. В качестве проверочного набора данных были взяты 10% из набора данных.

Судя по результату первого обучения (рис. 1), можно сделать промежуточный вывод, что на обучающем наборе данных доля правильных ответов медленно растет (выделено синим), но на проверочном наборе данных доля правильных ответов остается примерно одинаковой (выделено красным). Для бинарной классификации точность правильных ответов всего 50% означает, что это случайное угадывание.

```
Epoch 1/20
176/176 [==============================] - 1s 6ms/step - loss: 0.5197 - accuracy: 0.6616 - val_loss: 3.0706 - val_accuracy: 0.4976
Epoch 2/20
176/176 [==============================] - 1s 8ms/step - loss: 0.5160 - accuracy: 0.6694 - val_loss: 3.1161 - val_accuracy: 0.4968
Epoch 3/20
176/176 [==============================] - 1s 8ms/step - loss: 0.5282 - accuracy: 0.6663 - val_loss: 2.6753 - val_accuracy: 0.5008
Epoch 4/20
176/176 [==============================] - 2s 11ms/step - loss: 0.5497 - accuracy: 0.6632 - val_loss: 3.0442 - val_accuracy: 0.5032
Epoch 5/20
176/176 [==============================] - 2s 11ms/step - loss: 0.5310 - accuracy: 0.6725 - val_loss: 2.6422 - val_accuracy: 0.4996
Epoch 6/20
176/176 [==============================] - 2s 11ms/step - loss: 0.5261 - accuracy: 0.6709 - val_loss: 2.8198 - val_accuracy: 0.5024
Epoch 7/20
176/176 [==============================] - 2s 10ms/step - loss: 0.5140 - accuracy: 0.6697 - val_loss: 2.9226 - val_accuracy: 0.5072
Epoch 8/20
176/176 [==============================] - 1s 9ms/step - loss: 0.5070 - accuracy: 0.6742 - val_loss: 2.6499 - val_accuracy: 0.5060
Epoch 9/20
176/176 [==============================] - 2s 10ms/step - loss: 0.5155 - accuracy: 0.6736 - val_loss: 2.8728 - val_accuracy: 0.4964
Epoch 10/20
176/176 [==============================] - 1s 8ms/step - loss: 0.5071 - accuracy: 0.6836 - val_loss: 2.9979 - val_accuracy: 0.5148
Epoch 11/20
176/176 [==============================] - 1s 8ms/step - loss: 0.5095 - accuracy: 0.6786 - val_loss: 3.0587 - val_accuracy: 0.5092
Epoch 12/20
176/176 [==============================] - 1s 8ms/step - loss: 0.5080 - accuracy: 0.6808 - val_loss: 2.7310 - val_accuracy: 0.4980
Epoch 13/20
176/176 [==============================] - 1s 7ms/step - loss: 0.5065 - accuracy: 0.6842 - val_loss: 2.7397 - val_accuracy: 0.5088
Epoch 14/20
176/176 [==============================] - 1s 6ms/step - loss: 0.5088 - accuracy: 0.6819 - val_loss: 2.6438 - val_accuracy: 0.5048
Epoch 15/20
176/176 [==============================] - 1s 4ms/step - loss: 0.4920 - accuracy: 0.6890 - val_loss: 2.7306 - val_accuracy: 0.4996
Epoch 16/20
176/176 [==============================] - 1s 4ms/step - loss: 0.5069 - accuracy: 0.6881 - val_loss: 2.8397 - val_accuracy: 0.5040
Epoch 17/20
176/176 [==============================] - 1s 4ms/step - loss: 0.5062 - accuracy: 0.6858 - val_loss: 2.9935 - val_accuracy: 0.5036
Epoch 18/20
176/176 [==============================] - 1s 4ms/step - loss: 0.5078 - accuracy: 0.6872 - val_loss: 3.1562 - val_accuracy: 0.5064
Epoch 19/20
176/176 [==============================] - 1s 4ms/step - loss: 0.5049 - accuracy: 0.6884 - val_loss: 2.8298 - val_accuracy: 0.5040
Epoch 20/20
176/176 [==============================] - 1s 4ms/step - loss: 0.4932 - accuracy: 0.6892 - val_loss: 2.9769 - val_accuracy: 0.5020
```

Рис. 1. Результаты обучения полносвязной нейронной сети

С помощью функции **pit.piot** можно построить график обучения. Ниже провидены два графика на разных этапах обучения (рис. 2), по ним можно сделать вывод, что доля правильных ответов на учебном наборе данных стабильно растет, а на проверочном наборе данных не изменяется.

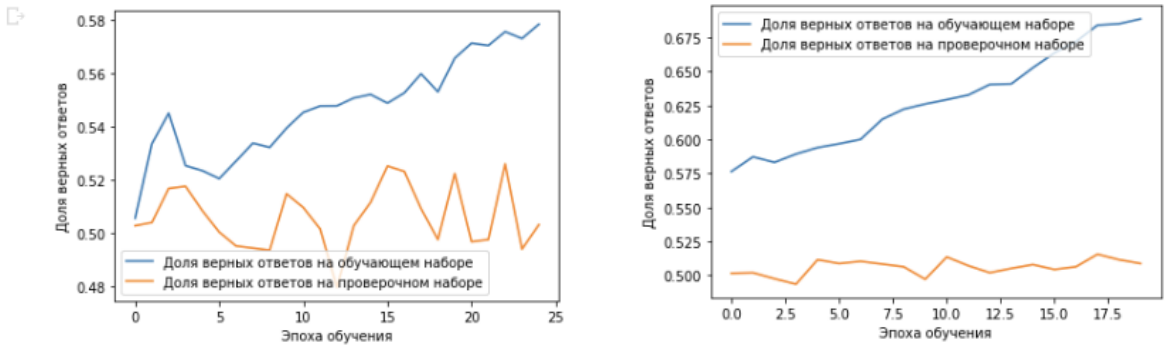


Рис. 2. Сравнение графиков после двух циклов обучения

Производим проверку работы сети на тестовом наборе данных. Доля правильных ответов остается в рамках 50%. Таким образом можно сказать, что сеть выбирает ответ случайно.

Теперь для сравнения выполним точно такую же задачу, но используя рекуррентную нейронную сеть. Это такой вид нейронных сетей, где связи между элементами образуют направленную последовательность. Благодаря этому появляется возможность обрабатывать серии событий во времени или последовательные пространственные цепочки [5].

Различие с первым способом заключается в том, что при тексте короче 200 символов, нули добавляются не в конце текста, а в начале. Это делается из-за того, что нейронная сеть запоминает, что было на предыдущих этапах, но делает это на не большой промежуток времени, поэтому важно, чтобы в

конце набора данных содержались осмысленные данные, если в конце данных содержатся нули, то рекуррентная нейронная сеть преимущественно будет анализировать эти нули, а не осмысленную часть данных. Поэтому результат работы будет не очень качественным.

Обучение рекуррентной сети идет значительно медленнее, чем обучение полносвязной сети. Всего эпох обучения 15. На рис. 3 можно увидеть, что на последнем этапе доля правильных ответов на обучающем наборе составляет 95% (синий), а на проверочном 85% (красный). Результат хороший, но на 14 шаге результат был чуть выше (86%), пошло переобучение. Необходимо уменьшить количество эпох. В этом заключается существенное различие между рекуррентными нейронными сетями и полносвязными. Рекуррентную сеть проще переобучить.

```
Epoch 1/15
176/176 [==============================] - 35s 181ms/step - loss: 0.6138 - accuracy: 0.6833 - val_loss: 0.5757 - val_accuracy: 0.7080
Epoch 2/15
176/176 [==============================] - 32s 184ms/step - loss: 0.4650 - accuracy: 0.8227 - val_loss: 0.4238 - val_accuracy: 0.8332
Epoch 3/15
176/176 [==============================] - 32s 183ms/step - loss: 0.3860 - accuracy: 0.8519 - val_loss: 0.4153 - val_accuracy: 0.8172
Epoch 4/15
176/176 [==============================] - 31s 178ms/step - loss: 0.3351 - accuracy: 0.8715 - val_loss: 0.3668 - val_accuracy: 0.8492
Epoch 5/15
176/176 [==============================] - 31s 177ms/step - loss: 0.2870 - accuracy: 0.8908 - val_loss: 0.3364 - val_accuracy: 0.8580
Epoch 6/15
176/176 [==============================] - 31s 178ms/step - loss: 0.2574 - accuracy: 0.9044 - val_loss: 0.3344 - val_accuracy: 0.8652
Epoch 7/15
176/176 [==============================] - 31s 175ms/step - loss: 0.2319 - accuracy: 0.9150 - val_loss: 0.3336 - val_accuracy: 0.8700
Epoch 8/15
176/176 [==============================] - 31s 177ms/step - loss: 0.2167 - accuracy: 0.9223 - val_loss: 0.3410 - val_accuracy: 0.8572
Epoch 9/15
176/176 [==============================] - 32s 181ms/step - loss: 0.1937 - accuracy: 0.9311 - val_loss: 0.3520 - val_accuracy: 0.8508
Epoch 10/15
176/176 [==============================] - 34s 191ms/step - loss: 0.1826 - accuracy: 0.9358 - val_loss: 0.3489 - val_accuracy: 0.8580
Epoch 11/15
176/176 [==============================] - 31s 177ms/step - loss: 0.1723 - accuracy: 0.9404 - val_loss: 0.3643 - val_accuracy: 0.8588
Epoch 12/15
176/176 [==============================] - 31s 174ms/step - loss: 0.1641 - accuracy: 0.9450 - val_loss: 0.3791 - val_accuracy: 0.8652
Epoch 13/15
176/176 [==============================] - 31s 175ms/step - loss: 0.1544 - accuracy: 0.9466 - val_loss: 0.3708 - val_accuracy: 0.8572
Epoch 14/15
176/176 [==============================] - 31s 178ms/step - loss: 0.1471 - accuracy: 0.9502 - val_loss: 0.3925 - val_accuracy: 0.8612
Epoch 15/15
176/176 [==============================] - 31s 177ms/step - loss: 0.1411 - accuracy: 0.9529 - val_loss: 0.3913 - val_accuracy: 0.8544
```

Рис. 3. Результат обучения рекуррентной нейронной сети

На рис. 4 представлен график обучения нейронной сети.

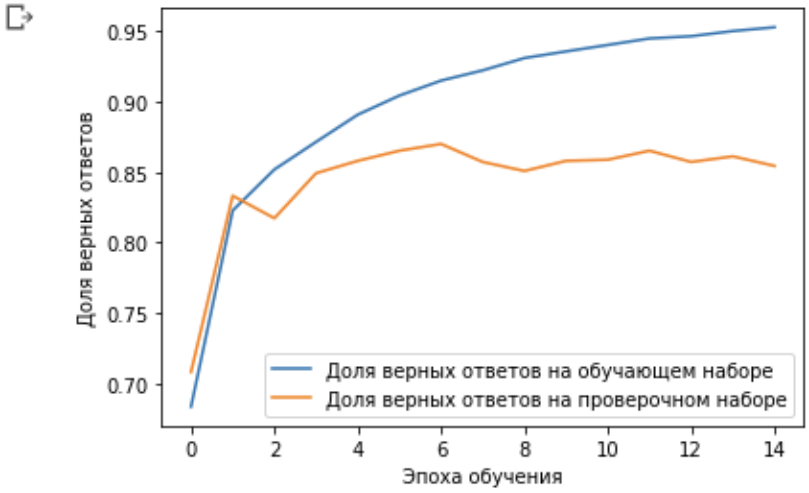


Рис. 4. Диаграмма с данными о результатах обучения

По результатам работы можно сделать вывод. В данной статье были использованы два способа анализа тональности текста. С использованием полносвязной нейронной сети и с использованием рекуррентной сети.

В первом способе не все варианты представления текста в виде набора чисел подходят для анализа, самый простой вариант, который использует по умолчанию Keras не подходит для обучения нейронной сети.

Второй способ оказался эффективным. Использовать реккурентную сеть достаточно просто. Единственное, нужно уделить внимание двум вещам: дополнение данных должно выполняться сначала, содержательные данные должны находиться в конце и необходимо следить за количеством эпох, чтобы не было переобучения.

Список используемых источников:

1. Самигулин Т. Р., Джурабаев А. Э. У. Анализ тональности текста методами машинного обучения // Научный результат. Информационные технологии. Т. 6, N 1, 2021.

2. Sergey Smetanin, Анализ тональности в русскоязычных текстах, часть 1, 2020 [Электронный ресурс] URL: https://habr.com/ru/companies/vk/articles/516214/ (дата обращения: 16.10.2023).

3. Soslan Tabuev, Рекуррентные нейронные сети (RNN) с Keras, 2020 [Электронный ресурс] URL: https://habr.com/ru/articles/487808/ / (дата обращения: 15.10.2023).

4. Виткова Л. А., Лешукова А. М. Детектирование объектов на изображениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы XII Междунар. науч.-технич. и науч.-методич. конф., Санкт-Петербург, 28 фев.-01 марта 2023 г. СПб. : СПбГУТ, 2023. С. 272-275.

5. Меняйлов Д. В., Преображенский А.П. Сравнительный анализ результатов, полученных при решении задачи анализа тональности текста с помощью сверточной и рекуррентной нейронных сетей // Моделирование, оптимизация и информационные технологии. 2021. N 9(4).

Kurmanov I., Leshukova A., Petrova T.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Neural networks for analyzing text tone.

In the modern world, which is becoming increasingly dependent on information technology, text sentiment analysis is of great importance. Neural networks trained to recognize and classify the emotional tone of texts play an important role in areas such as social media, marketing, finance and many others. In this article we will consider the relevance of this topic, scope of application, existing architectures, and also consider in practice which architecture is better suited for text sentiment analysis.

Key words: data set, text sentiment, information technology, information, fully connected neural networks, recurrent neural networks.

УДК 004.056.5
ГРНТИ 49.33.95

ИННОВАЦИОННЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ СЕТЯХ: РОЛЬ ОБОРУДОВАНИЯ S-TERRA CSP И ШИФРОВАНИЯ ГОСТ

И. О. Курманов, В. С. Синельщиков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В наше время, когда киберугрозы становятся все более сложными и разнообразными, обеспечение надежной кибербезопасности в корпоративных сетях становится первостепенной задачей. Эта статья исследует инновационные подходы к обеспечению кибербезопасности, с особым вниманием к роли оборудования S-Terra CSP и шифрования ГОСТ. Мы рассмотрим актуальные угрозы кибербезопасности, технические особенности S-Terra CSP и надежность ГОСТ-шифрования, а также покажем, как их совместное использование может значительно усилить защиту корпоративных сетей.

кибербезопасность, S-Terra, шифрование, вредоносное ПО

1. Введение

В нашу эпоху цифровой трансформации и растущей зависимости бизнеса от информационных технологий, кибербезопасность становится неотъемлемой частью функционирования организаций. Корпоративные сети становятся мишенью для хакеров, кибертеррористов и кибершпионов. В этом контексте встает задача разработки инновационных подходов к обеспечению кибербезопасности.

Данная статья посвящена исследованию современных подходов к решению проблемы кибербезопасности в корпоративных сетях. Мы обратим внимание на два ключевых компонента этой задачи: оборудование S-Terra CSP и использование шифрования ГОСТ.

2. Современные угрозы кибербезопасности в корпоративных сетях

2.1 Обзор актуальных видов киберугроз

В данной секции главы, проведем обширный анализ современных видов киберугроз, которые представляют актуальные угрозы для корпоративных сетей. Эти угрозы включают в себя:

DDoS-атаки (*Distributed Denial of Service*) – вид атак, при котором злоумышленники стремятся перегрузить сетевую инфраструктуру, делая веб-сервисы и другие системы недоступными для легитимных пользователей. Эти атаки могут оказать сильное воздействие на доступность онлайн-сервисов и бизнес-процессов.

Фишинг (phishing) - разновидность попыток несанкционированного доступа, когда жертву провоцируют на разглашение информации, посылая ей фальсифицированное электронное письмо с приглашением посетить веб-сайт, который на первый взгляд связан с законным источником. [5]

Вымогальщики - вредоносное программное обеспечение, которое зашифровывает данные организации, требуя выкуп за их расшифровку. Атаки рэнсомваров могут нанести значительный ущерб, как финансовый, так и для репутации компании.

Утечка данных и внутренние угрозы: внутренние угрозы могут происходить со стороны сотрудников, которые могут неосторожно или намеренно утечь конфиденциальные данные. Кроме того, организации должны бороться с угрозами, связанными с утечкой информации и нарушением безопасности.

2.2 Угроза вымогальщиков

В 2011 году произошла атака на Криптошлюз RSA SecurID, которая является одной из наиболее серьезных атак на криптографическое оборудование и системы идентификации. RSA SecurID представляет собой систему аутентификации, широко используемую организациями и корпорациями для обеспечения безопасного доступа к сети и приложениям.

Злоумышленники, известные как APT (*Advanced Persistent Threat*), начали атаку с отправки фишинговых электронных писем с вредоносными вложениями сотрудникам RSA. Один из сотрудников компании открыл вредоносное вложение, что привело к заражению его рабочей станции.

Сначала взломан был рабочий компьютер сотрудника, но затем атакующие начали двигаться глубже в сеть RSA. Они использовали скомпрометированный компьютер для получения доступа к серверам, содержащим информацию о системах аутентификации RSA SecurID.

Злоумышленники успешно выкрали информацию, связанную с системой RSA SecurID, включая алгоритмы и сиды (начальные значения) для генерации одноразовых паролей. Эта информация дала им возможность взломать системы RSA SecurID, используемые клиентами RSA для двухфакторной аутентификации.

Атака привела к серьезной компрометации систем RSA SecurID, что могло повлиять на безопасность множества организаций и компаний, использующих эту систему для защиты доступа к своим данным и ресурсам.

Злоумышленники, обладая доступом к системе RSA SecurID, могли потенциально распространить атаку на клиентов RSA, использующих уязвимые версии системы, что вызвало беспокойство в сообществе информационной безопасности. Атака повлекла за собой потерю доверия к системам безопасности и заставила множество организаций пересматривать свои подходы к аутентификации и безопасности данных.

В результате этой атаки организации столкнулись с необходимостью усилить меры безопасности и обновить свои системы аутентификации, чтобы предотвратить подобные инциденты в будущем.

2.3 Важность адаптивных методов защиты

Помимо технических мер, работники должны быть должным образом обучены и информированы о потенциальных рисках. Они должны знать, как

обращаться с конфиденциальной информацией и как обнаруживать подозрительную активность в сети.

Важным элементом защиты системы RSA SecurID является непрерывный мониторинг сети и системы. Это позволяет выявлять необычную активность, связанную с попытками несанкционированного доступа и идентификацией аномалий, которые могли бы указывать на потенциальные атаки.

В случае атаки или даже подозрения на инцидент, необходимо немедленно приступать к действиям. Быстрое реагирование на инциденты, включая изоляцию заразившихся систем и блокировку потенциальных источников атаки, помогает предотвратить дополнительные ущерб и распространение инцидента.

Атака на Криптошлюз RSA SecurID в 2011 году подчеркивает, что в области кибербезопасности не существует абсолютно надежных методов защиты. Обучение сотрудников, постоянный мониторинг и разработка четких процедур реагирования на инциденты являются важными шагами в обеспечении безопасности при работе с критической информацией. [3]

3. Особенности оборудования S-Terra CSP

3.1. Описание оборудования S-Terra CSP и его технических характеристик

S-Terra Client предназначен для защиты от несанкционированного доступа, сетевых атак, создания защищенных VPN соединений между устройством, на котором он установлен, и другими взаимодействующими с ним доверенными VPN-шлюзами и VPN-клиентами.[1]

Продукт S-Terra Client выполняет следующие функции:

защиту трафика на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP

пакетную и контекстную фильтрацию любого исходящего и входящего трафика на хост с использованием информации в полях заголовков сетевого, транспортного и прикладного уровней;

фильтрацию с учетом входного и выходного сетевого интерфейса;

фильтрацию запросов на установление виртуальных соединений;

фильтрацию по любым значимым полям IP-заголовка и полям данных сетевого пакета;

фильтрацию с учетом даты и времени;

аутентификацию пользователя и аутентификацию узла сети;

идентификацию и аутентификацию администратора при доступе с целью администрирования;

событийное протоколирование;

реализацию заданной дисциплины взаимодействия (аутентификацию и/или защиту трафика) для каждого защищенного соединения, доступ в заданном защищенном режиме только для зарегистрированных, в том числе и для мобильных партнеров по взаимодействию;

регулируемую стойкость защиты трафика.[1]

3.2 Рассмотрение возможностей оборудования для обеспечения безопасности корпоративных сетей

Оборудование S-Terra оснащено многоядерным процессором, что обеспечивает высокую производительность и способность обрабатывать большие объемы сетевого трафика. Это особенно важно для эффективного функционирования корпоративных сетей.

Защита включает в себя систему обнаружения вторжений (IDS) и систему предотвращения вторжений (IPS). Эти методы позволяют обнаруживать и предотвращать различные виды атак, обеспечивая безопасность сети.

Глубокий анализ сетевого трафика: Оборудование S-Terra обеспечивает глубокий анализ сетевого трафика, что позволяет выявлять скрытые атаки и аномалии в сетевой активности.

Шифрование и управление доступом: S-Terra предоставляет возможность высокоуровневого шифрования данных как в процессе передачи, так и при их хранении. Механизмы контроля доступа позволяют управлять доступом к ресурсам и сети, обеспечивая только авторизованным пользователям доступ к важной информации.

Интеграция в корпоративную инфраструктуру: Оборудование S-Terra легко интегрируется в корпоративную инфраструктуру, что упрощает процесс внедрения и обеспечивает совместимость с другими системами и приложениями.

Поддержка стандартов и регулирований: S-Terra учитывает особенности российской информационной среды и соблюдает стандарты и требования безопасности, что делает его идеальным выбором для организаций, работающих в России.

Оборудование S-Terra предоставляет надежные и эффективные средства для обеспечения безопасности корпоративных сетей, обеспечивая высокий уровень защиты данных и системы в целом.

4. Шифрование ГОСТ и его применение в кибербезопасности

4.1 История и развитие ГОСТ

Стандарты ГОСТ имеют свои корни в Советском Союзе, где они были разработаны для обеспечения безопасности важной информации и коммуникаций. С течением времени эти стандарты претерпели ряд изменений и обновлений, чтобы соответствовать современным требованиям. Это включает в себя развитие более сильных криптографических алгоритмов и методов шифрования.

4.2 Алгоритмы и принципы шифрования

ГОСТ-шифрование включает разнообразные алгоритмы и принципы шифрования, которые обеспечивают защиту конфиденциальных данных. Среди них:

Блочные шифры: ГОСТ использует блочные шифры, которые делят данные на блоки и шифруют их по-отдельности. Это обеспечивает эффективную защиту данных в движении. [2]

Асимметричное шифрование: ГОСТ включает асимметричные шифры, которые позволяют безопасно обмениваться ключами и обеспечивать конфиденциальность данных.

4.3 Надежность ГОСТ

Оценка надежности стандартов ГОСТ включает сравнение с международными стандартами шифрования, такими как AES и RSA. Принципиальное различие шифров AES и «Кузнечик» заключается в алгоритме развертки ключа. Это позволяет определить, насколько ГОСТ соответствует современным методам атак и взлома. [4] Следует учитывать, что ГОСТ обладает рядом преимуществ, включая соблюдение российских законов о кибербезопасности, что может быть важным для организаций, действующих на российском рынке.

5. Заключение

Оборудование S-Terra CSP, предоставляет многоуровневую защиту сетей, включая DDoS-защиту, шифрование данных и контроль доступа.

ГОСТ-шифрование продолжает развиваться и предоставляет надежные методы защиты информации. Соблюдение современных стандартов безопасности несомненно играет важную роль.

Несмотря на разнообразие методов защиты, кибербезопасность требует постоянного обновления и готовности к реагированию на новые угрозы. Стратегии кибербезопасности должны быть комплексными и гибкими.

Важно помнить, что безопасность информации становится все более важным аспектом современного мира, и наша статья призвана помочь организациям лучше понимать и применять адаптивные методы защиты и соблюдать современные стандарты безопасности.

Список используемых источников:

1. Программный комплекс С-Терра Клиент. Версия 4.1. Руководство пользователя [Электронный ресурс] https://studylib.ru/doc/2675895/csp-vpn-client.-rukovodstvo-pol._zovatelya---s/ (дата обращения: 23.10.2023)

2. ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. М. : Стандартинформ, 2018.

3. Jarmoc J. RSA compromise: impacts on SecurID // Secureworks, March. 2011. Т. 7.

4. Соболев М. А. Сравнительный анализ российского стандарта шифрования по ГОСТ Р 34.12-2015 и американского стандарта шифрования AES / М. А. Соболев // Политехнический молодежный журнал. 2022. N 4(69). DOI 10.18698/2541-8009-2022-4-785. EDN NZADXD.

5. ГОСТ Р 56205-2014. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели. М. Стандартинформ, 2014.

Kurmanov I., Sinelschikov V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Innovative Approaches to Ensuring Cyber Security in Corporate Networks: The Role of S-Terra CSP Equipment and GOST Encryption.

At a time when cyber threats are becoming more complex and diverse, ensuring strong cybersecurity in corporate networks has become a top priority. This article explores innovative

approaches to cybersecurity, with a particular focus on the role of S-Terra CSP hardware and GOST encryption. We will look at current cybersecurity threats, technical features of S-Terra CSP and the reliability of GOST encryption, and also show how their combined use can significantly strengthen the protection of corporate networks.

Key words: cybersecurity, S-Terra, encryption, malware.

УДК 004.056
ГРНТИ 81.93.29

КОНЦЕПТ КИБЕРИММУННЫХ ОПЕРАЦИОННЫХ СИСТЕМ НА ПРИМЕРЕ KASPERSKY OS

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

В связи с повсеместным распространением цифровых технологий, в том числе на производствах, возникает потребность в создании информационной системы, которая была бы защищена по умолчанию. Решением может стать создание системы с кибериммунным подходом, который подразумевает защиту системы, встроенную на уровне архитектуры.

кибериммунитет, защищенные системы, ОС, secure by design, кибербезопасность

В настоящее время информационные системы сталкиваются с непрерывно возрастающим количеством кибератак [1] (рис 1.).

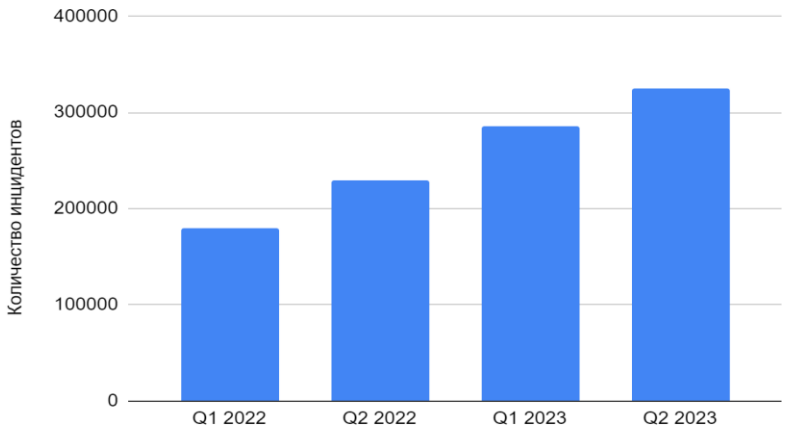


Рис. 1. Статистика инцидентов за первый и второй кварталы

Для более эффективной борьбы с киберугрозами, необходимо пересмотреть подходы к созданию информационных систем. Одним из способов повышения защищенности и надежности может стать разработка систем, которые изначально обладают высоким уровнем защиты – "кибериммунных" систем.

Понятие “кибериммунитет” подразумевает, что информационные системы должны быть спроектированы и разработаны изначально защищенными. В то время, как классический подход подразумевает использование дополнительных продуктов безопасности, кибериммунитет предполагает интеграцию таковых в каждый этап жизненного цикла разработки системы. Такой подход позволяет нивелировать существующие угрозы ИБ и поддерживать систему функциональной даже при частичном отказе некоторых компонентов. Таким образом повышается уровень

отказоустойчивости информационных систем, также сокращаются расходы, связанные с восстановлением после успешных кибератак. Важно понимать, что кибериммунитет это не набор технических мер безопасности, а принципиально новая методология построения защищенных систем.

Реализация кибериммунного подхода включает в себя ряд ключевых принципов:

- *Secure by Design*. Этот принцип подразумевает интеграцию мер безопасности в каждый этап жизненного цикла разработки информационной системы. Безопасность должна быть учтена с самого начала проектирования, а не добавляться в систему впоследствии;
- Принцип наименьших привилегий. Пользователи и процессы должны иметь только те привилегии, которые необходимы для выполнения задач;
- Четкое определение объекта защиты и условий, в которых может эксплуатироваться система. Например, объектом защиты может быть конфиденциальность данных;
- Изоляция компонентов. Каждый компонент (группа компонентов) должен быть вынесен в собственный домен безопасности, с назначением каждому из них уровня доверия;
- Ограничение взаимодействия информации внутри системы. Прямое взаимодействие между доменами исключается и контролируется системой безопасности.

Примером кибериммунной системы может послужить разработка “Лаборатории Касперского” – операционная система “*Kaspersky OS*”. Ключевая особенность данной системы заключается в использовании микроядра, которое содержит в себе несколько десятков строк кода [2], по сравнению с другими операционными системами, такими как семейство *Linux*, ядро (версии 5.19) которых содержит около 30 миллионов строк кода [3] (рис. 2).

Рис. 2. Сравнение количества строк кода, содержащихся в ядрах систем

Помимо микроядра также стоит выделить Kaspersky Security System [4] – подсистему, которая проверяет корректность межпроцессных сообщений. Таким образом, сущности изолированы и не могут взаимодействовать напрямую, все взаимодействие регулируется политиками безопасности и подсистемой KSS, что не позволяет эксплуатировать уязвимости системы. Схема межпроцессного взаимодействия представлена на рис. 3.

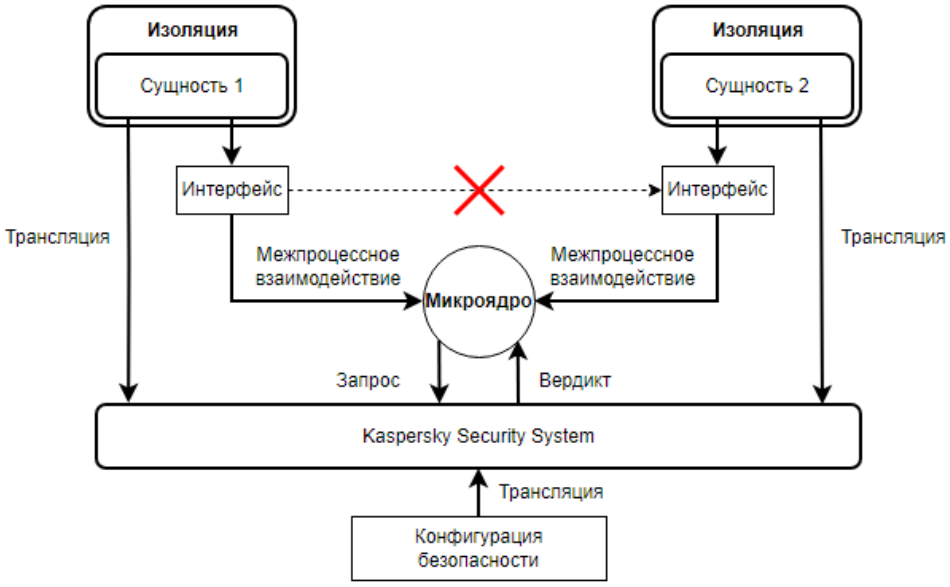


Рис. 3. Принцип взаимодействия в системе *Kaspersky OS*

Такая система дает несколько преимуществ, например запрет любых взаимодействий, которые не разрешены. Также разделены системы безопасности и код приложений, что позволяет изменять их независимо друг от друга.

Кибериммунный подход имеет следующие преимущества:

- Повышение отказоустойчивости и надежности. Благодаря структуре таких систем большинство атак неэффективны и даже при успешном проведении атаки система остается функциональной;
- Снижение затрат на наложенное ПО. Использование систем с защитой на уровне архитектуры позволяет снизить расходы на дополнительные продукты безопасности.

Однако, можно выделить и некоторые недостатки:

- Затраты на начальное проектирование. Создание кибериммунной системы с нуля может потребовать больших финансовых затрат;
- Сложность реализации. Создание проприетарной кибериммунной системы требует высокой квалификации и наличия знаний в области разработки подобных ИС;
- Ограничение в гибкости. Учитывая специфику создания таких систем и принцип их работы, могут возникнуть сложности во взаимодействии уже существующих программных и аппаратных продуктов с подобными системами.

Таким образом, в связи с цифровым развитием и увеличением количества ИС, в том числе с выходом в сеть Интернет, увеличивается и количество возникающих угроз. Классические подходы к обеспечению безопасности могут стать малоэффективными, поэтому необходима разработка принципиально новых решений. В целом, кибериммунитет представляет собой перспективный подход к обеспечению безопасности информационных систем, который дает возможность повысить эффективность борьбы с существующими и принципиально новыми киберугрозами.

Список используемых источников:

1. Количество кибератак на российские организации в 2023 году заметно выросло [Электронный ресурс]. URL: https://rg.ru/2023/07/27/kolichestvo-kiberatak-na-rossijskie-organizacii-v-2023-godu-zametno-vyroslo.html (дата обращения: 27.10.2023).
2. Микроядро KasperskyOS. Основа микроядерной операционной системы [Электронный ресурс]. URL: https://os.kaspersky.ru/technologies/microkernel/ (дата обращения: 27.10.2023).
3. Ядру Linux исполнился 31 год [Электронный ресурс]. URL: https://www.opennet.ru/opennews/art.shtml?num=57675 (дата обращения: 27.10.2023).
4. Микроядерная операционная система для отраслей с повышенными требованиями к информационной безопасности [Электронный ресурс]. URL: https://os.kaspersky.ru/wp-content/uploads/sites/29/2022/09/kasperskyos_tech_ru.pdf (дата обращения: 27.10.2023).

Kutuev T.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

The Concept of Cyber-Immune Operating Systems on The Example of Kaspersky OS.

Due to the ubiquity of digital technologies, including in production, there is a necessity to create an information system that would be secured by design. The solution may be to create a system with a cyber-immune approach, which implies the protection of the system embedded at the architecture level.

Key words: cyber-immunity, secure systems, OS, secure by design, cybersecurity

УДК 004.056.5
ГРНТИ 81.93.29

ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ, СВЯЗАННЫХ С ПРИМЕНЕНИЕМ ДИПФЕЙКОВ

Е. А. Лободина, Т. Д. Наумова, С. М. Шестаков
Санкт-Петербургский государственный университет промышленных технологий и дизайна

Из года в год люди все чаще сталкиваются с чем-то, в создании чего в той или иной степени принимал участие искусственный интеллект. Одним из продуктов генерации чего-то нового на базе уже существующего посредством синтеза является дипфейк. Дипфейки могут быть как безобидны, так и представлять угрозы, связанные с кражей данных в результате дезинформирования. Необходимо здраво оценивать риски, которые использование дипфейков в корыстных целях может создавать для бизнеса и общественности.

дипфейк, искуственный интеллект, дезинформация, безопасность

За последнее десятилетие новостные статьи и заметки, так или иначе связанные с применением искусственного интеллекта в различных областях науки и медицины, а также в повседневной человеческой жизни, все чаще становятся поводами для дискуссий людей из совершенно разных сфер занятости.

Спектр видов технологий на базе искусственного интеллекта стабильно расширяется, уже сегодня человечество имеет шанс наблюдать как нейросети генерируют изображения по текстовым описаниям, используются для судебной консультации перед вынесением приговора [1], осуществляют наложения некоторых изображений и видео на уже существующие фото и видеоролики.

В данной работе речь как раз идет о последнем пункте из всего вышеперечисленного, а именно о технологии синтеза изображений и голоса, называемой дипфейком.

Термин дипфейк объединяет в себе понятия глубокого обучения нейросетей (*deep learning*) и чего-то, что не является настоящим (*fake*). В основе такого метода лежит использование алгоритмов машинного обучения для создания измененных или искусственных изображений, видео или аудиозаписей. Эти алгоритмы позволяют компьютеру "подделать" лицо человека на фотографии или видео, заменить голос в аудиозаписи и многое другое.

При создании дипфейков обычно используется генеративно-состязательная сеть (*GAN*), которая состоит из двух составляющих: генератора и дискриминатора. Генератор создает новый контент, а дискриминатор пытается определить, настоящий ли это контент или дипфейк. В процессе обучения эти две части нейронной сети постоянно совершенствуются и приводят к более реалистическим дипфейкам.

Получив широкую известность в 2017 г. из-за возникновения некоторых этических проблем [2] в результате применения технологии, использование дипфейков и в настоящем времени может создавать инциденты и риски, затрагивающие вопросы информационной безопасности. Оценка угроз безопасности, связанных с дипфейками, является важным аспектом в борьбе с их негативными последствиями.

В первую очередь, одной из главных проблем является возможность распространения дезинформации. Дипфейки могут быть использованы для создания фальшивых новостей, подделки публичных выступлений или искажения фактов, что может серьезно нарушить доверие к достоверности получаемой информации.

Помимо этого, дипфейки могут стать средством манипуляции и воздействия на массы. Под видом настоящего человека или происходящего события они могут повлиять на общественное мнение, изменить представления о действительности, создать настроения, не соответствующие реальному положению дел, запустить процессы, угрожающие различными негативными последствиями для отдельных индивидов, какой-либо инфраструктуры, а также для общества в целом.

Например, целевой фишинг [3] рассчитан на то, чтобы обмануть конкретных сотрудников определённой компании и заставить их выполнить вручную какую-либо операцию, которой может стать оплата поддельного платёжного поручения или предоставление нужных злоумышленнику файлов и документов.

Противодействие угрозам безопасности, связанным применением дипфейков, включает несколько аспектов.

Во-первых, необходимо разрабатывать и улучшать алгоритмы и технологии, которые могут идентифицировать дипфейки. Различные исследования по разработке систем распознавания фальшивых видео или аудиозаписей помогут выявить и предупредить их использование.

Во-вторых, обучение и информирование общества о том, как распознавать и анализировать подозрительные видео или аудиозаписи, является важным шагом в борьбе с угрозами безопасности, связанными с дипфейками. Это поможет людям стать более разборчивыми и бдительными в отношении цифровой информации, которую они потребляют.

Наконец, сотрудничество между государствами, технологическими компаниями и общественностью имеет большое значение в обеспечении безопасности и противодействии дипфейкам. Совместные усилия, разработка правового регулирования и совершенствование технологий помогут более эффективно бороться с этой проблемой.

Таким образом, оценка угроз безопасности, связанных с применением дипфейков, является актуальной и сложной задачей. Тем не менее, продолжается работа над развитием новых методов и подходов, чтобы научить общественность и специальные алгоритмы отличать оригинальную

достоверную информацию от модифицированной посредством синтеза речи и изображения.

Список используемых источников:

1. Судья в Колумбии использовал ChatGPT для вынесения приговора [Электронный ресурс]. URL: https://habr.com/ru/news/714982/ (дата обращения: 11.10.2023).

2. Технология двойного назначения: вред или польза дипфейков [Электронный ресурс]. URL: https://trends.rbc.ru/trends/industry/637738a09a79478e6797b557 (дата обращения: 11.10.2023).

3. Технологии Deepfake как угроза информационной безопасности [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Deepfakes-as-a-information-security-threat (дата обращения: 11.10.2023).

Lobodina E., Naumova T., Shestakov S.

Saint-Petersburg State University of Industrial Technologies and Design

Assessment of security threats associated with the use of deepfake technology.

From year to year, people are increasingly faced with something in the creation of which artificial intelligence took part to one degree or another. One of the products of generating something new based on something already existing through synthesis is a deepfake. Deepfakes can be harmless or pose threats involving data theft as a result of misinformation. It is necessary to sensibly assess the risks that the use of deepfakes for personal gain can create for businesses and the public.

Key words: Deepfake, artificial intelligence, disinformation, security.

УДК 004.056
ГРНТИ 81.93.29

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ LORA ДЛЯ СОЗДАНИЯ ЗАЩИЩЁННЫХ РАДИОМАЯКОВ БПЛА

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

Разработчики и производители беспилотных летательных аппаратов постоянно работают над повышением надежности и снижением вероятности потери аппарата. Системы управления передают GPS-координаты, но они могут быть неточными. Для более надежного поиска упавшего аппарата необходима резервная автономная система связи. В данной работе рассмотрены особенности и выдвинуты требования к такой системе. Разработан прототип и подведены итоги его испытаний.

БПЛА, поисковой модуль, защита радиоканала, шифрование

В наше время беспилотные летательные аппараты (БПЛА) находят применение во многих сферах нашей жизни, что упрощает выполнение ряда сложных работ, которые занимают много времени или требуют значительных финансовых вложений. На сегодняшний день БПЛА используются в различных областях, таких как:

- Логистика и доставка,
- Аграрная индустрия,
- Аэрофотосъёмка,
- Геодезия и поиск полезных ископаемых аэромагнитной съемкой,
- Поисково-спасательные операции,
- Тепловизионная съёмка.

Разработчики и производители БПЛА постоянно работают над повышением надежности и снижением вероятности потери аппарата. Одной из причин аварийных посадок является человеческий фактор. Системы управления передают GPS-координаты, но они могут быть неточными. Для более надежного поиска упавшего аппарата необходима резервная автономная система связи. Радиомаяк является эффективным способом поиска, но существующие радиомаяки имеют недостатки, которые могут приводить к сбоям и потере связи. Необходимо улучшить их качество, так-как они могут быть подвержены помехам и не обладают достаточной точностью передачи данных. Также важно обеспечить безопасность передачи данных, используя защиту на программном уровне. Это позволит предотвратить компрометацию данных и кражу оборудования.

При конструировании радиомаяка для беспилотных летательных аппаратов, необходимо учитывать ряд важных требований, чтобы обеспечить его эффективность и надежность в работе.

1. Автономность,
2. Универсальность,

3. Простота использования,
4. Компактность,
5. Защищённость канала связи,
6. Длительное время работы,
7. Дальность действия.

На данный момент на рынке представлено несколько вариантов подобных маяков.

Радиомаяк Rockwell B5

Программируемый радиомаяк, использующий аналоговую передачу данных на частоте 433 МГц. Для поиска используется пеленгация при помощи тоновых сигналов.

Радиомаяк tBeacon Onyx

Радиомаяк для поиска упавших авиамоделей. Автономный со встроенным приемником GPS/ ГЛОНАСС. Использует технологию передачи Lora.

Миниатюрный GPS трекер TKSTAR TK913

GPS GSM трекеры часто используются вместо радиомаяков, но их главным недостатком является возможность работы только при наличие сотовой связи.

ТАБЛИЦА 1. Анализ существующих решений

	шифрование	Дальность	Тип сигнала
ROCKWELL B5	-	3-5 км	аналоговый
tBeacon Onyx	-	до 20 км в прямой видимости	цифровой (Lora)
TKSTAR TK913	+	Работает в зоне дейсвия сотовой связи	GSM

При обзоре существующих решений, было выявлено, что большинство радиомаяков для БПЛА основаны на протоколе передачи данных GSM, что определенным образом ограничивает их использование. Например, стоимость использования GSM-модуля может оказаться значительно выше, чем в случае использования других видов связи. Некоторые решения, использующие Lora-технологию, также были проанализированы. Но ни одно из них не использует шифрование данных. В целом, имеется множество радиомаяков для БПЛА, однако, каждый из них имеет свои преимущества и недостатки.

Из всего описанного выше можно сделать вывод, что наилучшим вариантом реализации поискового маяка является использование технологии Lora и программной реализации шифрования данных в соответствии. Что решит проблемы дальности передачи данных и их защиты.

Таким образом, целью данной работы является разработка макета и тестирование защищённого маяка с применением технологии Lora.

В таблице 2 представлен список комплектующих для реализации макета:

ТАБЛИЦА 2. Список комплектующих

Arduino UNO	2 шт.
Модуль LoRa ebyte e32 433 Мгц	2 шт.
Модуль GPS Beitian BN-180	1 шт.
Модуль Bluetooth HC-06	1 шт.

Arduino - это открытая платформа для разработки, основанная на микроконтроллере семейства AVR, который может быть запрограммирован для управления различными устройствами и компонентами [1]. Эта платформа позволяет легко создавать прототипы и тестировать проекты, а также легко модифицировать их в процессе разработки.

Модуль LoRa ebyte e32 433 Мгц – радиомодуль на основе технологии *LoRa*, обеспечивающий беспроводную связь с большой дальностью передачи данных [2].

Модуль GPS Beitian BN-180 – миниатюрный GPS-модуль, предназначенный для определения координат и времени.

Модуль Bluetooth HC-06 – модуль беспроводной связи на базе технологии Bluetooth, обеспечивающий коммуникацию между микроконтроллером и смартфоном [3].

В качестве метода для защиты передаваемой информации было выбрано шифрование AES-128:

AES (Advanced Encryption Standard) - это цифровой алгоритм шифрования, который широко используется для защиты конфиденциальной информации. Основой AES является блочный алгоритм шифрования. Имеется два варианта AES - с длиной ключа в 128 бит и с длиной ключа в 256 бит [4]. AES работает по принципу подстановки и перестановки. Это означает, что каждый блок данных шифруется с помощью ключа. Каждый последующий блок, в свою очередь, зашифровывается путем изменения ключа, то есть он использует предыдущий блок в качестве ключа [5]. Это обеспечивает высокий уровень безопасности, потому что даже если кто-то узнает ключ, он не сможет расшифровать остальные блоки данных без знания предыдущих блоков. Одним из преимуществ AES является его быстрая скорость работы в сравнении с другими алгоритмами шифрования. Это связано с тем, что он простой в реализации и не требует больших вычислительных мощностей. Недостатком AES является его уязвимость к атакам по сторонним каналам. Например, злоумышленник может перехватывать электромагнитное излучение, которое создается компьютером при работе с ключом шифрования, и использовать его для взлома. Тем не менее, AES является одним из наиболее безопасных алгоритмов шифрования, который широко используется в банковском секторе, правительственных учреждениях, военных организациях и других институтах, где конфиденциальность является ключевым фактором.

Таким образом, в ходе проведения испытаний и анализа аналогичных решений было выявлено, что применение технологии Lora для создания

защищённых радиомаяков является перспективным направлением и требует дальнейшего исследования.

Список используемых источников:

1. docs.arduino.cc [Электронный ресурс] URL: https://docs.arduino.cc/learn/starting-guide/whats-arduino (дата обращения: 12.11.2023).
2. Lora EBYTE E32 User manual [Электронный ресурс] URL: https://www.ebyte.com/en/pdf-down.aspx?id=775 (дата обращения: 12.11.2023).
3. petegsx-projects.github.io HC-05/06 Bluetooth Programmer [Электронный ресурс] URL: https://petegsx-projects.github.io/bluetooth-programmer/index.html (дата обращения: 12.11.2023).
4. Habr.com Как устроен AES [Электронный ресурс] URL: https://habr.com/ru/articles/112733/ (дата обращения: 12.11.2023).
5. Habr.com Симметричный алгоритм блочного шифрования Advanced Encryption Standart [Электронный ресурс] URL: https://habr.com/ru/articles/534620/ (дата обращения: 12.11.2023).

Lyubashchenko T.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Application of lora technology to create protected uav beacons.

UAV designers and manufacturers are constantly working to improve reliability and reduce the likelihood of loss. The control systems transmit GPS coordinates, but they may be inaccurate. A redundant autonomous communication system is needed to more reliably locate a downed vehicle. In this paper, the features and requirements for such a system are discussed. A prototype is developed and the results of its tests are summarized.

Key words: UAV, search module, radio channel protection, encryption.

УДК 004.056
ГРНТИ 81.93.29

ОБЗОР ВОЗМОЖНОСТЕЙ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ VOIP

А. К. Макарова, А. В. Поляничева
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена теме решения проблемы безопасности VoIP-соединения с помощью машинного обучения. Актуальность данной темы обосновывается быстрым темпом развития отрасли искусственного интеллекта, его применение может, как принести пользу безопасности данных, так и столкнуть мир информационной безопасности с новыми, не виданными ранее угрозами. Для этого произведен обзор статей по заданной тематике, проанализированы работы других авторов и выделены способы реализации защиты VoIP связи. Затронут вопрос о потенциале развития данной области в рамках защиты VoIP. В результате получена сравнительная таблица с результатами исследования, проведен анализ полученных данных и дан вывод о возможным методах защиты VoIP связи.

VoIP, машинное обучение, безопасность, классификация методов

Введение

В контексте развивающейся отрасли искусственного интеллекта, его применение может, как принести пользу безопасности данных, так и столкнуть мир информационной безопасности с новыми, не виданными ранее угрозами. В связи с этим, необходимо понять есть ли потенциал развития данной области в сторону защиты VoIP, проанализировав работы других авторов по заданной тематике и выделить из статей способы реализации защиты VoIP связи. Данная статья направленна на выявление наиболее удачных методов защиты путем их сравнительного анализа по ряду выделенных критериев.

Для обзора было решено проанализировать статьи русского сегмента и зарубежные. Это было связано с малым количеством русскоязычных работ, тем не менее это поможет сравнить и поняв общий уровень развития данного направления в России, выделить общие наиболее удачные методы защиты.

C_1. Прогноз стратегии вторжения нарушителя.

Статья [1] посвящена разработке метода обеспечения безопасности VoIP-сети, повышающего безопасность, путем уменьшения времени, затрачиваемого на анализ действий нарушителя. Авторами, решается проблема недостаточной эффективности методов защиты VoIP-сетей. На основе составленной структуры системы управления ИБ, интегрируемой в сеть, разработан эффективный метод в борьбе с нарушителем. Он способствует минимизации времени, затрачиваемого на анализ действий нарушителя, и работает в условиях проведения атаки на VoIP-систему. Метод заключается в анализе цифрового потока, определении параметров протоколов и профилей атак нарушителя. Благодаря данному методу, авторы

получили графы реализации угрозы и разные состояния нарушителя, на основе которых было произведено математическое моделирование атак "Человек посередине" и "Спам". В дальнейшем, авторами планируется автоматизирование данного метода с применением нейронных сетей, что позволит системе самостоятельно принимать решения по локализации угрозы.

C_2. Распознавание мошенников по ключевым словам.

Статья [2] посвящена решению проблемы обнаружения мошеннических VoIP-звонков с помощью алгоритмов машинного обучения. Чтобы повысить точность метода определения мошеннического вызова, были подробно проанализированы характеристики текста мошеннических разговоров и выделены критерии, по которым эффективно вычисляются подобного рода звонки. Машинное обучение применяется для анализа данных и извлечения информации из предварительно собранного материала с целью создания наборов данных. Звуковой сигнал, входные данные, преобразуется в текстовую форму и подвергается предварительной обработке перед вводом в модель машинного обучения. Для итоговой классификации диалогов используется метод kNN (англ. k-Nearest Neighbor), который объединяет выводы двух модулей, осуществляющих выявление подозрительных словосочетаний в разговоре. Точность данного метода составила порядка 92%.

C_3. Методика управления безопасностью в условиях НСД.

Статья [3] посвящена решению проблемы постоянно развивающихся атак на VoIP-сетях и разработке усовершенствованных методов обнаружения аномалий с помощью машинного обучения за счет уменьшения времени анализа системы. Предлагается авторские структуры методики управления информационной безопасностью VoIP-сети, на ее основе анализируются динамика действий нарушителя в условиях НСД. Также, выделены другие методы выявления уязвимостей с возможностью обучения моделей угроз, пополняя базы данных (например, выявление с использованием выделенного сервера). Автором предложено решение для обнаружения и классификации сетевых атак на основе системы контроля. Предложено использование интеллектуальных систем, включая Нейронные Компьютерные Кластеры (НКК), для принятия решений в области предотвращения вторжений. Был проведен сравнительный анализ методов обнаружения и идентификации атак. Выделены характеристики и показатель точности распознавания аномалий: полнота, вероятность и временные затраты на обучение модели вторжений. Данные, полученные автором в ходе исследования, могут быть использованы для разработки новых систем раннего обнаружения и прогнозирования вторжений.

C_4. Обнаружение спама.

Статья [4] посвящена разработке нового метода для обнаружения спам звонков в VoIP сетях. Авторы рассмотрели ряд методов и предложили новый подход для быстрого, эффективного и высокоточного обнаружения вызовов

SPIT с использованием нейронных сетей и новых параметров вызовов. Вызовы SPIT и модели поведения обычных пользователей были проанализированы путем обработки данных с помощью методов интеллектуального анализа данных и статистических процедур. Выделены 7 параметров описывающие, как начинались отношения между пользователями и как продолжалось их общение согласно обработанным данным (Множественные вызовы (первый входящий успешный) (MFIS), NumberRatio, RelationsIndex, Множественные вызовы (сбой первого исходящего вызова) (MFOF), Множественные вызовы (первый исходящий успешный) (MFOS), Исходящие одиночные успешные вызовы (OSSC), Множественные вызовы (сбой первого входящего вызова) (MFIF) и т.д.). Наиболее эффиктивными алгоритмами МО, в сравнени со многими, в поиске SPIT оказались SVM или Random Forest, на их создание ушло наибольшее время, чем на другие алгоритмы МО.

C_5. Обнаружения аномалий в потоке SIP-сообщений

Статья [5] посвящена разработке онлайн-фильтра, который исследует поток входящих SIP-сообщений, происходит классификация сообщений в два этапа и разделение их на хорошие и плохие. Описывается общая архитектура двухэтапного фильтра, а затем исследуются несколько точек конфигурационного пространства SVM, чтобы определить хороший параметр конфигурации, который будет работать и подходить для классификации большой выборки SIP-сообщений, полученных из собранного реального трафика. Подход «обучения на примере», который используется во втором этапе, основан на использовании классифицированных на первом этапе сообщений. Классификатор работает на основе машинного обучения с применением метода опорных векторов (SVM), для выполнения необходим анализ каждого поступающего SIP-сообщения. Также, представлена эффективность классификации дополнительных сообщений, собранных из того же источника.

Сравнительный анализ

Для проведения сравнительного анализа рассмотренных методов обеспечения безопасности VoIP, выделены следующие критерии (включая их возможные значения):

1. Год публикации статьи;
2. Проблема, которая решается с помощью МО – область;
3. Используемый метод машинного обучения, с помощью которого решается проблема;
4. Реализовано ли в статье машинное обучение на практике;
5. Проверена ли работоспособность данного метода;
6. Применимость данного метода в реальных VoIP сетях (условиях): применимо; под вопросом; невозможно;

ТАБЛИЦА 1. Критериальное сравнение

	C_1	C_2	C_3	C_4	C_5
K_1	2022	2022	2022	2022	2012
K_2	НСД	Вишинг	НСД	Спам	Аномалии SIP
K_3	-	kNN	kNN	SVM, Random Forest	SVM
K_4	нет	да	да	да	да
K_5	нет	нет	нет	да	да
K_6	под вопросом	под вопросом	применимо	применимо	применимо

Результаты

В результате критериального сравнения (см. таблицу 1) получаем следующие выводы. Во-первых, развитие данного направления в России, довольно критично отстает от зарубежных стран. В данном сравнении найдено и рассмотрено всего 3 русскоязычных статьи, на тему защиты VoIP. Во-вторых, по K_1, ни одна из статей русскоязычного сегмента не была написана ранее 2022 года, тогда как иностранные журналы выпускали статьи уже с 2012. Все это говорит об уровне развития данного направления и о необходимости научного развития данной области. В-третьих, критерий K_2 показал, что большинство русскоязычных статей посвящено решению проблемы НСД. В-четвертых, значения по K_3, говорят о том, что наиболее часто используемыми методами являются SVM и kNN; это означает что данные методы являются наиболее часто реализуемыми для задач, связанных с классифицированием событий происходящих в VoIP-сетях.

Вывод

В рамках текущего исследования был проведен обзор существующих русскоязычных и зарубежных статей на заданную тематику. Критериальное сравнение решений позволило условно выделить наиболее популярные из методов реализации защит – kNN и SVM. Также, полученная сравнительная таблица дает представление об общем уровне развития данного направления – он ниже, чем в других странах.

Продолжением исследования должно стать критериальное сравнение зарубежного сегмента и увеличение количества исследуемых методов. Также выбор наименее защищенной области и реализация в нем наиболее подходящего метода.

Список используемых источников

1. Липатников В. А., Шевченко А. А., Косолапов В. С., Сокол Д. С. Метод обеспечения информационной безопасности сети VoIP-телефонии с прогнозом стратегии вторжений нарушителя. Информационно-управляющие системы, 2022, № 1, с. 54–67. doi:10.31799/1684-8853-2022-1-54-67

2. Борьба с телефонным мошенничеством на основе распознавания голоса с применением машинного обучения / К. Гончаров, Е. Плешакова, А. Шелягин, С.

Гатауллин // Информационные ресурсы России. – 2022. – № 4(188). – С. 96-104. – DOI 10.52815/0204-3653_2022_04188_96. – EDN WUQPFD.

3. Косолапов, В. С. Методика обеспечения информационной безопасности сети VOIP-телефонии в условиях несанкционированного доступа / В. С. Косолапов // Известия Тульского государственного университета. Технические науки. – 2022. – № 2. – С. 426-434. – DOI 10.24412/2071-6168-2022-2-426-435. – EDN RUXEVX.

4. Л. Бехан, Дж. Рожон, Дж. Шафарик, Ф. Резак и М. Вознак, «Эффективное обнаружение спама в интернет-телефонии с помощью алгоритмов машинного обучения», в *IEEE Access* , vol. 10, стр. 133412-133426, 2022 г., doi: 10.1109/ACCESS.2022.3231384.

5. Р. Фердос, Р.Л. Синьо и А. Зорат, «Об использовании SVM для обнаружения аномалий в потоке SIP-сообщений», *11-я Международная конференция по машинному обучению и приложениям, 2012 г.,* Бока-Ратон, Флорида, США, 2012 г., стр. 592. -597, номер документа: 10.1109/ICMLA.2012.109.

Makarova A., Polyanicheva A.

[1]*The Bonch-Bruevich Saint-Petersburg State University of Telecommunication*

Overview of machine learning capabilities for VoIP security.

This paper is devoted to the topic of solving the problem of VoIP connection security using machine learning. The relevance of this topic is justified by the rapid pace of development of the industry of artificial intelligence, its application can both benefit the security of data, and to confront the world of information security with new, not seen before threats. For this purpose, we have reviewed articles on the given subject, analyzed the works of other authors and highlighted the ways of implementation of VoIP communication protection. The question about the potential of development of this area within the framework of VoIP protection is touched upon. As a result, a comparative table with the results of the research is obtained, the obtained data is analyzed and a conclusion about possible methods of VoIP communication protection is given.

Key words: VoIP, machine learning, security, method classification.

УДК 004.624
ГРНТИ 20.53.23

СРАВНЕНИЕ БРОКЕРОВ СООБЩЕНИЙ

Д. А. Марочкин, А. С. Павленко
Санкт-Петербургский государственный университет промышленных технологий и дизайна

Данная статья посвящена анализу доступных решений в сфере брокеров сообщений, будут рассмотрены основные преимущества и недостатки таких систем как, Apache Kafka, RabbitMQ, AMS SNS и Redis. Оценочными критериями будут: пропускная способность, наличие хранилища данных, расширяемость, сложность структурирования и сложность развертывания, что позволит определить наиболее подходящий тип брокер-системы для разрабатываемого проекта.

сообщения, брокер, данные, хранилище, исполнитель, поручитель, очередь

С развитием программирования и построения приложений разработчики стали сталкиваться с проблемой общения между их частями, вследствие чего был придуман такой архитектурный паттерн как “Брокер сообщений”. Его цель - организовать бесперебойную связь между сервисами. При передаче данных напрямую, могут произойти ошибки, при которых данные не будут получены, что нарушит работу системы. Также, выключенный сервис не может принимать данные и обрабатывать их, эту и другие проблемы решают брокеры сообщений.

Как говорилось ранее, основная задача брокера - организовывать связь между компонентам. Для этого брокер может принимать и отправлять сообщения разным сервисам, а также предоставлять список пропущенных сообщений, если сервис-получатель в момент отправки сообщения был выключен.

Принцип работы брокеров сообщений

Общая схема работы брокера сообщений представлен на рис. 1.

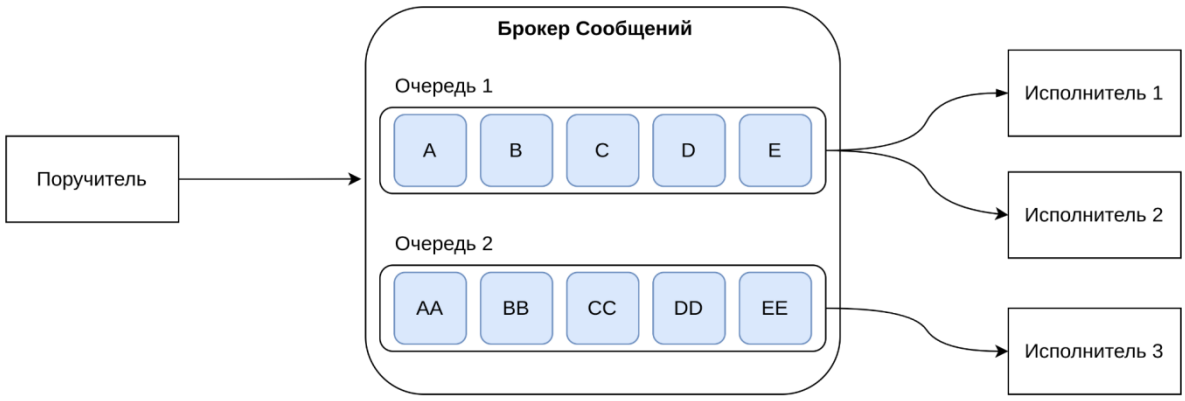


Рис. 1. Общая схема работы брокера сообщений

В работе принимают участие 3 основных объекта: Поручитель, Брокер и Исполнитель. Поручитель создает задачи и отправляет их брокеру сообщений для хранения и оповещения исполнителей. Брокер при получении

нового сообщения добавляет его в очередь для выполнения, с которой работают исполнители. Исполнитель, в свою очередь, подписываясь на обновления в очереди, получает новые сообщения и обрабатывает их.

Далее будут рассмотрены некоторые из существующих на рынке решений, такие как RabbitMQ, Apache Kafka и Amazon Simple Queue Service. В некоторых случаях в качестве брокера сообщений используется Redis, он также будет рассмотрен как один из доступных вариантов.

RabbitMQ

Принцип работы RabbitMQ показан на рис. 2.

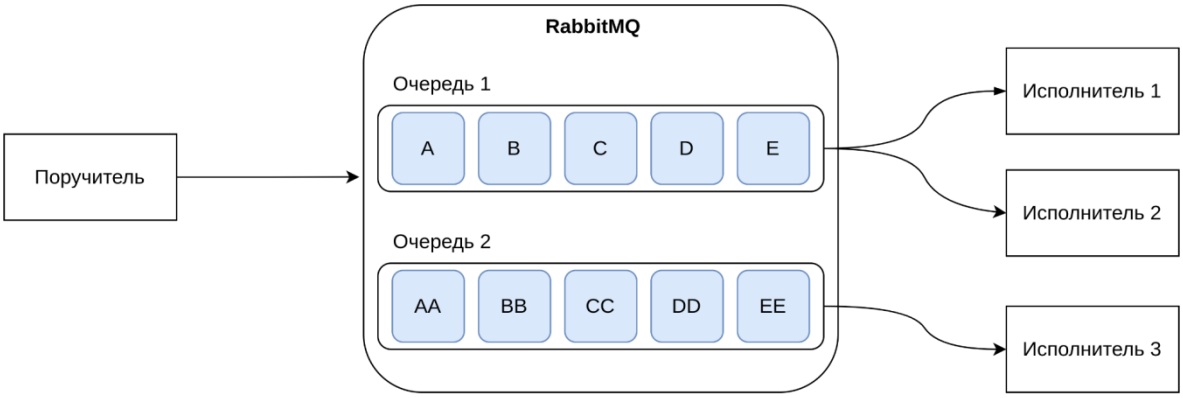


Рис. 2. Схема работы RabbitMQ

RabbitMQ — это брокер сообщений с открытым исходным кодом, разработанный компанией Ericsson в середине 1980-х. Он основан на отказоустойчивой архитектуре Earlang/Beam и протоколе AMQP (Advanced Message Queuing Protocol). Это открытый протокол передачи сообщений, который нужен для общения разных частей системы между собой.

Преимуществами RabbitMQ являются: простота разработки, удобное администрирование в режиме реального времени и открытый исходный код, адаптированный под множество современных языков программирования.

Главным недостатком классической модели RabbitMQ является отсутствие гибкости при горизонтальном масштабировании в рамках поля одного кластера: необходимо вносить дополнительный уровень кластеризации, который в большинстве случаев приводит к значительному падению производительности.

RabbitMQ подойдет для проектов, в которых нужен безотказный порядок получения сообщений с наличием нестандартный и сложных путей или запутанной очередности доставки данных.

Apache Kafka

Принцип работы Apache Kafka показан на рис. 3.

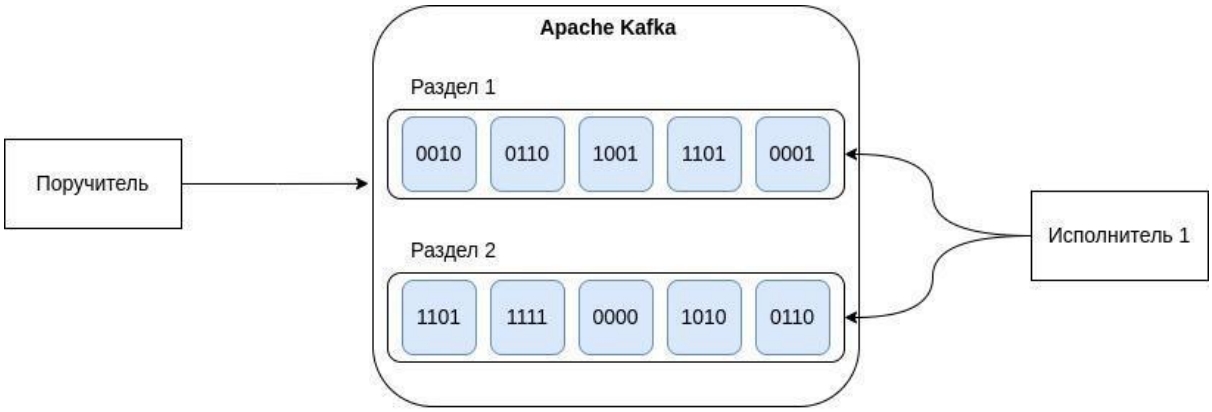


Рис. 3. схема работы Apache Kafka

Kafka — брокер сообщений с открытым исходным кодом, разрабатываемый компанией Apache на языках Java и Scala, первый выпуск которого состоялся в 2010-ом году. Kafka поддерживается всеми основными языками программирования и является более низкоуровневым брокером сообщений, имеющим меньшее количество сущностей и ролей, но за счет большого количества мало затратных операций чтения и записи, данные выдаются, когда приходит соответствующий запрос. В Kafka, качестве хранилища используется физический диск: файл бинарная карта topic и файл с сообщениями - commit log, в конец которого попадает каждое последнее сообщение: соответственно, место бита сообщения в бинарной карте совпадает со строкой сообщения в файле. Само сообщение с точки зрения Kafka представляется просто набором байт.

Несмотря на простоту концепции, сложность реализации брокера сообщений Kafka во многом зависит от масштаба архитектуры проекта. В его концепции нет выдачи (push-механизма), из-за чего сам получатель-consumer обращением pull получает информацию из брокера.

За счет такой системы обработки данных Kafka имеет большой запас по пропускной способности — миллионы сообщений в секунду с возможностью увеличения производительности, что позволяет перечитывать сообщения, так как информация записывается и не удаляется, тем самым позволяя сразу получать уже загруженные сообщения большими группами, не нагружая сеть в конкретные временные периоды.

Минусом концепции беспрерывного очередного чтения сообщений является проблема «мертвых» писем - dead letter, если письмо не получается обработать, оно будет бесконечно «крутиться» в очереди, пока не будет прочитано. Зачастую это обходят созданием специальных хранилищ для битых писем, либо битые письма удаляются навсегда. Также для корректной работы нужно постоянное хранение точки последнего сообщения, прочитанного исполнителем, причем для каждого исполнителя, что значительно усложняет систему при наличии большого количества исполнителей.

Данный брокер сообщений подходит для конвейерной обработки и обработки огромных массивов данных, из-за чего Kafka и стал стандартным решением в крупных корпорациях.

Amazon Simple Queue Service (SQS + SNS)

Принцип работы Amazon Simple Queue Service показан на рис. 4.

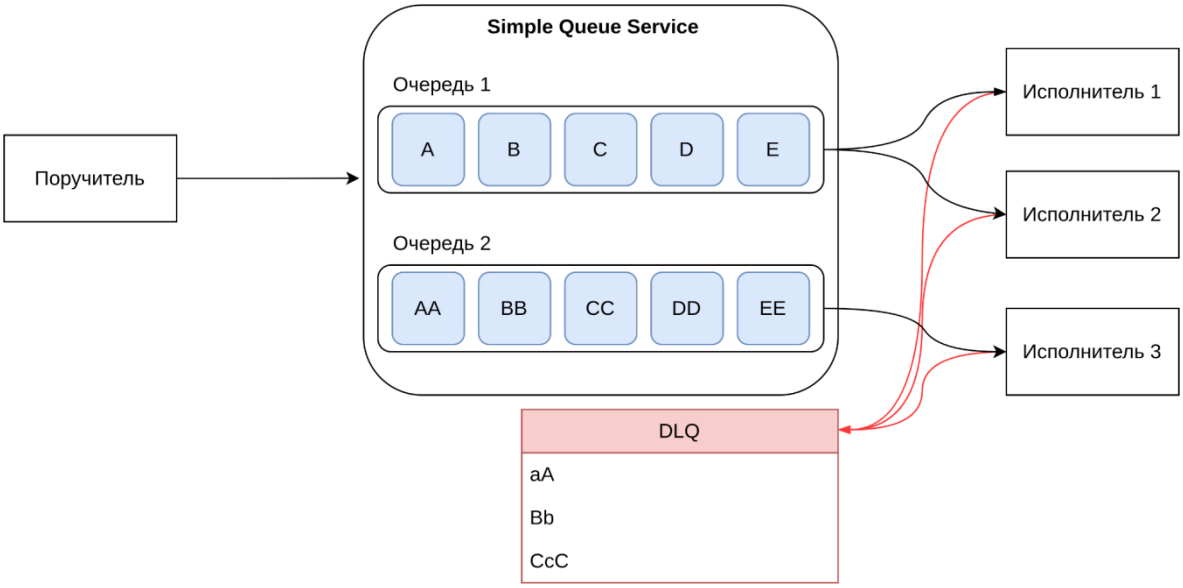


Рис. 4.Схема работы Amazon Simple Queue Service

SQS — брокер сообщений, разработанный Amazon в 2004-ом году. Как и другие брокеры, он позволяет изолировать, организовывать связь и масштабировать микросервисы и бессерверные приложения. SDK брокера поддерживает несколько языков: Java, Ruby, Python, .NET, PHP и Javascript.

Для своей работы SQS использует SNS - сервис для обмена сообщениями между приложениями и для общения клиента с сервером. Для обмена используется модель «pub-sub» (издатель-подписчик) где поручитель публикует сообщение, а подписчики их обрабатывают. SNS используется в масштабных системах для параллельной обработки данных, рассылке уведомлений и других задачах. При передаче сообщений не гарантируется сохранение их очередности и отсутствие дубликатов, однако пропускная способность SNS практически ничем не ограничена.

Когда сообщения не могут быть обработаны получателями они отправляются в DLQ - очередь необработанных сообщений. Эти сообщения больше не будут обрабатываться и будут храниться в очереди для дальнейшей диагностики.

Основным плюсом SQS является ее популярность за рубежом. Это обусловлено безопасностью, автоматическим бэкапами, простотой отправки уведомлений и встроенным хранилищем необработанных сообщений. Также причиной популярности является интеграция с другими сервисами Amazon.

Однако полная зависимость от Amazon также является и минусом продукта, так как в случае неполадок или проблем перейти на другого поставщика будет непростой задачей.

SQS является отличным решением, если вы уже работаете с другими сервисами Amazon и вам нужна простота в использовании и безопасность.

Redis

Изначально разработанный, как система быстрого хранения данных с открытым исходным кодом, Redis, может быть преобразован в брокер сообщений. Проект возник в 2009-ом году, когда Сальваторе Санфилиппо, изначальный разработчик Redis, захотел улучшить масштабируемость стартапа в Италии.

Redis позволяет значительно снизить скорость отклика, вплоть до миллисекунд и позволяет приложениям, работающим в режиме реального времени, выполнять миллионы простых запросов. Redis занял свою нишу в сегменте потребительских клиентских приложений по типу: игр, финансовых сервисов, чатов, служб доставки и такси и небольших проектов с отправкой сообщений по модели Publisher - Subscriber.

Redis не используется физическое хранилище данных и предоставляет собственную память, что обеспечивает минимальную задержку и максимальную пропускную способность. Redis оснащен большим количеством встроенных структур данных: строки, списки, множества, хеш-таблицы, JSON, потоки, и команд, что значительно упрощает работу разработчикам, которым не придется заниматься проблемами совместимости разных структур данных.

Преимуществами Redis являются простота интеграции и реализации, высокая гибкость и настройка всех компонентов под различные нужды проекта, идеально подойдет для обращения с сообщениями с коротким жизненным циклом, но не обеспечивает отказоустойчивость и хранение данных, поэтому обычно выступает промежуточной точкой между сервером и клиентом, а сообщение в последствие записывается в отдельную базу данных.

Сравнение решений.

Сравнивая решения, мы должны обратить внимание на ряд характеристик. Пропускная способность и отказоустойчивость обеспечивают высокую доступность решения для пользователей. Масштабируемость позволяет расширить платформу в будущем. Хранение данных полезно для всех пользователей, а открытый исходный код обеспечивает возможность для доработки и поддержки системы. Связь one-to-one и one-to-many обеспечивает гибкость и полное использование системы. Для рассмотренных решений была построена сравнительная таблица таблице 1.

ТАБЛИЦА 1.Сравнение рассмотренных решений

Решение Критерий	RabbitMQ	Apache Kafka	Amazon SQS	Redis
Пропускная способность	средняя	очень высокая	регулируемая	очень высокая
Отказоустойчивость	средняя	очень высокая	высокая	низкая
Масштабируемость	низкая	высокая	высокая	очень высокая
Хранение данных	выборочно	постоянное хранение	временное хранение	не предусмотрено
Открытый исходный код	открытый исходный код	открытый исходный код	проприетарное ПО	открытый исходный код
Связь one-to-one	поддерживается	не поддерживается	поддерживается	поддерживается
Связь one-to-many	поддерживается	поддерживается	достигается	поддерживается

Заключение.

Брокеры сообщений являются ценным инструментом в арсенале разработчика, который помогает наладить взаимодействие между отдельными элементами приложения.

Исходя из изложенного материала, можно сделать вывод, что желаемый результат достигается за счет правильного подхода к выбору брокера сообщений, а выбор конкретного брокера зависит от поставленных задач.

Например, Kafka подойдет для крупных предприятий, для которых наиболее важными критериями является высокая пропускная способность и безотказная работа, а Redis для небольших проектов и клиентских приложений, требующих высокую скорость обмена сообщениями и не нуждающихся в долгосрочном хранении.

Список используемых источников:

1. Redis: Redis is an open source (BSD licensed), in-memory data structure store, used as a database, cache, and message broker. Redis provides data structures … [Электронный ресурс]. URL: https://redis.io/ (дата обращения: 2.02.23)

2. Apache Kafka: Apache Kafka: A Distributed Streaming Platform. [Электронный ресурс].URL: https://kafka.apache.org/ (дата обращения: 2.02.23)

3. RabbitMQ: RabbitMQ is the most widely deployed open source message broker [Электронный ресурс]. URL: https://www.rabbitmq.com/ (дата обращения: 2.02.23)

4. Amazon SQS. [Электронный ресурс]. URL: https://aws.amazon.com/sqs/ (дата обращения: 2.02.23)

5. Habr: Брокеры сообщений, или Как происходит взаимодействие в рамках распределённой инфраструктуры [Электронный ресурс]. URL: https://habr.com/ru/company/sberbank/blog/669456/ (дата обращения: 2.02.23)

6. Google Books: Web Services Business Strategies and Architectures [Электронный ресурс]. URL: https://books.google.ru/books?id=2EonCgAAQBAJ&pg=PA71&redir_esc=y#v=onepage&q&f=false с. 71–84 (дата обращения: 2.02.23)

Marochkin D., Pavlenko A.

Saint Petersburg State University of Industrial Technologies and Design

Message broker comparison.

This article is devoted to the analysis of available solutions in the field of message brokers, the main advantages and disadvantages of such systems as Apache Kafka, RabbitMQ, AMS SNS and Redis will be considered. Evaluation criteria will be: bandwidth, availability of data storage, extensibility, complexity of structuring and complexity of deployment, which will determine the most appropriate type of broker system for the project being developed.

Key words: messages, broker, data, storage, executor, guarantor, queue.

УДК 004.056.2
ГРНТИ 50.41.01

УЯЗВИМОСТИ, ВОЗНИКАЮЩИЕ ПРИ ПЕРЕНОСЕ КОДА С 32-БИТНОЙ НА 64-БИТНУЮ ПЛАТФОРМУ И ИХ УСТРАНЕНИЕ

Д. Р. Мартыненко, А. А. Шиян
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире все чаще используется 64-разрядное программное обеспечение, созданное для процессоров соответствующей разрядности. Но до сих существуют приложения, которые имеют только 32-битную версию. Но при переносе программ с 32-битной платформы на 64-битную, ранее безопасный код имеет большие риски обзавестись уязвимостями.

процессор, память, программное обеспечение, Си, кибербезопасность

Первый 32-битный процессор «Intel 80386» был выпущен компанией «Intel» 17 октября 1985 года. Уже через 13 лет, в 1998 году компания «Sun» выпускает свой 64-битный процессор под названием «SPARC».

Данное изменение в структуре процессора вызвало большой скачок технических мощностей ЭВМ, благодаря увеличению количества адресов памяти процессора.

В то время как 32-битные процессоры для адресации памяти используют только 2^{32} бит, 64-битные процессоры используют 2^{64} бит. Такое многократное увеличение количества адресов памяти, которые может использовать процессор, значительно повышает размеры оперативной памяти, которую может использовать программное обеспечение. Предел оперативной памяти для 32-битного процессора составляет 4 гигабайта, в то время как 64-битный процессор может оперировать 16 эксабайтами.

Главное преимущество 64-битных процессоров – количество регистров в памяти, позволяет программному обеспечению быстрее работать с большими объемами данных, которые можно полностью хранить в оперативной памяти, избегая подкачки данных с жесткого диска, что может заметно замедлить программу. Но большое количество программного обеспечения не требуют таких объемов памяти, из-за этого до сих пор существуют 32-битные программы. Также важно отметить, что несмотря на это, современные операционные системы (такие как «Windows 11», «MacOs») уже не имеют 32-битных версий, из данного факта следует тенденция на постепенный уход от 32 бит. Для разработчиков ПО это означает, что многие программы должны иметь 64-битную версию как основную, для более быстрой коммуникации с современными операционными системами.

Почему же нельзя так быстро и легко оптимизировать код программы под процессоры с тактовой частотой в 64 бит. Самая главная причина – возникающие при этом уязвимости. Существуют примеры подобных

уязвимостей в программном обеспечении, такие как «CVE-2013-0211» [1] или «CVE-2021-27219» [2].

Для демонстрации подобных уязвимостей была подготовлена программа, написанная на языке С и скомпилированная в двух версиях – 64-битной и 32-битной, с которой вы можете ознакомиться по ссылке «https://github.com/glassh0use/32to64.git».

Данная программа, принимает на вход один аргумент – количество выводимых цифр после запятой числа пи, вывод ограничен 20 цифрами после запятой. 32-битная версия этой программы не имеет уязвимостей, размеры записываемых и вводимых данных ограничены, что не позволит злоумышленнику выполнить переполнение кучи или буфера. Вывод программы – рис. 1.

```
┌──(kali㉿kali)-[/media/sf_VMshared]
└─$ ./vuln2_32 10
3,1415926535

┌──(kali㉿kali)-[/media/sf_VMshared]
└─$ ./vuln2_32 20
Sorry, we didn't calculated this amount of digits of pi =)

┌──(kali㉿kali)-[/media/sf_VMshared]
└─$ ./vuln2_32 -1
Sorry, we didn't calculated this amount of digits of pi =)
```

Рис. 1. Вывод 32-битной версии программы

Как можно заметить, при вводе отрицательного числа, программа работает корректно и не выводит результат

Но если программа будет скомпилирована в 64 битах, то сравнение переменной «*Len*» (количества выводимых цифр, вводимых пользователем) и «*Size*» (размером буфера, который хранит выводимые значения), станет уязвимым местом программы. Все из-за измененного размера типа данных «*long*» в 64-битной версии [3] (таблица 1).

ТАБЛИЦА 1. Сравнение размеров типов данных в разных системах

Тип данных	*char*	short	int	long	long long	float	double	Long double	pointer
32-бит (*ILP32*)	1	2	4	4	8	4	8	16	4
64-бит (*LP64*)	1	2	4	8	8	4	8	16	8

Проблема вытекает из особенности языка С, который при одинаковом размере типов данных неявно приводит их к одному типу [4]. Получается, что в 32-битной версии значение «-1», при приведении к типу «*unsigned*» отбрасывает свой знак и становится максимальным положительным числом, что явно больше размеров буфера. В 64-битной версии, все как раз наоборот.

Тип «*long*» теперь имеет вес в 8 байт и не преобразовывается при сравнении, поэтому он легко проходит сравнение с размером буфера и приводит к его переполнению в момент выделения памяти функцией «*memcpy*». Вывод программы – рис. 2.

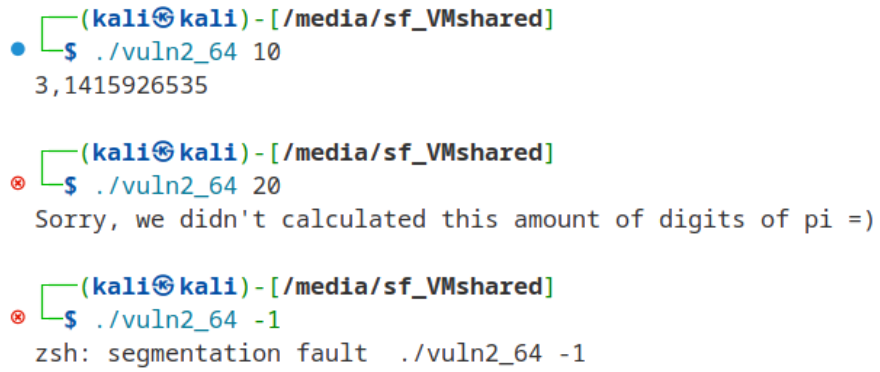


Рис. 2. Вывод 64-битной версии программы с уязвимостью

Из вышесказанного можно сделать вывод, что уязвимости при переходе к 64-битной версии ПО возникают из-за преобразования типов данных как явного, так и неявного. Где неявные преобразования являются самыми опасными, так как они происходят не по воле программиста.

Для исправления данной уязвимости достаточно привести переменную “*long*” к типу “*unsinged integer*” или любому другому типу, вес которого равен 4 байтам. Вывод исправленной программы – рис. 3.

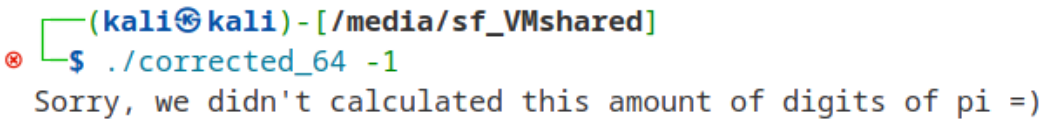


Рис. 3. Вывод 64-битной версии программы с устраненной уязвимостью

В настоящее время мы наблюдаем стремительный переход от 32-битных к 64-битным процессорам. На наш взгляд, изучение вышеописанной проблемы было бы полезно в рамках лабораторного практикума для студентов ИТ-направлений, это позволит повысить их навыки в создании безопасных приложений. Также умение находить такие закономерности поможет создавать более безопасный код и смотреть глубже в структуру языка программирования, ведь приведенный пример обращает внимание на особенности главных уязвимостей языка Си.

Список используемых источников:

1. The MITRE Corporation // CVE-2013-0211: [Электронный ресурс]. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0211 (дата обращения: 20.10.2023)

2. The MITRE Corporation // CVE-2021-27219: [Электронный ресурс]. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27219 (дата обращения: 20.10.2023)

3. IBM // ILP32 and LP64 data models and data type sizes: [Электронный ресурс]. URL: https://www.ibm.com/docs/en/zos/2.3.0?topic=environments-ilp32-lp64-data-models-data-type-sizes (дата обращения 23.10.2023)

4. Керниган Брайан, Ритчи Деннис. Язык программирования С. М. : Вильямс, 2019. 288 с.

Martynenko D., Shiyan A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Vulnerabilities that arise when porting code from a 32-bit to a 64-bit platform and their mitigation.

In the modern world, 64-bit software is increasingly being used, designed for processors of corresponding architecture. However, there are still applications that only have a 32-bit version. When migrating programs from a 32-bit system to a 64-bit one, previously secure code carries greater risks of vulnerabilities.

Key words: C, processor, computer memory, cybersecurity, software

УДК 004.056.57
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

М. И. Муравьев
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В современном мире возникает всё больше распределённых информационных систем, но ещё больше становится атак на эти системы. В связи с этим необходимо использовать системы обнаружения вторжений и оптимизировать их работу с помощью искусственного интеллекта и анализа Больших данных

искусственный интеллект, анализ больших данных, распределённые информационные системы, системы обнаружения вторжений

Сейчас, когда человечество неуклонно развивает информационные технологии, простой компьютер есть почти у каждого жителя почти каждой страны. Но помимо простых граждан существуют и иные структуры, пользующиеся благами умных машин. Государства, крупные компании и даже простые офисы объединяют множество компьютеров в единую сеть, образуя информационные системы, парой, огромных масштабов. Но с ростом системы растёт и риск атаки на неё.

Для защиты информационных систем были созданы системы обнаружения вторжений. Они играют важную роль в обеспечении дополнительного уровня защиты компьютерных систем, помогая обнаруживать различные виды вредоносной активности, которая может угрожать безопасности.

Существует несколько способов классификации СОВ в зависимости от типа и расположения сенсоров, а также используемых методов анализа. В некоторых простых системах все компоненты могут быть реализованы в виде одного модуля или устройства. Однако, с развитием технологий и требований безопасности, СОВ становятся более сложными и гибкими, что позволяет эффективнее защищать информационные системы от вторжений.

В работе [1] пояснено, почему в контексте обеспечения безопасности распределенных информационных систем становится все более важным автоматизировать процесс обнаружения потенциально возможных атак и принятия соответствующих мер. Независимо от того, способен ли сетевой администратор определить возможную угрозу, эффективное управление при огромном и одновременном количестве атак в режиме реального времени зачастую оказывается непосильной задачей. В связи с этим возникает необходимость разработки правил безопасности, по аналогии с правилами брандмауэра. Однако, создание этих правил может уменьшить

эффективность системы в целом, так как нужно ограничить доступ для вредоносных узлов и злоумышленников, при этом обеспечивая остальным пользователям безопасный доступ, чтобы выявить злоумышленников среди потока обычных пользователей можно задействовать различные решения, включая применение машинного обучения и анализа Больших данных. Именно такие подходы, базирующиеся на использовании методов машинного обучения, показывают значительный потенциал в решении данной задачи и предоставляют возможность эффективного обнаружения и предотвращения потенциально возможных атак в распределённых информационных сетях.

Чтобы обнаружить вторжений можно использовать глубокие нейронные сети. В работе [2] авторы представляют использование GRU-RNN (Gated Recurrent Unit Recurrent Neural Network). Данный подход был протестирован на наборе данных NSL-KDD и продемонстрировал достаточно высокую точность обнаружения - 89%. Авторы работы пришли к выводу, что GRU-RNN действует весьма эффективно и не способствует снижению производительности сети.

Также, для решения данной задачи можно воспользоваться многослойным персептроном. Например, авторы работы [3] использовали модель, базирующуюся на нейронной сети, обученной на наборе данных NSL-KDD. Нейронная сеть состоит из 6 входных нейронов, соответствующих 6 выбранным признакам потока данных (время соединения (количество секунд); тип протокола; количество байтов, переданных от получателя к источнику; количество байтов, переданных от источника к получателю; количество подключений к хосту, используемому текущим соединением (в течении последних 2 секунд); количество подключений к сервису, используемому текущим соединением (в течении последних 2 секунд)), и трех скрытых слоев (12, 6 и 3 нейрона). На выходе сети находятся 2 нейрона. Этот метод показал хороший потенциал и достиг точности около 76%, что можно сравнить с известными алгоритмами машинного обучения. Таким образом, нейронные сети могут использоваться для обнаружения аномального поведения трафика.

В работе [4] описана модель обнаружения DDoS-атак и система защиты, базирующаяся на глубоком машинном обучении в программно-конфигурируемой сети. Для оценки эффективности были представлены к сравнению такие нейронные сети как: 3LSTM, CNN/LSTM, GRU и LSTM, на наборе данных ISCX. Из результатов экспериментов выяснилось, что модель 3LSTM показала наилучший результат с точностью обнаружения атак в 99%.

Эти результаты позволяют сделать вывод, что схема обнаружения DDoS-атак, базирующаяся на глубоком машинном обучении, обладает слабой зависимостью от аппаратных и программных устройств и обладает высокой точностью обнаружения. Кроме того, она обеспечивает простое обновление сетевой модели, что является важным преимуществом по сравнению с существующими схемами обнаружения DDoS-атак.

В работе [5] представлена модель обработки больших данных, которая включает использование дополнительных сервисов и систем для расширения множества механизмов защиты (рис. 1) при выявлении новых угроз безопасности. Данная модель также определяет взаимосвязь между оценкой защищенности и выбором защитных мер, а также предлагает построение идентификатора риска для беспрепятственной работы с системой больших данных. Полученные на каждом этапе выходные данные используются в качестве входных данных для следующего этапа.

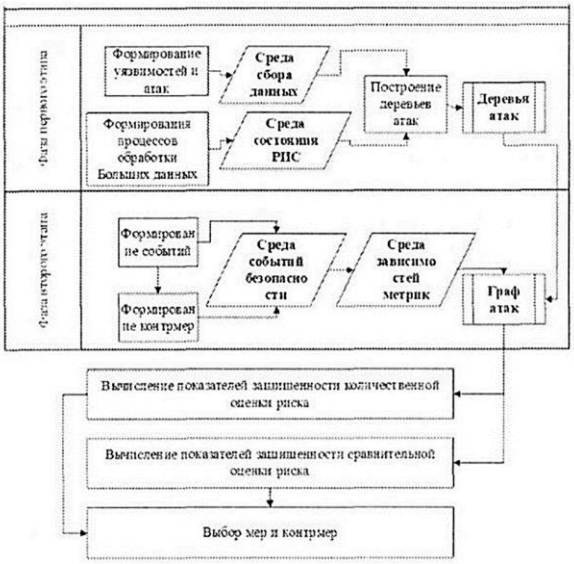


Рис. 23. Связь между оценкой завершённости и выбором защитных мер в модели обработки Больших данных

При обработке данных операции сбора, очистки, нормализации, агрегации и сокращения размерности Больших данных распределены между различными локальными агрегатами и подсистемами идентификации. Функционирующие в данной схеме (рис. 2) программные агенты осуществляют переработку, включая очистку и нормализацию данных в соответствии с методикой обнаружения вторжений.

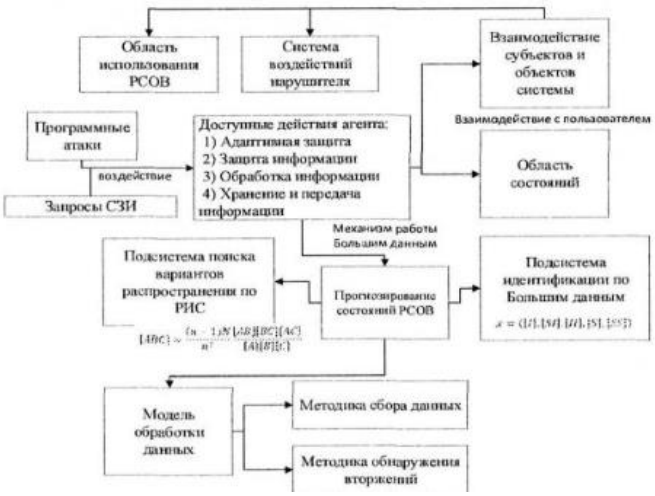


Рис. 24. Структурная схема распределённой системы обнаружения вторжений

При использовании структурной схемы происходит сокращение времени процессов выполнения распределённой системы обнаружения вторжений и достигается требуемое значение вероятности устойчивости функционирования распределённых информационных систем.
Таким образом, в работе рассмотрены научно-технические методы применения систем искусственного интеллекта и анализа Больших данных для обнаружения вторжений в распределённых информационных системах.

Список используемых источников:

1. Волков С. С., Курочкин И. И. Применение методов машинного обучения в SDN в задачах обнаружения вторжений [Электронный ресурс] // International Journal of Open Information Technologies. 2019. N 11. T. 7. URL: https://cyberleninka.ru/article/n/primenenie-metodov-mashinnogo-obucheniya-v-sdn-v-zadachah-obnaruzheniya-vtorzheniy/viewer (дата обращения: 12.10.2023).
2. Tang T. A. et al. Deep recurrent neural network for intrusion detection in sdn-based networks // 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft). IEEE, 2018. С. 202-206.
3. Tang T. A. et al. Deep learning approach for network intrusion detection in software defined networking // 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM). IEEE, 2016. С. 258-263.
4. Li C. et al. Detection and defense of DDoS attack-based on deep learning in OpenFlow-based SDN // International Journal of Communication Systems. 2018. Т. 31. N 5. С. 3497.
5. Штеренберг С. И. Обнаружение вторжений в распределенных информационных системах на основе методов скрытого мониторинга и анализа больших данных : автореферат дис. ... кандидата технических наук : 05.13.19/ Штеренберг Станислав Игоревич. СПб., 2018. 16 с.

Muraviev M.

Saint Petersburg State University of Industrial Technologies and Design

Research of artificial intelligence systems for intrusion detection in distributed information systems.

In the modern world, there are more and more distributed information systems, but there is even more demand for these systems. In this regard, it is necessary to use intrusion detection systems and optimize their work with the help of artificial intelligence and Big Data analysis

Key words: artificial intelligence, big data analysis, distributed information systems, intrusion detection systems.

УДК 004.056.5
ГРНТИ 81.93.21

ПРИЕМУЩЕСТВА СИСТЕМЫ УПРАВЛЕНИЯ ИДЕНТИФИКАЦИЕЙ НА ОСНОВЕ БЛОКЧЕЙНА

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

Решения по управлению идентификацией разрабатываются для облегчения управления цифровыми удостоверениями. В последние годы предпринимались попытки внедрить решения для управления идентификацией на основе блокчейна, которые позволяют пользователю взять на себя контроль над своей собственной личностью. В этой статье будет обзор существующих решений по управлению идентификацией на основе блокчейна. На основе анализа будет определены потенциальные пробелы и возможности в исследованиях.

блокчейн, система управления идентификацией, суверенная личность

1. Введение

Цифровая идентичность играет большую роль в современном мире. Например, у большинства пользователей сети есть ряд цифровых личностей, связанных с работой, личной жизнью и другими аспектами. Это способствует растущей зависимости от управления идентификационной информацией и ее обработкой. Опираясь на популярность блокчейна, предпринимались попытки интегрировать блокчейн в разработку новых решений по управлению идентификацией [1].

В типичной системе управления идентификацией на основе блокчейна имеется большое количество распределенных узлов [2]. Такие узлы можно использовать для обеспечения распределенного хранения, надежного доступа и вычислительных возможностей. Пользователь в такой системе выступает в роли узла в сети; таким образом, позволяя перенести хранение конфиденциальных пользовательских данных с серверов на пользовательские устройства/узлы. Это облегчает самостоятельную идентификацию (SSI).

В этой статье делается упор на изучении систем управления идентификацией на основе блокчейна. Будут представлены соответствующие концепции управления идентификацией и модели, три существующие системы управления идентификацией на основе блокчейна. В конце будут представлены выводы и потенциальные исследовательские проблемы.

2. Модель управления идентификацией

Управление идентификацией (IdM) относится к системе политик и технологий, гарантирующих, что только авторизованные лица могут получить доступ к соответствующим ресурсам в организации [3]. IdM является относительно старой темой, учитывая большое количество

стандартов и инфраструктур [4], однако по мере того, как наше общество становится все более взаимосвязанным и цифровым, со значительным увеличением количества и типов систем и идентичностей, которыми необходимо управлять, также возникает необходимость пересмотреть традиционные парадигмы IdM. Например, как обсуждалось ранее, были попытки использовать характеристики блокчейна (например, децентрализацию, открытость, надежность и безопасность)

Для простоты рассмотрим сценарий, в котором пользователь запрашивает подтверждение личности у поставщика удостоверений, а поставщик удостоверений отвечает на токен (рис. 1). В этой упрощенной ситуации происходит обмен информацией между обоими объектами (например, реальным человеком или несколькими объектами). Если поставщики удостоверений являются отдельными объектами, то это становится трехсторонней моделью управления идентификацией, включающей пользователей, поставщиков удостоверений и зависимых лиц. В такой модели, поскольку поставщик удостоверений является отдельным объектом, ресурс удостоверений, используемый для аутентификации, хранится только в поставщике удостоверений, а зависимый от удостоверений может проверить аутентификацию личности пользователя только путем запроса поставщика удостоверений. Помимо предоставления удостоверений пользователей, поставщики удостоверений также должны иметь функции управления удостоверениями, сброса удостоверений, отзыва удостоверений и другие соответствующие функции.

Рис 1. Система управления идентификацией

Существует ряд трудностей [5], лежащих в основе системы управления идентификацией (IdM), здесь мы рассмотрим только две:

•**Доступ и ресурсы.** Система должна предопределить несколько уровней доступа, для различных ролей или различных ресурсов. Например, в системе управления идентификацией в учебном учреждении могут

существовать идентификации, такие как преподаватели (постоянные и временные), административный персонал (не являющийся преподавателями) и студенты. В такой системе каждый человек имеет определенные роли и доступы.

•**Доверие.** Существуют два ключевых доверенных элемента: пользователь доверяет поставщику идентификации, и поставщик услуг доверяет поставщику идентификации. Мошеннический поставщик идентификации может потенциально получить доступ к услуге, используя идентификацию пользователя без его согласия и ведома. Поэтому разработчику следует учитывать возможность такого сценария в проектировании системы. Поставщик услуг также должен обеспечить, чтобы поставщик идентификации уведомлял их о добавлении нового поставщика в доверенный домен. Это позволит поставщику услуг получать соответствующие атрибуты пользователя от поставщика идентификации для определения, может ли пользователь воспользоваться его услугой. При добавлении нового поддомена поставщика идентификации истинным решателем доступа становится поставщик идентификации, а не поставщик услуг, что ставит под угрозу доверительное отношение.

3. Системы управления идентификацией на основе блокчейна

Системы управления идентификацией на основе блокчейна решают существенные проблемы традиционных решений. Вот несколько примеров существующих систем:

•**Sovrin.** Разработан на базе Hyperledger для использования цифровых удостоверений личности. Sovrin обладает самостоятельной идентичностью, не зависящей от централизованных органов, и не поддается уничтожению.

•**uPort (Serto + Veramo).** uPort представляет собой систему самостоятельной идентичности. Она зависит от Ethereum, поэтому суть идентичности — это адрес учетной записи Ethereum, с которым взаимодействуют пользователи.

•**ShoCard.** ShoCard — это мобильная система управления идентификацией на основе блокчейна, позволяющая пользователям сохранять и защищать свои цифровые личности.

4.Возможные исследовательские проблемы

Несмотря на то, что блокчейн может решить проблемы традиционных систем, все равно остается ряд проблем:

•**Проблемы, связанные с идентичностью**

○ **Утечка.** Если "кошелек" идентичности успешно взломан, то могут быть получены полезные сведения о пользователе. Такая информация может быть использована для незаконных действий.

○ **Изменение идентичности.** Идентичность пользователя не является постоянной и может быть изменена. Традиционные централизованные поставщики идентичности могут отозвать или обновить статус идентичности своевременно, например, во время смены паспорта. Однако в системе управления идентичностью на основе блокчейна, из-за

постоянства блокчейна и SSI, любое изменение информации об идентичности пользователя требует участия пользователя. Изменение идентичности может быть сложно реализуемой задачей.

- **Экономические проблемы**
  - **Инфраструктура.** SSI – новая технология и может быть не поддерживаема существующими системами управления идентичностью и их инфраструктурой. Экономические последствия, связанные с модернизацией инфраструктуры, обучением персонала, обслуживания оборудования может замедлить развертывание системы на основе блокчейна.
  - **Управление ключами.** В отличие от системы на основе пароля, в системе на основе блокчейна нет механизма сброса забытого пароля. Таким образом, одним из жизнеспособных подходов является внедрение такой функции или аутсорсинг управления ключами третьей стороне. Однако управление частным ключом противоречит концепции SSI, поэтому поддержка SSI требует значительных затрат.

5. Заключение

В данной статье представлен обзор систем управления идентичностью на основе блокчейна. В рамках обзора было выявлено ряд проблем, например с хранением блочных данных. Еще одной проблемой является классификация деавторизации. Некоторые узлы могут участвовать в ведении учета, в то время как другие могут только просматривать блочные данные. Это может потенциально привести к делению цепочки на части из-за существования уникальных идентификаторов узлов.

Системы управления идентификацией на основе блокчейна решают ряд ограничений традиционных систем. Пользователь становится владельцем своей идентичности, и это не требует от него жертв безопасности в угоду удобству.

Список используемых источников:

1. Куперберг М., Управление идентификацией на основе блокчейна: исследование с точки зрения предприятия и экосистемы [Электронный ресурс] // IEEE Transactions on Engineering Management (2019), URL: https://ieeexplore.ieee.org/document/8792372 стр. 1008 – 1027 (дата обращения: 24.10.2023).

2. Чжу С., Бадр Ю. Обзор систем управления идентификацией на основе блокчейна для Интернета вещей [Электронный ресурс] // Международная конференция IEEE по Интернету вещей (IoT) и IEEE Green Computing and Communications (GreenCom) и IEEE Cyber, Physical, 2018 г. социальные вычисления (CPSCom) и интеллектуальные данные IEEE (SmartData), IEEE, 2018, URL: https://pure.psu.edu/en/publications/a-survey-on-blockchain-based-identity-management-systems-for-the- С. 1568–1573. (дата обращения: 25.10.2023).

3. Страуд Ф, Что такое управление идентификацией и доступом (IAM)? определение в вебпедии [Электронный ресурс]. URL: https://www.webopedia.com/TERM/I/iam-identity-and-access-management.html (дата обращения: 25.11.2022).

4. Лим С. Ю., Фотсинг П. Т., Алмасри А., Муса О., Киах М. Л. М., Анг Т. Ф.,. Исмаил Р., Технология блокчейна — разрушитель услуг управления идентификацией и аутентификации. [Электронный ресурс] // Международный журнал по передовой науке, инженерии и информационным технологиям. N 8 (4-2). 2018.

URL: https://researchportal.hw.ac.uk/en/publications/blockchain-technology-the-identity-management-and-authentication- стр. 1735–1745. (дата обращения: 25.11.2022).

5. Шеффнер М. «Анализ и оценка самостоятельных систем идентификации на основе блокчейна» [Электронный ресурс] URL: https://wwwmatthes.in.tum.de/file/1oua980d9tgxx/Sebis-Public-Website/-/Master-s-Thesis-Martin-Schaeffner/Masters%20Thesis%20Martin%20Scha%CC%88ffner.pdf С. 133 (дата обращения: 26.11.2022).

6. Роуден М., Идентичность: преобразование производительности посредством интегрированного управления идентификацией (2017). [Электронный ресурс] URL: https://www.taylorfrancis.com/books/mono/10.4324/9781351156165/identity-mark-rowden стр. 250 (дата обращения: 27.11.2022).

Nechaev A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Advantages of a blockchain-based identity management system.

Identity management solutions are being developed to make digital identities easier to manage. In recent years, there have been attempts to implement blockchain-based identity management solutions that allow the user to take control of their own identity. This article will provide an overview of existing blockchain-based identity management solutions. Based on the analysis, potential research gaps and opportunities will be identified.

Key words: Identity management system, blockchain, self-sovereign

УДК 004.056.2
ГРНТИ 20.53.19

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ ПРИ ИСПОЛЬЗОВАНИИ БЛОКЧЕЙН УЗЛОВ НА ПРИМЕРЕ СИСТЕМЫ ГОЛОСОВАНИЯ

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

Рассматривается подход к реализации обеспечения безопасности систем при использовании блокчейн. Предложены оригинальные методы и инструменты реализации блокчейн узла, объединения блокчейн узлов для обеспечения безопасности систем. Представлен пример обеспечения безопасности на системе голосования. Подход может быть использован в практических решениях и несет в себе перспективы развития использования блокчейн технологии в системах для обеспечения безопасности.

blockchain, распределенный реестр, blockchain сеть, защита информации, ключ, подпись

Главной идеей технологии blockchain [1] является то, что обрабатываемая ей информация связана, каждый последующий блок данных сочленен с предыдущим [1, 2, 3] (рис. 1).

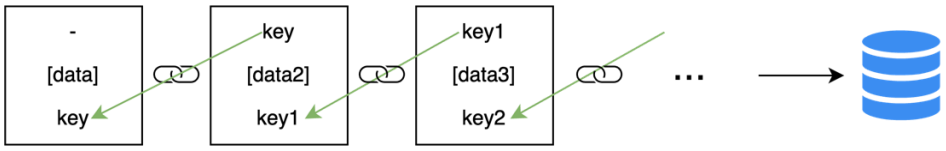


Рис. 1. Представление связей блоков данных в технологии blockchain

Под blockchain узлом понимается отдельный экземпляр [4] blockchain сети [5], который содержит в себе все необходимые механизмы хранения, обработки и передачи данных.

Однако, отдельное использование blockchain узла не безопасно, так как мощности современных компьютеров позволяют без труда пересчитать все последовательные блоки. Чтобы предотвратить пересчет всех последовательных блоков, используется децентрализация в виде blockchain сети. Blockchain сеть является P2P сетью [6, 8], что означает отсутствие серверов, которые обрабатывают и отдают данные, и клиентов, которые используют эти серверы. В подобной сети имеются узлы, каждый из которых является ее полноправным членом, узел – и клиент, и сервер. Узлы сети связаны друг с другом напрямую.

Blockchain узлы P2P сети могут играть разные роли [8]. Используя несколько blockchain узлов, мы получим простую blockchain сеть:

– Центральный узел. К данному узлу будут подключаться все остальные узлы для синхронизации.

– Узел кошелька / пользователя. Смысл данного узла состоит в создании новых транзакций и хранении экземпляра blockchain.

– Узел майнера. Данный узел будет хранить новые транзакции в пуле транзакций. При достижении определенного количества транзакций в пуле узел будет создавать новый блок.

Сценарий работы простой blockchain сети (рис. 2):

1. Центральный узел создает blockchain экземпляр.
2. Узел пользователя подключается к центральному узлу и загружает весь экземпляр к себе.
3. Узел майнера подключается к центральному узлу и загружает весь экземпляр к себе.
4. Узел пользователя создает транзакцию.
5. Узел майнера получает транзакцию от узла майнера и сохраняет ее в своем пуле памяти.
6. Когда в пуле памяти достаточно транзакций, узел майнера начинает создавать новый блок.
7. После создания нового блока он отправляется на центральный узел.
8. Узел пользователя синхронизируется с центральным узлом.
9. Пользователь узла кошелька проверяет, что его платеж прошел успешно.

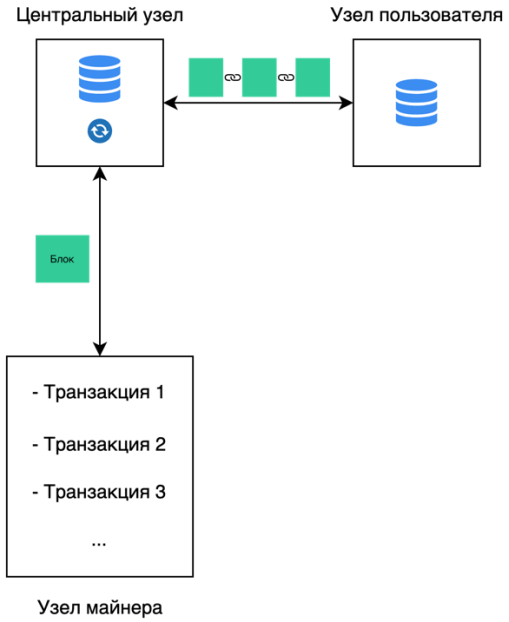


Рис. 2. Пример работы blockchain сети

Жесткое связывание адресов является ошибкой с точки зрения безопасности. Вместо связывания адресов используются DNS-сервера, которые знают адреса некоторых центральных узлов.

Использование подобной blockchain сети возможно во множестве проектов, где важна прозрачность обработки данных и децентрализация.

Система электронного голосования. Например, между тремя университетами A, B и C необходимо провести электронное голосование, в котором могут участвовать только студенты. Вариант данной системы с использованием blockchain сети выглядит следующим образом (рис. 3 - рис. 4):

- Каждый из университетов имеет центральный узел.
- Каждый университет имеет DNS-сервер для хранения информации о всех центральных узлах.
- Каждый университет имеет узел с ролью “Miner”.
- Каждый пользователь выступает в роли “SPV” и подключается к любому центральному узлу посредством DNS-сервера.

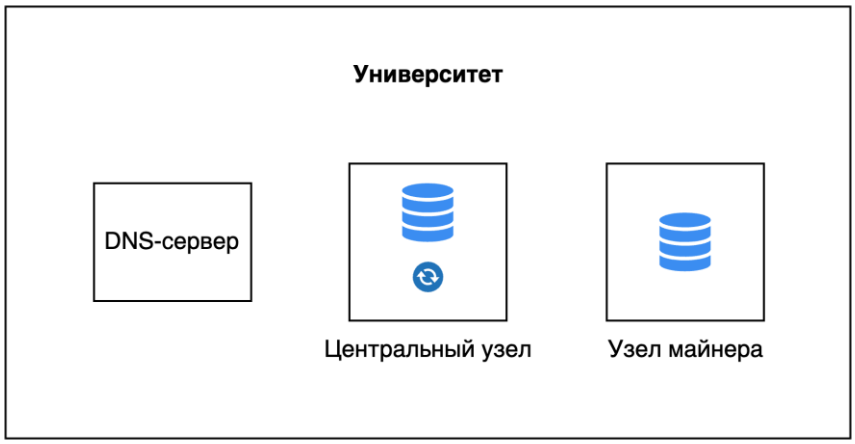


Рис. 3. Пример университета

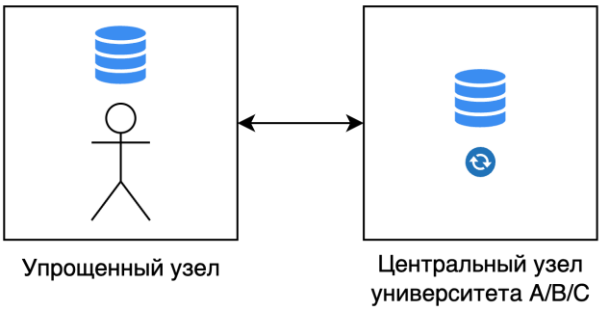


Рис. 4. Подключение студентов

Каждая монета в сети является голосом и у каждого студента она одна. Отправка монеты студентом на определенный кошелек является голосованием. Вопрос изначального распределения монет между студентами остается открытым.

Прозрачность обработки достигается благодаря использованию blockchain технологии. Децентрализация достигается путем использования нескольких независимых узлов несколькими университетами.

Чем больше независимых узлов используется, тем выше безопасность системы. Минимальное число независимых предприятий, необходимое для функционирования системы, равняется трем, так как если хотя бы один узел

будет скомпрометирован, он будет подавлен правотой оставшихся двух - большинством (рис. 5).

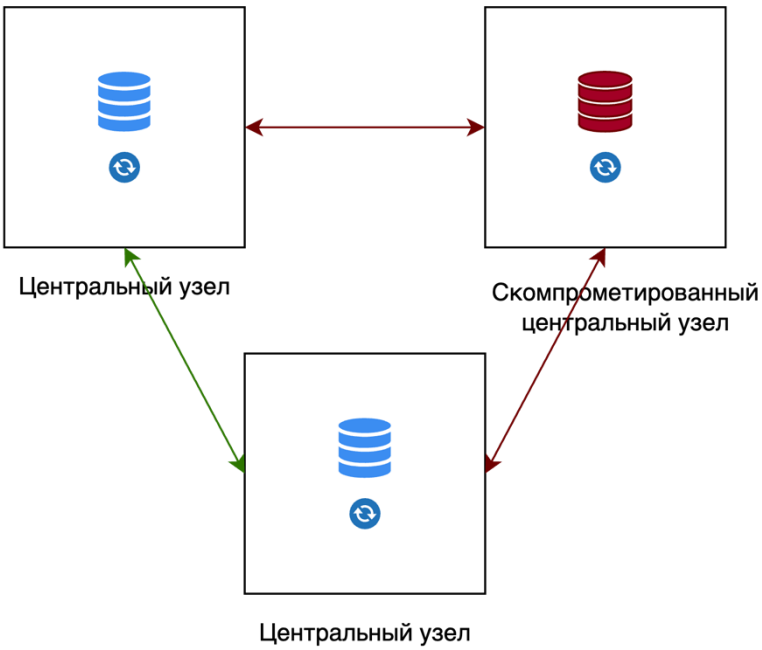


Рис. 5. Компрометация одного из центральных узлов

В рамках данной статьи был исследован подход к реализации обеспечения безопасности систем при использовании blockchain узлов на примере системы голосования.

Перспективой данной работы является тестирование предложенного подхода в реальных условиях как на системе голосования, так и на системах, которым важна прозрачность обработки данных и децентрализация. Также важно брать в расчет, что в приведенном примере системы голосования не закрыты все вопросы, которые необходимо отдельно исследовать.

Список используемых источников:

1. Bitcoin address generation in pure python: [Elektronnyj resurs] // STRM. URL: https://strm.sh/posts/bitcoin-address-generation-in-pure-python. (date of the application: 27.05.2022).

2. Haber S., Stornetta W. S. How to time-stamp a digital document. J. Cryptology 3, 99–111 (1991).

3. Moshe Babaioff, Shahar Dobzinski, Sigal Oren, Aviv Zohar: On Bitcoin and Red Balloons [Electronic resource] // Microsoft. URL: http://research.microsoft.com/pubs/156072/bitcoin.pdf (date of the application: 27.05.2022).

4. Никонов Е. Р. Особенности проектирования основных компонентов блокчейн системы // Молодежная научная школа кафедры "Защищенные системы связи". 2022. N 4. С. 122-126.

5. Кушнир Д. В. Особенности проектирования 2p2 сети blockchain / Д. В. Кушнир, Е. Р. Никонов // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы XII Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 28 фев. – 01 марта 2023 г. Т. 1. СПб. г: СПбГУТ, 2023. С. 750-754. – EDN WNETJQ.

6. Jeffrey A. Tucker. Bit by Bit: How P2P Is Freeing the World // The global community Liberty.me. 2015.
7. Diego Geroni. Blockchain Nodes: An In-Depth Guide [Electronic resource] // 101blockchains. URL: https://101blockchains.com/blockchain-nodes (date of the application: 20.02.2023).

Nikonov E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Ensuring the security of systems when using blockchain nodes on the example of a voting system.

An approach to implementing systems security with blockchain nodes is considered. Original methods and tools for implementing a blockchain node and combining them into a network to ensure system security are proposed. Security is illustrated by the example of a voting system. The approach can be used in practical solutions and carries prospects for the development of the use of blockchain technology to ensure the security of systems.

Key words: blockchain, distributed ledger, blockchain network, information security, key, signature.

УДК 004.056
ГРНТИ 81.93.29

ПОДХОДЫ К ТЕСТИРОВАНИЮ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ

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

В современном мире информационные технологии, включая веб-приложения, играют ключевую роль в повседневной жизни людей. Онлайн-запись к врачу и заказ продуктов на дом – лишь небольшая часть многочисленных сервисов, доступных онлайн. Однако, с увеличением числа веб-приложений также растет угроза кибератак и уязвимостей. В связи с этим, исследование подходов к тестированию безопасности веб-приложений становится жизненно важным для обеспечения защиты данных и конфиденциальности пользователей в современном информационном мире.

безопасность, веб-приложение, SAST, DAST, IAST, тестирование безопасности

Потенциальные угрозы, а также непрерывное расширение объема исходного кода веб-приложений влечет за собой растущее количество уязвимостей и повышение рисков эксплуатации их со стороны злоумышленников. В связи с этим современные разработчики используют различные инструменты для тестирования безопасности приложений (AST). Применение AST (Application Security Testing) представляет собой метод усиления уровня безопасности приложений путем обнаружения потенциальных уязвимостей в исходном программном коде.

Существуют три основных подхода к тестированию безопасности веб-приложений. К ним относятся: SAST, DAST и IAST.

Ниже будут рассмотрены подходы к тестированию приложений:

1) SAST (Static Application Security Testing)

SAST – статическое тестирование безопасности приложения. Данный подход представляет собой анализ кода на наличие ошибок и уязвимостей. SAST позволяет разработчикам находить уязвимости безопасности в исходном коде на ранних этапах жизненного цикла разработки программного обеспечения. Также данный подход обеспечивает соответствие руководствам и стандартам кодирования без фактического выполнения базового кода. Использование статического тестирования помогает контролировать качество разработки, снижает риски.

Преимущества SAST:

- Применение подхода на этапе разработки продукта;
- Высокая вероятность обнаружения критических уязвимостей (SQLi, XSS, SSRF);
- Точное определение уязвимого участка кода, что является важным для больших проектов, где количество строк года доходит до миллионов.

Из недостатков данного подхода стоит отметить огромное количество ложных срабатываний, что негативно отражается на разработке и тестировании приложений, когда сроки ограничены.

SAST-анализаторы: Checkmarx, PVS-Studio, Micro Focus, Synopsys, Veracode.

2) DAST (Dynamic Application Security Testing)

DAST – динамическое тестирование безопасности приложений. Данный подход представляет собой имитирование атак на веб-приложение с помощью известных уязвимостей. С помощью данного подхода обнаруживаются уязвимости и слабые места в работающем приложении. Это достигается за счет использования методов внедрения ошибок в приложении, таких как передача вредоносных данных в ПО для выявления распространенных уязвимостей, например SQL-инъекций, межсайтового скриптинга. DAST также помогает найти проблемы аутентификации и конфигурации сервера, недостатки, видимые только при входе известного пользователя. С помощью SAST подобные уязвимости обнаружить нельзя.

Преимущества DAST:

- Возможность тестирования во время выполнения кода, что открывает дополнительные векторы для поиска уязвимостей;
- Поиск ошибок, которые могут возникнуть при взаимодействии пользователя с приложением;
- DAST не привязан к языкам программирования.

DAST-инструменты: WhiteHat Security, IBM, Accenture, Pradeo Security Solution.

Стоит отметить, что до недавнего времени SAST-инструменты использовались чаще DAST. Однако, в связи повсеместным распространением смартфонов, в которых появляется все больше приложений, взаимодействующих с конфиденциальными данными пользователей, доля DAST-решений увеличилась и продолжает расти с каждым годом.

Для большей безопасности рекомендуется использовать оба подхода, так как оба метода нейтрализуют слабые стороны друг друга.

3) IAST (Interactive Application Security Testing)

IAST – интерактивное тестирование безопасности приложений. Является относительно новым методом, относительно DAST и SAST. Данный подход позволяет проводить тестирование приложения изнутри во время его работы.

Таким образом:

- SAST работает с кодом приложения без его запуска;
- DAST работает во время работы приложения, без доступа к коду;
- IAST работает с кодом приложения прямо во время работы.

IAST отслеживает выполнение кода и ищет конкретные события, которые могут привести к уязвимости. IAST работает внутри приложения и проводит анализ:

- Кода приложения;

- Конфигурации;
- Поток данных;
- HTTP-запросов и ответов;
- Библиотек и фреймворков;
- Информации о внутреннем соединении.

Таким образом, IAST работает с большим объемом кода и предоставляет более точные данные касательно безопасности приложения. Интерактивное тестирование безопасности приложений позволяет проверять более широкий набор правил безопасности, выявлять большее количество уязвимостей, избегая ложных срабатываний.

Тестирование безопасности веб-приложений является важным аспектом концепции обеспечения информационной безопасности современных информационных технологий. В связи с повышением частоты и серьезности кибератак, применение AST для проверки кода, поиска уязвимостей и контроля безопасности входных данных, становится необходимым процессом для повышения безопасности приложений.

Следует отметить, что не существует одного единственного решения для обеспечения полной безопасности приложения. Рекомендуется использовать комплексный подход, включающий в себя применение SAST на ранних этапах разработки. Совместное применение SAST и DAST методов, а также попытки внедрения IAST-метода, который является сложным, однако достаточно эффективным за счет универсальности. Тестирование безопасности веб-приложений следует проводить по отношению к любому разрабатываемому коду, так как нельзя точно знать, является ли он безопасным.

Список используемых источников:

1. Кинтонова А. Ж., Баенова Г. М., Урынбасарова А. Ж. Вопрос безопасности веб приложений // Компьютерные и информационные науки. 2020. N 13. С. 12-13.

2. Гонжур М. А., Дьяченко Н. В., Отакулов А. С. Анализ методологий DevOps и DevSecOps // Компьютерные и информационные науки. 2021. N 5. С. 8-10.

3. Фатхи В. А., Дьяченко Н. В. Тестирование безопасности приложений // Компьютерные и информационные науки. 2021. N 5.

Novikov D.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Approaches to Web Application Security Testing.

In the modern world, information technologies, including web applications, play a pivotal role in people's daily lives. Online doctor appointments and home product deliveries are just a small fraction of the numerous services available online. However, with the increasing number of web applications, the threat of cyberattacks and vulnerabilities also grows. Consequently, researching approaches to web application security testing becomes critically important for safeguarding data and user privacy in the contemporary information age.

Key words: security, web application, SAST, DAST, IAST, security testing.

УДК 004.056
ГРНТИ 81.93.29

МЕТОДИКИ ОБФУСКАЦИЙ И ДЕОБФУСКАЦИЙ JAVA КОДА

Е. Б. Овсянников
Санкт-Петербургский государственный университет промышленных технологий и дизайна

Данная статья посвящена анализу методик обфускации и деобфускаци Java кода. В ходе исследования будет сформирован краткий обзор на данные методики. Для того что бы в будущем правильно выбрать методику при конкретных поставленных задачах.

обфускация, деобфускация

Обфускация - это процесс изменения программного кода или данных с целью сделать его трудночитаемым или непонятным для людей, при этом сохраняя его функциональность и работоспособность для компьютерных систем. Этот процесс обычно применяется разработчиками программного обеспечения для защиты кода от несанкционированного доступа, взломов или обратного проектирования.

Основные методы обфускации Java [1].

1. Упаковка локальных переменных в битовые поля (PLVB)
2. Замена инструкций if(non)null блоками Try-Catch (RIITCB).
3. Операторы частичного перехвата переключателей (PTSS)
4. Добавление операторов переключения мертвого кода (ADSS).
5. Преобразование ветвей в инструкции jsr (CB2JI).

Обфускация, Java

Методика обфускации, известная как "Упаковка локальных переменных в битовые поля" (PLVB), предназначена для усложнения чтения и понимания программного кода на языке Java. Она основана на использовании битовых полей для хранения значений локальных переменных.

Процесс обфускации с использованием методики PLVB включает следующие шаги:

1. Идентификация локальных переменных, которые требуется обфусцировать. Это могут быть переменные, хранящие чувствительные данные или важные значения.

2. Создание структуры данных, которая будет использоваться для хранения значений этих переменных в виде битовых полей. Обычно это делается с использованием классов-оберток или специально созданных классов.

3. Изменение кода программы таким образом, чтобы операции с локальными переменными выполнялись через созданную структуру данных. Это может включать изменение объявлений переменных, замену операций над переменными на вызовы методов структуры данных и т. д.

4. Добавление дополнительных операций для увеличения сложности анализа кода. Это могут быть случайные операции с

переменными, дополнительные проверки или условия, фиктивные операции и т. д.

5. Компиляция обфусцированного кода в исполняемый файл.

В результате применения методики PLVB, читаемость и понимание кода усложняются.

Обфускация, данные, PLVB

Методика обфускации Замена инструкций if(non)null блоками Try-Catch (RIITCB). [2]

Конструкция try-catch в языке Java может использоваться для создания потока управления либо с помощью явного оператора throw, либо путем вставки оператора, который, как известно, создает исключение. Эта обфускация использует хорошо известный факт Java: вызов метода экземпляра для объекта null всегда приводит к исключению NullPointerException.

Обфускация, код

Методика обфускации операторов частичного перехвата переключателей (PTSS) в Java коде предназначена для усложнения анализа и понимания программы за счет изменения структуры переключающего оператора (switch statement).

Методика PTSS предлагает следующие шаги для обфускации данного оператора:

1. Изменение порядка значений: значения переключающей переменной, указанные после ключевого слова case, переставляются случайным образом. Это усложняет понимание логики оператора.
2. Вставка пустых блоков и кода: в случайном порядке вставляются пустые блоки ({}) и/или блоки кода, необходимые для других значений или поддержки дополнительной функциональности. Это создает дополнительный шум и затрудняет анализ кода.
3. Добавление дополнительных значений: в переключатель могут быть добавлены дополнительные значения, которые не используются в коде. Это приводит к еще большей конфузии и усложнению понимания программы.

Обфускация, оператор, PTSS

Методика обфускации с использованием операторов переключения мертвого кода (ADSS). Использование конструкции switch в байт-коде Java представляет собой эффективный метод для запутывания потока управления. Эта конструкция предоставляет органическую возможность создать граф потока управления, имеющий узел с более чем двумя последователями, за исключением структуры try-catch. Это приводит к серьезному усложнению структуры метода.

Это запутывание увеличивает связность и общую сложность метода.

Обфускация, код, ADSS

Методика обфускации преобразования ветвей в инструкции JSR (CB2JI) в Java коде заключается в изменении логики выполнения программы путем

замены условных операторов и операторов перехода на инструкции JSR (Jump to SubRoutine).

Байт-код jsr (Java-подпрограмма) представляет собой механизм, аналогичный операции go to, за исключением того, что он сохраняет обратный адрес в стеке. Обычно обратный адрес сохраняется в регистре после выполнения jsr, и для возврата к месту вызова используется байт-код ret.

Однако, конструкция jsr - ret имеет некоторые сложности, особенно при решении проблем, связанных с вводом текста.

Для обфускации этой сложности, вместо целей if и goto, внутри кода заменяются на инструкции jsr. К каждой исходной цели перехода добавляется соответствующая инструкция pop, которая удаляет обратный адрес, помещенный в стек. Если предшествующий участок кода перед целью в последовательности не выполняется, вставляется инструкция goto, направленная непосредственно к исходной цели, обходя тем самым неиспользуемую конструкцию jsr.

Таким образом, преобразование ветвей в инструкции JSR (CB2JI) изменяет структуру программы и усложняет ее анализ и чтение.

Обфускация, jsr

Деобфускация - процесс преобразования кода или данных, которые были обфусцированы или зашифрованы с целью запутывания или скрытия. Вовремя деобфускации используются различные методы и алгоритмы, чтобы восстановить исходный вид кода или данных, делая их более читаемыми и понятными для разработчиков или исследователей. Деобфускация может использоваться для анализа вредоносного кода, повышения безопасности программы или для других целей.

Основные методики деобфуккации [3].

1. Сопоставление шаблонов.
2. Автоматический статический анализ.
3. Автоматический динамический анализ.
4. Ручной анализ.

Деобфускация, методики

Сопоставление шаблонов. Это наиболее простой и быстрый метод анализа, который заключается в синтаксическом разборе бинарного кода программы для выявления статических последовательностей инструкций, с применением регулярных выражений и интеллектуальных классификаторов на базе машинного обучения.

В отличие от статического и динамического анализа, сопоставление шаблонов ограничивается исключительно синтаксическим анализом кода и не проводит анализ семантики программы. Варианты шаблонов могут включать в себя как простые бинарные последовательности, так и регулярные выражения, а также скриптовые языки с возможностью использования метасимволов.

Сопоставление шаблонов, метод

Автоматический статический анализ. это метод анализа, который сосредотачивается на понимании семантики бинарного кода, не требуя фактического выполнения программы. Одними из наиболее распространенных инструментов, реализующих автоматический статический анализ, являются дизассемблеры.

Инструменты автоматического статического анализа могут применяться для различных целей, таких как:

- обзор кода, что позволяет создавать граф потока управления для анализируемого кода;
- оптимизация кода;
- обнаружение ошибок;
- доказательство отсутствия ошибок;
- реверс-инжиниринг.

Некоторые примеры инструментов, которые применяют методы статического анализа, включают CODESURFER/X86, JAKSTAB и BAP.

Однако, важно учесть, что у синтаксического анализа есть своя слабость по сравнению с динамическим анализом - в результирующем графе выполнения могут быть представлены даже те участки программы, на которые управление фактически никогда не переходит.

Автоматический статический анализ, инструменты

Автоматический динамический анализ. Представляет собой метод, в рамках которого инструменты для анализа бинарного кода запускают целевую программу на выполнение и наблюдают за её действиями во время выполнения.

Преимущество динамического анализа заключается в том, что он позволяет получить очень детальное представление о поведении программы в контексте конкретных выполненных трасс (путей выполнения), которые можно извлечь из графа потока управления программы.

Однако данные, собранные в результате одного или нескольких запусков программы, могут быть недостаточными для того, чтобы сделать полные выводы о поведении программы в целом.

Примеры инструментов, реализующих методы автоматического динамического анализа:

- управляемые фаззеры (такие, как AFL)
- утилиты, основанные на символическом выполнении
- динамические генераторы тестов

Подобные инструменты, реализующие методы динамического анализа, являются на сегодняшний день важной частью криминалистики.

По сравнению со статическим анализом практическое преимущество динамического анализа при распутывании кода, подвергнутого обфускации, в том, что инструменты, реализующие методы динамического анализа, более легко оперируют бинарными файлами.

Поэтому утилиты динамического анализа могут легко отслеживать самомодифицирующийся код, воспринимая его как обычный код.

Автоматический динамический анализ, инструменты

Ручной анализ. Остается неотъемлемой частью процесса, несмотря на наличие продвинутых автоматизированных утилит для анализа. Эти утилиты могут предоставить максимальную ценность, когда используются опытными специалистами в режиме автоматизации, а не полностью автоматически.

Дизассемблер IDA де-факто стандарт, так как включает в себя декомпилятор для всех трех распространенных архитектур процессоров: x86, x64 и ARM.

Ручной анализ

Выше были рассмотрены и кратко описаны основные методики обфускации и деобфускации Java кода. Однако, следует отметить, что использование данных методик обфускаций может усложнить отладку и поддержку программы, поэтому при выборе необходимо отталкиваться от поставленных задач.

Список используемых источников:

1. Java Obfuscation Techniques [Электронный ресурс] // URL: https://www.sable.mcgill.ca/JBCO/examples.html#RDS (дата обращения: 26.10.2023).

2. Obfuscating Java: The Most Pain for the Least Gain [Электронный ресурс] // URL: https://link.springer.com/content/pdf/10.1007/978-3-540-71229-9_7.pdf (дата обращения: 26.10.2023).

3. Полная классификация методов [Электронный ресурс] // URL: https://samag.ru/archive/article/3830 (дата обращения: 26.10.2023).

Ovsyannikov E.

Saint Petersburg State University of Industrial Technologies and Design

Techniques for obfuscation and deobfuscation of JAVA code.

This article is devoted to the analysis of methods of obfuscation and deobfuscation of Java code. In the course of the study, a brief overview of these methods will be formed.

Key words: obfuscation, deobfuscation, Java code, method.

УДК 003.27
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕТОДОВ СТЕГОАНАЛИЗА ДЛЯ ЛИНГВИСТИЧЕСКИХ СТЕГОСИСТЕМ

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

Исследования показали, что применение лингвистической стеганографии может скрыть факт передачи информации и сделать его практически незаметным для потенциального противника. Лингвистическая стеганография позволяет скрыто передавать информацию, внедряя её в текст, будь то письменный или устный, и встраивая скрытое сообщение в контекст, что создает стегообъект, не вызывающий подозрений у случайных наблюдателей. При этом первоначальное значение текста остается неизменным и не искажается. Таким образом, стегообъект можно передавать по открытым коммуникационным каналам, и в то же время, его обнаружение сложно для неподготовленных лиц.

особенности лингвистических стегосистем

Лингвистические стегосистемы основаны на использовании языковых структур, таких как слова, фразы, и синтаксические конструкции, для встраивания секретной информации. Это представляет собой вызов для традиционных методов стегоанализа, которые могут быть неэффективными при обнаружении таких стегосистем. Например, использование статистических методов может быть затруднено из-за сохранения лингвистической структуры

Техники Лингвистического Стегоанализа

Разработка методов стегоанализа для лингвистических стегосистем требует учета специфики языковых структур. Одним из методов является анализ статистических распределений слов и фраз в тексте. Лингвистические стегосистемы могут изменять эти распределения, и алгоритмы стегоанализа должны быть чувствительны к таким изменениям.

Другой подход включает в себя использование методов машинного обучения для обнаружения аномалий в тексте. Нейронные сети, обученные на больших объемах языковых данных, могут выявлять отклонения, вызванные встраиванием скрытой информации.

Актуальные Тенденции в Разработке Лингвистических Стегосистем

С развитием технологий и появлением новых методов обработки естественного языка (Natural Language Processing, NLP), лингвистические стегосистемы становятся более сложными и неприметными. Эмбеддинги слов, а также модели генерации текста на основе нейронных сетей, открывают новые возможности для внедрения секретной информации. Из-за этого становится жизненно важным дополнительное исследование техник стегоанализа, специально направленных на эти современные вызовы.

Этические и Юридические Аспекты Лингвистических Стегосистем

С ростом использования лингвистических стегосистем возникают вопросы этики и законности. Например, как использование таких технологий влияет на конфиденциальность коммуникации и какие могут быть юридические последствия использования стегосистем с противоправными целями? Исследование этих аспектов становится важным направлением в контексте развития стеганографии.

Критерии эффективности стегосистем

Исходя из определения стегосистемы, можно выделить три основных направления оценки эффективности стегосистем:

- количество информации, которое можно погрузить в ПО (чем больший объём секретной информации можно погрузить, тем лучше стегосистема);
- сложность обнаружения (показывает на сколько легко, для кого-либо обнаружить секретное сообщение. Как правило существует прямая связь между количеством вложенной информации и временем необходимым для её обнаружения. По мере увеличения объёма вложенной информации растёт вероятность того, что вложение секретной информации будет обнаружено);
- сложность удаления (заключает в себе тот принцип, что кто-либо, перехватив секретное сообщение не смог бы легко его удалить).

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. Часть 1. Цифровая стеганография. СПб. : Изд-во СПбГУТ, 2016. 226 с.

2. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М. : СОЛОН-ПРЕСС, 2009. 265 с.

3. Fridrich J. Steganography in Digital Media: Principles, Algorithms and Applications. Campridge University Press, 2010. 462 p.

Oleinik A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Research and development of methods of steganalysis for linguistic stegosystems.
Linguistic stegosystems represent an exciting area of research in the field of steganography. Stegoanalysis for such systems is a challenge that requires the development of innovative methods and technologies. The development of modern methods of steganalysis based on the linguistic features of the text is a key direction for ensuring security in the field of transmission of hidden information.

Key words: information security, steganography, linguistic steganography, naturalness of language.

УДК 004.056.5
ГРНТИ 81.93.29

РАЗРАБОТКА АЛГОРИТМА АНАЛИЗА ОБРАЗОВАНИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ ПО СЕВЕРО-ЗАПАДНОМУ ОКРУГУ ПО НАПРАВЛЕНИЯМ ОБУЧЕНИЯ 10.00.00

А. А. Павловская, М. В. Павловский
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Оценка образования кандидатов по специальности 10.00.00 для работодателей - проблема из-за несоответствия идеальных стандартов университетским программам, что затрудняет найм сотрудников. Автоматизация проверки выпускных квалификаций может помочь подходить к образованию более детально и улучшать точный отбор персонала.

информационная безопасность, ФСТЭК, оценка образовательной программы

Большой проблемой для работодателя является оценка уровня образования кандидатов на должность, так как идеальная картина не соответствует реальному уровню по многим пунктам.

Университеты не всегда следуют спискам ФГОС, включают в учебный план не все необходимые предметы или оставляют на них меньшее количество часов в пользу непрофильных, часто у преподавателей по ключевым дисциплинам отсутствует базовое образование по профилю, что тоже отражается на качестве знаний выпускников, и, как следствие – кадрового состава немаловажных отраслей государства.

Часто на сайте университета нет необходимой информации по профилю или найти ее крайне сложно, что тоже усложняет жизнь работодателю. Возможность проанализировать качество образования по специальности в различных университетах дает будущим работодателям более цельную картину возможностей и навыков тех, кого они планируют нанимать.

Зная особенности учебных планов, нюансы преподавания и соответствие программ обучения профстандартам, работодатель сможет подбирать персонал по более четкой системе с наглядным соответствием их требованиям.

Чтобы решить эту проблему, необходимо автоматизировать сбор анализа данных по университетам для более структурного хранения, удобного контроля соблюдения норм и быстрого доступа к информации о важных для работодателя нюансах подготовки выпускников.

Плюс, это поможет автоматизировать контроль над поддержанием качества образования в связи с переходом от болонской системы к новым стандартам. Для этого необходимо разработать специальную программу, которая будет собирать и анализировать данные о учебных планах, нагрузке преподавателей, соответствии программ профстандартам и другим важным параметрам.

Такая автоматизация позволит работодателям получать более полную и достоверную информацию о качестве подготовки выпускников различных университетов. Это поможет им принимать взвешенные решения при найме персонала и более точно оценивать уровень знаний и навыков потенциальных сотрудников.

Для автоматизации анализа университетов по направлению подготовки 10.00.00 выбраны следующие направления:

-Соответствие реализации программ с учетом ФГОС
-Процент содержания необходимых дисциплин в программе
-Процент преподавателей, имеющих базовое образование по профилю
-Материальная базу кафедры
-Соответствие профстандартам

На основе автоматизированного сбора данных будет видна цельная картина реализации кадров по данному направлению подготовки в Северо-Западном округе, что облегчит анализ качества программ ФСТЭК и даст работодателям возможность более тщательного подбора кадров для конкретных целей, что представлено на рис. 1.

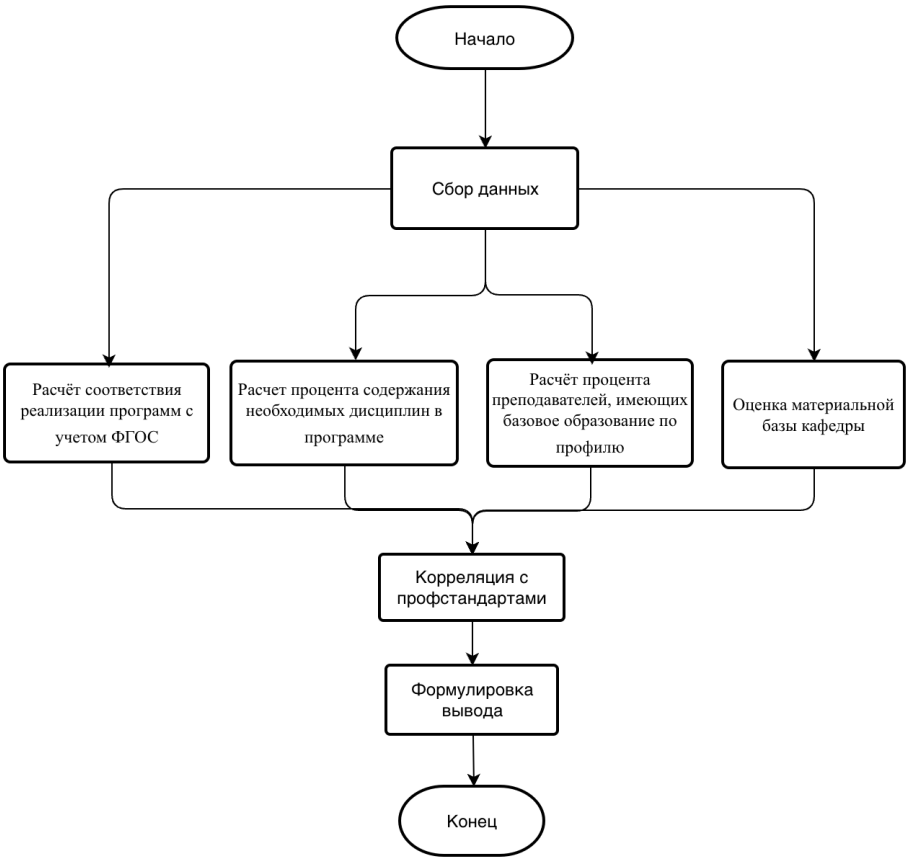


Рис. 25. Алгоритм работы системы анализа образовательной программы

В качестве образца для анализа выбран Санкт-Петербургский политехнический университет Петра Великого, где процент профильных дисциплин по специальности «Информационная безопасность» варьируется от 18 до 64 % в зависимости от уровня квалификации. Часть материальной

базы кафедры базируется на зарубежных комплектующих, оставшаяся описана поверхностно, без указания производителя. На данном направлении обучения это может считаться нерациональным, так как это может сказываться на безопасности государства, поскольку зарубежные спецслужбы могут отслеживать процесс обучения специалистов, часть из которых в дальнейшем будут работать на стратегически важных объектах страны. В условиях санкций и становления государства на рельсы самостоятельного развития образования и промышленности крайне важно взять под контроль процесс подготовки кадров высшими учебными заведениями. Утечка информации в данном случае недопустима. Для достижения этих целей необходимо контролировать объем отечественной материальной базы на кафедрах информационной безопасности.

Важно соблюдение правил и процедур, которые помогут предотвратить утечку информации и сохранить национальную безопасность. Это может включать в себя проверку специального программного обеспечения для мониторинга и контроля сетевого трафика, а также проведение регулярных проверок и аудитов учебных заведений.

В целом, увеличение объема отечественной материальной базы кафедры является необходимым шагом для обеспечения безопасности государства и самостоятельного развития образования и промышленности. Только через контроль и усиление национального потенциала мы сможем достичь своих стратегических целей и создать независимую и процветающую страну.

Важно отметить, что 64 % преподавателей данной кафедры имеют ученую степень. Однако, на текущий момент недоступна информация о специальности, по которой было получено высшее образование. Этот аспект является крайне важен для грамотной оценки подготавливаемых кадров работодателем. Уточнение специальности, в которой преподаватель получил свою ученую степень, позволит более точно определить его знания и навыки, что будет способствовать более эффективному обучению студентов.

Более подробный анализ показал, что лишь 33% преподавателей прошли повышение квалификации за последние 3 года. Возможно, часть информации не обновлена, но это вызывает определенные сомнения в соблюдении правил, согласно которым все сотрудники должны проходить дополнительное обучение не реже 1 раза за 3 года. Регулярное повышение квалификации является важной составляющей профессионального роста преподавателя и обеспечения высокого уровня образования для студентов.

Чтобы провести автоматизацию процессов и тщательный анализ, перед нами стоят следующие задачи:

1. Разработать методику анализа программ подготовки университетов с учетом ФГОС, включающую критерии оценки и их взаимосвязь.
2. Провести анализ программ подготовки университетов по направлению 10.00.00 с учетом ФГОС и определить степень соответствия каждой программы требованиям.

3. Разработать методику определения процента содержания необходимых дисциплин в программе подготовки университетов и применить ее для анализа выбранных направлений.

4. Провести анализ программ подготовки университетов по проценту содержания необходимых дисциплин и определить эффективность реализации каждой программы.

5. Разработать методику и провести анализ преподавателей по направлению 10.00.00, определить процент преподавателей, имеющих базовое образование по профилю, и оценить его влияние на качество подготовки студентов.

6. Провести анализ материальной базы кафедр университетов по направлению 10.00.00, определить ее соответствие требованиям и оценить влияние на качество подготовки студентов.

7. Разработать методику анализа соответствия программ подготовки университетов профстандартам и определить степень соответствия каждой программы требованиям и эффективность реализации каждой программы

8. Разработать методику комплексного анализа университетов по всем выбранным направлениям и определить рейтинговую оценку для каждого университета.

9. Провести комплексный анализ выбранных университетов по всем направлениям и сформулировать рекомендации по улучшению качества подготовки студентов.

Список используемых источников:

1. Алешкин А. С., Артюнов И. С., Жуков Д. О. Создание и использование интеллектуальных систем тестирования знаний // Современные технологии в задачах управления, автоматики и обработки информации : материалы XI Междунар. науч.-технич. семинара. Алушта, 2002. С. 172-173.

2. Берестнева О. Г., Марухина О. В. Компьютерная система принятия решений по результатам экспертного оценивания в задачах оценки качества обюразования // Educational Technology & Society. 2002. N 5.

3. Беспалько В. П., Татур Ю. Г. Системно-методическое обеспечение учебно-воспитательного процесса подготовки специалистов. М. : Высшая школа, 1989. 125 с.

4. Андрончев И. К., Дмитриев Д. С., Соловова Н. В. Управление образовательным процессом ВУЗа средствами информационно-коммуникационных технологий // Вестник СамГУ. 2014. N 8 (119). С.240-247.

5. Григораш О. В. Методика планирования учебной нагрузки с учётом результатов работы преподавателей // Научный журнал КубГАУ - Scientific Journal of KubSAU. 2013. N 92. URL: http://cyberleninka.ru/article/n/metodika-planirovaniya-uchebnoy-nagruzki-s-uchyotom-rezultatov-raboty-prepodavateley.

6. Towards Multi-Perspective Modeling with BPMN, 2015 г., Richard Braun, Werner Esswein, URL: https://www.researchgate.net/publication/274697790

7. Using the Business Process Model and Notation for Modeling Enterprise Integration Patterns, 2014 г., Daniel Ritter, URL:https://www.researchgate.net/publication/260873267

8. Нагорняк А. А. Современные подходы к организации процесса обучения в ВУЗе // Успехи современного естествознания. 2013. N 5. С.75-77.

Pavlovskaya A.*, *Pavlovsky M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development of an algorithm for analyzing the education of higher educational institutions in the North-Western District by areas of study 10.00.00.
Assessment of candidates' education in specialty 10.00.00 is a problem for employers because of the discrepancy between ideal standards and university programs, which makes it difficult to hire employees. Automating the verification of graduate qualifications can help approach education in more detail and improve accurate personnel selection.

Key words: information security, FSTEC, educational program evaluation.

УДК 004.021
ГРНТИ 20.53.23

АЛГОРИТМ НАСТРОЙКИ DMVPN НА УСТРОЙСТВАХ РОССИЙСКОГО ВЕНДОРА

А. В. Панков, И. А. Ушаков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье исследуется применение технологии DMVPN (Dynamic Multipoint VPN) для создания виртуальных частных сетей с использованием устройств российского вендора. Рассматриваются алгоритмы настройки DMVPN на указанных устройствах, а также анализируются преимущества импортозамещения в сфере сетевых технологий. Результаты исследования позволят эффективно применять DMVPN на устройствах российского производства и способствовать развитию отечественного рынка сетевого оборудования.

DMVPN, виртуальные частные сети, кибербезопасность, отказоустойчивость, импортозамещение

VPN, или виртуальная частная сеть (англ. virtual private network), является технологией, которая предоставляет возможность установки одного или нескольких сетевых соединений поверх другой сети. Она позволяет обеспечить коммуникацию между устройствами, используя сети с низким уровнем доверия, к примеру, публичные сети. Благодаря использованию криптографии уровень доверия к логической сети не зависит от уровня доверия к базовым сетям. Таким образом, VPN-сервис обеспечивает безопасную передачу данных по интернету и защищает конфиденциальную информацию.

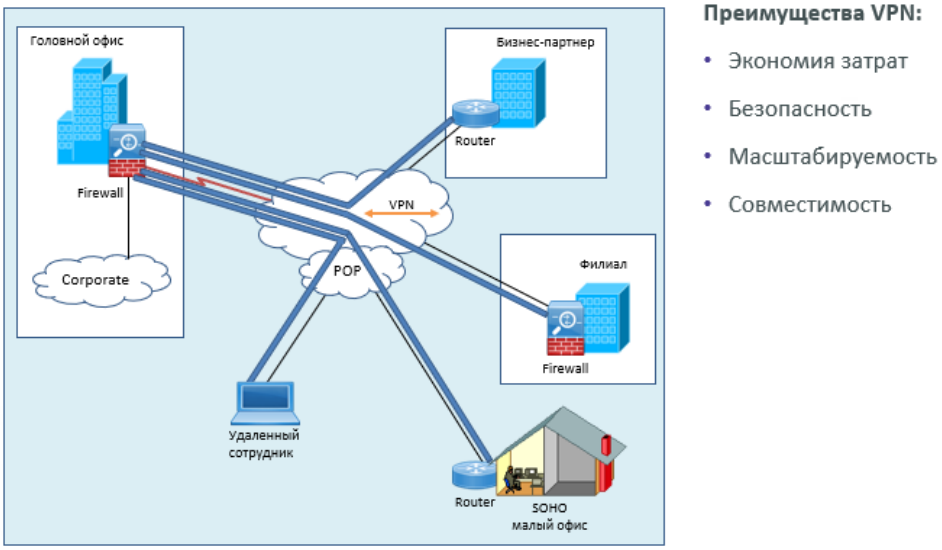


Рис. 1. Схематичное изображение принципа работы VPN

DMVPN использует два ключевых протокола:

GRE (Generic Routing Encapsulation), который позволяет упаковать разные типы трафика в единую структуру и передавать его по сети;

NHRP (Next Hop Resolution Protocol), который способствует нахождению маршрутов до удаленных узлов, что значительно упрощает маршрутизацию и обработку пакетов в VPN сети.

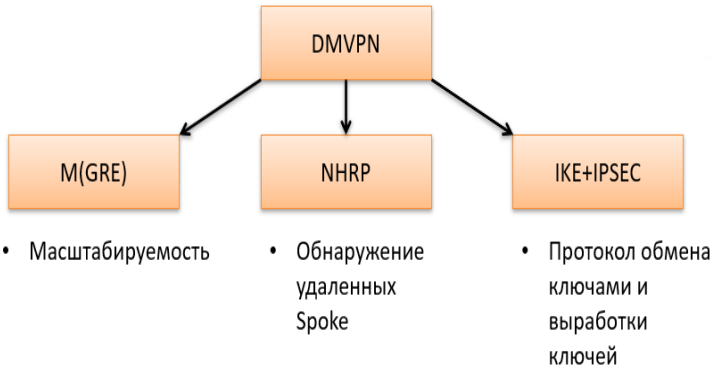


Рис. 2-3. Общая схема и компоненты DMVPN

DMVPN также предлагает гибкую настройку и позволяет создавать более сложные схемы подключения для вашей сети. Он может использоваться для подключения удаленных сетей и удаленных пользователей и надежно защищает данные от киберугроз и атак.

Для проверки работоспособности данной топологии использовались маршрутизаторы ESR-200 производства компании Eltex. Общую схему используемой топологии можно рассмотреть на изображении:

Рис. 4-5. Маршрутизатор Eltex ESR200 и коммутатор доступа Eltex MES2308P, использовавшиеся в лабораторной установке

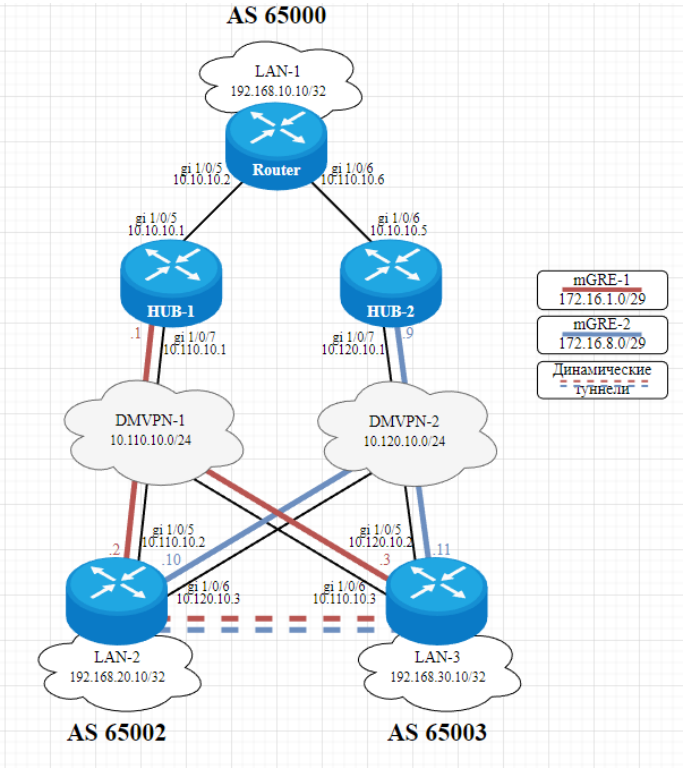


Рис. 5. Схема лабораторной установки

На маршрутизаторах были настроены протоколы BGP и IKE отдельно для каждой из двух используемых виртуальных частных сетей. Также для каждой сети в отдельности были сконфигурированы IPSec.

Предполагалось, что один из маршрутизаторов Hub будет искусственно выведен из строя в ходе имитации неожиданно возникшей неисправности, а оставшийся должен будет взять на себя его функции.

Тестирование отказоустойчивости сети проводилось путём отправки эхо-запросов между локальными сетями.

```
    10.110.10.2 > 10.110.10.3: ESP(spi=0xcc653697,seq=0x58), length 168
10:33:41.912446 a8:f9:4b:af:91:ae > a8:f9:4b:af:80:cf, ethertype IPv4 (0x0800), lengt
tos 0x0, ttl 16, id 34668, offset 0, flags [DF], proto GRE (47), length 108)
    10.110.10.2 > 10.110.10.3: GREv0, Flags [none], proto IPv4 (0x0800), length 88
        (tos 0x0, ttl 64, id 5515, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.20.10 > 192.168.30.10: ICMP echo request, id 262, seq 5, length 64
10:33:41.987971 a8:f9:4b:af:91:ae > a8:f9:4b:af:83:6a, ethertype IPv4 (0x0800), lengt
tos 0xc0, ttl 64, id 0, offset 0, flags [DF], proto ESP (50), length 156)
    10.110.10.2 > 10.110.10.1: ESP(spi=0xcbd28bd1,seq=0x41), length 136
10:33:42.219425 a8:f9:4b:af:91:ae > a8:f9:4b:af:83:6a, ethertype IPv4 (0x0800), lengt
tos 0xc0, ttl 64, id 0, offset 0, flags [DF], proto ESP (50), length 156)
    10.110.10.2 > 10.110.10.1: ESP(spi=0xcbd28bd1,seq=0x42), length 136
10:33:42.219717 a8:f9:4b:af:91:ae > a8:f9:4b:af:83:6a, ethertype IPv4 (0x0800), lengt
```

Рис. 6. Неактивен интерфейс gi 1/0/5 маршрутизатора Spoke 1

На иллюстрации выше красным цветом выделено время отправки последнего пакета, 10:33:41, далее пакеты по этому интерфейсу не могут быть отправлены.

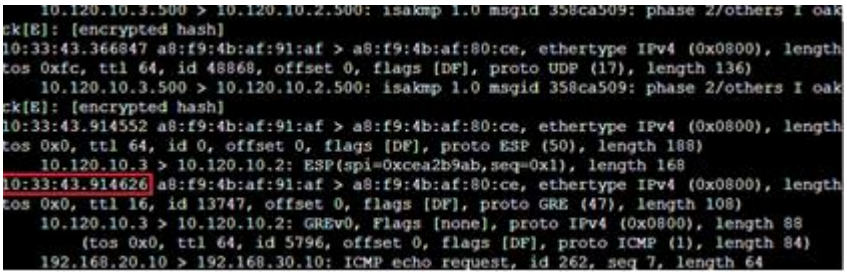


Рис. 7. Мониторинг интерфейса gi 1/0/5 маршрутизатора Spoke-2

На данном снимке экрана видно, как в 10:33:42 начинается согласование параметров резервного туннеля, а в 10:33:43 по данному туннелю уже отправляется первый пакет. Таким образом, можно заключить, что в данном случае на восстановление работоспособности сети понадобилось две секунды.

Описанный тест проводился несколько раз, результаты вносились в приведённую далее таблицу 1:

ТАБЛИЦА 1. Результаты проведенных тестов отказоустойчивости

Номер теста	Время последнего ICMP-пакета	Время первого ICMP-пакета	Количество потерянных пакетов	Время переключения, с
1	10:33:41	10:33:43	1	2
2	10:49:49	10:49:50	0	1
3	10:52:06	10:52:07	0	1
4	10:56:41	10:56:43	1	2
5	11:01:15	11:01:16	0	1

Анализ результатов пяти проведённых тестов даёт возможность сделать вывод, что исследуемая топология позволяет пользователям игнорировать выход из строя любого из маршрутизаторов Hub. По результатам проведённой работы разработан и проверен на практике путём, в том числе, проведённого выше эксперимента алгоритм, позволяющий достигнуть высокого уровня отказоустойчивости сети.

Список используемых источников:

1. Анализ угроз информационной безопасности виртуальных частных сетей, построенных на базе сети MPLS / А. А. Кузьмич, И. А. Кузьмич, Г. А. Киреев, И. В. Сизов // Состояние и перспективы развития современной науки по направлению «Информационная безопасность» : материалы III Всерос. научно-технич. конф., Анапа, 21–22 апр. 2021 г. Анапа: Федеральное государственное автономное учреждение "Военный инновационный технополис "ЭРА", 2021. С. 328-333.

2. Исследование и оценка наиболее значимых количественных характеристик оборудования MPLS / П. В. Карельский, И. П. Зуев, М. М. Ковцур, Д. В. Юркин // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 1. С. 62-68.

3. Исследование методики сравнения VPN решений / М. М. Ковцур, Д. В. Сахаров, Б. С. Мисливский, А. В. Михайлова // Информационная безопасность регионов России :

материалы XII Санкт-Петербургской межрегион. конф., Санкт-Петербург, 27–29 нояб. 2021 г. СПб. : Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2021. С. 387-388.

4. Исследование эффективности VPN туннелей для организации удаленного доступа / Е. В. Гавриленко, А. Д. Докшин, М. М. Ковцур, Б. С. Мисливский // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы материалы X Междунар. науч.-технич. и науч.-методич. конф., Санкт-Петербург, 24–25 фев. 2021 г. СПб. : СПбГУТ, 2021.С. 201-205.

5. Ушаков И. А., Панков А. В., Елфимов А. В. Проверка отказоустойчивости DMVPN в разных конфигурациях // Экономика строительства. 2023. N 5. С. 129-133.

6. Мингбо Л., Чжао Ч., Шань Ю. Оценка производительности сети DMVPN при использовании разных протоколов маршрутизации // Информационно-управляющие системы. 2019. N 2. С. 54-59.

7. Обеспечение безопасности передачи multicast-трафика в IP-сетях / А. В. Красов, Д. В. Сахаров, И. А. Ушаков, Е. П. Лосин // Защита информации. Инсайд. 2017. N 3(75). С. 34-42.

8. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPv6 / Д. В. Сахаров, А. В. Красов, И. А. Ушаков, Э. В. Бирих // Защита информации. Инсайд. 2020. N 1(91). С. 51-57.

Pankov A., Ushakov I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Algorithm for setting up DMVPN on devices of a Russian vendor.

This article examines the use of DMVPN (Dynamic Multipoint VPN) technology for creating virtual private networks using devices from a Russian vendor. Algorithms for setting up DMVPN on these devices are considered, and the advantages of import substitution in the field of network technologies are analyzed. The results of the study will make it possible to effectively use DMVPN on Russian-made devices and contribute to the development of the domestic network equipment market.

Key words: DMVPN, virtual private network, cybersecurity, fault tolerance, import substitution.

УДК 004.42
ГРНТИ 20.23.25

АНАЛИЗ ЭФФЕКТИВНЫХ СРЕД БОЛЬШИХ ДАННЫХ В СФЕРЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ И МАШИННОГО ОБУЧЕНИЯ

А. А. Панфилов
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В современном информационном обществе взрывной рост объемов данных, известный как "большие данные", стал вызовом и возможностью одновременно. Большие объемы данных требуют эффективных методов анализа и обработки, особенно в контексте облачных технологий и машинного обучения. Исследование представляет собой обширный обзор современных методов и инструментов обработки больших данных в облачных вычислениях.

большие данные, облачные технологии, машинное обучение

Современный мир переживает взрывной рост объемов данных, который ставит перед бизнесом, наукой и технологическими разработками существенные вызовы. Эти данные, часто называемые "большими данными" (Big Data), стали неотъемлемой частью повседневной жизни и имеют глубокое влияние на процессы принятия решений. Сферы, такие как медицина, финансы, маркетинг и научные исследования, сталкиваются с необходимостью эффективного анализа и использования этих данных для достижения выдающихся результатов и конкурентных преимуществ.

Однако, с ростом объемов данных возникают сложности в их обработке, хранении и анализе. Именно здесь выявляется ключевая роль технологий облачных вычислений и машинного обучения.

Облачные технологии, такие как Amazon Web Services (AWS), Microsoft Azure и Google Cloud Platform (GCP), предоставляют возможность масштабировать вычисления в зависимости от потребностей, предоставляя доступ к высокопроизводительным вычислительным ресурсам и гибким хранилищам данных. Вместе с тем, машинное обучение, основанное на алгоритмах и искусственном интеллекте, позволяет извлекать ценные знания из этих данных, создавая прогностические модели и автоматизируя процессы принятия решений.

Рассмотрим пять ведущих облачных платформ: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud и Alibaba Cloud, выделяя их ключевые характеристики и особенности.

Amazon Web Services (AWS): AWS является лидером в области облачных вычислений и предоставляет широкий спектр услуг. Amazon S3 обеспечивает масштабируемое и надежное хранилище данных, а Amazon EMR позволяет запускать распределенные вычисления на базе Apache Hadoop и Spark. AWS также предлагает множество сервисов машинного обучения, включая Amazon SageMaker, который обеспечивает интеграцию с

популярными библиотеками и инструментами машинного обучения. Amazon SageMaker – это управляемый сервис для разработки, обучения и развертывания моделей машинного обучения. С SageMaker, исследователи данных и разработчики могут легко создавать модели с использованием встроенных алгоритмов или собственных алгоритмов, обучать их на больших объемах данных и автоматически развертывать в производственных окружениях. SageMaker поддерживает популярные библиотеки машинного обучения, такие как TensorFlow и PyTorch. [1]

Microsoft Azure: Azure предоставляет обширные возможности для анализа данных и машинного обучения. Azure Blob Storage и Azure Data Lake Storage обеспечивают высокопроизводительное и масштабируемое хранилище данных. Azure Machine Learning позволяет создавать, обучать и развертывать модели машинного обучения, интегрируясь с популярными фреймворками и инструментами. Azure Machine Learning предоставляет средства для разработки, обучения и развертывания моделей машинного обучения. Сервис интегрируется с другими продуктами Azure, обеспечивая легкость использования и масштабируемость. Azure Machine Learning поддерживает создание моделей с использованием Python и R, что делает его популярным выбором для исследователей данных. [2]

Google Cloud Platform (GCP): GCP предлагает высокопроизводительные хранилища данных, такие как Google Cloud Storage и Google Cloud Bigtable. Сервис Google Cloud Dataproc обеспечивает быстрое развертывание и управление кластерами Apache Spark и Hadoop. Google AI Platform предоставляет инструменты для разработки и развертывания моделей машинного обучения с использованием TensorFlow. Google AI Platform предоставляет инструменты для создания, обучения и развертывания моделей машинного обучения с использованием TensorFlow. Этот сервис позволяет разработчикам создавать and-to-and пайплайны машинного обучения, включая предобработку данных, создание моделей, обучение и инференс. Google AI Platform также предоставляет доступ к предварительно обученным моделям и интегрируется с другими инструментами GCP. [3]

IBM Cloud: IBM Cloud предоставляет гибкие и безопасные облачные услуги для анализа данных. IBM Db2 обеспечивает мощные средства анализа и обработки данных, а Watson Studio позволяет создавать и обучать модели машинного обучения с применением различных языков программирования и библиотек. Watson Studio – это платформа для создания, обучения и развертывания моделей машинного обучения и искусственного интеллекта. Она интегрируется с различными источниками данных и обеспечивает возможность работы с данными в рамках рабочего процесса машинного обучения. Watson Studio также поддерживает работу с Jupyter ноутбуками, что обеспечивает удобство в экспериментах с данными и моделями. [4]

Alibaba Cloud: Alibaba Cloud предоставляет обширные услуги для обработки больших данных и машинного обучения. Облачное хранилище данных (Object Storage Service) и сервисы обработки данных в режиме

реального времени (DataWorks) обеспечивают эффективный анализ данных. Machine Learning Platform for AI предоставляет гибкие средства для разработки и развертывания моделей машинного обучения. Machine Learning Platform for AI предоставляет графический интерфейс для разработки и развертывания моделей машинного обучения. Он включает в себя широкий набор инструментов и библиотек для создания моделей, а также предварительно обученные модели для различных задач. Этот сервис интегрируется с другими продуктами Alibaba Cloud, обеспечивая комплексный подход к анализу данных и машинному обучению.

В облачных средах аспекты машинного обучения охватывают весь цикл разработки моделей, начиная от подготовки данных и создания моделей до обучения и развертывания в производственных условиях. Платформы предоставляют различные инструменты и сервисы, которые упрощают и ускоряют процесс разработки и внедрения моделей машинного обучения, делая их доступными для широкого круга специалистов.

Важно учитывать технические характеристики и инновационные возможности при выборе подходящей платформы для конкретного проекта.

Одним из главных преимуществ является масштабируемость, позволяющая быстро масштабировать вычислительные ресурсы в зависимости от потребностей проекта. Это особенно важно для проектов, требующих обработки больших объемов данных или внезапных пиковой активности. Облачные платформы также обеспечивают гибкость, позволяя выбирать и настраивать необходимые сервисы и ресурсы в соответствии с требованиями проекта. Это способствует оптимизации затрат и улучшению эффективности бизнес-процессов.

Еще одним важным преимуществом является безопасность данных. Облачные платформы предоставляют высокий уровень защиты данных, включая механизмы шифрования, многоуровневые системы аутентификации и мониторинг безопасности. Особенно важно для проектов, связанных с обработкой чувствительных данных или персональной информации.

Среди других преимуществ можно выделить постоянные инновации. Облачные платформы постоянно внедряют новые технологии и сервисы, что позволяет проектам оставаться конкурентоспособными и использовать новейшие методы анализа данных и машинного обучения.

Однако существуют и ограничения облачных платформ. Одним из них является зависимость от интернет-соединения. Для эффективной работы с облачными ресурсами необходимо стабильное и быстрое подключение к Интернету. Также важно учитывать стоимость. Хотя облачные услуги предлагают гибкое ценообразование, неправильное планирование и управление ресурсами может привести к неожиданным расходам. Еще одним ограничением является контроль над данными, особенно в случае обработки конфиденциальных данных или соблюдения законодательных норм и стандартов.

Важно учитывать как преимущества, так и ограничения облачных платформ при принятии решения о переходе к облачным ресурсам, а также разрабатывать стратегии управления рисками и оптимизации затрат.

Рассматриваемые среды предоставляют разнообразные возможности для машинного обучения, каждая из которых обладает своими уникальными особенностями. AWS, с сервисом SageMaker, выделяется возможностью создания высокопроизводительных моделей глубокого обучения и удобными инструментами для обучения с учителем и без учителя. Azure, в свою очередь, предоставляет Azure Machine Learning, интегрированный с многими другими сервисами Microsoft, что облегчает разработку и эксперименты с моделями машинного обучения. GCP, с использованием TensorFlow, обеспечивает превосходные возможности для обучения и развертывания сложных нейронных сетей, а также предоставляет специализированные API для обработки изображений, речи и текста.

Например, в сфере обработки изображений и видео аналитики, GCP с его Vision AI и Video AI API предоставляет возможности для распознавания объектов, лиц и даже анализа эмоций в видеорядах. AWS SageMaker может быть использован для создания интеллектуальных систем, способных предсказывать потребительские предпочтения на основе анализа покупательского поведения. Azure Machine Learning легко интегрируется с Microsoft Excel, что делает его идеальным инструментом для анализа больших объемов данных и прогнозирования трендов в бизнесе. IBM Watson предоставляет широкий спектр когнитивных сервисов, включая анализ тональности текста, классификацию исследований и даже создание чат-ботов. В то время как Alibaba Cloud, с его сервисом Machine Learning Platform for AI, предоставляет множество готовых решений для бизнеса, включая рекомендательные системы для электронной коммерции и системы мониторинга качества продукции в производстве. Каждая платформа предоставляет уникальные инструменты и API для специфических задач машинного обучения, что позволяет выбирать подходящее решение в зависимости от требований проекта.

Список используемых источников:

1. About AWS [Электронный ресурс]. URL: https://docs.aws.amazon.com/whitepapers/latest/gxp-systems-on-aws/about-aws.html (дата обращения 26.10.2023).

2. Azure for developers overview [Электронный ресурс]. URL: https://learn.microsoft.com/en-us/azure/developer/intro/azure-developer-overview/ (дата обращения 26.10.2023).

3. Introduction to AI Platform [Электронный ресурс]. URL: https://cloud.google.com/ai-platform/docs/technical-overview (дата обращения 26.10.2023).

4. Documentation for Cloud Pak for Data as a Service [Электронный ресурс]. URL: https://dataplatform.cloud.ibm.com/docs/content/wsj/getting-started/welcome-main.html?context=analytics&audience=wdp/ (дата обращения 26.10.2023).

Panfilov A.

St. Petersburg State University of Industrial Technologies and Design

Analysis of effective big data environments in the field of cloud technologies and machine learning.
In today's information society, the explosive growth of data, known as "big data," has become both a challenge and an opportunity. Large volumes of data require efficient analysis and processing methods, especially in the context of cloud technologies and machine learning. The study provides an extensive overview of modern methods and tools for processing big data in cloud computing.

Key words: Big data, cloud technologies, machine learning.

УДК 004.056
ГРНТИ 81.93.29

Преимущества хостовых IDS в обнаружении ботнет-сетей

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

В современном мире одной из самой большой опасностью является ботнет. В связи с этим требуется особое внимание уделить методам их обнаружения для минимизации ущерба. В данной статье рассматривается опасность ботнета как масштабного средства реализации атак на системы и выдвинуто предположение об эффективности использования хостовых IDS для своевременного их обнаружения. В рамках подтверждение правильности предположения будет реализован исследовательский стенд для изучения реакции системы на сетевые атаки.

ботнет, IDS, хостовая IDS, сетевые атаки, безопасность

Ботнет представляет собой множество устройств, зараженных при помощи специального программного обеспечения – бота [1]. В процессе создания бота злоумышленник реализует в нем возможность самостоятельного распространения по сети, захватывая все больше устройств, и способность удаленно принимать и выполнять переданные команды. Основная цель при создании масштабной сети из ботов – реализация DDoS-атаки, которая направлена на нарушение работы информационной системы посредством исчерпания её вычислительных ресурсов.

Не менее популярной атакой, реализуемой с помощью ботнет, является фишинг. Реализация происходит посредством рассылки спам-писем, создаваемых ботами. В случае успешной атаки может происходить не только обычное заражение устройства ботом, но и кража банковской информации пользователя.

С целью распространить бота или получить конфиденциальную информацию не только пользователей, но и компаний, злоумышленник может прибегать не только к фишингу, но и к атаке типа брутфорс, т.е. получении доступа к учетной записи при помощи перебора логина и пароля. Так, в октябре 2023 года компанией QNAP была обнаружена массовая брутфорс-атака, нацеленная на сетевые хранилища со слабым паролем [2].

Так же целью злоумышленника может стать и эксплуатация уязвимостей оборудования. В июле 2023 года компанией Fortinet было заявлено, что целью нескольких ботнетов, реализующих DDoS-атаки, стала эксплуатация уязвимости Zyxel. CVE-2023-28771 позволяла злоумышленнику без прохождения аутентификации произвести выполнение произвольного кода удаленно, отправляя модифицированные пакеты на уязвимое оборудование [3].

Несмотря на реализацию настолько массовых атак, сам бот может не оказывать какую-либо значительную нагрузку на подчиненное им устройство, а значит опознать его в системе обычному пользователю будет практически невозможно. Стоит брать во внимание и тот факт, что злоумышленник может и не оставить следов в процессе реализации атаки. Поэтому для своевременного определения бота в системе или обнаружения атаки необходимо прибегать к анализу трафика в сети.

С этой целью может внедрятся IDS (от англ. Intrusion Detection System) – система обнаружения вторжений (устройство или ПО), которая производит анализ сетевого трафика на наличие вредоносной активности и нарушения политик безопасности [4]. В случае обнаружения подозрительной активности формируется оповещения администратору для последующего реагирования.

Детектирование вредоносной активности строится на одном из двух методов:

1. Обнаружение на основе сигнатур: обнаружение вторжения происходит на основе сравнение текущего трафика с имеющимися образцами сигнатуры атак.

2. Обнаружение на основе аномалий: сравнивается эталон доверенного трафика контролируемой системы с текущей активностью в сети и, в случае отклонения, производится оповещение администратора.

Также существует разновидность IDS в зависимости от расположения: хостовая IDS (далее - HIDS) или IDS на основе сети (NIDS). В случае HIDS происходит отслеживание не только трафика, проходящего через сетевую карту оконечного оборудования, но и также может производится отслеживание активности приложений в системе. В свою очередь NIDS производит анализ трафика, проходящего через сетевое устройство – коммутатор, маршрутизатор и т.д.

В предстоящем проекте будет проанализирована эффективность использования хостовой IDS с целью обнаружения атаки со стороны ботнет-сети. Исходя из поставленной цели первоначально требуется проанализировать потребность в использовании именно хостовой IDS и необходимы ли дополнительные средства диагностики для сбора и анализа информации.

Определим перечень информационных ресурсов, на основе которых можно обнаружить аномальную активность в режиме реального времени:

– журнальные файлы ОС – файлы, содержащие информацию о работе ОС;

– журнальные файлы приложений – файлы, содержащие информацию о работе конкретного приложения;

– файлы в файловая система – любое изменение файлов, не считая журнальных (изменение владельца, свойств и т.д);

– сетевые соединение – анализ активности сокета;

– запущенные процессы – анализ запущенных приложений в системе;

– загруженность системы – в рамках анализа за показатель примем загруженность диска;

– настроенные политики безопасности – анализ политик на отсутствие несогласованных внедрений.

Проанализируем возможность определения конкретной активности бота в системе не только на основе перечисленных информационных ресурсов, но и в случае использования HIDS и NIDS. Результаты анализа приведены в таблице 1.

ТАБЛИЦА 2. Возможность детектирования аномального трафика с использованием конкретного информационного ресурса

Компьютерная атака / Список ресурсов	Установка бота/вредоносного ПО	Соединение с сервером злоумышленника	Сканирование портов	Брутфорс SSH	DDoS-атака	Эксплуатация уязвимости
Журнальный файл ОС	+	-	-	+	-	-
Журнальный файл приложений	-	-	-	+	+	+
Файлы в файловой системе	+	-	-	-	-	-
Сетевое соединение	-	+	+	+	-	+
Наличие процесса в системе	+	+	-	-	-	-
Загруженность системы	-	-	-	-	+	-
Настроенные политики безопасности	-	+	-	-	-	+
HIDS	+	+	+	+	+	+
NIDS	-	+	+	+	+	-

Стоит учесть, что, в зависимости от уровня знаний злоумышленника, вредоносная активность, отмеченная как определяемая без использования HIDS и NIDS, может быть не зафиксирована. Например, при реализации атаки брутфорс может и не оставить следов в журнальном файле ОС и атаку можно обнаружить при реализации анализатора трафика на текущий момент. Так же и в случае DDoS-атаки: зафиксировать повышение нагрузки на веб-сервис будет возможно по журналу ПО, задействованному в поддержании работоспособности атакуемого сервиса при условии, что имеющаяся система систематизации данных предоставляет необходимую информацию.

Значит внедрение IDS необходимо для повышения точности обнаружения вредоносного трафика в сети. Учитывая результаты анализа – именно хостовая IDS позволит с большей вероятностью детектировать ботнет-сеть.

Для практического изучения эффективности HIDS разработан стенд, представленный на рис. 1, на основе виртуальных машин (далее – ВМ). Со стороны ботнет будет использоваться ОС Kali Linux, предназначенная для тестирования безопасности. ВМ установленной и настроенной IDS создана на ОС Ubuntu.

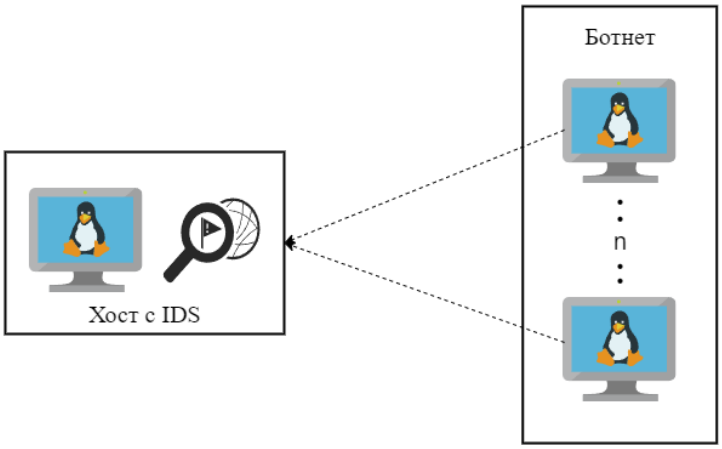


Рис. 26. Схема взаимодействия ВМ

Рассмотрим работу хостовой IDS на примере брутфорс-атаки. Упрощенная схема реализации приведена на рис. 2.

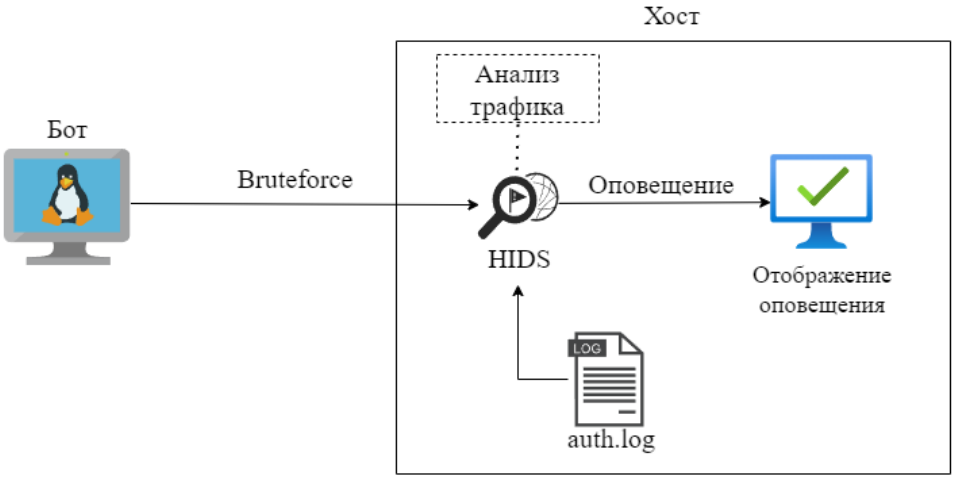


Рис. 27 – Упрощенная схема реагирование HIDS на брутфорс-атаку

В рамках тестирования HIDS, помимо анализа трафика на хосте, настроен также и анализатор журналов системы с целью повышения точности определения попытки несанкционированного доступа к системе. Бот генерирует вредоносный трафик, направленный на получение доступа к конкретной учетной записи администратора. HIDS, получая данные сетевой

активности и запись из журнала, производит сравнение с заранее заданным эталоном поведения. По итогу сравнения и обнаружение аномалии будет сформировано оповещение, которое отобразится на мониторе администратора.

Таким образом, реализуя атаки, схожие с вредоносным трафиком со стороны ботов, будут получены статистические данные, на основе которых можно оценить эффективность HIDS в обнаружении ботнет. Кроме этого, подобная информация может оказаться крайне полезной при организации безопасности системы, так как в ходе настройки хостовой IDS выявятся наиболее уязвимые участки системы.

Список используемых источников:

1. Косенко, М. Ю. Вопросы обеспечения защиты информационных систем от ботнет атак / М. Ю. Косенко, А. В. Мельников // Вопросы кибербезопасности. 2016, № 4(17), с. 20-28.

2. QNAP, in Collaboration with Digital Ocean, Successfully Prevents NAS Weak Password Attacks to Ensure User Data Security [Электронный ресурс]. URL: https://www.qnap.com/en/security-news/2023/qnap-in-collaboration-with-digital-ocean-successfully-prevents-nas-weak-password-attacks-to-ensure-user-data-security (Дата обращения: 20.10.2023).

3. DDoS Botnets Target Zyxel Vulnerability CVE-2023-28771 [Электронный ресурс]. URL: https://www.fortinet.com/blog/threat-research/ddos-botnets-target-zyxel-vulnerability-cve-2023-28771 (Дата обращения: 20.10.2023).

4. IDS (система обнаружения вторжений) [Электронный ресурс]. URL: https://encyclopedia.kaspersky.ru/glossary/ids-intrusion-detection-system/ (Дата обращения: 20.10.2023).

Perminova Y.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Advantages of Host-based IDS in Botnet Detection.

In the modern world, one of the biggest dangers is botnet. In this regard, special attention should be paid to the methods of their detection to minimize damage. This article examines the danger of botnet as a large-scale means of implementing attacks on systems and suggests the effectiveness of using host IDS for their timely detection. As part of the confirmation of the correctness of the assumption, a research stand will be implemented to study the system's response to network attacks.

Key words: botnet, IDS, Host-based IDS, network attacks, security.

УДК 004.7
ГРНТИ 20.01

RESEARCH ON WEB-APPLICATION SECURITY TESTING USING METASPLOIT FRAMEWORK

A. Chiziba, R. Petriv
Saint Petersburg State University of Telecommunication name after Prof. M.A Bonch-Bruevich

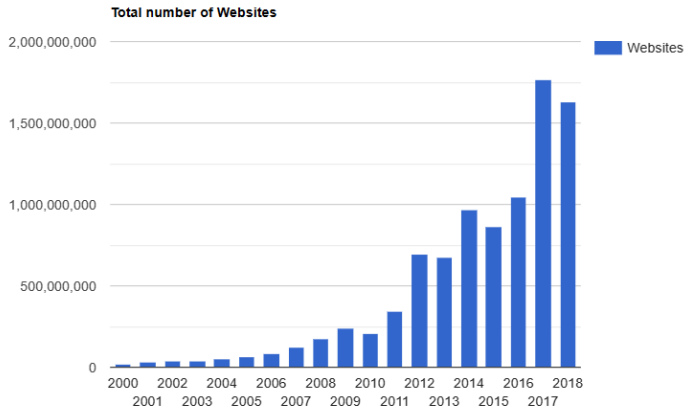
In recent years there has an exponential increase in the number of web applications and websites that have been deployed by individuals, institutions, and organizations to provide services and information to people.

web applications, vulnerabilities, SQL injection, cross-site request forgery (CSRF), authentication bypass

B The rise in the use of web applications has been rapid, fundamentally reshaping how we interact with digital technology. These dynamic, interactive platforms accessed through web browsers have become a normal part in our daily lives. This surge is fueled by several key factors. Firstly, the convenience and accessibility of web apps transcend device limitations, enabling users to seamlessly transition from desktops to mobile devices. The introduction of high-speed internet and the advent of 5G technology further optimize the user experience, ensuring smooth and responsive application performance.

Moreover, web applications have simplified software access. They eliminate the need for complex installations or updates, allowing users to instantly leverage powerful tools and services. Major tech giants, offering a diverse array of web-based solutions, have catalyzed this revolution. Additionally, cloud computing plays a pivotal role, providing the infrastructure backbone for web applications, allowing them to scale, adapt, and handle massive user loads.

This has led to an increase in users and the development and deployment of web applications. The image (img.1) below shows the increase in number of web applications over 18 years.



Img. 1. Statics of Web Applications over an 18year Period

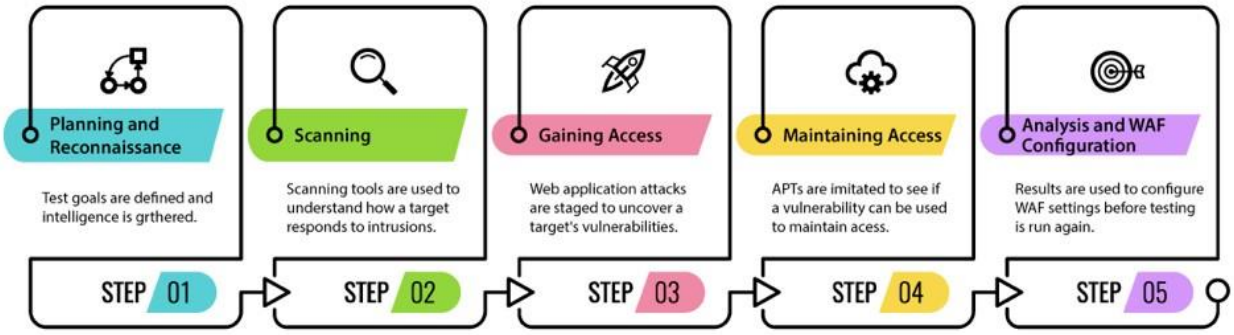
With the rise in web applications, this has also led to an increase to cyber-attacks on these websites. There are different types of attacks that are carried out depending on the desired outcome.

Some of the different types of attacks that are commonly carried out and their methodologies are listed in table 1.

TABLE 1. Common types of cyber-attacks and their methodologies

Attack	Method
DoS and DDos	Overwhelms target server with requests thereby denying service to other legitimate clients
SQL Injection	Involves sending malicious SQL query to database to penetrate the system and gain access
URL Interpretation	Altering and fabricating URL addresses and using them to gain access to restricted parts of the website
Brute Force Attack	The attacker tries to gain access to the web application by trying possible login details. This can be done manually or with the help of bots that a supplied with a list of possible login credentials
Session Hijacking	The attacker takes over a session between an authentic client and the server. The computer being used in the attack substitutes its IP address for that of the client computer and continues the session with the server
Ransomware	The hacked system is held hostage until a certain sum is paid to the attacker and instructions are given on how the target can regain control of their web application

With this is mind, it is relevant to carry out research on web-application security testing using Metasploit framework as it allows to emulate most of the attacks and provide post-exploit analysis. The image (Img. 2) below show the stages of security testing (penetration testing) of web application using the Metasploit framework.



Img. 2. Stages of Web Application Security (Penetration) testing using Metasploit framework

This topic of research will involve several stages to systematically identify and address vulnerabilities. Below are some of the planned key stages:

Define Objectives: Clearly state the goals of the security testing, including the scope, target applications, and specific vulnerabilities to focus on.

Obtain Authorization: Ensure proper authorization and consent from the relevant stakeholders before conducting any security testing.

Gather Information: Collect information about the target web application, including its technology stack, architecture, and any known vulnerabilities.

Metasploit Integration: Use Metasploit to search for and select modules targeting identified vulnerabilities. Load the appropriate module for exploitation.

Configure and Execute Exploits: Set the necessary parameters for the selected module and execute it to exploit the identified vulnerability.

Record Findings: Document the identified vulnerabilities, successful exploits, and any compromised systems.

Recommendations: Provide recommendations for addressing the vulnerabilities, including patches, configuration changes, or additional security measures.

Risk Assessment: Evaluate the potential impact and likelihood of exploitation for each identified vulnerability.

Review: Review the testing process to identify areas for improvement in future security assessments.

List of sources used:

1. Total number of Websites [Electronic resource]. URL: https://www.internetlivestats.com/total-number-of-websites// (date of access 31.10.2023).
2. Types of Cyber Attacks [Electronic resource]. URL: https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks/ (date of access 31.10.2023).
3. Metasploit Documentation [Electronic resource]. URL: https://docs.metasploit.com/ (date of access 31.10.2023).
4. Metasploit — A Walkthrough Of The Powerful Exploitation Framework [Electronic resource]. URL: https://www.freecodecamp.org/news/metasploit-a-walkthrough-of-the-powerful-exploitation-framework/ (date of access 31.10.2023).

Петрив Р., Чизиба Э.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Исследования по тестированию беопасности веб-приложений с использованием METASPLOIT FRAMEWORK.

В последние годы наблюдается экспоненциальный рост числа веб-приложений и веб-сайтов, которые были развернуты отдельными лицами, учреждениями и организациями для предоставления услуг и информации людям.

веб-приложения, уязвимости, SQL-инъекция, подделка межсайтовых запросов (CSRF), обход аутентификации.

УДК 004.056.53
ГРНТИ 81.93.29

СИНТЕЗ МЕТОДА ВЫЯВЛЕНИЯ ФИШИНГОВЫХ САЙТОВ

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

Сейчас в Интернете остро стоит проблема кражи личных данных посредством фишинговых сайтов. На данный момент существуют инструменты, предупреждающие пользователя о том, что ссылка, по которой он пытается перейти, введет на поддельный сайт. Но они не гарантируют полную защиту от фишинга из-за их принципа работы.

фишинг, интернет, сайты, проблемы, современные технологии

Фишинг (от англ. **fishing** — рыбачить, выуживать) — это вид кибератаки, при которой злоумышленник пытается получить доступ к личной информации пользователя, например к логину и паролю от электронной почты или данным банковской карты.

Фишинг отличается от других видов хакерских атак тем, что мошенники активно манипулируют базовыми человеческими эмоциями, такими как любопытство и страх, а также используют информацию, которые смогли собрать из открытых источников о человеке.

Изучив статью [5] 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 рисунке 1.

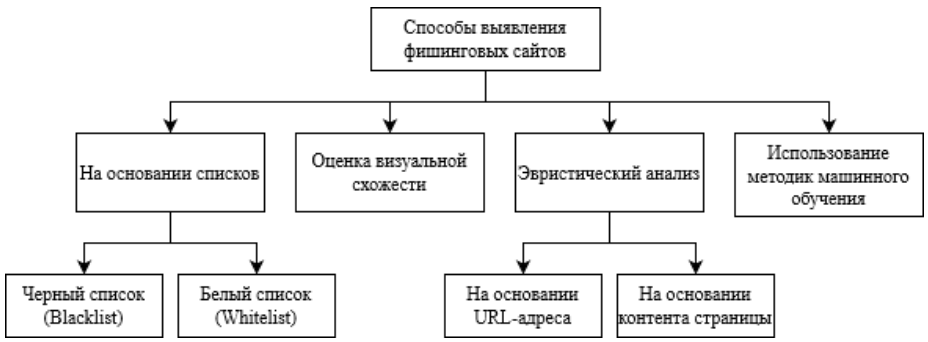


Рис. 1. Способы выявления фишинговых сайтов [3]

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. Рассмотрим методы выявление фишинговых сайтов.

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.

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[7].

Традиционно для обнаружения фишинговых атак использовались специальные методы на основе содержимого, URL-адреса веб-страницы и т. Д. В основном существует три режима обнаружения фишинга:

Контентно-ориентированный подход: анализирует текстовое содержимое страницы с использованием авторских прав, ссылок с нулевым нижним колонтитулом, нулевых ссылок основного HTML-кода, ссылок с максимальными частотными доменами. Используя только чистый алгоритм TF-IDF, 97% фишинговых веб-сайтов могут быть обнаружены с 6% ложных срабатываний.

Подход на основе URL: использует рейтинг страницы и объединяет его с другими показателями, полученными из URL на основе априорных знаний. Этот метод может обнаружить до 97% фишинговых сайтов.

Подход машинного обучения: используются различные модели машинного обучения, обученные таким функциям, как наличие в URL-адресе @, наличие перенаправления с двойной косой чертой, рейтинг страницы URL-адреса, количество внешних ссылок, встроенных на веб-страницу, и т. д. Этот подход может получить до 92% истинных положительных результатов и 0,4% ложных срабатываний.

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;
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;
8. Применить МО;
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 рисунке 2.

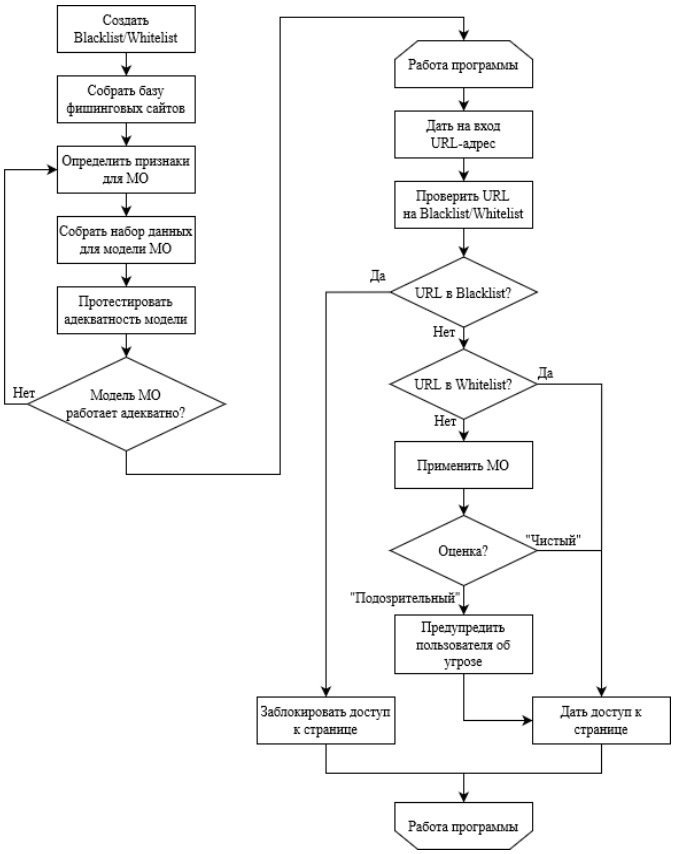


Рис. 2. Общая схема метода

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[4].

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 [9]. 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.

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.

Список использованной литературы:

1. Астахов А. М. Искусство управления информационными рисками. М. : Изд-во: ДМК Пресс, 2010. 312 с.

2. Информационная безопасность открытых систем. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников и др. М. : Огни**,** 2022**.** 536 с.

3. IT риски [Электронный ресурс]. URL: https://www.risk-academy.ru/portfolio-items/it-risks/. (дата обращения: 14.10.2023).

4. Медведовский И. Современные методы и средства анализа и контроля рисков информационных систем компаний [Электронный ресурс]. URL: http://citforum.ru/products/dsec/itrisk/. (дата обращения 05.10.2023).

5. Методологии управления ИТ-рисками [Электронный ресурс]. URL: https://www.osp.ru/os/2006/08/3584582. (дата обращения: 14.10.2023).

6. RiskWatch International: Risk Assesment Software [Электронный ресурс]. URL: https://riskwatch.com/. (дата обращения: 14.10.2023).

7. Муханмеджанова А. М. Методика оценки рисков информационной безопасности // Молодой ученый. 2017. N 22. С. 136-139.

Petrov P.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Synthesis of a method for detecting phishing sites.

The problem of identity theft via phishing sites is acute on the Internet right now. At the moment, there are tools that warn the user that the link he or she is trying to click on will lead to a fake site. But they do not guarantee full protection against phishing because of the way they work.

Key words: phishing, internet, websites, modern technology.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ СПЕЦИФИЧНЫХ ДЛЯ АСУ ТП ТАКТИК И ТЕХНИК, ИСПОЛЬЗУЕМЫХ ДЛЯ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

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

Автоматизированные системы управления технологическим процессом используются практически во всех сферах деятельности и большинство из них относятся к объектам критической информационной инфраструктуры, что делает их потенциальными целями злоумышленников для реализации компьютерных атак. Одной из основных задач автоматизированных систем управления технологическим процессом является автоматизация выполнения производственных процессов различной сложности. С появлением новых технологий и возможностей, возникают и новые угрозы безопасности информации, которые могут быть использованы для нарушения работы автоматизированной системы управления технологическим процессом и причинения имущественного ущерба владельцам таких систем.

автоматизированная система управления технологическим процессом, техника, тактика, угроза безопасности информации, вектор атаки

Введение.

Современный мир в значительной степени зависит от применения автоматизированных систем управления технологическим процессом (АСУ ТП), например, невозможно представить ни одно предприятие промышленной сферы без АСУ ТП – горнодобывающие комбинаты, нефтеперерабатывающие заводы, атомные электростанции, оборонно-промышленные предприятия и т.д [1]. Все эти объекты представляют интерес для террористических и экстремистских организаций, нацеленных на нанесение имущественного и репутационного ущерба владельцам таких объектов, а также ущерба государству в социальной, экономической и политической сферах. Уязвимыми объектами являются, как правило, не сами системы, а используемое прикладное программное обеспечение, устаревшее системное программное обеспечение, а также слабости применяемых мер защиты. Для реализации угроз безопасности информации злоумышленнику необходимо наличие нескольких факторов, таких как, существующий вектор атаки, тактика и техника для реализации сценария компьютерной атаки. В связи с особенностями построения и архитектуры АСУ ТП, можно выделить несколько специфичных тактик и техник реализации сценариев угроз безопасности информации из перечня типовых тактик и техник, представленного в Методическом документе ФСТЭК России [2].

Определение векторов атак на АСУ ТП.

Под вектором атаки подразумевается последовательность действий или средства для получения злоумышленником несанкционированного доступа к

защищённой информационной системе. Для усложнения потенциального вектора атаки необходимо логически и физически разделять корпоративную информационную систему (КИС) и технологическую сеть (ТП). При этом реализуются следующие требования: в КИС, как правило, организована отдельная подсеть автоматизированной системы управления производством (АСУП), где агрегируются и обрабатываются данные, полученные от компонентов АСУ ТП, между КИС и ТП применяется шлюз, который обеспечивает однонаправленную передачу данных из ТП в КИС, компоненты АСУ ТП не должны быть доступны из внешних сетей, в том числе из КИС, а управление технологическим процессом возможно только в пределах ТП с автоматизированных рабочих мест операторов и инженеров АСУ ТП. Ниже представлены основные векторы атак на АСУ ТП:

– Физический доступ: злоумышленник получает физический доступ к системе, например, путем взлома замков или проникновения в помещение, где находится система.

– Социальная инженерия: злоумышленник манипулирует людьми, чтобы получить доступ к системе или конфиденциальной информации. Это может быть достигнуто посредством обмана, угрозы или другими методами манипуляции.

– Вредоносное программное обеспечение: злоумышленник создает и распространяет вредоносное программное обеспечение, которое может использоваться для сбора информации, изменения настроек системы или причинения другого вреда. Например, громкая компьютерная атака на иранские ядерные объекты с использованием червя Stuxnet [3].

– Сетевые атаки: злоумышленник пытается проникнуть в сеть АСУ ТП с целью получения доступа к системе или уничтожения информации. Это может быть достигнуто через перехват сетевого трафика (аутентификационных данных легитимных пользователей), использование уязвимостей в сетевых протоколах или внедрение вредоносного программного обеспечения.

Типовая схема атаки на ТП предполагает следующие шаги:

1. Получение и повышений привилегий в операционной системе на узлах КИС: В случае отсутствия привилегий в КИС, то есть атака по типу внешнего нарушителя, злоумышленнику необходимо получить доступ к корпоративной сети. Для этого можно использовать, гостевой Wi-Fi или получить доступ посредством внешней сети – «Интернет». После получения доступа к КИС основной задачей нарушителя является получение и повышение локальных привилегий на серверах и рабочих станциях работников, а также проведение разведки с целью выяснения топологии сети, информации об используемых устройствах и ПО. В случае наличия физического доступа злоумышленника к КИС сразу проводится этап разведки.

2. Развитие атаки и закрепление в КИС: С целью закрепления в КИС после получения максимальных локальных привилегий на одном или

нескольких узлах, нарушителю необходимо развить атаку на другие доступные ресурсы в сети и выявить устройства, с которых возможно осуществить доступ к ТП. Развитие атаки в корпоративной сети осуществляется с использованием уязвимостей ПО, ОС и веб-приложений, недостатков сегментации сетей и т.п. Кроме того, может использоваться информация, полученная с общедоступных файловых хранилищ (например, учетные данные или конфигурационные файлы оборудования). Целью нарушителя являются получение максимальных привилегий в домене и выявление точек проникновения в ТП, сбор информации. На рис. 1 представлены наиболее распространенные уязвимости сети КИС промышленных предприятий [4].

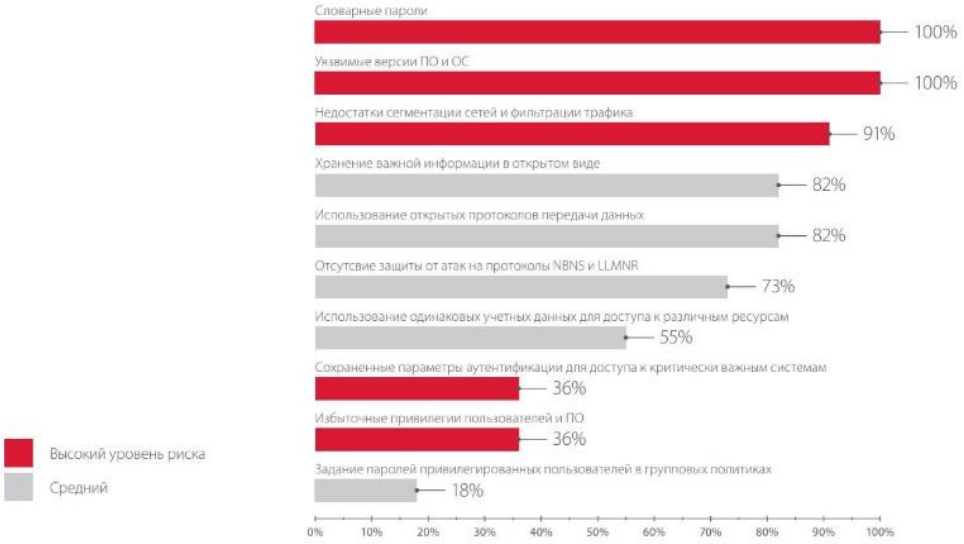


Рис. 28. Топ-10 уязвимостей КИС

3. Получение доступа к критически важным системам и развитие атаки в ТП: Результатом второго этапа является получение привилегий администратора домена и множества учетных записей других привилегированных пользователей. На данном этапе нарушитель уже обладает знаниями о процессах в компании, используемых системах, а также другой информацией, которая может быть использована для проникновения в ТП.

Реализация каждого этапа может проводится различными методами, однако стоит понимать, что нарушитель будет действовать максимально эффективно и незаметно. На рис. 2 представлена цепочка Kill Chain, то есть предположительная последовательность действий злоумышленника для реализации атаки типа шифрование инфраструктуры.

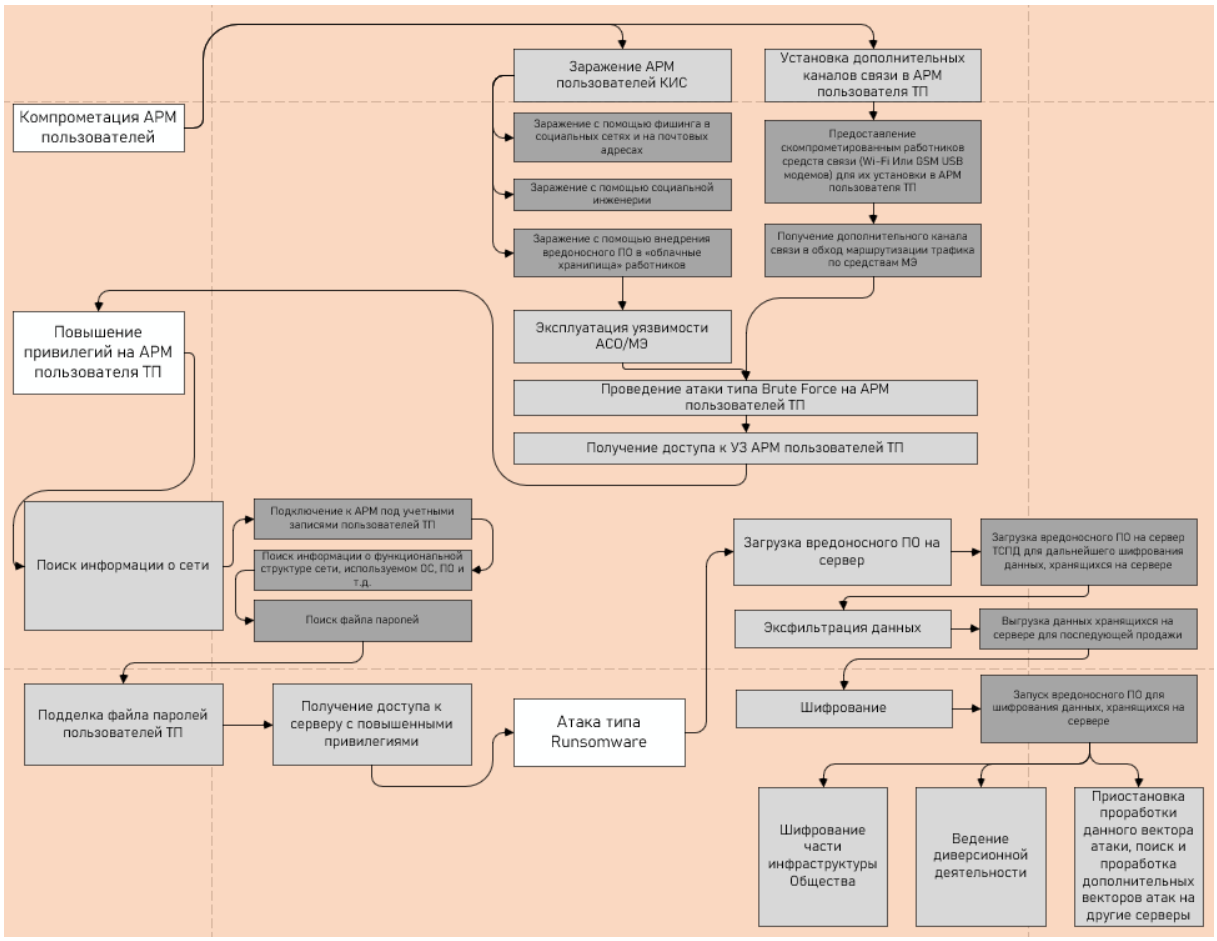


Рис. 29. Kill Chain для атаки типа шифрование инфраструктуры

Определение специфичных для АСУ ТП тактик и техник.

После рассмотрения наиболее возможных векторов атак на АСУ ТП был проанализирован перечень тактик и техник, используемых для реализации угроз безопасности информации, представленный ФСТЭК России. В процессе анализа из 10 возможных тактик и 145 соответствующих техник было выявлено 8 техник, применение которых возможно только в отношении АСУ ТП. Выявленные техники представлены ниже.

– Т.1.18: Сбор и анализ данных о прошивках устройств, количестве и подключении этих устройств, используемых промышленных протоколах для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в АСУ ТП, в том числе на критически важных объектах;

– Т1.19: Сбор и анализ специфических для отрасли или типа предприятия характеристик технологического процесса для получения информации о технологических установках, системах и ПО на предприятиях в АСУ ТП, в том числе на критически важных объектах;

– Т1.20: Сбор и анализ специфических для отрасли или типа предприятия характеристик технологического процесса для получения информации о технологических установках, системах и ПО на предприятиях в АСУ ТП, в том числе на критически важных объектах;

– T7.5: Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности АСУ ТП и управляемого (контролируемого) объекта и (или) процесса;

– T10.12: Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или нарушения функций управления, в том числе на АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов;

– T10.13: Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или нарушения функций управления, в том числе на АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов;

– T10.14: Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности, в том числе критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов;

– T10.15Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности, в том числе критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов.

Заключение.

Таким образом, были определены специфичные для АСУ ТП техники, рассмотрение которых возможно только в отношении автоматизированных систем. Данный перечень техник позволит облегчить процесс моделирования угроз безопасности информации и определения векторов атак в отношении различных типов систем.

Список используемых источников:

1. Безопасность промышленных систем в цифрах [Электронный ресурс]. URL: https://filearchive.cnews.ru/doc/2012/06/scada.pdf (дата обращения: 22.10.2023).

2. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 05.02.2023 г., с. 65-83 [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 22.10.2023).

3. Статья TAdviser Червь Stuxnet [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B5%D1%80%D0%B2%D1%8C_Stuxnet (дата обращения 23.10.2023).

4. Статья Positive Technologies [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018/#%D0%92%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D1%8B%D0%B0%D1%82%D0%B0%D0%BA (дата обращения 23.10.2023)

Potomako D.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Automated process control systems are used in almost all areas of activity and most of them belong to critical information infrastructure facilities, which makes them potential targets for cyber attacks by cybercriminals. One of the main tasks of automated process control systems is the automation of production processes of varying complexity. With the advent of new technologies and capabilities, new threats to information security arise that can be used to disrupt the operation of an automated process control system and cause property damage to the owners of such systems.

Key words: automated process control system, technology, tactics, threat to information security, attack vector

УДК 004.056
ГРНТИ 81.93.29

РАЗРАБОТКА МОДЕЛИ ИНСАЙДЕРА И АЛГОРИТМОВ ИХ ОБНАРУЖЕНИЯ В КОМПЬЮТЕРНЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В. Д. Проничев, И. А. Ушаков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Защита информации в современных компьютерных сетях имеет важное значение в современном информационном мире. Внутренние нарушители, именуемыми инсайдерами, представляют серьезную и актуальную угрозу информационной безопасности в корпоративных средах. В данной статье проводится анализ статистики по актуальным за 2023 год киберугрозам, и дается обзор возможной политики информационной безопасности, а также алгоритма по обнаружению инсайдера. Кроме того, представлен план дальнейших исследований, который будет реализован в рамках магистерской диссертации.

инсайдеры, внутренний нарушитель, модель инсайдера, информационная безопасность, угроза безопасности

Современные атаки на российские организации, в том числе на объекты КИИ (критическая информационная инфраструктура), представляют собой серьезное и актуальное явление в области кибербезопасности. Россия, как страна с развитой информационной инфраструктурой и стратегическими компаниями, становится объектом интереса для различных злоумышленников, в том числе и внутренних нарушителей – инсайдеров.

По результатам исследования компании positive technologies количество инцидентов безопасности за 2 квартал 2023 увеличилось на 15% по сравнению с аналогичным периодом предыдущего года [1]. На рис. 1 показана сводная статистика по инцидентам в 2022 и 2023 годах по кварталам.

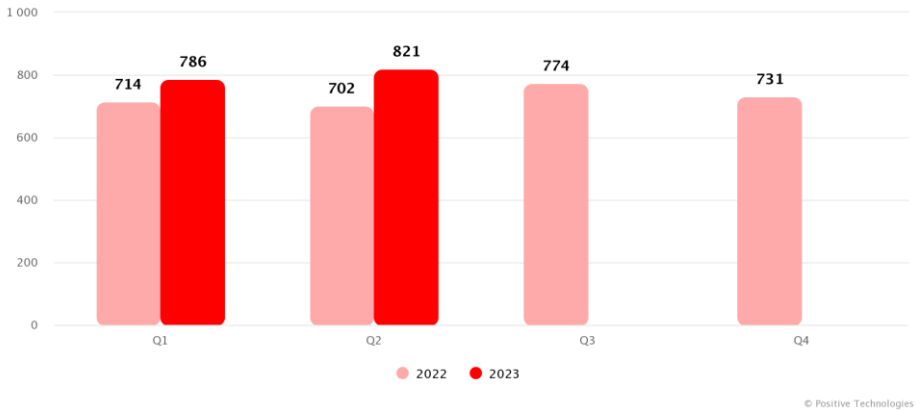


Рис. 1. Сводная статистика за 2022-2023 года [1]

Также стоит отметить отчет компании Gurucul и интернет-сообщества CybersecurityInside, в котором говорится, что внутренние угрозы вызывают наибольшую озабоченность в организациях всех типов, что подтверждает их же статистика – около 60% компаний подвергались хотя бы одной внутренней атаке за прошедший год [2].

Причины и мотивации для инсайдерских атак различны, ниже перечислены некоторые из них [3]:

- Финансовая выгода (получение денежных средств за передачу конфиденциальной информации, предлагаемые третьей стороной);
- Конфликт инсайдера с руководством;
- События в личной жизни инсайдера;
- Идеологические и политические причины (что стало наиболее актуально с 2022 года);
- Расширенные права доступа сотрудников к конфиденциальной информации;
- Социальная инженерия (неосведомлённость пользователей в сфере информационной безопасности ведет к росту числа непреднамеренных утечек данных);
- Пренебрежительная настройка политик безопасности инженерами по безопасности (что может повлечь к несанкционированному доступу к данным и последующую утечку конфиденциальной информации);
- и др.

С учетом вышеупомянутой статистики становится очевидной неотложная потребность в разработке/модернизации передовых методов обнаружения и защиты организаций от внутренних нарушителей. Эти меры кибербезопасности играют критически важную роль в обеспечении безопасности данных и непрерывного функционирования организаций.

Можно применять различные методы для выявления и классификации внутренних нарушителей, ниже представлены некоторые из них [4]:

- Использование различных технических решений, включая: SIEM (система управления безопасностью и событиями безопасности), DLP (система предотвращения утечек информации), IPS (система предотвращения вторжений), IDS (система обнаружения вторжений);
- UBA/UEBA-системы (технология, в основе которой лежит анализ поведения пользователей, используемых ими устройств и приложений, а также других элементов в информационной системе);
- Алгоритмы машинного обучения;
- Архитектуры на основе правил (rule-based);
- Решения на основе анализа Больших данных.

В рамках данной статьи будет рассмотрен алгоритм обнаружение инсайдеров в компьютерных сетях с использованием rule-based архитектуры [5].

Rule-based архитектура основывается на создании политики безопасности, исходя из собственного опыта работы в корпоративных средах, и мнений специалистов в области информационной безопасности.

Сама политика состоит из следующих элементов:

- Правило политики;
- Критерий соответствия правилу;
- Степень критичности.

Пример возможной политики безопасности для поведения пользователя в корпоративной сети представлен в таблице 1.

ТАБЛИЦА 1. Пример политики безопасности [5]

Правило политики	Критерий соответствия правилу	Степень критичности
Предотвращение перебора логина/пароля пользователя	Более 3 неудачных попыток аутентификации	Подозрительное действие
	Более 10 неудачных попыток аутентификации	Действие запрещено

Создание таких политик информационной безопасности нацелено на разработку алгоритмов обнаружения инсайдеров, способных с высокой точностью исходя из установленных правил и атрибутов пользовательского поведения идентифицировать внутренних нарушителей.

Расширение числа подобных политик имеет немаловажное значение, так как это позволит улучшить эффективность работы алгоритма по обнаружению инсайдера.

На рис. 2 показана простая блок-схема алгоритма обнаружения инсайдеров, основанная на rule-based архитектуре.

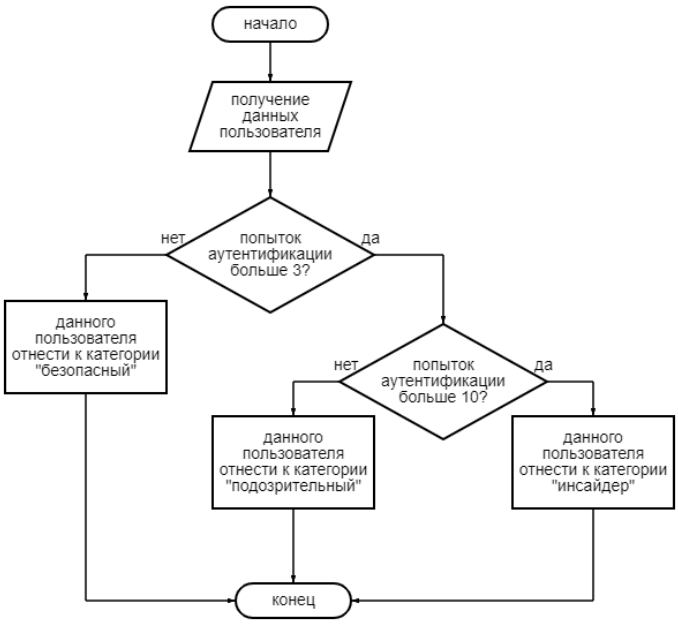


Рис. 2. Блок-схема алгоритма обнаружения инсайдера

Таким образом, в рамках данной статьи было приведено обоснование важности защиты от атак со стороны внутренний нарушителей или инсайдеров. В дальнейшей работе планируется следующее:

1. Расширение возможных атрибутов поведения пользователей для составления более детального профиля пользователя;
2. Расширение политик безопасности для rule-based архитектуры;
3. Разработка алгоритма обнаружения инсайдеров на основе ранее созданных политик безопасности и атрибутов пользователей;
4. Реализовать использование методов обработки Больших данных.

Список используемых источников:

1. Актуальные киберугрозы: 2 квартал 2023 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/#id3 (дата обращения 28.10.2023).
2. Более половины компаний столкнулись с инсайдерской угрозой за последний год [Электронный ресурс]. URL: https://it-ros.ru/news/368-soglasno-poslednim-dannym-bolee-poloviny-kompanii-stolknulis-s-insaiderskoi-ugrozoi-za-poslednii.html (дата обращения 28.10.2023).
3. Инсайдерская атака: понятие, виды и меры защиты [Электронный ресурс]. URL: https://polit-inform.ru/insaiderskaya-ataka-ponyatie-vidy-i-mery-zashhity/ (дата обращения 29.10.2023).
4. Щипцов Д. И., Федоров В. А. Классификация и способы обнаружения инсайдерских угроз в компьютерных сетях // Инновационные аспекты развития науки и техники. 2020. N 3. URL: https://cyberleninka.ru/article/n/klassifikatsiya-i-sposoby-obnaruzheniya-insayderskih-ugroz-v-kompyuternyh-setyah (дата обращения 30.10.2023).
5. Ушаков И. А. Обнаружение инсайдеров в компьютерных сетях на основе комбинированных экспертных правил, методов машинного обучения и обработки больших данных: автореф. дис. ... к-та техн. наук : 05.13.19 / Ушаков Игорь Александрович. СПб., 2020. 215 с.

Pronichev V., Ushakov I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development of an insider model and algorithms for their detection in computer networks. Information protection in modern computer networks is of great importance in today's information world. Insider intruders, referred to as insiders, pose a serious and urgent threat to information security in corporate environments. This paper analyzes the statistics of current cyber threats for the year 2023 and provides an overview of a possible information security policy as well as an algorithm to detect an insider. In addition, a plan for further research is presented, which will be implemented as part of a master's thesis.

Key words: insiders, insider intruder, insider model, information security, security threat.

УДК 004.056.55
ГРНТИ 81.93.29

АНАЛИЗ ВОЗДЕЙСТВИЯ РАЗЛИЧНЫХ МЕТОДОВ ШИФРОВАНИЯ НА ПРОПУСКНУЮ СПОСОБНОСТЬ СЕТЕВОГО ТРАФИКА В ОБЛАЧНОЙ ИНФРАСТРУКТУРЕ

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

В работе приведены результаты экспериментального исследования различных методов шифрования сетевого трафика в объектах облачной инфраструктуры. В материале рассмотрено понятие облачных вычислений, описана необходимость шифрования трафика в облачной инфраструктуре и осуществлен обзор и сравнение методов шифрования и защиты трафика в облачной инфраструктуре.

компьютерная безопасность, шифрование, защита данных

Данная статья представляет результаты экспериментального исследования, посвященного воздействию различных методов шифрования на пропускную способность сетевого трафика в контексте облачной инфраструктуры. В эпоху нарастающей важности облачных вычислений и необходимости обеспечения конфиденциальности данных в облачной среде, выбор эффективных методов шифрования становится ключевым аспектом сетевой безопасности.

В рамках исследования были проведены эксперименты, охватывающие различные методы шифрования, включающее такие популярные протоколы, как Wireguard и IPsec. Анализ воздействия этих методов на пропускную способность сетевого трафика осуществлялся в разнообразных сценариях, специфичных для облачной инфраструктуры, и на различных типах сетевых соединений в облаке и не только.

Выбор Методов Шифрования:

1. Tinc позволяет выбирать различные алгоритмы шифрования для защиты данных внутри виртуальной частной сети. Основные алгоритмы, поддерживаемые Tinc, включают:

- AES (Advanced Encryption Standard): AES - это симметричный алгоритм шифрования, который обеспечивает высокий уровень безопасности и эффективность. Он может использоваться для шифрования трафика внутри сети Tinc.
- RSA (Rivest-Shamir-Adleman): RSA - это асимметричный алгоритм шифрования, используемый для аутентификации и обмена ключами. Tinc может использовать RSA для безопасной идентификации участников сети.
- HMAC (Hash-based Message Authentication Code): HMAC - это метод проверки целостности данных, который может быть использован для защиты от подмены данных внутри сети Tinc.

2. **IPsec** предоставляет разнообразные алгоритмы шифрования и аутентификации для обеспечения безопасности сетевой связи. Основные алгоритмы включают:

- DES (Data Encryption Standard): DES - это симметричный алгоритм, который был широко использован в прошлом, но сейчас считается устаревшим из-за своей уязвимости. Он все еще может быть поддерживаем IPsec для обратной совместимости.
- 3DES (Triple Data Encryption Standard): 3DES - это усиленная версия DES, которая предоставляет более надежное шифрование.
- AES: аналогично Tinc, IPsec поддерживает AES для обеспечения высокой безопасности и производительности.
- SHA (Secure Hash Algorithm): SHA - это алгоритм для вычисления хеш-кодов, используемый в IPsec для проверки целостности данных.
- IKE (Internet Key Exchange): IKE - это протокол для безопасного обмена ключами, который используется в IPsec.

3. WireGuard также предоставляет современные алгоритмы шифрования и аутентификации для обеспечения безопасности сети. Основные алгоритмы включают:

- Curve25519: Это алгоритм для обмена ключами в WireGuard, который предоставляет высокую стойкость к атакам и высокую производительность.
- ChaCha20: ChaCha20 - это симметричный алгоритм шифрования, который обеспечивает хорошую производительность и безопасность.
- Poly1305: Poly1305 - это алгоритм для проверки целостности данных, который используется в WireGuard для защиты данных от изменений во время передачи.

Экспериментальная настройка

Была настроена сеть, включающую несколько узлов, и были проведены ряд экспериментов, в которых каждый метод шифрования использовался в разных сценариях. В каждом случае измерялась пропускная способность сравнивались результаты. Принципиальная схема тестовой инфраструктуры изображена на рис. 1.

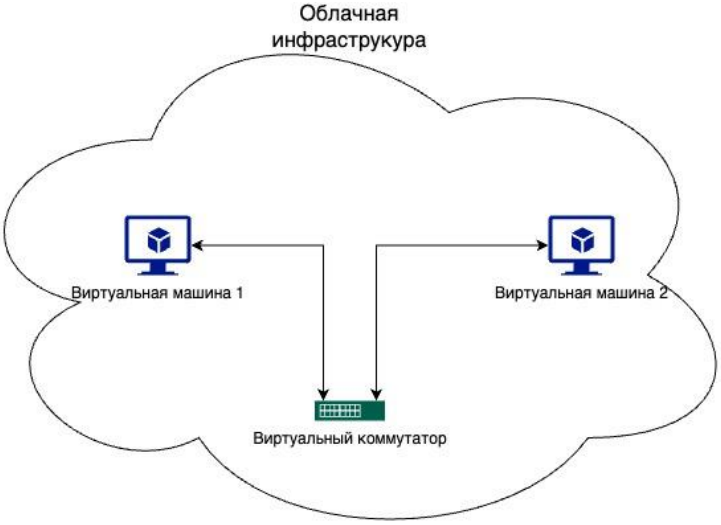


Рис. 1. Принципиальная схема тестовой инфраструктуры

Было произведено несколько тестов с разными размерами буфферов, а также с разным количеством потоков.

Результаты и Обсуждение

На рис. 2 представлены результаты тестирования пропускной способности в однопоточном режиме. Где wire_1 – Протокол wireguard, ipsec_1 – Протокол ipsec, hh_1 – протокол tinc, bare_1 – режим работы без шифрования.

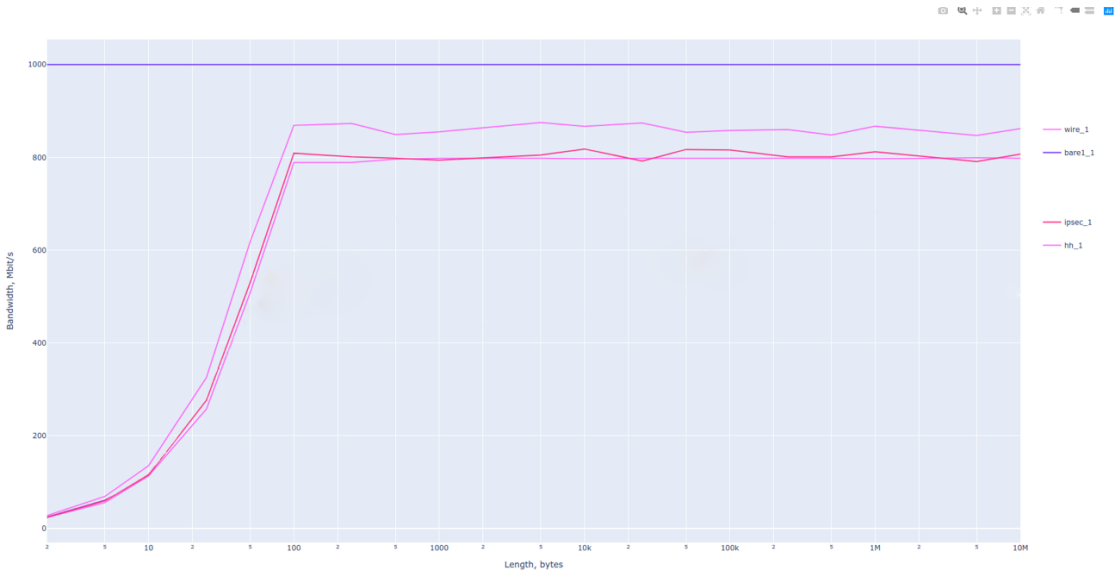


Рис. 2. Результаты тестирования в однопоточном режиме

На рис. 3 представлены результаты тестирования пропускной способности в режиме 25 потоков. Где wire_25 и wire2_25 – Протокол wireguard, ipsec_25 – Протокол ipsec, hh_25 – протокол tinc, bare_25 – режим работы без шифрования.

Рис. 3. Результаты тестирования в однопоточном режиме

Результаты показали, что каждый метод шифрования оказывает различное воздействие на пропускную способность сетевого трафика. Tinc, хотя и обеспечивает надежное шифрование, имеет наименьшее воздействие на пропускную способность, что делает его подходящим для сценариев с ограниченной пропускной способностью.

IPsec и WireGuard также предоставляют высокий уровень безопасности, но могут оказывать более заметное воздействие на пропускную способность. Однако, WireGuard демонстрировал худшую производительность по сравнению с IPsec в режиме многопоточности, что может быть важным фактором в контексте современных высокоскоростных сетей.

В данной статье представлены результаты экспериментального исследования, сравнивающего воздействие трех различных методов шифрования на пропускную способность сетевого трафика. Результаты могут служить рекомендациями для инженеров и администраторов, помогая им выбрать наилучший метод шифрования в зависимости от конкретных требований к безопасности и производительности в их сетевых средах. Данное исследование подчеркивает важность учета как безопасности, так и производительности при выборе методов шифрования в сетевых системах.

Список используемых источников:

1. Абелдинов Д. А., Абрамова Е. В., Митрофанов А. И. Проблемы и методы обеспечения безопасности в облачных вычислениях // Актуальные проблемы административного, банковского, медицинского и экологического права. 2017. N 8. С. 150-157.

2. Бекетов А. Н., Казаринов Е. В. Сравнительный анализ протоколов шифрования в облачных вычислениях // Вестник Новосибирского государственного университета. Информатика, телекоммуникации и управление. 2019. N 19 (4). С. 33-42.

3. Забродин А. В., Михайлов В. П. Исследование применения технологии VPN в облачных вычислениях // Вестник Нижегородского университета имени Н. И. Лобачевского. 2015. N 3. С. 147-152.

4. Перетятко Ю. А., Казакова О. В. Применение протоколов VPN в облачных вычислениях // Научные исследования и разработки в современном мире. 2018. N 1. С. 31-37.

5. Родионов П. В. Методы шифрования данных в облачных хранилищах // Современные проблемы науки и образования. 2017. N 2. С. 216.

6. Семенов, А.Г., & Лазарев, М.В. (2017). Сравнительный анализ методов шифрования в облачных вычислениях. Вестник Московского университета, (3), 16-21.

7. Пестов И. Е. Атаки на облачную инфраструктуру // Инновационные решения социальных, экономических и технологических проблем современного общества : материалы круглого стола со всерос. и междунар. участием, Москва, 15–16 дек., 2021 г. Т. 8. М. : ООО «КОНВЕРТ», 2021. С. 113-115.

8. Шемякин С. Н., Пестов И. Е., Федоров П. О., Кошелева С. А. Использование теории графов для моделирования безопасности облачных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. N 2. С. 31-35. DOI 10.46418/2079-8199_2021_2_5.

9. Пестов И. Е., Смуров И. А., Федоров П. О., Федорова Е. С. Мониторинг информации инстансов облачной инфраструктуры // Подготовка профессиональных кадров в магистратуре для цифровой экономики : материалы Всерос. научно-технич. и

научно-методич. конф., магистрантов и их руководителей, Санкт-Петербург, 06–08 дек. 2022 г. СПб. : СПбГУТ, 2023. С. 216-220.

10. Бугрова Е. С., Пестов И. Е., Тарабанов И. Ф., Швидкий А. А. Анализ методов повышения отказоустойчивости облачной инфраструктуры средствами мониторинга и предсказания состояния компонентов // Актуальные проблемы инфотелекоммуникаций в науке и образовании : XI Междунар. научно-технич.я и научно-методич. конф., Санкт-Петербург, 15–16 фев. 2022 г. Т. 1. СПб. : СПбГУТ, 2022. С. 188-192.

11. Штеренберг С. И., Пестов И. Е., Казаков Д. Б., Ильин М. В. Основные рекомендации для организаций перед переносом своих данных в облачную среду. Анализ эффективности на примере ЗКУ РВС // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. – N 1. С. 26-36. – DOI 10.46418/2079-8199_2022_1_4.

12. Сахаров Д. В., Левин М. В., Фостач Е. С., Виткова Л. А. Исследование механизмов обеспечения защищенного доступа к данным, размещенным в облачной инфраструктуре // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. N 2. С. 40-46.

13. Красов А. В. Проблемы обеспечения безопасности облачных вычислений / А. В. Красов, М. В. Левин, Е. С. Фостач // Информационная безопасность регионов России (ИБРР-2017) : материалы конференции, Санкт-Петербург, 01–03 нояб. 2017 г. СПб. : Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2017. С. 520-522.

Romaniuk E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Analysis of the impact of various encryption methods on the network traffic capacity in cloud infrastructure.

The paper presents the results of an experimental study of various methods of encrypting network traffic in cloud infrastructure objects. The material covers the concept of cloud computing, describes the necessity of traffic encryption in cloud infrastructure, and provides an overview and comparison of encryption and traffic protection methods in cloud infrastructure.

Key words: Computer security, encryption, data protection.

УДК 004.75
ГРНТИ 20.15.05

БУДУЩЕЕ КИБЕРБЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

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

С постоянным развитием технологии и увеличением объемов цифровых данных, кибербезопасность стала ключевой областью для предприятий и организаций по всему миру. Атаки становятся все более сложными и высокотехнологичными, и необходимы новые методы для выявления и анализа потенциальных рисков. В этой статье проводится исследование, как нейронные сети могут быть использованы для обеспечения безопасности, предостерегая организации от потенциальных угроз и атак.

нейронная сеть, Информационная безопасность, Кибербезопасность, Автоматизация, Машинное обучение.

Искусственная нейронная сеть (ИНС) — математическая модель, а также её программная или аппаратная реализация, построенная по принципу организации и функционирования биологических нейронных сетей — сетей нервных клеток живого организма. Она состоит из большого количества взаимосвязанных и взаимодействующих искусственных нейронов, которые обрабатывают и передают информацию между собой.

Нейронные сети предоставляют ряд преимуществ в области кибербезопасности, делая их мощным инструментом для выявления и предотвращения киберугроз.

- Обнаружение аномалий:

Нейронные сети способны анализировать нормальное поведение системы и обнаруживать аномалии. Это позволяет выявлять нестандартные или подозрительные действия, которые могут указывать на потенциальные угрозы[1].

- Способность адаптироваться:

Нейронные сети могут обучаться на опыте предыдущих поколений. Они способны адаптироваться к новым методам атак и угрозам, что делает их более эффективными в борьбе с эволюцией киберугроз.

- Масштабируемость:

Нейронные сети могут обрабатывать большие объемы данных в реальном времени. Это особенно важно в контексте кибербезопасности, где необходимо быстро реагировать на угрозы.

- Снижение ложных срабатываний:

С применением сложных алгоритмов и обучения на больших данных, нейронные сети могут снижать количество ложных срабатываний.

- Способность к комплексному анализу данных:

Нейронные сети могут анализировать множество различных видов данных, включая текст, изображения, временные ряды и даже аудио. Это позволяет обнаруживать угрозы, которые могут быть скрыты в разных источниках данных[2].

- Автоматизация:

Нейронные сети позволяют создавать автоматизированные системы безопасности, которые могут реагировать на атаки и предпринимать меры для их предотвращения или уменьшения ущерба без участия человека.

- Улучшение реакции на инциденты:

Путем анализа данных и создания предсказательных моделей нейронные сети могут помочь предсказать, какие инциденты могут произойти в будущем, что позволяет организациям быть готовыми к ним[3].

Область информационной безопасности постоянно развивается, и ожидается, что будут внедрены новые методы и технологии. Вот некоторые из них:

- Обучение с подкреплением для кибербезопасности:

Обучение с подкреплением - это метод машинного обучения, в котором сеть обучается принимать решения, чтобы максимизировать эффективность. Искусственные нейросети могут быть обучены для принятия решений в режиме реального времени, чтобы предотвращать атаки и максимизировать защиту.

- Генеративные адверсариальные сети (GANs):

GANs могут быть использованы для создания синтетических данных, которые могут быть использованы для обучения нейронных сетей на случайных угрозах и атаках. Это позволяет улучшить способность сетей обнаруживать новые угрозы, которые ранее не были заранее известными.

- Автоматическое обучение и настройка гиперпараметров:

Методы автоматического обучения и настройки гиперпараметров могут значительно упростить процесс развертывания и оптимизации нейронных сетей в системах кибербезопасности[4].

- Дифференциальное обучение нейронных сетей:

Этот метод позволяет обучать нейронные сети с учетом конфиденциальных данных, минимизируя риск утечки информации. Это особенно важно в случаях, когда необходимо защитить конфиденциальные данные при обучении.

- Использование квантовых вычислений:

Квантовые компьютеры могут предоставить значительный выигрыш в производительности при решении сложных задач в области криптографии. Нейронные сети также могут быть оптимизированы для выполнения на квантовых вычислителях.

- Улучшенные техники передачи знаний:

Техники передачи знаний позволяют обученным моделям передавать свои знания другим моделям, что особенно полезно в контексте безопасности, где не всегда есть достаточно данных для обучения.

- Интеграция с блокчейн-технологиями:

Блокчейн может использоваться для обеспечения прозрачности и подтверждения целостности данных и алгоритмов, используемых в системах на основе нейронных сетей.

- Интеллектуальные контракты для автоматизации реакции на инциденты:

С помощью интеллектуальных контрактов на блокчейне можно автоматизировать реакцию на киберинциденты, включая блокировку доступа к уязвимым ресурсам.

Использование нейронных сетей позволяет развивать способы анализа и предотвращения киберугроз, делая их более интеллектуальными, адаптивными и эффективными[5].

Следует отметить, что с развитием технологий, угрозы также становятся более сложными. Это означает, что система должна оставаться на пути развития и постоянно совершенствовать методы анализа и обнаружения[6]. Также стоит обратить внимание на то, что несмотря на множество преимуществ, нейронные сети имеют проблемы с ложными срабатываниями и неоднозначностью, для решения которых требуется усовершенствование методов обучения и анализа[7][8].

Будущее безопасности будет зависеть от совместных усилий специалистов в области информационной безопасности, исследователей и разработчиков, работающих над созданием более интеллектуальных и надежных систем, что позволит появиться перспективам для развития новых методов, инструментов и технологий, которые помогут защитить цифровой мир и обеспечить безопасность информации в будущем.

Список используемых источников:

1. Сахаров Д. В., Гельфанд А. М., Казанцев А. А., Пестов И. Е. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IoT-сети // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2020. N 2. С. 86-94. EDN DLMENT.

2. Krasov A. A., Pestov I. E., Gelfand A. M. [et al.]. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network // ACM International Conference Proceeding Series : 4, St. Petersburg, 26–27 нояб. 2020 г. St. Petersburg, 2020. P. 3442605. DOI 10.1145/3440749.3442605. EDN JOYJIQ.

3. Бугрова Е. С., Пестов И. Е, Тарабанов И. Ф., Швидкий А. А. Анализ методов повышения отказоустойчивости облачной инфраструктуры средствами мониторинга и предсказания состояния компонентов // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы XI Междунар. науч.-технич. и науч.-методич. конф., Санкт-Петербург, 15–16 фев. 2022 года. Том 1. СПб. : СПбГУТ, 2022. С. 188-192. EDN VHRJMG.

4. Цветков А. Ю. Анализ существующих методов атак типа переполнения буфера на операционные системы семейства Microsoft // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VIII Междунар. науч.-технич. и науч.-методич. конф., Санкт-Петербург, 27–28 фев. 2019 г. Том 1. СПб. : СПбГУТ, 2019. С. 751-756. EDN XATXVB.

5. Цветков А. Ю., Рузманов Е. Ю. Рассмотрение тестирования на проникновение в задачах защиты информации // Приоритетные направления инновационной деятельности в промышленности : материалы XI междунар. науч. конф., Казань, 29–30 нояб. 2021 года. Том Часть 2. Казань : ООО "КОНВЕРТ", 2021. С. 55-56. EDN ZVTTVO.

6. Катасонов А. И., ЦветковА. Ю. Анализ механизмов разграничения доступа в системах специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы IX Междунар. науч.-технич. и науч.-методич. конф., Санкт-Петербург, 26-27 фев. 2020 г. Том 1. СПб. : СПбГУТ, 2020. С. 563-568. EDN VDWJMM.

7. Штеренберг С. И., Красов А. В, Цветков А. Ю. Компьютерные вирусы. СПб. : СПбГУТ, 2015. 63 с. EDN CMMEML.

8. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства GNU LINUX // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 2. С. 50-56. DOI 10.46418/2079-8199_2020_2_8. EDN EUMWWI.

Rudenko S.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

The future of cybersecurity using neural networks.

With the constant development of technology and the increasing volume of digital data, cybersecurity has become a key area for businesses and organizations around the world. Attacks are becoming more complex and high-tech, and new methods are needed to identify and analyze potential risks. This article investigates how neural networks can be used to ensure security, warning organizations against potential threats and attacks.

Key words: Neural network, Information Security, Cybersecurity, Automation, Machine Learning.

УДК 004.056.53
ГРНТИ 81.93.29

АНАЛИЗ МЕТОДОВ АУТЕНТИФИКАЦИИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Г. А. Самохин
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В современном цифровом мире, где информация играет ключевую роль, обеспечение безопасности данных становится все более важным. Аутентификация, процесс проверки подлинности пользователей и устройств, является одним из основных механизмов защиты информационных систем. Однако, с развитием технологий и появлением новых угроз, необходимо постоянно анализировать и оценивать существующие методы аутентификации, чтобы обеспечить эффективную защиту данных.

аутентификация, проверка, биометрия, безопасность

Информационная безопасность является одной из наиболее важных задач в современном мире, особенно в контексте все большего использования цифровых технологий и передачи данных через сети. Одним из ключевых аспектов обеспечения безопасности информации является аутентификация, процесс проверки подлинности пользователей и устройств, чтобы предотвратить несанкционированный доступ к конфиденциальным данным. Сегодня эргономика и оценка рисков не являются единственными метриками, помогающими в выборе методов аутентификации и реализации их. Сейчас законодательное регулирование со стороны государственных нормативных актов и отраслевых стандартов становится основополагающим фактором в этом процессе.

Проблемы методов аутентификации в информационной безопасности включают уязвимость надежности паролей, утерю или кражу аппаратных устройств, используемых для аутентификации, возможность социальной инженерии, при которой злоумышленники могут обмануть пользователей и получить доступ к их учетным записям, а также ограниченную применимость некоторых методов, которые могут быть неудобными или неприменимыми в определенных ситуациях. Эти проблемы требуют постоянного совершенствования и разработки новых методов аутентификации, чтобы обеспечить более надежную защиту информации.

Фактор аутентификации – это, обобщенно говоря, атрибут, по которому удостоверяется подлинность пользователя. В роли фактора могут выступать материальные объекты (аппаратные устройства, части тела) или нематериальные сущности (кодовые слова, файлы). Простейший случай аутентификации – использование одного фактора.[3]

Парольная аутентификация - это широко распространенный метод проверки подлинности в области информационной безопасности, который основывается на использовании уникального пароля, который пользователь

вводит для получения доступа к системе или ресурсам. Она проста в использовании и низкая по затратам, но может быть уязвима из-за слабых паролей или повторного их использования. Легкие пароли легко запомнить, но вредитель может его подобрать с помощью специального программного обеспечения. Рекомендуется использовать длинные и сложные пароли, а также регулярно их менять. Концепция временных или одноразовых паролей при каждом входе в систему может заменить постоянные пароли. В таком случае нам не надо где-то хранить или запоминать кодовое слово. Пользователю нужно иметь с собой некоторое дополнительное средство для получения пароля, как телефон или почта. Дополнительные меры безопасности, такие как двухфакторная аутентификация, могут усилить безопасность парольной аутентификации.

Цифровой сертификат — это электронный документ, который подтверждает принадлежность определенного открытого ключа шифрования конкретному пользователю или сети. Мы часто взаимодействуем с цифровыми сертификатами при использовании защищенных соединений с ресурсами в Интернете по протоколу SSL. Так пользователь может быть уверен, что подключается к настоящему сайту, а не к копии от некоторого злоумышленника. Технология цифровых сертификатов лежит в работе электронных цифровых подписей. Открытый ключ проверяет подпись, а сертификат указывает на достоверность пользователя. Электронные цифровые подписи тоже являются средством аутентификации, потому что они подтверждают личность определенного автора документа.

Биометрическая аутентификация представляет собой удобную и эффективную систему проверки, которая идентифицирует пользователей на основе их уникальных анатомических особенностей и поведенческих черт. Методы данного вида анализа надежней базовых парольных методов, где пароли могут быть легко утеряны или украдены, потому что в качестве идентификации используют человеческие параметры пользователя. Различают статические и динамические методы. Первые методы основаны на физиологических характеристиках человека, которые остаются неизменными на протяжении всей жизни и не могут быть потеряны, украдены или скопированы. Эти характеристики включают отпечаток пальца, радужку и сетчатку глаза, термограмму лица и геометрию руки. Динамические методы, такие как голос и почерк, основаны на поведенческих характеристиках людей. Биометрическая аутентификация работает путем сравнения эталонного и предъявленного образца с некоторой погрешностью, которая заранее вычисляется и устанавливается для достижения оптимального баланса между коэффициентом ложного принятия и коэффициентом ложного отказа. Эти две характеристика должны быть минимальными. Серьезное средство биометрической аутентификации должно позволять настроить коэффициент ложного принятия до величин порядка 0,01–0,001 % при коэффициенте ложного отказа до 3–5 %. [2]

Еще одно распространенное специальное устройство для аутентификации пользователей - аппаратный токен. В элементарном случае, токен может сразу служить удостоверением, которое пользователь имеет при себе для подтверждения в системе, например, подключая некоторый носитель информации к компьютеру или поднеся специальную карту к сканнеру. Технологический прогресс предоставляет возможность на программном уровне усовершенствовать концепцию карт для подтверждения в удобной виртуальной форме. Однако, физические карты или токены являются средством удостоверения личности, пока внутри аутентификация работает на основе временных паролей или криптографических шифров. Опасность такого метода лежит в том, что злоумышленник может украсть предмет подтверждения личности и система никак это не отследит.

Концепция многофакторной аутентификации заключается в использовании нескольких различных факторов для повышения безопасности. Чаще всего применяется двухфакторная аутентификация, где пользователи должны предоставить как постоянный пароль, так и одноразовый код. Например, система, основанная на аппаратных ключах, может быть усилена путем добавления парольного механизма, где злоумышленникам будет сложно получить доступ без обоих факторов. Таким образом, многофакторная аутентификация обеспечивает более надежную защиту, устраняя недостатки отдельных факторов и требуя комбинации различных ключевых рисков.

Методы аутентификации нужны для защиты от возможного несанкционированного доступа к конфиденциальным данным и от кибератак хакеров. Каждый из этих методов имеет свои преимущества и недостатки, а также требует более детального рассмотрения. Парольные системы просты в создании, но подвержены рискам утери, кражи или взлома базы кодовых слов. Многофакторная аутентификация и аутентификация на основе сертификатов предоставляют дополнительные уровни безопасности, но могут быть неудобными для пользователей. В целом, комбинация различных методов аутентификации, таких как двухфакторная аутентификация или использование биометрических данных в сочетании с паролями, может обеспечить более надежную защиту информации. Однако, важно помнить, что безопасность информации является непрерывным процессом, требующим постоянного обновления и адаптации к новым угрозам.

Список используемых источников:

1. Обзор способов и протоколов аутентификации в веб-приложениях [Электронный ресурс]. URL: https://habr.com/ru/companies/dataart/articles/262817/ (дата обращения: 13.10.2023).

2. Мартынова Л. Е. Исследование и сравнительный анализ методов аутентификации / Л. Е. Мартынова, М. Ю. Умницын, К. Е. Назарова, И. П. Пересыпкин [Электронный ресурс] // Молодой ученый. 2016. N 19 (123). С. 90-93. URL: https://moluch.ru/archive/123/34077/ (дата обращения: 22.10.2023).

3. Системы и методы аутентификации пользователей [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/overview-of-user-authentication-systems-and-methods (дата обращения: 13.10.2023).

Samokhin G.

Saint-Petersburg State University of Industrial Technologies and Design

Analysis of authentication methods in information security.
In today's digital world, where information plays a key role, ensuring data security is becoming increasingly important. Authentication, the process of verifying the authenticity of users and devices, is one of the main mechanisms for protecting information systems. However, with the development of technology and the emergence of new threats, it is necessary to constantly analyze and evaluate existing authentication methods to ensure effective data protection.

Key words: Authentication, verification, biometrics, security.

УДК 004.056.53
ГРНТИ 81.93.29

МЕТОДИКИ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ В СЕТЯХ УМНОГО ДОМА

И. А. Саразова, А. А. Чахир
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В современном мире люди всё больше стремятся к упрощению, автоматизации бытовой жизни. А где упрощение для пользователя, там же ухудшение, ослабление и недоработка составляющей безопасности.

методики обнаружения уязвимостей, безопасность домашних сетей, системы умного дома, несанкционированный доступ

Умные дома становятся все более популярными и широко используемыми. Они предлагают удобство, эффективность и повышенный уровень комфорта для проживания. Однако, вместе с растущей популярностью умных домов возникает серьезная проблема безопасности. С сетевым взаимодействием между устройствами и хранилищами данных внутри умного дома возникает риск кибератак и утечки персональных данных.

Целью данной статьи является анализ методик обнаружения уязвимостей в сетях умного дома для выявления потенциальных недостатков и брешей в безопасности, а также рассмотрение возможных угроз, связанных с коммуникацией и обменом информацией между установленными устройствами. В рамках обзора будут изучены уже известные случаи атак и эксплойтов, анализ их потенциальных последствий для безопасности пользователей. Будут рассмотрены преимущества и ограничения методики, а также возможные пути ее развития и улучшения.

Результаты исследования могут быть использованы специалистами по кибербезопасности для повышения уровня безопасности умных домов и общества в целом.

В системах умного дома могут использоваться различные сетевые протоколы, в зависимости от конкретных устройств и их производителей. Наиболее распространенной и популярной в сетях умного дома технологией является Wi-Fi (беспроводная связь по стандарту IEEE 802.11). Wi-fi позволяет подключать устройства к домашней беспроводной сети для передачи данных и управления ими.

Также не стоит забывать про Bluetooth, который используется для беспроводной связи между устройствами в непосредственной близости друг от друга. В умных домах Bluetooth может использоваться, например, для соединения смартфона с умными замками или датчиками при приближении пользователя, а также с мобильной или компьютерной периферией

ZigBee. Протокол ZigBee[1] используется для создания сетей малого радиуса действия (например, внутри дома) с низким энергопотреблением. Он часто применяется для связи между устройствами умного дома, такими как датчики, освещение, умные розетки и др, которые не подключаются напрямую к Wi-Fi-роутеру, а используют Bluetooth для подключения к управляющему хабу.

Аналогично Zigbee, протокол Z-Wave предназначен для создания беспроводной сети малого радиуса действия в умных домах. Он также обладает низким энергопотреблением и поддерживает взаимодействие различных устройств [2].

Протокол Ethernet (стандарт IEEE 802.3) используется для проводного подключения устройств в домашней сети. В умных домах Ethernet может использоваться для подключения маршрутизаторов и других сетевых устройств, в том числе, например, камер с PoE-подключением.

Кроме того, в системах умного дома также могут использоваться другие протоколы, такие как NFC (Near Field Communication) для бесконтактного взаимодействия, MQTT (Message Queuing Telemetry Transport) для передачи сообщений между устройствами и др. Выбор конкретных протоколов зависит от функций устройств, их совместимости и требований пользователей.

Начнём с обзора существующих уязвимостей в сетях умного дома.

Примеры известных уязвимостей включают: недостаточную аутентификацию устройств, уязвимости протоколов связи, недостатки защиты приложений и множество других уязвимостей, которые могут быть использованы злоумышленниками для несанкционированного доступа и контроля над системой умного дома. В целом, существует два основных типа уязвимости: избыточные разрешения и небезопасные сообщения.

Существуют различные подходы к обнаружению уязвимостей в сетях умного дома:

- сканирование сети на наличие уязвимостей,
- анализ сетевого трафика с целью выявления аномалий,
- использование известных эксплойтов,
- применение методов социальной инженерии.

Это всегда актуальные направления обнаружения уязвимостей в любой системе, в том числе системах “Умный дом”. Рассмотрим каждый подробнее:

1. Автоматическое сканирование сети.

Данный подход включает использование специальных инструментов и программ для автоматического сканирования устройств с возможностями обнаружения открытых портов, анализа служебной информации (журналы, логи), проверки наличия определенного ПО и других тестах на безопасность. Примерами таких программ могут быть NMap, OpenVAS, Tenable Nessus, Goby и т.д.

2. Анализ сетевого трафика.

Данный подход основан на анализе потоков данных в сетях умного дома. Специализированные программы могут мониторить трафик и

обнаруживать аномалии или подозрительную активность, которая может указывать на наличие уязвимостей или попытки несанкционированного доступа. Это может включать анализ пакетов данных, проверку целостности и шифрования трафика. Для злоумышленника полезной информацией может стать отслеживание времени активности и бездействия пользователя, специфичность кадров, а также доступные неиспользуемые каналы. Примеры программ и утилит: Wireshark, Scapy.

3. Использование известных эксплойтов.

Один из важных подходов к обнаружению и устранению уязвимостей заключается в регулярном обновлении программного обеспечения всех устройств в умном доме. Производители выпускают обновления, которые включают патчи безопасности и исправления уязвимостей. Важно регулярно проверять наличие обновлений и устанавливать их, чтобы минимизировать риски. Для необновленного ПО злоумышленник может использовать уже известные эксплойты и сценарии, при которых атака может пройти быстро и почти незаметно. Злоумышленник может реализовать атаки типа Man-in-the-Middle, подслушивать жертву или получить доступ к определенной системе и ее содержимому [3]. Примеры программ: metasploit, Ettercap.

4. Обучение пользователей.

Пользователи умного дома должны быть грамотно просвещены о возможных угрозах и методах защиты. Обучение может включать информирование о возможных уязвимостях, использование надежных паролей, установку многофакторной аутентификации, ограничение доступа к устройствам и сети, а также обращение к надежным и проверенным источникам при покупке новых устройств умного дома.

Комбинация этих подходов к обнаружению уязвимостей в сетях умного дома позволяет снизить риски и защитить домашние сети и пользователей от потенциальных угроз. Защита умного дома требует постоянного внимания и обновления, учитывая постоянное развитие как самих устройств, так и новых методов атак со стороны злоумышленников.

Уязвимости в сетях умного дома могут иметь серьезные последствия для безопасности домашних сетей и пользователей. Злоумышленники могут получить доступ к видеонаблюдению и аудиозаписям, управлять устройствами, снижать уровень безопасности системы или проводить атаки на другие устройства в сети. Потенциальные последствия включают кражу ПДн, угрозу физической безопасности и нарушение частной жизни пользователей. Важно проводить регулярное обновление и контроль системы умного дома, чтобы минимизировать риски и обнаруживать уязвимости до их эксплуатации.

Безопасность является основополагающим аспектом, который необходимо учитывать при создании и расширении сети умного дома. Но, конечно, остаются и другие не затронутые в статье аспекты, такие как, например, защита от физического доступа или управление привилегиями.

Также можно задаться вопросом о стандартизации и регуляризации технической и программной составляющих устройств умного дома.

Список используемых источников:

1. Полет пчелы. Как работают сети ZigBee и как искать уязвимости в них [Электронный ресурс]. URL: https://xakep.ru/2019/09/30/zigbee-exploits/ (дата обращения: 15.10.2023).
2. Анализ защищенности систем «умного дома», функционирующих в Zigbee сетях [Электронный ресурс]. URL: http://synergy-journal.ru/archive/article2739 (дата обращения: 15.10.2023).
3. Виткова Л. А., Едемская Е. Д. Изучение уязвимостей в системе «умного» дома и методов их обнаружения // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы XI междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 15-16 фев. 2022 г. СПБ. : 2022. С. 267-270.

Sarazova I., Chakhir A.

Saint Petersburg State University of Industrial Technologies and Design

Methods for detecting vulnerabilities in smart home networks.

In the modern world, people are increasingly striving for simplification and automation in everyday life. But where there is simplification for the user, there is also a weakening of security.

Key words: methods of detecting weaknesses, security of home networks, smart home systems, unauthorized access

УДК 004.382.4
ГРНТИ 20.53.21

МОДЕЛЬ АССОЦИАТИВНОЙ ПАМЯТИ В СРЕДЕ ОБРАБОТКЕ БОЛЬШИХ ДАННЫХ

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

В современном мире нейронные сети становятся неотъемлемой частью человеческой жизни. В частности, нейронные сети стали применятся для задач построения средств защиты информации, в связи с этим, постепенно начала возникать необходимость в укреплении и совершенствовании механизмов самого искусственного интеллекта, в том числе при использовании технологии больших данных.

нейронные сети, искусственный интеллект, большие данные

Рассмотрим основные концепции работы с технологией Больших данных, в частности обработки ассимиляционной памяти для построения в РИС общей визуальной картины происходящей ситуации наличия ПА и ПО. Модель ассимиляционной памяти – важный компонент, который оценивает состояние РИС, запоминает события, выдает корреляционные показатели и накапливает информацию для потенциальной интеллектуальной СОВ.

Построенная ассоциативная память может использоваться для построения, например, эффективных структур бортовых баз геоинформационных данных, особенно при использовании в автономных транспортных средствах (например, БПЛА). Применение системы обнаружения вторжений (IDS - Intrusion Detection System) [1] для защиты бортовых баз геоинформационных данных в транспортных средствах может повысить безопасность и целостность данных.

Ассоциативная память в системе обнаружения вторжений может использоваться в качестве механизма запоминания и распознавания шаблонов атак. Она позволяет системе быстро идентифицировать ранее неизвестные атаки на основе их схожести с уже известными атаками. Ассоциативная память работает путем сопоставления входных данных с существующими шаблонами атак. Если совпадение найдено, система может выдать предупреждение о возможном вторжении. Этот процесс может быть автоматизированным или может требовать вмешательства человека для подтверждения. Дополнительно ассоциативную память в YaVi сонастроили на определения ПО и ПА в РИС за счет дополнительной кластеризации и агрегации параметров «на лету» со сбором сведений об объектах защиты [2].

Одним из преимуществ использования ассоциативной памяти в СОВ является ее способность обрабатывать большие объемы данных и быстро реагировать на новые атаки. Однако, как и любая СОВ, она также может столкнуться с ложными срабатываниями и ошибками из-за сложности точной идентификации всех возможных атак.

Данный ход процессов берет начало от репликации в Больших данных РИС, где закладывается элемент вычислительного момента для интеллектуальной СОВ [3]. Затем применяется схема воздействия для компонента ассоциативной памяти, после чем к каждом кластере достигается нормализация переданных процессов и данных для НС.

При этом НС чаще выглядят следующим образом при оценке параметров систем (рис. 1). Здесь учитывается разнообразие количества узлов и корреляционные показатели, которые возникают в случае возникновений вешнего несанкционированного воздействия (атак или вторжений) [4].

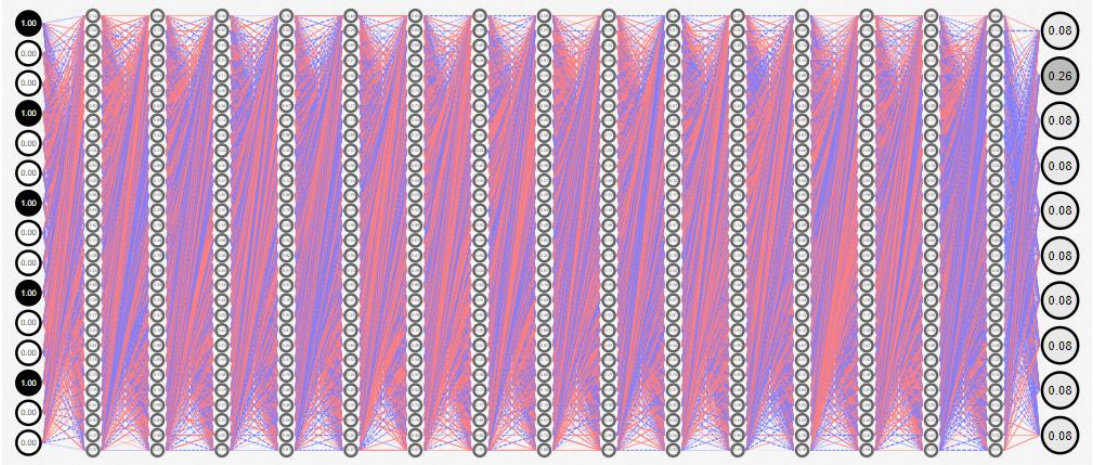


Рис. 1. Многослойная многоуровневая НС для операций поискового алгоритма с целью найти оптимальные данные для решения задачи сохранения комбинаторных функций интеллектуальной СОВ.

Чаще берется многоуровневая многослойная НС, где вводятся случайные параметры. На рис. 2 видно, что один из узлов будет иметь больший выходной коэффициент обработки данных. Его НС в концепте YaVi и будет стараться обходить.

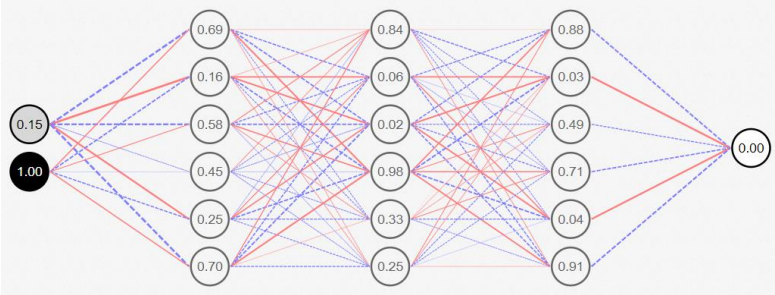


Рис. 2. Сведение разных выходных параметров для получения 100% результата обработки данных

В дальнейшем, для повышения точности вычислений, используя предложенную ранее кластеризацию, можно добиться точности вычислений обработки данных, а именно. Если точно высока. То выходной параметр будет стремиться к значению 0.00. На рис. 3 видно, что даже при разных параметрах, позже процесс сглаживается и в целом ассоциативная память будет работать на 100% точности в РИС.

По функции Хевисайда (рис. 3) все равно наблюдается процесс корреляционных изменений. Здесь НС все равно, даже за 7644 операции в сумме, будет иметь ошибки. Максимальная погрешность ошибки при этом - 0.17325846492581165 искаженных данных, на произвольные 6015 операций.

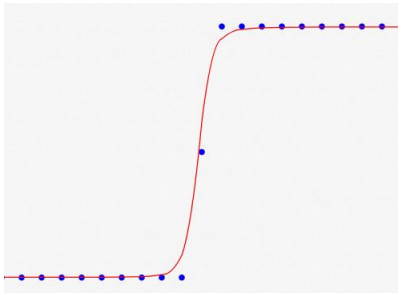


Рис. 3. Полученная функция Хевисайда в результате сведения разных выходных параметров обработки данных

В общем своем исполнении ПА модуль Kitovras, имея стандартное генеративное обучения выдает следующие данные на переобучении, имея, например из 3-ех, только один не испорченный (со значением 0.00) (см. рис. 4).

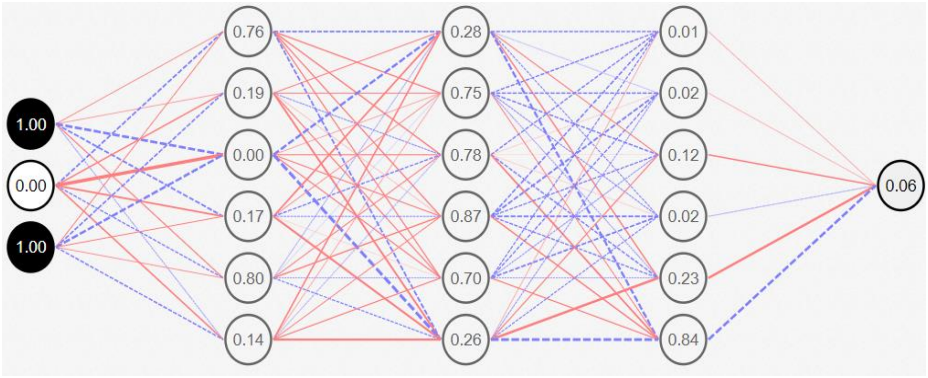


Рис. 4. Вычисления в модуле ПА Kitovras

Здесь коэффициент ошибки при вычислении упал до 0.19953693773445622 при 497256 шагах обработки данных, но на выходе все равно появился искаженный элемент данных. Т.е. ассоциативная память Mokosh запомнила не всё. Т.е. данные самоизучения РИС точны на 94%. Зависимость связей в Mokosh можно визуализировать и посмотреть критерии заполнения каждого блока ПА Kvasura (см. рис. 5).

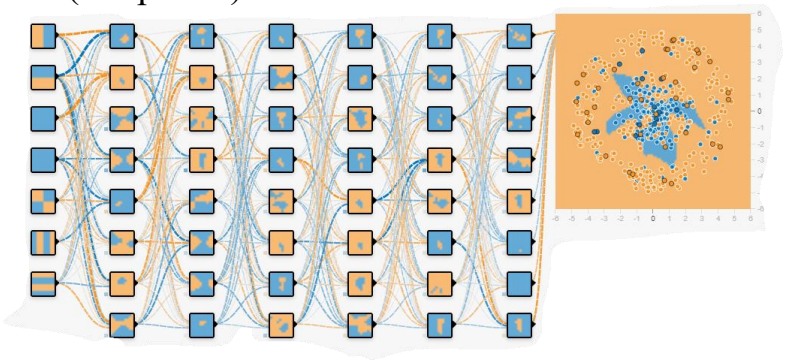


Рис. 5. Визуализация сведений обработки данных в модуле ПА Kvasura.

Делается предположение о накоплении вычисляемой информации при помощи ассоциативной памяти интеллектуальной СОВ. Например, при воздействии на целостность (установка или разархивирование модулей YaVI) весь ИИ ведет себя следующим образом:

1. Оранжевые точки – знание о сохраненной ПО (чем крупнее, тем больше данных содержит ПО).
2. Синие точки - знание о сохраненной ПА (чем крупнее, тем больше данных содержит ПА).
3. Оранжевые области – неисследованная, но возможно занятая область ПО в РИС.

Синие области – неисследованная, но возможно занятая область ПА в РИС.
Однако, со временем, картина исследования ассоциативной памяти меняется, а именно синей области становится больше (см. рис. 6). Прошло около 15 секунд, По осталось на месте, но начала уменьшатся оранжевая область, что говорит о потенциальном влиянии и распространении отдельных ПА в РИС.

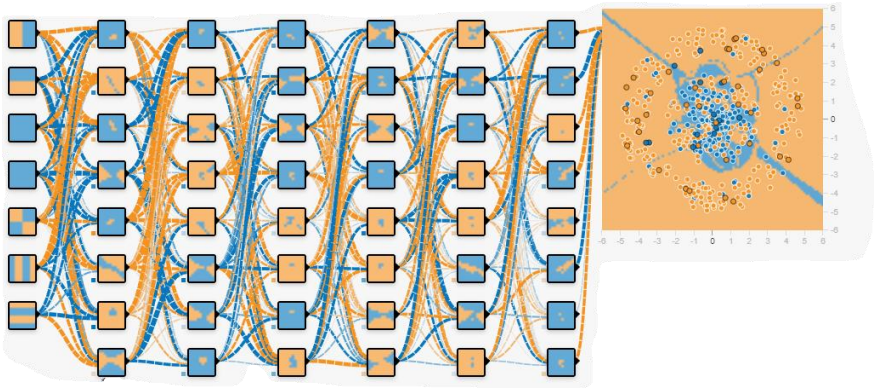


Рис. 6. Визуализация сведений обработки данных в модуле ПА Kvasura (спустя 15 секунд).

Данный анализ является ключевым в построении дальнейшего взаимодействия интеллектуальной СОВ в РИС. Можно сделать ключевое обозначение, что модель ассоциативной памяти в среде обработки Больших данных учитывает новые факторы хранения и обработки информации, четко разделяя, что есть ПО, а что есть ПА в РИС.
Данный результат обладает полезностью, т.к. для НС в целом становится возможно накоплять информацию и готовить потенциальный ИИ для дальнейшей самозащиты в РИС. Имеет место получение оценок показателей ИБ после атаки на ресурсы РИС, где видно как ассоциативная память определила структуры ПО и ПА четко разделив их. Погрешность в модели составила 6%.

Список используемых источников:

1. Штеренберг С. И. Проектирование архитектуры системы обнаружения вторжений с глубоким и машинным обучением на основе квазибиологической парадигмы // Вестник

Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. N 1. С. 86-91.

2. Штеренберг С. И. Разработка методологии защиты системы искусственного интеллекта в распределенных информационных системах. // Вестник СибГУТИ. 2023. N 17(3). С. 78-86.

3. Красов А. В., Штеренберг С. И., Голузина Д. Р. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей // Электросвязь. 2019. N 11. С. 39-47.

4. Штеренберг С. И. Методика управления системами обработки и сбора больших данных с поддержкой мониторинга встроенными программными агентами // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 4. С. 26-35.

Sevostyanov V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

MODEL OF ASSOCIATIVE MEMORY IN A BIG DATA PROCESSING ENVIRONMENT.

In the modern world, neural networks are becoming an integral part of human life. In particular, neural networks began to be used for the task of constructing information security tools; in connection with this, the need gradually began to arise to strengthen and improve the mechanisms of artificial intelligence itself, including when using big data technology.

Key words: Neural networks, artificial intelligence, big data

УДК 004.588
ГРНТИ 14.35.09

АНАЛИЗ ИННОВАЦИОННЫХ IT-ТЕХНОЛОГИЙ В ОБРАЗОВАНИИ

Н. В. Скородумов
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В современном мире образование претерпевает значительные изменения, связанные с внедрением инновационных IT-технологий. Информационные технологии открывают новые горизонты для обучения, делая образовательный процесс более интересным, доступным и эффективным.

образование, информационные технологии, искусственный интеллект, виртуальная реальность, дистанционное обучение

Инновационные IT-технологии в образовании представляют собой использование новейших информационных и коммуникационных технологий для улучшения образовательного процесса. Они предоставляют новые возможности для учителей и учеников, повышают качество образования и доступность к образовательным ресурсам. Актуальность темы заключается в необходимости использования инновационных IT-технологий в образовании для того, чтобы привлечь внимание большого количества людей к новому способу получения знаний, сделать обучение более интересным и доступным и, тем самым, увеличить количество образованных людей в мире. Именно поэтому последнее время IT-технологий называют основой современного образования.

Одним из видов современных IT-технологий, который можно использовать в образовании является виртуальная и дополненная реальность: VR и AR технологии позволяют учащимся визуализировать и взаимодействовать с абстрактными концепциями и предметами, делая учебный процесс более наглядным и понятным.

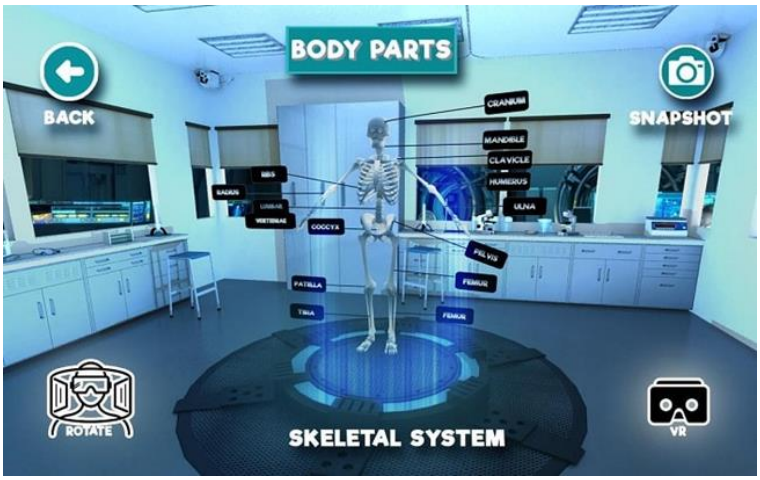


Рис. 1. Изучение скелета человека с помощью VR-технологий

Следующая инновация, которую можно обсудить, создание мобильных приложений для обучения. Специальные приложения могут предлагать интерактивные задания, игры и уроки, чтобы сделать обучение более привлекательным для учащихся. Такой вид обучения я считаю самым интересным, особенно для детей, которые будут с удовольствием учиться в игровом формате.

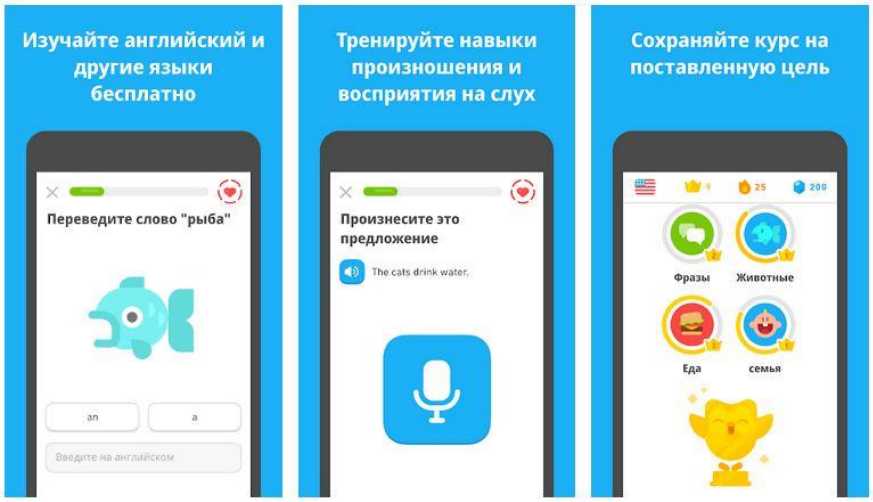


Рис. 2. приложение “Duolingo” для изучения иностранных языков

Также в современное образование можно добавить использование искусственного интеллекта и аналитических инструментов: алгоритмы и ИИ могут помочь анализировать данные о производительности учащихся и предоставлять персонализированные рекомендации для обеспечения эффективного обучения. В таком случае можно будет раскрыть возможности каждого обучающегося в той или иной научной отрасли, что положительно скажется на всем процессе обучения.

Внедрение инновационных IT-технологий в образование имеет потенциал для значительного усиления процесса обучения и развития учащихся. Новые технологии сделают образование доступнее для людей, также они могут помочь создать динамичное и интерактивное образование, учитывающее потребности и интересы каждого ученика.

Список используемых источников:

1. Краюшкин Н. Виртуальная реальность в образовании [Электронный ресурс]. URL: https://hsbi.hse.ru/articles/virtualnaya-realnost-v-obrazovanii/ (дата обращения: 18.10.2023).

2. Дульская Э. Лучшие мобильные приложения для студента [Электронный ресурс]. URL: https://www.gostudy.cz/blog/sovety-eksperta/mobilnye-prilozheniya-dlya-studentov (дата обращения: 18.10.2023).

Skorodumov N.

Saint-Petersburg State University of Industrial Technologies and Design

Analysis of innovative IT technologies in education.
In the modern world, education is undergoing significant changes associated with the introduction of innovative IT technologies. Information technologies open up new horizons for learning, making the educational process more interesting, accessible and effective.

Key words: education, information technology, artificial intelligence, virtual reality, distance learning.

УДК 004.056
ГРНТИ 81.93.29

СРАВНИТЕЛЬНЫЙ АНАЛИЗ И ПРИМЕНЕНИЕ МАТРИЦ АТАК MICROSOFT KUBERNETES THREAT MATRIX И MITRE ATT&CK MATRIX

Д. П. Спиридонов, Е. В. Федорченко
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данном исследовании описываются матрицы атак: Microsoft Kubernetes Threat Matrix и Mitre ATT&CK matrix, в контексте оркестратора облачных инфраструктур Kubernetes. Каждая из существующих матриц описывает стратегии атак, применяемые злоумышленниками. Их можно использовать для своевременного выявления атак на инфраструктуру и разработки стратегии защиты В статье проводится сравнительный анализ данных матриц в целях применения в задачах моделирования и реагирования на кибератаки.

кибербезопасность, матрицы атак, Kubernetes

Введение. В настоящее время контейнеры применяются повсеместно. Для управления контейнера используется Kubernetes. Это платформа с открытым исходным кодом. Неправильная конфигурация и уязвимости Kubernetes могут использоваться злоумышленниками при проведении кибератак. При обеспечении безопасности Kubernetes могут использоваться матрицы кибератак.

Матрицы атак. Матрица атак предоставляет собой структурированный список известных техник, используемых злоумышленниками, разделенный на тактики и методы, и представленный в виде таблиц (матриц).Примерами таких матриц являются MITRE ATT&CK и Microsoft Kubernetes Threat Matrix.

MITRE ATT&CK — это база знаний о кибератаках от организации MITRE [1, 2]. ATT&CK состоит из трех частей, или матриц: ATT&CK для предприятий, которая охватывает кибератаки в отношении корпоративных сетей и облаков, ATT&CK для мобильных устройств и ATT&CK для промышленных систем управления. Матрица для предприятий (Enterprise) включает тактики и техники, которые злоумышленники применяют в ходе атаки на предприятия. Она содержит информацию об атаках для следующих операционных систем: Windows, macOS, Linux, а так же информацию об атаках для облачных сервисов. В данном разделе представлена матрица для контейнерных инфраструктур (рис. 1).

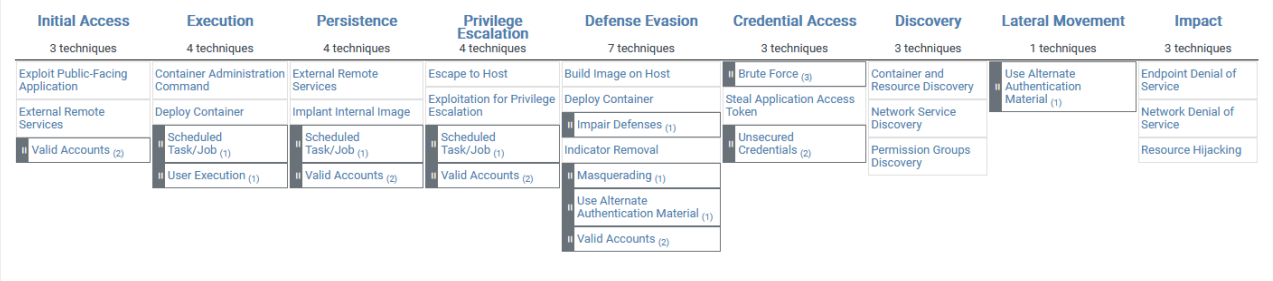


Рис. 1. Матрица MITRE ATT&CK Containers [1]

Матрица для мобильных устройств (Mobile) содержит информацию для следующих платформ: Android, iOS.

Матрица для промышленных систем управления (ICS) включает тактики и техники, которые используются в атаках на промышленные системы управления.

Каждая матрица представляет собой таблицу, в которой заголовки столбцов соответствуют тактикам злоумышленников, то есть основным этапам атаки или подготовки к ней, а содержимое ячеек — методикам реализации этих тактик, или техникам. Так, если сбор данных согласно MITRE ATT&CK — это тактика атаки, то способы сбора, например, автоматический сбор или сбор данных со съемных носителей, — это техники.

Помимо матриц, в базе знаний MITRE ATT&CK доступны перечни техник, которыми пользуются известные APT-группировки, а также списки вредоносного инструментария этих группировок. Кроме того, на сайте MITRE ATT&CK представлены основные методы усиления защиты организации.

Microsoft Kubernetes Threat Matrix — это матрица угроз, разработанная Microsoft, которая описывает различные угрозы и атаки, связанные с использованием именно Kubernetes (рисунок 2) [3]. Матрица включает в себя широкий спектр тактик и техник, которые могут быть использованы злоумышленниками для компрометации инфраструктуры Kubernetes.

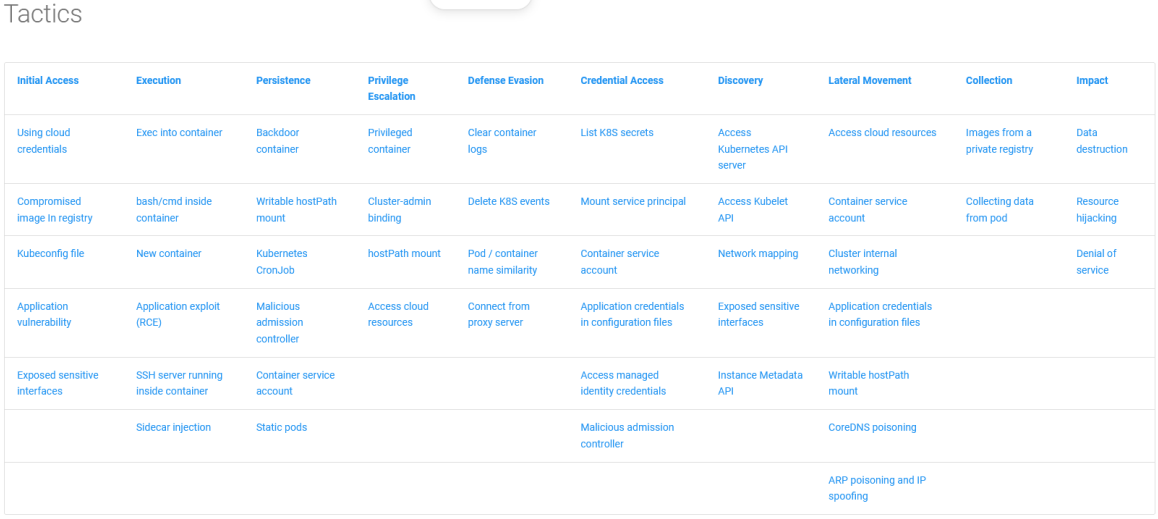


Рис. 2. Матрица Microsoft Kubernetes Threat Matrix [3]

В последней версии матрицы от Microsoft были представлены две новых техники атак, статические капсулы и сбор данных из модуля, и дополнительная классификация существующих методов:

Сравнение матриц MITRE ATT&CK и Microsoft Kubernetes Threat Matrix.

Поскольку матрица ATT&CK представляет собой детальное описание действий злоумышленников при взломе систем, она полезна для решения задач моделирования, прогнозирования и анализа атак, а также выбора мер защиты.

Матрица угроз для Kubernetes позволяет получить представление об уникальной поверхности атак Kubernetes и оценить степень защиты от этих угроз.

Матрица MITRE ATT&CK для контейнеров не имеет эквивалентного метода для каждого из методов в матрице угроз Microsoft для Kubernetes. Если в матрице MITRE нет эквивалентного метода, методы Microsoft могут быть сопоставлены с методом MITRE, который не является частью матрицы контейнеров MITRE, но имеет тот же принцип. Например, метод Backdoor Container (MS-TA9012) объясняет, что злоумышленники могут использовать контроллеры Kubernetes для запуска своего кода и выживания при перезагрузке модулей\узлов. Это очень похоже на метод создания или изменения системного процесса MITRE (T1543), который предполагает использование служб для той же цели. Другим примером является сопоставление между контроллером вредоносного доступа (MS-TA9015) и выполнением по событию MITRE. Хотя MITRE не говорит о контейнерной среде, в основе этих двухметодов лежит одна и та же идея [2].

Заключение. Проведенный анализ показал, что матрица Microsoft Kuber netesThreat Matrix является предпочтительной для обеспечения безопасности Kubernetes, т.к. специализируется исключительно на угрозах, связанных с Ku bernetes.

Список используемых источников:

1. Containers Matrix [Электронныйресурс]. URL:https://attack.mitre.org/matrices/enterprise/containers/ (дата обращения: 21.10.2023).

2. MITRE ATT&CK Matrix for Kubernetes [Электронный ресурс]. URL:https://www.weave.works/blog/mitre-attack-matrix-for-.kubernetes (дата обращения: 21.10.2023).

3. Threat Matrix for Kubernetes [Электронный ресурс]. URL: https://microsoft.github.io/Threat-Matrix-for-Kubernetes/ (дата обращения: 21.10.2023).

Spiridonov D., Fedorchenko E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Comparative analysis and application of Microsoft Kubernetes Threat Matrix and Miter Att&ck matrix.

This study describes two attack matrices: the Microsoft Kubernetes threat matrix and the MITRE ATT&CK matrix. Each matrix describes the attack strategies used by attackers and, based on various approaches, suggests a change in protection and timely impact on the infrastructure. The paper provides the results of a comparative analysis of the matrices in the context of Kubernetes security.

Key words: Cyberscurity, attack matrices, Kubernetes.

УДК 004.432.2
ГРНТИ 50.05.09

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОСНОВНЫХ ТИПОВ КИБЕРАТАК НА ВЕБ-ПРИЛОЖЕНИЯ И СПОСОБЫ БОРЬБЫ С НИМИ

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

Данная статья представляет сравнительный анализ разнообразных типов кибератак. В статье приведены основные принципы атак каждого типа и предлагаются методы для эффективной защиты от них.

веб-безопасность, кибератаки, веб-приложение

Современный мир цифровых технологий предоставляет бесконечные возможности для улучшения бизнеса и общественной жизни. Однако вместе с этим ростом цифровой зависимости появляется и растущая угроза в виде кибератак. Киберпреступники и хакеры постоянно совершают новые атаки, используя разнообразные методы, чтобы получить доступ к информации, повредить системы и нарушить нормальное функционирование онлайн-сервисов и приложений.

Согласно сайту Positive Technologies, доля веб-приложений, содержащих уязвимости высокой степени риска, составила 66% в 2020 году, а в 2021 году — 62%, что значительно больше показателя 2019 года (рис. 1).

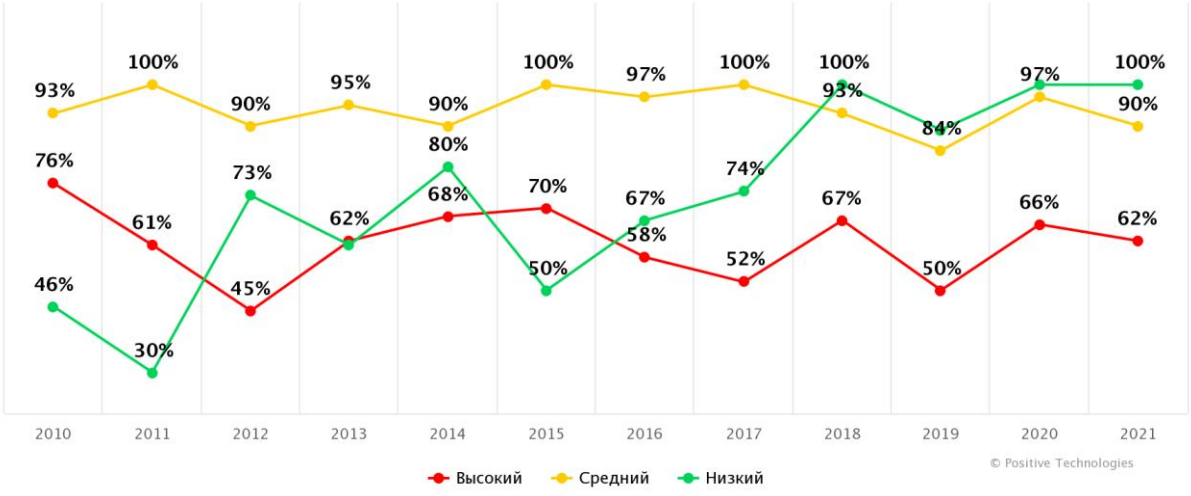


Рис. 30. Доля уязвимостей различной степени риска

В данной статье мы рассмотрим разнообразные типы кибератак, а также методы и техники борьбы с ними:

1. **SQL-инъекции (SQL Injection)**

Это один из наиболее распространенных видов кибератак на веб-приложения, при котором злоумышленник вводит вредоносный SQL-код во

входные поля или параметры URL с целью выполнения нежелательных операций на базе данных сайта. Этот тип атаки возникает из-за недостаточной обработки и фильтрации входных данных, которые передаются в базу данных. В результате SQL-инъекции, злоумышленник может получить доступ к конфиденциальной информации, изменить или уничтожить данные, а также выполнить другие опасные действия.

2. Межсайтовый скриптинг (XSS, Cross-Site Scripting)

Это тип кибератаки, при которой злоумышленник внедряет вредоносный JavaScript-код в веб-страницы или веб-приложения, выполняемый в браузерах других пользователей. Атаки XSS происходят из-за недостаточной фильтрации и экранирования данных, передаваемых между браузером пользователя и веб-сервером.

Существует несколько видов атак XSS:

- Сохраненные XSS (Stored XSS): Злоумышленник внедряет вредоносный скрипт, который сохраняется на сервере и выполняется каждый раз, когда другой пользователь просматривает зараженную страницу.
- Отраженные XSS (Reflected XSS): Злоумышленник внедряет вредоносный код в URL или другие параметры запроса, и жертва выполняет его, перейдя по этой ссылке. Вредоносный код отражается обратно на жертву через уязвимое приложение.
- DOM-инъекции (DOM-based XSS): Этот вид XSS связан с манипуляцией Document Object Model (DOM) в браузере жертвы. Злоумышленник внедряет вредоносный код, который изменяет DOM и влияет на взаимодействие пользователя с веб-страницей.

3. Межсайтовая подделка запроса (CSRF, Cross-Site Request Forgery)

Это вид кибератаки, при которой злоумышленник заставляет авторизованного пользователя выполнять нежелательные действия в веб-приложении без его ведома или согласия. Атаки CSRF происходят из-за недостаточной защиты от подделки запросов, и они могут привести к изменению данных пользователя, изменению настроек, выполнению ненужных действий или даже созданию учетной записи под контролем злоумышленника.

Процесс работы атаки CSRF выглядит следующим образом:

- Злоумышленник создает поддельное вредоносное веб-приложение или веб-страницу, которая содержит ссылки или формы, выполняющие нежелательные действия на целевом веб-приложении.
- Злоумышленник отправляет жертве эту поддельную страницу или ссылку, обманывая ее, чтобы перейти по ней.
- Поскольку жертва авторизована на целевом веб-приложении, браузер выполняет запросы, как если бы они были инициированы самой жертвой. Это может включать в себя изменение данных, отправку сообщений, покупку товаров и другие действия.
- Все действия выполняются без ведома и согласия жертвы, что делает атаку особенно опасной.

4. Атаки на переполнение буфера (Buffer Overflow Attacks)

Это вид кибератак, при котором злоумышленник пытается внедрить вредоносный код, превышающий выделенный буфер памяти, чтобы выполнить произвольный код на атакуемой системе. Эти атаки могут быть особенно разрушительными, так как они могут привести к выполнению нежелательных операций, взлому системы или даже удалению данных. Атаки на переполнение буфера часто встречаются в прикладном программном обеспечении, особенно в низкоуровневых языках программирования, таких как C и C++.

Сравнительный анализ четырех видов кибератак, а именно SQL-инъекции, межсайтового скриптинга (XSS), межсайтовой подделки запроса (CSRF) и атак на переполнение буфера:

- **SQL-инъекции и межсайтовый скриптинг (XSS):**
  - **SQL-инъекции:**
    - **Цель атаки:** Получение доступа к базе данных приложения.
    - **Уязвимости:** Связаны с неправильной обработкой SQL-запросов.
    - **Последствия:** Кража данных, изменение содержимого базы данных.
    - **Способы защиты:** Использование параметризованных запросов или хранимых процедур, санитаризация ввода данных.
  - **XSS:**
    - **Цель атаки:** Внедрение вредоносных скриптов в веб-страницы.
    - **Уязвимости:** Связаны с недостаточной санитаризацией выводимых данных.
    - **Последствия:** Кража данных, выполнение нежелательных действий в браузере пользователя.
    - **Способы защиты:** Санитаризация и экранирование выводимых данных, использование заголовка HTTP Content Security Policy (CSP), который позволяет указать, какие источники скриптов и ресурсов разрешены на веб-странице.
- **Межсайтовая подделка запроса (CSRF) и атаки на переполнение буфера:**
  - **CSRF:**
    - **Цель атаки:** Заставить пользователя выполнить нежелательное действие в приложении.
    - **Уязвимости:** Связаны с недостаточной проверкой происхождения запросов.
    - **Последствия:** Выполнение нежелательных действий от имени пользователя.
    - **Способы защиты:** Использование токенов CSRF, проверка происхождения запросов.
  - **Атаки на переполнение буфера:**

- **Цель атаки:** Изменение поведения программы или операционной системы.
- **Уязвимости:** Связаны с неправильной обработкой данных в памяти.
- **Последствия:** Сбои системы, выполнение вредоносного кода.
- **Способы защиты:** Безопасное программирование, использование безопасных функций, регулярное обновление и патчи.

В результате проведенного сравнительного анализа можно выделить несколько ключевых моментов:

- Каждый вид атаки нацелен на разные уровни уязвимости в системах и приложениях. Например, SQL-инъекции и межсайтовый скриптинг атакуют уровень приложения, в то время как атаки на переполнение буфера нацелены на уровень операционной системы или программы.
- Уязвимости, которые эксплуатируются при разных атаках, различны. SQL-инъекции связаны с недостаточной обработкой SQL-запросов, XSS - с недостаточной санитаризацией выводимых данных, CSRF - с недостаточной проверкой происхождения запросов, а атаки на переполнение буфера - с неправильной обработкой данных в памяти.
- Последствия различных атак похожи, все они могут привести к краже или потере данных.
- Защита от каждой из этих атак требует применения разных методов и средств безопасности.

В заключение, различные виды кибератак представляют разные угрозы для информационной безопасности, и для их предотвращения необходимо применять соответствующие меры безопасности на разных уровнях системы. Понимание разнообразных угроз и методов их предотвращения является важным аспектом обеспечения безопасности в цифровой эпохе.

Список используемых источников:

1. Дибиров Г. М., Ковцур М. М., Бабков И. Н. XI Конгресс молодых учёных. Сборник научных трудов. Санкт-Петербург, 2022. С. 131-135.
2. Positive Technologies, 2022. Уязвимости и угрозы веб-приложений в 2020–2021 гг. [Электронный ресурс] Available at: https://www.ptsecurity.com/ru-ru/research/analytics/web-vulnerabilities-2020-2021/
3. Kaspersky. Что такое SQL-инъекция? Определение и описание [Электронный ресурс] Available at: https://www.kaspersky.ru/resource-center/definitions/sql-injection
4. SecurityLab.ru, 2023. Основные типы кибератак и способы борьбы с ними [Электронный ресурс] Available at: https://www.securitylab.ru/analytics/535598.php.
5. Jon Erickson. Hacking: The Art of Exploitation. No Starch Press, 2018. С. 496.
6. Dafydd Stuttard, Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. John Wiley & Sons, 2011. 878 с.

Stepanov M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Comparative analysis of the main types of cyber-attacks on web applications and ways to deal with them.
This article presents a comparative analysis of various types of cyber-attacks. The article presents the basic principles of attacks of each type and suggests methods for effective protection against them.

Key words: web security, cyber-attacks, web application

УДК 004.056.5
ГРНТИ 06.01.05

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В РАЗЛИЧНЫХ ОТРАСЛЯХ

А. Н. Стукалов
Санкт-Петербургский государственный университет промышленных технологий и дизайна

Технология блокчейн, изначально разработанная для поддержки криптовалюты Bitcoin, стала объектом интереса во многих отраслях. Ее децентрализованная и надежная природа предлагает потенциал для революции в различных областях, открывая новые возможности и привнося инновации.

Блокчейн, применение технологий, криптография, децентрализация

Блокчейн нашел применение в различных отраслях, включая финансы, логистику, здравоохранение, государственный сектор, интеллектуальную собственность и другие. Он может быть использован для упрощения процессов, повышения безопасности, улучшения прозрачности и снижения рисков мошенничества.

Блокчейн - это децентрализованная и распределенная технология, которая позволяет записывать и хранить информацию в виде блоков, образуя непрерывную цепочку. Каждый блок содержит данные, временную метку и уникальный идентификатор (хэш), который связывает его с предыдущим блоком. Это обеспечивает надежность, прозрачность и безопасность системы.

Основным принципом блокчейна является децентрализация: Блокчейн не хранится на одном центральном сервере, а распределен между множеством компьютеров (узлов) в сети. Каждый узел имеет копию всей цепочки блоков, что делает систему устойчивой к отказам и атакам.

Другими не менее важными принципами блокчейна являются:

1. Прозрачность: Все транзакции и изменения в блокчейне видны всем участникам сети. Это обеспечивает открытость и доверие, так как каждый может проверить историю операций.
2. Безопасность: Каждый блок содержит хэш предыдущего блока, что делает цепочку неизменяемой. Любое изменение в одном блоке приведет к изменению хэшей во всех последующих блоках, что затрудняет манипуляции и подделки данных.
3. Смарт-контракты: Блокчейн позволяет создавать и выполнять смарт-контракты - программы, которые автоматически выполняют условия сделки при выполнении определенных условий. Это упрощает и автоматизирует процессы, устраняя необходимость в посредниках.

Благодаря основным принципам блокчейна многие отрасли заинтересовались данной технологией.

Финансовый сектор является крупнейшим пользователем технологии блокчейна, согласно второму глобальному сравнительному исследованию, проведенному Cambridge Centre For Alternative Finance. Исследование приведено в таблице 1.

ТАБЛИЦА 1. Статистика доли блокчейн в различных отраслях

Отрасль	Доля Блокчейн на рынке
Финансы и страхование	43%
Другие	12%
Межотраслевая	9%
Услуги по проживанию и питанию	6%
Здравоохранение и социальная помощь	6%
Розничная торговля	4%
Горное дело, разработка и добыча	4%
Транспортировка и хранение	4%
Искусство, развлечения и отдых	3%
Оптовая торговля	3%
Государственное управление	3%
Недвижимость, аренда и лизинг	3%

Основная часть применения технологии блокчейн приходится на финансовую отрасль. Технология применяется для упрощения и ускорения процессов платежей и переводов, обеспечение безопасности и прозрачности в финансовых операциях, создание умных контрактов для автоматизации сделок.

Другая отрасль применения снабжение и логистика. Применяется для отслеживания цепочки поставок и подлинности товаров, улучшение эффективности логистических процессов, снижение рисков мошенничества и контрафактной продукции.

Важная часть применения в сфере здравоохранения: безопасное хранение и обмен медицинской информацией, улучшение прослеживаемости лекарственных препаратов, упрощение процесса медицинской аутентификации.

В государственный секторе: обеспечение прозрачности и борьба с коррупцией, улучшение процессов голосования и выборов, создание электронных удостоверений и документов.

Интеллектуальная собственность: защита авторских прав и интеллектуальной собственности, улучшение процесса лицензирования и управления правами.

Технология блокчейн имеет огромный потенциал для применения в различных отраслях. Она может улучшить безопасность, прозрачность и эффективность процессов, а также снизить риски мошенничества. Однако, необходимо учитывать вызовы, связанные с масштабированием, регулированием и принятием стандартов для успешной реализации технологии в каждой конкретной отрасли.

Список используемых источников:

1. Дрешер Д. Основы блокчейна: вводный курс для начинающих в 25 небольших главах. М. : ДМК Пресс, 2017. 311 с.
2. Равал С. Децентрализованные приложения. Технология Blockchain в действии. СПб. : Питер, 2017. 240 с.
3. Винья П., Кейси М. Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок. М. : Издательство «Манн, Иванов и Фербер», 2017. 430 с.

Stukalov A.

Saint Petersburg State University of Industrial Technologies and Design

Application of Blockchain technology in various industries.

Blockchain technology, originally developed to support the cryptocurrency Bitcoin, has become an object of interest in many industries. Its decentralised and secure nature offers the potential to revolutionise various fields, opening up new opportunities and bringing innovation.

Key words: Blockchain, application of technology, cryptography, decentralization.

УДК 004.056.53
ГРНТИ 81.93.29

ПАКЕТНЫЕ НЕЙРОСЕТЕВЫЕ ПРОГРАММЫ В РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ.

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

В современном мире вряд ли можно встретить человека, который не слышал об машинном обучении, нейронной сети или искусственном интеллекте. Нейронные сети сейчас выполняет такие задачи как управление беспилотными автомобилями, дронами, сайтами, используется для автоматизации процессов, улучшения качества обслуживания, прогнозирования и т.д. Всё это требует обработки и анализа больших объемов данных и рационально использовать распределённые информационные системы, которые обеспечивают такие показатели как: высокую производительность, отказоустойчивостью безопасность и удобство использования.

Описание и способы представления ПНП в РИС.

Процесс получения новых знаний человеком во много раз превосходит по своей сложности самые совершенные алгоритмы машинного обучения, но у нейросетей есть преимущество ввиду большого объёма памяти и использования распределённой информационной системы для запоминания, обработки, и вывода огромного объёма данных. Накапливаемый опыт нейросетей представлен в форме данных за большой период времени, обработанных с помощью специальных алгоритмов. (рис. 1).

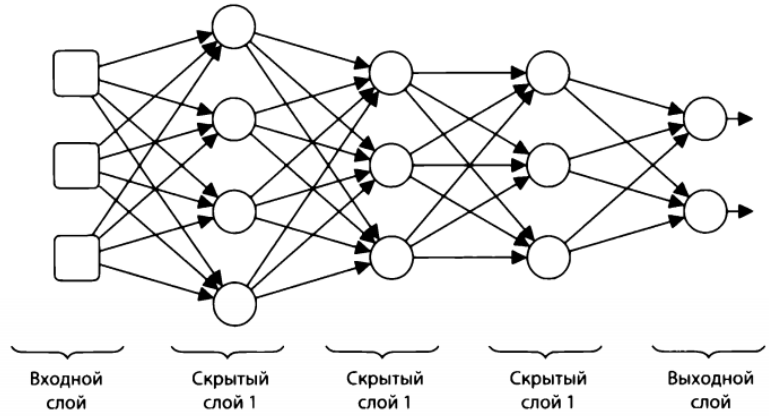


Рис. 1. Схематическое изображение нейронной сети.

Прямоугольники на входном уровне представляют ячейки памяти, которые хранят введенные данные. Эти ячейки называются нейронами восприятия, они не обрабатывают информацию, а только выводят хранящиеся в них значения.

Круги на схеме представляют нейроны, которые обрабатывают информацию. Каждый такой нейрон принимает на вход множество числовых значений и связывает их с одним выходным значением. Вход каждого

обрабатывающего нейрона может быть либо выходом нейрона ввода, либо выходом другого обрабатывающего нейрона.

Стрелки на схеме показывают передачу информации по сети от выхода одного нейрона ко входу другого. Каждое соединение в сети соединяет два нейрона и имеет направление: информация передается только в одну сторону по этому соединению. У каждого соединения есть свой вес - это число, которое играет важную роль в обработке информации нейроном. Вес соединения определяет то, как нейрон обрабатывает входящую информацию. Обучение искусственной нейронной сети в основном сводится к поиску наилучшей (или оптимальной) комбинации весов.

Пакетные нейросетевые программы представляют собой алгоритмы машинного обучения, основанные на искусственных нейронных сетях. Они используются для обработки и анализа больших объемов данных и решения сложных задач, таких как распознавание образов, классификация, регрессия и кластеризация. (рис. 2).

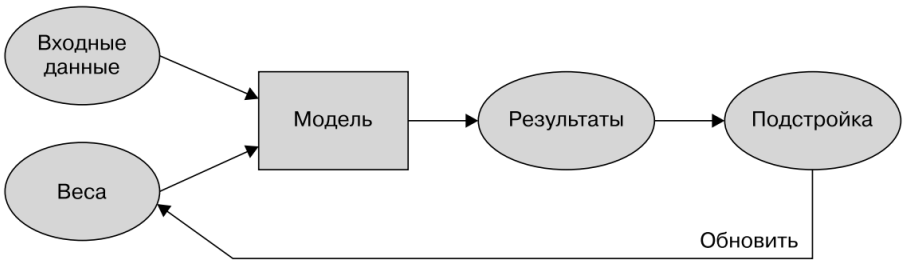


Рис. 2. Алгоритм обучения нейронной сети.

В распределенных информационных системах пакетные нейросетевые программы могут быть представлены различными способами, в зависимости от архитектуры системы и требований к обработке данных. Вот некоторые из них:

Параллельное обучение: В этом подходе несколько нейросетей обучаются параллельно на разных узлах системы. Результаты обучения объединяются и выбирается наилучшая модель.

Распределенное обучение: В распределенном обучении каждый узел системы обучается на своей части данных, и результаты обучения объединяются в общий результат. Этот подход позволяет ускорить процесс обучения и повысить его эффективность.

Асинхронное обучение: Асинхронное обучение предполагает, что каждый узел системы может обучаться независимо от других узлов, и результаты их обучения объединяются только после завершения процесса обучения.

Обучение с градиентным спуском: Этот метод основан на использовании градиента функции ошибки для оптимизации весов нейронной сети.

В распределенных системах градиент вычисляется на каждом узле и передается на центральный сервер для обновления весов.

Обучение с использованием графических процессоров (GPU): GPU-ускорение позволяет значительно ускорить процесс обучения, поскольку графические процессоры обладают высокой вычислительной мощностью.

Выбор способа представления пакетной нейросетевой программы в распределенной информационной системе зависит от требований к производительности, масштабируемости и гибкости системы.

Распределенные информационные системы (рис. 3) обладают рядом преимуществ, таких как масштабируемость, отказоустойчивость, повышенная доступность данных и гибкость. Они позволяют организациям более эффективно использовать свои ресурсы, обеспечивая при этом высокий уровень надежности и безопасности данных.

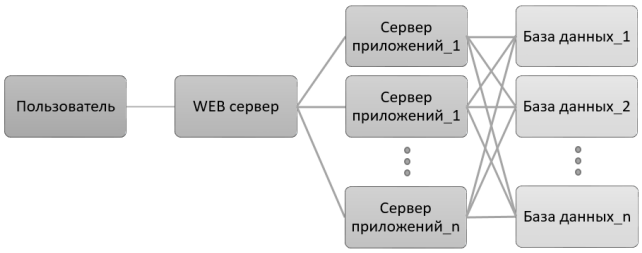


Рис. 3. Схематическое изображение распределённых систем на примере сервиса мобильных приложений.

Однако, распределенные информационные системы также имеют свои недостатки, такие как сложность управления и настройки, повышенные требования к сетевому оборудованию и необходимость обеспечения совместимости между компонентами системы. Кроме того, распределенные системы могут быть более уязвимыми для атак на сетевые коммуникации и требуют более сложных механизмов безопасности для защиты данных.

Уязвимости пакетных нейросетевых программ в распределенных информационных системах могут быть связаны с различными аспектами работы таких систем. Например, это может быть связано с уязвимостями в алгоритмах обучения нейросетей, в способах передачи данных между узлами системы, а также в безопасности самих узлов.

Кроме того, уязвимости могут возникать из-за недостатков в реализации алгоритмов и протоколов, используемых в распределенных информационных системах. Например, если система не обеспечивает достаточную защиту от атак на сетевые коммуникации, это может привести к утечке конфиденциальной информации.

Также следует учитывать, что распределенные информационные системы могут быть сложными для понимания и настройки, что может привести к уязвимостям, связанным с неправильной конфигурацией системы. Например, неправильная настройка сетевых параметров может привести к снижению производительности системы или к появлению уязвимостей в системе безопасности.

В целом, для предотвращения уязвимостей в пакетных нейросетевых программах в распределенных информационных системах необходимо

уделять внимание всем аспектам работы системы, включая алгоритмы обучения, протоколы передачи данных и безопасность узлов системы.

Для сохранения принципов целостности рассинхронизированных децентрализованных пакетных нейросетевых программ в распределенных информационных системах необходимо выполнение следующих требований:

– Обеспечение безопасности данных: системы должны иметь механизмы защиты данных от несанкционированного доступа, изменения или уничтожения.

– Поддержка отказоустойчивости: системы должны быть спроектированы таким образом, чтобы они могли продолжать работу даже в случае отказа некоторых компонентов.

– Обеспечение масштабируемости: системы должны быть способны обрабатывать большие объемы данных и увеличивать свою производительность по мере необходимости.

– Использование надежных алгоритмов шифрования: для обеспечения безопасности данных необходимо использовать надежные алгоритмы шифрования, такие как AES, RSA и т.д.

– Регулярное обновление программного обеспечения: для поддержания безопасности системы необходимо регулярно корректировать программное обеспечение и исправлять обнаруженные уязвимости.

– Обучение и повышение квалификации сотрудников: сотрудники, работающие с системой, должны проходить обучение и повышать свою квалификацию для обеспечения должного уровня безопасности.

Список используемых источников:

1. Бурков А. Машинное обучение без лишних слов. СПб. : Питер, 2020. 192с.

2. Бринк Х., Ричардс Д., Феверолф М. Машинное обучение. СПб. : Питер, 2017. 336 с.

3. Ховард Д., Гуггер С. Глубокое обучение с fastai и PyTorch: минимум формул, минимум кода, максимум эффективности. СПб. : Питер, 2022. 624 с.

4. Келлехер Джон Д. Глубокое обучение. Самый краткий и понятный курс : пер. с англ. М. : Эксмо, 2022. 160 с.

Talakin E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Distributed neural network.

In the modern world, you can hardly meet a person who has not heard of machine learning, neural network or artificial intelligence. Neural networks now solve problems such as controlling unmanned vehicles, drones, websites, and are used to automate processes, improve the quality of service, forecast, etc. All this requires the processing and analysis of large volumes of data and the intelligent use of distributed systems, which determine indicators such as: high performance, fault tolerance, security and ease of use.

Key words: machine learning, ML, artificial intelligence, AI, distributed neural network.

УДК 004.056
ГРНТИ 49.33.29

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЕШЕНИЙ ДЛЯ ГЕНЕРАЦИИ КОМПЬЮТЕРНЫХ АТАК С ЗАДАННЫМИ ХАРАКТЕРИСТИКАМИ

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

С развитием технологий и доступностью различных инструментов, злоумышленники стали все более изобретательными в создании атак, которые могут причинить ущерб как отдельным пользователям, так и организациям. Для выявления уязвимостей необходим инструмент, который автоматизировано выполнит наиболее популярные атаки в их различном проявлении и оставит "след", чтобы в дальнейшем уязвимость смогли устранить.

APTSimulator, тактики и техники атак, вредоносное ПО, компрометация

Выявление компьютерных угроз является одной из важнейших задач в информационной безопасности с момента появления компьютера. Искусство кибератак неуклонно развивается, и злоумышленники становятся все более изощренными в своих начинаниях. Помочь обеспечить безопасность системы призвана матрица MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge). Она представляет собой схематичное описание различных тактик, техник и процедур, которые используются злоумышленниками при кибератаках[1]. Эти матрицы включает в себя список тактик и связанных с ними техник, которые могут использоваться злоумышленниками при атаках на системы. Каждая тактика представляет собой набор действий, а техники – конкретные методы и средства, которые применяются для достижения целей. Матрица MITRE ATT&CK постоянно обновляется и расширяется, чтобы отражать актуальные угрозы и методы злоумышленников.

Для выявления слабых мест в компьютере, которые могли бы использовать хакеры, необходимо использовать так называемые APT (Advanced Persistent Threats) симуляторы – симуляторы целенаправленных продвинутых атак. Такие симуляторы начали появляться примерно в 2017 году, и с того времени их количество заметно увеличилось. К наиболее популярным относятся: CALDERA, ATOMIC RED TEAM, Metta и Infectation Monkey[2].

Стоит отличать целенаправленные и массовые атаки. Особенность APT-атак в том, что их большая часть нацелена на конкретные компании или даже людей, тогда как массовые атаки используются для одновременного воздействия на множество целей и устройств. Целенаправленные атаки обычно хорошо спланированы и включают в себя несколько этапов – от разведки, внедрения и получения информации до сокрытия своих следов.

Злоумышленники изучают информационные объекты жертвы, узнают программное обеспечение[3].

Рассмотрим некоторые виды APT-атак[4]:

•Collect (сбор информации) – это атаки, целью которых является сбор разнообразной информации о системе или организации. Эта информация может включать в себя данные о структуре сети, уязвимостях, логинах, паролях, а также корпоративные данные.

•Command and Control (C2) (управление и контроль) – данный тип компьютерной атаки нацелены на установление связи между атакующими и зараженными устройствами или системами. Она представляет собой попытку хакеров установить управление над зараженными устройствами, обычно с целью кражи данных, внедрения вредоносного ПО или выполнения различных вредоносных программ в системе.

•Credential access (доступ к учётным данным) – эти атаки относятся к процессу получения доступа к учетным данным, таким как логины и пароли, для дальнейшего незаконного использования. Так же является одним из этапов, поскольку учетные данные могут предоставить им широкие полномочия и доступ к целевым системам и данным. Злоумышленник также может создавать учетные записи с целью их последующего использования в атакуемой среде.

•Defense evasion (уклонение от защиты) – данная атака представляет собой попытку злоумышленников избежать или обойти средства защиты, установленные в компьютерных системах. Она направлена на обход обнаружения и блокировки, позволяя злоумышленникам остаться незамеченными и продолжить свои действия.

•Discovery (обнаружение, исследование) – атака, в которой злоумышленники пытаются собрать информацию о целевой системе, в которую получили доступ, чтобы лучше понять её структуру и уязвимости. Она позволяет определить, существующие слабые места в системе.

•Execution (выполнение) – процесс запуска различных команд, сценариев и исполняемых файлов с целью достижения поставленных целей в атакуемой системе.

•Lateral Movement (боковое движение) – метод в котором злоумышленник, уже находящийся внутри компьютерной системы, пытается распространить свой доступ и контроль на другие части системы. Боковое движение позволяет получать информацию из удаленных систем без использования дополнительных инструментов.

•Persistence (закрепление) – атака, целью которой, является обеспечение долгосрочного и постоянного доступа к системе жертвы после успешного вторжения. После того как злоумышленник получил начальный доступ, он стремятся сохранить свой контроль и доступ даже после реагирования на инциденты безопасности со стороны жертвы.

•Privilege Escalation (повышение привилегий) – атака, в которой атакующий пытается получить расширенные права и привилегии в системе.

Взломанные учетные записи обычно имеют ограниченные права, и злоумышленники стремятся повысить свой статус в системе и получить более высокие привилегии, что позволяет им выполнять такие действия, как изменение системных настроек, доступ к конфиденциальным данным или управление системой.

Для понимания работы и структуры симулятора целенаправленных атак на тестовую виртуальную машину под управлением операционной системы Windows 10, был установлен APTSimulator от Nextron System[5]. Выбор пал на эту систему, потому что она отличается простотой в использовании, а также позволяет создавать в ней собственные атаки. Как и все симуляторы, данный продукт может эмулировать как поэтапную атаку на систему, так и выбрать определённую атаку.

Данный симулятор запускается из bat-файла и открывается в командной строке. Интерфейс APTSimulator представлен на рис. 1.

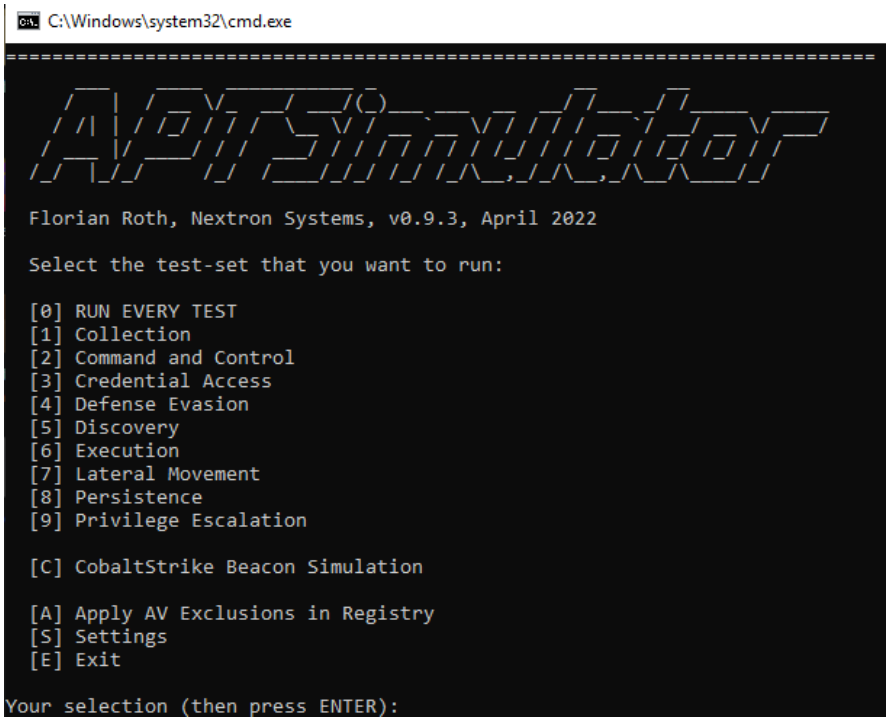


Рис. 1. Интерфейс APTSimulator

Отдельные пункты соответствуют этапам атаки на систему. Каждый из них включает в себя заранее записанные скрипты, которые выполняют определённые действия для обхода систем защиты системы и выполнения вредоносного кода. Всё это сделано для автоматизации симуляции, чтобы при тестировании системы не приходилось собственноручно прописывать команды и создавать скрипты. В APTSimulator собрана лишь малая часть атак, так как, по большей мере, данный продукт служит для ознакомления с принципами работы такого рода симуляторами.

Чтобы понимать, как защититься от злоумышленника, нужно знать, какие тактики, техники и процедуры (TTPs) могут быть применены к потенциально уязвимой системе[6].

Тактика – обобщённое понятие поведения злоумышленника.

Техника – это описание того, как будет вести себя атакующий, используя ту или иную тактику.

Процедура – технические подробности при использовании злоумышленником выбранной техники: этапы проведения атаки.

В случае использования APT симуляторов мы точно знаем, какие атаки заложены в тот или иной этап, что позволяет нам лучше понять, какие элементы системы наиболее уязвимы и принять меры по обеспечению их безопасности.

В таблице 1 приведена степень угрозы компьютерной атаки, в зависимости от способа их исполнения.

ТАБЛИЦА 1. Степень угрозы компьютерных атак

Характеристики атаки	Степень угрозы компьютерной атаки		
	APT симуляторы	Атаки, производимые человеком	Генераторы трафика
Сложность воспроизведения	Низкая	Высокая	Средняя
Вариативность	Низкая	Высокая	Низкая
Автоматизация	Высокая	Низкая	Высокая
Предсказуемость	Высокая	Низкая	Средняя
Сложность	Средняя	Высокая	Средняя

Под сложностью воспроизведения понимается количество необходимых навыков и наличие готового вредоносного программного кода, для реализации атаки. Вариативность – количество возможных атак, которые можно реализовать с помощью того, или иного способа. Автоматизация – это качество, которое показывает наличие определённых сценариев, для автоматического выполнения определённых этапов атаки. Предсказуемость в данном контексте относится к понятию, когда атаки или их методы уже известны и защитные механизмы могут легко распознать и заблокировать угрозу. Сложность атаки включает в себя непосредственно качество реализации и изощрённость вредоносной программы.

Исходя из данных в таблице можно сделать вывод, что хоть APT симуляторы и обладают высокой автоматизацией и простотой в воспроизведении, они не могут обеспечивать полною гарантию того, что злоумышленник не сможет взломать систему. Аналогичная ситуация и с генераторами трафика – имея высокую автоматизацию, данный инструмент обладает низкой вариативностью, что позволяет лучше предсказывать поведение данных систем.

В зависимости от поставленной задачи можно использовать те или иные инструменты для обеспечения безопасности системы, но на сегодняшний день идеального решения нет. APT симуляторы за последние годы вобрали в себя множество популярных тактик и техник, но полностью предсказать поведение злоумышленника невозможно.[7] К тому же, все атаки, которые используют эти системы есть в матрице MITRE ATT&CK, и если

злоумышленник будет использовать методы, которые ещё не были обнаружены, то велика вероятность того, что он добьётся успеха.

Список используемых источников:

1. MITRE ATT&CK: что это и как применять в целях кибербезопасности [Электронный ресурс] URL: https://www.anti-malware.ru/analytics/Technology_Analysis/MITRE-ATT-CK-for-cybersecurity-purposes (дата обращения: 21.10.2023).
2. Introduction to CHEIRON, The Adversarial Behavior Simulator [Электронный ресурс] URL: https://tech.somma.kr/APT-Emulators-EN/ (дата обращения: 21.10.2023).
3. Что такое целевая атака: признаки, объекты и последствия [Электронный ресурс] URL: https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-celevaya-ataka-priznaki-obekty-i-posledstviya/ (дата обращения: 21.10.2023).
4. Изучаем Adversarial Tactics, Techniques & Common Knowledge (ATT@CK). Enterprise Tactics. Часть 1-11 [Электронный ресурс] https://habr.com/ru/users/bassmack/publications/articles/ (дата обращения: 21.10.2023).
5. A toolset to make a system look as if it was the victim of an APT attack [Электронный ресурс] URL: https://github.com/NextronSystems/APTSimulator#c2-connects (дата обращения: 21.10.2023).
6. Почему так важно понимать поведение и методы киберпреступников [Электронный ресурс] https://habr.com/ru/articles/650463/ (дата обращения: 21.10.2023).
7. Advanced Persistent Threat – расставляем точки над "i" [Электронный ресурс] https://lib.itsec.ru/articles2/target/advanced-persistent-threat-rasstavlyaem-tochki-nad-i (дата обращения: 21.10.2023).

Taratynov I.

The Bonch-Bruevich Sain-Petersburg State University of Telecommunication

Comparative analysis of solutions for generating computer attacks with specified characteristics.
With the advancement of technology and the availability of various tools, cybercriminals have become increasingly inventive in creating attacks that can cause harm to individual users and organizations. Detecting vulnerabilities requires a tool that will automatically perform the most popular attacks in their various manifestations and leave a "trace" for the vulnerabilities to be addressed in the future.

Key word: APTSimulator, attack tactics and techniques, malware, compromise.

УДК 004.832.38
ГРНТИ 20.15.05

АНАЛИЗ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ ГЛУБОКОГО ОБУЧЕНИЯ НА ПРИМЕРЕ ЗАДАЧИ РАСПОЗНАВАНИЯ РЕЧИ

В. С. Тур
Санкт-Петербургский государственный университет промышленных технологий и дизайна

Данная статья посвящена анализу эффективности алгоритмов глубокого обучения на примере задачи распознавания речи. В ходе исследования будет сформирован краткий обзор на наиболее успешные архитектуры глубоких нейронных сетей и методов, обеспечивающие высокую точность распознавания. Будут выделены основные преимущества и отражена специфика каждого метода.

глубокое обучение, алгоритмы глубокого обучения

Глубокое обучение - область машинного обучения, которое представляет собой нейронную сеть с тремя или более уровнями. Эти нейронные сети призваны имитировать поведения человеческого мозга, позволяя ему «учиться» на больших объемах данных. Глубокое обучение лежит в основе многих приложений и служб искусственного интеллекта (ИИ), которые улучшают автоматизацию, выполняя аналитические и физические задачи без вмешательства человека [1].

Что касается обучения алгоритмов, в процессе они используют неизвестные элементы во входном распределении для извлечения функций, объектов и обнаружения полезных шаблонов данных. Это происходит на нескольких уровнях, используя алгоритмы для построения моделей.

Модели глубокого обучения используют несколько алгоритмов. Хотя ни одна сеть не считается идеальной, некоторые алгоритмы лучше подходят для выполнения конкретных задач. Чтобы выбрать правильные из них, полезно получить четкое представление обо всех основных алгоритмах, которые в рамках задачи распознавания речи могут считаться эффективными.

Основными алгоритмами, которые можно считать эффективными для задач распознавания речи можно считать:

1. Сверточные нейронные сети (CNN);
2. Рекуррентные нейронные сети (RNN);
3. Сверточные рекуррентные нейронные сети (CRNN);
4. Модели с использованием transformers.

сверточные нейронные сети в задачах распознавания речи

CNN основана на математической операции свертки - упорядоченной процедуры смешивания двух источников информации. [2]

CNN обычно состоят из трех слоев: сверточных, объединяющих и полностью связанных. Сверточный слой является основным и содержит все ключевые вычислительные операции. На объединяющем слое объем выходных данных уменьшается для более эффективной дальнейшей

обработки. На связанном слое матрица, полученная на предыдущем слое, преобразуется в вектор столбца, так что модель CNN способна определять ключевые характеристики объектов и в результате классифицировать их.

Преимуществами CNN можно считать:

1. Способность извлекать иерархические признаки из аудиоданных;
2. Способность работать с входными данными различных размеров;
3. CNN обладают хорошей способностью картировать входные аудиофайлы на выходные классы.

В целом, сверточные нейронные сети являются мощным инструментом для обработки и анализа аудиоданных в задачах распознавания речи. Особенно они эффективны в таких задачах:

1. Распознавание речи по изображению графем (когда на вход приходит изображение графемы, представляющей собой графическое представление фонемы). CNN может изучать специфические признаки (края, углы, текстуры) на разных уровнях в слоях свертки;
2. Распознавание речи по спектрограмме (вход: представление спектра аудио);
3. Распознавание речи по волновому представлению (вход: временная последовательность звукового сигнала). CNN может выделять временные шаблоны на разных уровнях в слоях свертки.

В общем случае, если входные данные имеют пространственную структуру, CNN может быть эффективным выбором для задач распознавания речи.

рекуррентные нейронные сети в задачах распознавания речи

Рекуррентные нейронные сети (RNN) — это тип нейронной сети, который используется для анализа последовательных данных [3]. RNN состоят из входных, выходных и скрытых слоев, которые связаны несколькими слоями нейронов. Особенностью рекуррентных или повторяющихся сетей является наличие направленных связей между элементами. Рекуррентные нейронные сети обладают своего рода памятью и могут обрабатывать последовательности данных.

Преимущества рекуррентных нейронных сетей (RNN) в задачах распознавания речи включают следующие:

1. Учет контекста: RNN способны учитывать предыдущий контекст входной последовательности;
2. Долгосрочная зависимость: RNN способны обрабатывать последовательности произвольной длины и сохранять информацию о долгосрочных зависимостях в речи;
3. Адаптация к изменениям: RNN могут адаптироваться к изменениям входных данных и обновлять свои внутренние состояния на основе новой информации;
4. Моделирование вероятности: RNN могут предоставлять вероятности для каждого возможного выходного символа;

5. Эффективность обучения: RNN могут быть эффективно обучены с помощью алгоритма обратного распространения ошибки и алгоритмов оптимизации, таких как стохастический градиентный спуск.

Эффективнее всего использовать RNN для задач распознавания речи, когда важна последовательная зависимость между входными данными. Например:

1. Распознавание и транскрибация речи;
2. Машинный перевод;
3. Определение тональности;
4. Автоматическая генерация речи.

В этих и других задачах, где важна последовательная зависимость данных, RNN обычно показывают лучшие результаты по сравнению с другими типами нейронных сетей, такими как сверточные нейронные сети.

рекуррентные сверточные нейронные сети в задачах распознавания речи

Рекуррентные сверточные нейронные сети совмещают в себе свойства и сверточных и рекуррентных нейронных сетей и используется для обработки последовательных данных.

В CRNN сверточные слои способны извлекать признаки из пространственной информации с помощью сверточных фильтров. Рекурреннтные слои, с другой стороны, позволяют моделировать последовательность входных данных и учитывать контекстную информацию для лучшей классификации или распознавания [4].

Данная архитектура обычно используется как раз для работы с аудио-временными данными, такими как речь и звуковые сигналы. Одним из основных преимуществ сверточных рекуррентных нейронных сетей является их способность обрабатывать последовательные данные и поддерживать пространственную информацию одновременно [5].

Еще одним преимуществом CRNN является их способность эффективно извлекать объекты из входных данных, устраняя необходимость в ручном проектировании объектов.

В целом, CRNN предлагают мощное и универсальное решение для задач, связанных с последовательными и пространственными данными.

Если перечислять конкретные преимущества CRNN для задач распознавания речи, то можно выделить:

1. Учет контекста;
2. Хорошая адаптация к длине входа;
3. Совмещение локальной и глобальной информации;
4. Автоматическое изучение признаков;
5. Высокая точность распознавания;
6. Меньшее количество параметров.

Эффективнее всего использовать CRNN если необходим комбинированный анализ. В некоторых случаях, когда важно анализировать как спектральную, так и временную информацию.

трансформеры в задачах распознавания речи

Трансформеры (Transformer) - это модель машинного обучения, которая применяется в задачах обработки естественного языка, в том числе в задачах распознавания речи.

Базовая архитектура трансформера включает в себя кодер и декодер, основанный на механизме внимания, причем каждый модуль состоит из стека идентичных блоков. Ключевым в вопросе эффективности нейронной сети является механизм внимания [5].

Механизм внимания в трансформерах - это способность модели автоматически фокусировать свою внимательность на наиболее важных элементах входных данных.

В трансформерах внимание реализовано с помощью механизма под названием "Scaled Dot-Product Attention" (взвешенное скалярное произведение внимания). Он представляет собой математическую операцию, которая вычисляет веса для каждого элемента входных данных в соответствии со значимостью этого элемента для распознавания или генерации выхода модели.

Механизм внимания в трансформерах основывается на трех ключевых компонентах:

1. Запросы (Queries) - это векторы, которые представляют текущий временной шаг модели и которые сравниваются с остальными векторами для определения их значимости;
2. Ключи (Keys) - это векторы, которые представляют каждый элемент входных данных и используются для сравнения с запросами;
3. Значения (Values) - это векторы, которые содержат информацию о каждом элементе входа и используются для генерации выхода модели.

Каждая пара запрос-ключ сравнивается с помощью скалярного произведения и проходит через softmax-функцию для получения весов. Веса затем умножаются на соответствующие значения и суммируются для обновления выхода модели.

Этот механизм позволяет трансформеру сосредоточиться на наиболее релевантных частях входных данных и учитывать их в процессе обработки и генерации выхода. Он является одним из ключевых элементов, обеспечивающих высокую производительность и качество моделей на большом количестве задач обработки естественного языка и распознавания речи

Трансформеры имеют преимущество в понимании речи, поскольку они анализируют все предложение одновременно, тогда как RNN или вовсе CRNN обрабатывает вводимые слова одно за другим.

Сравнительный анализ алгоритмов глубокого обучения в задачах распознавания речи

Как уже было сказано, выбор архитектуры зависит от специфики задачи распознавания речи и объема доступных данных для обучения. Выбрать оптимальную архитектуру задача не всегда простая, часто она может быть

достигнута путем комбинирования различных типов сетей и вариаций их слоев, как например сверточная рекуррентная сеть. В таблице 1 отражены самые актуальные и при каких условиях они показывают себя наиболее эффективно:

ТАБЛИЦА 1. Условия наибольшей эффективности архитектур глубокого обучения

Наименование архитектуры	Обозначение	Условия наибольшей эффективности
Сверточные нейронные сети	CNN	Если входные данные имеют пространственную структуру, CNN может быть эффективным выбором для задач распознавания речи
Рекуррентные нейронные сети	RNN	Эффективнее всего, когда важна последовательная зависимость между входными данными.
Сверточные рекуррентные нейронные сети	CRNN	Эффективнее всего если необходим комбинированный анализ. Также эффективны если важно анализировать как спектральную, так и временную информацию.
Трансформеры	Transformer	Эффективнее всего, когда необходимо учитывать контекст и глобальную информацию при обработке аудиосигналов.

Список используемых источников:

1. IBM: What is deep learning [Электронный ресурс] // URL: https://www.ibm.com/topics/deep-learning (дата обращения: 24.10.2023).

2. Романюк А.Г., Смирнов А.Н., Антонова В.М. Использование глубокого обучения нейросети для распознавания голосовых команд пользователя // Журнал радиоэлектроники. 2019. N 11. С 2-3.

3. Simplilearn: deep learning algorithms you should know [Электронный ресурс] // URL: https://www.simplilearn.com/tutorials/deep-learning-tutorial/deep-learning-algorithm (дата обращения: 24.10.2023).

4. Schneppat AI: Convolutional Recurrent Neural Networks [Электронный ресурс] // URL: https://schneppat.com/convolutional-recurrent-neural-networks-crnn.html#:~:text=Convolutional%20Recurrent%20Neural%20Networks%20(CRNN),the%20limitations%20of%20traditional%20models (дата обращения: 24.10.2023).

5. A Review of Deep Learning Techniques for Speech Processing Networks [Электронный ресурс] // URL: https://arxiv.org/abs/2305.00359v3 (дата обращения: 24.10.2023).

Tur V.

Saint Petersburg State University of Industrial Technologies and Design

Analysis of the effectiveness of deep learning algorithms using the example of speech recognition problem.

This article is devoted to the analysis of the effectiveness of deep learning algorithms on the example of the speech recognition problem. In the course of the study, a brief overview of the most successful architectures of deep neural networks and methods that provide high recognition accuracy will be formed. The main advantages will be highlighted and the specifics of each method will be reflected.

Key words: deep learning, neural networks, deep learning algorithms, speech recognition.

УДК 004.056
ГРНТИ 81.93.29

МАСШТАБИРУЕМОЕ HONEYPOT-РЕШЕНИЕ ДЛЯ АНАЛИЗА И УЧЕТА СТАТИСТИКИ СЕТЕВЫХ АТАК

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

В статье описаны принципы работы honeypot-систем и объяснятся их востребованность в сфере информационной безопасности. Представлена теория о зависимости количества и разновидностей сетевых атак от региона. Продемонстрировано масштабируемое решение, которое будет использоваться в качестве исследовательского стенда для анализа сетевых атак и частоты их появления в разных странах с целью изучения данной теории.

honeypot, автоматизация, информационная безопасность, сетевые атаки

В эпоху развивающейся сферы информационных технологий наблюдается значительный рост, особенно в технических аспектах. Заметным фактом является всестороннее использование компьютерных систем с целью автоматизации и увеличения эффективности различных процессов.

Однако, одновременно с этим наблюдается скачок киберпреступности. Происходит все больше различных инцидентов, в которых злоумышленники намеренно искажают информацию или занимаются вторжением в систему с целью получения несанкционированного доступа к персональным данным и срыва бизнес-операций [1, 2].

Одним из таких случаев является атака на Национальный центр готовности к инцидентам и стратегии кибербезопасности (NISC) [3]. На протяжении девяти месяцев никто не замечал нарушений целостности системы, вызванных в результате хакерской деятельности. На протяжении этого времени злоумышленники, имея доступ к электронной почте компании, получали персональные данные тех, кто связывался с центром.

В наши дни подобных случаев все больше и больше. Ежегодно количество кибератак растет. Эти слова подтверждает вице-премьер Российской Федерации Дмитрий Чернышенко [4]. Он утверждает, что за 2023 год атак произошло на 65% больше, чем за весь 2022. Важно отметить следующую информацию: большинство атак предназначались не для нанесения ущерба, а для выявления слабых мест системы, чтобы в последствии эти уязвимости могли быть использованы для дополнительных атак, которые могли привести к сбоям или потере информации.

Для предотвращения подобных атак и инцидентов можно использовать honeypot-системы, специализированные информационные системы, которые предназначены для имитации уязвимых элементов компьютерной сети с целью привлечения внимания злоумышленников [5].

Honeypot-системы давно доказали свою эффективность в качестве ключевого инструмента для обеспечения информационной безопасности, так как позволяют обнаруживать и регистрировать различные события, такие как атаки на веб-приложения, эксплуатация уязвимостей, атаки с повышением привилегий, сканирование сети и другие. Одним из популярных подходов для выявления компьютерных атак является использование преднамеренно ненадёжных систем с предварительно известными уязвимостями. За счет этого, при помощи honeypot-системы можно отслеживать все действия злоумышленников, направленные на нарушение целостности системы, для их дальнейшего анализа, что способствует разработке и внедрению мер по улучшению безопасности компьютерных сетей [6].

В рамках предстоящего проекта планируется разработка honeypot-системы со свободной системой распространения, которая будет размещаться на арендованных серверах в разных странах мира с целью сбора информации об актуальных сетевых атаках и их количестве.

Предполагается, что данный продукт будет использоваться организациям для ведения статистики, отслеживания и изучения новых или уже известных методик нарушения целостности. На основе этой информации компании смогут выбрать наиболее безопасный регион и провайдера вычислительных услуг для размещения своего информационного продукта и оптимальную систему безопасности.

Предлагается ввести модель, которая будет основываться на теории, что количество атак и их разновидности зависят от региона, на котором находится атакуемый объект.

Модель будет иметь следующий вид:

$$A = \{R, P, TA, NA, AS, N\},$$

где A – это зафиксированное событие, направленное на нарушение целостности системы, которое представляет множество, в которое входят R – регион, P – провайдер (поставщик вычислительных ресурсов), TA – тип атаки, NA – сетевая адресация, AS – атакуемый сервис и N – количество атак.

На основе данной модели будут проводиться следующие исследования:

– изучение типов атак, преобладающих в различных странах, и их количество;

– поиск зависимости количества и типа кибератак при смене сетевой адресации в рамках одного провайдера.

Для достижения постеленных целей планируется использование схемы, представленной на рис. 1.

Рис. 11. Схема проекта

Сервер, на котором разворачивается программное обеспечение, имеет прямой доступ в Интернет, чтобы злоумышленники могли непосредственно с ним взаимодействовать. Расположение сервера, а именно странна и IP-адрес, каждый раз будут меняться, что позволит собирать информацию о разновидностях сетевых атак и частоты их появлений в разны регионах для исследования представленной теории.

Схема лабораторного стенда, устанавливаемого на сервер представлена на рис. 2.

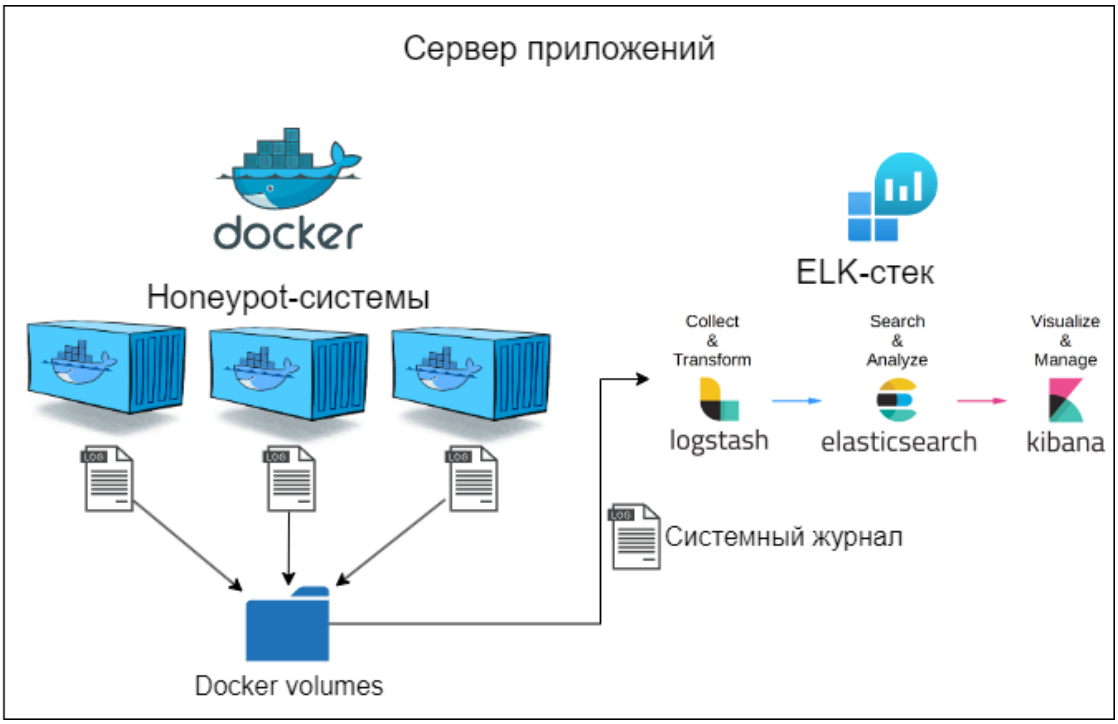


Рис. 12. Схема лабораторного стенда

На данный момент планируются реализация системы при помощи использования Docker-контейнеров, в которых будут размещаться honeypot-системы, например, Endlessh (фиктивный SSH-сервер).

Все системные журналы приманок будут хранится на самой ВМ благодаря томам (volumes) в программном обеспечении Docker, предоставляющих возможность монтировать директории хоста к файловым системам контейнеров. Благодаря этому Logstash, сборщик системных журналов, будет иметь доступ к логам, чтобы в дальнейшем передать их в Elasticsearch, поисковую и аналитическую систему, и визуализировать полученные данные при помощи Kibana.

Данная архитектура является оптимальной, так как имеет возможность для масштабирования системы за счет добавления любых Docker-контейнеров в систему без необходимости конфигурирования самого сервера. Кроме этого, изоляция контейнеров дополнительно снижает риски проникновения на сам сервер приложений, чтобы злоумышленники никак не смогли воздействовать на анализатор логов.

Необходимо отметить, что подобная структура и концепция проекта позволит любому пользователю в автоматизированном режиме разворачивать данный проект, так как для это планируется использование следующих технологий: Terraform для создания виртуальных машин на стороне облачного провайдера, Ansible для удаленного конфигурирования удаленных хостов и Python с целью объединения и автоматизирования всех процессов при создании и конфигурировании хостов.

Данный проект позволит оптимизировать расходы и минимизировать время для изучения различных уязвимостей и атак. На основе полученных данных организация сможет организовать или модернизировать собственную инфраструктуру с учетом современных тенденций в сфере ИБ. Кроме этого, информация, которая будет получена в рамках данного проекта, может оказаться крайне полезной для учета глобальной статистики атак во всем мире, так как на данный момент нет универсального инструмента для этого.

Список используемых источников:

1. The Latest 2023 Cyber Crime Statistics: [Электронный ресурс]. URL: https://aag-it.com/the-latest-cyber-crime-statistics. (дата обращения: 25.10.2023)

2. Актуальные киберугрозы: итоги 2022 года: [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022. (дата обращения: 25.10.2023)

3. В Японии девять месяцев не замечали взлом национального центра кибербезопасности: [Электронный ресурс]. URL: https://iz.ru/1566066/2023-08-29/v-iaponii-deviat-mesiatcev-ne-zamechali-vzlom-natcionalnogo-tcentra-kiberbezopasnosti. (дата обращения: 26.10.2023)

4. Число кибератак на информационные системы России выросло на 65%: [Электронный ресурс]. URL: https://tass.ru/obschestvo/17190435. (дата обращения: 27.10.2023)

5. Ханипот (honeypot): [Электронный ресурс]. URL:https://encyclopedia.kaspersky.ru/glossary/honeypot. (дата обращения: 27.10.2023)

6. 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. N 3. С. 86-97.

Ursegov A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Scalable honeypot solution for analyzing and recording network attack statistics.
The article describes the operating principles of honeypot systems and explains their relevance in the field of information security. Presented a theory about the dependence of the number and types of network attacks on the region. A scalable solution has been demonstrated that is going to be used as a research bench to analyze network attacks and the frequency of their occurrence in different countries in order to study this theory.

Key words: honeypot, automation, information security, network attacks.

УДК 004.056.5
ГРНТИ 81.93.29

СОВРЕМЕННАЯ SIEM-СИСТЕМА: ЧТО ВАЖНО ДЛЯ ЭФФЕКТИВНОГО ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ

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

В статье рассматриваются вопросы контроля состояния информационной безопасности в организациях с использованием SIEM-систем. Проводится анализ принципов работы SIEM-системы. Представлена функциональная модель современной SIEM-системы и рассмотрены ее ключевые возможности. Выбраны основные показатели эффективности SIEM-системы, способствующие повышению качества ее работы. Определены дальнейшие перспективы и тенденции развития SIEM-систем.

информационная безопасность, информационные системы, SIEM-система, корреляция данных, показатели эффективности, защита информации

Введение

В связи с увеличением количества кибератак на информационные ресурсы организаций в Российской Федерации, все большее число руководителей признают необходимость внедрения современных средств защиты информации (ЗИ), таких как: модули комплексной системы защиты информации, системы предотвращения утечки данных, системы управления информацией и событиями безопасности (SIEM-системы). Эти средства ЗИ подробно рассматривались в статье «Сравнение способов контроля состояния информационной безопасности на предприятии» [1]. Сравнительный анализ показал, что наиболее приемлемым подходом для большинства организаций является внедрение SIEM-системы.

Механизм работы SIEM-системы

Необходимость в мониторинге и реагировании на инциденты становится базовой потребностью для организаций.

В отличие от других способов контроля состояния информационной безопасности, SIEM-система способна в автоматизированном режиме осуществлять сбор информации из отдельных источников в корпоративной сети (операционных систем, баз данных, антивирусных средств, межсетевых экранов, сканеров уязвимостей, систем обнаружения вторжений и др.), приводить полученные данные к общему виду, анализировать их, выявлять потенциальные угрозы, фиксировать инциденты и оповещать сотрудников служб информационной безопасности (ИБ) и информационных технологий (ИТ), предоставляя необходимую для проведения расследования информацию.

SIEM-система предназначена для обработки потока событий, выявления инцидентов ИБ и реагирования на них. Механизмы SIEM-системы позволяют производить сбор, фильтрацию, классификацию, агрегацию, корреляцию

событий, хранение, а также визуализацию данных (в том числе генерацию отчетов) и отправку предупреждений в режиме реального времени, тем самым, повышая эффективность обработки инцидентов, экономя время и ресурсы специалистов ИБ [2].

Ключевые компоненты SIEM-системы

Функциональная модель SIEM-системы представлена на рис. 1.

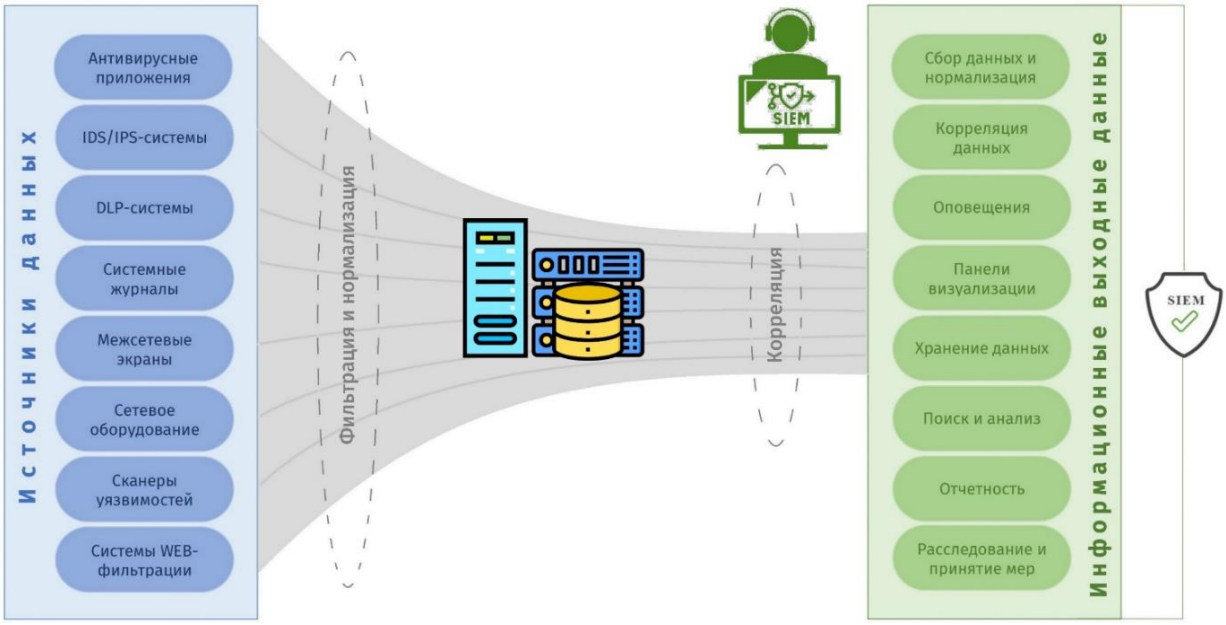


Рис. 1. Функциональная модель SIEM-системы

Ключевые функциональные возможности современных SIEM-систем приведены в таблице 1.

ТАБЛИЦА 1. Функциональные возможности SIEM-систем

№	Функции	Описание	Способы оптимизации
1	Сбор данных, нормализация	От источников, указанных на рисунке 1, автоматизировано обеспечивается сбор данных, их агрегация и обработка с помощью фильтров и правил, что позволяет получить полную картину происходящего в информационной системе организации [3].	Возможность собирать любые события, а также их нормализовать в зависимости от потребностей сотрудников службы ИБ, т.е. определять, какие поля необходимы для поступившего события. Возможность автоматизи-рованно подключать новые источники событий по мере их появления в сети организации.
2	Корреляция	Правила корреляции представляют собой набор логических условий и шаблонов, которые позволяют анализировать и сопоставлять данные разнообразных событий из множества источников информации.	Снизить количество ложных срабатываний и улучшить точность обнаружения инцидентов возможно при регулярной донастройке правил корреляции, то есть создании новых и редак-тировании существующих.

№	Функции	Описание	Способы оптимизации
		Главная цель правил корреляции – выявление скрытых угроз, которые могли бы остаться незамеченными при обычном мониторинге [4].	
3	Оповещение	При обнаружении инцидента ИБ, выполняется немедленное извещение служб безопасности о возможной угрозе ИБ с помощью индикации на консоли управления SIEM, e-mail, SMS, веб-интерфейса и т.д. [5].	Создание рекомендаций по реагированию на выявленные инциденты, их расследованию и обработке. Базой таких рекомендаций может быть внутренняя экспертиза или правила реагирования, добавленные в систему.
4	Реагирование	Современные SIEM могут автоматически выполнять действия, предписанные политиками безопасности и установленными правилами с использованием решения по оркестрации, автоматизации и реагирования на инциденты безопасности (система SOAR).	Возможность интеграции SIEM с системами других классов, например SOAR. В то время как SIEM собирает и анализирует события, выявляя инциденты ИБ, SOAR использует полученные данные для принятия ответных мер и в автоматическом режиме выполняет правила и сценарии реагирования, отвечающие потребностям организации.
5	Визуализация	Механизм, позволяющий отображать на графических панелях большие объемы информации о состоянии безопасности в форме перечней, таблиц, графиков различных типов и форматов и пр. Благодаря этому, можно сократить трудозатраты сотрудников и время принятия решений по поступающей информации.	Предоставление интуитивно понятного интерфейса и визуализации данных, улучшение пользовательского опыта поможет аналитикам безопасности лучше воспринимать информацию, ускоряя процесс обнаружения и реагирования на инциденты.
6	Хранение данных	Функция для расследований, анализа, экспертиз инцидентов за прошлые периоды, с целью выявления отклонений, а также проверки соответствия систем управления ИБ существующим нормам и требованиям, в том числе политике информационной безопасности (ПИБ) организации [6,7].	Применение различных настроек по условиям и длительности хранения, что особенно эффективно в ситуациях с большим разнообразием систем-источников. Периодический пересмотр ПИБ на основании анализа, отчетов, мониторинга и аудита, с учетом новых угроз.
7	Поиск и	В рамках расследований	Возможность отслеживать

№	Функции	Описание	Способы оптимизации
	анализ	инцидентов ИБ производится контекстный поиск. Выполняется анализ собранных данных с использованием заданных правил и политик безопасности, что позволяет внести улучшения в систему защиты информационных ресурсов организации.	жизненный цикл инцидента, объединять в одно расследование несколько событий, присваивать статусы хода расследования, добавлять комментарии и подводить итоги. По результатам расследований можно создавать новые правила корреляции.
8	Отчетность	Для периодического информирования о текущих событиях, инцидентах, трендах производится формирование настраиваемых отчетов с различной степенью детализации.	Возможность создания промежуточной отчетности. Наличие таких функций, как: предустановленные отчеты, встроенный конструктор отчетов, рассылка отчетов по расписанию, оперативный поиск событий.

Оценка эффективности SIEM-систем

SIEM-система играет важную роль в обеспечении безопасности информации и своевременном обнаружении угроз в организации. Для оценки эффективности функционирования SIEM-систем используются различные критерии и показатели, которые помогают оценить качество ее работы и выявить возможные проблемы.

Чаще всего используются следующие:

– количество выявленных инцидентов;

– среднее время обнаружения и реагирования на инцидент;

– выделение ложных срабатываний;

– наличие модулей прогнозирования;

– корреляция данных;

– эффективность проведенных расследований;

– показатели по улучшению общего уровня безопасности предприятия и уровню снижения финансовых потерь;

– выполнение требований законодательства, стандартов и ПИБ;

– стабильность работы системы;

– устойчивость SIEM-системы к сбоям и ее защищенность от компрометации.

Если SIEM-система работает неэффективно, то в первую очередь это сказывается на полноте сбора событий и возможности дальнейшей работы с ними. В дальнейших исследованиях планируется расширение списка показателей эффективности для SIEM-системы в организации и формирование соответствующих оценочных критериев.

Перспективы в развитии SIEM-систем

В условиях постоянно меняющихся угроз, требующих соответствующего и оперативного реагирования, развитие и расширение

функционала SIEM-систем это задачи, цель которых – соответствие решения актуальным потребностям рынка.

Основными трендами на рынке SIEM-систем являются автоматизация подключения инфраструктуры для мониторинга, использование технологий машинного обучения и искусственного интеллекта (ИИ) для анализа событий и построения цепочек атак, а также возможность совместной работы с другими системами безопасности, участвующими в процессе выявления аномальных событий и анализа зарегистрированных инцидентов, для обеспечения полного цикла защиты информации.

Хорошей перспективой было бы совершенствование алгоритмов таким образом, чтобы непосредственное участие человека было минимальным [8].

Существенным преимуществом использования технологий ИИ и машинного обучения в SIEM-системах является автоматизация процесса анализа данных, повышение точности обнаружения инцидентов, снижение количества ложных срабатываний, выявление скрытых угроз и аномалий, оптимизация реагирования на инциденты, и как следствие снижение нагрузки на аналитиков при работе с системой.

Машинное обучение позволит в десятки раз сократить объем информации, требующий внимания специалистов, уменьшит время анализа для оставшихся событий и снизит требования к компетенции сотрудников.

Интеграция ИИ в SIEM-системы расширяет их возможности и повышает эффективность обнаружения и реагирования на кибератаки. Самое большое ограничение для развития использования технологий ИИ – это необходимость большого количества данных для обучения, времени и вычислительных мощностей.

SIEM-системы в ближайшие годы будут дополняться возможностями автоматизации и широко интегрироваться с другими решениями по безопасности.

Заключение

В реалиях сегодняшнего дня кибербезопасность является одним из ключевых аспектов эффективного развития бизнеса, а построить надежную защиту организации довольно сложно без внедрения эффективной SIEM-системы, являющейся важным элементом, вокруг которого выстраиваются процессы мониторинга и реагирования на инциденты.

Список используемых источников:

1. Бабков И. Н., Федорова З. А. Сравнение способов контроля состояния информационной безопасности на предприятии // Подготовка профессиональных кадров в магистратуре для цифровой экономики : материалы Всерос. научно-технич. и научно-методич. конф., магистрантов и их руководителей. СПб. : СПбГУТ, 2023. Т. 1. С. 433–437.

2. Власова А. В., Дударев В. А., Новикова Т. И. Обзор основных решаемых задач и архитектуры типового SIEM-решения // Инновационные научные исследования в современном мире : материалы IX Междунар. научно-практич. конф., Уфа, 22 нояб. 2022 г. Научно-издательский центр «Вестник науки». 2022. Часть 2. С. 185-189.

3. Зарубин С.В., Оболонская А.В., Мелузов Г.В. Специфика функционирования систем управления инцидентами безопасности // Охрана, безопасность, связь. 2022. N 7-2.

С. 17-23.

4. Порошин В. SIEM «Платформа Радар»: 600 тысяч событий в секунду с новым коррелятором // Information Security/Информационная безопасность. 2023. N 4. С. 18-19.

5. Котенко И. В., Паращук И. Б. Модель системы управления информацией и событиями безопасности // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2020. N 2. С. 84-94.

6. Бабков И. Н., Федорова З. А. Политика информационной безопасности – инструмент повышения эффективности защиты информации на предприятии // Фундаментальные и прикладные исследования: концепты, методики, новации : vатериалы VI Всерос. научно-практич. конф., Ростов-на-Дону, 12–13 мая 2022 г. Ростов-на-Дону : Профпресслит. 2022. С. 45-49.

7. Кузнецова А. Д., Сахаров Д. В. Обзор состояния исследований информационной безопасности и применение SIEM-систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы VIII Междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 27–28 фев. 2019 г. СПб. : СПбГУТ. 2019. Т. 1., С. 626-631.

8. Акишев О., Виткова Л., Вылегжанин Д., Дашков А., Лагутина Е., Маркелов И., Порошин В. и др. SIEM: в поиске совершенства в безопасности // Information Security. Информационная безопасность. 2023. N 4. С. 32-37.

Fedorova Z.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Today's SIEM system: focus on the most important issues for effective incident detection.
The article discusses the issues of information security control in organizations using SIEM-systems. It provides an analysis of the working principles of SIEM-systems. It presents a functional model of a modern SIEM-system and considers its key features. The article defines the main indicators of SIEM-system efficiency, contributing to the quality of its work. Defined further perspectives and trends in the SIEM-systems development.

Key words: information security, information systems, SIEM-systems, data correlation, effectiveness indicators, information protection.

УДК 004.056.57
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ В ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID

В. А. Фомичев
Санкт-Петербургский государственный университет промышленных технологий и дизайна

Операционная система Android - это одна из самых популярных платформ для мобильных устройств в мире. Её популярность привела к активному развитию приложений и сервисов, но также сделала её целью для злоумышленников. С учетом постоянных изменений в архитектуре и быстрого технологического развития, безопасность Android стала крайне важной.

android, безопасность, уязвимости, угрозы, мобильные устройства, мобильные приложения

В последние годы операционная система Android утвердила свое господство на рынке мобильных устройств. Несмотря на активные усилия Android в области усовершенствования механизмов безопасности и исправления уязвимостей в ходе обновления своей версии, новые уязвимости продолжают возникать. Эксплуатация этих уязвимостей является распространенным методом для получения расширенных привилегий в операционных системах Android.

Для более полного и глубокого понимания этой проблемы, в данной статье мы представляем обзор публичных эксплойтов для устройств, работающих на Android. Исходя из анализа реальных эксплойтов, мы разрабатываем классификацию эксплойтов для Android и выявляем сходства и различия, а также преимущества и недостатки различных видов эксплойтов.

С другой стороны, мы также проводим оценку выбранных эксплойтов на наших тестовых устройствах. Исходя как из теоретического анализа, так и из результатов экспериментов, мы выражаем свое мнение о ситуации с эксплуатацией Android.

Изменения в категориях эксплойтов на временной шкале отражают три основные тенденции:

Отдельные эксплойты все больше зависят от конкретных устройств и версий операционной системы;

Количество эксплойтов, нацеленных на настройки производителей устройств, постоянно растет, в то время как рост других видов эксплойтов замедляется;

Повреждение памяти постепенно становится основным способом инициирования эксплуатации;

Современные смартфоны и планшеты стали неотъемлемой частью повседневной жизни людей. С развитием мобильных технологий и

доступностью интернет-сервисов, интеллектуальные мобильные устройства превратились в важных цифровых спутников, которые используются людьми для получения информации, обмена сообщениями, социальных сетей, онлайн-банкинга и многих других интернет-сервисов.

Операционная система Android занимает доминирующее положение на рынке мобильных устройств. С момента её выпуска в 2008 году доля рынка устройств с Android постоянно растет. Согласно последней статистике IDC [1] на первый квартал 2017 года, Android удерживает 85,0% мирового рынка смартфонов. При этом с 2015 года годовые поставки новых устройств Android увеличиваются в среднем на 10%.

Из-за высокой популярности мобильных устройств и особенно Android, вопросы конфиденциальности и безопасности привлекают большое внимание как со стороны пользователей, так и специалистов в области информационной безопасности. Android также становится целью злоумышленников, и несмотря на усиление механизмов безопасности и регулярные обновления, уязвимости Android продолжают появляться и использоваться для получения несанкционированного доступа к устройствам.

Эксплуатация уязвимостей является распространенным методом для получения повышенных привилегий в системах Android. Злоумышленники и исследователи безопасности давно интересуются взломом Android, начиная с момента его появления в 2008 году. Программы-эксплойты могут помочь пользователям обойти механизмы безопасности своих устройств Android, например, для получения прав администратора (рут-прав) или могут использоваться злоумышленниками для несанкционированного доступа к данным и финансовым ресурсам пользователей.

Список используемых источников:

1. Joshua Swingle et al. IDC: Android Captures 85% Of Smartphone Market In Q1 2017 [Электронный ресурс] // Android headliners. URL: https://www.androidheadlines.com/2017/07/idc-android-captures-85-of-smartphone-market-in-q1-2017.html (дата обращения: 14.10.2023).

2. Уязвимости Android 2020 [Электронный ресурс] // habr. URL: https://habr.com/ru/companies/otus/articles/547160/ (дата обращения: 14.10.2023).

Fomichev V.

Saint Petersburg State University of Industrial Technologies and Design

Vulnerability research in android operating system.

The Android operating system is one of the most popular mobile device platforms in the world. Its popularity has led to the rapid development of applications and services, but it has also made it a target for attackers. With constant changes in architecture and rapid technological development, Android security has become extremely important.

Key words: android, security, security, vulnerabilities, threats, mobile devices, mobile applications

УДК 004.056
ГРНТИ 49.33.29

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЦИФРОВОГО МИРА: КОМПЛЕКСНОЕ РУКОВОДСТВО ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Хамед Мохамед. М, С. И. Штеренберг
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В современном все более взаимосвязанном и цифровом мире нельзя недооценивать важность информационной безопасности. Сразвитием технология возрастают и угрозы и уязвимости, которые могут подвергнуть опасности конфиденциальные данные и цифровые активы. Это комплексное руководство глубоко исследует мир информационной безопасности, предоставляя понимание ее основ, актуальной угрозой ситуации, передовых практик и взгляд в будущее этой важной области.

Безопасность, информационная безопасность, угроза, цифровой мир, опасность

В эпоху, когда цифровые технологии проникают во все сферы нашей жизни, обеспечение безопасности информации не имеет альтернативы. Информационная безопасность, часто называемая InfoSec, представляет собой практику защиты данных, систем и сетей от несанкционированного доступа, раскрытия, изменения или уничтожения. Это комплексное руководство направлено на исследование глубоких аспектов информационной безопасности, предоставляя понимание её основ, развивающейся угрозной ситуации, передовых практик и взгляд в будущее этой важной области [1].

Информационная безопасность охватывает несколько ключевых принципов [2]:

Конфиденциальность: гарантия, что информация доступна только для авторизованных лиц

Целостность: обеспечение точности и целостности данных;

Доступность:обеспечение доступности информации по требованию;

Аутентификация и авторизация:проверка личности пользователей и управление их доступом;

Управление рисками:оценка и управление рисками в области безопасности;

Политики и процедуры безопасности: установление фреймворков для мер безопасности.

Информация представляет собой ценный актив, и её нарушение может иметь серьезные последствия, включая финансовые убытки, ущерб репутации и даже национальную безопасность.

Изучение истории информационной безопасности позволяет понять её эволюцию. В частности можно выделить следующие этапы [3]:

Криптография в Древние времена: древние цивилизации использовали коды и шифры для обеспечения безопасной связи;

Вторая Мировая Война и Энигма: взлом кода Энигма подчеркнул важность криптографии в разведке во время войны;

Эра компьютерной безопасности: начальные меры безопасности компьютеров фокусировались на физическом контроле доступа;

Эра интернета и киберугрозы: рост интернета создал новые вызовы в области безопасности.

Следует также выделить общие угрозы информационной безопасности [4]:

Вредоносное ПО: вирусы, трояны, черви и вымогательское ПО могут нарушить работу систем и украсть данные;

Атаки по перехвату: обманчивые тактики направлены на обман пользователей и получение от них чувствительной информации;

Атаки DoS и DDoS:перегрузка системы или сети с целью недоступности;

Утечки данных: несанкционированный доступ к базам данных ведёт к утечке данных;

Внутренние угрозы:работники или партнёры могут злоупотреблять своим доступом.

Несмотря на общие угрозы в современном мире также следует определить и новые угрозы, такие как [5]:

Атаки с использованием ИИ и машинного обучения: злоумышленники используют искусственный интеллект и машинное обучение для сложных автоматизированных атак;

Проблемы безопасности интернета вещей:распространение устройств IoT (интернета вещей) вводит новые уязвимости;

Блокчейн и информационная безопасность:поднимается вопрос о безопасности в контексте использования блокчейна.

Важно отметить, что ошибки человека и социальная инженерия вносят значительный вклад в нарушения, среди которых [6]:

Социальная инженерия: злоумышленники манипулируют людьми для получения конфиденциальной информации;

Осведомленность о фишинге: программы обучения о фишинге обучают сотрудников распознавать и реагировать на подобные атаки;

Анализ поведения пользователей: инструменты помогают выявлять необычные паттерны активности, указывающие на нарушения безопасности.

Основы информационной безопасности [7]:

Принципы информационной безопасности – информационная безопасность руководствуется основными принципами: конфиденциальность, целостность, доступность, аутентификация, авторизация, управление рисками и политики безопасности;

Тройственность (CIA Triad) – подчеркивает важность конфиденциальности, целостности и доступности, обеспечивая баланс

между этими принципами;

Защита в глубину (DefenseinDepth) –защита в глубину предполагает использование нескольких мер безопасности для защиты от различных угроз и снижения рисков.

В политике и практике информационной безопасности следует выделить следующее [8]:

Разработка политики информационной безопасности – организации должны создать фреймворк политики безопасности, провести оценку рисков и классификацию данных для разработки эффективных политик информационной безопасности;

Управление доступом на основе ролей – управление доступом на основе ролей назначает разрешения на основе ролей пользователей, следуя принципу наименьших привилегий;

Шифрование и защита данных – шифрование данных в пути и на хранении и внедрение планов резервного копирования и восстановления данных имеют решающее значение для защиты данных.

Следует также иметь ввиду технологии и инструменты кибербезопасности [9]:

Брандмауэры и системы обнаружения вторжений – защищают сети от несанкционированного доступа и мониторят подозрительную активность;

Антивирусное и анти-малварное ПО – обеспечивают защиту от известных сигнатур вредоносных программ и различных видов вредоносного ПО;

Системы управления информацией о безопасности (SIEM) – решения SIEM собирают и анализируют данные о безопасности, помогая выявить и реагировать на инциденты безопасности в реальном времени.

В каждом случае необходимо реагирование на инциденты и восстановление. К ним относится [10]:

Подготовка к кибератакам–организации должны иметь план реагирования на инциденты, команду реагирования на инциденты и проводить регулярные тесты и учения;

Обнаружение и реагирование на инциденты – обнаружение, ограничение, ликвидация инцидентов и тщательное расследование - важные шаги в реагировании на инциденты;

Восстановление и уроки, извлеченные из инцидентов – восстановление, документирование и непрерывное усовершенствование - критические шаги после инцидентов для организаций.

Невозможно оставить без внимания и тренды в информационной безопасности [7]:

Искусственный интеллект в кибербезопасности и машинное обучение все чаще используются для выявления угроз в реальном времени и автоматизированного реагирования на инциденты;

Проблемы безопасности интернета вещей – рост числа устройств Интернета вещей вводит новые уязвимости, которые необходимо учитывать;

Блокчейн и информационная безопасность –блокчейн повышает целостность данных и представляет возможности и вызовы, особенно в использовании криптовалют.

Необходимо также обратить внимание на соблюдение и правовые аспекты [7]:

GDPR и защита данных – накладывает строгие требования по защите данных на организации, обрабатывающие персональную информацию;

HIPAA и защита медицинской информации – устанавливает стандарты для защиты медицинских данных, требуя от медицинских организаций внедрения мер безопасности;

Киберзащита и соблюдение – различные отрасли имеют отраслевые регуляции по кибербезопасности, чтобы обеспечить соблюдение мер безопасности, невыполнение которых влечет за собой серьезные последствия.

Важно не забывать о практиках информационной безопасности, таких как [5]:

Обучение и привлечение сотрудников к проблемам безопасности – регулярные программы обучения по безопасности неотъемлемы для информирования сотрудников о существующих угрозах и безопасных практиках. Эти программы обучают персоналу распознавать и реагировать на угрозы безопасности, такие как фишинговые письма или атаки методом социальной инженерии. Они также подчеркивают важность соблюдения протоколов безопасности и лучших практик;

Регулярные аудиты и оценки безопасности – проведение регулярных аудитов и оценок безопасности имеет важное значение для организаций. Сканирование на уязвимости и пенетрационное тестирование - это методы, которые используются для выявления и устранения уязвимостей безопасности.

Сканирование на уязвимости помогает выявить слабые места в программном обеспечении, системах или сетях, а пенетрационное тестирование моделирует атаки в реальных условиях для оценки уровня безопасности организации;

Культура совместной безопасности – стимулирование культуры совместной безопасности в организации побуждает сотрудников принимать активное участие в обеспечении безопасности. Это подразумевает общую ответственность, при которой каждый сотрудник играет роль в защите чувствительных данных и в сообщении о событиях безопасности. Крепкая безопасностная культура способствует повышению осведомленности, сотрудничеству и соблюдению протоколов безопасности.

Будущее информационной безопасности заключается в следующих аспектах:

Эволюция ландшафта угроз – ландшафт угроз постоянно эволюционирует, поскольку киберпреступники разрабатывают более сложные методы атак. Этот подраздел подчеркивает необходимость для организаций оставаться бдительными и адаптироваться к новым угрозам.

Он отмечает, что угрозы станут все более сложными и разнообразными, требуя применения продвинутых мер безопасности и стратегий;
Ожидаемые технологические достижения – в этом подразделе обсуждается роль предстоящих технологий в информационной
безопасности. Упоминаются квантовые вычисления, кибербезопасность на основе искусственного интеллекта и вычисления на периферийных устройствах. Квантовые вычисления могут нарушить существующие методы шифрования, что потребует новых средств безопасности.

Искусственный интеллект будет использоваться для выявления и реагирования на угрозы в реальном времени. Вычисления на периферийных устройствах представляют вызовы в области безопасности, так как обработка данных будет происходить на устройствах, а не на централизованных серверах;

Роль профессионалов в области кибербезопасности–поскольку растет спрос на квалифицированных специалистов в области кибербезопасности, становится важным постоянное обучение и повышение квалификации. В этом подразделе подчеркивается значение того, чтобы специалисты в области кибербезопасности оставались в курсе новых угроз и технологий. Также акцентируется важность прохождения сертификаций и постоянного обучения для удовлетворения требований быстро меняющейся области кибербезопасности.

На основе изложенного выше следует заключить, что информационная безопасность имеет первостепенное значение в цифровой эпохе. Она охватывает фундаментальные принципы, динамичный ландшафт угроз, соблюдение и лучшие практики, а также перспективы развития новых технологий. Поскольку организации и частные лица всё больше полагаются на цифровые технологии, обеспечение безопасности данных, систем и сетей становится постоянной задачей. Будущее информационной безопасности представляет вызовы и возможности, требуя бдительности, адаптации и сотрудничества для защиты цифрового мира.

Список используемых источников:

1. Смит Д. Введение в Информационную Безопасность [Электронный ресурс] // Издательство ABC. 2020. URL: selfpub.ru/?utm_source=yandex&utm_medium=cpc&utm_campaign=izdatelstvo_
poisk&utm_content=utp5&utm_term=электронные%20издательства&yclid=447823002484
342783 (дата обращения: 05.10.2023).

2. Джонсон М. Ландшафт Угроз в Кибербезопасности: Тенденции и Вызовы // Журнал Кибербезопасности. 2019. N 8 (2). С. 45-62.

3. Лучшие Практики по Защите Устройств Интернета Вещей [Электронный ресурс] // Агентство Кибербезопасности и Инфраструктуры (CISA). 2022. URL://ozuz.ru/luchshie-praktiki-v-oblasti-kiberbezopasnosti-zashhita-vashih-cifrovyhaktivov/?
ysclid=lnseun2ozu499639948 (дата обращения: 06.10.2023).

4. Смит Э. Будущая Роль Профессионалов в Кибербезопасности: Вызовы и Возможности // Журнал Кибербезопасности. 2019. N 15(4). С. 321-335.

5. Андерсон Д. Влияние ИИ на Кибербезопасность // Международная Конференция по Кибербезопасности. 2021. (ICC). С.123-140.

6. Общее Регулирование по Защите Данных [Электронный ресурс] // Европейский Союз.

2018. URL:ru.wikibrief.org/wiki/General_Data_Protection_Regulation (дата обращения: 07.10.2023).

7. Закон о Переносимости и Ответственности в Области Здравоохранения [Электронный ресурс] // Министерство Здравоохранения и Социальных Служб США. 2009. URL: ranslated.turbopages.org/proxy_u/en-ru.ru.d16feef3-652cc007-03fd9364-74722d776562/https/htm.fandom.com/wiki/Health_Insurance_Portability_and_Accountability_Act (дата обращения 08.10.2023).

8. NIST Кибербезопасности [Электронный ресурс] // Национальный Институт Стандартов и Технологий. 2018. URL: www.nist.gov/cybersecurity (дата обращения: 09.10.2023).

9. Квантовые Вычисления и Квантовая Криптография [Электронный ресурс] // Национальный Институт Стандартов и Технологий. 2020. URL: moscowtest. ru/content/kvantovye-vychisleniya-i-kvantovayakriptografiya?ysclid=lnsf08ar43462915551 (дата обращения: 10.10.2023).

10. Программы Сертификации в Области Кибербезопасности [Электронный ресурс] // Международная Ассоциация Профессионалов в Области Кибербезопасности. 2021. URL:habr.com/ru/articles/746154/ (дата обращения: 11.10.2023).

Hamed Mohamed M., Shterenberg S.

Ensuring the security of the digital world: comprehensive guide to information security In today's increasingly interconnected and digital world, the importance of information security cannot be underestimated. With the development of technology, threats and vulnerabilities that can endanger confidential data and digital assets are increasing. This comprehensive guide deeply explores the world of information security, providing an understanding of its fundamentals, the current threat of the situation, best practices and a look into the future of this important area.

Key words: Security, information security, threat, digital world, danger.

УДК 004.056.53
ГРНТИ 81.93.29

МЕТОДИКА ОПРЕДЕЛЕНИЯ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ КИБЕРУГРОЗ С ИСПОЛЬЗОВАНИЕМ HONEYPOT

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

В современном информационном обществе, сфера кибербезопасности приобретает все более критическое значение. Вместе с увеличением сложности атак, появляется потребность в эффективных методах для их выявления и предотвращения. Одним из перспективных средств для анализа киберугроз являются honeypot- технологии. Honeypot представляет собой вымышленный или уязвимый компьютер/файл, предназначенный для привлечения атакующих и анализа их методов. В данной статье предлагается методика определения вероятности реализации киберугроз с использованием honeypot-технологий.

информационная безопасность, кибератаки, стратегия защиты, ловушка для хакеров, сетевая безопасность, угрозы

В современном мире информационных технологий, вопросы кибербезопасности приобретают критическое значение. С развитием технологий атаки становятся все более сложными и изощренными. В связи с этим возникает неотложная необходимость в эффективных методах выявления и предотвращения киберугроз. Одним из перспективных инструментов в этой области являются технологии honeypot.

Целью данного исследования является разработка методики, позволяющей точно определить вероятность реализации киберугроз с использованием технологии honeypot. Для достижения этой цели предполагается решение следующих задач:

1. Проведение комплексного обзора существующей литературы по теме технологии honeypot и оценке киберугроз.
2. Реализация и конфигурирование honeypot-систем в контролируемых средах для сбора актуальных данных.
3. Анализ собранных данных с целью выявления закономерностей и тенденций в поведении киберугроз.
4. Формирование вероятной модели для оценки вероятности реализации киберугроз на основе данных, полученных с honeypot.

Обзор литературы будет охватывать широкий спектр источников, включая научные статьи, отраслевые отчеты и экспертные анализы. Основные аспекты включают:

- Технология Honeypot: этот раздел затронет основы honeypot, их классификацию и роль в кибербезопасности. Также будут рассмотрены различные стратегии развертывания и их эффективность в привлечении и анализе киберугроз.
- Киберугрозы: проведётся глубокий анализ текущих и новых киберугроз с особенным вниманием к методологиям, целям и

потенциальным последствиям атак. Этот раздел послужит основой для понимания рисков, на смягчение которых направлена технология honeypot.

- Моделирование в кибербезопасности: в этом разделе будет рассмотрено существующие подходы к моделированию в области кибербезопасности. Будет оцениваться их применимость к конкретному контексту использования данных honeypot для анализа угроз [1].
- Практические применения: будут рассмотрены реальные примеры успешного использования технологии honeypot для анализа киберугроз.

Изучение реальных ситуаций предоставит ценные практические знания о применимости предложенной методики.

Кибербезопасность включает в себя комплекс мер и технологий, направленных на защиту информации от несанкционированного доступа, а также предотвращение и реагирование на киберугрозы. Это включает в себя аутентификацию, авторизацию, шифрование, мониторинг сетевой активности и другие методы [2].

Технологии Honeypot представляют собой специально созданные средства, которые имитируют уязвимые ресурсы или системы с целью привлечения потенциальных атакующих. Они делятся на несколько типов в зависимости от целей и способов применения, таких как:

- Low-Interaction Honeypots: эти Honeypot имитируют уязвимости, но не предоставляют реального доступа к системе. Они предназначены для сбора базовой информации о потенциальных угрозах.
- High-Interaction Honeypots: такие Honeypot создают реальные, уязвимые среды, позволяя исследователям наблюдать и анализировать атаки в реальном времени.
- Medium-Interaction Honeypots: следующие предоставляют средний уровень интерактивности, имитируя реальные системы с ограниченными возможностями.

Для эффективного анализа киберугроз необходимо применять различные методы, как мониторинг сетевого трафика, анализ вредоносных программ, применение алгоритмов машинного обучения, исследование сценариев атак.

В диссертации представлены теоретические основы кибербезопасности, а также принципы и типы honeypot-технологий. Кроме того, описаны основные методы анализа киберугроз, которые являются основополагающими для разработки методики определения вероятности их реализации при использовании honeypot-технологий.

Для успешной реализации методики определения вероятности реализации киберугроз необходимо грамотно подходить к выбору и развертыванию Honeypot-системы. При этом следует учитывать следующие аспекты [3]:

I. Выбор типа Honeypot: в зависимости от конкретных целей и характеристик среды необходимо определить, будет ли использоваться low-interaction, high-interaction или medium-interaction Honeypot.

II. Конфигурация Honeypot: настройка Honeypot-системы должна быть проведена с учетом имитации реальной среды и уязвимостей. Это включает в

себя выбор подходящих операционных систем, уязвимостей и поддельных данных.

III. Размещение Honeypot: важно выбрать оптимальное место размещения Honeypot-системы, учитывая возможные точки входа для потенциальных атакующих.

Собранные данные являются основой для последующей оценки вероятности реализации киберугроз. Этап сбора и анализа данных включает в себя следующие шаги [4]:

- Мониторинг активности: система должна непрерывно мониторить взаимодействия с потенциальными атакующими, фиксировать и анализировать их действия.
- Запись событий: регистрация всех событий и взаимодействий с Honeypot-системой позволяет детально анализировать происходящее.
- Анализ паттернов атак: идентификация характерных паттернов и методов атак позволяет выявить угрозы с высокой вероятностью реализации.

На основе собранных данных и анализа атакующих методов, необходимо разработать математическую модель для оценки вероятности реализации киберугроз. Это включает в себя выделение ключевых параметров и характеристик, влияющих на вероятность реализации киберугроз, разработку статистической модели [5], позволяющей количественно оценить вероятность риска, а также тщательную проверку модели и тестирование на различных наборах данных, чтобы удостовериться в ее надежности и точности.

Для проведения экспериментов по определению вероятности реализации киберугроз с использованием технологии Honeypot была создана специальная экспериментальная среда [6]. Основные характеристики среды включают:

- Состав Honeypot-системы: описаны основные характеристики выбранной Honeypot-системы, включая тип, операционную систему, уязвимости и другие параметры.
- Настройки среды: рассматриваются параметры конфигурации, необходимые для создания реалистичной среды, способствующей привлечению потенциальных атакующих.
- Инфраструктура сети: описывается схема сети, включая размещение Honeypot-системы, сетевые сегменты и другие компоненты.

Один из разделов диссертации посвящен подробному описанию проведенных экспериментов. Ключевые аспекты включают выбор сценариев атак (определены типичные сценарии атак, которые могли быть предприняты в отношении Honeypot-системы), мониторинг активности (фиксировались все взаимодействия с Honeypot-системой, включая попытки взлома, сканирования и другие атаки), запись данных (все события и данные, связанные с экспериментами, были документированы для последующего анализа).

В работе также представлены результаты проведенных экспериментов и их анализ. Это включает в себя:

- Статистический анализ данных: произведен анализ собранных данных с использованием статистических методов для выявления закономерностей и особенностей атак.
- Оценка вероятности реализации киберугроз: на основе данных экспериментов разработана методика оценки вероятности реализации киберугроз с использованием Honeypot.
- Сравнение с традиционными методами [7]: результаты были сопоставлены с традиционными методами анализа киберугроз для оценки эффективности предлагаемой методики.

Эксперименты и их анализ играют ключевую роль в разработке и проверке методики определения вероятности реализации киберугроз с использованием Honeypot. Полученные результаты обеспечивают основу для дальнейших рекомендаций и стратегий по обеспечению кибербезопасности.

Разработанная методика определения вероятности реализации киберугроз с использованием технологии Honeypot представляет собой мощный инструмент в области кибербезопасности. Для успешного применения данной методики в реальных условиях рекомендуется следующее:

- Выбор оптимального Honeypot: в зависимости от специфики организации и среды, необходимо выбрать тип Honeypot, наиболее эффективно соответствующий потребностям.
- Регулярное обновление уязвимостей: важно периодически обновлять уязвимости в Honeypot-системе, чтобы сохранять реалистичность среды.
- Анализ результатов в реальном времени [8]: важно проводить мониторинг активности на Honeypot-системе, реагируя на потенциальные угрозы в реальном времени.

Непрерывное совершенствование методики является неотъемлемой частью обеспечения кибербезопасности. Для оптимизации и улучшения методики рекомендуется рассмотреть следующие аспекты: интеграция с другими системами мониторинга, улучшение алгоритмов анализа данных, обучение персонала [9].

Важно понимать, что киберугрозы постоянно эволюционируют [10], и методика должна соответствующим образом развиваться и адаптироваться. Практические рекомендации предоставляют основу для постоянного совершенствования методики и повышения уровня кибербезопасности в организации.

В ходе данного исследования была разработана методика определения вероятности реализации киберугроз с использованием технологии Honeypot. Основные выводы таковы:

1. Honeypot-технологии представляют собой мощный инструмент в анализе киберугроз, позволяя эффективно привлекать и анализировать потенциальных атакующих.
2. Эффективность методики подтверждена экспериментальными исследованиями, где были собраны и анализированы данные о попытках атак на Honeypot-систему.

3. Разработанная методика позволяет количественно оценить вероятность реализации киберугроз на основе собранных данных, что делает ее ценным инструментом для обеспечения кибербезопасности.

Несмотря на достигнутые результаты, существует несколько направлений для дальнейших исследований:

- Расширение набора данных: проведение более обширных экспериментов на различных типах Honeypot-систем и в разных средах для улучшения надежности методики.
- Интеграция с системами безопасности: разработка методов интеграции разработанной методики с другими средствами обеспечения кибербезопасности.
- Адаптация к новым угрозам: с учетом постоянно меняющейся обстановки, необходимо постоянное обновление методики для эффективной защиты.
- В заключении следует отметить, что разработанная методика представляет собой значимый вклад в область кибербезопасности. Ее применение в реальных условиях может существенно улучшить защиту информационных систем от потенциальных угроз.

Список используемых источников:

1. Шнайер Б. Данные и Голиаф: Скрытая борьба за ваши данные и контроль над своим миром, У. W. Norton Company, 2015.
2. Гребенников В. Управление информационной безопасностью. Стандарты СУИБ, 2018.
3. Смирнов М. Методы анализа и обработки данных в кибербезопасности, 2018.
4. Григорьев С. Технологии информационной безопасности. Методы обеспечения информационной безопасности, 2020.
5. Григорьев П. Математические методы анализа и моделирования в кибербезопасности, 2018.
6. Романов И. Создание экспериментальных сред в кибербезопасности, 2020.
7. Иванов А. Сравнение традиционных и инновационных методов анализа киберугроз, 2020.
8. Смирнов М. Методы реагирования на киберугрозы в реальном времени, 2020.
9. Сидоров П. Обучение персонала в сфере кибербезопасности: методы и практика, 2017.
10. Иванова Н. Эволюция киберугроз: анализ и прогнозирование, 2019.

Khachatryan A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Methods for determining the probability of cyber threat realization using honeypot.

In the modern information society, the field of cybersecurity is acquiring increasingly critical importance. Alongside the escalating complexity of attacks, there arises a need for effective methods for their detection and prevention. One of the perspective tools for analyzing cyber threats is honeypot technology. A honeypot is a made-up or vulnerable computer/file designed to attract attackers and analyze their behaviour. This article proposes a methodology for determining the probability of cyber threat realization using honeypot technologies.

Key words: Information security, cyberattacks, defense strategy, trap for hackers, network security, threats

УДК 004.056.53
ГРНТИ 81.93.29

СОВРЕМЕННЫЕ УГРОЗЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ТЕСТОВ ТЬЮРИНГА В ОБЛАСТИ ВЕБ-ПРИЛОЖЕНИЙ.

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

Современные системы защиты веб-ресурсов от автоматизированных атак играют важную роль в сфере кибербезопасности. В статье рассматриваются атаки на широко применяемые системы защиты Google reCAPTCHA и Cloudfare. Приведенные атаки ставят под угрозу эффективность использования указанных систем, что вызывает необходимость разработки нового решения к защите от атак на веб-ресурсы. В качестве альтернативы предлагается разработка теста Тьюринга на основе голоса пользователя.

кибербезопасность, reCAPTCHA v3, машинное обучение, Selenium Web Driver, голосовые тесты Тьюринга, автоматизированные атаки.

Кибербезопасность в современном мире играет ключевую роль в обеспечении безопасности как информации, так и общества в целом. Эта область находится в постоянном развитии и совершенствовании. В последние годы одним из важнейших инструментов в сфере кибербезопасности стала технология *reCAPTCHA*, разработанная компанией *Google*.

reCAPTCHA представляет собой систему, предназначенную для выявления ботов и автоматизированных запросов на веб-ресурсах. Версия *v3* была представлена *Google* в 2018 году и быстро завоевала популярность среди разработчиков и владельцев веб-сайтов. В отличие от предыдущих версий *reCAPTCHA, v3* не требует от пользователей решения головоломок или ввода текста для подтверждения их человеческой природы. Вместо этого *reCAPTCHA v3* использует методы машинного обучения и анализа поведения пользователей для определения, является ли запрос подлинным или подозрительным.[1]

Однако в последнее время были обнаружены способы обхода *reCAPTCHA v3*, что угрожает ее эффективности. Известные методы включают в себя использование *Selenium Web Driver* и моделирование действий пользователя с использованием искусственного интеллекта.[2] Эти методы представляют серьезную угрозу для безопасности веб-ресурсов и требуют внимания специалистов в области кибербезопасности.

Исследование, проведенное М.Акраутом, демонстрирует успешные способы обхода *reCAPTCHA v3* с использованием методов машинного обучения. Это решение, основанное на методе обучения с подкреплением (*Reinforcement Learning*), позволяет искусственному интеллекту обмануть

систему *reCAPTCHA v3*, анализируя поведение пользователей и воспроизводя его так, чтобы система не могла отличить бота от реального пользователя. [3]

Метод обучения с подкреплением включает создание агента, который взаимодействует с целевым веб-сайтом, выполняя различные действия, такие как навигация по страницам, клики и заполнение форм. Агент получает положительное подкрепление, когда его действия успешно обходят *reCAPTCHA v3*, и отрицательное подкрепление, когда система обнаруживает подозрительную активность. С течением времени агент улучшает свои действия и становится более эффективным в обходе системы.[4]

Этот метод требует значительных вычислительных ресурсов и специализированных навыков в области машинного обучения. Однако он показывает, что даже самые современные системы кибербезопасности могут быть обмануты с использованием современных технологий. Это подчеркивает важность непрерывного совершенствования системы *reCAPTCHA v3* и других аналогичных методов защиты.

Другим методом обхода *reCAPTCHA v3* является использование *Selenium Web Driver*. *Selenium* - это инструмент для автоматизации действий веб-браузера, который часто используется для тестирования веб-приложений. Однако его также можно использовать для обхода *reCAPTCHA v3*.

С помощью *Selenium Web Driver* злоумышленники могут автоматизировать взаимодействие с веб-сайтом, включая выполнение действий, которые обманывают не только систему *reCAPTCHA v3*, но и технологии защиты *Cloudflare*. Например, они могут создавать ботов, которые имитируют клики и движения мыши, а также заполняют формы на веб-страницах. Это создает ложное впечатление о поведении настоящего пользователя и позволяет злоумышленникам успешно обойти защиту.

Пример кода на языке программирования *Python* для обхода защиты с использованием *Python Selenium Web Driver*:

```
from selenium import webdriver
from selenium.webriver.chrome.service import Service
import time

options = webdriver.ChromeOptions()
options.add_argument("--disable-blink-features=AutomationControlled")
options.add_experimental_option("excludeSwitches", ["enable-automation"])
options.add_experimental_option('useAutomationExtension', False)

s = Service(executable_path='path_to_driver/chromedriver.exe')
driver = webriver.Chrome(service=s, options=options)

driver.execute_cdp_cmd("Page.addScriptToEvaluateOnNewDocument", {
    'source': '''
        delete window.cdc_YourCdcCode_Array;
        delete window.cdc_YourCdcCode_Promise;
        delete window.cdc_YourCdcCode_Symbol;
    '''
```

```
})

try:
    driver.maximize_window()
    driver.get('https://www.example.com/target_page')
    time.sleep(5)
except Exception as ex:
    print(ex)
finally:
    driver.close()
    driver.quit()
```

Учитывая тот факт, что существующая система защиты может быть подвергнута риску с использованием современных технологий, таких как машинное обучение и *Selenium Web Driver*, существует настоятельная необходимость в создании новых и более надежных методов проверки человеческой активности на веб-ресурсах. Один из подходов к этой проблеме заключается во внедрении голосовых тестов Тьюринга, где пользователю предоставляется задача произнести слова или фразы, а затем их голосовой образ анализируется для определения степени его соответствия установленным критериям.

Голосовые тесты Тьюринга представляют собой перспективный метод защиты от ботов и автоматизированных атак. Этот метод проверки требует не только знания текста, но и способности произнести его с учетом определенной интонации и акцента, что делает его более сложным для обхода.

Для обеспечения адекватного уровня целесообразности внедрения голосовые тесты Тьюринга должны обладать следующими свойствами:

1) Голосовой образ пользователя должен храниться и передаваться в безопасном режиме, чтобы предотвратить утечку конфиденциальной информации. Для обеспечения безопасности голосовых образов могут использоваться современные технологии шифрования и защиты данных.

2) Голосовая капча должна быть защищена от атак спуфинга, когда злоумышленники попытаются обмануть систему, используя записи голосов других лиц. Для этой цели могут применяться биометрические методы аутентификации, такие как анализ голосовых характеристик.

3) Голосовая капча должна оставаться удобной для пользователей и не вызывать излишних неудобств. Пользователям следует предоставлять альтернативные методы проверки, в случае если у них имеются ограничения, связанные с использованием голоса.

4) Система должна способствовать надежному различению голосов человека от аудиозаписей или синтетических звуков.

В свете современных угроз в области кибербезопасности, неоспоримо важно работать над разработкой более надежных методов защиты. Внедрение голосовых тестов Тьюринга представляет собой перспективное решение, способное обеспечить высокую эффективность проверки

человеческой активности на веб-ресурсах. Основными задачами здесь являются обеспечение безопасности, создание удобства для пользователей и эффективное различение человеческого голоса от синтетических или записанных аудиофайлов. Внедрение такого механизма позволит усилить кибербезопасность в контексте современных вызовов в области технологий.

Список используемых источников:

1. Google. Представляем reCAPTCHA v3: новый инструмент защиты от роботов [Электронный ресурс]. URL: https://webmasters.googleblog.com/2018/10/introducing-recaptcha-v3-new-way-to.html (дата обращения: 25.10.2023).

2. Selenium. The Selenium Browser Automation Project [Электронный ресурс]. URL: https://www.selenium.dev/documentation/ (дата обращения: 26.10.2023).

3. Akrout M., Akrout I., Feriani A. Hacking Google reCAPTCHA v3 using Reinforcement Learning [Электронный ресурс]. URL: https://arxiv.org/pdf/1903.01003.pdf (дата обращения: 26.10.2023).

4. Richard S. Sutton and Andrew G. Barto. Reinforcement Learning: An Introduction. The MIT Press. 2015. 352 c.

Shagisultanov T.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Modern threats and prospects for the development of Turing tests in the field of web applications.

Modern systems for protecting web resources from automated attacks play an important role in the field of cybersecurity. The article discusses attacks on the widely used Google security systems reCAPTCHA and Cloudfare. These attacks jeopardize the effectiveness of using these systems, which necessitates the development of a new solution to protect against attacks on web resources. As an alternative, it is proposed to develop a Turing test based on the user's voice.

Key words: cybersecurity, reCAPTCHA v3, machine learning, Selenium Web Driver, voice Turing tests, automated attacks.

УДК 004.056.57
ГРНТИ 81.93.29

УЯЗВИМОСТИ СИСТЕМЫ NFC: РИСКИ И МЕТОДЫ ЗАЩИТЫ

А. В. Шайер
Санкт-Петербургский государственный университет промышленных технологий и дизайна

Система бесконтактных платежей NFC (Near Field Communication) в настоящее время широко используется в мобильных устройствах, таких как смартфоны и планшеты. NFC позволяет передавать данные на короткое расстояние без необходимости физического подключения, что делает его удобным и эффективным способом для совершения транзакций.

NFC, near field communication, RFID, стандарт радиочастотной идентификации, скимминг, джег-тагинг, ретагинг

NFC передает информацию по радиоволнам. В большинстве случаев это достигается с помощью стандарта радиочастотной идентификации (RFID). Важным ключом к пониманию того, как работает NFC, является понимание основ RFID.

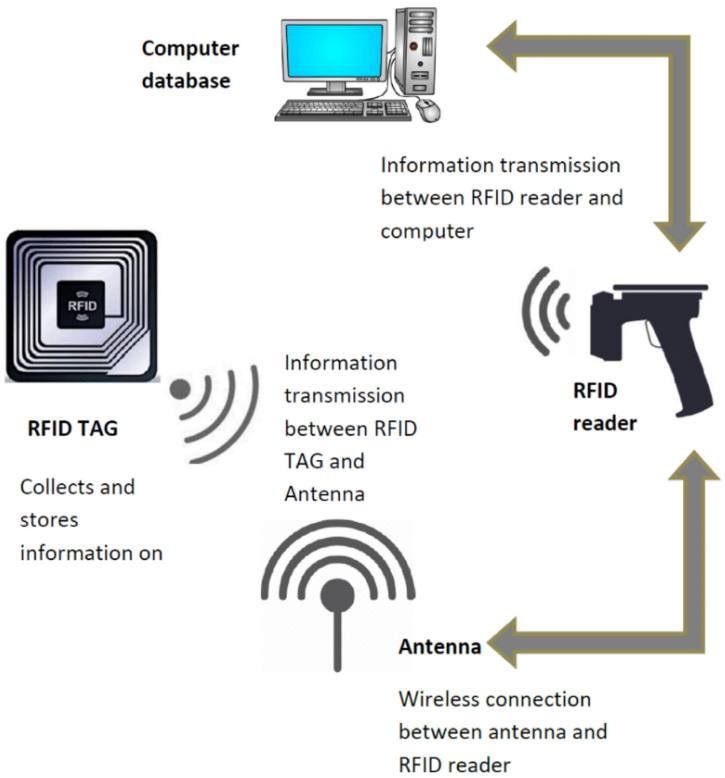


Рис. 1. Принцип работы системы RFID

Самая основная функция RFID — это позволить устройствам обмениваться данными посредством радиоволн. RFID также позволяет однозначно идентифицировать предметы с помощью этих радиоволн. Как минимум, система RFID состоит из считывателя, метки и антенны, где:

- Теги содержат данные.
- Считыватели читают и декодируют данные, хранящиеся в тегах.
- Антенны передают данные между считывателями и метками.

RFID также можно разделить на пассивный и активный. В пассивных системах RFID используются метки, которые работают без специального внутреннего источника питания. На самом деле метки питаются от энергии, передаваемой непосредственно от RFID-считывателя. Обычно вы увидите пассивные метки RFID, используемые для контроля доступа, например, когда вы используете брелок для входа в здание с ограниченным доступом; или для управления логистикой/цепочкой поставок, где иногда используются похожие карточки.

В активных системах RFID используются метки, которые работают от батареи. Как правило, эти метки с батарейным питанием непрерывно передают сигнал (при включении) независимо от наличия считывателя RFID. Активные метки RFID также имеют больший диапазон считывания, чем пассивные метки. Такое непрерывное и независимое вещание делает активные RFID-метки и системы весьма полезными для отслеживания в реальном времени.

Одной из наиболее распространенных уязвимостей является возможность перехвата данных посредством атаки "скимминг" (skimming), при которой злоумышленник использует специализированное оборудование для чтения передаваемых данных через NFC. Например, они могут подсунуть фальшивое устройство-считыватель в близком поле устройства NFC, чтобы перехватить финансовую информацию с бесконтактных платежных карт или личную информацию со смартфонов.

Подобные случаи уязвимостей NFC уже были зафиксированы. В 2019 году специалисты по безопасности обнаружили уязвимость в системе NFC платежных карт, которая позволяла злоумышленникам внедрять вредоносные программы на устройствах магазинов для сбора конфиденциальной информации. Также были сообщения о случаях взлома бесконтактных платежных карт посредством атаки "скимминг" в общественных местах, таких как общественные терминалы для оплаты.

Еще одной уязвимостью является возможность атаки между двумя устройствами NFC, известная как "Джег-тагинг" (tag-jacking). Злоумышленник может создать фальшивое устройство-метку и выдать его за легитимное. Когда другое устройство NFC подключается к этой метке, злоумышленник может осуществить атаку и получить доступ к данным или запустить вредоносный код на устройстве.

Также существуют уязвимости в протоколах коммуникации NFC. Например, атака "ретагинг" (retagging) позволяет злоумышленнику перехватить и модифицировать данные, передаваемые между устройствами NFC, что может привести к несанкционированному доступу или изменению информации.

Повреждение данных и манипулирование ими происходят, когда преступник манипулирует данными, отправляемыми считывателю, или вмешивается в

отправку данных, поэтому они повреждаются и становятся бесполезными по прибытии. Чтобы этого не произошло, для связи следует использовать защищенные каналы. Некоторые устройства NFC «прослушивают» атаки, связанные с повреждением данных, и предотвращают их до того, как они смогут начать работу.

Подобно манипулированию данными, атаки с перехватом продвигают этот тип цифровых преступлений на шаг дальше. Человек выступает посредником между двумя устройствами NFC, получая и изменяя информацию при ее передаче между ними. Этот тип атаки сложен и менее распространен. Чтобы этого не произошло, устройства должны находиться в активно-пассивном сопряжении. Это означает, что одно устройство получает информацию, а другое отправляет ее вместо того, чтобы оба устройства получали и передавали информацию.

Никакое шифрование не сможет защитить потребителя от украденного телефона. Если смартфон украден, вор теоретически может воспользоваться им над кард-ридером в магазине, чтобы совершить покупку.

Теперь обратимся к методам защиты, которые вы можете использовать для минимизации рисков, связанных с уязвимостями NFC:

1. Включите NFC только тогда, когда это необходимо: не оставляйте NFC включенным постоянно, особенно в общественных местах, где могут находиться злоумышленники с оборудованием для перехвата данных. Включайте NFC только тогда, когда собираетесь проводить бесконтактную транзакцию.
2. Устанавливайте обновления: регулярно обновляйте программное обеспечение своего устройства, чтобы получить последние исправления уязвимостей. Производители постоянно работают над улучшением безопасности NFC.
3. Используйте защищенные приложения: Устанавливайте только официальные и проверенные приложения, которые имеют хорошую систему безопасности. Избегайте скачивания и использования неизвестных и подозрительных приложений.
4. Защита с помощью пароля или шифрования: Некоторые устройства и приложения поддерживают функцию работы NFC только с помощью пароля или шифрования. При необходимости используйте эти функции, чтобы повысить безопасность ваших данных.
5. Будьте осторожны в общественных местах: Будьте бдительны при использовании NFC в общественных местах, особенно в тесных местах, где злоумышленники могут легко подойти и попытаться перехватить данные. Попробуйте быть около безопасных зон, чтобы защитить свою конфиденциальную информацию.

Уязвимости NFC могут представлять серьезную угрозу для безопасности и конфиденциальности пользователей. Однако, если принять соответствующие меры предосторожности и использовать разумные методы обеспечения

безопасности, можно уменьшить риски и насладиться преимуществами бесконтактных платежей NFC.

Список используемых источников:

1. Skimming [Электронный ресурс] URL: https://learningcenter.unc.edu/tips-and-tools/skimming/(дата обращения 14.10.2023).
2. Skimming and Scanning The University of Tennessee at Chattanooga [Электронный ресурс] URL:https://www.utc.edu/enrollment-management-and-student-affairs/center-for-academic-support-and-advisement/tips-for-academic-success/skimming (дата обращения 14.10.2023).
3. Is NFC/RFID Skimming a Real Threat... Yet? Avoidthehack![Электронный ресурс] URL:https://avoidthehack.com/nfc-rfid-skimming-a-real-threat (дата обращения 14.10.2023).
4. Security Concerns with NFC Technology Avoidthehack![Электронный ресурс] URL:http://nearfieldcommunication.org/nfc-security.html (дата обращения 14.10.2023).

Shaier A.

St. Petersburg State University of Industrial Technologies and Design

NFC system vulnerability: risks and protection methods.

The NFC (Near Field Communication) contactless payment system is now widely used on mobile devices such as smartphones and tablets. NFC allows data to be transferred over a short distance without the need for a physical connection, making it a convenient and efficient way to make transactions.

Key words: NFC, near field communication, RFID, standard radio frequency identification, skimming, jagging, retagging.

УРДК 004.056.5
ГРНТИ 81.93.29

МЕТОДИКА ЗАЩИТЫ ОРГАНИЗАЦИИ ОТ АТАК С ИСПОЛЬЗОВАНИЕМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ МЕХАНИЗМАМИ АВТОМАТИЗИРОВАННЫХ ПРОГРАММ

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

социальная инженерия, кибербезопасность, психологические аспекты, методы защиты, будущее, атаки

Поскольку информационно-коммуникационные технологии в наше время стали неотъемлемой частью всевозможных сфер деятельности человека: от развлечений и общения до трудового процесса, проблема защиты от киберугроз является очень актуальной. Для предотвращения утечек важной информации были разработаны различные методы поиска и устранения технических уязвимостей сетей.

Киберпреступники, в свою очередь, придумывают все более изощренные способы получения доступа к данным, поэтому развитие специальных систем для обеспечения безопасности остается актуальным.

Организации активно внедряют межсетевые экраны нового поколения (NGFW) и системы управления событиями безопасности (SIEM), строят центры мониторинга и реагирования на инциденты информационной безопасности, развертывают системы резервного копирования и восстановления данных. Конечно, это все немаловажно для обеспечения стойкой защиты организации от вторжений, но не стоит забывать, что самым уязвимым звеном во всей системе информационной безопасности все же является человек. Именно через человеческие слабости злоумышленники могут раскрыть конфиденциальную информацию и получить доступ к сетям данных, не обладая при этом особыми техническими знаниями.

Взломать компьютерную систему можно двумя способами: техническим – с помощью уязвимости сети, и с помощью обмана человека, который работает с компьютером. Именно второй способ и определяется термином «социальная инженерия».

Информационная безопасность является важной частью защиты любого государственного учреждения, включающей в себя совокупность меры, направленных на обеспечение защиты ИСПДн.

В зону юрисдикции политики информационной безопасности входят все автоматизированные и телекоммуникационные системы, обладателем и управляющим которых является предприятие.

Для реализации ИСПДн любая часть информационной системы должна рассматриваться как часть целого информационного комплекса в

защищенном исполнении при рациональном соотношении технических и организационных мероприятий.

Основной целью проведения политики ИБ является защита информационных ресурсов от нанесения разного рода моральных, физический, материальных ущербов на процессы обработки и передачи, её носители.

Для минимизирования рисков необходимо правильно решить важнейшие задачи, такие как: прогнозирование атак на ИБ и создание реагирования на них, защита от постороннего вмешательства на процесс функционирования информационных систем.

Так, разработка политики информационной безопасности включает в себя нечто большее, чем просто формулирование и осуществление политики. Если организации не уделяет должного внимания деталям, необходимым для разработки политики безопасности, они рискуют разработать политику, которая является плохо продуманной, неполной, избыточной и неактуальной, и которая не будет полностью придерживаться пользователями. Многие инциденты информационной безопасности происходят из-за халатности и непреднамеренного поведения внутренних сотрудников, приводящих к серьезной внутренней угрозе безопасности активов организации. Соблюдение правил и положений безопасности в значительной степени зависит от осознания угрозы и навыков справляться с ситуациями [9]. Квалифицированный руководитель должен объективно анализировать положение дел и грамотно распоряжаться ресурсами (см. рис. 1).

Рис. 1. Взаимосвязанные параметры поля информационной безопасности

На первом этапе необходимо определить от чего предприятию нужно защищаться в первую очередь.

Сначала строится модель нарушителя, которая описывает его квалификацию, имеющиеся ресурсы для реализации тех или иных атак, обычное время действия и т. п. На этом этапе проводится поиск и анализ уязвимых мест, а также возможные варианты реализации угроз безопасности, оценивается вероятность атак и следующих за ними последствий [10].

Вместе с анализом существующей технологии должна производиться разработка политики информационной безопасности и свода организационно-распорядительных документов, которые являются основой создания инфраструктуры информационной безопасности (см рисунок 2).

Рис. 2. Составляющие инфраструктуры информационной безопасности

Таким образом, мы можем сделать вывод, что для разработки политики информационной безопасности нужно учитывать все возможные виды угроз безопасности ИСПДн, знать цели и методы защиты данных, знать основные понятия и инфраструктуру безопасности, понимать, как справляться с внутренними и внешними, локальными и сетевыми угрозами.

Список используемых источников:

1. Пестов И. Е., Сахаров Д. В., Сергеева И. Ю., Чернбородов И. С. Выявление угроз безопасности информационных систем // 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. 525-527.

2. Пестов И. Е., Шинкарева П. С., Кошелева С. А., Бурмистров М. Д. Разработка программно-аппаратной системы контроля и управления доступом // Эргодизайн. 2020. N 1 (7). С. 19-24.

3. 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 Международной научно-технической и научно-методической конференцияи : в 4 т. 2019. С. 270-275.

4. Гандрабура В. А. Проблемы защиты ПДн в гос. учреждениях и анализ решений / В. А. Гандрабура, А. А. Захаров // Безопасность информационного пространства : материалы XIII Всерос. научно-практич. конф. студентов, аспирантов и молодых учёных, Челябинск, 26–28 нояб. 2014 г. Челябинск : Издательский центр ЮУрГУ, 2015. С. 208-211.

5. Методология управления потоками трафика в программно-определяемой адаптивной сети / А. В. Красов, М. В. Левин, С. И. Штеренберг, П. А. Исаченков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2016. N 4. С. 3-8.

6. Штеренберг С. И. Разработка методики внедрения и выявления эффективности siem-системы / С. И. Штеренберг, Ю. С. Данилова // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 3. С. 40-45.

7. Разработка методов обеспечения безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения / С. И. Штеренберг, А. И. Москальчук, В. А. Коптелова, О. М. Виноградова // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. N 1. С. 32-38.

8. Комплексный подход к защите электронного документооборота / С. И. Штеренберг, Л. А. Виткова, В. И. Андрианов, К. А. Небаева. СПб. : СПбГУТ, 2016. 93 с.

9. Штеренберг С. И. Разработка комплекса мер для защиты предприятия от фишинговых атак / С. И. Штеренберг И. В. Стародубцев, В. С. Шашкин // Защита информации. Инсайд. 2020. N 2 (92). С. 24-31.

10. Исследование типов фреймов, применяемых для определения местоположения / В. А. Петров М. М. Ковцур А. Ю. Киструга, С. И. Штеренберг // Региональная информатика и информационная безопасность : материалы XII Санкт-Петербургской межрегион. конф., Санкт-Петербург, 27–29 нояб. 2021 г. Вып. 10. СПб. : Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2021. С. 62-67.

11. Штеренберг С. И. Методика обеспечения безопасности доменных систем доверенной зоны / С. И. Штеренберг, Г. С. Бударный, И. В. Чумаков // Региональная информатика и информационная безопасность : материалы Юбилейной XVIII Санкт-Петербургской междунар. конф., Санкт-Петербург, 26–28 окт. 2022 г. Вып. 11. СПб. : Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2022. С. 621-625.

Shterenberg O.

St. Petersburg State University of Industrial Technologies and Design

Methodology for protecting an organization from attacks using social engineering by automated program mechanisms.

Since information and communication technologies have become an integral part of various spheres of human activity in our time: from entertainment and communication to the labor process, the problem of protection from cyber threats is very relevant. To prevent leaks of important information, various methods have been developed to find and eliminate technical vulnerabilities of networks. Cybercriminals, in turn, are coming up with increasingly sophisticated ways to gain access to data, so the development of special systems to ensure security remains relevant. Organizations are actively implementing new generation firewalls (MESPS) and security event management systems (SIEM), and build information security

incident monitoring and response centers, deploy data backup and recovery systems. Of course, this is all important to ensure the stable protection of the organization from intrusion, but do not forget that the most vulnerable link in the entire system.

Key words: social Engineering, cybersecurity, psychological aspects, defense methods, future, attacks.

УДК 004.42
ГРНТИ 50.53.17

СИСТЕМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ ДАННЫХ

Д. В. Шуваев
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В современном мире информация играет ключевую роль в деятельности любого предприятия или организации. Ценность информации постоянно возрастает, что приводит к увеличению рисков, связанных с ее утратой или повреждением. Одним из наиболее эффективных способов минимизации этих рисков является использование систем резервного копирования данных.

защита информации, информационные технологии, резервные копии, безопасность данных, программное обеспечение.

Системы резервного копирования данных стали неотъемлемой частью многих организаций и предприятий. Они обеспечивают надежное хранение и восстановление данных в случае их потери или повреждения.

Система резервного копирования - это комплекс аппаратных и программных средств, предназначенных для создания копий данных на случай их утраты или повреждения. Она необходима для защиты информации от различных сбоев, вирусов, ошибок пользователей и других факторов, которые могут привести к потере данных. Система резервного копирования работает по следующему принципу: она автоматически создает копии всех важных данных на специальных носителях (например, жестких дисках или оптических дисках), которые затем хранятся в надежном месте. При необходимости, эти копии могут быть использованы для восстановления информации.

К программному обеспечению относятся программы и утилиты, которые выполняют непосредственно процесс резервного копирования, а также обеспечивают управление системой и контроль за ее работой.

Рис. 1. ПО для резервного копирования и восстановления данных от ADATA.

Аппаратное обеспечение включает в себя устройства для хранения резервных копий (жесткие диски, оптические приводы, ленточные накопители и т.д.), а также сетевые компоненты, обеспечивающие передачу данных между устройствами.

Рис. 2. Жесткий диск

Системы резервного копирования являются необходимым инструментом для обеспечения надежности и безопасности информационных систем. Правильный выбор типа системы, ее параметров и настроек позволяет минимизировать риски потери данных и обеспечить быстрое восстановление работоспособности системы в случае возникновения непредвиденных ситуаций. Кроме того, постоянное совершенствование технологий резервного копирования позволяет создавать более эффективные и надежные системы, способные работать в условиях постоянно растущих объемов информации и увеличения требований к безопасности данных.

Список используемых источников:

1. Миронович В. Обзор систем резервного копирования и восстановления данных [Электронный ресурс]. URL: https://www.computerra.ru/235234/obzor-sistem-rezervnogo-kopirovaniya-i-vosstanovleniya-dannyh/ (дата обращения 20.10.2023).

2. Резервное копирование данных [Электронный ресурс]. URL: https://syscode.ru/programmnoe-obespechenie/rezervnoe-kopirovanie-dannyh/ (дата обращения: 20.10.2023).

Shuvaev D.

Saint-Petersburg State University of Industrial Technologies and Design

Data backup systems.

In the modern world, information plays a key role in the activities of any enterprise or organization. The value of information is constantly increasing, which leads to an increase in the risks associated with its loss or damage. One of the most effective ways to minimize these risks is to use data backup systems.

Key words: Information security, information technology, backups, data security, software.

УДК 004.056
ГРНТИ 81.93.29

ЗАЩИТА ПЕРИМЕТРА СЕТИ С ИСПОЛЬЗОВАНИЕМ OPEN SOURCE-ИНСТРУМЕНТОВ. РЕГУЛЯРНЫЙ ПЕНТЕСТ.

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

Роль сетевой безопасности за последние несколько лет выросла в геометрической прогрессии, особенно с учетом значительного количества атак, нацеленных на все типы организаций и служб. Таким образом, потребность защиты периметра сети становится неотъемлемой частью безопасности информационных систем. Существует ряд open source-инструментов, которые позволяют анализировать сетевой трафик и обнаруживать уязвимости. В данной статье рассмотрено, как можно проверять защищённость внешних информационных ресурсов компании через пентест, целью которого является поиск проблем сетевой безопасности и выявление уязвимостей.

пентест, nmap, сканирование, уязвимость, безопасность, периметр сети

Поскольку большая часть сети центров обработки данных переходит в облачную инфраструктуру и инфраструктуру виртуализации, во многих ситуациях пакет может даже не покинуть физический сервер. Потребность в практическом решении, способном обеспечить защиту периметра — это первое, что должна реализовать любая система сетевой безопасности.

Пентест - это метод оценки безопасности системы, который состоит в моделировании действий киберпреступника, которые он может совершить с информационными ресурсами. Одним из основных отличий этого подхода от хакинга является незыблемое правило - воздерживаться от доведения своих действий до деструктивных последствий. Цель пентестера заключается в выявлении уязвимостей, а не их эксплуатации. Иными словами, пентестер по своей сути является тестировщиком, который использует инструменты хакеров.

1. Настройка рабочего окружения для пентестов.

Важно действовать как "внешний нарушитель" и осуществлять атаки извне, в таком случае лучший вариант — развернуть виртуальную машину в облаке [1], снаружи периметра - это необходимо для получения достоверных результатов. Сетевые правила и конфигурация внутреннего компьютера могут производиться по-разному, поэтому в локальной сети возможно увидеть больше информации, чем во внешней.

Под подобные задачи подойдёт VPS с установленной операционной системой Linux: сервер с 2-4 ядрами процессора, 4-8 ГБ оперативной памяти и не менее 30 ГБ жесткого диска. Важно иметь статический IP-адрес, чтобы сервер не был заблокирован администраторами.

Существует несколько вариантов подготовки тестового хоста:

I. Использовать готовую сборку операционной системы для пентеста, такую как Kali Linux [2], в которой уже предварительно установлены необходимые инструменты.
II. Создать виртуальную машину с операционной системой, например, Ubuntu 18.04. Для этого необходимо предварительно обновить пакеты и установить компонент nmap - сетевой сканер, используя команду: *sudo apt update && sudo apt upgrade && sudo apt install nmap –y*

2. Получение информации о сетевой инфраструктуре компании с помощью nmap.

Для начала необходимо определить цели, которые требуется достичь при сканировании. В данной фазе важно собрать максимальное количество информации о сетевом оборудовании, используемом в сети, о его связи и о белых сетях, используемых на пограничном оборудовании. Анализируя конфигурацию пограничного оборудования, можно определить список используемых IP-адресов. Эти адреса должны рассматриваться как цели для сканирования.

Чтобы выбрать соответствующий набор параметров для сканирования, нужно проанализировать условия сети, чтобы понять, какие порты, протоколы или службы могут быть открытыми и уязвимыми.

Для проведения сканирования следует выбрать период, когда нагрузка на сервисы минимальна, и заранее оповестить системных администраторов. Рекомендуется добавить IP-адрес хоста для тестирования в список исключений в системах IDS/IPS [3].

Далее определяется список сканируемых портов. Nmap («Network Mapper») [4] — бесплатная утилита с открытым исходным кодом для обнаружения сетей и аудита безопасности. Nmap сканирует по умолчанию первую тысячу портов. Если имеется информация, об используемых портах, то в параметрах можно указать конкретные значения — например, -p 443 или явно указывать все порты (-p 0-65535), что скажется на скорости сканирования.

Статусы портов:

- open — открытый порт;
- closed — закрытый порт;
- filtered — фильтруется, неизвестно, закрыт или открыт;
- unfiltered — не фильтруется, неизвестно, закрыт или открыт;
- open|filtered — порт либо открыт, либо фильтруется;
- closed|filtered — порт либо закрыт, либо фильтруется.

Nmap работает в многопоточном режиме с динамическим изменением количества портов на каждом потоке, а также может использовать несколько ядер процессора. Однако, даже с множеством оптимизаций в своем коде, Nmap не самый быстрый инструмент для сканирования.

Для повышения скорости в Nmap есть предустановленные шаблоны агрессивности сканирования. Их всего шесть (от 0 до 5), и выбор можно сделать с помощью опции –T: *sudo nmap -T3 x.x.x.x*

Третий шаблон является значением по умолчанию и представляет собой определенный компромисс между скоростью и точностью сканирования в медленных сетях. Однако в настоящее время, когда минимальная скорость проводного доступа в сеть превышает 30 Мбит/с, лучшим выбором будет -T4 или даже -T5, необходимо учесть, что T5 следует использовать только в стабильных сетях без снижения скорости.

Более низкие значения предназначены для обхода систем обнаружения вторжений. Например, -T0 отключает многопоточное сканирование и устанавливает пятиминутную задержку между проверками портов; потратив весь день на сканирование, можно надеяться, что само сканирование не будет замечено. Шаблон -T1 обеспечивает более быстрый режим со 15-секундной задержкой, -T2 — с задержкой в 0,4 секунды, -T3 — с задержкой в 10 мс, а -T4 — с задержкой в 5 мс, режим -T5 – 2,5 мс.

Команда сканирования с записью результатов в файл nmap.txt, в результате которой будут обнаружены открытые порты, выглядит так: *sudo nmap x.x.x.x --open -T4 -p 0-65535 -v > nmap.txt*

Чтобы узнать версии операционной системы и приложений, работающих на целевом хосте, запустите nmap со следующими параметрами: *sudo nmap x.x.x.x -p 22,80 -sV -O -v > nmap.txt*

Благодаря сканированию только открытых портов, определённых на предыдущем этапе, скорость процесса значительно увеличивается. Теперь возможно обнаруживать информацию о сервисах, которые работают на открытых портах, а также получить версию ядра Linux. Исходя из этой информации о версиях операционной системы, ее ядра и программного обеспечения, можно определить, устарели ли используемые операционные системы и программное обеспечение, а также наличие в них известных уязвимостей. Если нужно узнать дополнительные сведения, можно обратиться к ресурсу: https://cve.mitre.org/

Одним из ключевых компонентов Nmap является скриптовый движок NSE (Nmap Scripting Engine), который предоставляет возможность использовать скрипты для автоматизации задач сканирования и сбора информации. NSE является мощным инструментом, который позволяет расширить функциональность Nmap и обнаружить различные уязвимости, собрать дополнительную информацию о целевой сети или выполнить специфические скрипты для анализа безопасности, включая проверку на наличие открытых портов, определение версии программного обеспечения и ОС, и многое другое.

Для использования скриптового движка NSE с Nmap, пользователь может указать конкретные скрипты для выполнения с помощью аргумента командной строки "--script". Примеры некоторых скриптов, доступных в

NSE, включают "http-enum" для перечисления веб-ресурсов на сервере, "ftp-brute" для перебора паролей на FTP-сервере.

Сканирование с помощью скриптов категории vuln проверяют наличие определенных известных уязвимостей и обычно сообщают о результатах только в случае их обнаружения. Запустить расширенное сканирование можно следующей командой: *sudo nmap x.x.x.x -T4 -A -p 22,80 --script "vuln" -v > nmap.txt*

Используя известное DNS-имя веб-приложения, можно также получить информацию о списке доступных из интернета расположений, что может быть полезно для проверки настроек разграничения доступа к определенным ресурсам. Для осуществления сканирования веб-приложения, требующего авторизации для доступа к его содержимому, запустим следующую команду: *sudo nmap --script http-enum test.ru -v > nmap.txt*

В результате выполнения команды выводится список каталогов и файлов сайта, доступных без авторизации.

Утилита nmap предлагает еще более широкие возможности, не ограничиваясь только приведенными примерами. Для расширения спектра сканирования можно использовать иные категории скриптов.

В результате проведенного сканирования была получена следующая информацию о целевых хостах: перечень открытых портов, версии операционных систем, версии используемого программного обеспечения и существующие уязвимости для операционной системы и ПО.

По итогам данного этапа необходимо сформировать карту сети в удобном табличном формате, где важно указать такие параметры как: ip, домен, порт, служба, ОС, пояснения

3. Формирование плана регулярной проверки внешнего сетевого периметра компании.

План включает исследование обнаруженных сервисов и выбор инструментов для их проверки. Необходимо указать команды и краткое описание этих инструментов. План следует составить для сохранения информации о доступных инструментах пентестинга, поскольку их количество сейчас непрерывно растёт, и использование каждый раз мануалов для конкретного инструмента может быть неэффективным и затратным.

При анализе сервисов и разработке плана проверки необходимо понимать, какие атаки могут быть применены к этим сервисам.

Например, установлено, что сотрудники компании используют SSH для удаленного подключения. Этот протокол подвержен атакам Brute Force, а также имеет различные уязвимости в разных версиях, включая RCE и DOS. Также возможны "мисконфигурации". Каков план действий? Необходимо запустить проверку на устойчивость к атакам Brute-Force, можно использовать такие решения с открытым исходным кодом, как Patator, Hydra, MSF. Важно, чтобы для аутентификации SSH использовались RSA-ключи, а не логин и пароль. Если это невозможно из-за каких-либо причин, то требуем установить защиту от перебора, такую как блокировка IP-адреса после 10

неудачных попыток авторизации. Также нужно провести сканирование версии OpenSSH, обращаясь к базам данных уязвимостей. Если обнаруживаем уязвимости в текущей версии, направляется запрос администраторам системы на обновление [5].

Когда по каждому типу сервисов сформирован список в плане, отвечающий на вопросы: что, чем и как искать, можно переходить к следующему этапу.

4. Формирование регламента регулярных проверок.

Необходимо установить регулярность проведения тестирования. Оптимальным вариантом будет ежемесячное проведение комплексного тестирования внешней сетевой инфраструктуры. В ходе этого процесса необходимо сканировать ресурсы компании, обновлять карту сети каждый месяц и проверять обнаруженные сервисы.

5. Автоматизация.

Автоматизируя процессы, можно сэкономить время и силы. Например, можно автоматизировать процесс "Брутфорса" с помощью скриптов. Для этого необходимо создать словари, сохранить нужные команды и просто запускать готовый скрипт, указав адрес и порт сервиса, или даже список исследуемых сервисов целиком.

Автоматизация сканирования сетевых адресов осуществляется с помощью скрипта nmap и сервиса на Linux под названием Cron. Такая реализация позволяет получать только результаты сканирования, не требуя непосредственного участия. Можно настроить два типа сканирования: полное, включающее все порты и скрипты, и, соответственно, требующее большего времени. Второй тип сканирования быстрее и будем опрашивать только популярные порты, что позволит обнаружить открытие нового порта, уже через 1-2 часа. Таким образом, данная система позволяет недорого и эффективно следить за внешней сетевой инфраструктурой.

Однако важно отметить, что автоматизация не заменяет ручное тестирование и экспертизу специалистов в области пентеста. Ручное тестирование все еще необходимо для осуществления более глубокого и тщательного анализа системы и выявления уязвимостей, которые могут быть упущены автоматизированными инструментами.

Таким образом, для обеспечения безопасности внешней сетевой инфраструктуры компании рекомендуется регулярно проводить проверку на проникновение (пентест). Для повышения эффективности такой проверки можно применять сканеры уязвимостей, которые могут сканировать сеть, оценивать уязвимости в обнаруженных сервисах, подбирать дефолтные учетные данные и предоставлять информацию в удобочитаемом формате. Однако не следует полностью полагаться на данные сканеров, так как их результаты иногда могут быть ошибочными. Для сканирования внешнего сетевого периметра можно включить проверку на веб-уязвимости. При этом стоит учитывать то, что веб-технологии достаточно сложны и для их анализа необходима специализация и опыт. На начальном этапе можно использовать

сканеры веб-уязвимостей, такие как Arachni, VEGA, OWASP ZAP, NetSparker, Standoff365 [6].

Список используемых источников:

1. Пестов И. Е. и др. Мониторинг информации инстансов облачной инфраструктуры // Подготовка профессиональных кадров в магистратуре для цифровой экономики: материалы Всерос. науч.-технич. и науч.-методич. конф. магистрантов и их руководителей, Санкт-Петербург, 06-08 дек. 2022 г. СПб. : СПбГУТ, 2023. С. 216-220.
2. Сахаров С. Л., Иванов К. А. Применение kali linux для тестирования защищенности локальной сети учреждения уис // Техника и безопасность объектов уголовно-исполнительной системы. 2022. С. 270-272.
3. Кольцов А. С., Коротких Л. П., Попов Н. Н. Организация защиты периметра телекоммуникационной сети учреждения уис //Актуальные проблемы деятельности подразделений УИС. 2017. С. 28-30.
4. Asokan J. et al. A Case Study Using Companies to Examine the Nmap Tool's Applicability for Network Security Assessment //2023 12th International Conference on Advanced Computing (ICoAC). IEEE, 2023. С. 1-6.
5. Жуков М. М., Баркалов Ю. М., Телков А. Ю. Методологический подход к имитационному моделированию при исследовании практической эффективности систем защиты от сетевых кибератак // Вестник Воронежского института МВД России. 2022. N 1. С. 24-39.
6. Черепов А. А., Рябцев А. А., Банников А. И. Обзор современных инструментов для проведения пентеста на объекте // Цифровой регион: опыт, компетенции, проекты. 2023. С. 965-969.

Yurova U.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Network perimeter protection using open source tools. Regular pentest.

The role of network security has grown exponentially over the past few years, especially given the significant number of attacks targeting all types of organizations and services. Thus, the need to protect the perimeter of the network becomes an integral part of the security of information systems. There are a number of open source tools that allow you to analyze network traffic and detect vulnerabilities. In this article, how can we check the security of external information resources of the company through a pentest, the purpose of which is to search for network security problems, that is, we limit ourselves to identifying vulnerabilities.

Key words: Pentest, nmap, scanning, vulnerability, security, network perimeter.

УДК 004.052.3
ГРНТИ 81.93.29

УЯЗВИМОСТИ BLUETOOTH УСТРОЙСТВ И МЕРЫ ПРОТИВОДЕЙСТВИЯ ИХ ЭКСПЛУАТАЦИИ

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

С каждым новым днем, Bluetooth находит все новые возможности для расширения сфер применения и все активнее используется не только в личных целях, но и в разных аспектах профессиональной деятельности. Однако, так ли безопасно повсеместное использование данного варианта беспроводного соединения? Насколько обмен данными между устройствами с применением данного типа беспроводной связи уязвим для различных атак со стороны нарушителей?

Bluetooth, механизмы защиты, типы атак, рекомендации по защите

Изначально, Bluetooth-соединение задумывалось как современный стандарт радиосвязи между персональными устройствами, расположенными поблизости друг с другом. Принцип действия основывается на применение радиоволн в диапазоне частот 2,4 ГГц, с использованием метода расширения спектра со скачкообразной перестройкой частоты – FHSS (Frequency Hopping Spread Spectrum). Данный метод позволяет обеспечить высокую устойчивость к широкополосным помехам, что не дает устройствам поблизости, не входящим в контакт с Bluetooth-парой, мешать подключению. Обеспечивается это благодаря тому, что несущая частота сигнала изменяется 1600 раз в секунду, тогда как последовательность переключения между частотами для каждого соединения псевдослучайна и известна только отправителю данных и их получателю.

Установка Bluetooth-соединения происходит в три этапа:

- Генерация ключа (Kinit),
- Генерация ключа связи (Link Key),
- Аутентификация

Процедура сопряжения между устройствами проходит на этапе генерации ключа и ключа связи, которые будут использоваться во время дальнейшего использования при передачи данных между устройствами. Ключ (Kinit) формируется с применением алгоритма E22. Для создания ключа связи устройства обмениваются случайно генерируемыми словами LK_RAND(A) и LK_RAND(B), после чего следует побитовый XOR с ключом инициализации Kinit и заключительный обмен полученными значениями. Последним этапом генерации ключа является вычисления сгенерированных ключей при помощи алгоритма E21. После перечисленного, следует взаимная аутентификация устройств, основанная на схеме «запрос-ответ», за которой следует окончание процесса установления соединения.

В качестве защитных механизмов Bluetooth-соединения выступает шифрование данных и авторизация устройств. Шифрование проводится посредством ключа, эффективная длинна которого может составлять от 8 до 128 бит. За счет этого, Bluetooth-устройства не способны бесконтрольно соединятся между собой, не позволяя происходит повсеместным утечкам данных пользователей в руки к посторонним лицам.

Кроме того, следует отметить и то, что возможно сконфигурировать режим безопасности Bluetooth, предоставив пользователю самостоятельно решить уровень необходимой защищенности:

1. Не защищенный режим – используется устройствами при заводских настройках. В этом режиме не применяется ни шифрование, ни аутентификация, в то время как само устройство ведет деятельность в широковещательном режиме.
2. Режим обеспечения защиты на уровне приложения/служб – в данном режиме, после установления соединения, менеджер безопасности осуществляет аутентификацию устройств, позволяя ограничить доступ к устройству.
3. Режим защиты на уровне канала связи – режим, в котором аутентификация производится до установки соединения, при этом используется прозрачное шифрование.
4. Режим обеспечения защиты на уровне приложения/служб при помощи применения протокола ECDH – представляет собой улучшенный вариант режима защиты на уровне приложений/служб, в котором функция безопасности также реализуется лишь поле установления соединения, но для генерации ключа соединения используется протокол ECDH.

Однако, даже использование режима защиты, обеспечивающего максимально возможный уровень защищенности Bluetooth-связи, не позволяет назвать рассматриваемый вариант беспроводного подключения безупречно защищенным.

На сегодняшний день, существует множество разнонаправленных Bluetooth-атак, обладающих различными уровнями негативных последствий на устройство-жертву. Наиболее популярными из подобных являются:

1. Атака Bluesnarf – один из наиболее распространенных типов атак Bluetooth, основывающийся на протоколе OBEX, используемый для импорта различных объектов. При использовании запроса OBEX GET атакующий получает доступ ко всем файлам на устройстве жертвы, если программное обеспечение драйвера Bluetooth-жертвы было установлено неверно.
2. Атака Bluesnarf++ - атака, похожая по своей методике проведения на предыдущую атаку, с отличающимся подходом злоумышленника к процессу получения доступа к файловой системе. Основная задача нападающего – при работе сервера на протоколе передачи файлов (FTP) на OBEX – подключение к данной службе без создания пары с устройством-жертвой, используя службу OBEX Push. Итог проведения атаки

– получение доступа к личным файлам жертвы, возможность редактирования файлов без аутентификации и сопоставления.

3. Атака BlueDump – реализация данной атаки возможна, если злоумышленнику известен адрес устройства Bluetooth (BD_ADDR), с которым сопряжено устройство Bluetooth. Данным адресом является уникальный идентификатор, присваиваемый производителем каждому устройству. Дальнейшее действие злоумышленника состоит в том, чтобы подменить свой адрес на адрес устройства, к которому подключена жертва, для дальнейшего подключения к жертве. Так как злоумышленник не имеет ключа подключения, устройство жертвы не вернет ключ подключения («HCI_Link_Key_Request_Negative_Reply»), при попытке подключения. В определенных случаях, подобное может привести к очистке ключа подключения со стороны устройства жертвы, для повторного входа в режим сопряжения. Злоумышленник способен войти в режим сопряжения и прочесть возможные изменения ключа, в целях удаления бывшего доверенного устройства из списка для повторного подключения, устроенного между устройством-жертвой и подменным атакующим устройством.

4. Атака BlueSmack – атака, которую принято относить к DoS-атакам. Реализация данной атаки происходит при помощи Bluetooth-слоя Linux BlueZ, позволяющего атакующему отправлять пакеты данных, перегружающие целевое устройство. Достигается это за счет уровня протокола L2CAP, основывающего свою работу на проверке соединения и измерении необходимого для приема-передачи файлов времени. Главный инструмент атаки – I2ping, при помощи которого злоумышленник может изменять размер отправляемых пакетов (для использования необходимо применить параметр –s, после которого указывается требуемый размер), выводя устройство-жертву из работоспособного состояния.

5. Перечень атак BrakTooth – комплекс уязвимостей, воздействующий на Bluetooth в наиболее распространенных SoC, используемых в ноутбуках, смартфонах, промышленных устройствах. В теории, данные уязвимости позволяют не только выводить устройство из строя – но и способствуют выполнению произвольного кода, с вытекающими возможностями захвата систем. Главная проблема данной уязвимости – её повсеместность. Согласно статистике, одинаковая уязвимая прошивка использовалась более чем в 1400 SoC, служивших основой для различных девайсов, общее количество которых может исчисляться миллиардами.

Благодаря всестороннему распространению Bluetooth-устройств, в перспективе, обладающих одной из перечисленных раннее, или, даже несколькими, уязвимостями, были разработаны рекомендации, способствующие сократить возможное вмешательство со стороны Bluetooth-атакующего. Данные рекомендации советуют:

- Устанавливать устройства Bluetooth на наиболее низкий, необходимый и достаточный уровень мощности. При помощи этого, установленный радиус сигнала остается в защищённом периметре пользователей/организаций;

•Устройства Bluetooth обязаны быть настроены как «не видимые», за исключением ситуаций, когда это необходимо для спаривания устройств. Это позволит скрыть Bluetooth-устройство от других устройств;

•Необходимо применять шифрование соединения, так как без шифрования соединение может быть открыто для прослушивания атакующей стороной;

•Сократить возможное количество выполняемых сопряжений до минимума, даже в безопасной зоне, в которой злоумышленники не способны перехватить фреймы с обменом ключами доступа между устройствами при их сопряжении;

•В случаях использования устройств Bluetooth 2.1 и выше, в которых применяется протокол SSP, не использовать режим спаривания «Just Works». При создании пары в данном режиме, отсутствует гарантия защиты от атаки «Man In The Middle»;

•При использовании устройств Bluetooth с версиями 4.0 и 4.1 необходимо при любой возможности применять режим защиты на канале связи. Так как остальные режимы защиты не способны обеспечить необходимого уровня защищенности устройств.

За 25 лет существования беспроводной технологии Bluetooth, ей удалось найти применение во всех сферах жизни общества, открыв множество возможностей для каждого. Однако, наряду с открывшимися возможностями использования, нельзя забывать и об открывшихся возможных угрозах, способных приводить к утечкам конфиденциальных данных, взлома чужого оборудования или нарушения работы устройств. Как следует из написанного - не стоит полагаться на разработанные и существующие методы защиты и шифрования, встроенные в Bluetooth-стек. Необходимо, также, во время использования данной сети, придерживаться выдвинутых рекомендаций, способствующих сократит перспективное число атак злоумышленников.

Список используемых источников:

1. Калачев А. В., Пелихов М. Е., Лапин М. В. Основы работы с технологией Bluetooth Low Energy. Лань, 2022. 224 с.

2. Крюков М. Технология Bluetooth // Компоненты и технологии. 2002. N 6. 64 с.

3. Иванова Е. В., Алексеева М. С. Уязвимость технологии Bluetooth // Молодой учёный. Технические науки. 2014. N 17. С. 62-63.

4. Лепихин И. Существует ли альтернатива Bluetooth? // Компоненты и технологии. 2003 г. N 7. С. 76-79.

5. Михайлов Д. М., Жуков И. Ю. Защита мобильных телефонов от атак. М. : Издательство «ФОЙЛИС», 2010.

6. Hermelin M. and Nyberg K. Correlation properties of the Bluetooth combiner generator // Information Security and Cryptology, LNCS 1787. Springer-Verlag, 1999. P. 17–29.

7. Саенко М. А., Мельников Д. А., Данилов М. А. Анализ уязвимостей беспроводных каналов передачи информации // Образовательные ресурсы и технологии. Информационные технологии. 2023. N 1. С. 82-90

Yakubovich S.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Vulnerabilities of Bluetooth devices and countermeasures for their operation.
With every new day, Bluetooth finds new opportunities to expand its scope and is increasingly used not only for personal purposes, but also in various aspects of professional activity. However, is it safe to use these wireless connections? How does data exchange between devices using this wireless connection vulnerability for various attacks from adversaries?

Key words: Bluetooth, protection mechanisms, types of attacks, protection recommendations.

УДК 004.056.5
ГРНТИ 81.93.29

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ КИБЕРАТАК И МЕТОДЫ ЗАЩИТЫ

И. А. Якубовский
Санкт-Петербургский государственный университет промышленный технологий и дизайна, г. Санкт-Петербург, Россия

социальная инженерия, кибербезопасность, психологические аспекты, методы защиты, будущее, атаки

Социальная инженерия и психологические аспекты кибератак приобретают особую актуальность в современном цифровом мире. Рост кибератак, переход к цифровым технологиям, развитие социальных сетей и увеличение онлайн-присутствия человека делают угрозы, связанные с социальной инженерией, более изощренными и широко распространенными. В мире, где данные становятся ключевым активом, защита от социальной инженерии становится критически важной. Развитие технологий, таких как искусственный интеллект и аналитика данных, дает злоумышленникам более эффективные средства манипуляции. Это подчеркивает необходимость исследования и борьбы с этими угрозами для обеспечения безопасности информации и защиты от потенциальных угроз.

Социальная инженерия остается одним из наиболее популярных методов атак на организации и частных лиц, что по статистике компании *Positive Technologies* стоставляет 50% и 91% соответственно. Основным каналом социальной инженерии в атаках на организации является электронная почта (86%), а на частных лиц — веб-ресурсы и сервисы (59%)[1], что представленно на рис. 1.

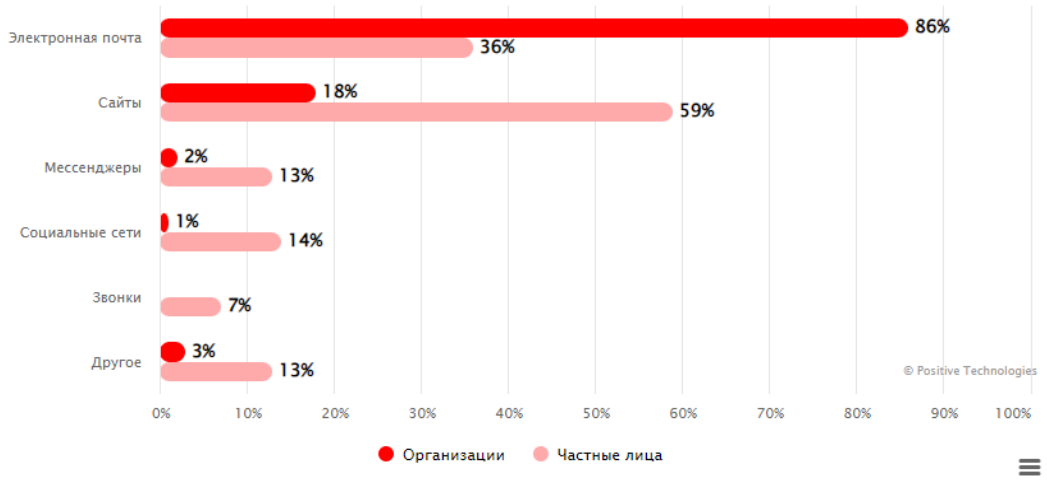


Рис. 1. Используемые злоумышленниками каналы социальной инженерии

Социальная инженерия, как метод, изначально опирается на психологические механизмы. Злоумышленники исследуют человеческие слабости и используют их в своих целях. В этом контексте проводится глубокий анализ психологических аспектов, используемых в кибератаках, рассматриваются методы манипуляции, применяемые социальными инженерами, и приводятся конкретные примеры успешных атак для демонстрации использования психологических уловок для достижения целей.

Социальная инженерия может принимать разнообразные формы, и рассматриваются типичные сценарии, включая фишинг, манипуляции через социальные сети и вредоносные звонки. Анализируется эффективность таких сценариев, предоставляются стратегии и тактики для предотвращения подобных атак, помогая лучше понимать, как злоумышленники могут использовать различные методы социальной инженерии для достижения своих целей.

Несмотря на изощренность атак, существуют эффективные методы защиты. Обучение персонала и повышение их осведомленности о социальной инженерии являются ключевыми стратегиями. Сотрудники должны быть информированы о методах атак и научены распознавать подозрительные ситуации. Это включает в себя проведение симуляций атак и тренингов для готовности к действию в случае атаки.

Рассматривается также важность разработки и внедрения политик и процедур безопасности. Корпорации и организации должны иметь четкие правила и положения относительно обработки конфиденциальной информации, а также планы действий в случае инцидентов безопасности.

Чтобы лучше понять, как работает защита от социальной инженерии, рассматриваются успешные случаи предотвращения атак. Эти кейсы представляют собой реальные истории, где хорошо настроенные системы безопасности справились с атаками социальной инженерии. Однако также анализируются случаи, когда недостатки в защите привели к успешным атакам, чтобы извлечь уроки и улучшить будущую защиту.

Сегодняшние угрозы быстро эволюционируют, и социальная инженерия не остается в стороне. Бросается взгляд в будущее, рассматриваются тенденции в развитии методов социальной инженерии и методы их преодоления. Особое внимание уделяется роли искусственного интеллекта и аналитики данных в предотвращении атак социальной инженерии[2].

В заключении, следует подчеркнуть, что актуальность темы социальной инженерии в контексте кибербезопасности непреложно растет. В мире, где цифровые технологии становятся неотъемлемой частью нашей повседневной жизни, и при увеличении киберугроз, понимание психологических аспектов, использованных социальными инженерами для атак, становится неотъемлемым элементом обеспечения безопасности. Эффективное обучение персонала, технические инновации и анализ данных - всё это важные компоненты борьбы с социальной инженерией, требующие постоянного

совершенствования. Учитывая растущую зависимость от цифровых технологий, актуальность этой темы остается высокой, и дальнейшие исследования и разработки в этой области необходимы для обеспечения кибербезопасности и защиты информации и ресурсов.

Список используемых источников:

1. *Positive Technologies* Актуальные киберугрозы: I квартал 2023 года [Электронныйресурс].URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q1/ (дата обращения: 07.10.2023).

2. Гущина А. А., Пчелинцева Н. В., Шацкий В. А. Применение искусственного интеллекта в обеспечении безопасности данных //В сборнике: Инженерное обеспечение инновационных технологий в АПК. Материалы Международной научно-практической конференции. Мичуринск-наукоград РФ.2021. С. 79-81.

3. Хэднаги К. Искусство обмана. Социальная инженерия в мошеннических схемах. : пер. с англ. М. : 2020. 301с.

Yakubovkii I.

St. Petersburg State University of Industrial Technologies and Design

Social engineering: psychological aspects of cyber attacks and defense methods.

Social engineering and psychological aspects of cyberattacks are of particular relevance in today's digital world. The rise of cyberattacks, digitalization, social media, and the increasing online human presence make social engineering threats more sophisticated and widespread. In a world where data is becoming a key asset, defense against social engineering becomes critical. Advances in technologies such as artificial intelligence and data analytics are giving attackers more effective means of manipulation. This emphasizes the need to research and combat these threats to ensure information security and protect against potential threats.

Key words: social Engineering, cybersecurity, psychological aspects, defense methods, future, attacks

УДК 004.056.53
ГРНТИ 81.93.29

АВТОМАТИЗАЦИЯ ПРОВЕРКИ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ НА БАЗЕ БЕСПРОВОДНОГО ОТЕЧЕСТВЕННОГО ОБОРУДОВАНИЯ ELTEX

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

В настоящее время одной из главных задач современного образования является повышение качества подготовки выпускников. Для достижения этой цели необходимо внедрение новых методик и технологий обучения. Одной из таких методик является автоматизация процесса проверки выполнения лабораторных работ.

Автоматизация процесса проверки выполнения лабораторных работ позволяет значительно сократить время на проверку и оценку работ студентов. Кроме того, это позволяет уменьшить количество ошибок при оценке работ, что повышает качество обучения.

Для автоматизации процесса проверки выполнения лабораторных работ будут использоваться два способа проверки, которые позволяют автоматически оценивать работы студентов. Эти способы могут анализировать правильность выполнения заданий, соответствие результатов эксперимента заданным значениям, а также другие параметры.

Таким образом, автоматизация процесса проверки выполнения лабораторных работ является эффективным инструментом для повышения качества обучения и улучшения подготовки выпускников.

Автоматизация проверки выполнения работы, беспроводная локальная сеть, защита беспроводной локальной сети, WLAN-контроллер, 802.1x, 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 состояние всех Wi-Fi клиентов сети;
- сбор сервисной и аварийной информации.

Комплекс лабораторных состоит из трех работ. В первой рассматривается базовая настройка точки доступа и авторизации на базе WPA2-PSK, во второй рассматривается организация беспроводной сети на базе IEEE 802.1x авторизация WPA2-Enterprise. В третьей студенты получают навыки настройки портальной авторизации пользователей.

При выполнения первой работы, необходимо выполнить настройку беспроводной сети с режимом безопасности WPA2-PSK и осуществить привязывание данной сетью к точке доступа так же, как показано на рис. 1, проверить работоспособность организованной сети. Помимо этого, возможна настройка таких функций как изоляция беспроводных клиентов и ограничение скорости сети семейства IEEE 802.11.

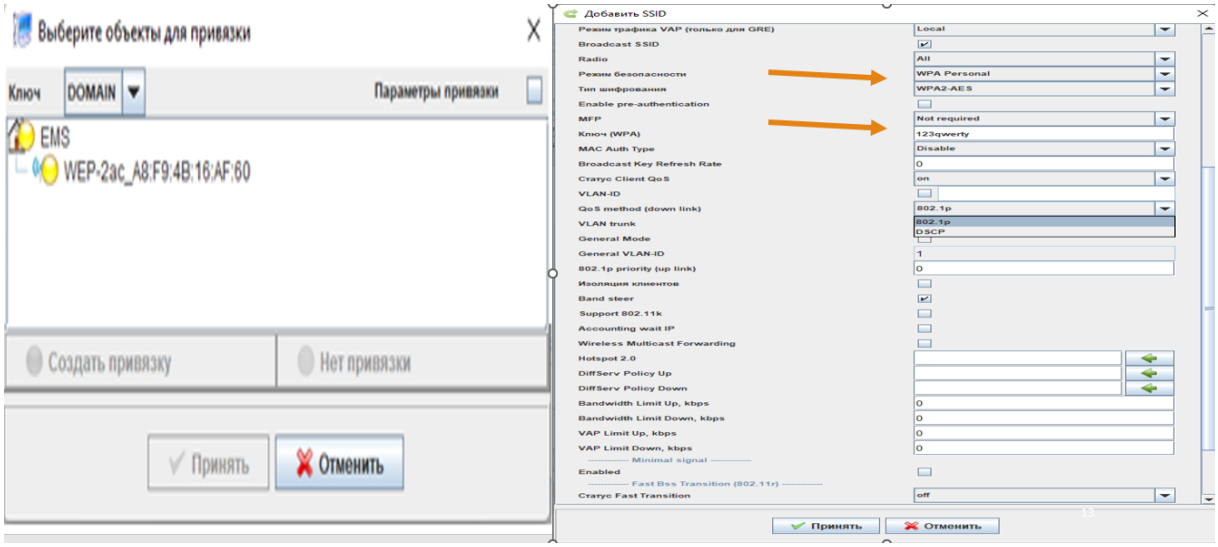


Рис. 1. Настройки точки доступа

В рамках второй лабораторной работы выполняется настройка IEEE 802.1x.

Аутентификация производится между рабочей станцией и сервером аутентификации. На рис. 2 наглядно изображена схема беспроводной локальной сети организации.

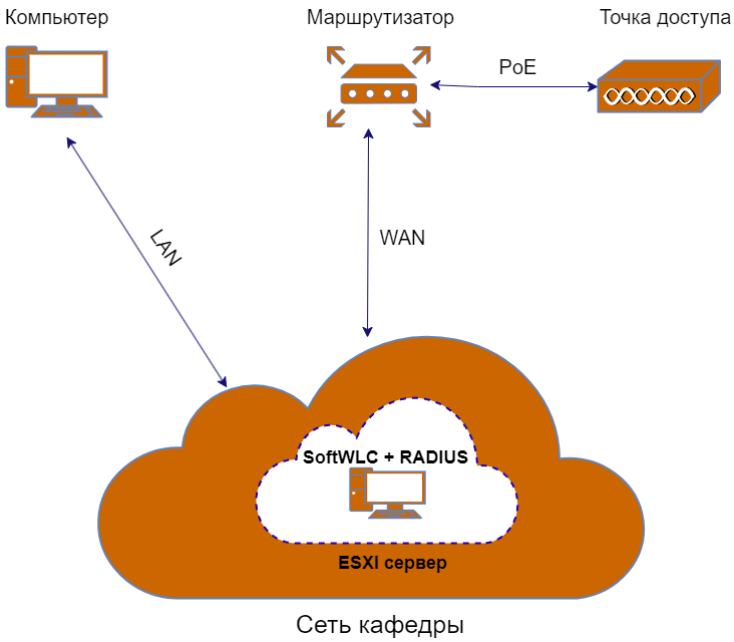


Рис. 2. Схема беспроводной локальной сети организации

Для выполнения второй лабораторной необходимо изменить созданную ранее WLAN и вручную выставить режим безопасности WPA2-Enterprise, а также тип шифрования WPA2-AES (рис. 3).

Далее необходимо указать настройки RADIUS-сервера, а именно IP-адрес сервера.

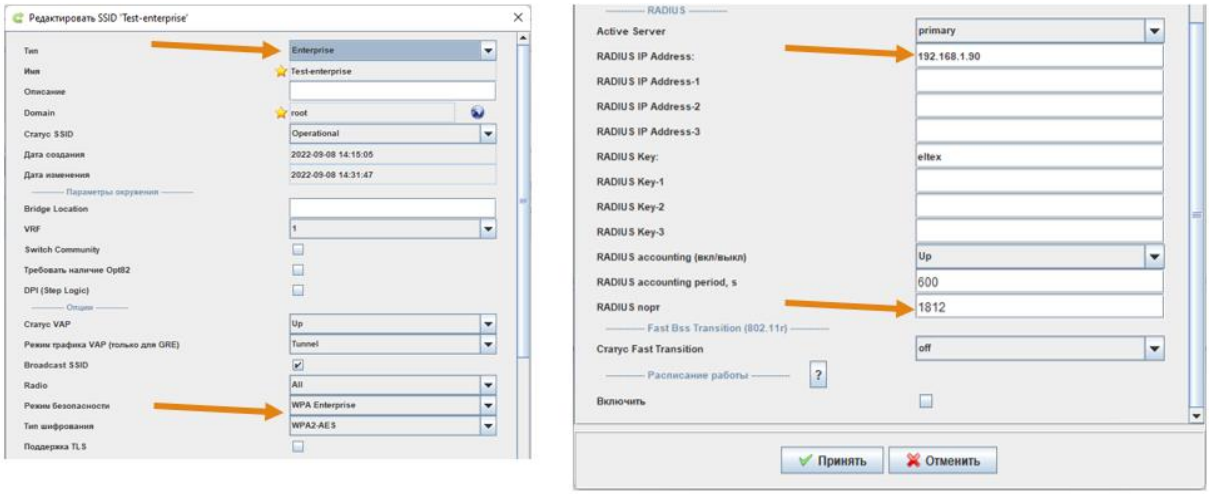


Рис. 3. Настройка WPA2-Enterprise

Создание пользователя происходит через модуль управления пользователя. Для того, чтобы создать пользователя нужно указать всю необходимую информацию, а также выдать логин и пароль для успешной авторизации через RADIUS-сервер.

После последнего пункта осуществляется подключение к беспроводной локальной сети посредством WPA2-Enterprise.

В следующей работе будет выполняться настройка портальной авторизации пользователей. Сперва происходит создание беспроводной сети

как и на примере первой лабораторной работы, далее настраивам сеть как показано на рис. 4.

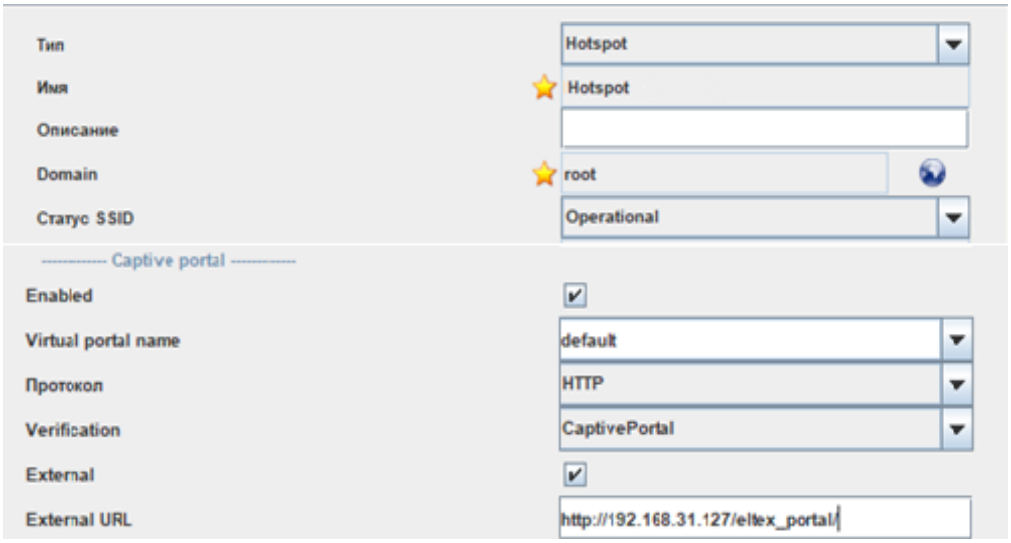


Рис. 4. Настройка сети для портальной авторизации

Далее производятся настройки беспроводной сети в веб интерфейсе конфигурации порталов. После заполнения всех необходимых полей для настройки, после чего появляется сеть, при подключении к которой, появляется портал, на котором и происходит авторизация пользователей (рис. 5).

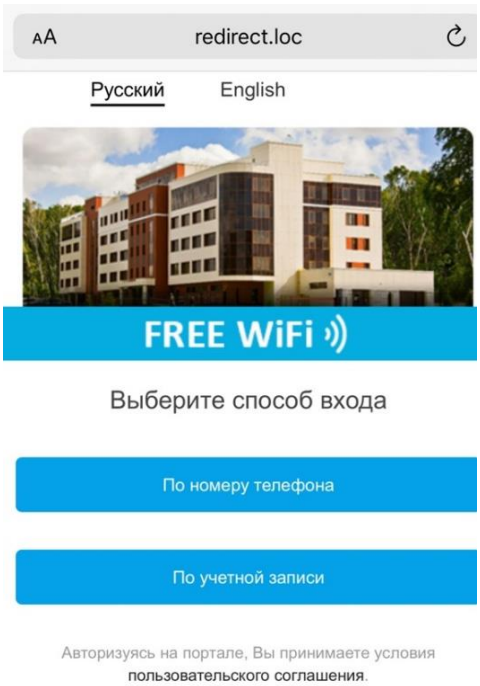


Рис.5. Портал авторизации пользователей

Существует два основных способа автоматизации процесса проверки лабораторных работ. Первый из них предполагает использование конфигурационных файлов и базы данных для хранения информации о заданиях и

их результатах. Второй способ основан на использовании сенсоров беспроводной сети для сбора данных о выполненных заданиях.

Для автоматизации процесса проверки работы студента через файлы конфигурации и базы данных необходимо выполнить следующие шаги:

- Создать конфигурационный файл, который содержит информацию о задании, его критериях оценки и других деталях.
- Сохранить этот файл на сервере и передать его студентам.
- Студенты должны выполнить задание и отправить результаты обратно на сервер.
- На сервере происходит проверка результатов и оценка работы каждого студента.

Конфигурационный файл может содержать различные параметры, такие как тип задания, количество заданий, длительность выполнения, критерии оценки и т.д. База данных может хранить информацию о каждом задании, включая его название, дату выполнения, оценку и другую информацию.

При использовании второго способа проверки с помощью сенсора операционной системы Linux и адаптера Wi-Fi необходимо выполнить следующие шаги:

- Установить драйверы для адаптера Wi-Fi и настроить систему на сбор данных с помощью специальных программных средств.
- Разработать код программы, который будет собирать данные о выполнении задания с помощью сенсора. Например, для сбора данных о времени выполнения заданий можно использовать утилиту wifi-tools, которая позволяет собирать информацию о текущем времени и уровне загрузки процессора.
- Запустить программу на компьютере с операционной системой Linux и подключенным адаптером Wi-Fi, чтобы начать сбор данных.
- Создать задание и определить критерии оценки, которые будут использоваться для проверки результатов.
- Отправить собранные данные на сервер, где будет проводиться анализ и оценка результатов.
- Проанализировать данные и оценить результаты студентов в соответствии с установленными критериями оценки.

Оба подхода имеют свои преимущества и недостатки. Конфигурационные файлы и база данных позволяют более гибко настраивать задания и оценивать работу студентов, но требуют больше времени и усилий для создания и поддержки системы. Второй способ может быть более универсальный и позволяет проверять выполнение лабораторной работы без дополнительных действий для студента.

Список используемых источников:

1. Защита сетевых информационных технологий: учебное пособие / Г. М. Чернокнижный. СПб. : Изд-во СПбГЭУ, 2018. 131 с.

2. Ахрамеева К. А., Ворошнин Г. Е., Ковцур М. М. Исследование устойчивости оборудования mikrotik к атаке association flood на беспроводную сеть семейства ieee 802.11 // Региональная информатика и информационная безопасность.: сб. трудов. СПб. : СПбГУТ. 2021. С. 354-358.

3. Герлинг Е. Ю., Модели нарушителей информационной безопасности / Герлинг Е. Ю., Кулишкина Е. И., Бирих Э. В., Виткова Л. А. // Известия высших учебных заведений. Технология легкой промышленности. 2017. Т. 35. N 1. С. 27-30.

4. Кирилова К. С. Проблема обезвреживания руткитов уровня ядра в системах специального назначения // К. С. Кирилова А. Ю. Цветков В. Н. Волкогонов // I-methods. – 2020. Т. 12. N 3. С. 1-9.

5. Ковцур М. М, Винников С. А., Трезовор В. И., Киструга А. Ю. Исследование сетей Wi-Fi 6E на устойчивость к распространенным атакам // Сборник материалов (тезисов) 51-й международной конференции "Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом". СПб. : ЗАО "Национальный институт радио и инфокоммуникационных технологий", 2023. С. 33-35.

6. 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. N 4. С. 66-71.5

7. Юркин Д. В., Системы обнаружения вторжений в сетях широкополосного радиодоступа стандарта IEEE 802.11 / Юркин Д.В., Никитин В.Н. // Информационно-управляющие системы. 2014. N 2 (69). С. 44-49.

8. Balueva A., Desnitsky V., Ushakov I. Approach to detection of denial-of-sleep attacks in wireless sensor networks on the base of machine learning. 2020. Т. 868. С. 350-355

9. 802.11ax-2021 - IEEE 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 1: Enhancements for High-Efficiency WLAN //IEEE STANDARTS ASSOCIATION URL:https://ieeexplore.ieee.org/document/9442429 (дата обращения: 05.10.2023)

10. Architecting Next Generation Wireless Network with Catalyst Wi-Fi 6E Access Points // Ciscolive URL: https://www.ciscolive.com/c/dam/r/ciscolive/global-event/docs/2022/pdf/BRKEWN-2024.pdf (дата обращения: 23.10.23).

11. A Tutorial on IEEE 802.11ax High Efficiency WLANs // IEEE Xplore URL: https://ieeexplore.ieee.org/document/8468986 (дата обращения: 30.10.23).

12. Consumer WLAN Infrastructure // 650 group URL: https://650group.com/reports/consumer-wlan infrastructure/ (дата обращения: 21.10.2023).

13. Deauthentication // Aircrack-ng URL: http://aircrack-ng.org/doku.php?id=deauthentication (дата обращения: 20.10.2023).

Yacer M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Automation of laboratory work verification based on domestic wireless equipment Eltex. Currently, one of the main tasks of modern education is to improve the quality of training of graduates. To achieve this goal, it is necessary to introduce new teaching methods and technologies. One of these techniques is the automation of the process of checking the completion of laboratory work.

Key words: Automation of work verification, wireless LAN, wireless LAN security, WLAN controller, 802.1x, laboratory work.

Секция 3.2.
Интернет вещей и гетерогенные сети

УДК 004.7
ГРНТИ 50.41.01

ОСОБЕННОСТИ ТЕСТИРОВАНИЯ ИНТЕРНЕТА ВЕЩЕЙ

Т. И. Белая, В. В. Воробьева
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Экосистема интернета вещей постоянно расширяется и влияет на различные аспекты современной жизни, в следствие чего обеспечение надежности, безопасности и производительности программного обеспечения Интернета вещей имеет первостепенное значение. В этой статье рассматриваются фундаментальные компоненты архитектуры Интернета вещей, а также содержится информация о различных уровнях тестирования программного обеспечения для устройств Интернета вещей. Кроме того, в статье освещаются общие проблемы тестирования. В статье подчеркивается важность тщательного тестирования для обеспечения функциональности и безопасности устройств IoT.

тестирование, Интернет вещей, IoT

Введение

Интернет вещей (IoT) — это быстро развивающаяся экосистема, в рамках которой физические объекты и устройства, оборудованные сенсорами и подключенные к интернету, способны собирать, обменивать и анализировать данные, а также взаимодействовать между собой и с центральными системами. Цель IoT — увеличение автоматизации, мониторинг и создание новых возможностей в различных сферах, включая умные дома, сельское хозяйство, транспортную систему, здравоохранение и многое другое. Интернет вещей обеспечивает более эффективное управление ресурсами, что способствует улучшению качества жизни [1].

Поскольку IoT затрагивает многие аспекты повседневной жизни человека, если его программное обеспечение ненадежно, это может привести к серьезным проблемам, включая потенциальные угрозы для здоровья и безопасности. Вследствие чего успех развертывания системы зависит от тщательного тестирования программного обеспечения (ПО). Надежное тестирование гарантирует качество и безопасность IoT-устройств, способствует доверию пользователей и содействует успешной интеграции Интернета вещей в повседневную жизнь. В следствие чего потребность в профессиональных тестировщиках и специализированных методах тестирования постоянно увеличивается, и возникают два ключевых вопроса: какие аспекты следует тестировать в сфере Интернета вещей и какие проблемы существуют в области тестирования ПО для IoT-устройств?

Архитектура Интернета вещей

Архитектура IoT состоит из следующих основных компонентов:

1. *Устройства:* состоит из физических объектов или устройств, оборудованных сенсорами, микроконтроллерами и другими компонентами, которые позволяют им собирать данные, выполнять действия и

подключаться к сети. Например, датчики температуры, камеры, умные термостаты и др.

2. *Сети:* на этом уровне происходит процесс передачи данных между устройствами. Это может включать в себя разнообразные протоколы и технологии, такие как Wi-Fi, Bluetooth, LTE-M, Zigbee, СТРИЖ, LoRa, сотовые сети и даже проводные соединения.

3. *Сервисы:* здесь данные, собранные устройствами, отправляются на обработку на стороне устройства, в облачные вычисления или на краю сети (edge computing). Здесь данные анализируются, фильтруются и преобразуются в полезную информацию. Например, с помощью машинного обучения и искусственного интеллекта.

4. *Приложения:* это могут быть мобильные приложения, веб-приложения или голосовые ассистенты. Они позволяют пользователям взаимодействовать с данными и контролировать IoT-устройства.

Все эти компоненты взаимодействуют в единой системе, обеспечивая сбор, передачу, обработку данных и управление устройствами, что делает IoT возможным и мощным инструментом в различных сферах умных городов [3].

Уровни тестирования Интернета вещей

Тестирование программного обеспечения для устройств Интернета вещей включает в себя несколько уровней, каждый из которых предназначена для проверки конкретных аспектов функциональности Интернета вещей [2].

1. *Уровень тестирования безопасности*

Включает себя идентификацию и устранение уязвимостей, которые могут подвергнуть IoT-устройства риску кибератак. В том числе:

- проверку аутентификации;
- проверку шифрования данных;
- проверку уровня доступа и защиты от атак.

2. *Уровень тестирования компонентов*

Подразумевает проверку на функциональность и работоспособность отдельных IoT-устройств:

- аппаратное обеспечение;
- программное обеспечение;
- сетевые подключения;

приложения;

сервисы.

3. *Уровень функционального тестирования*

Подразумевает проверку того, что IoT-устройство выполняет все свои функции в соответствии с требованиями и пользователь может надежно управлять им. Таким образом включает в себя:

- проверку правильности работы функциональных возможностей устройства;
- проверку взаимодействия между устройствами;
- проверку обработки ошибок.

4. *Тестирование производительности*

Включает в себя оценку производительности программного обеспечения в условиях стресса:

- проверку производительности устройства;
- проверку скорости передачи данных;
- проверку масштабируемости устройства.

Виды тестирования Интернета вещей

Ниже представлены некоторые из основных видов системного тестирования IoT, проводимых тестировщиками в рассматриваемых областях тестирования Интернета вещей [2].

1. *Тестирование удобства пользователя*

Тестирование удобства пользователя для устройств Интернета вещей важно, поскольку оно направлено на обеспечение комфорта пользователей, повышения привлекательность продукта и снижения количество ошибок. Для его проведения следует:

- провести опрос целевой аудитории, чтобы собрать отзывы;
- убедиться, что пользовательские интерфейсы интуитивно понятны и доступны для реальных пользователей.

Регулярное обновление программного обеспечения на основе отзывов повышает удовлетворенность пользователей.

2. *Тестирование производительности*

Имеет решающее значение для программного обеспечения Интернета вещей, поскольку гарантирует его эффективную работу в различных условиях. Для его проведения необходимо создать сценарии, имитирующие различные условия использования, и измерить производительность устройства, чтобы гарантировать его надежность и эффективность.

3. *Функциональное тестирование*

Функциональное тестирование для устройств Интернета вещей (IoT) важно для проверки корректной работы функций и возможностей устройств. Оно направлено на проверку соответствия работы устройств функциональным требованиям. Для его проведения необходимо определить функциональные требования, создать тестовые сценарии и проверить, выполняются ли эти требования в реальных условиях эксплуатации устройства.

Заключение

В заключение, тестирование устройств Интернета вещей — это неотъемлемая часть процесса разработки IoT-решений, требующая особых усилий и внимания к деталям [4]. Четко определенный набор требований и комплексный план тестирования являются основополагающими элементами тестирования ПО Интернета вещей. Следуя передовым практикам, внедряя автоматизацию и уделяя особое внимание безопасности, возможно уменьшить влияние распространеных проблем и предоставить надежные и эффективные решения IoT.

Важно отметить, что эта статья обеспечивает основу для начала тестирования интернета вещей, но не является всеобъемлющей. Во время тестирования Интернета вещей также необходимо учитывать многие аспекты, идеи и новые технологии.

Список используемых источников:

1. Мачей К. Интернет вещей*:* новая технологическая революция. М. : Эксмо, 2018. 336с.

2. Чанцис Ф., Стаис И., Кальдерон П., Деирменцоглу Е., Вудс Б. Практический хакинг интернета вещей : пер. с англ. Л. Н. Акулич. М. : ДМК Пресс, 2022. 480 с.

3. Ли П. Архитектура интернета вещей : пер. с англ. М. А. Райтман. М. : ДМК Пресс, 2018. 454 с.

4. Мачей К. Интернет вещей*:* новая технологическая революция. М. : Эксмо, 2018. 336с.

Belaya T., Vorobeva V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Features of testing the Internet of Things.

The Internet of Things (IoT) ecosystem is constantly expanding and impacting various aspects of modern life, making the assurance of reliability, security, and performance of IoT software a paramount concern. This article discusses the fundamental components of IoT architecture and provides information on various levels of software testing for IoT devices. Additionally, common testing challenges are highlighted in the article, emphasizing the importance of thorough testing to ensure the functionality and security of IoT devices.

Key words: Testing, Internet of Things, IoT.

УДК 621.391
ГРНТИ 49.03.03

ПРИМЕНЕНИЕ СИГНАЛЬНО-КОДОВЫХ КОНСТРУКЦИЙ НА ОСНОВЕ ЭЛЕМЕНТОВ ТРОИЧНОГО ПОЛЯ ГАЛУА И КОДОВ РИДА-СОЛОМОНА ДЛЯ СЕТЕВОГО КОДИРОВАНИЯ

С. С. Владимиров, В. Д. Волков, И. Р. Скакунов, М. Н. Шалагинов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлен метод физического сетевого кодирования сигнально-кодовых конструкций на основе элементов троичного поля Галуа, кодов Рида-Соломона и дифференциальной фазовой модуляции. Приведены формулы, определяющие процедуру сетевого кодирования и декодирования. Результаты имитационного моделирования передачи данных с использованием представленного метода приведены для разных видов модуляции.

сетевое кодирование, помехоустойчивое кодирование, коды Рида-Соломона, поля Галуа

Сетевое кодирование как подход к обработке пакетов данных при, котором их кодирование производится как на оконечных узлах, так и на промежуточных маршрутизирующих узлах был предложен в конце 90-х – начале 2000-х годов [1, 2]. Существуют различные варианты применения сетевого кодирования, одним из которых является показанная на рис. 1 передача в двустороннем релейном канале связи (ДРК), подробно рассмотренная в различных источниках [3-5]. Как показано на рис. 2, при традиционном сетевом кодировании на промежуточном маршрутизирующем узле R выполняется сложение содержимого пакетов P_1 и P_2 от оконечных узлов A и B и последующая передача итогового пакета P_{NC} обоим узлам, которые восстанавливают из него предназначенные им пакеты [3-5]. Оператором «звездочка» на рис. 2 показана обратимая операция сетевого кодирования, которая в простейшем случае соответствует сложению по модулю два.

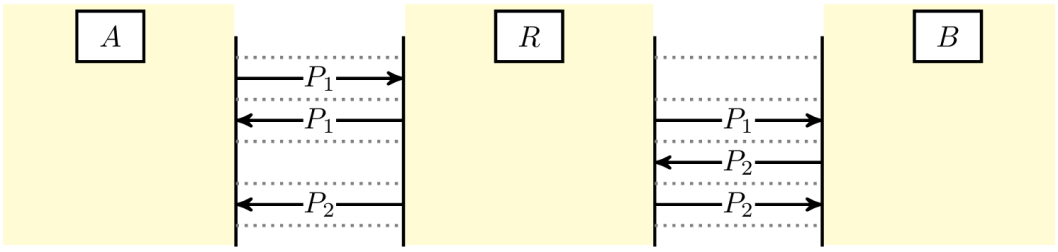


Рис. 1. Передача пакетов в ДРК

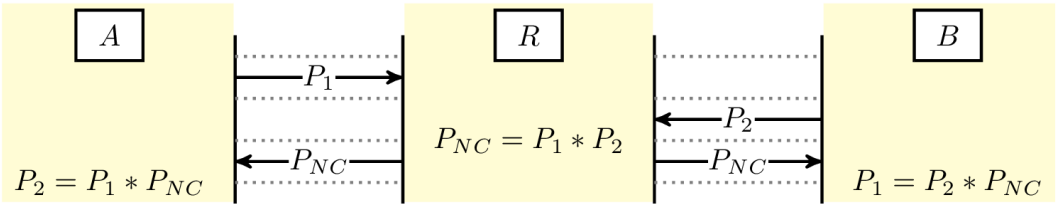


Рис. 2. Передача пакетов в ДРК с сетевым кодированием

Эта процедура требует от узла R преобразовывать передаваемые по эфиру сигнально-кодовые конструкции (СКК) пакетов P_1 и P_2 в двоичные данные, а после выполнения сетевого кодирования преобразовывать пакет P_{NC} в СКК для передачи. Это оправдано в случае применения сетевого кодирования в сети со звездообразной топологией, где выполняется маршрутизация пакетов, априори требующая восстановления заголовков пакетов с адресной информацией. Если же рассматривается вариант ретрансляции с двумя оконечными узлами, то это преобразование выглядит избыточным, что привело к появлению идеи физического сетевого кодирования, при котором формирование пакета P_{NC} производится на уровне СКК, а не двоичных данных, что позволяет выполнять кодирование на физическом уровне приемопередатчика, например в модеме, не выполняя полную процедуру восстановления пакетов до исходных данных [4, 6].

В качестве операции физического сетевого кодирования могут выступать как обычное сложение амплитуд сигналов, так и одновременные операции с фазой и амплитудой сигнала [4, 6-8]. Ранее на кафедре сетей связи и передачи данных СПбГУТ был предложен метод физического сетевого кодирования, основанный на сложении изменений фаз сигналов при использовании дифференциальной фазовой модуляции DPSK-9 [9]. При этом исходные двоичные данные предварительно разбиваются на 3-битовые блоки, которые представляются в виде элементов троичного поля Галуа GF(3^2), как показано в таблице 1.

ТАБЛИЦА 1. Соответствие исходных двоичных данных элементам троичного поля Галуа GF(3^2)

Исходный 3-битовый блок	Элемент поля Галуа GF(3^2)	Смещение фазы Δf, рад
—	0	$0 = 2\pi$
000	$\varepsilon^0 = 1$	$2\pi/9$
001	ε^1	$4\pi/9$
010	ε^2	$6\pi/9$
011	ε^3	$8\pi/9$
100	ε^4	$10\pi/9$
101	ε^5	$12\pi/9$
110	ε^6	$14\pi/9$
111	ε^7	$16\pi/9$

Использованные элементы троичного поля формируют мультипликативную группу элементов, в которой отсутствует нулевой

элемент по операции сложения (ноль). В связи с этим в качестве обратимой операции над элементами группы выступает совокупность операций умножения и деления элементов группы, которые соответствуют сложению и разности степеней элементов группы. Если каждому элементу группы соответствует смещение фазы Δf (табл. 1) при модуляции DPSK-9, то сложению/разности степеней элементов поля соответствует сложение/разность смещений фаз с учетом перехода через нулевое значение, которое вызвано отсутствием нулевого элемента в мультипликативной группе. Процедура сетевого кодирования с опорой на степени элементов поля GF(3^2) определяется формулой (1), а сетевого декодирования — формулой (2).

$$\varepsilon^a \times \varepsilon^b \Rightarrow \begin{cases} \Delta f_{a+1} + \Delta f_{b+1} - \Delta f_1 \equiv \Delta f_{a+b+1}, \text{ если } a+b \le 7; \\ \Delta f_{a+1} + \Delta f_{b+1} \equiv \Delta f_{(a+b+2)\bmod 9}, \text{ если } a+b > 7. \end{cases} \quad (1)$$

$$\varepsilon^a / \varepsilon^b \Rightarrow \begin{cases} \Delta f_{a+1} - \Delta f_{b+1} + \Delta f_1 \equiv \Delta f_{a-b+1}, \text{ если } a \ge b; \\ \Delta f_{a+1} - \Delta f_{b+1} \equiv \Delta f_{(a-b)\bmod 9}, \text{ если } a < b. \end{cases} \quad (2)$$

Применение данного подхода к физическому сетевому кодированию обеспечивает отсутствие необходимости бит-стаффинга, поскольку нулевое состояние сигнала отсутствует и сигнал априори меняет значение фазы относительно предыдущего значения. Отсутствие смены фазы свидетельствует об ошибке при передаче.

Проведенные исследования показывают, что передача данных, использующая сетевое кодирование, подвержена влиянию ошибок. В частности, отмечается размножение ошибок при проведении операции сетевого кодирования. В связи с этим сетевое кодирование следует применять совместно с помехоустойчивым кодированием [10, 11].

Поскольку предлагаемый метод физического сетевого кодирования основан на разбиении данных на 3-битовые блоки, для него удобно использовать помехоустойчивые коды, у которых длины информационного и кодового слов кратны трем битам. При этом следует отметить, что с точки зрения программной реализации кодеков помехоустойчивого кода удобным является применение кодов с длинами информационного и кодового слов кратными 1 байту. В работе рассмотрим применение помехоустойчивого кода Рида-Соломона (12, 6) над полем GF(2^4), который соответствует двоичному коду (48, 24). В этом коде информационное слово состоит из 3 байт (8 блоков по 3 бита), а кодовое слово — из 6 байт (16 блоков по 3 бита).

Таким образом, в работе исследуются СКК на основе кода РС (12, 6), элементов троичного поля Галуа GF(3^2) и модуляции DPSK-9.

Моделирование передачи исследуемых СКК проведено в системе моделирования Octave согласно блок-схеме, показанной на рис. 3. В качестве модели канала передачи выбрана модель АБГШ. Возле каждой операции указано к какому узлу согласно рис. 1–2 она относится.

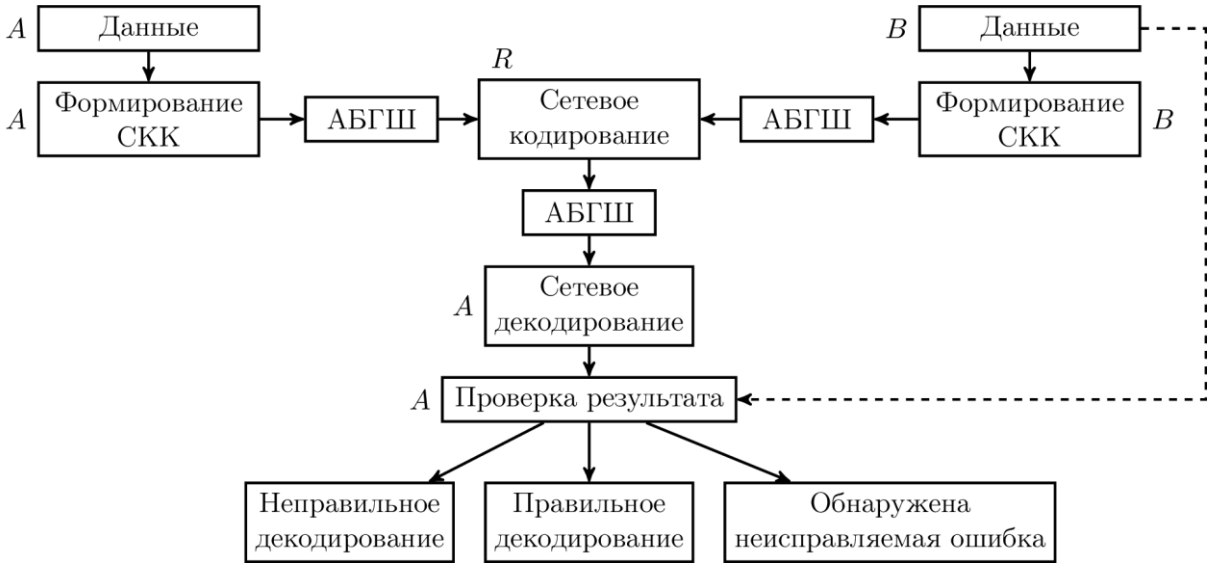


Рис. 3. Блок-схема моделирования передачи СКК в ДРК

Результаты моделирования представлены на графиках на рис. 4. Для сравнения дополнительно показана передача СКК на основе модуляции DPSK-8, при использовании которой отсутствует запрещенный нулевой элемент. На графиках представлены вероятности правильного декодирования кодового слова, неправильного декодирования (необнаруженной ошибки) и обнаружения неисправляемой ошибки.

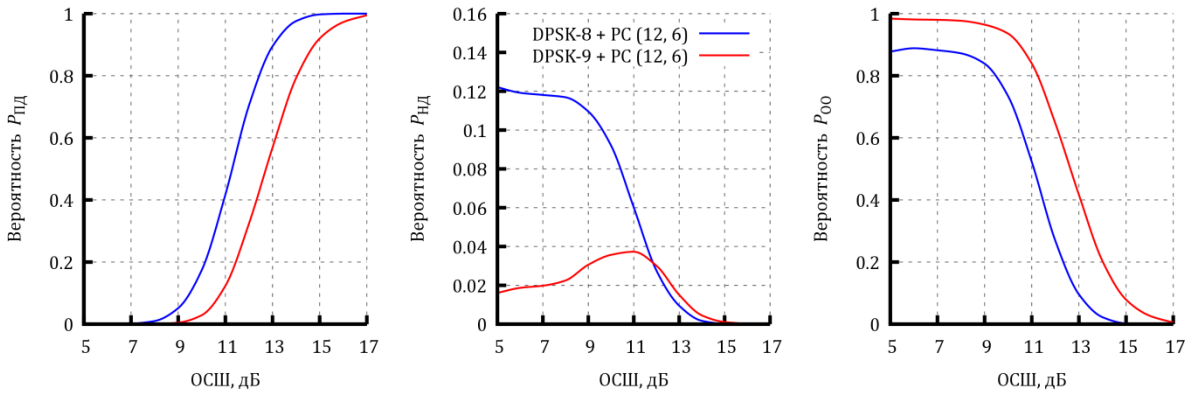


Рис. 4. Вероятностные характеристики СКК с помехоустойчивым кодированием в ДРК

Из графиков видно, что применение СКК на основе троичных элементов поля GF(3^2), кода РС (12, 6) и модуляции DPSK-9 обеспечивает обнаружение большего количества неисправляемых ошибок в сравнении с применением модуляции DPSK-8 за счет наличия запрещенного нулевого символа.

Исследование выполнено в рамках исполнения ПНИ по государственному заданию СПбГУТ на 2023 год.

Список используемых источников:

1. Yeung R. W., Zhang Z. Distributed source coding for satellite communications // IEEE Transactions on Information Theory. 1999. Vol. 45. No. 4. P. 1111-1120.

2. Ahlswede R., Cai N., Li S.-Y. R., Yeung R. W. Network information flow // IEEE Transactions on Information Theory. 2000. Vol. 46. No. 4. P. 1204-1216.

3. Fragouli C., Le Boudec J.-Y., Widmer J. Network coding: an instant primer // ACM SIGCOMM Computer Communication Review. 2006. Vol. 36. No 1. P. 63-68.

4. Liew S. C., Zhang S., Lu L. Physical-layer network coding: Tutorial, survey, and beyond: Network Coding and its Applications to Wireless Communications // Physical Communication. 2013. Vol. 6. Physical-layer network coding. P. 4-42.

5. Amanowicz M., Krygier J. On Applicability of Network Coding Technique for 6LoWPAN-based Sensor Networks // Sensors. 2018. Vol. 18. No. 6. P. 1718.

6. Zhang S., Liew S. C., Lam P. P. Hot topic: physical-layer network coding // Proceedings of the 12th Annual International Conference on Mobile Computing and Networking, MOBICOM 2006. Los Angeles, CA, USA: ACM, 2006. P. 358-365.

7. Chen P., Xie Z., Fang Y., Chen Z., Mumtaz S., Rodrigues J. J. P. C. Physical-Layer Network Coding: An Efficient Technique for Wireless Communications // IEEE Network. 2020. Vol. 34. No. 2. P. 270-276.

8. Jeong S. Y., KabSeok K., Hu J., Bang C. J. Performance analysis of physical-layer network coding with QPSK modulation in wireless IoT networks // ICT Express. 2022. Vol. 8. Iss. 3. P. 419-423.

9. Владимиров С. С. Сетевое кодирование недвоичных сигнально-кодовых конструкций при передаче данных // Электросвязь. 2022. N 7. С. 16-22.

10. Biczok G., Chen Y., Kralevska K., Overby H. Combining forward error correction and network coding in bufferless networks: A case study for optical packet switching // 2016 IEEE 17th International Conference on High Performance Switching and Routing (HPSR). Yokohama, Japan: IEEE, 2016. P. 61-68.

11. Martinez-Penas U., Kschischang F. R. Reliable and Secure Multishot Network Coding Using Linearized Reed-Solomon Codes // IEEE Transactions on Information Theory. 2019. Vol. 65. No. 8. P. 4785-4803.

Vladimirov S., Volkov V., Shalaginov M., Skakunov I.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Application of signal-code constructions based on elements of ternary Galois field and Reed-Solomon codes for network coding.

The paper presents a method for physical network coding of signal-code structures based on elements of the ternary Galois field, Reed-Solomon codes and differential phase shift-keying. Formulas of the network coding and decoding procedure are given. The results of simulation of data transmission using the presented method are given for different types of modulation.

Key words: network coding, error correcting coding, Reed-Solomon codes, Galois fields.

УДК 004.75
ГРНТИ 49.33.29

ТЕХНОЛОГИИ КРОССЧЕЙН СИСТЕМ В DeFi: ИССЛЕДОВАНИЕ И МОДЕЛИРОВАНИЕ

А. А. Козлова, В. Д. Минеева
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья исследует технологию кроссчейн сетей для внедрения в DeFi технологий, а также рассматривается проблема верификации блоков и транзакций при передаче данных между несколькими блокчейнами. Основное внимание направлено на исследование OFMF кроссчейна и Bytom архитектуры, позволяющие реализовать алгоритм пороговой подписи TSS, необходимой для повышения верификации.

OFMF, TSS, DeFi, кроссчейн, Bytom, SideChain, MainChain

1. Введение

DeFi технологии позволяют пользователям пользоваться финансовыми услугами, не полагаясь на централизованные организации. DeFi построены на общедоступном блокчейне, и большинство из них имеют открытый исходный код, что обеспечивает прозрачность. Существуют децентрализованные организации управления DAO’s, гарантирующие, что все знают о том, что произошло в сети, и гарантируют, что злоумышленник не сможет принимать злонамеренные решения в одиночку. Самым большим преимуществом DeFi является то, что он может устранить посредников и работать в условиях нулевого контроля.[3].

До сих пор существует проблема объединения блокчейн сетей и передача данных между различными блокчейнами. Одним из решением такой проблемы становится технология кроссчейн. Существующие модели кроссчейн архитектур выдвигают проблему гарантии верификации блока и последующих транзакций. Без гарантированной завершенности отмененная транзакция в исходной цепочке может привести к неблагоприятным последствиям для цепочки назначения.

В статье представлена модель интеграции OFMF кроссчейна в концепте архитектуры Bytom, а также проведено имитационное моделирование с целью исследования влияния алгоритмов пороговой подписи на количество верифицированных блоков.

2. Предлагаемая система

Экосистема DApp существует в сотнях блокчейнов. Однако блокчейны не обладают встроенной способностью взаимодействовать с внешними системами или API. Это ограничение не только не позволяет блокчейнам взаимодействовать с существующей веб-инфраструктурой, но и с другими блокчейнами.[5]. Основным элементом межсетевого взаимодействия, межсетевым мостом является инфраструктура, которая позволяет отправлять транзакции из исходного блокчейна (source blockchain) в целевой блокчейн (destination blockchain).[3].

Решение базируется на разделении блокчейн цепочки на MainChain и SideChain, что должно увеличить количество верифицированных блоков и последующих транзакций. Для проведения исследования было решено использовать концепт архитектуры Bytom.

SideChain работают как небольшие независимые блокчейны. Отличает их от основных сетей то, что они, как правило, меньше, быстрее и более централизованы. Их работа заключается в обработке и проверке данных для основной цепочки или добавлении функциональности, такой как запуск смарт-контрактов для блокчейнов, которые не могут этого сделать, таких как Биткойн.

Архитектурная концепция Bytom, объединяет архитектуру MainChain и SideChain в единую платформу блокчейн-сети с интегрированным протокол DeFi для оптимизации эффективности потока активов.

Данная архитектура состоит из 3 основных модулей:

1.Value Exchange Engine Magnetic Contract (Magnet);

2.Decentralized Cross-Chain Gateway (OFMF);

3.Layer 2 High Speed Side chain (Vapor).

Архитектура Bytom интегрирует протокол byte-asset DeFi, оптимизируя эффективность потока данных. Основной технологический стек направлен на обслуживание унифицированной кроссчейн платформы.

Технологический стек включает в себя:

•Механизм консенсуса Bytom реализован на базе алгоритма PoW - повышение завершенности консенсуса.

•Инновационная и масштабируемая контрактная система - контрактная система Bytom поддерживает различные операторы и имеет полный язык контрактов по Тьюрингу, но может быть совместима с внешними иными контрактными языками.

•Кроссчейн система OFMF - это система межсетевого взаимодействия, где определен набор открытого универсального формата межсетевого протокола, который обеспечивает безопасность и атомарность всей маршрутизации межсетевых сообщений, имеет полную структуру управления и механизм без доверия, прозрачную работу и интегрированную систему безопасности с несколькими подписями. Предоставляет решение с несколькими подписями: спонсор, маркет-мейкер и обслуживающая сторона создают кошелек, отделяют торговлю от операций по вводу и выводу средств и выбирают адрес вывода средств с помощью механизма белого списка. Любая другая общественная сеть может независимо получить доступ к интероперабельной сетевой системе в соответствии со стандартами открытых протоколов и механизмами доступа.[3].

3. Результаты эксперимента

Для того, чтобы проанализировать качественную эффективность архитектуры Bytom на базе OFMF кроссчейна в рамках внедрения в текущие сетевые модели было предложено использовать блоки данных bitcoin.

Для проведения моделирования была выбрана модель BlockSim, где были заданы ключевые параметры блока и сетевые характеристики, а также изменен алгоритм консенсуса. В качестве основного фреймворка был взят

OFMF кроссчейн.[4]. OFMF фреймворк представляет собой отказоустойчивую распределенную сетевую систему без разрешений. Ее основная функция обновлена для координации всех узлов Fednode для децентрализованного безопасного хранения и передачи межсетевых активов, а также анализа и выполнения межсетевых транзакций с помощью защищенных множественных вычислений (sMPC) и алгоритмов консенсуса. Fednodes — это более открытый федеративный узел. Он предоставляет процессор и хранилище для распределенной сети шлюзов. Любая роль в любой экосистеме может стать Fednodes через сопутствующие услуги.

Схема пороговой подписи обеспечивает распределенную подпись среди n узлов таким образом, что любая подгруппа размером t + 1 может подписать, в то время как любая группа с t или меньшим количеством узлов не может

В технологии TSS, n-ое количество узлов, проводят вычисления публичного ключа, каждый из которых обладает своей собственной секретной долей (индивидуальной частью секретного ключа). Из публичного ключа генерируется публичный адрес таким же образом, как и в традиционной системе, делая блокчейн независимым от количества совместных узлов.

Алгоритмами, используемыми для создания биткойн-адреса из открытого ключа, являются алгоритм безопасного хэширования (SHA) и дайджест сообщений оценки примитивов целостности (RIPEMD), в частности SHA256 и RIPEMD160.

В данном исследовании генерация публичного ключа была реализована за счет алгоритма RIPEMD - 160. Начиная с открытого ключа K, вычисляется хэш SHA256, а затем вычисляется хэш RIPEMD160, получая 160-битное (20-байтовое) число.

$$A = RIPEMD160(SHA256(K)),$$ где

A – результирующий биткойн адрес;

K – открытый ключ.

Преимущество заключается в том, что приватный ключ больше не является единственной точкой отказа, поскольку его части распределены среди всех участников.

Данные - средняя задержка распространения транзакции на ноды, количество генерируемых транзакций в секунду - 10 были взяты, исходя из средних показателей архитектуры Bitcoin сети. [1]

В качестве исходных данных были заданы следующие параметры: количество генерируемых транзакций в секунду - 10 тр/с., общее количество обрабатываемых транзакций - 200 тр., количество узлов на одном шлюзе - 10 шл., количество шлюзов в сети - 2 шл.

А также параметры симуляции: средняя задержка распространения транзакции на ноды - 0,006 секунд, время симуляции - 10 секунд, количество итераций симуляции - 5

Исходя из проведенных симуляций модели - были получены следующие данные (рис. 1): задержка отправки транзакции примерно одинаковая и не

зависит от типа технологии кроссчейн. Средние показатели равняются 10,012 мс для OFMF with TSS кроссчейн и 11,707 мс для IBC кроссчейн.

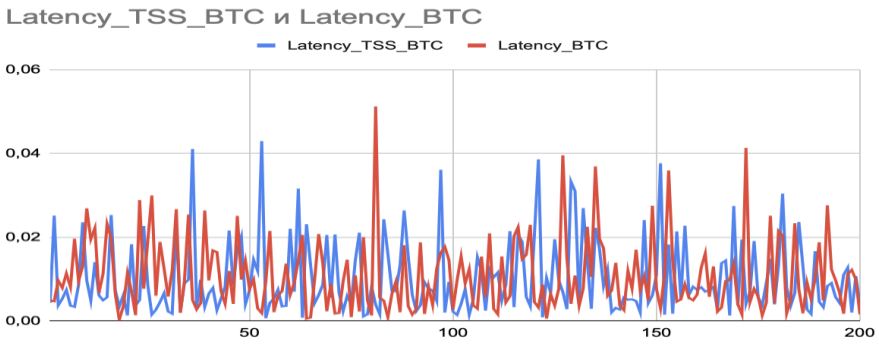


Рис. 1. Показатели задержек отправки транзакции

При этом наиболее ключевыми стали показатели верификации блоков. В приведенной таблице представлены процентные показатели верифицированных блоков в результате проведения моделирования.

ТАБЛИЦА 1. Показатели верификации блоков на MainChain и SideChain

	% of main blocks	**% of side blocks**
OFMF_TSS	100	93,11
IBC	66,67	27,59

Проведенное исследование показало, что действительно существует проблема гарантии верификации блока и последующих транзакций. Количество подтвержденных данных на source chain показаны на рис. 2, 3.

Рис. 2. Сравнение показателей верификации на SideChain OFMF и IBC кроссчейнов

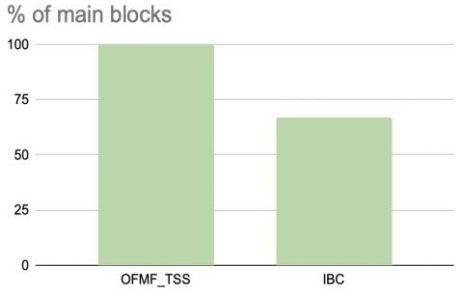


Рис. 3. Сравнение показателей верификации на MainChain OFMF и IBC кроссчейнов

Без гарантированной завершенности отмененная транзакция в исходной цепочке (например, реорганизация блока) может привести к неблагоприятным последствиям для цепочки назначения.[2].

Существующие модели кроссчейн сетей показывают, что для запуска полноценного узла необходимы большие временные, сетевые и аппаратные ресурсы. Количество полных узлов в сети меньше, чем количество легких, соответственно нагрузки на сеть увеличиваются.

По мере распространения блокчейн пользователи, привыкшие доверять централизованным системам, считают процесс создания полноценного узла слишком громоздким. В результате конечные узлы не запускают свой собственный полноценный узел, а подключаются к RPC-провайдерам, которые не гарантируют передачу транзакции в сеть и информирование их о текущем состоянии блокчейна. Соответственно процесс дальнейшей верификации данных и безопасность самопроверки снижается. Предложенная модель OFMF кроссчейна с интегрированным алгоритмом TSS реализует интероперабельное блокчейн-решение для устранения рисков, которые могут возникнуть в процессе верификации данных и последующих транзакциях.

Список используемых источников:

1. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2009.
2. Cosmos SDK Contributors, The cosmos sdk: X/ibc. https://github.com/cosmos/cosmos-sdk/tree/master/x/ ibc
3. Ethan Frey, IBC protocol specification v0.3.1. https://github.com/cosmos/ics/blob/master/archive/v0_ 3_1_IBC.pdf
4. P. Technologies. Substrate: The platform for blockchain innovators. https://github.com/paritytech/ substrate, 2020.
5. Buterin V. Standartized Contract APIs. 2015. [Электронный ресурс]. URL:https://github.com/ethereum/wiki/wiki/Standardized_Contract_APIs/499c882f3ec123537fc2fccd57eaa29e6032fe4a
6. Andreas M. Antonopoulos. MASTERING BITCOIN PROGRAMMING THE OPEN BLOCKCHAIN. 2nd ed.1005 Gravenstein Highway North, Sebastopol, 2015. pp.746-786.

Kozlova A., Mineeva V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Crosschain systems technologies in DeFi research and modeling.
This paper investigates crosschain network technology for implementation in DeFi technologies, and considers the problem of block and transaction verification when transferring data between multiple blockchains. The focus is on the study of OFMF crosschain and Bytom architecture to enable the implementation of TSS threshold signature algorithm required to enhance verification.

Key words: OFMF, TSS, DeFi, кроссчейн, Bytom, SideChain, MainChain.

УДК 004.725.5
ГРНТИ 49.33.29

MANET-СЕТЬ И ЕЕ ПРОТОКОЛЫ. ДВУХРАНГОВАЯ MANET-СЕТЬ.

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

Время бежит все быстрее, появляются новые технологии, протоколы, а для них новые требования. В данной статье рассказывается про MANET-сеть, технология, которая актуальна в данный момент и поможет решить некоторые из задач нашего времени. Рассматривается какие протоколы могут подойти для использования, а также где может использоваться эта технология.

MANET сеть, ad-hoc сети, мобильные сети, самоорганизующиеся сети

Рубеж второго и третьего тысячелетия позволил расширить область применения беспроводных широкополосных сетей благодаря двум задачам: последней мили и построения децентрализованных сетей.

Суть задачи последней мили в предоставлении доступа к сервисам проводной инфраструктурной сети для конечных пользователей. Для этого в проводной сети появилась точка доступа, к которой по беспроводному каналу подключались клиенты, так называемая «клиент-серверная» архитектура.

Децентрализованными сетями, также называемыми ad-hoc сетями – самоорганизующиеся сети, которые создаются из равнозначных станций при необходимости, без проводной инфраструктуры. Задача может быть решена наделением полномочиями «сервера» некоторого устройства, по отношению к другим, которые являются «клиентами».

Отказываясь от «клиент-серверной» архитектуры, построение сетей класса ad-hoc для решения вышеописанных задач становится совершенно разным, это отражается в стандарте IEEE 802.11 беспроводных локальных сетей – в стандарте описаны два типа сетей: ad-hoc сети и инфраструктурные сети. [3]

Сети, называемые инфраструктурными, использующие ресурсы проводных сетей и предоставляющие точки Wi-Fi доступа различным мобильным устройствам пользователей к ресурсам Интернета. Отличие беспроводных ad-hoc сетей заключается в случайном соединении между собой мобильных устройств.

Одним из самых развитых вариантов беспроводных ad-hoc сетей считаются одноранговые мобильные сети с произвольной структурой – MANET сети. Они создаются из множества мобильных узлов, которые перемещаются в пространстве, а таже способны к работе изолировано или

иметь доступ к выходу в стационарную сеть. У сетей MANET следующие особенности:

- У сети нет инфраструктуры и нет централизованного управления;
- В сети отсутствуют базовые станции и маршрутизаторы;
- Мобильные устройства имеют ограниченную емкость батарей;
- Изменение топологии сети происходит в произвольные время из-за мобильных узлов;
- Частое изменение подключенных новых и отключенных узлов от сети;
- Повреждения связности сети. [4]

Задача протокола транспортного уровня сети MANET в обеспечении сервиса эффективной и надежной передачи данных на основе коммутации пакетов в беспроводных мобильных сетях.

- Эффективность – это минимизация количества повторных передач, если потерян пакет, нарушена связь, смена маршрута, а ещё снижение вероятности перегрузок в сети.
- Надежность — это извещение пользователя об одной из двух ситуаций, возникающих при доставке данных: об успешно доставленных данных адресату или неустранимой ошибки и доставка данных не произошла.
- Транспортный протокол, который обеспечивает вышеописанные качества в условиях меняющейся топологии сети показывает устойчивость передачи данных в сетях MANET.

В сети MANET, которая состоит из нескольких мультиузловых беспроводных связей, могут происходить потери пакетов из-за ошибок физического и канального уровней. В этих условиях TCP показывает существенные недостатки, которые можно выделить в группы:

1) конфликты и коллизии, которые приводят к ошибкам;
2) недочеты, которые появляются из-за мобильности узлов;
3) невозможность обработки потока неупорядоченных пакетов;
4) высокая энергозатратность.

Сейчас уже есть решение этих проблем – специально созданные транспортные протоколы, являющиеся модификацией протокола TCP или созданные с «нуля». Выделяются три класса протоколов: TCP с обратной связью (TCP-F, TCP-ELFN, ATCP); TCP без обратной связи (TCP-Fixed-RTO, TCP-DOOR, TPA, ATP, ITP) и протоколы, которые используют специальные изменения на других уровнях стека протоколов (Neighbourhood RED и др.).

Обратная связь, несущая информацию о причине перегрузки сети, позволяет TCP различать проблемы, подобные перегрузке сети, обрыв маршрута, ошибки канала и т.д. Следует отметить, что механизм обратной связи влечет за собой дополнительные сложность и увеличенную стоимость в мобильных сетях. [1]

В данный момент используют несколько протоколов, которые обеспечивают маршрутизацию мобильных самоорганизующихся сетей. Их можно условно разделить на протоколы с проактивной (табличной)

маршрутизацией, протоколы с реактивной маршрутизацией (работающие по запросу) и их гибриды.

Так как протоколы, которые разработаны для маршрутизации проводных сетей, не предназначены для работы с MANET сетями, для этих сетей придумали специальные протоколы маршрутизации, которые успешно применяются и в других топологиях сетей. Одним из таких протоколов является Ad hoc On-Demand Distance Vector (AODV). Это протокол динамической маршрутизации, который относится к реактивным, потому что устанавливает маршрут к адресату по требованию, за основу вычисления которого взят дистанционно-векторный алгоритм маршрутизации. Другим известным протоколом является Dynamic Source Routing (DSR), протокол маршрутизации для MANET с топологией mesh. Его основа заключается в формировании маршрута по требованию, передавая широковещательные адреса, также этот протокол не использует таблицы маршрутизации на каждом промежуточном устройстве.

Optimized Link-State Routing (OLSR) – протокол маршрутизации, использующийся как в MANET, так и в других беспроводных сетях. Его основа — работа с таблицами. Есть гибридный протокол маршрутизации, который создан при разработке протокола 802.11s – Hybrid Wireless Mesh Protocol (HWMP), известный как Wi-Fi. Он совместил в себе протокол дистанционно-векторной маршрутизации по запросу и механизмы, работающие на MAC-уровне, при этом эти два режима могут быть как отдельными друг от друга, так и одновременными.

Еще одним видов протоколов являются протоколы маршрутизации, использующие геоданные. У каждого такого протокола свой принцип работы.

Протокол GPSR использует стратегию «жадной пересылки» (рис. 1) - поиск для передачи данных ближайшего к месту назначения узла, в случае отсутствия такого узла, поиск альтернативного маршрута.

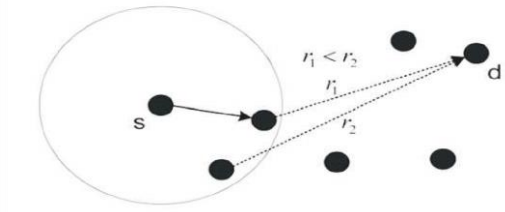


Рис. 1. «Жадная» пересылка (где r - наиболее подходящий узел)

Протоколы DREAM и LAR используют пересылку пакетов всем соседним узлам, располагающихся по направлению к пункту назначения.

Протокол LAKER (потомок DSR и LAR), его принцип — сведение к минимуму нагрузки на сеть во время процесса открытия маршрута за счет уменьшения зоны, в которую будут переадресованы пакеты запроса маршрута, и протокол MOvement based Routing Algorithm (рис. 2), принимающий во внимание направление движения соседних узлов.

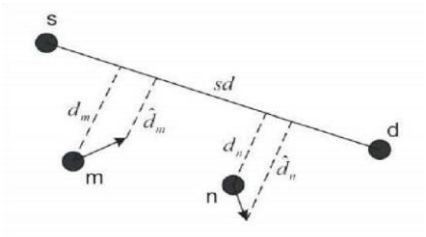


Рис. 2. Направление положения узлов в протоколе MORA

Есть протоколы, маршрутизация которых структурирована в двух слоях, другими словами, имеют иерархию (иерархическая маршрутизация). Эти протоколы используются для маршрутизации на длинные и короткие расстояния, при этом используется геомаршрутизация на длинных дистанциях, а для коротких расстояний, внутри определенной зоны или объединения узлов, применяются схемы маршрутизации других видов. Наиболее известный протокол, использующий данные о местоположении абонентов сети (ГЛОНАСС).

Для анализа любого протокола маршрутизации, который используется в беспроводных сетях, за основу стоит брать параметры производительности сети и задержки передачи данных. Выбор алгоритма для самоорганизующейся сети должен исходить из комплекса различных показателей, которые характеризуют качество протокола, так как разные протоколы имеют свои преимущества и недостатки. [5]

Двухуровневое представление в рамках одного сегмента сети MANET позволит использовать алгоритмы маршрутизации на каждом из уровней, это уменьшит объем служебного трафика. Двухранговая сеть содержит стандартные узлы связи и станции привязки, как показано на рис. 3. Узлы занимаются построением маршрута внутри сети, используя реактивный протокол маршрутизации AODV. Первый радиоинтерфейс станций привязки выполняет обмен информацией внутри подсети MANET, используя протокол AODV, второй радиоинтерфейс служит для взаимодействия между подсетями на основе протокола OSLR, мощность на передачу такого узла выше, чем у обычных узлов, имеющих только один интерфейс взаимодействия внутри сети.

Сравнивая одноранговую и двухранговую сеть MANET растет коэффициент PDR (процент доставки пакетов) на 15%, пропускная способность становится выше на 25%, а средняя задержка уменьшается на 30%. [2]

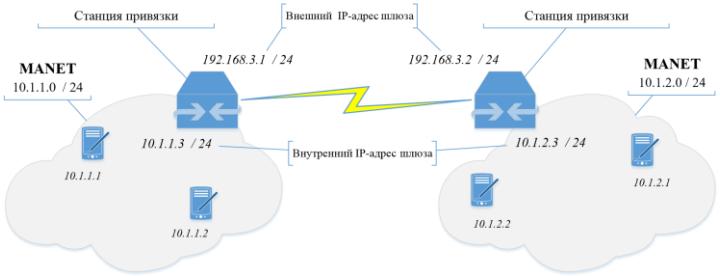


Рис. 3. Сегмент взаимодействия подсетей в двухранговой сети MANET

Одно из направлений развития беспроводных мобильных самоорганизующихся сетей связи MANET – это формирование систем связи, предназначенных для передачи интенсивного трафика и трафика реального времени (информации, передаваемой через голосовое сообщение или видеоинформацию). Нужно отметить, что эти сети обладают низкой стоимостью, высокой скоростью развертывания, а также высокой эффективностью.

MANET сети можно использовать в самых разных сферах, в сетях военного назначения, аварийных сетях при ЧС, на территориях удаленных районов, где нет стационарной инфраструктуры. «Умный дом», как пример использования сети MANET, а также различные дроны и их системы. [5]

Список используемых источников:

1. Иовлев Д. И., Бойченко И. В., Абрамов В. В. Повышение устойчивости передачи данных в сетях MANET // Доклады ТУСУР. 2012. N 2. Ч. 1. С. 171-177.

2. Волков А. С., Муратчаев С. С., Кульпина Ю. А. Разработка имитационной модели двухранговой сети MANET // Труды МАИ. 2019. N 109.

3. Хоров Е. М. Знакомство с современными беспроводными технологиями. Многошаговые беспроводные сети: принципы построения и открытые задачи // Институт проблем передачи информации им. А. А. Харкевича Российской академии наук. 2013.

4. Сомов С. К. Использование репликации данных в мобильных сетях произвольной структуры MANET // Управление развитием крупномасштабных систем: материалы XIV Междунар. конф., Москва, 27-29 сент. 2021 г. М. : ИПУ РАН, 2021. С. 1478-1485.

5. Воженников А. А. Сравнение протоколов маршрутизации в MANET-сетях // Технические науки. Евразийский Союз Ученых. N 1 (22), 2016. С. 44-46.

Lokhov D.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

MANET network and its protocols. Two-rank MANET network.

Time is passing faster and faster, new technologies and protocols are appearing, and new requirements for them. This article talks about the MANET network, a technology that is relevant at the moment and will help solve some of the problems of our time. It looks at what protocols might be suitable for use, as well as where this technology might be used.

Key words: MANET, ad-hoc networks, mobile networks, wireless self-organizing networks.

УДК 004.021
ГРНТИ 49.33.35

КЛАСТЕРИЗАЦИЯ КАК МЕТОД УМЕНЬШЕНИЯ ПОМЕХ В СЕТЯХ ВЫСОКОЙ ПЛОТНОСТИ

М. Р. Матукас, А. И. Парамонов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Кластеризация в сетях высокой плотности является эффективным методом уменьшения помех и повышения эффективности работы сети. В данной статье будут рассмотрены основные алгоритмы кластеризации и их преимущества. В результате будут приведено сравнение рассмотренных алгоритмов по требуемым входным данным. Рассмотренные алгоритмы могут быть использованы для уменьшения помех в сетях высокой плотности.

сети высокой плотности, помехи, кластеризация, FOREL, k-средних, DBSCAN, OPTICS

Большое количество устройств интернета вещей отражается на высокой их концентрации в пространстве. Это приводит к возникновению сетей высокой и сверхвысокой плотности [1]. Обычно, к сетям высокой плотности относят сети с одним и более устройством на квадратный метр.

В сетях высокой плотности, количество устройств, подключенных к сети, значительно выше, чем в обычных сетях. Это создает проблемы с управлением и эффективным использованием доступных ресурсов. Из-за высокой плотности устройств помехи в сети также значительно возрастают, что приводит к снижению скорости передачи данных и ухудшению качества связи. Метод кластеризации это один из способов, который позволяет решить эту проблему и улучшить производительность сети. Помимо кластеризации для борьбы с помехами в сетях высокой плотности можно использовать и другие методы, например, выравнивание помех и распределение ресурсов.

Кластеризация основывается на принципе разделения сети на более мелкие подсети (кластеры), так, чтобы объекты из одного кластера были более похожи друг на друга, чем на объекты из других кластеров.

В каждом кластере выбирается головной узел, который отвечает за распределение ресурсов внутри этого кластера. Кластеризация позволяет сократить объем вычислений, повысить эффективность и производительность работы сети.

В настоящее время исследования алгоритмов кластеризации в основном сосредоточены на теории графов и матриц. Узлы, ребро между узлами и вес ребра соответствуют устройству, помехам между кластерами и величине этих помех. Граф декомпозируется на множество подграфов, например, с помощью алгоритма k-средних. Каждый узел в подграфе является кластером. Головной узел отвечает за планирование ресурсов кластера и отправку других управляющих сигналов. Головной узел решает проблему

планирования только внутри кластера, что позволяет уменьшить размер сети и количество обрабатываемых операций. Алгоритм кластеризации на основе матрицы подсчитывает помехи между двумя узлами. Эти значения помех объединяются в матрицу.

Один из способов кластеризации заключается в том, чтобы разделить элементы с очень большими помехами между собой на кластеры. Таким образом, помехи между различными кластерами очень мала. Получается, что сначала гарантирует качество связи участников кластера, а затем подавляет межкластерные помехи. Большинство исследований по управлению помехами основано на этой идее.

Преимущества кластеризации в сетях высокой плотности:

1. Уменьшение помех.
2. Повышение производительности.
3. Увеличение масштабируемости.

Путем группировки устройств в кластеры и определения оптимальных маршрутов передачи данных, сеть становится более гибкой и способной обрабатывать большое количество устройств и данных. Это позволяет сети легко расширяться и адаптироваться к изменяющимся условиям и требованиям.

Алгоритмы кластеризации.

Алгоритм *k*-средних.

Алгоритм стремится минимизировать суммарное квадратичное отклонение точек кластеров от центров этих кластеров. Этот алгоритм требует указания количества кластеров. Он хорошо масштабируется для большого количества образцов и используется в широком диапазоне областей применения во многих различных областях.

Алгоритм сдвига среднего значения.

Алгоритм среднего сдвига в основном назначает точки данных кластерам итеративно, смещая точки в сторону максимальной плотности точек данных, то есть центроида кластера. В отличие от кластеризации алгоритмом k-средних это непараметрический алгоритм.

Разница между алгоритмом *k*-средних и среднего сдвига состоит в том, что не нужно указывать количество кластеров заранее, потому что количество кластеров будет определяться алгоритмом по данным. Данный алгоритм не предназначен для большого количества узлов.

Алгоритм FOREL.

Алгоритм кластеризации FOREL заключается в разделении объектов на кластеры на основе их близости друг к другу. Изначально число кластеров неизвестно, но они подбираются таким образом, чтобы минимизировать суммарное расстояние между объектами внутри каждого кластера. Кластеры, получаемые этим алгоритмом, имеют сферическую форму. Количество кластеров зависит от радиуса сфер: чем меньше радиус, тем больше получается кластеров.

Алгоритм DBSCAN.

Алгоритм DBSCAN - это плотностный алгоритм для кластеризации пространственных данных с присутствием шума. Идея алгоритм заключается в том, что внутри каждого кластера наблюдается типичная плотность точек, которая заметно выше, чем плотность снаружи кластера, а также плотность в областях с шумом ниже плотности любого из кластеров. Из-за этого кластеры, обнаруженные с помощью этого алгоритма, могут иметь любую форму, в отличие от k-средних, которое предполагает, что кластеры имеют выпуклую форму. Ещё точнее, что для каждой точки кластера её соседство заданного радиуса должно содержать не менее некоторого числа точек, это число точек задаётся пороговым значением. Таким образом, кластер представляет собой набор узлов, которые находится в области высокой плотности. Одиноко расположенные узлы помечается как шум.

Алгоритм OPTICS.

Алгоритм OPTICS сочетает в себе элементы иерархической и плотностной кластеризации. Алгоритм строит граф достижимости, который учитывает расстояния между точками и плотность данных. На основании графа определяются плотные области и границы кластеров.

Преимущество OPTICS перед DBSCAN в том, что OPTICS может обнаруживать кластеры различной плотности и формы. Главным минус заключается в том, что требуется большое количество вычислений.

Помимо этих алгоритмов есть множество других, например, усовершенствованный алгоритм DBSCAN [2], схема CPUCIC [3], усовершенствованный алгоритм *k*-средних [4], алгоритм на основе фрактальной размерности [5].

ТАБЛИЦА 1. Сравнение алгоритмов кластеризации на основе входных данных

Алгоритм	Плотность узлов в кластере	Количество кластеров	Размер кластера
k-средних	-	+	-
Сдвига среднего значения	-	-	-
FOREL	-	-	+
DBSCAN	+	-	-
OPTICS	-	-	-

По результатам анализа были рассмотрены основные алгоритмы кластеризации, приведено сравнение этих алгоритмов на основе входных данных в таблице 1, описан основной принцип их работы, их преимущества. Приведенный анализ можно использовать для выбора алгоритма кластеризации для уменьшения помех, так и для исследования и разработки новых алгоритмов кластеризации.

Список используемых источников:

1. Кучерявый А. Е., Трехмерные многослойные гетерогенные сверхплотные сети. / Кучерявый А. Е., Парамонов А. И., Маколкина М. А., Мутханна А. С. А., Выборнова А. И., Дунайцев Р. А., Захаров М. В., Горбачева Л. С., Чан З. Т., Марочкина А. В. // Информационные технологии и телекоммуникации. 2022. Т. 10. N 3. С. 1-12.
2. By Вьет Тханг, Пантюхин Д. В., Галушкин А. И. Гибридный алгоритм кластеризации FastDBSCAN // Труды МФТИ. 2015. Том 7.
3. Guomin Wu1, Guoping Tan, Defu Jiang, Fei Feng, Hanfu Xun, Qi Wang, Xinyu Shen, Ziming Sheng. User-Centered Interference Coordination in the Ultra-Dense Network: a Cluster and Priority Perspective // Mobile Networks and Applications. 2021. 26:1195–1205
4. Liu, L., Garcia, V., Tian, L., et al. Joint Clustering and Inter-Cell Resource Allocation for CoMP in Ultra Dense Cellular Networks // IEEE International Conference on Communications, London, 8-12 June 2015. 2560-2564.
5. Марочкина А. В. Моделирование и кластеризация трехмерной сети интернета вещей с применением метода оценки фрактальной размерности. // Электросвязь. 2023. N 6. С. 62-68.

Matukas M., Paramonov A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Clustering as a method of reducing interference in high-density networks.

Clustering in high-density networks is an effective method of reducing interference and improving network efficiency. This article will discuss the main clustering algorithms and their advantages. As a result, a comparison of the considered algorithms will be given according to the required input data. The algorithms considered can be used to reduce interference in high-density networks.

Key words: High-density networks, interference, clustering, FOREL, k-means, DBSCAN, OPTICS.

УДК 621.396.99
ГРНТИ 49.33.29

КОНВЕРГЕНЦИЯ ТЕХНОЛОГИЙ 5G И WI-FI 6

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

Беспроводная связь стала жизненно важным аспектом нашей повседневной жизни в связи с растущим спросом на более быстрые, надежные и безопасные беспроводные сети. По мере роста числа подключенных устройств потребность в надежной инфраструктуре беспроводной сети становится еще более острой. В статье рассматривается тема интеграции технологий фиксированного беспроводного доступа и мобильного радиодоступа, сценарии их использования.

беспроводная сеть, 5G, Wi-Fi 6, ATSSS

Согласно определению МСЭ-Т в контексте сетей 5G конвергенция фиксированных и мобильной сети 5G (FMC) – это объединение возможностей, которые предоставляют услуги и приложения конечным пользователям независимо от используемых технологий фиксированного или мобильного доступа и независимо от местоположения пользователей. [1]

Рассмотрим основные сценарии использования 5G и Wi-Fi 6:

- общедоступный и корпоративный Wi-Fi: расширяет возможности и сценарии развертывания для операторов и поставщиков услуг связи, позволяя им обеспечивать более качественное взаимодействие с пользователем и поддерживать общий контроль над различными сетями;
- индустрия 4.0: использование устройствами M2M и IoT сетей FMC как 5G NR, так и Wi-Fi, что позволит предприятиям, использующим данные в режиме реального времени, оптимизировать производство, минимизировать время простоя и снизить затраты; благодаря низкой задержке 5G и высокой пропускной способности предприятия могут передавать большие объемы данных в режиме реального времени, позволяя автоматизированным системам принимать немедленные решения на основе полученных данных; Wi-Fi 6 позволяет подключать большое количество датчиков и устройств с системами искусственного интеллекта и машинного обучения, что позволяет контролировать производственный процесс;
- умный город: сети доступа 5G NR и WiFi в сети FMC могут взаимодействовать для создания высоконадежных соединений, при которых становится проще управлять трафиком граничных и облачных вычислений и приложений, требующих больших объемов данных;
- домашнее использование 5G и WiFi 6: наличие опций доступа как к 5G NR, так и к Wi-Fi 6 позволяет обеспечить различные варианты передачи трафика в жилых помещениях, чтобы повысить возможности подключения и обеспечить более всестороннее взаимодействие с конечным пользователем;

- автономное использование устройств WiFi 6: конвергенция позволяет обеспечить доступность сервисов приложений 5G для большего числа устройств в удаленной и труднодоступной местности. [2]

Основой реализации FMC 5G и WiFi 6 является стандартизация для использования в сетях 5G PDU-сессии с множественным доступом (Multi-Access PDU Session). PDU-сессия – это сессия, трафик которой может быть отправлен через сеть радиодоступа или через сеть беспроводного доступа. 3GPP определил в Release 16 [3] функцию под названием ATSSS (Access Traffic Steering-Switching-Splitting), которая управляет конвергенцией сетей доступа 5G и Wi-Fi 6. ATSSS предназначена для выполнения функций управления, переключения и разделения трафика в сети доступа. К функции управления относится возможность выбора наилучшего канала для передачи трафика пользователя, функция переключения обеспечивает возможность выполнения передачи обслуживания без прерывания к другой сети, функция разделения отвечает за одновременное использование и связывание различных сетей.

Функция ATSSS позволяет поставщику услуг настраивать правила ATSSS и передавать их на устройство через ядро 5G. Эти правила будут определять, как устройство должно использовать сети доступа 3GPP и не-3GPP, которые могут быть у него доступны, особенно в отношении отправки восходящего трафика. И наоборот, для трафика по нисходящей линии связи ядро 5G может предоставлять правила для UPF (User Plane Function), которая определяет, какая сеть доступа должна использоваться для того или иного потока трафика (рис.1).

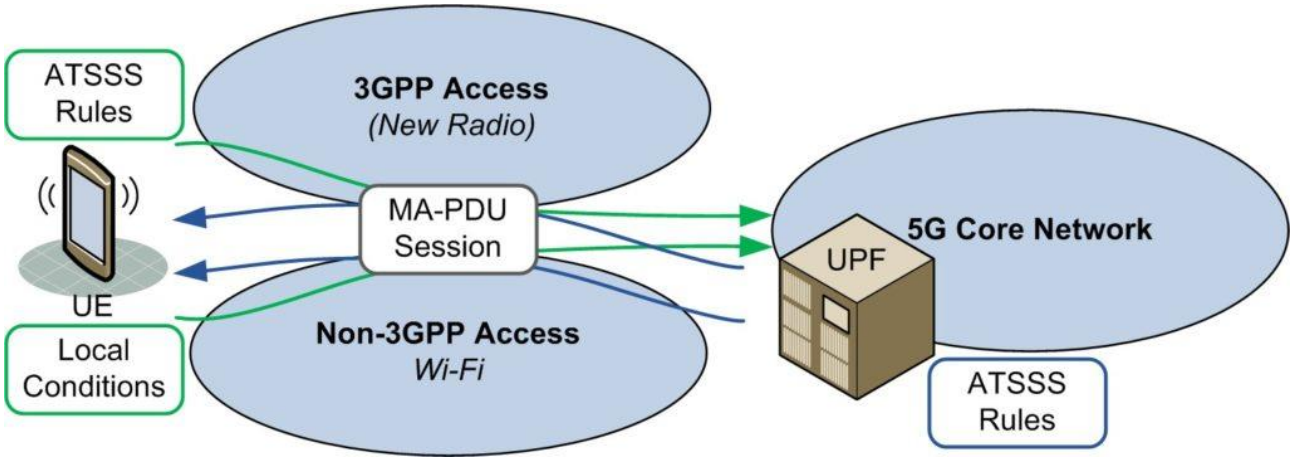


Рис. 1. Управление трафиком ATSSS

В рамках ядра 5G управление ATSS в основном осуществляется PCF (Policy Control Function), в обязанности которой входит предоставление правил ATSSS как устройству, так и SMF (Session Management Function) на основе политики поставщика услуг.

Для поддержки функции ATSSS архитектура ядра 5G (рис. 2) расширена новыми функциями N3IWF, TNGF, TWIF и W-AGF позволяющими

реализовывать доступ к услугам 5G через сеть беспроводного доступа с технологией WiFi 6 для доверенных и не доверенных сетей.

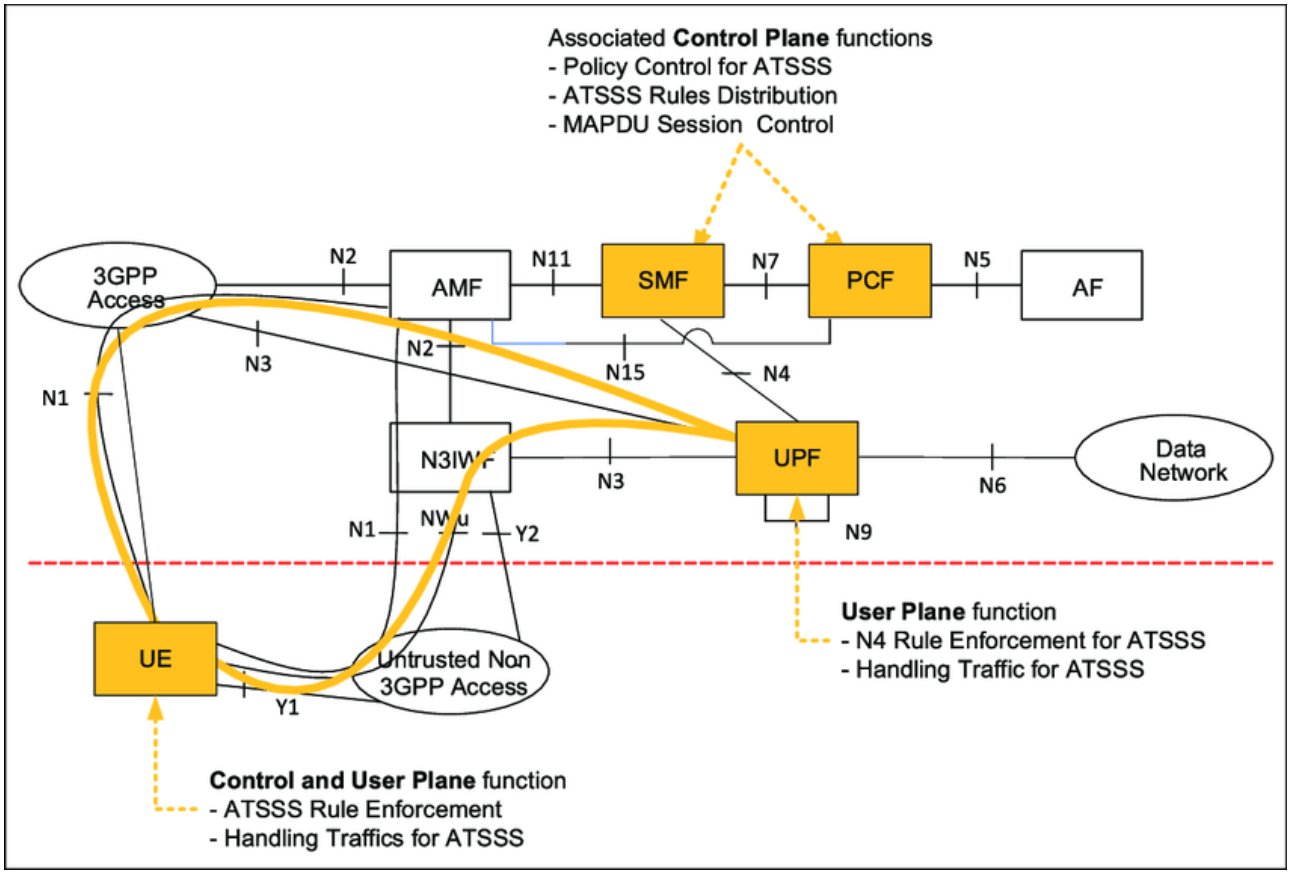


Рис. 2. Архитектура ядра 5G с поддержкой функции ATSSS

Объединение 5G и Wi-Fi 6 дает ряд преимуществ:

- высокоскоростное бесшовное соединение: 5G обеспечит высокоскоростное подключение, позволяя пользователям транслировать высококачественный видеоконтент, получать доступ к облачным сервисам и загружать файлы большого размера с высокой скоростью из любого места. Между тем, Wi-Fi 6 позволит одновременно подключать большее количество устройств на определенной территории, уменьшая перегрузку и повышая общую производительность сети.

- плавная передача обслуживания; 5G и Wi-Fi 6 обеспечат плавную передачу обслуживания между сотовыми сетями и сетями Wi-Fi, позволяя пользователям оставаться на связи даже при перемещении из одной зоны покрытия в другую; это обеспечит пользователям бесперебойную связь, особенно в районах с ограниченным покрытием сотовой связи.

- новые приложения; взаимодействие между 5G и Wi-Fi 6 также позволит создавать новые приложения и варианты использования, которые раньше были невозможны; например, благодаря высокоскоростному подключению и низкой задержке 5G и Wi-Fi 6 могут обеспечивать работу приложений в режиме реального времени, таких как управление дорожным движением и мониторинг окружающей среды.

Интеграция технологий 5G и Wi-Fi 6 принесет большую пользу устройствам Интернета вещей, обеспечивая более высокую скорость и меньшую задержку, обеспечивая более эффективную передачу данных. Кроме того, эта технология позволит подключать больше устройств одновременно, что упростит управление большими сетями устройств Интернета вещей и мониторинг за ними.

5G и Wi-Fi 6 могут использоваться для технологий дополненной реальности (AR) и виртуальной реальности (VR), которые смогут обеспечить пользователям глубокое погружение и реалистичность. В сочетании с искусственным интеллектом эти технологии могут создавать еще более привлекательный контент, который может быть применен в широком спектре отраслей.

Производители оборудования и многие операторы связи считают, что Wi-Fi 6 станет дополнительной технологией к 5G, способствующей созданию конвергентных сетевых сервисов. В частности, конвергенция приведет к стиранию границ между беспроводной и сотовой связью, что позволит операторам беспрепятственно перемещать трафик между сетями, сохраняя высокий уровень контроля и видимости.

Список используемых источников:

1. ITU-T Y.3100. Terms and definitions for IMT-2020 network Corrigendum 1, 2018.

2. Тихвинский В. О. Конвергенция 5G с Wi-Fi-6/Wi-Fi-6E [Электронный ресурс] // Wireless Russia & CIS: Сети LTE, 5G и IoT : материалы XIII Междунар. бизнес форума, Москва, 27-28 мая 2021 г. URL: https://www.niir.ru/wp-content/uploads/2021/05/Prof.-Tikhvinskiy-Convergence-5G-and-WiFi-6E.pdf (дата обращения: 31.10.2023)

3. Release 16 3GPP. 5G System; Access Traffic Steering, Switching and Splitting (ATSSS); Stage 3, 2020.

Nikiforov S.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Convergence of 5G and Wi-Fi 6 technologies.

Wireless connectivity has become a vital aspect of our daily lives due to the growing demand for faster, more reliable and secure wireless networks. As the number of connected devices grows, the need for a reliable wireless network infrastructure becomes even more acute. The article discusses the topic of integration of fixed wireless access and mobile radio access technologies, scenarios of their use.

Key words: wireless network, 5G, Wi-Fi 6, ATSSS

УДК 004.7
ГРНТИ 49.33.29

ЗАДАЧИ АНАЛИЗА ТРАФИКА И КАЧЕСТВА ОБСЛУЖИВАНИЯ В САМООРГАНИЗУЮЩИХСЯ СЕТЯХ С ПОДВИЖНЫМИ ПОЛЬЗОВАТЕЛЯМИ

А. И. Парамонов, А. М. Тихонов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются вопросы усовершенствования самоорганизующихся сетей с мобильными пользователями. На основе обзора технологий, используемых в существующих самоорганизующихся сетях, рассматривается вопрос об изменении режима работы узлов с симплексного на дуплексный для обеспечения более рационального использования частотного диапазона сети и улучшения ключевых характеристик сети. В данной работе также определены характеристики для анализа, такие как пропускная способность, задержка и надежность.

самоорганизующиеся сети, имитационная модель, трафик и качество обслуживания

Введение

В современном мире, где информационные технологии становятся неотъемлемой частью повседневной жизни, беспроводные самоорганизующиеся сети (БСС) занимают особое место, обеспечивая связь и обмен данных без необходимости физического подключения. Это важное направление развития телекоммуникационных систем представляет собой уникальную область исследований, где устройства могут сами организовываться и поддерживать сетевую инфраструктуру. Самоорганизующиеся сети представляют собой уникальный класс систем, способных организовывать свою структуру и функции без централизованного управления. Этот феномен подчеркивает важность исследований в области телекоммуникаций. На фоне стремительного развития цифровых технологий и растущей потребности в более гибких и устойчивых сетевых структурах, самоорганизующиеся сети представляют собой область, требующую глубокого исследования и инновационных подходов. Важность данной темы подчеркивается ее потенциалом в создании более эффективных и устойчивых систем связи, управления и взаимодействия между автономными устройствами.

Описание технологии

MANET, или "Mobile Ad-Hoc Network" (мобильные беспроводные сети) [2,3], представляет собой форму беспроводных сетей, в которых узлы могут свободно передвигаться и устанавливать соединения друг с другом без необходимости централизованной инфраструктуры. Такие сети обеспечивают гибкость и мобильность, что делает их идеальными для сценариев, где стационарная инфраструктура отсутствует или непрактична.

Основные характеристики MANET включают:

- **Динамичная топология:** Топология сети постоянно меняется из-за движения узлов. Это создает сложности в управлении маршрутизацией и обеспечении стабильной связи.
- **Отсутствие централизованной инфраструктуры:** В отличие от традиционных сетей, MANET не требует центральных точек доступа или базовых станций.
- **Самоорганизация:** Узлы в MANET способны самостоятельно организовываться и поддерживать сетевые функции, такие как маршрутизация и управление.
- **Ограниченные ресурсы:** Узлы могут иметь ограниченные вычислительные мощности, энергию и пропускную способность, что делает оптимизацию протоколов особенно важной.

Преимуществом данных сетей является то, что все узлы в таких сетях действуют не только как оконечные пользователи, но также как маршрутизаторы-ретрансляторы, передающие пакеты других пользователей от узла к узлу и участвующие в определении маршрутов к ним, данные сети обладают способностью к самоорганизации. Такие сети могут включать десятки, сотни или даже тысячи узлов [2]. Топология сети быстро изменяется, и количество соединений между узлами является переменной величиной. В связи с этим область покрытия самоорганизующейся сети может изменяться и не иметь постоянных параметров [1]. На рис.1 представлена структурная схема модели непосредственного взаимодействия узлов сети.

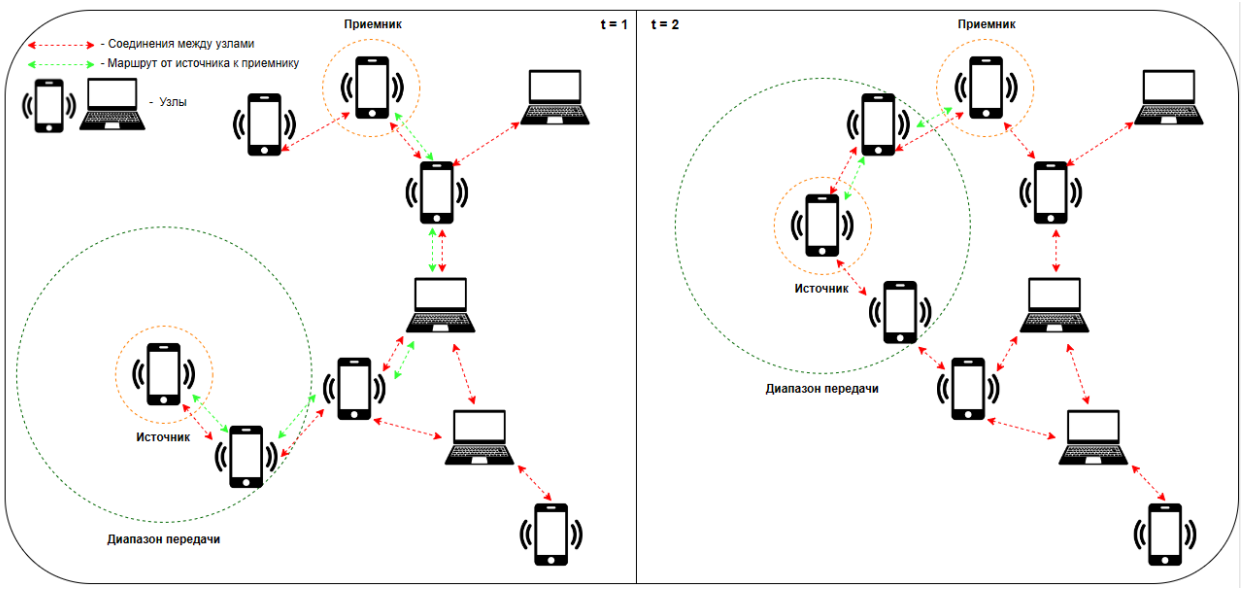


Рис. 1. Структура модели непосредственного взаимодействия узлов

Так же важной особенностью сетей такого типа является динамическая маршрутизация. Данные сети способны менять путь прохождения трафика в

зависимости от расположения узлов, их удаленности и количеству узлов, необходимых для ретрансляции трафика. На рис.1. мы видим как ведет себя сеть при различном расположении узлов. При t=1 в диапазоне передачи источника находится только 1 узел и для передачи трафика к приемнику трафику проходит через 4 узла. При t=2 в диапазоне передачи источника появляется второй узел, расположенный ближе к приемнику, поэтому трафик будет направлен к приемнику через этот узел.

Несмотря на преимущества, существуют и недостатки в реализации MANET. Например, проблемы с маршрутизацией из-за динамичной топологии и ограниченных ресурсов, проблемы безопасности и управление энергией являются ключевыми аспектами, требующими внимательного рассмотрения.

Особенности развертывания самоорганизующихся сетей с подвижными пользователями

При моделировании сетей класса MANET (Mobile Ad-Hoc network) следует учитывать определенные особенности:

- в связи с тем, что узлы передают данные на радиочастотах, невозможно одновременно передавать и принимать трафик на одной частоте;

-в сетях такого класса мобильность является важной особенностью, поэтому необходимо учитывать стремительное изменение топологии сети [3];

-поскольку сеть не имеет базовой станции и площади ее покрытия, необходимо учитывать расстояние между узлами.

В сетях MANET очень ценным ресурсом являются пропускная способность и энергоэффективность, поэтому следует минимизировать служебный трафик отключив периодические сообщения для выявления соседних узлов, а подключать их к сети по запросу [1].

Постановка задачи

В данной работе формулируются задачи для исследования имитационной модели сети ad-hoc, где узлами являются подвижные устройства. Из-за симплексного режима работы этих узлов возникают ограничения на пропускную способность сети. [2].

Основной целью исследования самоорганизующейся сети с подвижными пользователями является создание имитационной модели, в которой переход с симплексного режима на дуплексный позволит увеличить пропускную способность сети и осуществлять одновременную передачу и прием информации.

Дополнительно, второй задачей является проведение сравнительного анализа задержек и потерь данных в сетях с различными режимами работы - симплексным и дуплексным.

Заключение

В заключение, можно сказать, что в будущем самоорганизующиеся сети могут быть применены во множестве концепций. Несмотря на то, что их потенциал еще не полностью раскрыт, они уже используются в различных

областях. В перспективе эта технология будет применяться в умных домах, VANET, FANET и других концепциях. Дальнейшее развитие позволит быстро создавать сети с подвижными пользователями без необходимости базовых станций.

В данной работе был проведен обзор технологии MANET, проанализированы ее особенности и поставлены задачи по изучению модели самоорганизующейся сети с подвижными пользователями.

Список используемых источников:

1. 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 14.11.2023)

2. Самоорганизующиеся сети и новые услуги. [Электронный ресурс] // «ЭЛЕКТРОСВЯЗЬ»,. URL: https://elsv.ru/assets/uploads/2015/09/El_2009_01_page_19-231.pdf?ysclid=ltebprw6zz80561999. (Дата обращения 14.11.2023)

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

Paramonov A., Tikhonov A.

The Bonch-Bruevich 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, 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 and improving key network characteristics. In addition to this, the article characteristics for analysis such as throughput, latency, and reliability are defined.

Key words: self-organizing networks, simulation model, traffic and quality of service

УДК 004.732
ГРНТИ 49.33.29

ПРЕДСКАЗАНИЕ ДОЛИ ПОВТОРНЫХ ПЕРЕДАЧ ПРИ ИСПОЛЬЗОВАНИИ КОДИРОВАНИЯ LDPC В СЕТЯХ Wi-Fi

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

В данной статье рассматривается возможность и эффективность применения машинного обучения для предсказания процента повторных передач при использовании кодирования LDPC в сетях Wi-Fi. Актуальность темы заключается необходимости сокращения процента повторных передач для уменьшения задержек и увеличения скорости передачи в сетях Wi-Fi. С этой целью в среде разработки Microsoft Azure была построена модель для предсказания доли повторных передач с использованием алгоритма линейной регрессии и обучающего датасета, данные которого были получены в более ранних работах. Результаты проведенного эксперимента представлены в данной статье.

IEEE 802.11, LDPC, Wi-Fi, машинное обучение, линейная регрессия, помехоустойчивое кодирование

Wi-Fi – это стандарт широкополосной беспроводной связи семейства IEEE 802.11, работающий на физическом и канальном уровне модели ISO/OSI [1]. 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) [2]. Спрос на использование данного типа кодирования возник с развитием телекоммуникационных технологий [3].

Алгоритмы машинного обучения – это программы, которые помогают пользователям изучать и анализировать сложные наборы данных и находить в них закономерности. Каждый алгоритм представляет собой конечный набор однозначных пошаговых инструкций, которые компьютер может выполнить для достижения определенной цели. В модели машинного обучения целью является установление или обнаружение закономерностей, с помощью которых пользователи могут создавать прогнозы или классифицировать информацию. Линейная регрессия отображает либо прогнозирует связь между двумя переменными или факторами путем вписывания в представление данных непрерывной прямой линии [4]. Эта линия часто вычисляется с помощью функции Squared Error Cost (стоимость среднеквадратической погрешности). Линейная регрессия является одним из наиболее популярных видов регрессионного анализа.

Для реализации модели предсказания коэффициента повторных передач в работе будет использоваться облачная платформа Microsoft Machine

Learning Studio (classic). Она предоставляет возможность разработки, выполнения приложений и хранения данных на серверах, расположенных в распределенных дата-центрах.

Перед обучением модели необходимо составить датасет, на котором будет обучаться модель. Датасет – это обработанный и структурированный массив данных. В качестве него выберем данные по проведенному ранее эксперименту, в рамках которого исследовалось количество повторно переданных пакетов при использовании LDPC-кодов [1]. Данный датасет разделим на 2 категории: по восходящему и нисходящему потокам (см. рис. 1). В его столбцах будет содержаться следующая информация: номер канала (Channel), использование LDPC (LDPC mode), общее количество пакетов (All packets), количество повторно переданных пакетов (Retransmitted packets), процент повторно переданных пакетов (Percent of retransmitted packets). Каждый датасет необходимо сохранить в формате .csv.

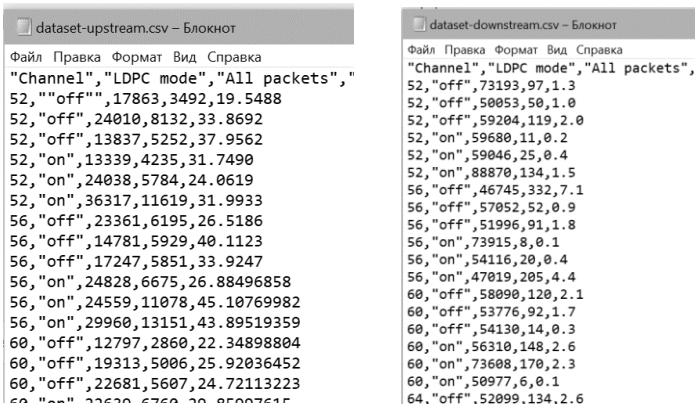


Рис. 1. Фрагменты датасетов в восходящем и нисходящем потоках

После составления датасетов необходимо составить схему эксперимента в Microsoft Machine Learning Studio (classic). Основными элементами схемы будут: алгоритм обучения, исходный датасет, блок выборки столбцов из датасета, блок разделения данных (в котором датасет стандартно делится в процентном соотношении 80% на обучение и 20% на вывод результата), модель обучения, модель оценки и модель стандартных метрик (см. рис. 2).

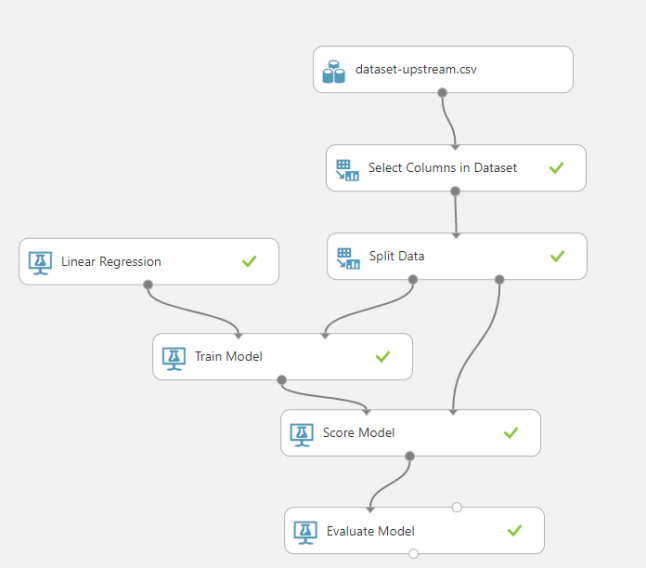


Рис. 2. Схема эксперимента по восходящему потоку

Оценивать модель будем по признаку процент повторно переданных пакетов. В блоках Select Columns in Dataset (блок разделения данных) и Train Model (модель обучения) выберем столбцы для обучения и дальнейшего предсказания процента повторных передач. В блоке Select Columns in Dataset выберем три столбца из исходного датасета для того, чтобы модель смогла более точно предсказать процент повторно переданных пакетов, обучаясь по этим данным (см. рис. 3).

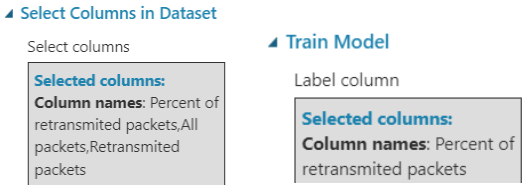


Рис. 3. Выборка по столбцам в блоках выбора столбцов и модели обучения

Для анализа данных по восходящему и нисходящему потокам будем исследовать блоки Score Model (модель оценки) и Evaluate Model (модель стандартных метрик).

По восходящему потоку блок Score Model показывает нам результат предсказаний по сравнению с исходными столбцами из датасета, которые были поданы на проверку после обучения (см. рис. 4).

All packets	Retransmited packets	Percent of retransmited packets	Scored Labels
36317	11619	31.9933	32.416865
21629	5277	24.397799	25.391222
22681	5607	24.721132	25.370985
21713	5030	23.165845	24.237898
19313	5006	25.920365	27.354945
14781	5929	40.1123	37.320801

Рис. 4. Результат работы блока Score Model

Столбец Scored Labels показывает результат предсказания модели. Как мы видим, в сравнении со столбцом Recent of retransmitted packets, результаты достаточно точные, модель предсказала процент повторных передач для восходящего потока, соотносимый с реальными данными.
Блок Evaluate Model показывает нам значения ошибок, которые оцениваются в рамках эксперимента с алгоритмом линейной регрессии. Наиболее важный показатель здесь – это среднеквадратическая ошибка. Она наиболее точно отражает то, на какой процент может ошибиться модель в предсказании результатов. По сравнению с выводимыми значениями, показанными в блоке Score Model, средний разброс ошибки равен примерно 1,5%. Следовательно, модель предсказывает процент повторных передач достаточно достоверно (см. рис. 5).

Metrics

Mean Absolute Error	1.227495
Root Mean Squared Error	1.44847
Relative Absolute Error	0.24013
Relative Squared Error	0.059049
Coefficient of Determination	0.940951

Рис. 5. Результат работы блока Evaluate Model

В эксперименте с нисходящим потоком исходный файл с данными по восходящему потоку в схеме на рис. 3 заменим на файл с данными по нисходящему потоку. В этом случае блок Score Model показывает следующие результаты (см. рис. 6).

All packets	Retransmited packets	Percent of retransmited packets	Scored Labels
52099	134	2.6	2.677649
57052	52	0.9	0.91523
53776	92	1.7	1.801366
54130	14	0.3	0.258796
88870	134	1.5	1.547888

Рис. 6. Результат работы блока Score Model

В нисходящем направлении процент повторно переданных пакетов был на порядок ниже, чем в восходящем. Однако модель так же предсказала искомые значения достаточно точно.

Блок Evaluate Model показал следующие значения основных ошибок (см. рис. 7).

Metrics

Mean Absolute Error	0.056667
Root Mean Squared Error	0.064074
Relative Absolute Error	0.088542
Relative Squared Error	0.006842
Coefficient of Determination	0.993158

Рис. 7. Результат работы блока Evaluate Model

Аналогично предыдущему эксперименту, значение среднеквадратической ошибки дает нам наиболее точное значение ошибки, которую допускала модель при предсказании процента повторных передач. Ее значение составило 0,05%, что меньше 5% от каждого значения из столбца Recent of retransmitted packets. Таким образом, модель предсказывает процент повторных передач достаточно точно.

Подводя итог, можно сказать, что алгоритм линейной регрессии подходит для прогнозирования процента повторных передач по входным данным. В рамках эксперимента модель с высокой точностью предсказала данный показатель в восходящем и нисходящем потоках. Полученные данные можно использовать для дальнейшего изучения сферы кодирования LDPC в сетях Wi-Fi с применением методов машинного обучения и создания обучающих датасетов.

Список используемых источников:

1. Смирнова А. А. Исследование эффективности применения кодирования LDPC в сетях Wi-Fi // Подготовка профессиональных кадров в магистратуре для цифровой экономики: материалы Всерос. науч.-технич. и науч.-методич. конф. магистрантов и их руководителей, Санкт-Петербург, 06-08 дек. 2022 г. СПб. : СПбГУТ, 2023. С.701–705.

2. Когновицкий О.С., Охорзин В. М., Небаев И. А. Теория помехоустойчивого кодирования. Часть 2. Сверточный коды. Турбокоды. СПб. : СПбГУТ. 2015. 64 с.

3. Панкратов А. В. Исследование LDPC декодеров // Молодой ученый. 2011. N 7 (30). Т. 1. С. 39-42.

4. Алгоритмы машинного обучения [Электронный ресурс]. URL: https://azure.microsoft.com/ru-ru/resources/cloud-computing-dictionary/what-are-machine-learning-algorithms#layout-container-uidb190 (дата обращения: 22.10.2023 г.).

Smirnova A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

Predicting the Retry Rate while Using LDPC Coding in Wi-Fi Networks.

The paper discusses the feasibility and effectiveness of using machine learning to predict the retry rate when using LDPC coding in Wi-Fi networks. The importance of this topic lies in the need to reduce delays and increase transmission speeds in Wi-Fi networks. For this purpose, a model was built in Microsoft Azure Studio to predict the share of retransmissions using a linear regression algorithm and a training dataset, the data of which were obtained in the earlier works. The results of the experiment are presented in this paper.

Key words: IEEE 802.11, LDPC, Wi-Fi, machine learning, linear regression, error-correcting coding.

УДК 004.725.7
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ МЕТОДОВ УМЕНЬШЕНИЯ ЗАДЕРЖЕК ДЛЯ URLLC В СЕТЯХ 5G

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

Снижение задержки в сверхнадежной связи с низкой задержкой в сетях 5G имеет решающее значение для различных приложений, включая автономные транспортные средства, промышленную автоматизацию и телемедицину. Из-за жестких требований к задержке в сети 5G требуется создание методов для удовлетворения требований. В статье будут рассмотрены несколько самых популярных методов снижения задержек в URLLC.

5G NR, URLLC, Edge Computing, sTTI, HARQ TTR

Пятое поколение (5G) — это новейшая и наиболее прогрессивная технология мобильной связи, которая обеспечивает более высокую скорость передачи данных, меньшую задержку и расширенную пропускную способность сети, соответствующую ее предшественнице, 4G LTE. Помимо расширенной мобильной широкополосной связи (EMBB), ожидается, что 5G обеспечит сверхнадежную связь с низкой задержкой (URLLC), при которой небольшие пакеты должны быть правильно переданы и приняты за очень короткое время (до 1 мс) с вероятностью успеха 99,999%.

Задержка в сети может возникать в различных точках сетевой архитектуры и процесса передачи данных. Понимание того, где может возникать задержка, имеет решающее значение для ее оптимизации и сокращения в конкретных случаях использования.

Поскольку требования к задержкам очень жесткие, ведется разработка новых и улучшение уже существующих технологий. Требования к задержке показаны на рис. 1.

Use case	Latency	Data rate	Remarks
Factory Automation	0.25-10 ms	1 Mbps	– Generally factory automation applications require small data rates for motion and remote control. – Applications such as machine tools operation may allow latency as low as 0.25 ms.
Intelligent Transport Systems (ITS)	10-100 ms	10-700 Mbps	– Road safety of ITS requires latency on the order of 10 ms. – Applications such as virtual mirrors require data rates on the order of 700 Mbps.
Robotics and Telepresence	1 ms	100 Mbps	– Touching an object by a palm may require latency down to 1 ms. – VR haptic feedback requires data rates on the order of 100 Mbps.
Virtual Reality (VR)	1 ms	1 Gbps	– Hi-resolution 360° VR requires high rates on the order of 1 Gbps while allowing latency of 1 ms.
Health care	1-10 ms	100 Mbps	– Tele-diagnosis, tele-surgery and tele-rehabilitation may require latency on the order of 1 ms with data rate of 100 Mbps.
Serious Gaming	1 ms	1 Gbps	– Immersive entertainment and human's interaction with the high-quality visualization may require latency of 1 ms and data rates of 1 Gbps for high performance.
Smart Grid	1-20 ms	10-1500 Kbps	– Dynamic activation and deactivation in smart grid requires latency on the order of 1 ms. – Cases such as wide area situational awareness require date rates on the order of 1500 Kbps.
Education and Culture	5-10 ms	1 Gbps	– Tactile Internet enabled multi modal human-machine interface may require latency as low as 5 ms. – Hi-resolution 360° and haptic VR may require data rates as high as 1 Gbps.

Рис. 1. Требования к задержке и скорости передачи данных для различных критически важных служб [1]

Технологии, которые помогут снизить задержку в сетях 5G

1) Граничные вычисления и мобильные граничные вычисления (MEC):

Обеспечение предполагаемой функциональности большинства современных сервисов типа URLLC требует выполнения вычислительно-ресурсоемких задач с собранными данными со строгими требованиями к задержке и надежности. Например, уличный датчик или камера должны выполнять обработку захваченных данных или видео в режиме реального времени, чтобы обнаруживать и предупреждать пешеходов, проходящих по улице. Однако эти устройства часто обладают ограниченной энергией и возможностями, что не позволяет им выполнять вычисления локальных задач. Таким образом, существует потребность в решении, позволяющем выполнять вычисления задач с учетом задержки и надежности для пользовательских устройств с низким энергопотреблением. [2]

В контексте 5G периферийные вычисления играют ключевую роль в обеспечении работы приложений и сервисов с низкой задержкой и высокой производительностью.

Граничные вычисления и 5G - это две технологии, которые меняют способ обработки и передачи данных. Граничные вычисления - это парадигма распределенных вычислений, которая приближает обработку данных и вычисления к источнику данных, которым может быть устройство или датчик, вместо того, чтобы полагаться на централизованные облачные центры обработки данных. С другой стороны, 5G, мобильные сети последнего поколения, обеспечивают повышенную пропускную способность, меньшую задержку и более высокую производительность приложений и сервисов.

В сочетании edge computing и 5G могут создать мощную сеть, способную обрабатывать и передавать данные более эффективно и быстро. Обрабатывая данные на границе сети, рядом с устройствами и датчиками, которые их собирают, пограничные вычисления уменьшают объем данных, которые необходимо передавать в центральный центр обработки данных. Это не только экономит время и снижает задержку, но и снижает нагрузку на сеть. [3] Структуру сети 5G можно увидеть на рис. 2.

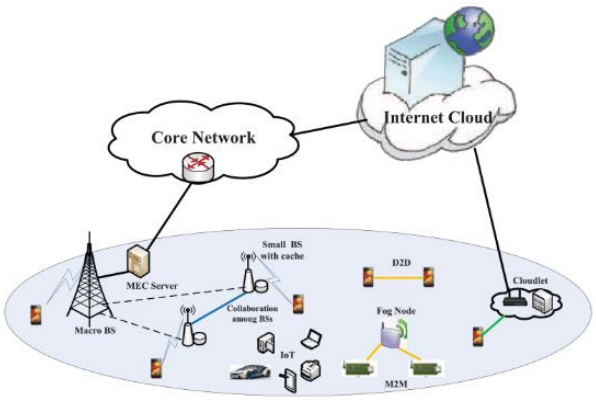


Рис. 2. Структура сети 5G

Граничные вычисления и 5G могут обеспечить различные новые варианты использования, включая удаленное здравоохранение, умные города и автономные транспортные средства.

Обрабатывая данные локально на границе сети, пограничные вычисления сокращают время ожидания, повышают надежность, повышают безопасность, снижают затраты, улучшают масштабируемость и обеспечивают лучший пользовательский опыт. Снижая задержки и улучшая общий пользовательский опыт, они также могут улучшить уже существующие приложения, такие как потоковое видео и онлайн-игры. [3]

2) Слайсинг сети:

Разделение сети позволяет создавать выделенные и изолированные сегменты сети, адаптированные к конкретным службам, включая URLLC. Оптимизируя срез сети для обеспечения низкой задержки, становится возможным сократить время, необходимое для про хождения данных по сети. Для каждого сегмента сети гарантированы выделенные ресурсы (например, ресурсы для виртуализированных серверов, QoS и т. д.). Поскольку слайсы изолированы друг от друга, ошибка или сбой, произошедшие в одном слайсе, не влияют на обмен данными в других слайсах. [4]

3) HARQ RTT (round trip time)

Среди многих потенциальных областей оптимизации для URLLC изучаются проблемы больших задержек при повторных передачах HARQ и неточной адаптации канала связи вследствие быстро меняющихся условий помех. Первое решается за счет сокращения длины TTI и времени прохождения HARQ в оба конца по сравнению с тем, что используется в LTE.

Для достижения короткого времени передачи данных HARQ RTT играют роль различные факторы, включая конфигурацию радиоинтерфейса, эффективные методы исправления ошибок, а также эффективное планирование и распределение ресурсов для минимизации времени, необходимого для повторной передачи данных в случае ошибок.

Предполагается, что HARQ RTT линейно масштабируется в зависимости от длины TTI. Предполагая асинхронную операцию HARQ, подобную LTE, с минимальным значением RTT, равным 8, даже при длительности TTI 0,143 мс, HARQ RTT не будет удовлетворять целевому значению задержки URLLC в 1 мс (т.е. $8 \cdot 0{,}143$ мс > 1 мс). Поскольку использование одной передачи привело бы к значительным затратам на спектральную эффективность, изучает случай, когда HARQ RTT сокращен до 4 TTI, чтобы оставить место для одной повторной передачи HARQ. Схема процедуры HARQ с уменьшенным RTT показана на рис. 3. При таких условиях максимальная длительность, предполагающая одну повторную передачу HARQ, уменьшается до $6 \cdot 0{,}143$ мс = 0,86 мс (без учета задержки в очереди). Следует обратить внимание, что предлагаемое сокращение HARQ RTT в основном требует улучшения возможностей обработки на UE и базовой станции. Дополнительным способом снижения требований к

обработке является применение так называемых методов ранней обратной связи [6], которые пытаются предсказать результат работы декодера до завершения всего декодирования.

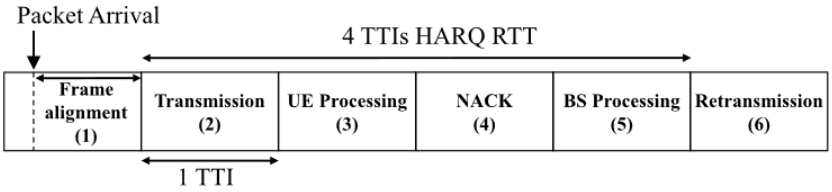


Рис. 3. Схема процедуры HARQ с уменьшенным RTT

Обширное моделирование производительности нисходящей линии связи на системном уровне показывает, что требования URLLC, т.е. задержки менее 1 мс и надежность 99,999%, достижимы при сценариях с низкой нагрузкой, тогда как при более высоких нагрузках наблюдается некоторое снижение производительности (задержка 1-3 мс) из-за увеличения задержки в очереди и межсотовых помех. [5]

4) Мини слоты

Частично высоконадежную связь с низкой задержкой обеспечивают благодаря использованию мини-слотов при формировании субкадра. Стандартный слот содержит в себе 14 OFDM (мультиплексирование с ортогональным частотным разделением каналов) символов. Мини-слот меньше стандартного слота и может содержать в себе 2, 4 или 7 OFDM символов. Использование мини-слотов позволяет обеспечить низкую задержку за счет незамедлительной передачи, без ожидания начала очередного стандартного слота. [7]

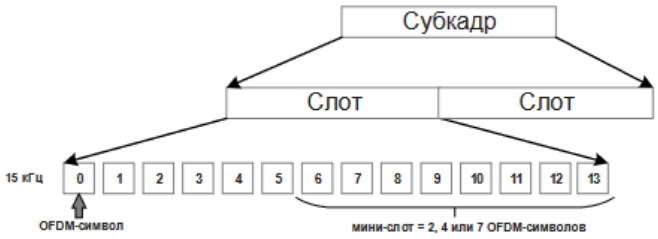


Рис. 4. Структурная схема субкадра

В заключение можно сказать, что снижение задержки в сетях 5G предполагает оптимизацию различных точек сети в зависимости от конкретного варианта использования. Для сверхнадежных приложений связи с низкой задержкой (URLLC) предпринимаются усилия по минимизации задержки на каждом этапе, от радиоинтерфейса до периферийных вычислений

Высокая пропускная способность 5G и низкая задержка дополняют пограничные вычисления, что приводит к более быстрой и эффективной обработке и передаче данных. Эта мощная комбинация передовых вычислений и 5G может обеспечить различные новые варианты

использования, включая удаленное здравоохранение, "умные города" и автономные транспортные средства, среди прочих.

URLLC с низкой задержкой является основополагающим элементом сетей 5G, поскольку он обеспечивает широкий спектр приложений, от жизненно важных сервисов до улучшения взаимодействия с пользователями и промышленной автоматизации. Речь идет о предоставлении гибкой, надежной и эффективной связи, которая необходима для успеха 5G, а также технологий и сервисов, которые она призвана поддерживать.

Список используемых источников:

1. Imtiaz Parvez, Ali Rahmati, Ismail Guvenc, Arif I. Sarwat, Huaiyu Dai. A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions, 2018
2. Elie El Haber, Latency and Reliability Aware Edge Computation Offloading in 5G Networks. Concordia University. 2022.
3. How Edge Computing and 5G will Help IoT? [Электронный ресурс] // TutorialsPoint. 2023. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.fc09f07c-6540107c-dde6d9e3-74722d776562/https/www.tutorialspoint.com/how-edge-computing-and-5g-will-help-iot (дата обращения 31.10.2023).
4. Подготовка профессиональных кадров в магистратуре для цифровой экономики. Сборник лучших докладов. СПб. : СПбГУТ, 2021. 450 с.
5. Gerardino, Guillermo Andrés Pocovi. Radio Resource Management for Ultra-Reliable Low-Latency Communications in 5G. 2017.
6. G. Berardinelli, S. Khosravirad, K. I. Pedersen, F. Frederiksen, P. Mogensen Enabling early HARQ feedback in 5G networks // IEEE Vehicular Technology Conference. 2016.
7. Дуплищева Н. В., Рогожников Е. В., Дмитриев Э. М., Новичков С. А., Лаконцев Д. В., Агеев Е. Ю. Обеспечение высокой надежности и низкой задержки трафика в 5G NR // T-Comm: Телекоммуникации и транспорт. 2022. Том 16. N 1. С. 22-29.

Stepanov A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Research of latency reduction methods for URLLC in 5G networks/

Reducing latency in ultra-reliable, low-latency communications in 5G networks is critical for a variety of applications, including autonomous vehicles, industrial automation, and telemedicine. Due to the strict latency requirements in the 5G network, it is necessary to create methods to meet the requirements. The article will discuss several of the most popular methods of reducing delays in URLLC.

Key words: 5G NR, URLLC, Edge Computing, sTTI, HARQ TT

УДК 004.725.5
ГРНТИ 49.03.05

ИССЛЕДОВАНИЕ ТЕХНОЛОГИИ STBC НА РЫНКЕ КЛИЕНТСКИХ УСТРОЙСТВ Wi-Fi

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

В данной статье будут рассмотрены основные принципы работы технологии STBC, которая позволяет снизить число битовых ошибок в радиоканале и улучшить помехоустойчивость системы. Также в работе содержится оценка распространенности технологии STBC среди клиентских устройств, поддерживающих стандарт IEEE 802.11.

STBC, пространственно-временное блочное кодирование, схема Аламоути

В 1998 году Сиаваш Аламоути изобрел схему передачи сигналов, которая впоследствии стала называться схемой Аламоути. Она была разработана для системы с двумя передающими антеннами. Позже появились пространственно-временные блочные коды, которые являлись обобщенным вариантом схемы Аламоути [1].

Пространственно-временной блочный код (Space-time block code, STBC) – это метод, используемый в беспроводной связи для передачи копий потока данных через несколько антенн за несколько тактовых интервалов. На своем пути сигнал попадает в среду, где он может рассеяться, отразиться или преломиться и, вследствие чего может быть неправильно распознан на принимающей стороне [2]. На двух тактовых интервалах с разных антенн передается один из сигналов и комплексное сопряжение другого сигнала. Таким образом, разнеся сигналы по времени и пространству (два сигнала проходят разными путями), достигается увеличение результирующего сигнала на приеме. На рис. 1, показана простейшая схема Аламоути с двумя передающими (Tx) и одной принимающей (Rx) антеннами.

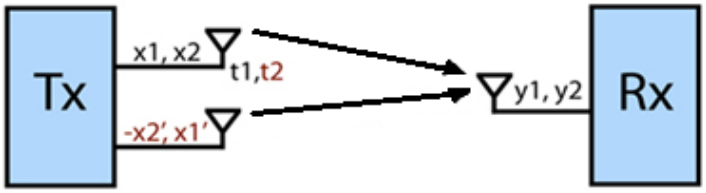


Рис. 1. Простейшая схема с двумя передающими и одной принимающей антеннами

Технология STBC была разработана для повышения производительности беспроводных передач, поскольку каждый сигнал может прийти с задержкой или иметь разное отношение сигнал/шум [3]. STBC компенсирует дополнительный шум и другие дополнительные потери в пространственных каналах и позволяет снизить уровень битовых ошибок.

Далее была проведена оценка рынка устройств, поддерживающих технологию STBC. Для этого использовалась база данных с различными производителями клиентских устройств и программное обеспечение Wireshark. В данной базе хранятся файлы с перехваченными кадрами запросов на ассоциацию (association request frame) [4]. Эти кадры содержат различную информацию о радиокарте устройства. С помощью Association Request [5] устройство начинает процесс создания связи с точкой доступа (ТД) и просит ТД выделить ресурсы для новой сессии, синхронизироваться с радиокартой клиентского устройства. Пример перехваченного кадра запроса на ассоциации представлен на рис. 2.

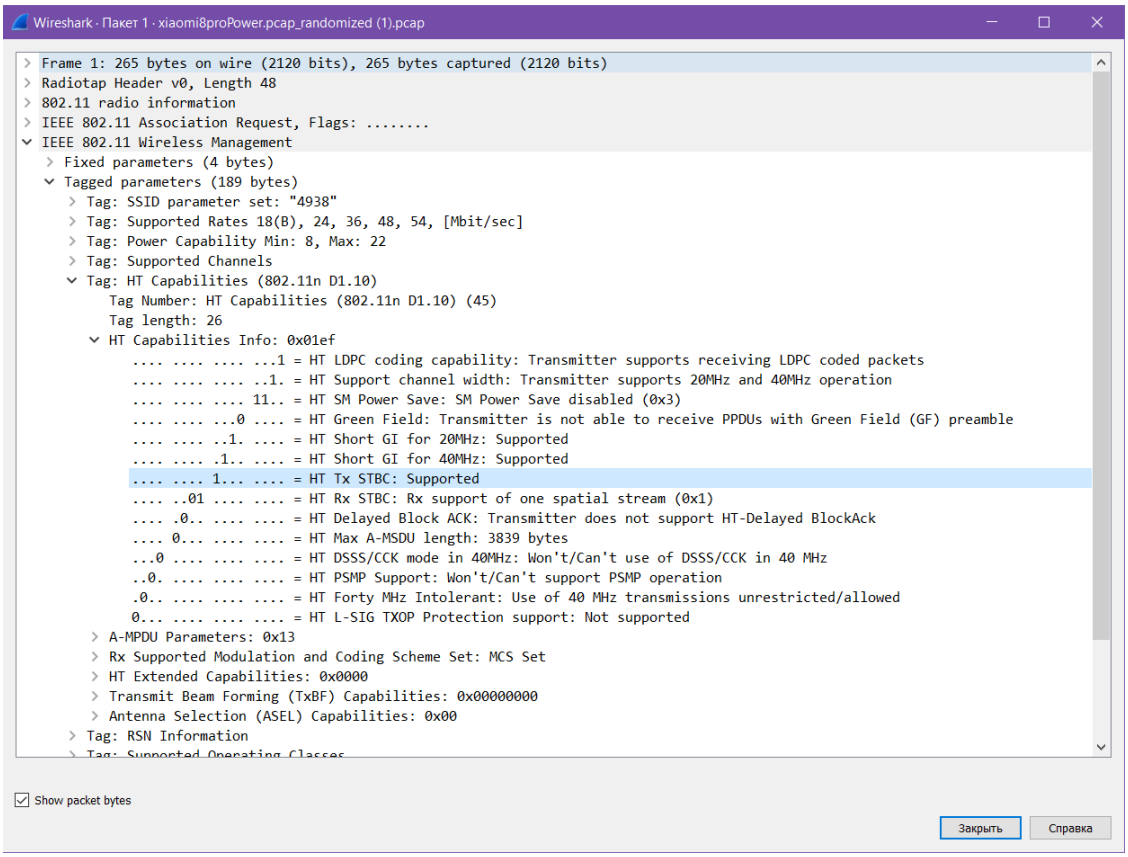


Рис. 2. Содержимое перехваченного кадра

Случайным образом для анализа было выбрано 15 клиентских устройств и использованы опубликованные в базе данных кадры Association Request с информацией об их технических возможностях. Перечень выбранных устройств приведен в таблице 1. Рассматривалось три типа устройств: смартфон, ноутбук и внешний адаптер.

ТАБЛИЦА 1. Перечень выбранных устройств

Производитель	Модель	Tx STBC	Rx STBC, кол-во потоков
Xiaomi	Mi 8 Pro	Поддерживается	Поддерживается, 0x1
Xiaomi	RedmiNote 5	Не поддерживается	Поддерживается, 0x1
Xiaomi	Pocophone F1	Поддерживается	Поддерживается, 0x1
Samsung	S8+	Поддерживается	Поддерживается, 0x1

Samsung	S9+	Поддерживается	Поддерживается, 0x1
Samsung	S10+	Не поддерживается	Не поддерживается
Apple	iPhone SE 2	Не поддерживается	Не поддерживается
Apple	iPhone XR	Не поддерживается	Не поддерживается
Apple	iPhone 11	Не поддерживается	Не поддерживается
Apple	Macbook Air Retina 13	Не поддерживается	Не поддерживается
Apple	Macbook Pro 2019	Не поддерживается	Не поддерживается
Apple	Macbook Pro 2017	Поддерживается	Поддерживается, 0x1
ASUS	Asus USB-AC68	Поддерживается	Поддерживается, 0x1
ASUS	Asus PCE-AC88	Поддерживается	Поддерживается, 0x2
ASUS	Asus USB-AC56	Поддерживается	Поддерживается, 0x1

Для Association Request для каждого устройства рассмотрено наличие поддержки технологии STBC и, при ей наличии, в каких направлениях она поддерживается: только на прием сигнала(Rx), на передачу (Tx) или в обоих направлениях. Так на рисунке 2 приведены технические возможности телефона Xiaomi Mi 8 Pro. Данное устройство поддерживает технологию STBC как на прием, так и на передачу, однако можно заметить, что на прием указывается конкретное число пространственных потоков и в данном случаем поддерживается только один такой поток.

В ходе анализа выбранных устройств были получены диаграммы процентного соотношения использования технологии STBC. На рис. 3 представлена диаграмма, иллюстрирующая процент устройств, имеющих поддержку STBC при передаче сигнала.

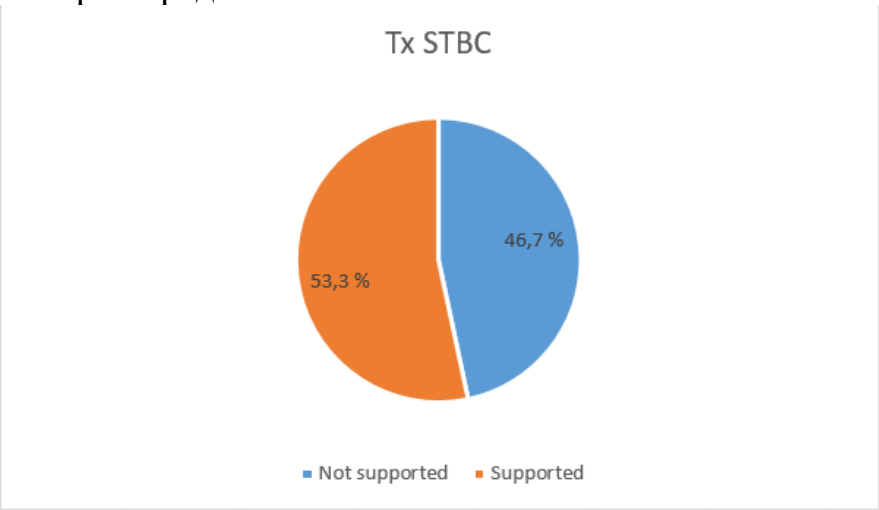


Рис. 3. Диаграмма процентного соотношения использования технологии STBC для передающей стороны

Исходя из получившейся диаграммы, можно сделать вывод, что у чуть больше половины устройств реализована передача сигнала с применением STBC.

Если же рассматривать диаграмму для принимающей стороны на рис. 4, можно с точностью сказать, что 60% рассмотренных устройств могут принимать сигнал с STBC. Однако стоит понимать, что если мы рассматриваем присутствие технологии STBC на принимающей стороне,

нужно учитывать количество пространственных потоков. Из диаграммы видно, что производители устройств если и включают STBC в свой продукт, то в большей степени предпочтение отдается всего одному пространственному потоку.

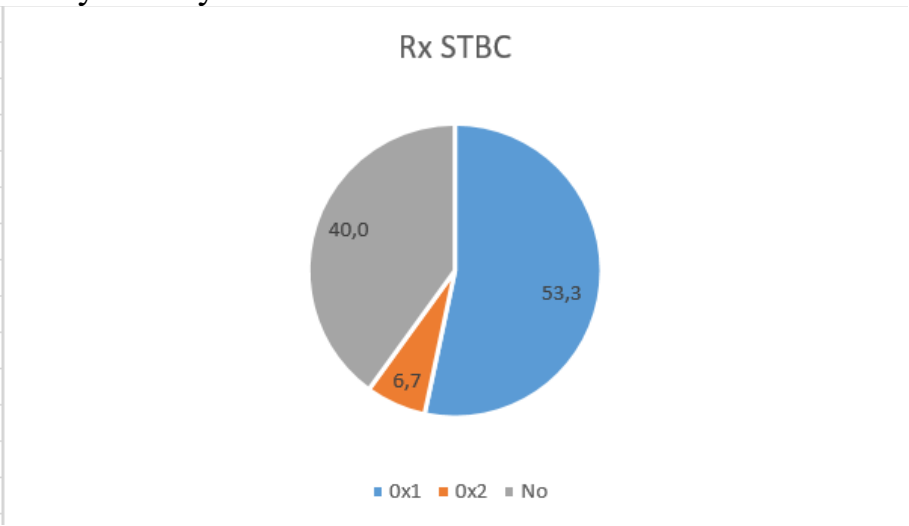


Рис. 4. Диаграмма процентного соотношения использования технологии STBC для принимающей стороны и поддерживаемого числа пространственных потоков

Также стоит отметить, что у всех рассмотренных устройств, кроме одного, наблюдалась следующая закономерность. Если устройство способно передавать сигнал с применением технологии STBC, то оно гарантированно умеет принимать сигнал с применением этой технологии. В технологии STBC для реализации полного функционала необходимо, чтобы и передающая сторона, и принимающая имели поддержку STBC.

Таким образом, проанализировав вышесказанное, можно сделать вывод о том, что не все производители считают необходимым реализовывать данную технологию в своих устройствах, несмотря на способность улучшать качество передачи сигнала.

Список используемых источников:

1. Новые алгоритмы формирования и обработки сигналов в системах подвижной связи / под редакцией профессора А. М. Шломы. М. : Горячая линия-Телеком, 2008. 344 с.
2. Основы построения беспроводных локальных сетей стандарта 802.11 : пер. с англ. М. : Издательский дом "Вильямс", 2004. 304 с.
3. Hassibi B., Hochwald B. High-rate codes that are linear in space and time // Transactions on IEEE Trans. Info. Theory. 2002. N 48(7). pp. 1804-1824.
4. База данных с различными производителями клиентских устройств [Электронный ресурс]. URL: https://sites.google.com/a/mikealbano.com/clients/home
5. Пролетарский А. В., Баскаков И. В., Федотов Р. А. Бобков А. В. Чирков Д. Н. Платонов В. А. Беспроводные сети Wi-Fi. М. : НОУ «ИНТУИТ», 2016. 284 с.

Shcheglov S.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

A Study of STBC technology in the device manufacturers' market.

This paper discusses the basic principles of STBC technology, which allows to reduce bit errors in the radio channel and improve the noise immunity of the system. The paper also contains an assessment of the prevalence of STBC technology among client devices that support the IEEE 802.11 standard.

Key words: Alamouti scheme, Space-time block code, request frame, transmitting side.

Секция 3.3.
Мультисервисные телекоммуникационные системы и технологии

УДК 654.1
ГРНТИ 50.41.23

АНАЛИЗ МОДЕЛИ УПРАВЛЕНИЯ УСЛУГАМИ 5G, ПРЕДЛАГАЕМОЙ В ОТКРЫТОЙ ЦИФРОВОЙ АРХИТЕКТУРЕ ОТ TM FORUM

А. А. Бойко, С. В. Кисляков, Д. М. Османов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследование посвящено тому, как Открытая цифровая архитектура (TM Forum) учитывает стандарты и рекомендации 3GPP, O-RAN, GSMA и поддерживает технологии виртуализации сети. Обсуждаются модели управления услугами в сетях 5G, основанные на технологии слайсинга, разработанные в рамках концепции Открытой цифровой архитектуры консорциума TM FORUM.

Open Digital Architecture, 5G, модель управления, управление услугами

Введение

Технология сетей 5G предоставила фундаментальную концепцию разделения сети, которая представляет собой возможность логически разделять услуги и сети, состоящие из специализированных сетевых функций, специфичных для конкретной технологии.

Концепция слайсинга стала обязательной для использования возможностей 5G. Кроме того, расширение возможностей виртуализации обеспечивает большую гибкость в настройке, развертывании и управлении сетями 5G. Еще одним важным изменением, влияющим на бизнес операторов связи, является потенциал увеличения доходов и расширения возможностей за счет поддержки все более сложных экосистем, состоящих из множества внешних партнеров, поставщиков услуг, а также поставщиков и интеграторов услуг Over the Top (OTT).

Это лишь вопрос времени, когда различные системы связи (спутниковые, IoT) потребуют совместимости с традиционными 4G, Wi-Fi и другими стандартами связи, то есть IoT SAREF, с соответствующими требованиями к функциональной и системной интеграции сложных систем и сетей.

В сочетании с необходимостью снижения эксплуатационных затрат, оптимального использования активов, более высокого уровня безопасности и переменного уровня качества в сетях с программным обеспечением, эти цели представляют собой серьезную проблему в способах проектирования, построения и эксплуатации операционных систем.

Для достижения этих целей необходима определенная степень стандартизации, иначе затраты и несогласованность, возникающие в результате отсутствия единого стандартного подхода, могут превысить выгоды, что приведет к разного рода проблемам безопасности и контроля качества.

С 2018 г. в TM Forum начали разрабатывать концепцию открытой цифровой архитектуры (Open Digital Architecture, ODA) под задачи стандартизации моделей услуг.

Функциональная архитектура ODA

Функциональная архитектура ODA предлагает набор из пяти блоков, представленных на рис. 1. Это такие унифицированные высокоуровневые блоки, которые содержат структурированный набор бизнес-операций оператора услуг.

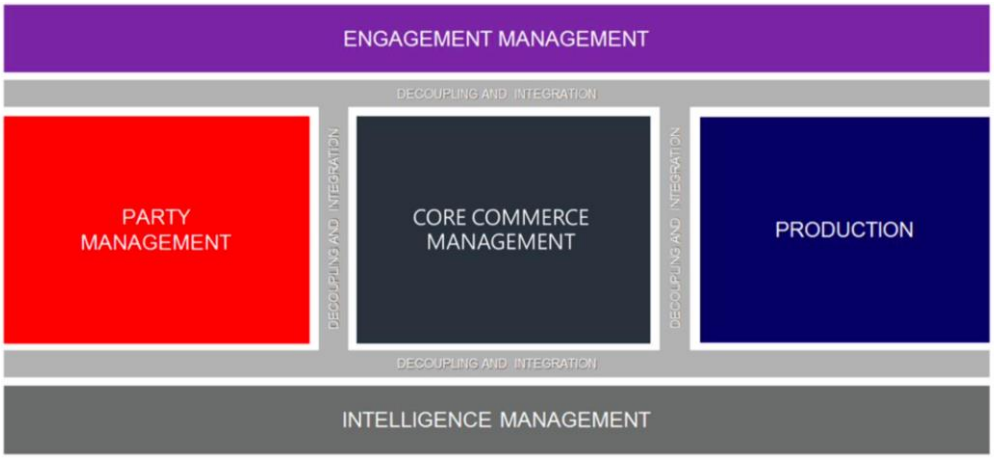


Рис. 1. Функциональная архитектура ODA

Блок управления взаимодействием (The Engagement Management Block – EGM) определяет взаимодействие между пользователями и процессами, выполняемыми другими функциями, такими как Intelligence Management, Party Management, Core Commerce Management or Production Blocks [4,5].

Блок управления взаимоотношениями с партнерами (Party Manage-ment – PM) обрабатывает все взаимодействия и данные, связанные с объек-тами или субъектами, которые вовлечены в бизнес-процесс или могут быть связаны с предприятием.

Блок Core Commerce Management (CCM) представляет собой часть предприятия, которая занимается непосредственно развитием продаж.

Производственный блок (Production Block) отвечает за производство и доставку услуг потребителю.

Блок Intelligence Management (IM) предоставляет возможности использования данных для получения бизнес-знаний.

Модели услуг TM Forum ODA

TM Forum ODA предлагает общую модель управления услугами 5G как по отношению к конечному пользователю, так и между операторскими организациями и партнерами на основе архитектуры ODA и требований 3GPP.

Предоставление услуг клиентам и организациям, внешним по отношению к оператору, регулируется соглашениями и контрактами на обслуживание. Разным клиентам требуются разные возможности управления,

а соглашения об уровне обслуживания (SLA) различаются с точки зрения атрибутов и политик – параметров, которыми можно и нужно управлять.

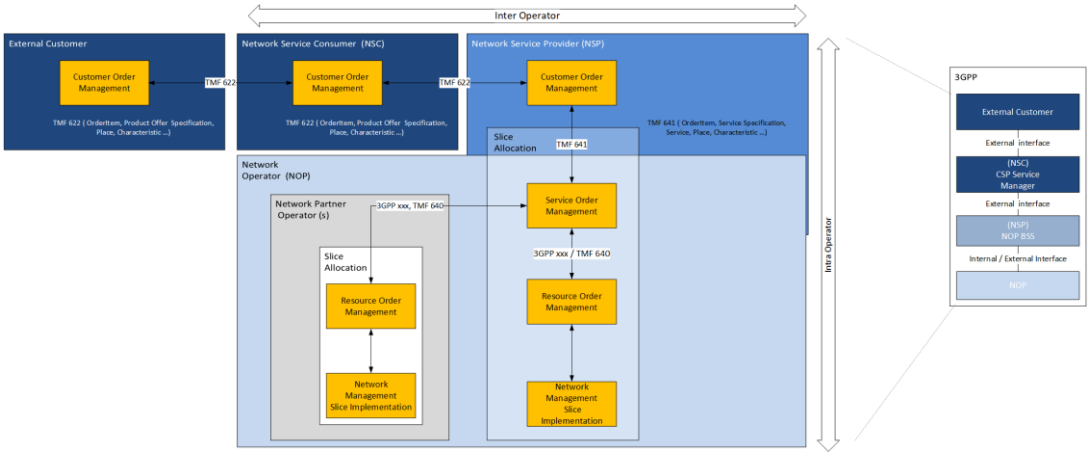


Рис. 2. Области ответственности поставщиков услуг

Для поддержки любых моделей взаимодействия оператора с клиентами или партнёрами, были проанализированы возможные роли, услуги, необходимость системной интеграции и управление слайсами на двух уровнях, а именно:

1) межоператорское управление продуктом/услугой/слайсом (inter-operator product / service / slice order);

2) внутриоператорское управление слайсом (intra-operator slice management).

На рис. 2 показаны функциональные области ответственности, распределенные по каждой роли, а также схемы взаимодействия/интерфейсы между ними. Роли формируют основу для определения коммерческих, административных и эксплуатационных областей, в которых оператор продает, развертывает и управляет своими услугами.

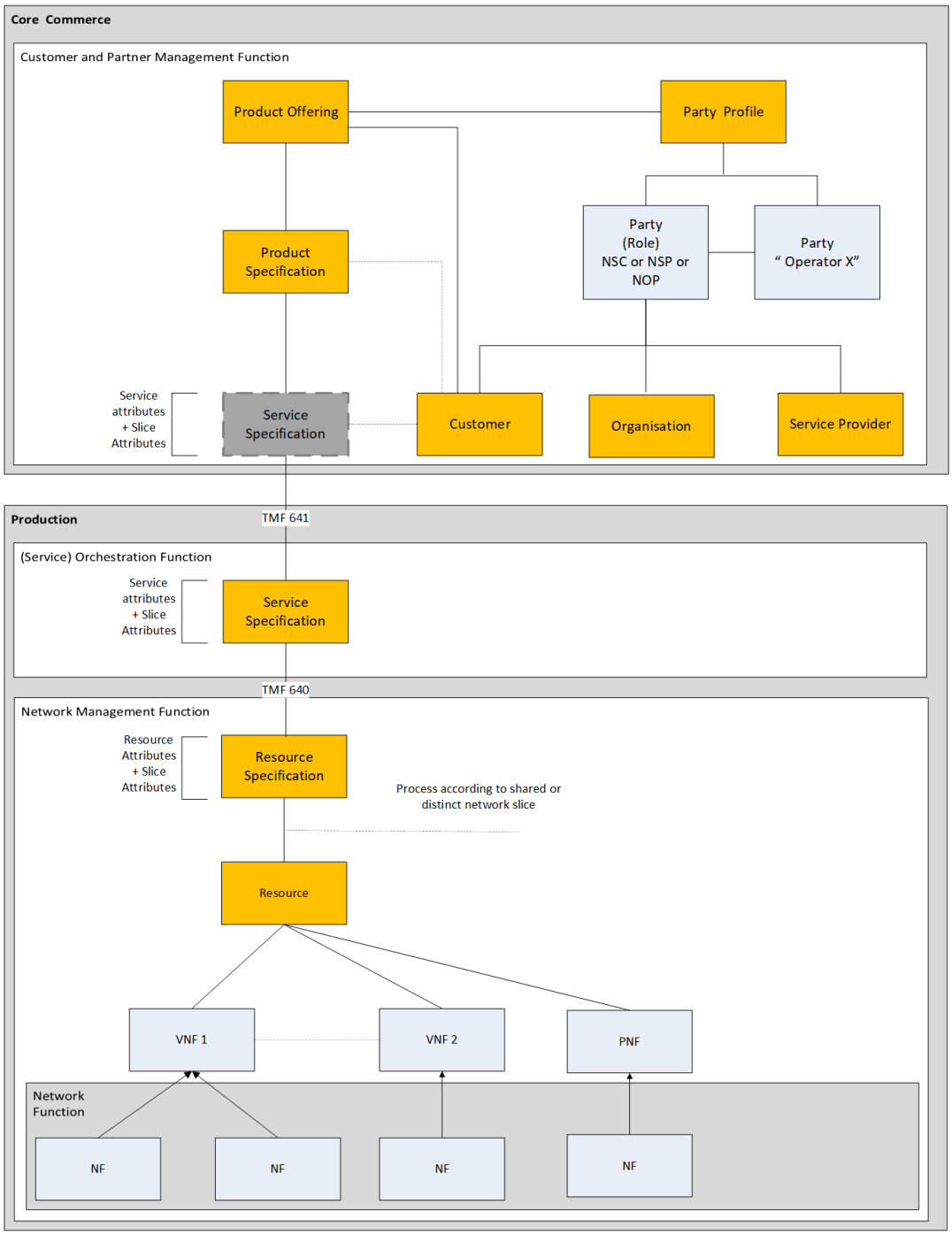


Рис. 3. Модель ODA управления услугами в сети 5G

Общий подход к моделированию сервисов основан на том принципе, что абонентский сервис состоит из множества многократно используемых технических компонентов. Службы относятся к коммерческому домену и могут быть связаны с продуктами в соответствии с выбранным методом развертывания.

Что касается требований 5G, компоненты сетевых ресурсов независимы и отделены от абстрактного представления продукта/услуги — можно предоставлять бизнес-услуги как через отдельную, так и через идентичную инфраструктуру ресурсов, что позволяет максимизировать использование и снизить эксплуатационные расходы. Кроме того, динамичный характер

новых услуг подразумевает, что распределение инфраструктуры не всегда известно заранее, и поэтому функциональность и мощность могут распределяться по требованию в соответствии с целями и возможностями виртуализации.

Отделение бизнес-сервисов независимо от их базовых требований к ресурсам упрощает рабочую нагрузку при проектировании, сборке и эксплуатации.

Концептуальная модель управления услугами, показанная ниже, поддерживает три области соответствии с ODA:

• Управление клиентами и коммерческие предложения по конкретным продуктам;

• Управление услугами;

• Управление ресурсами, обеспечивающее дальнейшую декомпозицию на виртуализированные функции и инфраструктуру.

На рисунке ниже показано, как оператор может играть одну или несколько ролей в экосистеме (5G), изменяя профили ролей сторон.

Список используемых источников:

1. Гольдштейн А. Б., Кисляков С. В. Концепция открытой цифровой архитектуры: эволюция или революция? Вестник связи. N 6, 2022. С. 21-25.

2. IG1166 ODA Architecture Vision R18.0.0. [Электронный ресурс]. URI: https://www.tmforum.org/resources/standard/ig1166-oda-architecture-vision-r18-0-0/ (дата обращения: 06.10.2023).

3. GB999 ODA Production Implementation Guidelines v4.0.1 [Электронный ресурс]. - URI: https://www.tmforum.org/resources/standard/gb999-oda-production-implementation-guidelines-v4-0/ (дата обращения: 10.10.2023).

4. GB998 Open Digital Architecture (ODA) Concepts & Principles v2.1.0 [Электронный ресурс]. URI: https://www.tmforum.org/resources/reference/gb998-open-digital-architecture-oda-concepts-principles-v2-1-0/ (дата обращения: 16.09.2023).

5. IG1211 ODA 5G Management Implementation Guidelines v.1.0.1 [Электронный ресурс]. URI: https://www.tmforum.org/resources/reference/ig1211-oda-5g-management-implementation-guidelines-v1-0-0/ (дата обращения: 15.09.2023).

Boyko A., Kislyakov S., Osmanov D.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

Analysis of the 5g service management model offered in the open digital architecture from tm forum.

The study is devoted to the topic "Open Digital Architecture" (TM Forum), compliance with standards and recommendations of 3GPP, O-RAN, GSMA and support for network virtualization technology. A service management model in 5G networks based on slicing technology, developed within the framework of the Open Digital Architecture concept of the TM FORUM consortium, is discussed.

Key words: Open Digital Architecture, 5G, management mode

УДК 004.8
ГРНТИ 49.33.01

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ НЕЙРОННЫХ СЕТЕЙ В СЕТЯХ СВЯЗИ

Е. Б. Воинков, В. С. Елагин
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Область применения искусственных нейронных сетей постоянно расширяется. В телекоммуникационных системах они находят применение при решении следующих важных задач: управление коммутацией, адаптивная маршрутизация, управление трафиком, оптимальное распределение загрузки каналов сети. Кроме того, перспективным является использование нейросетевых алгоритмов в задачах кодирования и декодирования информации.

нейронные сети, анализ трафика, трафик, структура сети связи, сетевая безопасность

Введение

В настоящее время нейронные сети развиваются очень быстрыми темпами, начинают затрагивать все больше сфер жизни человека. В сетях связи уже начинают внедряться нейросети для различных задач, полезных операторам связи, инженерам и обычным клиентам.

Нейронная сеть (также искусственная нейронная сеть, ИНС, или просто нейросеть) — математическая модель, а также её программное или аппаратное воплощение, построенная по принципу организации и функционирования биологических нейронных сетей — сетей нервных клеток живого организма. Нейросети не программируются в привычном смысле этого слова, они обучаются. Возможность обучения — одно из главных преимуществ нейронных сетей перед традиционными алгоритмами. В процессе обучения нейронная сеть способна выявлять сложные зависимости между входными данными и выходными, а также выполнять обобщение. Это значит, что в случае успешного обучения сеть сможет вернуть верный результат на основании данных, которые отсутствовали в обучающей выборке, а также неполных и/или «зашумленных», частично искажённых данных.

Нейронные сети могут быть использованы для анализа трафика или структуры сети, борьбы с мошенничеством, безопасности сети, управления сетью, управления качеством обслуживания, прогнозирования спроса на услуги связи [1].

Анализ

Анализ трафика

Развитие и внедрение новых сетевых технологий в настоящее время способствует постоянному увеличению объема данных, передающихся по сети, а также появлению новых сетевых протоколов прикладного уровня, что

делает задачу анализа сетевого трафика особенно актуальной. Анализ сетевого трафика позволяет решать следующие задачи: выявлять проблемы в работе сети, восстанавливать потоки данных, предотвращать различные сетевые атаки, вести статистику и определять характеристики сетевых соединений.

Анализ трафика в сети связи может быть выполнен с помощью различных методов машинного обучения, таких как регрессия, классификация и кластеризация. Для анализа трафика используются данные о передаче пакетов данных по сети, такие как количество пакетов, скорость передачи данных, задержки и другие параметры. Нейронные сети могут быть обучены на этих данных, чтобы определить паттерны использования сети и предсказать будущий трафик. Например, нейронная сеть может быть обучена на данных о количестве пакетов, скорости передачи данных и задержках в какой-либо промежуток времени. После обучения она может использоваться для прогнозирования будущего трафика в определенное время суток.

Анализ структуры сети

Анализ структуры сети может быть использован для решения следующих задач:

•Предсказание производительности. Используя данные о структуре сети, такие как конфигурация узлов, типы связей и пропускные способности, для обучения нейросети предсказывать производительность сети. Это может включать в себя прогнозирование задержек, уровня загрузки и других показателей.

•Нахождение аномалий в сетях может помочь выявлять нештатные ситуации, такие как необычные конфигурации узлов или отказы в связи.

•Классификация типов устройств. Используя данные о структуре сети для классификации узлов на различные типы (например, маршрутизаторы, коммутаторы, серверы). Нейросеть может обучиться распознавать уникальные характеристики устройств и классифицировать их.

•Оптимизация конфигурации. Нейросеть может использоваться для оптимизации конфигурации сети. Это может включать в себя предложения по изменению расположения узлов, оптимизации пропускных способностей связей и других параметров для улучшения производительности сети.

•Прогнозирование изменений в сети. Нейросеть может быть обучена анализировать изменения в структуре сети и предсказывать, как эти изменения могут повлиять на производительность или безопасность сети.

•Адаптация к динамике сети. Нейросеть может быть настроена для адаптации к динамике сети, что позволит ей обнаруживать и адекватно реагировать на изменения в структуре сети.

Безопасность

Особую значимость сегодня получает возможность обнаружения аномальных отклонений в состоянии сети, которые могут возникать из-за несанкционированного доступа к сети [2]. Обнаружение несанкционированного доступа представляет собой процесс

интеллектуального мониторинга событий, которые происходят в вычислительной сети или системе, осуществление их анализа на присутствие признаков нарушения политики безопасности, попытки обхождения механизмов безопасности сети. Решение данной задачи может быть реализовано с помощью нейросетей, способных в реальном времени осуществлять анализ трафика, распознавать наличие угроз для безопасности сети. Нейросети могут быть обучены распознавать сигнатуры вредоносных программ или другие признаки вредоносной активности. Это может помочь в раннем обнаружении вредоносных программ, даже если они не известны системе защиты. Возможность анализа больших объемов данных, чтобы выявлять необычные тенденции и угрозы. Они могут помочь в распознавании новых видов кибератак, которые могли бы быть упущены традиционными методами безопасности.

Нейронные сети могут использоваться для обнаружения мошеннических действий в сети связи, например, для определения несанкционированных подключений к сети или для обнаружения поддельных сообщений. Они могут обучаться на большом количестве данных о мошенничестве и определять паттерны поведения злоумышленников. Это позволяет операторам сети предотвращать мошеннические действия и улучшать безопасность своей инфраструктуры.

Управление качеством обслуживания

Нейронные сети могут быть использованы для решения следующих задач:

- Прогнозирование трафика позволяет заранее распознавать пиковые нагрузки и предпринимать меры для предотвращения перегрузок в сети.
- Адаптивное управление пропускной способностью может помочь в предотвращении узких мест и повышении эффективности сети.
- Оптимизация маршрутизации данных в сети, что способствует улучшению времени задержки и общего качества обслуживания [3].
- Определение типов трафика, которые имеют больший приоритет в конкретный момент времени, чтобы гарантировать лучшее качество обслуживания для важных приложений.
- Оптимизация распределения ресурсов в сети, в зависимости от текущих требований и загрузки, что позволяет более эффективно использовать имеющиеся ресурсы.
- Сбор обратной связи от сети и пользователей, что позволяет системе динамически адаптироваться к изменяющимся условиям и требованиям.

Заключение

Таким образом нейронные сети сильно помогут развитию сетей связи так как благодаря их внедрению будет улучшена безопасность сети, улучшен анализ, что даст большие возможности развития операторов.

Список используемых источников:

1. Комашинский В. И. Смирнов Д. А. Нейронные сети и их применение в системах управления и связи, 2003. 94 с.
2. Мустафаев А. Г. Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика // Вопросы безопасности. 2016. N 2. С. 1-7.
3. Федотов В. В. Применение нейронных сетей в телекоммуникационных сетях связи // Естественные науки. Приложения. 2004. N 5. С. 90-94.

Voinkov E., Elagin V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Possibility of using neural networks in communication networks.
The scope of artificial neural networks is constantly expanding. In telecommunication systems, they are used in solving the following important problems: switching control, adaptive routing, traffic management, optimal load distribution of network channels. In addition, the use of neural network algorithms in problems of encoding and decoding information is promising.

Key words: neural networks, traffic analysis, traffic, communication network structure, network security.

УДК 004.052.42
ГРНТИ 50.43.19

АНАЛИЗ ВОЗМОЖНОСТЕЙ ИСПОЛЬЗОВАНИЯ МЕТОДОВ ОТСЛЕЖИВАНИЯ СЕТЕВЫХ ПАКЕТОВ ДЛЯ ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

В. С. Елагин, А. А. Мельниченко, А. А. Швидкий
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обеспечение требуемого уровня производительности сети передачи данных в распределенных кластерных системах при использовании микросервисных архитектур в настоящее время является одной из самых труднорешаемых задач, так как постоянное взаимодействие между узлами и сервисами имеет неоднородную природу, при этом сами приложения, не являясь монолитным ядром не могут отследить возникновения таких проблем.

проблемы обработки сетевого траффика

В настоящее время распределенные кластерные системы значительно повышают свои требования к сетям передачи данных. В высокопроизводительных системах, где время обработки каждой операции значительно сокращается, сколько-нибудь значительные сетевые задержки могут негативно повлиять на производительность всех компонентов системы, в том числе на вычислительные возможности кластера и работу распределенных систем хранения данных. Классические методы построения сетей при обеспечении прохождения трафика не учитывают время прохождения пакетов, а значит не могут реагировать на деградацию показателей сети [1].

В связи с использованием в сетях центров обработки данных программных коммутаторов и маршрутизаторов, реализующих свою логику обработки сетевого трафика на вычислительных серверах проблемы значительно возрастают – появляется значительно количество дополнительных абстракций при передаче трафика (рис. 1).

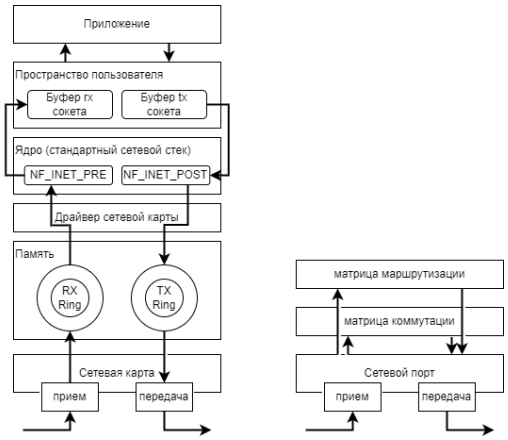


Рис. 1. Сравнение сетевого стека

При этом в связи с необходимостью применения виртуальных сетевых коммутаторов и маршрутизаторов в целях передачи траффика между виртуальными машинам, контейнерами и различными приложениями, встаёт необходимость повышения производительности и эффективности использования сетевого стека. При классическом подходе существует сразу несколько проблем [2]:

– Невозможно точно оценить время задержки пакетов на сетевых узлах
– Нет однозначных механизмов выявления узлов, негативно влияющих на производительность сети
– Снижение производительности сети за счёт необходимости многократного копирования в ядре операционной системы.

Фильтры в ядре операционной системы

Одним из таких подходов может является использование технологии eBPF[2,3], которая позволяет добавить в ядро скомпилированную программу, которой указаны необходимые действия с сетевыми пакетами (рис. 2).

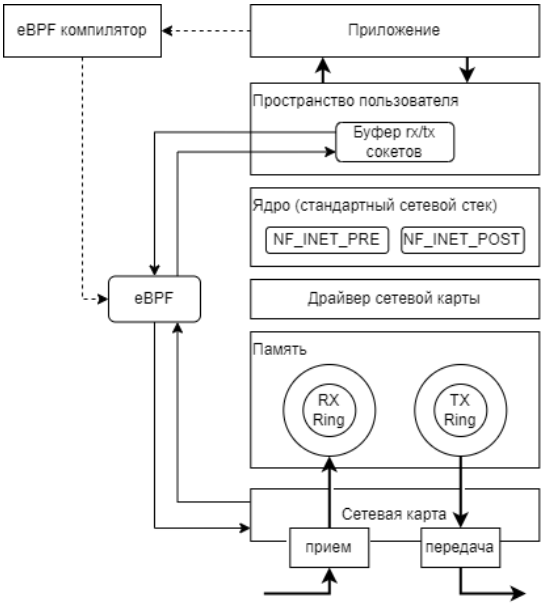


Рис. 2. eBPF в сетевом стеке Linux

Применение такой схемы позволяет добиться сразу нескольких преимуществ:

1) Такая программа позволит оценить время обработки сетевого пакета в ядре, с момента входя сетевого пакета до момента выхода, даже если это значение измерялось в наносекундах (для подсчёта можно использовать подсчёт процессорных тактов)[4].
2) Эта программа значительно сократит время нахождения пакета в ядре
3) Такая программа может перенести на уровень приложения логику обработки пакетов при перегрузках, в том числе организовать высокоуровневое взаимодействие с SDN сетью для перенаправления потоков траффика другими путями, при возможности.

Тестирование eBPF

Для проверки возможности извлечения информации был развернут стенд, включающий в себя 3 узла (рис. 3).

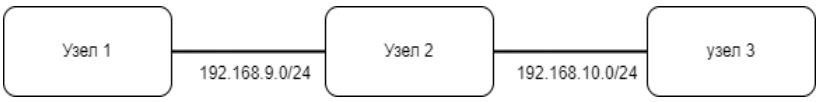


Рис. 3. Схема стенда

На узлах была установлена ОС Debian 12 (ядро Linux 6.2)

На узлах 1 и 3 было установлено приложение iperf

На узле 2 был развернут программный маршрутизатор, работавший во время тестов в 2 режимах:

1) XDP (eXpress Data Path),
2) Iptables.

Нагрузочное тестирование проводилось на протяжении 300 секунд. В первом случае были сконфигурированы правила Iptables для маршрутизации, во втором – в ядро была загружена программа для XDP (приложение 1) по результатам которого были построены графики общей производительности:

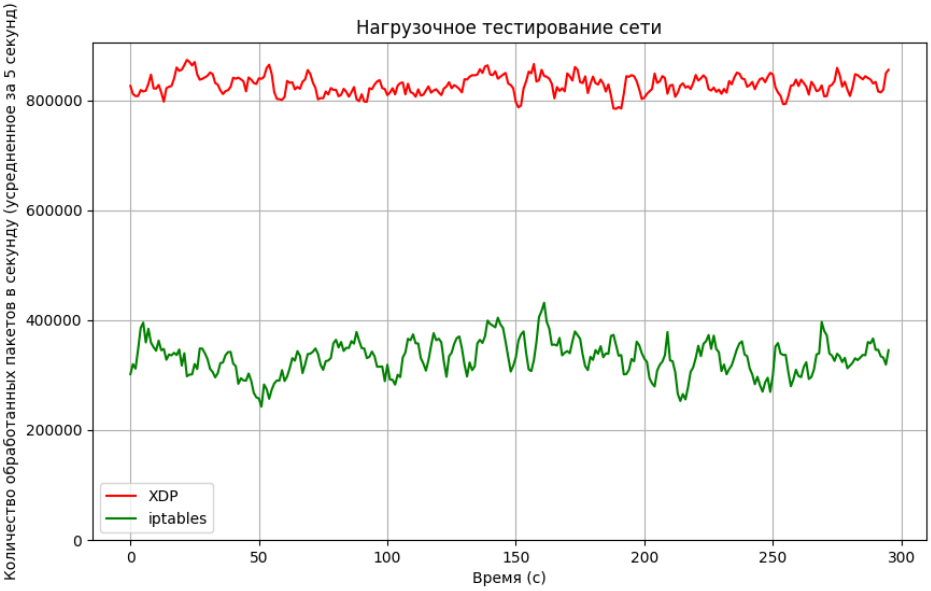


Рис. 4. Результат измерений

Также было выполнено измерение времени обработки каждого пакета, что в дальнейшем может быть агрегировано и использовано для анализа. Информацию о времени обработки, о количестве пакетов и о загрузки узлов можно использовать для создания агентов, который в распределенной системе будет использовать данные значения для изменения метрик протоколов динамической маршрутизации, что добавит возможность динамически управлять сетью на основании информации о фактической загрузке узла. Эти параметры (таблица 1) можно объединить и использовать для анализа.

ТАБЛИЦА 1. Параметры для анализа пакетов

Параметр	назначение
packet_core_time	Время обработки пакета траффика в ядре
packet_app_time	Время обработки пакета траффика приложением
packet_size	Размер пакета
packet_flow	Относится ли пакет к единому потоку

Заключение

На основании проведенного исследования была определена возможность использования методов отслеживания сетевых пакетов для повышения производительности сетей передачи данных. На основании полученных результатов нагрузочного тестирования (рис. 4) можно сделать вывод о том, что использование технологии eBPF в ядре операционных системы не только само по себе способно повысить производительность сети, но также позволяет получить дополнительную информацию (таблица 1), которую можно использовать для анализа загруженности сети.

Приложение 1

```
#include <linux/bpf.h>
#include <bpf/bpf_helpers.h>
#include <linux/if_ether.h>
#include <linux/ip.h>

SEC("xdp_router")
int xdp_ip_router(struct xdp_md *ctx) {
    void *data_end = (void *)(long)ctx->data_end;
    void *data = (void *)(long)ctx->data;

    struct ethhdr *eth = data;
    if ((void*)eth + sizeof(*eth) > data_end)
        return XDP_PASS;

    struct iphdr *ip = data + sizeof(*eth);
    if ((void*)ip + sizeof(*ip) > data_end)
        return XDP_PASS;
    if (ip->saddr == htonl(0xC0A80900) /* 192.168.9.0 */) {
    }
    return XDP_PASS;
}

struct bpf_map_def SEC("maps") packet_time_map = {
    .type = BPF_MAP_TYPE_HASH,
    .key_size = sizeof(unsigned long long),
    .value_size = sizeof(unsigned long long),
    .max_entries = 1024,
};
SEC("classifier")
int packet_start(struct __sk_buff *skb) {
    unsigned long long ts = bpf_ktime_get_ns();
```

```
    unsigned long long key = (unsigned long long)skb->hash;
    bpf_map_update_elem(&packet_time_map, &key, &ts, BPF_ANY);
    return TC_ACT_OK;
}

SEC("classifier")
int packet_end(struct __sk_buff *skb) {
    unsigned long long *start_ts, end_ts, delta;
    unsigned long long key = (unsigned long long)skb->hash;
    end_ts = bpf_ktime_get_ns();
    start_ts = bpf_map_lookup_elem(&packet_time_map, &key);
    if (start_ts) {
        // Вычисляем разницу
        delta = end_ts - *start_ts;
        bpf_map_delete_elem(&packet_time_map, &key);
    }
    return TC_ACT_OK;
}
```

Список используемых источников:

1. Васюткин А. В., Власов Д. В., Швидкий А. А. Анализ методов обеспечения взаимодействия сетевых устройств с приложениями в пользовательском пространстве операционной системы // Актуальные проблемы инфотелекоммуникаций в науке и образовании: материалы XI междунар. научно-технич. и научно-методич. конф., Санкт-Петербург, 15-16 фев. 2022 г. Т. 1, С. 239-243.

2. Sepehr Abbasi Zadeh, Ali Munir, Mahmoud Mohamed Bahnasy, Shiva Ketabi, and Yashar Ganjali. / On Augmenting TCP/IP Stack via eBPF. // Association for Computing Machinery, New York, NY, USA, 15–20. 2023. https://doi.org/10.1145/3609021.3609300

1. Andrea Mayer, Pierpaolo Loreti, Lorenzo Bracciale, Paolo Lungaroni, Stefano Salsano, Clarence Filsfils. / Performance Monitoring with Hˆ2: Hybrid Kernel // eBPF data plane for SRv6 based Hybrid SDN, Computer Networks, 2021, Volume 185, 2021, https://doi.org/10.1016/j.comnet.2020.107705.

2. O. Tilmans, O. Bonaventure / Continuously Observing Protocol Performance, arXiv preprint, https://arxiv.org/abs/1902.04280, 2019

Elagin V., Melnichenko A., Shvidkiy A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Analysis of the possibilities of using network packet tracking methods to improve the performance of data networks.

Ensuring the required level of data network performance in distributed cluster systems using microservice architectures is currently one of the most difficult tasks to solve, since constant interaction between nodes and services is of a heterogeneous nature, while the applications themselves, not being a monolithic core, cannot track occurrences such problems.

Key words: network traffic processing problems.

УДК 004.89
ГРНТИ 28.23.37

ПЕРСПЕКТИВНЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ НЕЙРОННЫХ СЕТЕЙ В СИСТЕМАХ ВИДЕОКОНФЕРЕНЦСВЯЗИ

В. С. Елагин, Ю. Е. Щегольский
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Нейронные сети стали популярными во многих областях человеческой жизни и телекоммуникации – не исключение. Исследования в области применения нейросетей для видеоконференцсвязи ведутся уже довольно давно. Эти исследования нацелены на улучшение качества видео и аудио передачи, а также на разработку инновационных функций, таких как автоматическое распознавание речи и фильтрация шумов.

Статья выделяет потенциал интеграции нейросетей в системы видеоконференцсвязи как ключ к улучшению коммуникативного опыта. Такой подход обещает не только повышение удобства и доступности видеоконференций, но и открывает новые горизонты для развития дистанционного взаимодействия в разнообразных сферах. Это значительный шаг вперед в понимании и применении машинного обучения для оптимизации современных систем коммуникаций.

нейронные сети, видеоконференцсвязь, идентификация трафика, классификация трафика

Введение

В последние годы наблюдается значительный рост использования систем видеоконференцсвязи в различных сферах деятельности. Это обусловлено потребностью в эффективных средствах коммуникации как в бизнесе, так и в личных взаимодействиях. Однако повышенный объём трафика и требования к качеству передачи данных ставят перед специалистами задачи оптимизации и улучшения работы систем видеоконференцсвязи.

В данной статье представлен анализ применения нейронных сетей в контексте работы с трафиком в системах видеоконференцсвязи. Основное внимание уделяется изучению способов улучшения качества изображения и звука, эффективности сжатия данных и снижения задержек в передаче информации.

Целью статьи является обобщение современных достижений в области машинного обучения и его вклада в решение актуальных задач, связанных с трафиком в системах видеоконференцсвязи.

Для каких целей использовать нейронные сети?

Нейронные сети могут быть использованы для обработки и оптимизации трафика в системах видеоконференцсвязи. Они могут помочь в следующих аспектах:

1. **Кодирование и декодирование видео:**

Нейронные сети могут быть использованы для сжатия видео, что особенно полезно в условиях ограниченной пропускной способности. В [1]

проведен анализ требований различных систем видеоконференцсвязи к пропускной способности, а также её влияние на качество изображения. Эффективное сжатие видео может улучшить качество видеоконференций, уменьшив задержки и потери кадров.

2. **Определение и коррекция ошибок:**

Нейронные сети могут помогать в обнаружении и коррекции ошибок в передаваемых видеоданных, что может быть полезно для улучшения качества видеоконференций в условиях нестабильного интернет-соединения.

3. **Улучшение качества видео:**

Алгоритмы машинного обучения могут быть использованы для улучшения качества видео в реальном времени, например, для устранения шума, улучшения освещенности или устранения размытия.

4. **Анализ поведения участников:**

Нейронные сети могут анализировать поведение участников во время видеоконференций, например, распознавая лица и выражения лица, что может быть полезно для бизнес-аналитики.

5. **Автоматическая генерация субтитров и перевод:**

Алгоритмы машинного обучения могут быть использованы для распознавания речи и автоматической генерации субтитров или перевода на другие языки в реальном времени.

6. **Оптимизация распределения ресурсов:**

Нейронные сети могут помогать в оптимизации распределения ресурсов сети, чтобы обеспечить лучшее качество видеоконференций.

7. **Обнаружение инцидентов безопасности:**

Алгоритмы машинного обучения могут быть использованы для обнаружения необычного или подозрительного поведения в видеопотоках, что может помочь в обеспечении безопасности видеоконференций.

Эти технологии могут быть весьма полезными для улучшения эффективности и качества видеоконференцсвязи в различных сферах.

Какие типы нейронных сетей подходят?

Для работы с трафиком видеоконференций можно использовать различные типы нейронных сетей. Вот несколько примеров:

1. **Long Short-Term Memory (LSTM)**, **Convolutional Neural Networks (CNN)** и **Sequence-to-Sequence (seq2seq) models**: Эти типы нейронных сетей были использованы для прогнозирования размеров видеокадров для видео в форматах H.264 и H.265. LSTM, CNN и seq2seq модели помогают захватить долгосрочные зависимости в данных видеотрафика, что может быть полезным для оптимизации передачи видео в реальном времени. [2]

2. В одном исследовании [3] были задействованы различные модели нейронных сетей сравнивались шесть моделей нейронных сетей по их способности предсказывать типы кадров MPEG-4 (I, P и B кадры).

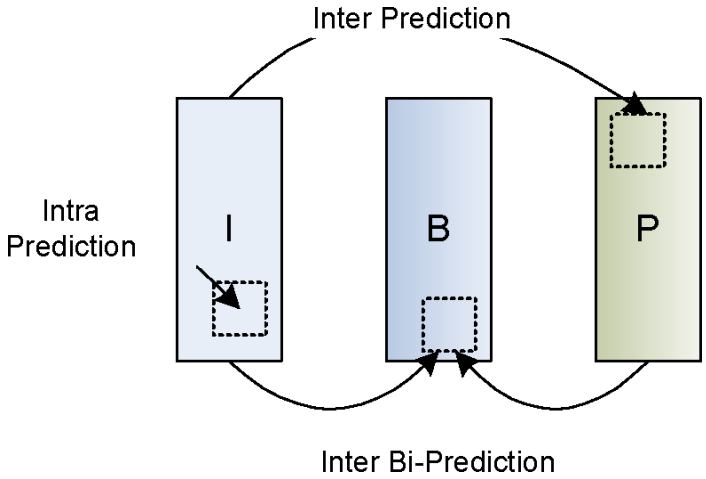


Рис. 31. Предсказание типов кадров

В [4] рассматривались задачи, с которыми отлично могут справиться методы машинного обучения. Одной из важнейших задач была – классификация трафика. Однако, традиционные методы машинного обучения требуют участия человека при извлечении признаков.

3. **Convolutional Neural Network (CNN), Ant-Lion Meta-Heuristic Algorithm (ALO)** и **Self-Organizing Map (SOM)**: Эти алгоритмы были использованы в комбинации для создания модели классификации трафика, которая может точно идентифицировать типы трафика. [5]

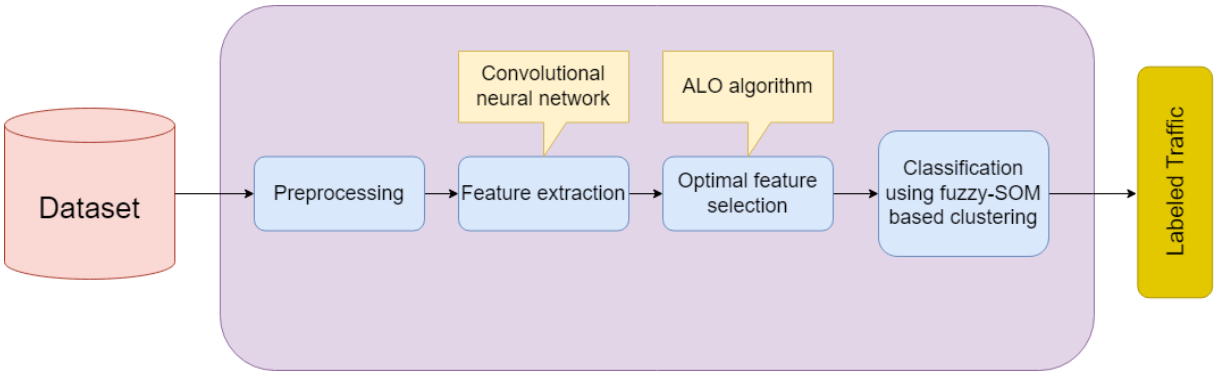


Рис. 32. Модель классификации трафика

4. **Graph Neural Network (GNN)**: Использование GNN для классификации трафика ассоциирует потоки пакетов с известными метками приложений, что важно для обеспечения безопасности сети и управления сетью. Это может быть полезным для анализа и оптимизации трафика видеоконференций. [6]

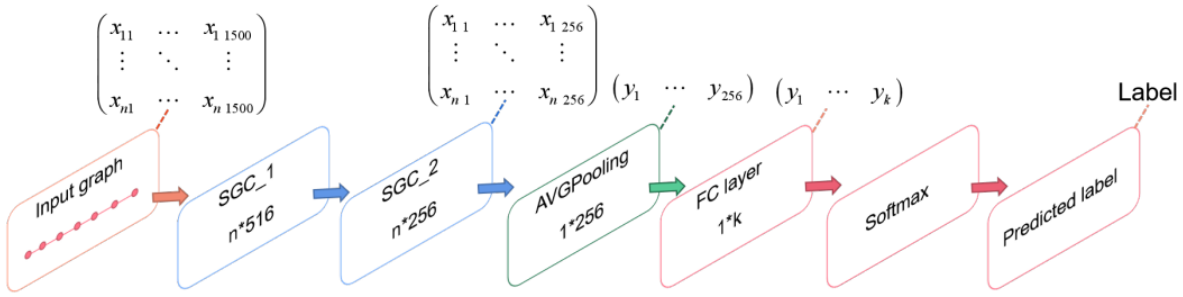


Рис. 33. Структура GNN

Эти модели могут быть адаптированы или интегрированы в системы видеоконференцсвязи для оптимизации трафика и улучшения качества видеопередачи. Особенно они могут быть полезными в сценариях с ограниченной пропускной способностью или нестабильными сетевыми условиями, помогая обеспечить высокое качество видеоконференций.

Заключение

С учетом все возрастающей роли видеоконференцсвязи в современном мире, важность оптимизации трафика и улучшения качества передачи видео и звука становится критически важной. Применение нейронных сетей предлагает инновационные подходы к решению этих задач. В этой статье были рассмотрены различные аспекты использования нейросетей, включая сжатие данных, улучшение качества изображения и звука, а также оптимизацию распределения ресурсов.

Нейросети предлагают разнообразные возможности для анализа и оптимизации трафика в системах видеоконференцсвязи. Они могут помочь в обеспечении высококачественных видеоконференций даже в условиях ограниченной пропускной способности или нестабильных сетевых условиях.

В заключение, интеграция нейросетей в системы видеоконференцсвязи открывает новые возможности для улучшения эффективности и качества коммуникаций. Такой подход не только способствует повышению удобства и доступности видеоконференций, но и может значительно повлиять на будущее дистанционных взаимодействий в бизнесе, образовании и других сферах.

Список используемых источников:

1. Елагин В. С., Некрасов В. Н. Анализ требования ВКС систем к ширине канала передачи // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы XII Междунар. науч.-технич. и науч.-методич. конф., Санкт-Петербург, 28 фев.-01 марта 2023 г. СПб. : СПбГУТ, 2023. Т. 1. С. 448–453, 2023.

2. Khandu O., Tanya M., Michael D., Kok W., Polychronis K. H.264 and H.265 video traffic modeling using neural networks // Computer Communications Vol. 184, Pp. 149-159, 2022.

3. Abdennour A., “Evaluation of neural network architectures for MPEG-4 video traffic prediction,” // IEEE Trans. Broadcast., vol. 52, no. 2, pp.184-192, 2006.

4. Елагин В. С., Щегольский Ю. Е. Обзор методов машинного обучения для задач анализа трафика [Электронный ресурс] // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы XII Междунар. науч.-технич. и науч.-методич. конф., Санкт-Петербург, 28 фев.-01 марта 2023 г. СПб. : СПбГУТ, 2023. Т. 1. С. 471–475.

5. Saadat I., Mahmood A., Rojia N. Network traffic classification using convolutional neural network and ant-lion optimization // Computers and Electrical Engineering Vol. 101, 2022.

6. Bo P., Yongquan F., Siyuan R., Ye W., Qing L., and Yan J. CGNN: Traffic Classification with Graph Neural Network. // In Proceedings of ACM Conference (Conference'17). ACM, New York, NY, USA, 16 pages, 2021.

Elagin V., Shchegolskiy Y.

The Bonch-Bruevich St. Petersburg State University of Telecommunications

Promising aspects of application neural networks in videoconferencing systems.

Neural networks have become popular in many areas of human life and telecommunications is no exception. Research in the application of neural networks for video conferencing has been going on for quite some time. This research is aimed at improving the quality of video and audio transmission as well as developing innovative features such as automatic speech recognition and noise filtering.

The paper highlights the potential of integrating neural networks into videoconferencing systems as a key to improving the communication experience. This approach promises not only to improve the convenience and accessibility of videoconferencing, but also opens new horizons for the development of remote interaction in a variety of domains. This is a significant step forward in understanding and applying machine learning to optimize modern communication systems.

Key words: neural networks, videoconferencing, traffic identification, traffic prediction, traffic classification.

УДК 654.1
ГРНТИ 50.41.23

АНАЛИЗ ПРИМЕНЕНИЯ ИНСТРУМЕНТОВ DEVOPS ПРИ РАЗВЁРТЫВАНИИ СИСТЕМ АВТОАТИЗАЦИИ, РАЗРАБОТАННЫХ НА ОСНОВЕ ODA-КОМПОНЕНТОВ

Й. Г. Камуежи, С. В. Кисляков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Инструменты DevOps успешно применяются для развёртывания и доставки программного обеспечения. Открытая цифровая архитектура, разрабатываемая консорциумом TM Forum, предполагает применение технологий DevOps для развёртывания систем автоматизации поставщиков цифровых услуг.

В статье рассматриваются место инструментария DevOps и его применение в рамках Открытой цифровой архитектуры.

open digital architecture, canvas, oda component, tm forum

Переход на Открытую цифровую архитектуру (Open Digital Architecture, ODA) подразумевает, что ИТ-ландшафт поставщика цифровых услуг (ПЦУ) будет формироваться из программных компонентов – ODA-компонентов, связанных между собой прикладными программными интерфейсами (API). ODA-компоненты рассматриваются как базовые блоки с конкретной узкой функциональностью (рис. 1). Вместо «монолита» OSS/BSS каждый сервис будет представлять собой четко определенный функционально самодостаточный компонент, взаимодействующий с другими компонентами. Развёртывание компонентов должно осуществляться средствами DevOps .

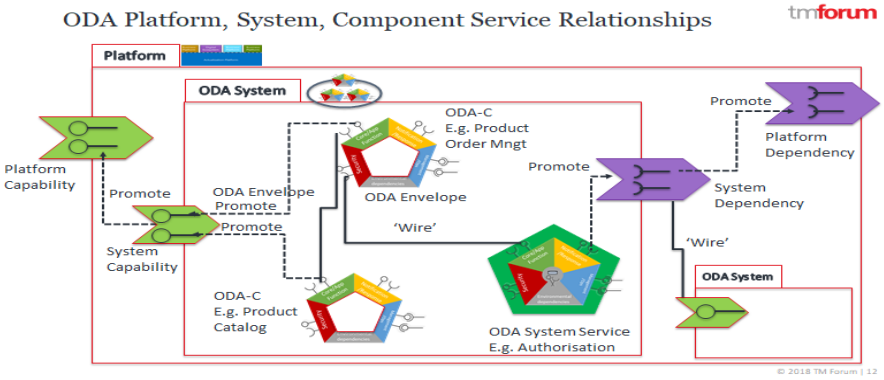


Рис. 1. Иллюстрация ИТ-ландшафта, построенного на основе ODA-компонентов

Анатомия компонента ODA

Компоненты ODA- это автономные программные сервисы, предназначенные для конкретных бизнес-целей .

Стандартный компонент имеет свою архитектуру (рис. 2), включающую:

Core Function – основная/базовая функциональность;

Notification/Reporting – уведомление/отчётность;

Management/Operation – управление;
Environment – взаимодействие с окружением;
Security – безопасность;

Для взаимодействия с другими компонентами нужен набор программных интерфейсов (API).

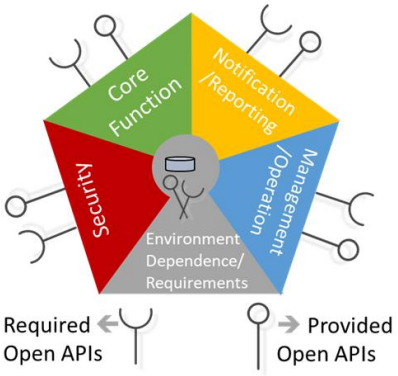


Рис. 2. Архитектура анатомия ODA-компонента

Основные возможности инструментов DevOps

Инструменты DevOps предоставляют ряд возможностей, которые способствуют повышению гибкости, качества и автоматизации процессов разработки и их эксплуатации. Вот некоторые из основных возможностей, предлагаемых этими инструментами.

Непрерывная интеграция (CI)

Непрерывная интеграция является одним из основных элементов DevOps. С помощью таких инструментов, как Jenkins, CircleCI и Travis CI, можно автоматизировать создание и тестирование приложений на постоянной основе. Эта же практика позволяет выявлять проблемы в цикле разработки, гарантировать поставку качественного программного обеспечения и снижать риск производственных сбоев.

Конвейер непрерывной интеграции (Continuous Integration, CI) формируется с помощью следующих шагов (рис. 3):

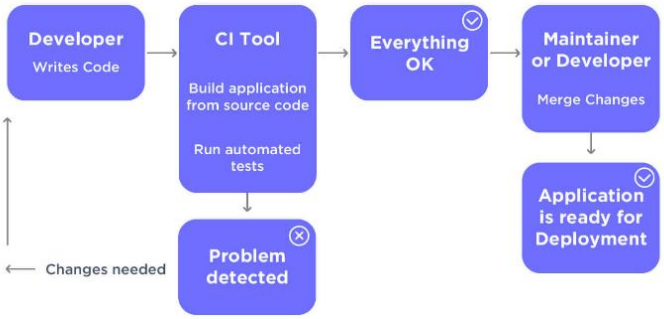


Рис. 3. Конвейер непрерывной интеграции

Непрерывная доставка (CD)

Непрерывная поставка - один из основополагающих этапов DevOps, на котором появляются инструменты для автоматизации процесса внедрения в производственные среды. Такие инструменты, как Ansible, Puppet и Chef,

позволяют быстро и безопасно выпускать новые версии программного обеспечения, гарантируя стабильность и надежность систем. Это сокращает время запуска ПО в производство, позволяя компаниям оперативно реагировать на запросы рынка.

Контроль версий

Одной из основных проблем разработки программного обеспечения является эффективное управление исходным кодом. Для этого в инструментах DevOps предусмотрены функции контроля версий, например Git. Git - это технология, которая широко используется для отслеживания изменений в исходном коде, что облегчает взаимодействие между членами команды и позволяет им работать более эффективно.

Мониторинг и протоколирование

Постоянный мониторинг производственной среды необходим для обеспечения бесперебойной работы приложений. В этой связи широко используются такие инструменты, как Prometheus, ELK (Elasticsearch, Logstash и Kibana) и Grafana. Эти инструменты позволяют отслеживать работоспособность и производительность приложений, а также упрощают анализ журналов и диагностику проблем. С их помощью команды DevOps могут проактивно обнаруживать и устранять проблемы, гарантируя непрерывную и удовлетворительную работу пользователей.

Технологии, используемые в инструментах DevOps

Инструменты DevOps [6] строятся на основе различных технологий, которые обусловливают их эффективность и способность интегрироваться с существующими системами. В качестве примера можно привести следующие технологии:

- Контейнеры: Docker - широко распространенная технология упаковки и развертывания приложений в контейнеры. Такой подход позволяет повысить переносимость и изолированность приложений, облегчая их развертывание и управление в различных средах.

- Оркестровка контейнеров: такие инструменты, как Kubernetes и Docker Swarm, обеспечивают оркестровку контейнеров в производственных средах. Они обеспечивают масштабируемость, балансировку нагрузки и автоматическое восстановление в случае сбоев.

- Инфраструктура как код: использование таких инструментов, как Terraform и CloudFormation, позволяет определять инфраструктуру, необходимую для запуска приложений, как код. Это позволяет автоматизировать и версионировать инфраструктуру, делая ее более гибкой и надежной.

Автоматизация конфигурирования: такие инструменты, как Ansible, Puppet и Chef, позволяют автоматизировать конфигурирование серверов и сред, снижая сложность и время, необходимые для обеспечения и управления инфраструктурой.

Среда *ODA Canvas*

Компоненты *ODA* развертываются на *ODA Canvas*, который представляет собой стандартизированную среду развёртывания *CI/CD*. *Canvas* является открытым исходным кодом и на 99,9% не зависит от технологий. В настоящее время у *ODA Canvas* есть только одна фиксированная технология: *Kubernetes*.

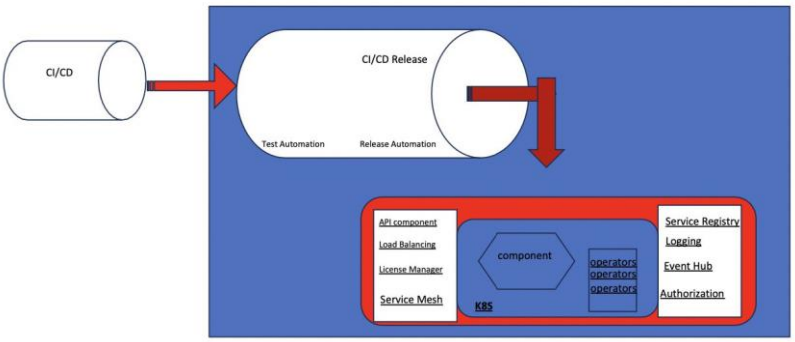


Рис. 4. ODA Canvas

Поэтому дальнейшей работой планируется построение полигона для развёртывания программных компонентов.

Список используемых источников:

1. Open Digital Architecture. [Электронный ресурс]. URL: https://www.tmforum.org/resources/whitepapers/open-digital-architecture (дата обращения: 23.10.23).

2. IG 1171 ODA Component Definition v4.0.0. [Электронный ресурс]. URL: https://www.tmforum.org/resources/standard/ig1171-oda-component-definition-v4-0-0 (дата обращения: 23.10.23).

3. IG 1171 ODA Component Definition v19.0.1. [Электронный ресурс]. URL: https://www.tmforum.org/resources/exploratory-report/ig1171-oda-component-definition-r19-0-0 (дата обращения: 23.10.23).

4. DevOps Concepts [Электронный ресурс]. URL: https://www.deal.com.br/blog/tudo-o-que-voce-precisa-saber-sobre-devops/ (дата обращения: 27.10.23).

5. DevOps Concepts [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/devops-concepts/viewer (дата обращения: 23.10.23).

6. DevOps Concepts [Электронный ресурс]. URL:https://blog.geekhunter.com.br/tudo-sobre-devops-iniciantes/ (дата обращения 23.10.23).

7. IG1222 Part 1: ODA Technical Architecture Overview. [Электронный ресурс]. URL: https://www.tmforum.org/resources/suite/ig1222-oda-technical-architecture-suite..

Camuegi Y.G., Kislykov S.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Analysis of devops tools in the deployment of automation systems based on oda components.

DevOps tools have been successfully used for software deployment and delivery. The open digital architecture developed by the TM Forum consortium provides for the use of DevOps technology to deploy automation systems for digital service providers.

This article examines the place of DevOps tools and its application within the framework of the Open Digital Architecture.

Key words: open digital architecture, canvas, oda component, tm forum.

УДК 004.72
ГРНТИ 49.03.11

ОБЗОР СИСТЕМЫ СЛАЙСИНГА СЕТИ С ПОМОЩЬЮ IBN ДЛЯ СЕТЕЙ 5G

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

Сеть пятого поколения предоставляет широкий спектр услуг, к которым предъявляются различные требования с точки зрения производительности, пропускной способности, надежности и задержки. Поэтому, виртуализация сети представляет собой надежное решение, называемое слайсингом сети, которое поддерживает гетерогенность услуг и предоставляет дифференцированные ресурсы для каждой службы.

сеть основанная на намерениях, 5G, слайсинг

Сеть, основанная на намерениях (*Intent-Based Networking*) - это новая технологическая концепция, направленная на применение более глубокого уровня интеллекта и предполагаемого состояния сети для замены ручных процессов конфигурирования и реагирования на сетевые проблемы. В концепции IBN сетевые администраторы определяют результат или намерение, а программное обеспечение сети определяет, как достичь этой цели, благодаря искусственному интеллекту и машинному обучению. Сетевые системы на основе намерений не только смогут автоматизировать трудоемкие задачи и обеспечивать видимость активности сети в реальном времени для подтверждения заданного намерения, но и прогнозировать возможные отклонения от этого намерения и предписывать действия, необходимые для его реализации. Это позволяет повысить скорость работы сети, сделать ее более гибкой и сократить количество ошибок. Сети на основе намерений имеют ряд весомых преимуществ по сравнению с обычными сетями и даже с программно-определяемыми сетями. Среди них такие преимущества, как сокращение количества ручных операций, более быстрый поиск и устранение неисправностей, снижение риска нарушения нормативных требований, оптимизированная аналитика [1].

В сетях мобильной связи пятого поколения представлен широкий спектр услуг, к которым предъявляются различные требования по производительности, пропускной способности, надежности и задержкам. Традиционные сети не способны обслуживать эти разнообразные услуги с помощью одной и той же физической инфраструктуры. Таким образом, виртуализация сети представляет собой надежное решение, получившее название «слайсинг», которое поддерживает неоднородность услуг и предоставляет дифференцированные ресурсы для каждой из них. Слайсинг позволяет операторам сетей создавать несколько логических сетей на общей физической инфраструктуре [2].

Здесь будет рассмотрена система нарезки сети на основе намерений, которая позволяет эффективно нарезать и управлять ресурсами базовой сети и сети радиодоступа (RAN). Это автоматизированная система, в которой пользователям достаточно предоставить конфигурацию сети более высокого уровня в виде намерений/контрактов для фрагмента сети, а в ответ система развертывает и конфигурирует запрошенные ресурсы соответствующим образом. Кроме того, система позволяет автоматизировать процесс конфигурирования сети и сократить объем ручного труда. Она оснащена инструментом создания сетей на основе намерений (IBN), который позволяет контролировать, управлять и отслеживать ресурсы сетевого слайса должным образом. Кроме того, для управления сетевыми ресурсами в ней используется модель глубокого обучения - генеративная состязательная нейронная сеть (GAN).

Слайсинг в сети 5G достигается с помощью технологий виртуализации сетевых функций (NFV) и программно-определяемых сетей (SDN). В отличие от расширенной мобильной широкополосной связи (eMBB) дизайн сети 5G может удовлетворить два новых требования к услугам: большое количество подключенных объектов, известное как массовая связь машинного типа (mMTC), и сверхнадежная связь с низкой задержкой (URLLC), которая требует высокой надежности и низкой задержки [3]. Основные три категории слайсов в сети 5G представлены на рис. 1.

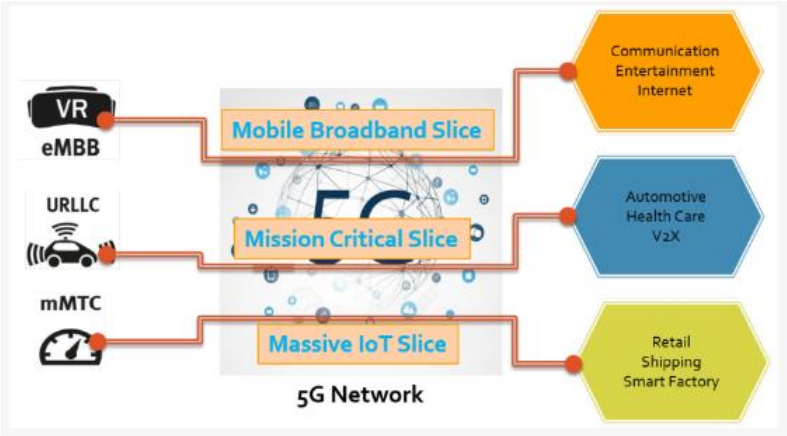


Рис. 1. Типы слайсов в сети 5G

Обозреваемая автоматизированная структура, получила название «*Intent-based Network Slicing*», в которой инструмент IBN используется для предоставления конфигураций верхнего уровня срезов сетевому оркестратору. Эта система включает в себя четыре основных модуля: инструмент IBN, сетевой оркестратор *Open-Source Mano* (OSM), контроллер сети радиодоступа FLEXRAN и модуль машинного обучения. Эта система может выполнять E2E-фрагментацию как для базовой сети, так и для сети доступа. Для сетей 5G необходима автоматизированная система управления, позволяющая создавать, удалять и обновлять сетевые фрагменты по

требованию, предоставляя лишь конфигурации абстрактного уровня. Таким образом, система позволяет автоматизировать процедуру создания сетевых фрагментов с помощью инструмента IBN.

Обозреваемая система состоит из четырех основных модулей: OSM (Open Source MANO), инструмент для построения сетей на основе намерений, SDN-контроллер FLEXRAN и модуль глубокого обучения (DL).

Платформа управления и оркестровки с открытым исходным кодом (OSM) - это проект ETSI, предоставляющий операторам связи оркестровщик сетевых услуг E2E для автоматического развертывания сетевых сервисов. OSM разработана на основе стандартов NFV и обеспечивает взаимодействие оркестратора с другими компонентами, такими как инфраструктурные менеджеры VIM, NFVI и сетевые функции.

Система IBN может автоматизировать процедуру нарезки сети, просто предоставляя конфигурации более высокого уровня из внешнего интерфейса инструмента IBN. Функциональность каждого компонента заключается в следующем: контрактный дизайн обеспечивает простой способ для пользователей (операторов, абонентов) системы определить свои намерения, используя «*front-end*» инструмента IBN. Пользователи системы определяют свои требования к ресурсам для создания фрагмента простым перетаскиванием на «*front-end*» портале системы. Менеджер намерений выступает в роли координатора для всех компонентов и общается с ними напрямую.

FLEXRAN - это программно-определяемая платформа RAN (SD-RAN) с открытым исходным кодом, которая разделяет плоскость управления RAN и плоскость данных. Она обеспечивает поддержку программирования на двух уровнях: первый - для разработки приложений контроля и управления над контроллером FlexRAN, второй - для разработки приложений внутри контроллера для выполнения автоматического развертывания функций управления. С помощью FlexRAN-протокола главный контроллер может контролировать и управлять работой каждой eNB. Абстрактное представление контроллера FlexRAN и его связи с плоскостью данных eNodeB показано на рис. 2.

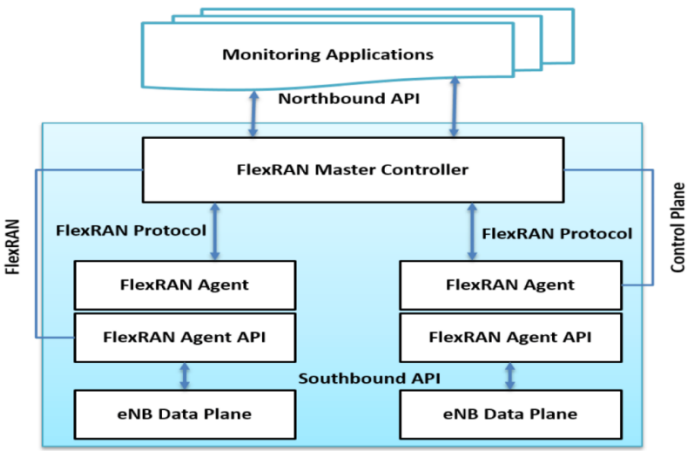


Рис. 2. Абстрактное представление контроллера FlexRAN

Расширенный модуль глубокого обучения GAN - это известная модель глубокого обучения, которая в основном используется для обработки изображений, видео и задач компьютерного зрения, но в данной системе она использована для прогнозирования и предсказания использования ресурсов на следующий период.

Пользователь определяет требования к слайсу на графическом интерфейсе инструмента IBN, включая информацию о нисходящем и восходящем канале, времени начала и окончания работы, а также SNSSAI слайса. После этого менеджер намерений системы IBN взаимодействует с хранилищем ресурсов и хранилищем политик для создания графа политики типа VNFFG. Созданный граф политики содержит информацию о запрашиваемых ресурсах ядра и RAN и связях между ними. Этот граф политики направляется в конфигураторы политики для дальнейшей обработки. Конфигураторы политики IBN являются очень важной частью системы IBN. В системе IBN существует два типа конфигураторов политики: конфигуратор политики OSM и конфигуратор слайсинга RAN. Задача конфигуратора политики OSM - получить граф политики и перевести его в формат строки JSON. Конфигуратор политики RAN, напротив, преобразует информацию графа политики в TOSCA, а затем в файл JSON. Более того, конфигуратор политики OSM передает эти конфигурации в OSM NFVO для развертывания ресурсов ядра EPC. С другой стороны, конфигуратор RAN отправляет JSON-файл контроллеру FlexRAN, и тот развертывает QoS слайса на eNodeB. Он также содержит информацию о выделенном MME и SNSSAI слайса, который соединяет слайс RAN с ядром EPC. VNF ядра EPC развертываются с помощью OSM NFVO и VIM (*OpenStack*) с использованием шаблона слайса в формате JSON-строки. После создания слайса пользователь получает уведомление с помощью IBN. Таким образом, создается сетевой слайс, не требующий ручной работы или специальных знаний. Пользователь может определить требования к QoS слайса на языке высокого уровня путем перетаскивания из графического интерфейса IBN, а система автоматически транслирует эти требования QoS в виде шаблона слайса и соответствующим образом размещает ресурсы.

В данном обзоре рассматривается реализация платформы для нарезки сетей E2E на основе намерений, которая позволяет операторам сетей развертывать сетевые сервисы гибким и настраиваемым образом. Сетевые операторы создают сетевой срез с помощью графического интерфейса приложения IBN, в котором пользователи просто вводят конфигурации верхнего уровня в виде требований QoS. Система IBN с помощью конфигураторов политик OSM и RAN разрабатывает шаблон фрагмента и отправляет эти конфигурации сетевому оркестратору OSM и контроллеру FlexRAN для развертывания ресурсов. Система позволяет операторам сети автоматизировать процесс конфигурирования сети и создания фрагментов.

Кроме того, модель глубокого обучения прогнозирует и предсказывает состояние сетевых ресурсов во время выполнения программы, что помогает менеджеру намерений принимать решение о допуске к использованию фрагментов. Тесты системы показали многообещающие результаты по созданию и управлению сетевыми фрагментами.

Список используемых источников:

1. Хизар Аббас, Мухаммад Афак, Тальха Ахмед Хан, Адиль Рафик, Ван-Чхоль Сон. Slicing the Core Network and Radio Access Network Domains through Intent-Based Networking for 5G Networks [Электронный ресурс] // Планирование и управление сетями радиодоступа: Кафедра компьютерной инженерии, Национальный университет Чеджу, Чеджуси, Корея. URL: https://www.mdpi.com/2079-9292/9/10/1710/htm (дата обращения: 11.10.2023).

2. Гребенщикова А.А., Елагин В.С. Моделирование данных трафика для оценки слайсинга в умной системе 5G на обратной линии связи [Электронный ресурс] // Информационные технологии и телекоммуникации. URL: https://elibrary.ru/item.asp?id=43882113 (дата обращения: 12.10.2023).

3. Елагин В. С., Врублевский Г. М., Мирзоев Э. И., Эктова А. И. Обзор основных направлений услуг сетей 5G и их интеграция с умеренным анализом сетевых данных [Электронный ресурс] // URL: https://elibrary.ru/item.asp?id=46412059 (дата обращения: 11.10.2023).

Mitin E.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Overview of network slicing system with IBN for 5G networks.

The 5G network provides a wide range of services with different requirements in terms of performance, bandwidth, reliability and latency. Therefore, network virtualization provides a reliable solution called network slicing that supports service heterogeneity and provides differentiated resources for each service.

Key words: Intent-Based Network, 5G, slicing

УДК 004.9
ГРНТИ 50.49.33

АНАЛИЗ ПРИМЕНИМОСТИ МЕТОДОВ АВТОМАТИЗИРОВАННОГО РАЗВЁРТЫВАНИЯ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ ДЛЯ РАБОЧИХ МЕСТ ПОЛЬЗОВАТЕЛЕЙ

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

В работе поднята тема применимости методов автоматизированного развёртывания облачной инфраструктуры для рабочих мест пользователей. В материале рассмотрено понятие облачных вычислений, описана необходимость автоматизированного развертывания облачной инфраструктуры и осуществлен обзор методов для реализации механизмов автоматизации.

автоматизированное развёртывание, облачная инфраструктура, PXE, Ansible, Terraform

В мире информационных технологий современные организации сталкиваются с растущей потребностью в развертывании и управлении рабочими местами пользователей. Для эффективного управления большим количеством рабочих мест, однотипных задач и постоянной необходимости поддержания рабочего состояния, методы автоматизированного развёртывания облачной инфраструктуры предоставляют существенные преимущества.

На рис. 1 представлена типовая схема облачной инфраструктуры.

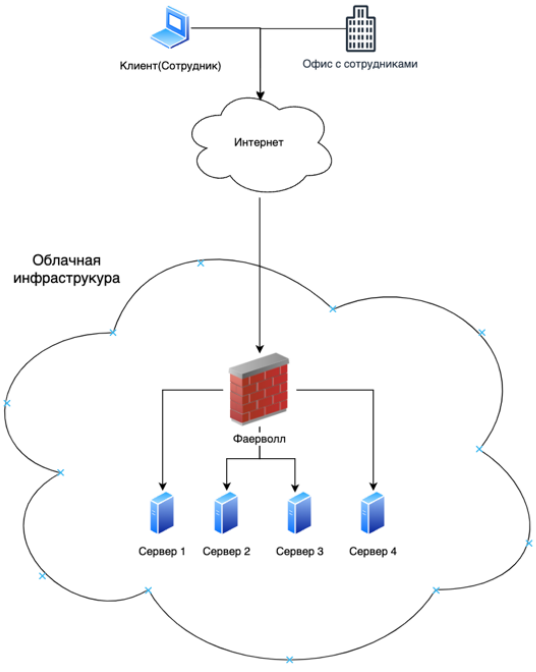


Рис. 1. Типовая схема облачной инфраструктуры

Облачные сервисы предоставляют гибкость, масштабируемость и доступность, что делает их привлекательными для организаций всех размеров. Вот некоторые ключевые аспекты, которые обосновывают необходимость автоматизации развертывания:

1. Гибкость и масштабируемость

Облачные ресурсы легко масштабируются в зависимости от потребностей компании. Это позволяет быстро адаптироваться к изменяющимся рыночным условиям.

2. Удаленный доступ

Пользователи могут работать из любой точки мира, что повышает мобильность и увеличивает производительность

3. Безопасность данных

Многие облачные провайдеры обеспечивают высокий уровень безопасности данных и автоматическое резервное копирование.

4. Снижение затрат

Компании могут сэкономить на ИТ-инфраструктуре, так как не требуется оборудование и обслуживание серверов.

5. Централизованное управление

Централизованное управление рабочими местами пользователей упрощает задачи администраторов. Они могут настраивать и обновлять приложения и операционные системы одновременно для всех пользователей.

Следует отметить, что одной из ключевых задач при использовании облачных ресурсов является эффективное управление и развёртывание рабочих мест для пользователей. В этой статье проведен обзор методов автоматизированного развёртывания облачной инфраструктуры:

1. PXE (Preboot eXecution Environment)

PXE — это мощный метод автоматизации развёртывания операционных систем на рабочих местах. Он особенно полезен в организациях с большим числом компьютеров, такими как киоски для обслуживания клиентов или точки продаж. PXE позволяет удаленно устанавливать и настраивать операционные системы через сеть, снижая ручное вмешательство и сокращая время развёртывания. Однако, его использование требует уровня экспертизы и может быть сложным для настройки.

2. Ansible

Ansible — это инструмент для автоматизации конфигурации и управления серверами, который также может использоваться для управления настройками и приложениями на рабочих станциях. Ansible предоставляет гибкость и легкость использования, позволяя создавать Playbooks для определения задач, таких как установка программного обеспечения и настройка конфигурации. Это особенно полезно для средних и крупных организаций.

3. Cloud-Init

Cloud-Init — это инструмент, который позволяет настраивать виртуальные машины в облаке при их создании. Он может использоваться

для определения параметров, установки SSH-ключей и выполнения скриптов при первом запуске рабочих станций. Этот метод подходит для сред организаций, где рабочие станции базируются на виртуальных машинах.

4. Terraform

Terraform — это инструмент для описания и управления инфраструктурой как кодом. Он может быть использован для создания и управления рабочими станциями в облаке, предоставляя возможность автоматизировать процесс развёртывания и настройки. Terraform особенно полезен в случае, когда необходимо масштабировать инфраструктуру и поддерживать её в актуальном состоянии.

5. Другие методы и инструменты

Кроме вышеперечисленных методов, существует множество других инструментов и подходов для автоматизации развёртывания рабочих мест в облаке. Например, Docker и контейнеры позволяют упаковывать приложения и их зависимости в контейнеры, что упрощает развёртывание и управление приложениями на рабочих станциях. Решения для управления мобильными устройствами (MDM) могут быть использованы для автоматизации развёртывания и управления ноутбуками и смартфонами пользователей. Также стоит учесть, что многие облачные провайдеры предоставляют собственные инструменты и API для управления инфраструктурой и рабочими станциями.

PXE предоставляет высокую степень контроля и унификации, но может потребовать значительной инфраструктуры и административных ресурсов.

Ansible и Terraform предоставляют максимальную гибкость и масштабируемость, но требуют навыков программирования и настройки.

CloudInit и инструменты облачных провайдеров обеспечивают удобство и быстроту развёртывания в облаке, но могут оказаться менее удобными при работе с локальными серверами.

Таки образом, автоматизация развёртывания облачной инфраструктуры для рабочих мест пользователей представляет собой важное звено в обеспечении гибкости и эффективности бизнес-процессов. Выбор методов и инструментов зависит от конкретных потребностей организации, размера и сложности инфраструктуры, а также уровня экспертизы в области автоматизации. Эффективное развёртывание обеспечивает высокую консистентность, безопасность и доступность для пользователей, что, в свою очередь, способствует повышению производительности и снижению операционных затрат.

Список используемых источников:

1. Официальный сайт Ansible [Электронный ресурс]. URL: https://www.ansible.com/ (дата обращения: 25.10.2023).

2. Официальный сайт Terraform [Электронный ресурс]. URL: https://registry.terraform.io/browse/providers (дата обращения: 25.10.2023).

3. Безпятый М.В. Автоматизация и оптимизация процессов разработки и развертывания в devops: применение современных методов и инструментов [Электронный

ресурс] // Инновации и инвестиции: электрон. научн. журн. 2023. N 7. URL: https://cyberleninka.ru/article/n/avtomatizatsiya-i-optimizatsiya-protsessov-razrabotki-i-razvertyvaniya-v-devops-primenenie-sovremennyh-metodov-i-instrumentov/viewer (дата обращения: 25.10.2023).

Shestakova V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Analysis of the applicability of methods for automated deployment of cloud infrastructure for user workplaces.
The work raises the topic of using methods for carefully deploying a cloud work environment for user workstations. The cloud computing resource describes the necessary cloud deployment requirements and provides overview methods for implementing automation.

Key words: Automated deployment, cloud infrastructure, PXE, Ansible, Terraform

Секция 3.4.
Оптоэлектронные технологии (фотоника) в инфокоммуникациях

УДК 004.7
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ РАЗЛИЧНЫХ ФОРМАТОВ МОДУЛЯЦИИ ДЛЯ УВЕЛИЧЕНИЯ РАДИУСА СЕТЕЙ NG-PON2 ПРИ ИСПОЛЬЗОВАНИИ ОТРАЖАТЕЛЬНОГО ПОЛУПРОВОДНИКОВОГО ОПТИЧЕСКОГО УСИЛИТЕЛЯ (RSOA)

А. А. Беляев, А. Ю. Слепогин
Санкт-Петербургский государственный университет Телекоммуникаций им. проф. М.А.Бонч-Бруевича

Архитектура PON с мультиплексированием по длине волны (TWDM-PON) является жизнеспособным важным решением для NG-PON2, которое обеспечивает большую полосу пропускания для двунаправленной передачи. В этой статье предлагается конструкция TWDM-PON расширенного радиуса действия на основе отражательного полупроводникового оптического усилителя (RSOA). TWDM-PON с использованием RSOA моделируется и исследуется для различных фотодетекторов. Анализ также проводится для различных расстояний и скоростей передачи данных. Сравнительный анализ различных форматов модуляции показывает, что дифференциальная фазовая манипуляция с подавлением несущей (CSRZ-DPSK) дает наилучшие характеристики на больших расстояниях и больших скоростях передачи данных, а возврат к нулю (RZ) дает наименьшую производительность.

FTTH, PON, NG-PON2, QoS, отражающий полупроводниковый оптический усилитель (RSOA), TWDM

Введение

С каждым годом в современном мире становится всё больше и больше высокопроизводительных сетевые системы, таких как ноутбуки, смартфоны, и их приложений, требующих большей пропускной способности, таких как Интернет вещей (IoT), удаленные медицинские услуги, облачные вычисления, общий доступ к файлам, облачные хранилища, видео- и веб-конференции, онлайн-аудио- и видеопотоки. Стремительный рост спроса на полосу пропускания для коммерческих приложений обусловливает острую потребность абонентов в высоких скоростях передачи данных. Абонентам с высокой пропускной способностью обеспечивается более высокая скорость передачи данных, снижение количества сбоев, отказов или сигналов занятости, более высокая производительность приложений, возможность одновременного использования большего числа пользователей, расширенные возможности передачи данных и обеспечение большей интерактивности и т.д. Технология NG-PON2 упреждает растущие запросы пользователей. NG-PON2 также предоставляет гибкие услуги по отношению к потребителю. Низкая задержка и качество обслуживания (QoE) свойственны NG-PON2.

Современным методом обеспечения высокой скорости передачи данных конечным пользователям является внедрение сети NG-PON2. TWDM-PON является ключевым методом для NGPON2. Это первый многоточечный широкополосный доступ, обеспечивающий скорость передачи данных 40

Гбит/с на расстоянии 40 км без усилителя, что является экономичным решением и обладает очень высокой эффективностью. Операторам связи требуются системы NG-PON2 для обеспечения большей пропускной способности, огромной полосы пропускания, большего числа пользователей и более широкого охвата.

В статье описывается TWDM-PON для восходящего потока с использованием пакетного режима и нисходящего потока с использованием непрерывного режима для передачи со скоростью 50 Гбит/с с использованием форматов модуляции с возвратом к нулю (NRZ) и оптических усилителей [1].

В другой статье предлагается двунаправленный TWDM-PON с использованием формата модуляции NRZ для обеспечения высокой пропускной способности 80 Гбит/с на расстоянии 50 км с минимальным BER с использованием процесса оптимизации мощности от 5 до 10 дБм [2].

В этой статье была проанализирована Манчестерская, дифференциальная фазовая манипуляция (DPSK) и дифференциальная квадратурная фазовая манипуляция (DQPSK) для разных расстояний и разных скоростей передачи данных. Они описаны в терминах частоты битовых ошибок (BER) и коэффициента качества (Q-factor) для оптических систем [3].

Новый NG-PON2 рассчитан на 2048 пользователей, использующих архитектуру TWDM-PON, и обеспечивает дальность действия до 100 км с использованием оптических усилителей. Моделируются и оцениваются мощность шума излучения усилителя и мощность насыщения потерь оптического усилителя и разветвителя. Конструкция анализируется по параметру QoS [4].

Предлагаемая сеть NG-PON2 с суммированием длин волн разработана и реализована в инструменте моделирования Optisystem 14.0 с использованием программного обеспечения Optiwave photonic. Моделирование проводится и исследуется на различном расстоянии от 10 км до 100 км для различных форматов модуляции. Моделирование также проводится и исследуется для различной скорости передачи данных от 10 Гбит/с до 80 Гбит/с для различных форматов модуляции. Анализ также проводится для различных типов конфигурации приемника, таких как PIN-фотодетектор и APD-фотодетектор, для вышеуказанных условий расстояния и скорости передачи данных и для различной модуляции.

Формат модуляции CSRZ-DPSK дает наилучшую производительность при значении BER $5*10^{-9}$, следующую хорошую производительность дает NZR-DPSK со значением BER $2{,}5*10^{-9}$, за ним следует RZ-DPSK и наименьшая производительность $5*10^{-7}$ для формата RZ на расстоянии 10 км. На расстоянии 100 км значение BER увеличивается с $4*10^{-8}$ до 10^{-7} . Для передачи данных на большие расстояния можно использовать выбор оптимального формата из CSRZ-DPSK, NRZ-DPSK, RZ-DPSK.

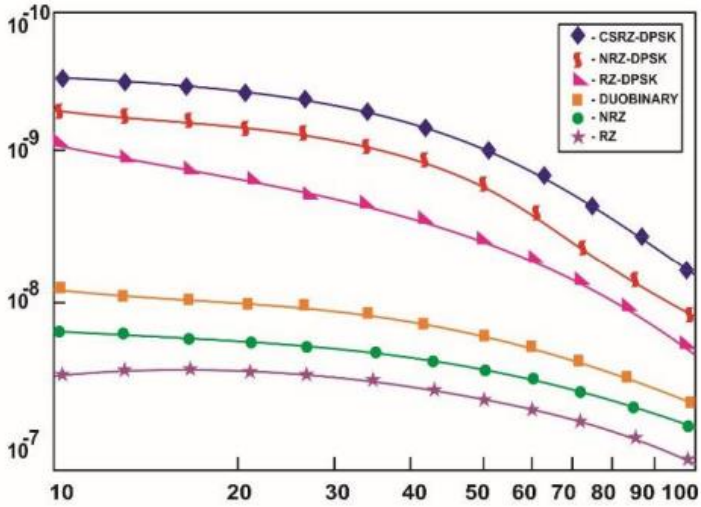


Рис. 1. Соотношение BER/дистанция для разных форматов модуляции (PIN-фотодиод)

Анализ добротности для различных расстояний: Влияние фактора расстояния анализируется с помощью PIN-приемника. Это показано на рис. 2.

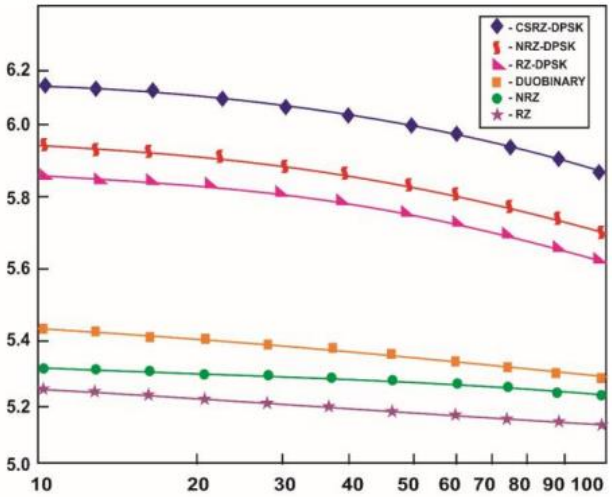


Рис. 2. Соотношение Q-фактор/дистанция для разных форматов модуляции (PIN-фотодиод)

Влияние расстояния анализируется с точки зрения добротности и сравнивается для всех шести типов форматов модуляции. Формат модуляции CSRZ-DPSK дает наилучшие показатели добротности, равные 6,19, следующие хорошие показатели дает NZR-DPSK со значением добротности 5,96, за которым следует RZ-DPSK, а наименьшие показатели дает формат RZ со значением 5,25 и наблюдаются на расстоянии 10 км. При максимальном расстоянии в 100 км добротность уменьшается с 5,97 до 5,12. Это показано на рис. 3.

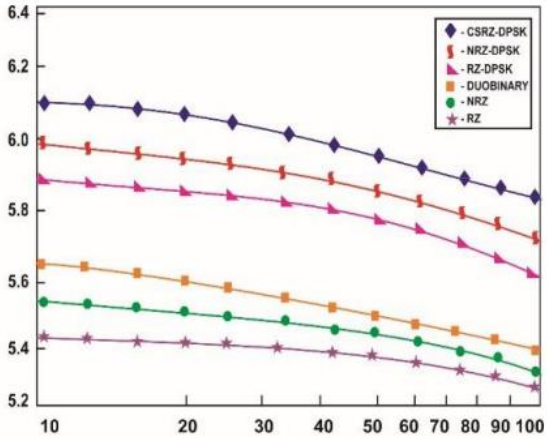


Рис. 3. Соотношение Q-фактор /дистанция для разных форматов модуляции (APD-фотодиод)

Влияние расстояния анализируется с точки зрения BER и сравнивается для всех шести типов форматов модуляции. Формат модуляции CSRZ-DPSK дает наилучшую производительность при значении BER $5{,}7*10^{-11}$, следующую хорошую производительность дает NZR-DPSK со значением BER $4*\ 10^{-11}$, за которым следует RZ-DPSK, а наименьшую производительность имеет формат RZ, равный $5*10^{-8}$ на расстоянии 10 км. На расстоянии 100 км значение BER увеличивается с $5*10^{-9}$ до $3*10^{-8}$. Это показано на рис. 4.

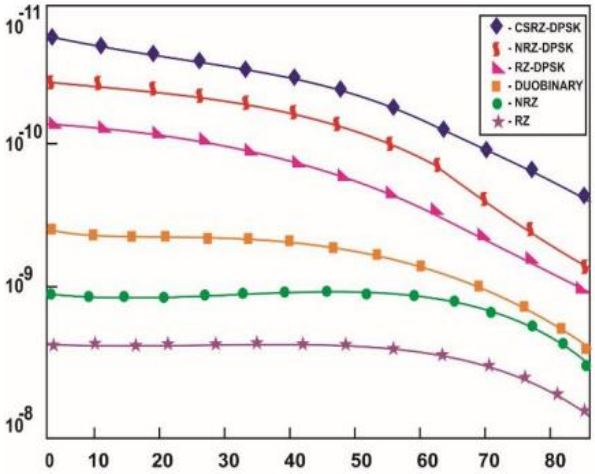


Рис. 4. Соотношение BER/дистанция для разных форматов модуляции (APD-фотодиод)

Заключение

В этой статье архитектура суммирования длин волн сети NGPON2 для расширенного охвата разработана, реализована и смоделирована для различных форматов модуляции с использованием усилителей RSOA. Конструкция анализируется с учетом различных факторов, а именно: увеличения расстояния и скорости передачи данных. Факторы также исследуются для различных режимов работы приемника, а также как для нисходящей, так и для восходящей передачи. Сравнительный анализ различных форматов модуляции показывает, что дифференциальная фазовая манипуляция с подавлением несущей (CSRZ-DPSK) дает наилучшие

характеристики на больших расстояниях и больших скоростях передачи данных, а возврат к нулю (RZ) дает наименьшую производительность.

Список используемых источников:

1. Borkowski, R., Schmuck, H., Cerulo, G., Debrégeas, H., & Bonk, R., “Single-Wavelength Symmetric 50 Gbit/s Equalization-Free NRZ IM/DD PON with up to 33 dB Loss Budget and Fiber Transmission over> 40 km”, Optical Fiber Communication Conference, pp. W2A-26, 2019.

2. Aly, M. H., & Saleh, M. B, “Evaluation and optimization of TWDMPON system capacity over single bidirectional optical fiber: Migration promising solution for the next generation PONs”, International Conference on Computer and Information Sciences, pp. 1-6, 2019.

3. Gill, H. K., Walia, G. K., & Grewal, N. S, “Performance analysis of mode division multiplexing IS-OWC system using Manchester, DPSK and DQPSK modulation techniques”, Optik, vol 177, pp. 93-101, 2019.

4. S. Rajalakshmi., T. Shankar., “Optimization of Optical Amplifier Saturation power in NG-PON2 using 2048 way Splitter”, Pakistan Journal of Biotechnology, Vol. 14 (Special Issue II) pp. 28-32, 2017.

Belyaev A., Slepogin A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Investigation of Different Modulation Formats for Extended Reach NG-PON2 using RSOA

The Time-Wavelength Multiplexed PON (TWDM-PON) architecture is a viable, important solution for NG-PON2 that provides more bandwidth for bidirectional transmission. This article proposes an extended-range TWDM-PON design based on a reflective semiconductor optical amplifier (RSOA). TWDM-PON using RSOA is modeled and investigated for various photodetectors. The analysis is also carried out for various distances and data transfer rates. A comparative analysis of various modulation formats shows that differential phase manipulation with carrier suppression (CSRZ-DPSK) gives the best performance over long distances and high data transfer rates, and a return to zero (RZ) gives the lowest performance.

Key words: TWDM-PON, APD, RSOA, QoS, FTTH, PON, NG-PON2

УДК 621.39
ГРНТИ 49.29.01

КЛАССИФИКАЦИЯ ПОДВОДНЫХ ЛИНИЙ СВЯЗИ

Я. А. Бовбель, Л. О. Дубовиков, Д. А. Юклутов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире, где телекоммуникации стали неотъемлемой частью нашей повседневной жизни, подводные линии связи играют важнейшую роль в обеспечении связи между континентами и островами по всей планете. Это инженерное решение стало незаменимым элементом глобальной коммуникационной инфраструктуры, обеспечивая передачу данных на огромные расстояния под водой. В данной статье мы более подробно рассмотрим основные типы подводных линий связи, их особенности, функциональные элементы и сферы применения.

подводные линии, ROPA (Remote Optically Pumped Amplifier), EDFA (Erbium Doped Fiber Amplifier), DWDM (Dense Wavelength Division Multiplexing)

ВВЕДЕНИЕ

У людей всегда была потребность в связи между собой на значительном удалении друг от друга. На этом расстоянии возникали водные преграды, и обход их вдоль водоемов всегда приводил к большим затратам. Поэтому перед инженерами связи ставится задача о прокладке кабеля по дну водоемов. Первая подводная линия связи была проложена по дну Ла-Манша между Великобританией и Францией в 1850 году. Со временем направляющие среды развивались и люди разработали оптическое волокно. Первой в мире трансокеанической волоконно-оптической линией связи была линия между Японией и США и составляла она 10 тысяч километров, была построена в 1988 году.

1 Классификация линий подводных связей

Современные подводные линии связи можно классифицировать по следующим признакам:

1)Протяженность: короткие (нет восстановления), длинные (есть восстановление).

2)Усилительные пункты: без усиления, усиление с дистанционной накачкой и волокна для накачки, усиления с дистанционным питанием и СУЭП.

В данной статье рассматриваются линии связи, классифицированные по признаку “Протяженность”. Рассмотрим подробнее каждую из категорий.

2 Короткие однопролетные линии связи

Для начала стоит отметить, что во всех вариантах рассматриваются линии с когерентным приемом. Использование некогерентного приема нецелесообразно так как возникает необходимость оптической компенсации хроматической дисперсии. Короткие линии связи как правило выполняются однопролетными (рис.1). Общая длина может достигать 180 км. Зачастую

они используются для перехода рек шириной до нескольких километров, если отсутствует возможность перехода по мостам. Такие подводные переходы включаются в состав наземных линий и с точки зрения дизайна *DWDM* систем ничем не отличаются от обычных. Ввиду малой протяженности используется стандартное *G.652* волокно. Ввиду необходимости сокращения количества подводных муфт из-за дороговизны, сложности их монтажа и обслуживания, для строительства используются большие строительные длины - 25 - 50 км.

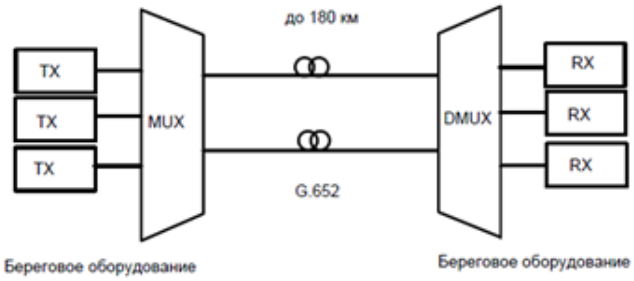


Рис. 1. Короткая однопролетная линия связи

3 Однопролетные линии с *ROPA*.

Более протяженные однопролетные линии связи включают в себя усилители с удаленной накачкой - *ROPA*. Такие линии соединяют острова или прокладываются вдоль береговой линии. Усилители *ROPA* (рис. 2) можно разделить на два функциональных блока: активное станционное оборудование и пассивное встраиваемое в пролет линии связи. На станции устанавливается генератор оптического излучения, называемого накачкой, на длине волны близкой к 1480 нм и специальный мультиплексор для ввода этой накачки в телекоммуникационное волокно с рабочими каналами линии связи. На расчетном расстоянии от начала линии, в нее встраивается подводная муфта с отрезком эрбиевого волокна, в котором происходит усиление сигнала. Кроме совместной доставки накачки с рабочими каналами по одному волокну, дополнительная накачка может быть доставлена по отдельным волокнам.

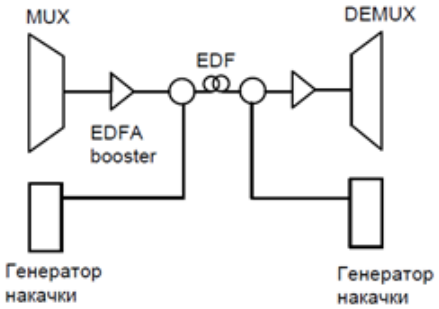


Рис. 2. Схема *ROPA*

Количество усилителей *ROPA* может варьироваться от одного до двух. А максимальная длина в реальной линии может достигать 300-350 км (рис. 3). Одной из задач в проектировании такой линии является выбор оптимального

места расположения усилителей *ROPA*. Для избежания большого количества подводных муфт, усилители на обоих направлений стараются разместить в одной точке. Как правило, под такие ВОЛС не используются стандартные строительные длины кабеля, а кабель сразу изготавливается отрезками необходимой длины. Используется волокно стандарта *G.652* или *G.654D*, специально разработанное для протяженных подводных линий связи.

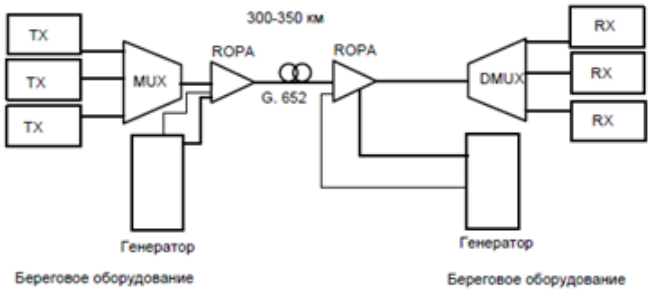


Рис. 3. Однопролетные линии с *ROPA*

Преимуществом вышеперечисленных линий связи, в отличии от рассматриваемых далее является отсутствие необходимости в электропитании подводных усилителей, что позволяет существенно снизить стоимость проекта.

4 Длинные линии связи до 800 км.

Линии связи длиннее 350 км строятся многопролетными ввиду того, что задача ввода необходимой мощности для усиления столь протяженной линии связи сильно усложняется из-за возрастания нелинейных эффектов, а использование большого количества дополнительных волокон накачки усложняет эксплуатацию, да и мощность самой накачки затухает во время доставки до места усиления. Многопролетные линии требуют установки *EDFA* усилителей и подведения к ним электропитания в подводных муфтах (Рис.4). Электропитание усилителей обеспечивается постоянным током через систему удаленного электропитания (СУЭП), которая состоит из блоков питания, токопроводящего элемента кабеля и устройства съема мощности на *EDFA*. Токопроводящий элемент в кабеле выполняется в виде сварной медной трубки, обернутой вокруг модулей с волокном. Также он служит дополнительной защитой волокон. Сами волокна в кабеле используются стандартов *G.652* или *G.654D*. Блоки питания, мощностью до нескольких киловатт, располагаются на концах подводной линии и резервируют друг друга. Как правило, такие линии включают в себя до 10 пролетов, такое ограничение накладывает неравномерное затухание на различных длинах волн, ввиду невозможности формирования абсолютно прямоугольной формы спектра на *GFF* фильтрах в составе *EDFA* усилителей. Сами пролеты выполняются длиной по 70-80 км из двух строительных длин кабеля, что обуславливается оптимальным значением *OSNR* для последующего усиления сигнала на каскаде из *EDFA*.

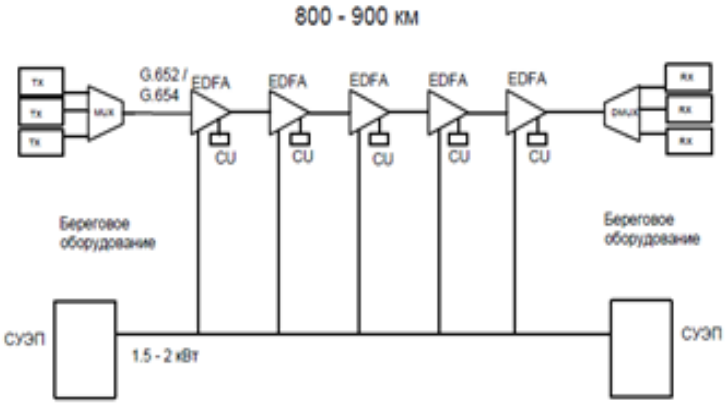


Рис. 4. Длинные линии связи до 800 км

Все усилители имеют модуль управления и контроля параметров, подключенный в служебный канал, который передается на отдельной длине волны по основному волокну и выводится через *OADM* на каждой муфте с *EDFA*. Ввиду возможности удаленного управления мощностями усилителей, есть возможность поочередно вводить в эксплуатацию каналы, благодаря этому система получила название “*Step by step*”.

5 Трансокеанические линии связи.

Самые длинные из существующих линий строятся по схожему принципу с предыдущими, но для сглаживания неравномерности формы спектра через каждые 8-10 пролетов устанавливаются поканальные переменные аттенюаторы (эквалайзеры), позволяющие откорректировать форму спектра и передать сигнал на значительно большее расстояние. Помимо этого, линии имеют ряд конструктивных отличий (Рис.5). Используются волокна стандарта *G.654D* с затуханиями 0,2 дБ/км. Повышаются мощности СУЭП до 12-16 киловатт. Помимо этого, в начале линии устанавливаются специальные мультиплексоры, которые могут вводить в частотную сетку либо рабочий информационный канал, либо постоянное излучение от широкополосного генератора эквивалентной мощности, которое включается на всех незадействованных каналах. Благодаря этому усилители изначально работают сразу с максимальным количеством каналов. Все оборудование линейного тракта настраивается единожды. При необходимости добавить информационный канал, происходит переключение с выхода генератора на выход транспондера. Данная технология называется “*Flex Less*”. Для контроля состояния линии, кроме модулей мониторинга *EDFA* используется контроль самого волокна когерентным рефлектометром. Рефлектометр, обозначенный как КР, подключается в линию через циркулятор. Также, на каждом усилительном пункте для зондирующего импульса предусматривается обход *EDFA*, состоящий из циркуляторов до и после *EDFA*.

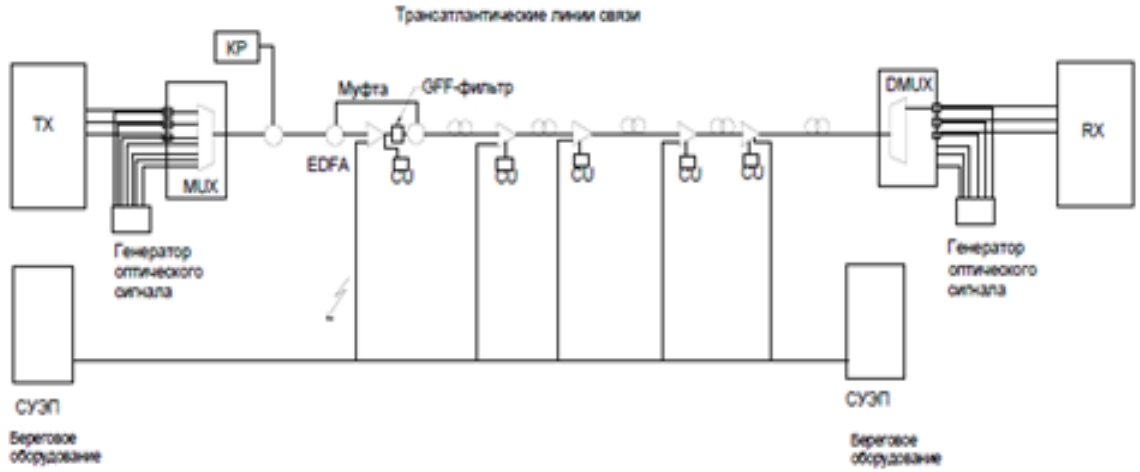


Рис. 5. Трансокеанические линии связи

Для увеличения надежности подводных усилительных пунктов, ввиду сложности их обслуживания, в конструкцию *EDFA* включаются несколько лазеров накачки. При выходе из строя одного лазера, на усилитель подается мощность от другого. Количество каналов в такой системе может достигать 100.

Заключение.

В заключении хотелось бы отметить, что подводные линии связи играют ключевую роль в телекоммуникациях современного мира, обеспечивая надежное и эффективное общение между странами и континентами. В зависимости от расстояния на которое нужно построить систему связи выбирается подходящее оборудование (тип усилителей, мощность СУЭП, длина волны накачки, оптимальное волокно и тд.), оптимальная структурная схема и схема прокладки кабеля. В зависимости от этих параметров будет определяться и цена проекта.

Список используемых источников:

1. Chesnoy J. Undersea Fiber Communication Systems. Second Edition: ELSEVIER, 2015. 679 с

2. Гайнов В. В., Конышев В. А., Леонов А. В., Лукиных С. Н., Наний О. Е., Скворцов П. И.,. Трещиков В. Н, Шихалиев И. И., Убайдуллаев Р. Р. Однопролетные оптические линии связи большой протяженности // Прикладная фотоника. Т. 2. N1. 18 с.

3. Гайнов В., Слепцов М., Однопролетные волс большой протяженности: как снизить стоимость транспортных сетей // Техносфера. Первая миля. 2015. N 2, , 80 с.

Bobevel Y., Dubovikov L.,Yklutov D.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Classification of underwater communication lines.

In the modern world, where telecommunications have become an integral part of our daily life, underwater communication lines play a crucial role in providing communication between continents and islands in the most remote corners of the planet. This engineering solution has

become an indispensable element of the global communications infrastructure, providing data, sound and video transmission over vast distances underwater. In this article we will take a closer look at the main types of underwater communication lines, their features, functional elements and applications.

Key words: Underwater lines, ROPA, EDFA, DWDM, Flex Less.

УДК 621.391.63
ГРНТИ 49.29.01

ВЛИЯНИЕ ДИЗАЙНА СЕТИ НА ЕЕ СТОИМОСТЬ

З. Э. Бутиков, Н. Т. Каадзе, Д. С. Славуцкий
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья рассматривает влияние дизайна сети на ее стоимость при проектировании оптических сетей. Обращается внимание на важность правильного дизайна сети, чтобы избежать непредвиденных затрат в будущем, а также подчеркивается важность учета перспективного развития сети. В статье указывается на необходимость балансировки между требованиями к сети и стоимостью дизайна. Также отмечается значение оптимизации оборудования оптического тракта для снижения стоимости.

дизайн сети, стоимость, оптическая сеть, проектирование, развитие сети, масштабирование, оборудование, оптимизация

В задании на проектирование и строительство необходимо прорабатывать множество деталей, которые существенно влияют на получаемый результат. Если образ будущей ВОЛС – это лишь представления Заказчика, не воплощенные в документ, то при ограниченности бюджетов и очевидном желании исполнителя получить больше прибыли с проекта, т.е. попросту сэкономить, практически неизбежным итогом будет ВОЛС, весьма далекая от ожиданий. При этом все дальнейшие доработки выливаются весьма в круглую сумму, опять-таки, увеличивая эксплуатационные расходы будущих периодов.

Топология сетей разнообразна, рассмотреть все в рамках данной статьи невозможно. В рамках данной работы рассмотрим варианты дизайна линейных DWDM участков, на примере которых мы можем продемонстрировать основные принципы.

Определим ключевые параметры сети:

- Количество каналов
- Пропускная способность
- Протяженность каналов

Очень важным является параметр перспективного развития сети. При проектировании сети стоимость оптического тракта линейной части несущественно зависит от количества каналов. В развитой сети стоимость каналообразующих блоков значительно превышает стоимость линейного тракта. Следовательно, необходимо стремиться к снижению стоимости оборудования оптического тракта:

- Использование каналообразующих блоков с более высокими линейными скоростями (для повышения эффективности использования спектрального ресурса волокна)

•Оптимизация конфигурирования оборудования оптического тракта для сокращения количества регенераций с OEO (optic-electric-optic)

•Оптимизация расстояния между усилителями 90-95 километров для достижения предпочтительного соотношения сигнал/шум

При соблюдении данных условий возможна организация 80-и каналов 100G на расстояние более 3500 километров без регенерации. Например, в апреле 2015 года компания "Т8" запустила на собственном DWDM-оборудовании "Волга" 100G-канал Москва – Новосибирск без регенерации сигнала. Каналы 100G переданы двумя путями: через Казань и через Екатеринбург, с резервированием 1+1. Длина двух плеч составляет, соответственно, 4250 и 3400 км[1].

При невозможности соблюдения условий расстояние между усилителями можно увеличить до 180-250 километров. Уменьшается общая длина безрегенерационного участка.

Стоит заметить, что стоимость постройки новой ЛЭП в 100 раз превышает стоимость оптической линии, поэтому наиболее лучшим вариантом будет использовать уже существующую инфраструктуру, например прокладывать линию вдоль путей РЖД.

Для организации регенерации предпочтительнее использовать транспондеры с функцией регенерации – тогда транспондер имеет один клиентский порт и несколько линейных[2]. Как правило это транспондеры имеющие функцию резервирования, это позволит сократить расходы примерно в 2 раза, на рис. 1, указаны два вида используемых транспондеров.

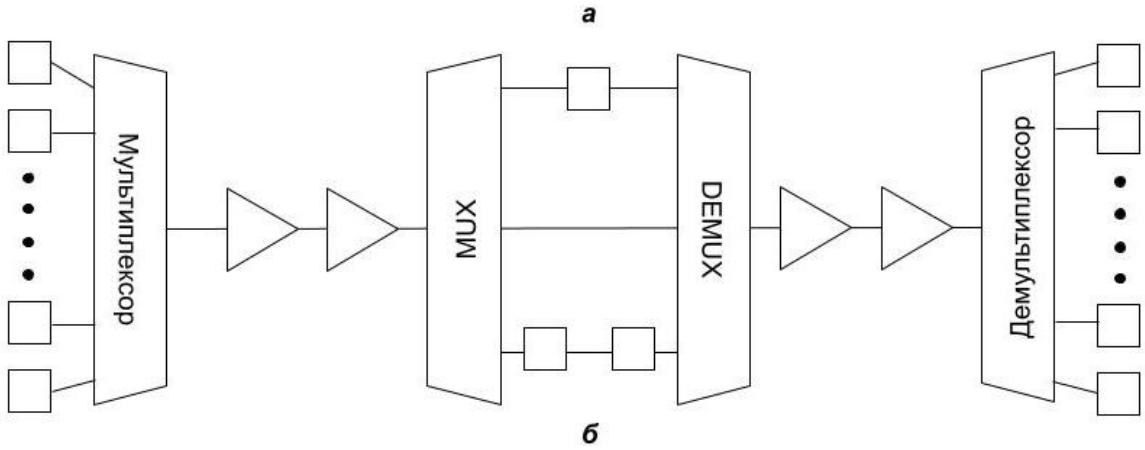


Рис. 1. Схема с двумя видами используемых транспондеров

Необходимо стремиться к повышению отказоустойчивости сети для снижения будущих затрат на устранение аварий и обслуживание. Аварийные ситуации в линейной части сети возникают при повреждении линии (обрыв волокна, выход из строя оборудования: транспондера, оптического усилителя или других компонентов). Очевидным решение этой проблемы является увеличение количества доступных физических трактов передачи, на которые будет осуществляться переключение при возникновении неисправности. Технически это достигается наращиванием числа световодов свыше

минимального значения. Данный прием получил название резервирования[3]. Передаваемый трафик разделяется на две независимые линии, например, по ЛЭП и по кабельной канализации.

Это не единственный случай оптимизации стоимости линий связи, в качестве примера (рис. 2.), при оптимизации дизайна необходимо правильно определить точку концентрацию трафика.

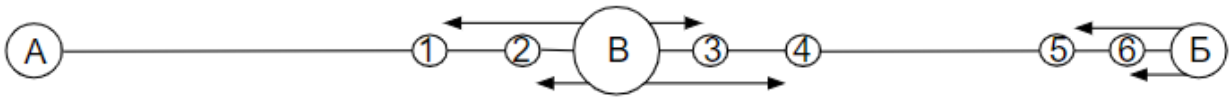


Рис. 2. Схема концентрации трафика

На изображении рис. 3 для организации оптической линии связи между населенными пунктами «А» и «Б», возникает задача отвода части оптического излучения из основного тракта передачи. Вместо покупки дорогостоящего каналообразующего оборудования эту задачу лучше решить с помощью пассивных оптических мультиплексоров. В поселки «В», «Г», «Д», выводятся отдельные каналы со своими длинами волн.

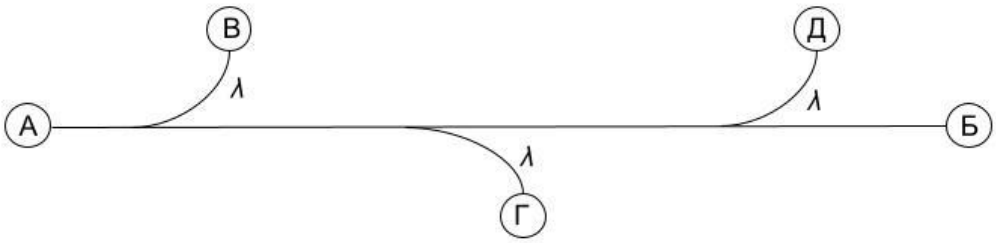


Рис. 3. Схема с выводом каналов

Понятно, что любую сеть нужно проектировать с учетом ее развития. Если при первоначальном проектировании не учесть дальнейших планов на потенциальное развитие сети, ее расширение может стать очень затратным. При этом нельзя допустить переоценки перспективы расширения сети (приводит к необоснованным капитальным потерям).

При правильной оценке необходимой пропускной способности участка сети порой можно неожиданно сделать вывод в отсутствии необходимости организации DWDM, достаточно просто организовать канал с высокой пропускной способностью, например на рис. 4, низкоскоростные каналы были агрегированы в один высокоскоростной канал.

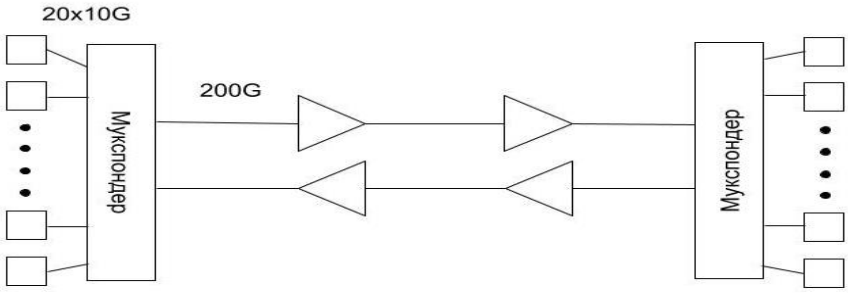


Рис. 4. Пример объединения каналов

Дизайн сети волоконно-оптической линии связи (ВОЛС) оказывает значительное влияние на ее стоимость. При ограниченности бюджетов и стремлении исполнителя проекта сэкономить, итоговая ВОЛС может сильно отличаться от изначальных представлений заказчика. Это может привести к значительным дополнительным затратам на доработку, что увеличивает эксплуатационные расходы в будущем. При проектировании ВОЛС необходимо учитывать множество параметров, таких как количество каналов, пропускная способность, протяженность каналов, стоимость реализации и перспективное развитие сети, важно найти баланс между этими параметрами, чтобы снизить стоимость оптического тракта и повысить пропускную способность. Учет этих факторов на этапе проектирования поможет снизить капитальные затраты при строительстве сети, дальнейшие эксплуатационные расходы и обеспечить долгосрочную эффективность сети.

Список используемых источников:

1. Леонов А., Слепцов М., Трещиков В.. Развитие скоростных DWDM-систем по нескольким поднесущим // Первая миля. 2016. С. 48.

2. Богданова Е. Г., Лукиных С. Н., Сачалин Е. А., Наний О. Е. Каналообразующее оборудование в системах DWDM. М. : Изд. «Т8», 2023. С. 30.

3. Горбашова М. А. Резервирование в системах DWDM. М. : Изд. «Т8», 2023. С. 4.

Butikov Z. E., Kaadze N. T., Slavutskiy D. S.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

The impact of network design on its cost.

This article examines the impact of network design on cost when designing optical networks. Emphasizes the importance of proper network design to avoid unexpected costs in the future, and also emphasizes the importance of considering the future development of the network. The article points out the need to balance between network requirements and design costs. The importance of optimizing optical path equipment to reduce cost is also noted.

Key words: network design, cost, optical network, design, network development, scaling, equipment, optimization.

УДК 621.372.832.43
ГРНТИ 47.45.31

МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ ИНТЕГРАЛЬНО-ОПТИЧЕСКОГО НАПРАВЛЕНИЯ ОТВЕТВИТЕЛЯ

М. С. Былина, В. А. Гоменица
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Для правильной работы волоконно-оптической системы связи необходимо отслеживать уровень мощности, а также управлять им, не внося потерь в линии передачи и нагрузку. Перечисленные вопросы решаются путем использования направленных ответвителей в линии передачи. Они позволяют осуществлять тщательное наблюдение за потоком оптической энергии в линии, уменьшая уровень мощности на известную фиксированную величину. В процессе выборки направленные ответвители вносят минимальные искажения в сигнал основной линии.

comsol Multiphysics, направленный ответвитель, волновод, туннелирование

Направленный ответвитель является измерительным устройством, установленным в линию передачи между нагрузкой и РЧ-источником, в качестве которого выступает генератор сигнала или передатчик. Ответвитель позволяет измерять энергию, передаваемую от источника к нагрузке (прямая передача), и отраженную мощность, поступающую от нагрузки в источник. Зная обе составляющие, можно рассчитать общую мощность, обратные потери, коэффициент стоячей волны нагрузки. У направленных ответвителей – четыре порта. Источник, как правило, подключается ко входу ответвителя, нагрузка – к его выходу или порту передачи. Сигнал на связанном выходе представляет собой ослабленный прямой сигнал.

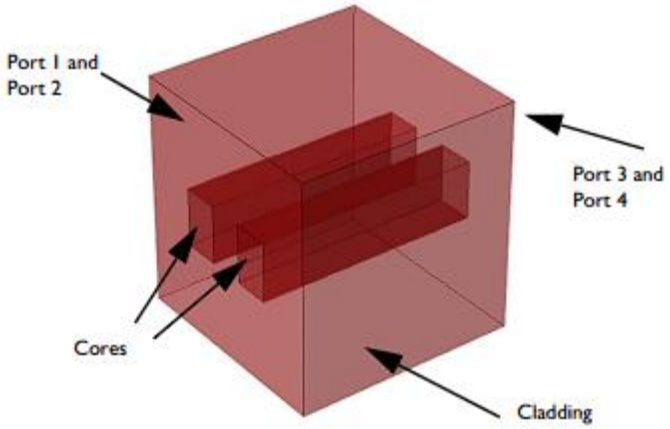


Рис. 1. Схематический чертеж волноводной структуры. Конструкция состоит из двух волноводных сердечников и окружающей оболочки. Порты 1 и 2 используются для возбуждения волноводов, а порты 3 и 4 поглощают волны

Поскольку ответвители являются симметричными устройствами, их можно подключать в обратном направлении. Выходы ответвителя обеспечивают оптический сигнал. Комбинацию направленного ответвителя и детектора называют рефлектометром.[2]

Свет, распространяющийся по диэлектрическому волноводу, имеет большую часть мощности, сосредоточенной в центральной сердцевине волновода[4]. Вне сердцевины волновода, в оболочке, электрическое поле экспоненциально убывает с увеличением расстояния от сердцевины. Однако, если вы поместите другой сердечник волновода близко к первому волноводу (см. рис. 1), этот второй волновод изменит режим работы первого волновода (и наоборот). Таким образом, вместо наличия двух мод с одинаковым эффективным показателем, одна локализована в первом волноводе, а вторая - во втором волноводе, режимы и их соответствующие эффективные индексы разделяются, и вы получаете симметричный супермод(см. рис. 2), с эффективным индексом, который немного больше эффективного индекса невозмущенного волноводного режима, и антисимметричный супермод (см. рис. 3)., с эффективным показателем, который немного ниже эффективного показателя невозмущенного волноводного режима.

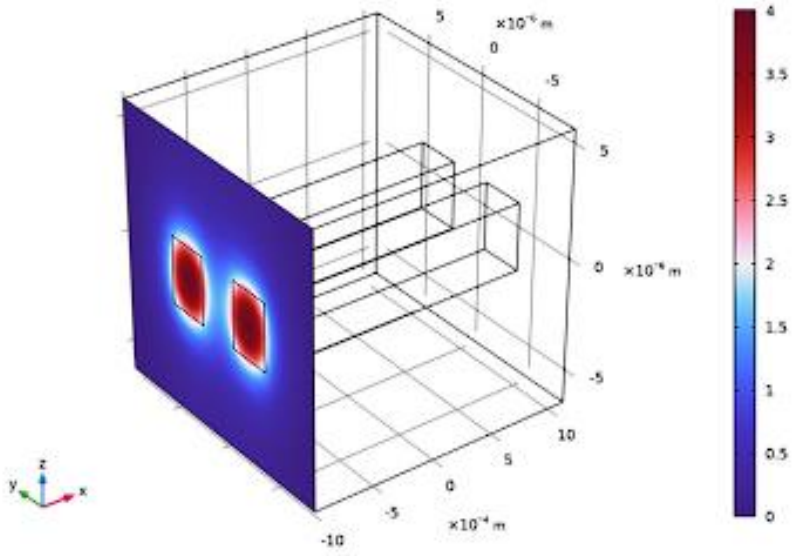


Рис. 2. Симметричный режим для z-поляризации

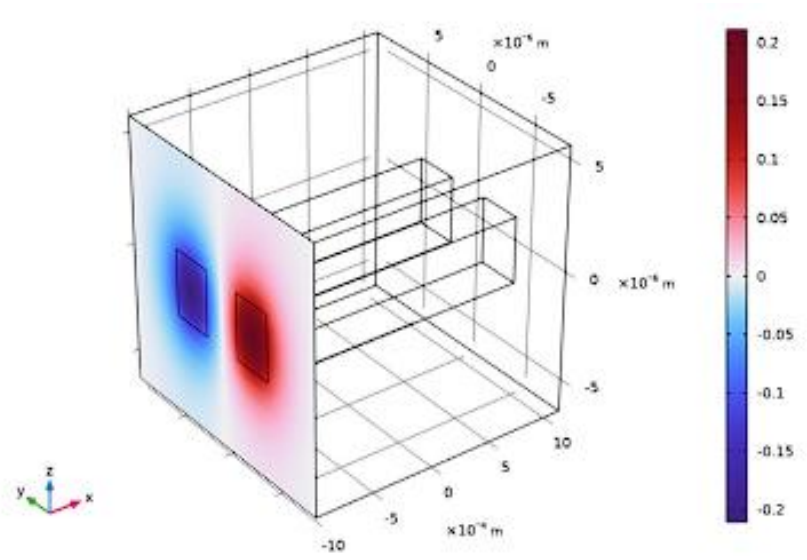


Рис. 3 Антисимметричный режим для z-поляризации

Поскольку супермоды являются решением волнового уравнения, если вы возбуждаете одну из них, она беспрепятственно распространяется по волноводу. Однако, если вы возбуждаете как симметричный, так и антисимметричный режим, которые имеют разные константы распространения, между этими двумя волнами возникает биение (Рис. 4).

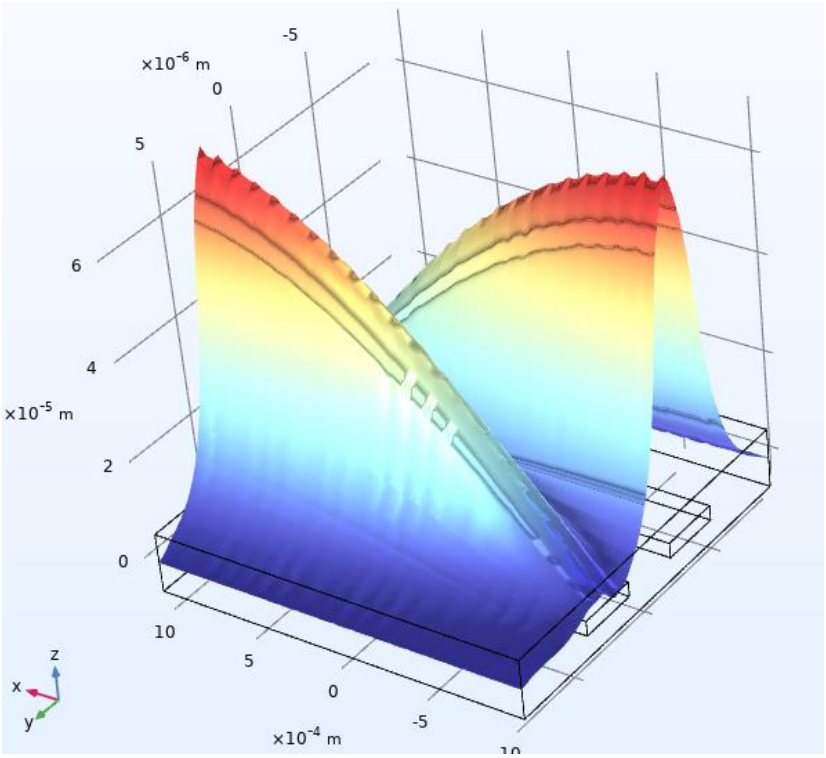


Рис. 4. Возбуждение симметричного и антисимметричного режимов

Таким образом, вы видите, что мощность колеблется взад и вперед между двумя волноводами, поскольку волны распространяются по волноводной структуре. Вы можете отрегулировать длину волноводной структуры, чтобы получить соединение от одного волновод к другому

волноводу. Регулируя разность фаз между полями двух супермод, вы можете решить, какой волновод возбуждается изначально.

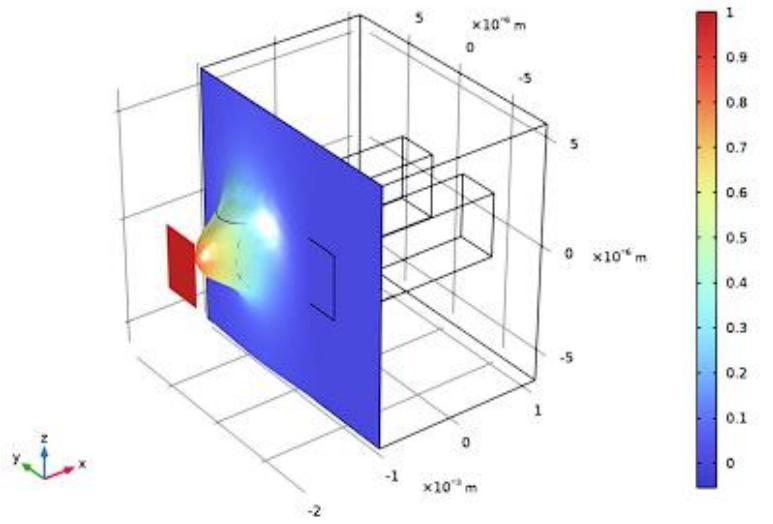


Рис. 5. Красный квадрат с амплитудой 1 В/м представляет целевую функцию. Показано, что общее входное поле локализовано в левом волноводе, как и ожидалось, с амплитудой, приближающейся к целевой амплитуде.

На рисунке 5 показано, что два режима накладываются друг на друга, чтобы приблизить целевое поле.

В результате можно сказать, что направленный ответвитель является полезным инструментом для измерений. Он позволяет разделить прямую и отраженную мощность. Ответвители имеют малый размер и совместимы с беспроводными устройствами.

Список используемых источников:

1. Полосковые СВЧ-делители/направленные ответвители [Электронный ресурс]. URL: https://habr.com/ru/articles/596167/ (дата обращения: 28.10.2023).

2. Электронные компоненты. [Электронный ресурс]. М. : ИД Электроника . 2020 . N 2 . С. 76-79 URL: https://rucont.ru/efd/694591 (дата обращения: 28.10.2023)

3. Снайдер А. Лав. Дж. Теория оптических волноводов. М. : Радио и связь 1987 г. 656 с.

4. Гончаренко В. А. Карпенко И. А. Гончаренко. Минск : Белорус. наука, 2009. 296 с. — ISBN 978-985-08-1024-3.

Bylina M., Gomenitsa V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

For the fiber-optic communication system to work properly, it is necessary to monitor the power level, as well as manage it without introducing losses into the transmission lines and load. These issues are solved by using directional couplers in the transmission line. They allow careful monitoring of the optical energy flow in the line, reducing the power level by a known fixed amount. During the sampling process, directional couplers introduce minimal distortion into the signal of the main line.

Key words: Comsol Multiphysics, directional coupler, waveguide, tunnelling.

УДК 621.375.82
ГРНТИ 49.46.33

ИССЛЕДОВАНИЕ ОПТИЧЕСКОГО УСИЛИТЕЛЯ EDFA

Я. В. Воробьев, Е. А. Панкова, В. К. Маринова
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается эрбиевый усилитель EDFA для DWDM-системы «Волга», измеряются параметры EDFA — зависимость коэффициента усиления EDFA от входной мощности, зависимость OSNR канала на выходе усилителя от мощности канала на входе в усилитель.

Усилитель EDFA, коэффициент усиления, мощность.

Существенное значение в проектировании волоконно-оптических систем связи занимает оптический усилитель, легированный ионами эрбия (EDFA), так как он позволяет усиливать мощность сигнала без оптоэлектронного преобразования.

EDFA – оптический усилитель, активной средой которого является EDF(Erbium Doped Fiber), волокно, легированное ионами эрбия. Структурная схема типового EDFA представлена на рис. 1.

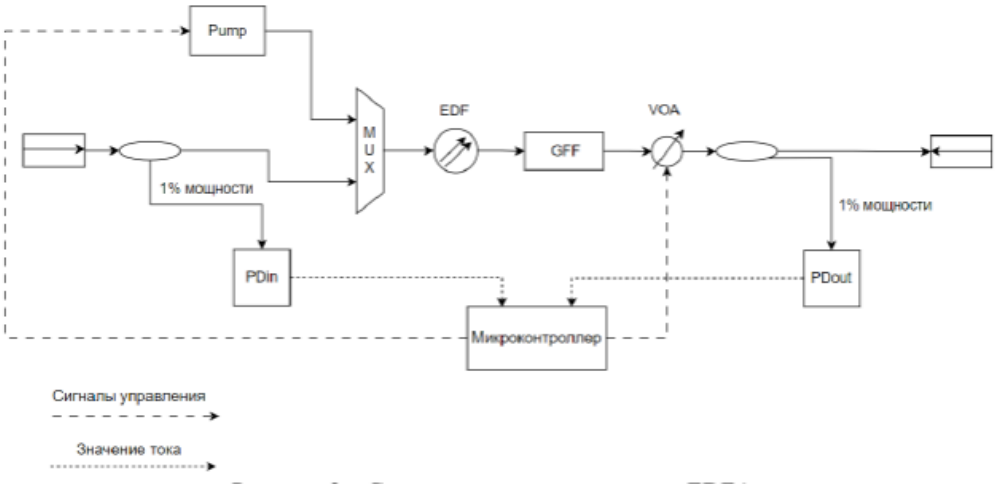


Рис. 1. Структурная схема типового EDFA

Она включает, кроме EDF, источник накачки (Pump), работающий на длине 980 или 1480 нм, MUX, объединяющий излучения усиливаемого сигнала и накачки в EDF, GFF, сглаживающий характеристику усиления EDF, VOA, используемый для изменения коэффициента усиления EDFA, а также изоляторы, фотодиоды и микроконтроллеры.

Работа EDFA основана на явлении вынужденного излучения фотонов ионами эрбия, возбужденными в результате поглощения фотонов накачки. При поглощении фотонов накачки 980 нм ионы Er3+ переходят из основного состояния 4I15/2 на короткоживущий уровень 4I11/2, с которого релаксирует

на метастабильный уровень 4I13/2. Термин «метастабильный» означает, что время жизни частиц в этом состоянии относительно велико (10 мс). Поэтому даже при умеренном уровне мощности накачки можно перевести почти все ионы эрбия в возбужденное состояние.

В традиционных волоконно-оптических системах используют регенераторы, повышающие качество передаваемого сигнала. Если длина между удаленными узлами начинает превосходить по условиям затухания сигнала максимальную допустимую длину пролета между соседними узлами, в промежуточных точках устанавливаются дополнительные регенераторы. С помощью их принимается слабый сигнал, они его усиливают в процессе оптоэлектронного преобразования, восстанавливают скважность, фронты и временные характеристики следования импульсов, и, после преобразования в оптическую форму, передают дальше правильный усиленный сигнал, в том же виде, в каком он был на выходе предыдущего регенератора. Хотя такие системы регенерации работают хорошо, они являются весьма дорогостоящими и, будучи установленными, не позволяют наращивать пропускную способность линии.

На основе EDFA потери мощности в линии преодолеваются путем оптического усиления. Такое "прозрачное" усиление не привязано к битовой скорости сигнала, в отличие от регенераторов, что позволяет передавать информацию на более высоких скоростях и наращивать пропускную способность, пока не вступят в силу другие ограничивающие факторы, такие как хроматическая дисперсия, поляризационная модовая дисперсия, нелинейные эффекты или, к слову о высокоскоростных сигналах, более высокие требования к значению отношения сигнала к шуму для спектральных каналов, работающих на больших скоростях. Также усилители EDFA способны усиливать многоканальный WDM сигнал, но с добавлением усиленного спонтанного излучения, которое в свою очередь является негативным явлением, шумом [1].

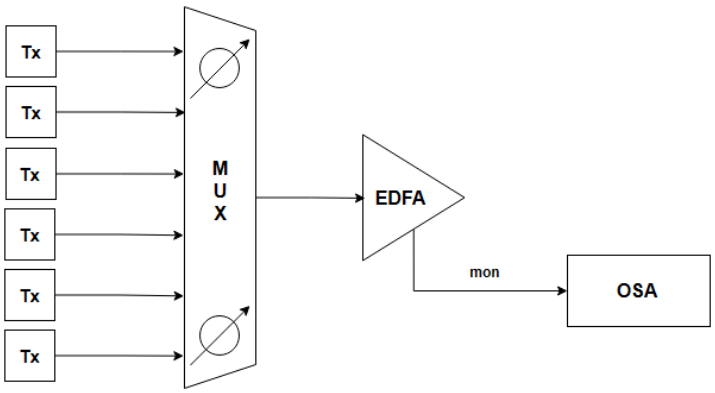


Рис. 2. Схема исследования EDFA

EDF характеризуется спектрами усиления/поглощения. Коэффициент усиления EDF определяется инверсией, которая, в свою очередь, зависит от мощности входного сигнала и мощности накачки.

Схема прямого управления используется в «одноканальных» EDFA – усилителях, предназначенных для усиления сигнала на одной длине волны (например, для КТВ). Для регулировки КУ EDFA с сохранением плоского спектра применяют VOA. Усилитель, состоящий из Fixed Gain-части и VOA называют VGA. Он может работать в режиме Pout с сохранением заданной формы спектра КУ.

Главной характеристикой EDFA является коэффициент усиления. Для этого был проведён эксперимент, целью которого было выявление зависимости коэффициента усиления от входной мощности. В ходе исследования на линейный порт усилителя подавались 6 спектральных каналов, изменялся уровень входной мощности при разных значениях токов диода накачки.

Влияние входной мощности в режиме стабилизации токов диодов накачки объясняется изменением спектров усиления/поглощения. С увеличением входной мощности при выбранных токах 80, 200 мА, наблюдается уменьшение коэффициента усиления, что показано рис. 3, 4.

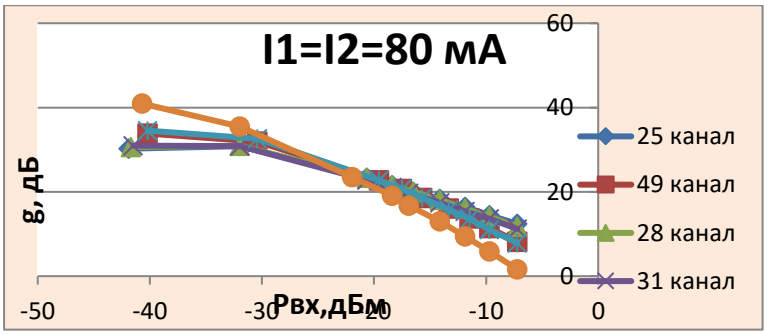


Рис. 3. График зависимости коэффициента усиления от входной мощности, при токе диодов I1=I2=80.

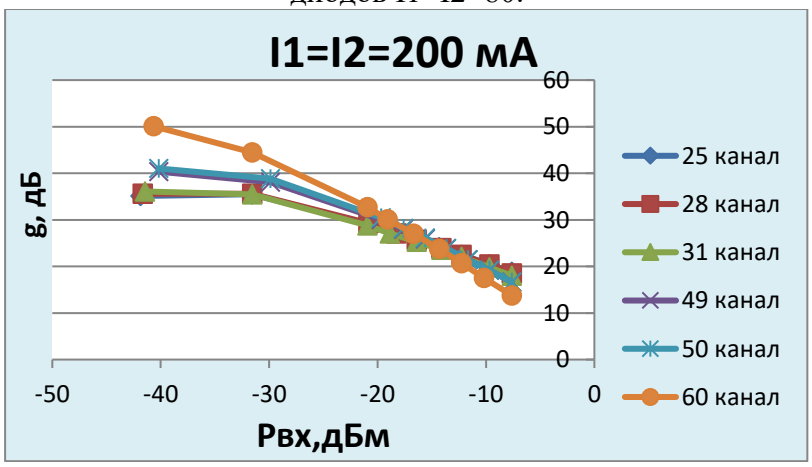


Рис. 4. График зависимости коэффициента усиления от входной мощности, при токе диодов I1=I2=200

На входной линейный порт исследуемого усилителя, подавались 6 спектральных каналов с одинаковым уровнем входной мощности. Так как усилитель работал в режиме стабилизации токов диода накачки – переменный аттенюатор и GFF-фильтр, призванные выравнивать

спектральную характеристику усиливаемого сигнала, были выключены. В следствии этого усиливаемое спонтанное излучение, генерируемое в активной среде EDFA, влияет на коэффициент усиления каналов в длинноволновой и коротковолновой части спектра, что видно на рисунке 3, 4.

В силу особенности работы оптического усилителя и добавление к полезному сигналу усиленного спонтанного излучения (шума), не менее важной характеристикой оптического усилителя является шум-фактор. Для подробного расчета данной величины предлагается построить график зависимости оптического отношения сигнала к шуму от входной мощности.

Качество оптического сигнала характеризуют величиной, которую принято называть оптическим отношением сигнал-шум (OSNR). Задачей исследования было выявление зависимости OSNR от мощности каналов на входе усилителя, когда другими шумами можно пренебречь, рисунок 5.

Для проведения исследования собирался макет, где единственным источником шума был сам EDFA. Режим стабилизации усилителя – Gain, поэтому в данной работе под источником шума понимается спектр усиленного спонтанного излучения, суммирующийся со спектральными каналами.

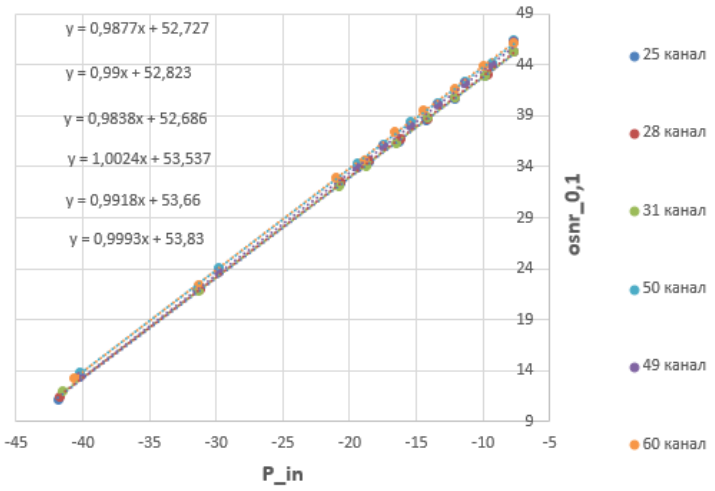


Рис. 5. График зависимости OSNR от входной мощности.

На рис. 5 представлена линейная зависимость osnr от входной мощности эрбиевого усилителя, предполагается, что:

$$osnr = 58 + p_{in} - nF \qquad (1)$$

По графику на рисунке 5 можно определить значение шум-фактора исследуемого усилителя. Сопоставляя уравнение прямой на плоскости и выражение 1 для определения osnr, получаем:

$$osnr = 58 + p_{in} - nF = p_{in} + 53{,}37 \qquad (2)$$

Из этого следует, что шум-фактор исследуемого усилителя примерно равен 5, что соответствует значению, заявленному производителем. Таким образом эксперимент проведён успешно.

В целом, усилители EDFA остаются важным и актуальным решением для современных телекоммуникационных систем. Это компонент позволяет усиливать мощность сигнала без оптоэлектронного преобразования, таким образом упреждая появление задержек, экономя итоговую стоимость проекта и давая возможность масштабировать сеть. Однако применение усилителя в линии должно сопровождаться учетом его влияния на качество сигнала. При неправильном применении EDFA, усиленное спонтанное излучение, формируемое в устройстве, отрицательно сказывается на значении отношения сигнала к шуму, а большая мощность на выходе устройства может спровоцировать нелинейное поведение среды и влияние последней на сигнал.

Список используемых источников:

1. Убайдуллаев Р. Р., Волоконно-оптические сети. М.: Эко-Трендз, 2001. С. 205-208.
2. Убайдуллаев Р. Р., Протяженные ВОЛС на основе EDFA // LIGHTWAVE russian edition. N 1 2003, С. 22-28
3. Трещиков В. Н., Листвин В. Н., «DWDM-системы 4» М. : Техносфера, 2023. С. 351-352.

Vorobyov Y., Pankova E., Marinova V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

EDFA optical amplifier research.

The article examines the erbium amplifier EDFA for the «Volga» DWDM system, measures the EDFA parameters - the dependence of the EDFA gain on the input power, the dependence of the OSNR of the channel at the amplifier output on the channel power at the input to the amplifier.

Key words: EDFA amplifier, gain, power.

УДК 535.015
ГРНТИ 29.31.27

ОЦЕНКА КАЧЕСТВА СВЯЗИ В ОПТИЧЕСКОМ ТРАКТЕ ВОСС ПО РЕЗУЛЬТАТАМ ИЗМЕРЕНИЯ ОТНОШЕНИЯ СИГНАЛА К ШУМУ

Ф.В.С. Делла-Корте, К.Э. Чесноков, Д.Н. Шенхорова

В статье приведена исследовательская работа, в которой представлена оценка качества связи в оптическом тракте ВОСС на основе измерения отношения сигнала к шуму.

OSNR, ВОСС, BER, шум, отношения сигнала к шуму

Волоконно-оптические системы связи (ВОСС) играют важную роль в современном мире, обеспечивая высокоскоростную передачу данных. Для обеспечения бесперебойной работы ВОСС необходимо контролировать качество связи в оптических системах.

Для оценки качества связи в электрическом тракте ВОСС используются:

- коэффициент битовых ошибок (bit error ratio, BER) представляющий собой отношение числа ошибочно принятых бит к общему числу принятых бит за некоторый промежуток времени;
- Q-фактор, представляющий собой отношение электрического сигнала к шуму на входе регенератора и однозначно связанный с величиной BER.

Для измерения BER используются специальные приборы – BER-тестеры. Q-фактор определяют по глаз-диаграмме, формируемой на экране быстродействующего осциллографа.

В ВОСП с использованием технологии плотного спектрального мультиплексирования (Dense Wavelength Division Multiplexing, DWDM) параметры BER и Q-фактор должны измеряться для каждого спектрального канала. Для этого перед измерениями многоканальный сигнал необходимо демультиплексировать на сигналы отдельных спектральных каналов.

Качество связи в оптическом тракте можно оценить, измеряя отношение оптического сигнала к шуму (Optical Signal to Noise Ratio, OSNR). OSNR представляет собой логарифмическое отношение пиковой мощности сигнала P_s к мощности шума P_n:

$$OSNR = 10 \cdot lg\left(\frac{P_S}{P_n}\right). \quad (1)$$

Величина OSNR коррелирована с BER и Q- фактором.

OSNR определяют, анализируя спектр оптического сигнала, регистрируемый оптическим спектроанализатором (Optical Spectrum Analyzer, OSA). Значения OSNR для всех спектральных каналов могут быть определены по спектрограмме многоканального сигнала без необходимости его демультиплексирования.

Основными источниками шумов в ВОСС являются:

1. Передающие устройства. Лазерные диоды создают некоторый уровень оптического шума при генерации излучения, обусловленный спонтанным излучением, флуктуациями тока накачки, колебаниями температуры и другими причинами.
2. Оптические усилители (ОУ). Шум ОУ представляет собой усиленное спонтанное излучение (Amplified Spontaneous Emission, ASE).
3. Приемные устройства. Фотодиоды с усилителями фототока при приеме излучения создают электрические дробовые и тепловые шумы. В ВОСС с ОУ возникают также электрические шумы биения между сигналом и ASE и между различными спектральными компонентами ASE.

Отметим, что OSNR не учитывает электрические шумы фотоприемного устройства (ФПУ), а также факторы, ухудшающие качество связи, но не изменяющие спектр сигнала – хроматическую и поляризационно-модовую дисперсию и временной джиттер.

В современных протяженных ВОСП основным источником оптических шумов является ASE, создаваемое ОУ. Для мощности ASE P_{ASE} справедливо выражение:

$$P_{ASE} = h \cdot \nu \cdot \Delta\nu \cdot F_n \cdot (G - 1), \quad (2)$$

где h = 6.63·10–34 Дж·с – постоянная Планка, Δν – полоса частот, в которой определяется мощность ASE, ν – частота, G – коэффициент усиления ОУ, F_n – шум-фактор ОУ.

Рассмотрим методику определения OSNR по спектрограмме. На рис. 1 представлена спектрограмма оптического многоканального сигнала DWDM в ВОСС с ОУ. Расположение спектральных каналов регламентируется рекомендацией Международного союза электросвязи G.694. Некоторые каналы могут отсутствовать, если они были выведены из многоканального сигнала с помощью оптических мультиплексоров ввода/вывода или используется сетка с неравномерным размещением каналов.

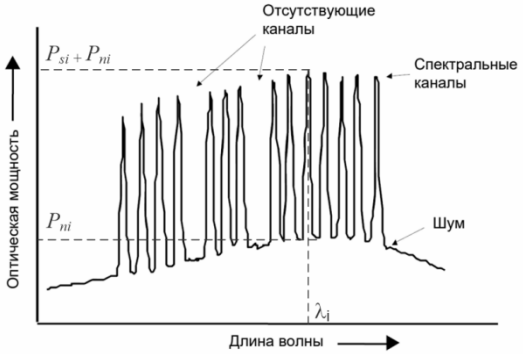


Рис. 1. Методика определения OSNR по спектрограмме

В соответствии с (1) для определения OSNR в *i*-том спектральном канале нужно отдельно измерить мощности сигнала P_{si} и шума P_{ni}. Из рис. 1 видно, что непосредственно измерить P_{si} нельзя, так как в полосе канала

присутствуют шумы и пиковая мощность сигнала суммируется с мощностью шума.

Таким образом, по спектрограмме может быть измерена величина $OSNR_{ism}$, для которой справедливо:

$$OSNR_{ism} = 10 \cdot lg\left(\frac{P_{Si}+P_{ni}}{P_{ni}}\right) = 10 \cdot lg\left(\frac{P_{Si}}{P_{ni}}+1\right). \quad (3)$$

Из (1) и (3) следует, что:

$$OSNR = 10 \cdot lg\left(10^{\frac{OSNR_{ism}}{10}}-1\right). \quad (4)$$

OSNR принято определять в полосе Δλ = 0.1 нм. Если установленное при регистрации спектрограммы разрешение OSA Δλosa ≠ Δλ, то для расчета «правильного» OSNR нужно использовать выражение:

$$OSNR = 10 \cdot lg\left(10^{\frac{OSNR_{ism}}{10}}-1\right) + 10 \cdot lg\left(\frac{\Delta\lambda_{osa}}{\Delta\lambda}\right). \quad (4)$$

В работе проведено экспериментальное исследование, в ходе которого определялось OSNR в ВОСС без использования и с использованием ОУ. Схемы исследования представлены на рис. 2.

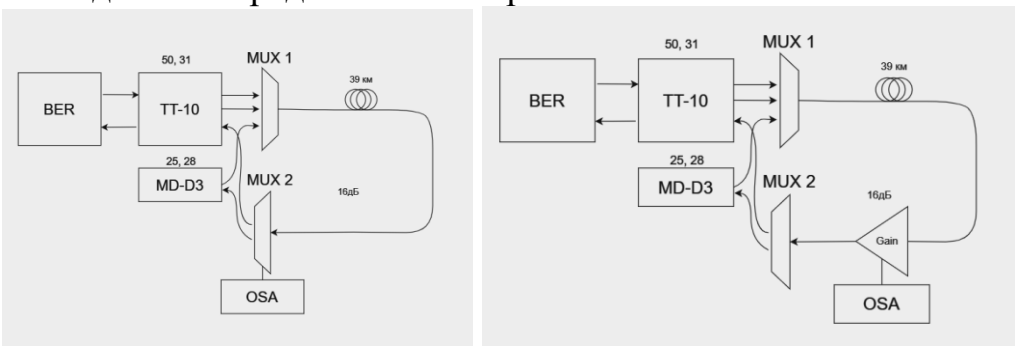


Рис. 2. Схемы исследуемых ВОСС: а – без ОУ, б – с ОУ

BER (Bit Error Rate) tester - устройство для измерения и оценки качества передачи данных. Используется, чтобы проверить, насколько точно данные передаются между двумя устройствами или системами.

TT - транспондер,устройство, которое выполняет функцию конвертации оптических сигналов с одной оптической длины волны на другую.

MD-D3 - устройство, которое собирает несколько оптических сигналов на разных длинах волн и объединяет их в один поток данных.

OSA - прибор, который используется для анализа оптического спектра.

Для эксперимента взяты два канала 31 и 50, данные которых передавались в мультиплексор, оттуда во второй мультиплексор (который в нашем эксперименте выполнял роль демультиплексора, поскольку нам необходимо было воспользоваться портом мониторинга, который имеется только на мультиплексоре. Информация же со второго мультиплексора передается на 25 канал. Собрана следующая схема (рис. 1)

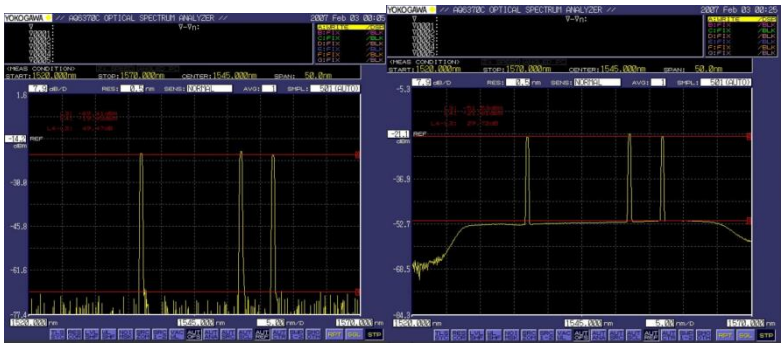


Рис. 3 Три спектральных канала (№25, 31, 50) на входе в линию и после EDFA

Результаты измерений представлены на следующих таблицах 1, 2 и 3.

ТАБЛИЦА 1 расчет OSNR на входе в систему

№ канала	*P* dBm	OSNR, дБ	OSNR
50	-19,64	49,67	56,66
31	-18,75	50,66	57,65
25	-19,93	49,47	56,46

ТАБЛИЦА 2 расчет OSNR на выходе со схемы без усилителя

№ канала	P_{in} , dBm	$OSNR_{ism}$, дБ	OSNR
50	-25,07	43,94	50,93
31	-24,47	44,64	51,63
25	-25,07	43,94	50,93

ТАБЛИЦА 3 расчет OSNR на выходе со схемы с усилителем

№ канала	P_{in} , dBm	$OSNR_{ism}$, дБ	OSNR
50	-22,2	30,61	37,59
31	-21,2	30,71	37,69
25	-21,81	29,72	36,71

Таким образом можно сделать вывод, что каждый из элементов собранной схемы вносит разной степени помехи, в свою очередь усилитель, являющийся необходимым элементом в больших системах вносит наибольшее число помех, нежели другие элементы.

Список используемых источников:

1. Былина М. С., Глаголев С. Ф. Методы и приборы для оптических измерений в инфокоммуникациях : учеб. пособие СПб. : СПбГУТ. С. 52-69.

2. Листвин В. Н. DWDM системы / В. Н. Листвин, В. Н. Трещиков. М. : Техносфера, 2017. 324 с.

Della-Corte F.V.S., Chesnokov K.E., Shenkhorova D.N.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

In the article, a research study is presented, which includes an assessment of the communication quality in the optical communication system (OCS) based on measuring the signal-to-noise ratio.

Key words: Signal-to-Noise Ratio (SNR), Optical Signal-to-Noise Ratio (OSNR), Bit Error Rate (BER), and noise.

УДК 004.72
ГРНТИ 49.33.29

ПЕРСПЕКТИВЫ МОДЕРНИЗАЦИИ ГОРОДСКИХ СИСТЕМ СВЯЗИ И ПЕРЕДАЧИ ДАННЫХ В УСЛОВИЯХ МЕГАПОЛИСА

М. А. Лоншаков, Б. К. Резников, Д. Д. Чемодуров, А. А. Шиян
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В России существует ряд государственных программ по модернизации городских систем связи, которые регулируются соответствующими правительственными указами и программами. Одна из таких программ – «Цифровая экономика России», которая была принята в 2018 году и предусматривает модернизацию городских систем связи и других инфраструктурных объектов. В рамках этой программы планируется расширение использования высокоскоростных сетей связи, включая 5G, в городах России. В данном исследовании будут рассмотрены аспекты модернизации городских систем связи и передачи данных в условиях мегаполиса, а также определены основные факторы, влияющие на эффективность таких систем.

городские сети связи, модернизация, передача данных, оптоволокно

1. 10G PON.

Сеть связи [1] является важным элементом инфраструктуры города, обеспечивающим передачу данных и информации между жителями, предприятиями и учреждениями. В связи с увеличением объемов передаваемых данных и постоянным развитием технологий, необходимо постоянно модернизировать городскую сеть связи.

Одним из наиболее эффективных способов модернизации городской сети связи является использование сети 10G PON (Passive Optical Network). Это технология передачи данных по оптическому кабелю, которая позволяет достичь скоростей передачи данных до 10 Гбит/с. [2]

Основным преимуществом сети 10G PON является ее высокая скорость передачи данных. Это позволяет жителям города быстро и удобно получать доступ к интернету, просматривать видео, играть в онлайн-игры и работать с большим объемом данных. Кроме того, сеть 10G PON обладает высокой надежностью и устойчивостью к внешним воздействиям, что обеспечивает бесперебойную работу городской сети связи.

Еще одним преимуществом сети 10G PON является ее экономичность. Использование оптического кабеля позволяет сократить затраты на обслуживание и ремонт городской сети связи, а также уменьшить энергопотребление.

Важно отметить, что модернизация городской сети связи с помощью сети 10G PON не только обеспечит жителям города быстрый и удобный доступ к интернету, но и способствует развитию экономики и инноваций в городе. Благодаря высокоскоростной сети связи, предприятия и учреждения смогут проводить быстрое и эффективное взаимодействие между собой, а также с клиентами и партнерами.

Использование сети 10G PON для модернизации городской сети связи является эффективным и перспективным решением, которое обеспечивает высокую скорость передачи данных, надежность и экономичность.

2. DWDM - Dense Wavelength Division Multiplexing.

DWDM — это технология передачи данных по оптическому кабелю, которая позволяет передавать несколько сигналов на разных длинах волн в одном оптическом кабеле. Использование DWDM для модернизации городской сети связи имеет множество преимуществ.[3]

Одним из основных преимуществ DWDM является возможность передачи большого объема данных на большие расстояния. Это позволяет городской сети связи обеспечивать высокоскоростной доступ к интернету, телевизионным и радиопрограммам, а также другим сервисам, которые требуют большой пропускной способности.

Другим важным преимуществом DWDM является его экономичность. Использование одного оптического кабеля для передачи нескольких сигналов позволяет сократить затраты на обслуживание и ремонт городской сети связи, а также уменьшить затраты на энергопотребление. Это делает DWDM более доступным и экономически выгодным для города.[4] Еще одним преимуществом DWDM является его высокая надежность и устойчивость к внешним воздействиям. Это обеспечивает бесперебойную работу городской сети связи, что очень важно для ее эффективной работы. DWDM также позволяет городской сети связи быть более гибкой и адаптивной к изменяющимся потребностям жителей города. Это позволяет быстро реагировать на изменения в спросе на услуги связи и предоставлять новые сервисы, которые могут быть полезны для жителей города.

Одним из основных примеров использования DWDM является городской транспорт. С помощью этой технологии можно обеспечить быстрый и надежный доступ к информации о расписании, задержках и других важных данных для пассажиров. Это позволит улучшить качество обслуживания и сделать городской транспорт более привлекательным для жителей.

3. AON - All Optical Network.

AON — это технология передачи данных по оптическому кабелю, которая использует активное оборудование для управления и перенаправления сигналов. Использование AON для модернизации городской сети связи имеет ряд преимуществ.[5]

Одним из основных преимуществ AON является возможность управления и контроля над передачей данных. Это позволяет городской сети связи обеспечивать более высокую степень безопасности и защиты данных, а также улучшить качество обслуживания.[6]

Гибкость сети в контексте оптической сети доступа (AON) относится к способности этой сети адаптироваться и реагировать на различные изменения и потребности. В данном контексте гибкость означает, что городская сеть связи, основанная на AON, может быстро и легко изменять

свою структуру и параметры в ответ на разнообразные факторы, такие как увеличение числа пользователей, расширение городской инфраструктуры, изменение трафика данных и даже внедрение новых технологий. Гибкость сети может выражаться в нескольких аспектах:

Масштабируемость: Городская сеть, построенная на основе AON, способна масштабироваться вертикально и горизонтально. Это означает, что она может увеличивать емкость и размеры, чтобы справиться с увеличивающимся объемом данных и новыми участниками.

Легкость конфигурации и переконфигурации: сеть должна быть спроектирована так, чтобы изменения в ее конфигурации могли быть внесены относительно быстро и без значительных трудозатрат. Это позволяет администраторам сети адаптировать ее к текущим потребностям.

Поддержка разнообразных сервисов: гибкая сеть должна быть способной предоставлять различные виды услуг, включая интернет, телефонию, видеоконференции и другие. Она должна быть готова поддерживать и внедрять новые сервисы с минимальными изменениями в инфраструктуре.

Сопротивление отказам: городская сеть должна быть способной реагировать на отказы и проблемы в сети, перераспределяя трафик и обеспечивая непрерывное функционирование важных сервисов.

Еще одним преимуществом AON является его экономичность. Использование активного оборудования позволяет сократить затраты на обслуживание и ремонт городской сети связи, а также уменьшить затраты на энергопотребление. Это делает AON более доступным и экономически выгодным для города.

В заключение, использование AON, DWDM, 10G-PON для модернизации городской сети связи является эффективным и перспективным решением, которое обеспечивает высокую степень безопасности и защиты данных, гибкость и масштабируемость, экономичность и возможность предоставления новых сервисов и услуг.

Список используемых источников:

1. Гольдштейн Б. С. Сети связи. СПб. : БХВ-Петербург, 2010.

2. Гаскевич Е. А. Сети абонентского доступа на базе технологии PON. М. : Мир телекома, 2012. 74 с.

3. Antil R., Pinki S. B., Beniwal S. An overview of DWDM technology & network // Int. J. Sci. Technol. Res. 2012. Т. 1. N 11. С. 43-46.

4. Валиев Р. И. и др. Система уплотнения каналов DWDM // Проблемы техники и технологии телекоммуникаций. Оптические технологии в телекоммуникациях. 2018. С. 199-201.

5. Былина М. С. Оптические волокна для телекоммуникаций : учеб. пособие / М. С. Былина, С. Ф. Глаголев. СПб. : СПбГУТ, 2018. 96 с.

6. Скляров О. К. Волоконно-оптические сети и системы связи: учеб. пособие. СПб. : «Лань», 2010. 272 с.

Chemodurov D., Lonshakov M.., Reznikov B.., Shiyan A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Research of aspects of modernization of urban communication and data transmission systems in a megalopolis.
In Russia, there are a number of state programs for the modernization of urban communication systems, which are regulated by relevant government decrees and programs. One of such programs is the "Digital Economy of Russia", which was adopted in 2018 and provides for the modernization of urban communication systems and other infrastructure facilities. As part of this program, it is planned to expand the use of high-speed communication networks, including 5G, in Russian cities. This study will consider aspects of the modernization of urban communication and data transmission systems in a megalopolis, as well as identify the main factors affecting the effectiveness of such systems.

Key words: city communication networks, modernization, data transmission, optical fiber.

УДК 681.7
ГРНТИ 49.44.31

ИССЛЕДОВАНИЕ МУЛЬТИПЛЕКСОРА AWG ДЛЯ СИСТЕМЫ DWDM

В. Е. Пылаев, В. В. Самарин, М. Д. Чернов

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

В статье представлено описание конструкции и принципа работы оптического мультиплексора на основе фазированной решетки волноводов, применяемого в волоконно-оптических сетях, использующих спектральное уплотнение, а также приведены результаты экспериментального исследования вносимых потерь в каждом канале мультиплексора.

Интегральная оптика, волоконные световоды, DWDM-система, мультиплексор AWG

Современные транспортные сети связи строятся с использованием технологии плотного спектрального уплотнения (Dense Wavelength Division Multiplexing, DWDM), которая позволяет одновременно передавать по одному оптическому волокну (ОВ) несколько высокоскоростных информационных сигналов, сформированных на разных длинах волн (спектральных каналов). Сигнал каждого канала формируется своим передающим устройством, затем все сигналы объединяются в одно ОВ с помощью оптического мультиплексора.

Оптические мультиплексоры разделяются на пассивные неуправляемые и активные управляемые устройства. В данной работе исследуется пассивный терминальный интегрально-оптический мультиплексор на основе фазированной решетки волноводов (Arrayed-Waveguide Grating, AWG).

Конструкция мультиплексора AWG представлена на рис. 1. Мультиплексор состоит из входных (input waveguides) и выходных (output waveguides) планарных волноводов, двух пластин (slab) и фазированной решетки AWG (array waveguides). Фазированная решетка образуется группой из N планарных волноводов разной длины, причем длины любых двух соседних волноводов отличаются на одну и ту же величину ΔL.

Рассмотрим работу этого устройства в режиме демультиплексирования. Излучение сигнала DWDM, содержащего N_{ch} спектральных каналов с длинами волн $\lambda_1 \ldots \lambda_{Nch}$, выходит из одного из входных волноводов в первую пластину с показателем преломления, одинаковым во всех точках. Излучение в пластине образует расходящийся гауссов пучок, который засвечивает торцы всех волноводов AWG. Степень расходимости пучка и необходимая длина пластины зависят от апертуры входного волновода.

Каждый из волноводов AWG захватывает часть излучения, падающего на его торец, и канализирует его в сторону второй пластины. Поскольку все

волноводы AWG имеют разную длину, распространяющиеся в них излучения приобретают разные фазы. Во второй пластине будет происходить интерференция выходящих из волноводов AWG излучений, в результате которой излучения длин волн $\lambda_1 \ldots \lambda_{Nch}$ будут сфокусированы каждая в свой выходной волновод.

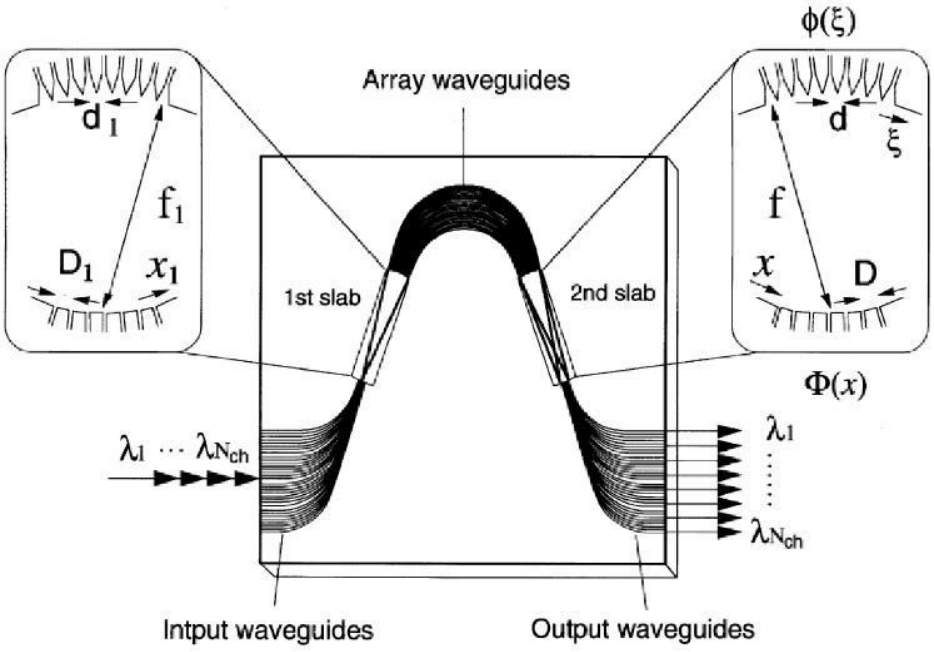


Рис. 34. Схема AWG мультиплексора

К основным оптическим параметрам мультиплексора относят вносимые потери a_{IL}, определяемые для каждого спектрального канала λ_i отдельно, а также затухание переходных помех a_{cross}, характеризующих взаимные влияния между спектральными каналами:

$$a_{IL}(\lambda_i) = 10 \cdot lg \frac{P_{in}}{P_{out}}, \qquad a_{cross}(\lambda_i, \lambda_j) = 10 \cdot lg \frac{P_{in}}{P_{cross}},$$

где P_{in} – мощность измерительного сигнала на длине волны λ_i, вводимая через i-тый вход мультиплексора, P_{out} – мощность измерительного сигнала, прошедшего на групповой выход мультиплексора, измеренная в полосе i-того канала, P_{cross} – мощность измерительного сигнала, прошедшего на групповой выход мультиплексора, измеренная в полосе j-того канала.

В работе было проведено экспериментальное исследование 40-канального мультиплексора AWG OM-40-AV-PM, входящего в состав оборудования «Волга» производства ООО «Т8»

Экспериментальные данные

Для проведения эксперимента по измерению потерь на каждом канале мультиплексора, была собрана схема, состоящая из эрбиевого усилителя (EDFA), мультиплексора (MUX) и анализатора спектра (OSA). Измерения проводились для широкополосного сигнала с усиленным спонтанным излучением (ASE) от усилителя EDFA. Именно эрбиевый усилитель является источником широкополосного сигнала в данной схеме. Режим работы EDFA:

ILD с током накачки равным 80 мА. На рисунке 2 изображена схема, с помощью которой проводились измерения.

Устройство исследовалось в режиме демультиплексирования, то есть выход усилителя подключался к групповому выходу с разрешением спектроанализатора λ_{res} = 0,5 нм.

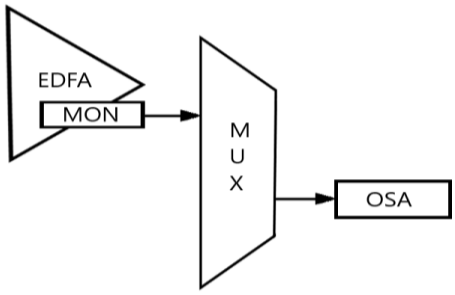


Рис. 35. Схема установки

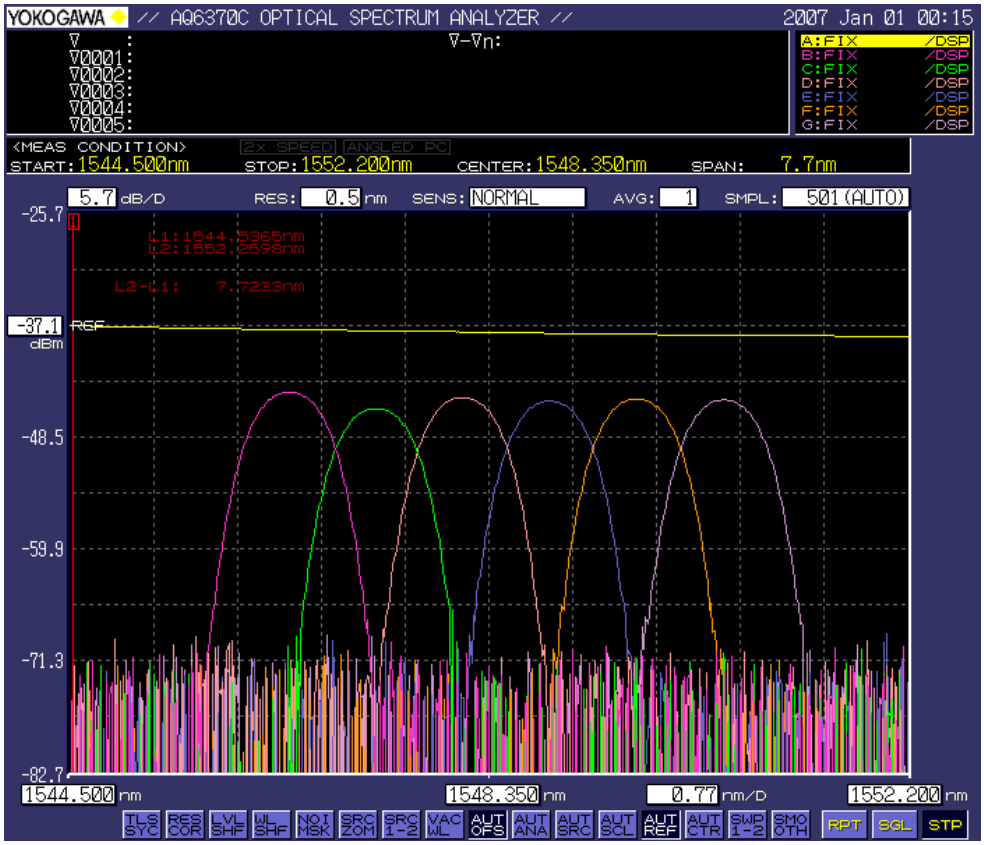


Рис. 36. Спектрограмма для 6 каналов (с 33 по 38)

Для каждого канала было проведено два измерения. Сначала по спектрограмме ASE, который использовался в качестве входного сигнала, был измерен уровень мощности входного излучения в полосе нужного спектрального канала (пересечение маркеров 2 и 3). Потом по спектрограмме этого канала определялся уровень прошедшей через устройство мощности (пересечение маркеров 2 и 4). Разность двух этих уровней дала вносимые потери в канале.

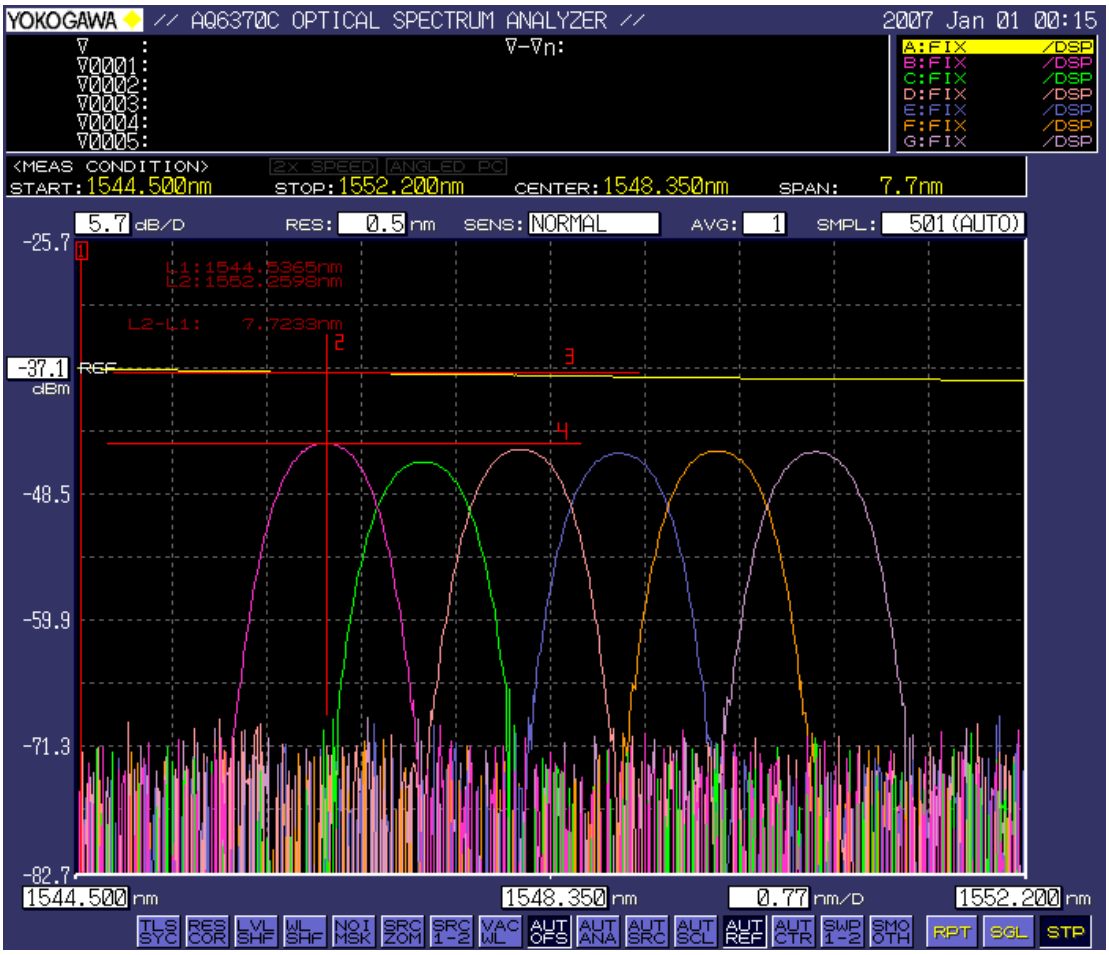


Рис. 37. Методика измерений

Таким образом, были произведены расчеты для сорока каналов демультиплексора. Результаты измерений представлены в таблицах 1.1-1.6

ТАБЛИЦА. Вносимые потери в каналах

№ канала	Длина волны, нм	Частота, ТГц	Потери, дБ	№ канала	Длина волны, нм	Частота, ТГц	Потери, дБ
Ch 21	1560,61	192,1	6,22	Ch 39	1546,12	193,9	6,52
Ch 22	1559,79	192,2	6,62	Ch 41	1544,53	194,1	6,22
Ch 23	1558,98	192,3	6,52	Ch 42	1543,93	194,2	6,22
Ch 24	1558,17	192,4	6,52	Ch 43	1542,94	194,3	6,71
Ch 25	1557,36	192,5	6,32	Ch 44	1542,14	194,4	6,32
Ch 26	1556,56	192,6	6,32	Ch 45	1541,35	194,5	6,22
Ch 29	1554,13	192,9	6,42	Ch 46	1540,56	194,6	6,22
Ch 30	1553,33	193	6,81	Ch 49	1538,19	194,9	6,62
Ch 31	1552,52	193,1	6,62	Ch 51	1536,61	195,1	6,71
Ch 32	1551,72	193,2	6,81	Ch 52	1535,82	195,2	6,42
Ch 33	1550,92	193,3	6,12	Ch 53	1535,04	195,3	6,42
Ch 34	1550,12	193,4	6,81	Ch 54	1534,25	195,4	6,52
Ch 35	1549,32	193,5	6,42	Ch 57	1531,90	195,7	6,32
Ch 36	1548,52	193,6	6,22	Ch 58	1531,12	195,8	6,42
Ch 37	1547,72	193,7	6,62	Ch 60	1529,55	196	6,22
Ch 38	1546,92	193,8	6,42				

Как видно из таблицы, вносимое демультиплексором затухание в разных каналах составляет от 6,12 дБ до 6,81 дБ. Среднее значение вносимого затухания составляет 6,45 дБ. По результатам измерений можно сказать, что вносимые демультиплексором потери соответствуют паспортным значениям.

На основе проведенных исследований предполагается подготовить новую лабораторную работу по изучению мультиплексора AWG и внедрить ее в учебный процесс кафедр ФиЛС и ВТС DWDM.

Список используемых источников:

1. Soldano L. B. and Pennings E. C., «Optical multi-mode interference devices based on self-imaging: Principles and applications». J. Light. Technol. 13, 615-627 (1995).

2. Katsunari Okamoto. «Fundamentals of Optical Waveguides», 2006.

3. Гончаров А. А., Светиков В. В., Свидзинский К. К., Сычугов В. А., Усиевич Б. А. // Квантовая электроника. 2004. Т 34, N 8. С. 755–760

4. Meint K. Smit. «PHASAR-Based WDM-Devices: Principles, Design and Applications», 1996

5. Venghaus H. «Wavelength Filters in Fiber Optics», 2006.

Pylaev V., Samarin V., Chernov M.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Research on AWG Multiplexer for DWDM Systems.

The article describes the design and principle of operation of an optical multiplexer based on a phased array of waveguides used in fiber-optic networks using spectral sealing, and also presents the results of an experimental study of insertion losses in each channel of the multiplexer.

Key words: integrated optics, fiber waveguides, DWDM system, AWG multiplexer.

УДК 621.39
ГРНТИ 49.44

ИССЛЕДОВАНИЕ МЕТОДОВ ОЦЕНКИ КАЧЕСТВА СВЯЗИ В ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМАХ

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

В работе рассмотрены методы и приборы для оценки качества связи в современных оптических системах. Основное внимание уделено методу оценки Q-фактора по глаз-диаграмме. Проведено экспериментальное исследование влияния хроматической дисперсии и формы оптических импульсов на величину Q-фактора в оптических системах с амплитудной модуляцией ASK и различными видами линейного кодирования. Определены допустимые значения накопленной дисперсии.

волоконно-оптическая система связи, качество передачи, Q-фактор, коэффициент ошибок, глаз-диаграмма, модуляция, линейное кодирование, хроматическая дисперсия

Одной из важнейших задач при эксплуатации волоконно-оптических систем связи (ВОСС) является контроль качества передачи данных. Для оценки качества в цифровых ВОСС в электрическом тракте используются измерения коэффициента ошибок и связанного с ним Q-фактора, а в оптическом тракте – измерение оптического отношения сигнала к шуму (Optical Signal to Noise Ratio, OSNR).

На качество связи оказывают влияние многие факторы. В работе анализируется влияние видов модуляции и бинарного линейного кодирования, а также хроматической дисперсии на величину Q-фактора.

Для исследования ВОСС с амплитудной модуляцией (Amplitude Shift Keying, ASK) была разработана схема [1], представленная на рис.1. Схема содержит передатчик Optical Transmitter, работающий со скоростью 10 Гбит/с и позволяющий выбрать один из двух способов линейного кодирования NRZ или RZ-50. Сигнал с выхода передатчика попадает на источник хроматической дисперсии Ideal Dispersion Compensation FBG, представляющий собой волоконную брэгговскую решетку (Fiber Bragg Grating, FBG) с переменным периодом, настроенную таким образом, чтобы отражать оптический сигнал с центральной длиной волны передатчика, одновременно внося в него искажения посредством установленной величины хроматической дисперсии. Отраженный от FBG сигнал принимается энергетическим приемником Optical Receiver. В схеме предусмотрен также второй приемник, регистрирующий прошедший через FBG сигнал.

Для проведения измерений и контроля качества передачи в схеме имеются измерительные приборы – визуализаторы оптического сигнала Optical Time Domain Visualizer, измерители оптической мощности Optical Power Meter и анализаторы качества связи BER Analyzer. BER Analyzer представляет собой

быстродействующий осциллограф, позволяющий наблюдать глаз-диаграмму принятого сигнала, измерять значение Q-фактора и рассчитывать соответствующий коэффициент ошибок. Основные параметры компонентов схемы представлены в таблице 1.

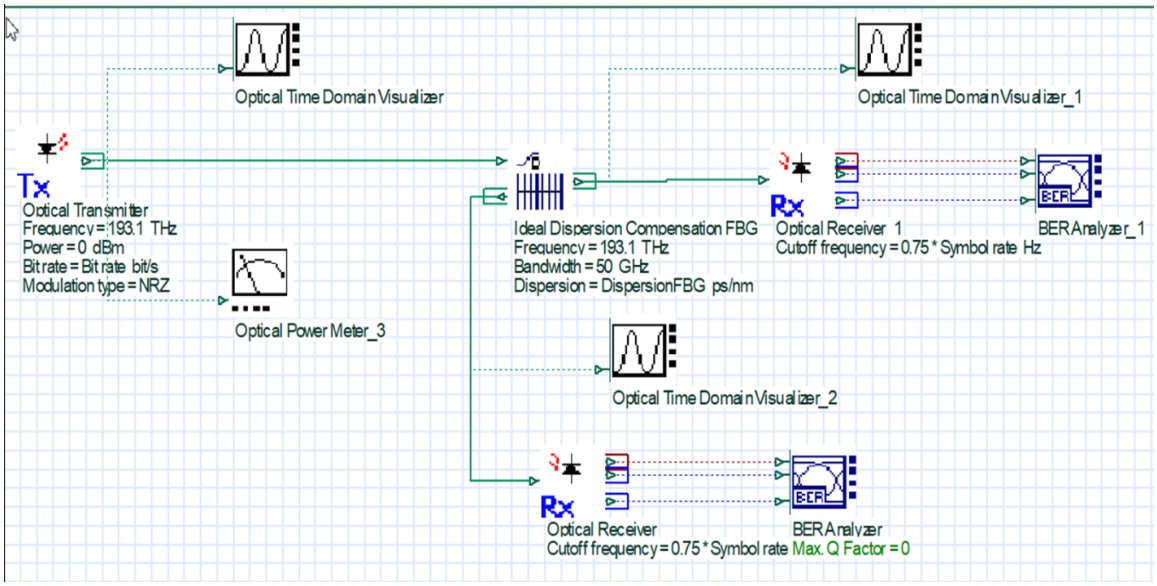


Рис. 1. Схема исследования ВОСС с ASK

ТАБЛИЦА 1. Параметры компонентов схемы ВОСС с ASK

Параметр	Значение
Центральная длина волны передатчика, нм	1552,52
Мощность передатчика, дБм	0
Скорость передачи, Гбит/с	10
Линейный код	NRZ и RZ-50
Диапазон изменения хроматической дисперсии FBG, пс/нм	0-1500

В ходе исследования определялась зависимость Q-фактора от установленного значения хроматической дисперсии FBG. Исследования для кодирования RZ-50 были проведены для двух форм оптических импульсов – прямоугольной и треугольной. Результаты моделирования представлены в таблице 2.

Из таблицы 2 видно, что с ростом хроматической дисперсии качество связи для сигнала NRZ монотонно снижается [2а]. Зависимость Q-фактора от величины хроматической дисперсии представлена на рис. 2а.

Считая, что минимально допустимое значение Q-фактора составляет 7, была определена максимальная допустимая величина хроматической дисперсии для NRZ сигнала, которая составила Dmax = 980 пс/нм.

ТАБЛИЦА 2. Результаты исследования ВОСС с ASK

Хроматическая дисперсия D, пс/нм	Q- фактор для линейного кода		
	NRZ	RZ-50, прямоуг. импульсы	RZ-50, треуг. импульсы
0	2032.02	3334.32	2131.3771
50	240.227	378.279	314.42289
100	147.899	190.358	155.21902
150	79.4096	127.984	106.4204
200	50.599	100.847	82.383395
250	36.6992	77.8216	68.027886
300	30.5502	69.2786	57.213566
350	25.9376	66.87	49.144437
400	22.261	63.866	43.489661
450	19.6317	55.4007	39.297916
500	18.1246	52.8797	35.439602
550	17.3296	48.0386	33.118971
600	17.0356	29.2675	30.396849
650	17.0475	19.9024	27.061221
700	17.1625	20.577	23.256096
750	17.1565	19.9975	19.468121
800	17.1661	2.75834	15.894971
850	16.5589	2.77269	12.902315
900	15.3382	2.77539	2.9285681
950	13.6389	2.76739	2.960755
1000	12.1083	2.74882	2.9972187
1050	10.817	2.7286	3.038185
1100	9.7847	2.71061	3.0822532
1150	8.97992	2.70291	3.1292371

Аналогичная зависимость ожидалась для RZ-50 с импульсами прямоугольной формы. Однако моделирование показало очень резкое падение качества связи при возрастании дисперсии до 800 пс/км. Для треугольных импульсов такого эффекта не наблюдалось [2б]. Полагая, что так как невозможно создать прямоугольные импульсы с идеально вертикальными фронтами, в реальности следует все-таки ожидать монотонное изменение Q-фактора, была проведена аппроксимация полученной зависимости монотонной функцией и определена максимальная допустимая величина хроматической дисперсии, которая составила 670 пс/нм, которое представлено на рис. 2б.

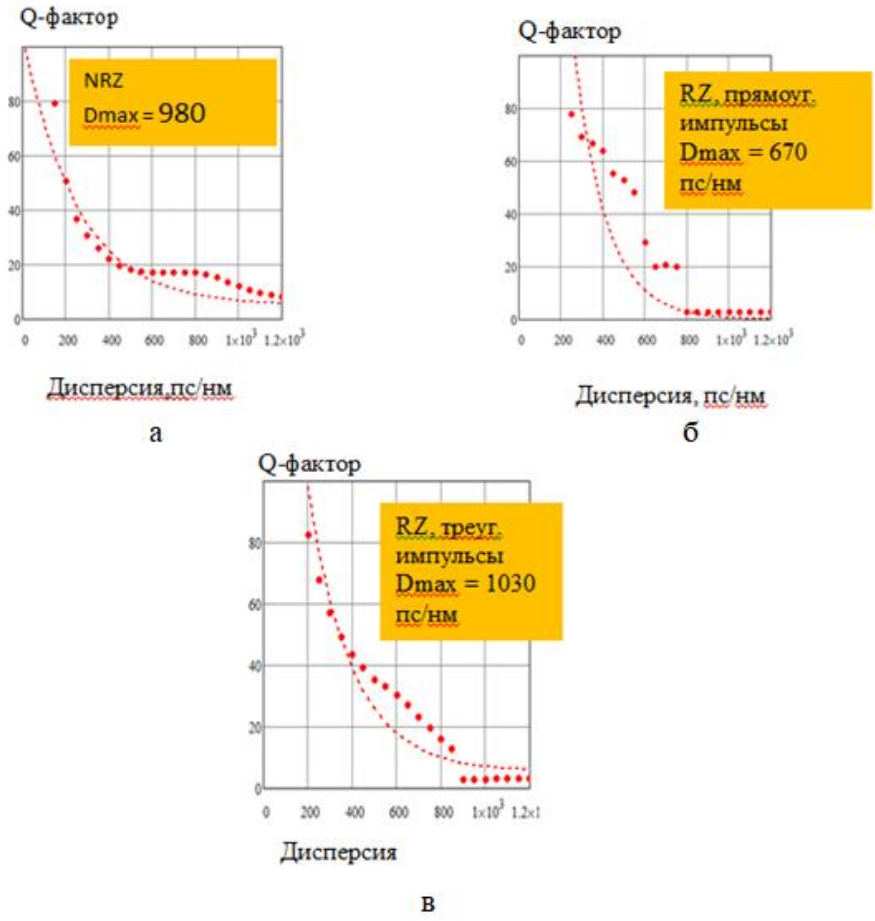


Рис. 2. Зависимости Q-фактора от хроматической дисперсии в ВОСС 10 Гбит/с с ASK при линейном кодировании NRZ (а), RZ-50 (б, в) и различной форме импульсов: а, б – прямоугольной, в – треугольной. Точками на графиках показаны результаты моделирования, пунктирными линиями – результат проведенной аппроксимации

Таким образом, в результате проведенного исследования было установлено, что наиболее устойчивы к хроматической дисперсии ВОСС с линейным кодированием RZ-50 и треугольной формой оптического импульса. Для них достигнуто максимальное значение допустимой дисперсии, равное 1030 пс/нм. Наихудшие результаты получены для кода RZ-50 и прямоугольной формы импульсов – 670 пс/нм. Кодирование NRZ также позволило получить большую допустимую дисперсию – 980 пс/нм.

Список используемых источников:

1. Макаров Т. В. Когерентные волоконно-оптические системы передачи : учебник / Макаров Т. В. Одесса: ОНАС им. А.С. Попова, 2009. 220 с.

2. Оптические волокна в телекоммуникациях : учеб. пособие / М. С. Былина, С. Ф. Глаголев. СПб. : СПбГУТ, 2019. 108 с.

3. Мандель А.Е. Метрология в оптических телекоммуникационных системах : учеб. пособие. Томск: Томский государственный университет систем управления и радиоэлектроники, 2014. 139 с.

4. Андреева Е. И., Былина М. С., Глаголев С. Ф. Методы и приборы для оптических измерений в инфокоммуникациях. Измерение параметров оптических волокон.

Поляризационные измерения. Рефлектометрия : учеб. Пособие. СПб. : СПбГУТ. 2020. 86 с.

Shishkina V.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Research of methods for assessing communication quality in fiber-optic systems.

The paper discusses methods and instruments for assessing the quality of communication in modern optical systems. The main attention is paid to the method of estimating the Q-factor using an eye diagram. An experimental study of the influence of chromatic dispersion and the shape of optical pulses on the value of the Q-factor in optical systems with ASK amplitude modulation and various types of linear coding was carried out. Acceptable values of accumulated variance have been determined.

Key words: fiber optic communication system, transmission quality, Q-factor, error rate, eye diagram, modulation, line coding, chromatic dispersion.

Секция 3.5.
Программная инженерия

УДК 004.946
ГРНТИ 28.17.33

СРАВНЕНИЕ ОПТИМИЗАТОРОВ В ЗАДАЧЕ КЛАССИФИКАЦИИ ИЗОБРАЖЕНИЙ MNIST НА ПРИМЕРЕ ТРЕХ НЕЙРОННЫХ СЕТЕЙ

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

Целью статьи является проведение сравнения эффективности применения оптимизаторов SGD, SGD_Nesterov, Adam, Adam_AMSGrad, AdaBelief, AdaBelief_AMSGrad, Adadelta, Adagrad, Adamax, Nadam, RMSprop, RMSprop_Centered на примере трех нейронных сетей: двухслойный персептрон, Linear-ReLU-сеть с Dropout, сверточной нейронной сети – в задаче классификации изображений MNIST. Актуальность поставленной задачи определена необходимостью развития инструментов для классификации данных.

нейронная сеть, обратное распространение, классификация изображений, MNIST

1. Введение.

Классификация изображений символов – одна из классических проблем глубокого обучения. Научить компьютеры эффективно распознавать символы довольно трудно. Поэтому существует потребность в эффективном методе, который позволит обеспечить высокую точность распознавания и высокую скорость вычислений.

Распознавание рукописных символов находит широкое применение. Например, распознавание рукописного ввода на планшетах и смартфонах, почтовых индексов для сортировки почтовых сообщений, записей в деловых документах, номерных знаков, текстов книг и др.

Было разработано и продолжает разрабатываться множество инструментов машинного обучения, таких как tensorflow, scikit-learn, scipy-image, theano и др., которые помогают разработчикам и исследователям разрабатывать различные модели машинного обучения, обучать и тестировать их, а также развертывать их в современных приложениях.

Набор данных MNIST – образцы рукописного написания латинских цифр [1]. Изображения размера 28×28 пикселей. 60.000 изображений для обучения, 10.000 – для тестирования.

MNIST содержит 13 ошибочно размеченных тестовых образцов [2] (99,87 в таком случае – максимально возможная точность). Несмотря на это, этот набор данных всё ещё остается наиболее популярным набором данных для сравнения производительности и точности моделей.

2. Обзор литературы.

В области распознавания рукописных цифр и букв было проведено множество исследований. F. Siddique, S. Sakib and M. A. B. Siddique в [3] представили результаты работы усовершенствованной свёрточной

нейронной сети в распознавании изображений MNIST (100% на обучающей выборке и 99.06% на тестовой, а также 98.94% на обучающей выборке и 99.24% на тестовой). Dixit Ritik, Kushwah Rishika и Pashine Samay в [4] представили результаты распознавания рукописных цифр MNIST с использованием многослойной нейронной сети, метода опорных векторов (SVM) и свёрточной нейронной сети (многослойная нейронная сеть: 99.92% на обучающей выборке и 98.85% на тестовой; метод опорных векторов: 99.98% на обучающей выборке и 94% на тестовой; свёрточная нейронная сеть: 99.53% на обучающей выборке и 99.31% на тестовой).

Несмотря на впечатляющие результаты работы сверточных нейронных сетей, их время обучения часто существенно больше.

3. Основная часть.

При помощи Python 3.7 и библиотек tensorflow, talos, numpy и др. были разработаны ipynb-модули для проведения тестирования.

Исследуемые оптимизаторы и их статические параметры:

– SGD и SGD_Nesterov;

– Adam и Adam_AMSGrad: beta1=0.9, beta2=0.999, epsilon=1e-7;

– AdaBelief и AdaBelief_AMSGrad: beta1=0.9, beta2=0.999, epsilon = 1e-14, weight_decay=0.0, rectify=True, warmup_proportion=0.1, min_lr=0.0, sma_threshold=5.0;

– Adadelta: rho=0.95, epsilon=1e-07;

– Adagrad: initial_accumulator_value=0.1, epsilon=1e-7;

– Adamax: beta_1=0.9, beta_2=0.999, epsilon=1e-7;

– Nadam: beta_1=0.9, beta_2=0.999, epsilon=1e-7;

– RMSprop и RMSprop_Centered: rho=0.9, momentum=0.0, epsilon=1e-7.

Архитектура двухслойного персептрона (261510 обучаемых параметров):

1. Dense(units=250, activation='sigmoid', use_bias=True, kernel_initializer = 'glorot_uniform', bias_initializer='zeros', input_shape=(784,));

2. Dense(units=250, activation='sigmoid', use_bias=True, kernel_initializer = 'glorot_uniform', bias_initializer='zeros');

3. Dense(units=10, activation='sigmoid', use_bias=True, kernel_initializer = 'glorot_uniform', bias_initializer='zeros').

Для каждого оптимизатора перебираются следующие параметры:

1. Batch size: 10, 15, 20, 25, 30, 35, 40;

2. Learning rate: 0.001, 0.01, 0.1, 1, 2, 5.

В результате выбраны наилучшие результаты, которые приведены в таблице 1.

ТАБЛИЦА 1. Лучшие результаты обучения двухслойного персептрона по оптимизаторам (50 эпох обучения)

Оптимизатор	Тип	Точность на обучающей выборке	Точность на тестовой выборке	Время
Adadelta learning_rate=5.0 batch_size=15	Лучший случай	100%	98.48%	272 с.
	В среднем	100%	98.373 ± 0.036%	273 с.
SGD_Nesterov learning_rate=1.0 batch_size=25	Лучший случай	100%	98.50%	136 с.
	В среднем	100%	98.372 ± 0.033%	143 с.
Adamax learning_rate=0.01 batch_size=30	Лучший случай	100%	98.41%	150 с.
	В среднем	99.99%	98.336 ± 0.033%	151 с.

Архитектура Dropout-Linear-ReLU сети (261510 обучаемых параметров):

1. Dropout(rate=dropout_rate, input_shape=(784,));
2. Dense(units=250, activation='linear', use_bias=True, kernel_initializer = 'glorot_uniform', bias_initializer='zeros');
3. ReLU(max_value=None, negative_slope=0, threshold=0);
4. Dense(units=250, activation='linear', use_bias=True, kernel_initializer = 'glorot_uniform', bias_initializer='zeros');
5. ReLU(max_value=None, negative_slope=0, threshold=0).
6. Dense(units=10, activation='linear', use_bias=True, kernel_initializer = 'glorot_uniform', bias_initializer='zeros').

Для каждого оптимизатора перебираются следующие параметры:

1. Batch size: 10, 15, 20, 25, 30, 35, 40;
2. Learning rate: 0.001, 0.01, 0.1, 1, 2, 5;
3. Dropout rate: 0.2, 0.3, 0.4, 0.5.

В результате выбраны наилучшие результаты, которые приведены в таблице 2.

ТАБЛИЦА 2. Лучшие результаты обучения Dropout-Linear-ReLU сети по оптимизаторам (50 эпох обучения)

Оптимизатор	**Тип**	**Точность на обучающей выборке**	**Точность на тестовой выборке**	**Время**
SGD_Nesterov learning_rate=0.1 batch_size=40 dropout_rate=0.3	Лучший случай	99.97%	98.84%	106 с.
	В среднем	99.945 ± 0.022%	98.624 ± 0.063%	106 с.
SGD learning_rate=0.1 batch_size=40 dropout_rate=0.3	Лучший случай	99.96%	98.72%	106 с.
	В среднем	99.948 ± 0.014%	98.588 ± 0.066%	106 с.
Adagrad learning_rate=0.1	Лучший случай	99.98%	98.64%	276 с.

batch_size=20 dropout_rate=0.3	В среднем	99.990 ± 0.003%	98.559 ± 0.053%	217 с.

Архитектура сверточной нейронной сети (CNN, 2377202 обучаемых параметров):

1) Conv2D(filters=32, kernel_size=(3, 3), strides=(1, 1), padding='same', data_format=None, dilation_rate=(1, 1), groups=1, activation='relu', use_bias=True, kernel_initializer='glorot_uniform', bias_initializer='zeros', input_shape=(28, 28, 1));

2) MaxPooling2D(pool_size=2, strides=2, padding="valid");

3) Conv2D(filters=48, kernel_size=(3, 3), strides=(1, 1), padding='same', data_format=None, dilation_rate=(1, 1), groups=1, activation='relu', use_bias=True, kernel_initializer='glorot_uniform', bias_initializer='zeros');

4) MaxPooling2D(pool_size=2, strides=2, padding="valid");

5) Dropout(rate=0.5);

6) Flatten();

7) Dense(units=250, activation='relu', use_bias=True, kernel initializer = 'glorot_uniform', bias_initializer = 'zeros');

8) Dropout(rate=0.3);

9) Dense(units=10, activation='softmax', use_bias=True, kernel initializer = 'glorot_uniform', bias initializer = 'zeros').

Для каждого оптимизатора перебирается параметр Learning rate: 0.001, 0.01, 0.1, 1, 2, 5. Параметр Batch size выбран равным 500 для приемлемого времени обучения.

В результате выбраны наилучшие результаты, которые приведены в таблице 3.

ТАБЛИЦА 3. Лучшие результаты обучения CNN по оптимизаторам (50 эпох обучения)

Оптимизатор	**Тип**	**Точность на обучающей выборке**	**Точность на тестовой выборке**	**Время**
Adadelta learning_rate=2.0 batch_size=500	Лучший случай	99.97%	99.56%	867 с.
	В среднем	99.969 ± 0.004%	99.455 ± 0.037%	867 с.
RMSprop learning_rate=0.001 batch_size=500	Лучший случай	99.58%	99.47%	886 с.
	В среднем	99.958 ± 0.006%	99.430 ± 0.021%	883 с.
RMSprop_Centered learning_rate=0.001 batch_size=500	Лучший случай	99.96%	99.50%	890 с.
	В среднем	99.962 ± 0.005%	99.422 ± 0.027%	891 с.

4. Выводы и дальнейшие перспективы исследования.

1. Эффективность оптимизаторов зависит от используемой архитектуры нейронной сети. Например, результаты обучения с использованием оптимизаторов SGD и SGD_Nesterov в случае сверточной нейронной сети –

худшие, результаты обучения с использованием оптимизаторов RMSprop и RMSprop_Centered – лучшие, а в случае Dropout-Linear-ReLU сети результат совсем обратный.

2. Оптимальные Learning rate для оптимизаторов: SGD и SGD_Nesterov – 0.1; Adam и Adam_AMSGrad – 0.001; AdaBelief и AdaBelief_AMSGrad – 0.001; Adadelta – 2.0; Adagrad – 0.1; Adamax – 0.01; Nadam – 0.001; RMSprop и RMSprop_Centered – 0.001.

3. В случае параметра Batch size определить наилучшее значение достаточно сложно. Кроме того, наилучшее значение зависит от оптимизатора и других его параметров.

Список используемых источников:

1. Yann Lecun, Léon Bottou, Yoshua Bengio, and Patrick Haffner. Gradient-based learning applied to document recognition // In Proceedings of the IEEE. 1998. С. 2278–2324.

2. Curtis G. Northcutt, Anish Athalye and Jonas Mueller. Label errors in ML Test Sets [Электронный ресурс]. URL: https://labelerrors.com/ (дата обращения 14.11.2023).

3. F. Siddique, S. Sakib and M. A. B. Siddique. Recognition of Handwritten Digit using Convolutional Neural Network in Python with Tensorflow and Comparison of Performance for Various Hidden Layers // 5th International Conference on Advances in Electrical Engineering (ICAEE), 2019. С. 541-546.

4. Dixit Ritik, Kushwah Rishika and Pashine Samay. Handwritten Digit Recognition using Machine and Deep Learning Algorithms // International Journal of Computer Applications : N 176(42), India, 2020. С. 27-33.

Ezhurov A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Comparison of optimizers in the image classification task on the mnist dataset using three neural networks.

The purpose of this article is to compare the efficiency of using the optimizers SGD, SGD_Nesterov, Adam, Adam_AMSGrad, AdaBelief, AdaBelief_AMSGrad, Adadelta, Adagrad, Adamax, Nadam, RMSprop, RMSprop_Centered in the case of three neural networks: a two-layer perceptron, a Linear-ReLU network with Dropout, and a convolutional neural network, in the task of image classification on the MNIST dataset. The relevance of the proposed task is determined by the need for the development of tools for data classification.

Key words: neural network, backpropagation, image classification, MNIST.

УДК 51-74
ГРНТИ 27.47.23

ЗНАЧИМОСТЬ МАТЕМАТИЧЕСКИХ МЕТОДОВ В СИСТЕМАХ МАШИННОГО ОБУЧЕНИЯ И АНАЛИЗА ДАННЫХ

В. Е. Конак
Санкт-Петербургский государственный университет промышленных технологий и дизайна

Математические способы представления систем машинного обучения и анализа данных являются неотъемлемой частью современной научной и технологической сферы. Понимание этих методов и их применение в различных областях анализа данных позволяет разрабатывать более эффективные алгоритмы машинного обучения, улучшать качество прогнозов и повышать точность результатов.

машинное обучение, анализ данных, искусственный интеллект, математика

В настоящее время нейронные сети и искусственный интеллект всё активнее применяются в различных сферах деятельности человека: от просчета опорных сооружений архитектурного проекта до анализа рентгенограмм для повышения точности конечного диагноза. Такое использование нейронных сетей позволяет многократно облегчить работу человека, давая ему возможность заняться другой умственной деятельностью.

Качество прогнозов, их точность и охват предметной области – все эти факторы определяются на этапе проектирования нейронной сети: выборка данных для обучения, определение способа обучения, итоговое время обучения и его эффективность. Правильное проектирование будущего ИИ невозможно без знания необходимой математической базы. По статистике, лишь каждый 5й человек берет во внимание математическую составляющую при знакомстве с машинным обучением [3].

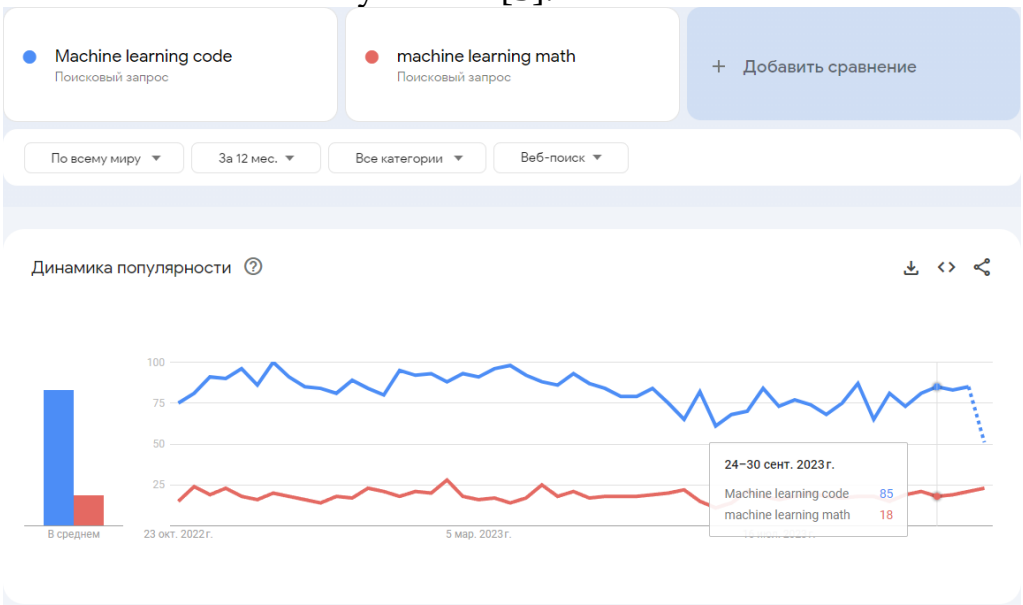


Рис. 1. Статистика поисковых запросов «Machine learning» в Google Trends

Знание математики играет ключевую роль при проектировании искусственного интеллекта и нейронных сетей. Математические методы позволяют формализовать задачи, решать их с помощью алгоритмов и оценивать результаты. Кроме того, знание математики помогает понять ограничения и возможности различных алгоритмов, что позволяет разрабатывать более эффективные решения для задач машинного обучения.

Какие разделы математики стоит изучат и какое они имеют применение в системах машинного обучения [1][2]:

1. **Линейная алгебра** используется для работы с векторами и матрицами, которые являются основой многих алгоритмов машинного обучения. Например, метод главных компонент основан на анализе векторных пространств, а логистическая регрессия использует линейные отображения между векторами признаков и целевыми значениями.
2. **Дифференциальное исчисление** используется для нахождения экстремумов функций, что важно для оптимизации моделей машинного обучения. Например, градиентный спуск использует производные для нахождения оптимальных параметров моделей.
3. **Дифференциальные уравнения** используются для моделирования процессов в машинном обучении, например, для моделирования временных рядов.
4. **Теория вероятностей и статистика** используются для работы с неопределенностью и оценки качества моделей машинного обучения с использованием метрик, таких как точность, recall и F1-score.
5. **Оптимизация** используется для поиска оптимальных параметров моделей машинного обучения. Алгоритмы оптимизации, такие как градиентный спуск, используют производные для поиска экстремумов функции потерь.
6. **Теория графов** – это раздел математики, который изучает свойства и взаимосвязи различных объектов, представленных в виде графов. Графы используются в машинном обучении для анализа сетевых структур и представления данных. Графы также могут быть использованы для представления моделей машинного обучения, таких как нейронные сети.
7. **Численные методы** используются для решения задач машинного обучения на компьютере. Например, численные методы используются для решения систем линейных уравнений, которые возникают при использовании методов линейной алгебры в машинном обучении.
8. **Многомерная статистика** используется для анализа многомерных данных, таких как изображения или временные ряды. Многомерная статистика используется для извлечения информации из данных и построения моделей машинного обучения.
9. **Байесовский вывод** используется для статистического анализа данных и построения вероятностных моделей. Байесовские методы широко

используются в машинном обучении для построения вероятностных классификаторов, регрессий и кластеризаций.

10. **Нелинейное программирование** используется для решения оптимизационных задач, которые могут иметь нелинейные ограничения. Это полезно, например, при решении задачи классификации, когда ограничения могут быть наложены на вероятности ошибок.

Невозможно переоценить значимость математики в сфере информационных технологий. За любым новым изобретением или технологией находится большой пласт математических знаний и расчётов. Нейронные сети и искусственный интеллект не стали исключением из этого правила.

Таким образом, мы приходим к выводу о значимости математических структур и алгоритмов, заложенных в методах машинного обучения и анализа данных.

Список используемых источников:

1. Воронцов К. В. Математические методы обучения по прецедентам (теория обучения машин).
2. Информационно-аналитический ресурс: MachineLearning.ru [Электронный ресурс]. URL: http://www.machinelearning.ru/(дата обращения: 16.10.2023).
3. Статистика поисковых запросов: Google Trends [Электронный ресурс]. URL: https://trends.google.ru/trends/explore?q=Machine%20learning%20code,machine%20learning%20math&hl=ru(дата обращения: 16.10.2023).

Konak V.

Saint-Petersburg State University of Industrial Technologies and Design

Mathematical ways of representing machine learning and data analysis systems. Mathematical ways of representing machine learning and data analysis systems are an essential part of today's scientific and technological fields. Understanding these methods and applying them to various areas of data analysis allows for the development of more efficient machine learning algorithms, better predictions, and more accurate results.

Key words: Machine learning, data analysis, AI, mathematics.

УДК 004.42
ГРНТИ 50.41.25

РАЗРАБОТКА ПРИЛОЖЕНИЯ ДЛЯ ФОРМИРОВАНИЯ ОБУЧАЮЩИХ НАБОРОВ ДАННЫХ С ПОМОЩЬЮ СЕРВИСОВ ВЕРТИКАЛЬНЫХ КОРОТКИХ ВИДЕОРОЛИКОВ

А. А. Правдин А. Л. Родионов А. С. Соловьев
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире всё больше растёт спрос на обучающие наборы данных для искусственных нейронных сетей, что сильно увеличивает их стоимость. В связи с этим имеет смысл автоматизировать процесс их формирования. Для решения это задачи предлагается создать приложения для формирования обучающих наборов данных на основе открытых сервисов вертикальных коротких видеороликов.

искусственные нейронные сети, обучающие наборы данных, видеоролики

На сегодняшний день в мире всё больше растёт потребность в обучающих наборах данных для тренировки искусственных нейронных сетей и для иных процессов принятия решений, основанных на данных. Это приводит к активному развитию рынка данных и росту цен. Так платформа сбора данных и бизнес статистики Statista приводит график [1] прогноза изменения объема рынка с 2011 по 2027 год, что представлено на рис. 1.

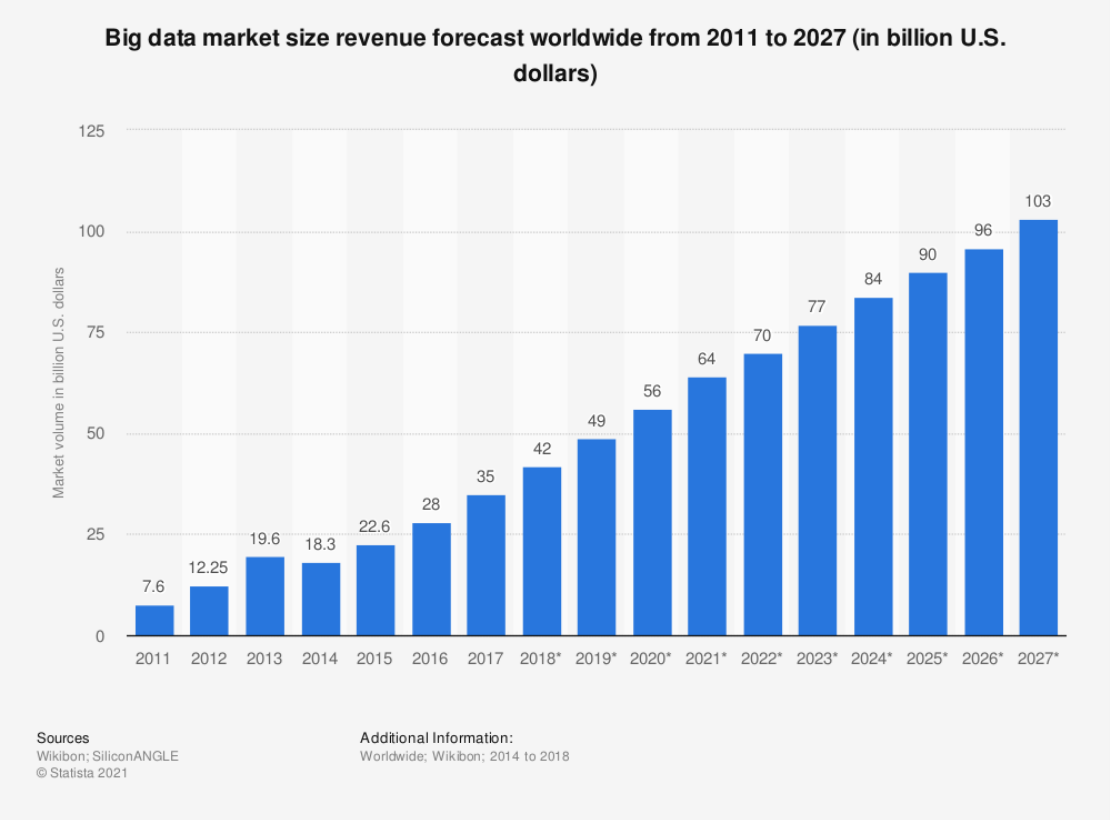


Рис. 1. Прогноз изменения объема рынка данных с 2011 по 2027 год

Таким образом, коммерческий рынок наборов данных становится недоступен для средних коммерческих или бюджетных организаций, что заставляет их искать другие методы получения данных. Рассмотрим наиболее распространённые из них в сравнении с покупкой данных на рынке:

1. Ручное формирование наборов данных

Ручное формирование предполагает наём большого количества сотрудников для мануального поиска данных, пригодных для обучения. Такой подход сильно уступает покупке данных, так как всё ещё требует высоких финансовых затрат на оплату работы большого количества дополнительных сотрудников, значительного количества времени, а также риск попадания ошибочных данных при некачественной организации контроля.

2. Поиск готовых наборов данных в публичном доступе

Метод основывается на поиске обучающих наборов данных из открытых источников. Данный метод полностью исключает финансовые затраты, но его использование не всегда представляется возможным, в связи с малым количеством публичных наборов данных. Также, публичные наборы данных зачастую уступают в своих размерах коммерческим, и не могу гарантировать качество каждого отдельного элемента в наборе, что может привести к ошибочным результатам в дальнейшем.

Проанализировав вышеперечисленные методы, можно сделать вывод, что они не позволяют в полной мере решить проблему высокой стоимости наборов данных, так как имеют свои условия применения или требуют значительного числа дополнительных сотрудников. Следовательно, необходимо разработать новый подход.

В качестве решения этой проблемы, предлагается пересмотреть подход ручного формирования наборов данных. Метод можно полностью автоматизировать, используя компьютерные мощности для поиска и анализа видеороликов. Для этого необходимо создать программное обеспечение, анализирующих сторонние публичные сервисы вертикальных коротких видеороликов (такие как YouTube Shorts, TikTok, Likee и подобные), и формирующее на их основе качественные наборы данных, используя при этом существующие искусственные нейронные сети.

Для улучшения качества поиска данных и их количества после обработки в итоговом обучающем наборе, можно использовать различные средства, такие как:

1. Определение списка ключевых слов для эффективного поиска
2. Отслеживание определенных аккаунтов видео сервиса
3. Использование заранее настроенного аккаунта для улучшенной выдачи видео алгоритмами сервиса
4. Автоматическое обрезание видео с целью удаления не подходящих кадров
5. Добавление шумов, зеркальное отображение и иные методы искажений видеороликов с целью увеличения объема набора данных

В качестве реализации приложения предлагается использовать программу, написанную на языке программирования Python с использованием искусственных нейронных сетей библиотеки OpenCV [2].

Всё это позволит получать обучающие наборы данных в практически неограниченных количествах исключая при этом риск человеческой ошибки и сокращая финансовые затраты до минимума. Скорость получения данных будет зависеть от вычислительных мощностей и качества интернет соединения. В дальнейшем, приложение можно улучшать, добавляя новые методы поиска, подключая другие сервисы и искусственные нейронные сети.

Список используемых источников:

1. Прогноз объема рынка больших данных и выручки по всему миру на период с 2011 по 2027 год [Электронный ресурс]. URL: https://www.statista.com/statistics/254266/global-big-data-market-forecast/ (дата обращения: 13.11.2023).
2. OpenCV: библиотека с открытым исходным кодом [Электронный ресурс]. URL: https://opencv.org/ (дата обращения: 13.11.2023).

Pravdin A. Rodionov A. Soloviev A.

The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Development of an application for the formation of training data sets using vertical short video services.

In the modern world, there is an increasing demand for training datasets for artificial neural networks, which greatly increases their cost. In this regard, it makes sense to automate the process of their formation. To solve this problem, it is proposed to create applications for the formation of training datasets based on open services of vertical short videos.

Key words: artificial neural networks, training datasets, videos.

СВЕДЕНИЯ ОБ АВТОРАХ

АБЗАЛОВ
Тимур Альфритович
студент группы ИБС-21
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
abzalovtimur04@mail.ru

АГАЯН
Дмитрий Александрович
студент группы РТ-31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
diman-agayan@mail.ru

АЛЕКСАНДРОВА
Агата Георгиевна
студент группы ИКТБ-27м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
agatka.aleksandrova27@mail.ru

АЛЕКСАНДРОВСКИЙ
Руслан Даниилович
студент группы БИ-21м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Ruslan_alex20001@mail.ru

АЛЕКСЕЙЧУК
Петр Дмитриевич
студент группы ИКТБ-37м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
alekseychukp@inbox.ru

АЛЕХНО
Александр Витальевич
студент группы ИКТС-22
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
sashaaalekhno@gmail.com

АЛЬКАТТАН
Самех
студент группы ИКТБ-37м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
sameh.kt94@gmail.com

АЛЬ-НАМИ
Башер Али
кандидат технических наук, старший преподаватель кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alnomibasheer@gmail.com

АМОСОВ
Даниил Александрович
студент группы ИКТС-23 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, amosov200931@gmail.com

АНДРЕЕВА
Татьяна Алексеевна
кандидат физико-математических наук, доцент, доцент кафедры бизнес-информатики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tandreeva@yahoo.com

АНДРИАНОВ
Дмитрий Максимович
студент группы ИСТ-331м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dimon60thief@gmail.com

АНТОНЦЕВ
Максим Владимирович
студент группы ИКТФ-36м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, donat1316@mail.ru

АРЕФЬЕВ
Алексей Сергеевич
студент группы Р-32м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tay3435@yandex.ru

АРТАМОНОВ
Артем Сергеевич
студент группы РТ-32м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
vesta2868@gmail.com

АСАКОВ
Максим Рашидович
студент группы ИБТС-31
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
max.asakov@gmail.com

АСТАФЬЕВА-
РУМЯНЦЕВА
Ирина Евгеньевна
кандидат философских наук, доцент кафедры
социально-политических наук
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича

АХРАМЕЕВА
Ксения Андреевна
кандидат технических наук, доцент, доцент
кафедры защищенных систем связи Санкт-
Петербургского государственного университета
телекоммуникаций
им. проф. М.А. Бонч-Бруевича

БАЖЕНОВА
Полина Андреевна
студент группы БИМ-21з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
bazhenovapo@icloud.com

БАРАНОВ
Максим Алексеевич
студент группы РТ-21м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
maxxbar@yandex.ru

БАРАНОВА
Диана Святославовна
студент группы ФП-11
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
dianabaranova2003@icloud.com

БАРЫГИН
Иван Сергеевич
студент группы ИКТС-21
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
letithrowaway@mail.ru

БАРЫШНИКОВ
Михаил Александрович
студент группы ИКТС-22
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
neofire9@yandex.ru

БАТАЛИН
Ярослав Леонидович
студент группы ИБТС-31
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
batalinyaroslaw@yandex.ru

БАТИН
Евгений Александрович
студент группы ИКТБ-38м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
zhenya0batin@mail.ru

БАУЛИНА
Диана Леонидовна
студент группы ИКТС-23
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
dianabaulina1@gmail.com

БЕКЕР
Иван Александрович
студент группы ИКТС-21
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича
beksrz123@outlook.com

БЕЛАЯ
Татьяна Иоанновна
кандидат технических наук, доцент кафедры
программной инженерии и вычислительной
техники Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
studentszip@yandex.ru

БЕЛОВ
Михаил Петрович
доктор технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, ius@sut.ru

БЕЛОЦЕРКОВСКИЙ
Максим Вадимович
студент группы ЭП-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mbwx00@mail.ru

БЕЛЯЕВ
Андрей Александрович
студент группы ИКТФ-26м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, adresat240@gmail.com

БЕНЧ
Максим Николаевич
студент группы ИКТБ-37М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bench140201@gmail.com

БЕССОНОВА
Екатерина Денисовна
студент группы ИКТС-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bessonova@t8.ru

БИЛЕВА
Ольга Дмитриевна
студент группы ИСМ-11з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Bilevaspb@gmail.com

БОБЕР
Александр Дмитриевич
студент группы ЭП-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gameswithraccoon@gmail.com

БОВБЕЛЬ
Ярослав Александрович
студент группы ИКБ-05
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
yaroslavbovbel@mail.ru

БОГОМАЗ
Мария Эдуардовна
студент группы ИКТЗ-21м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича, masha-
bogomaz@yandex.ru

БОЙКО
Александр Алексеевич
студент группы ИКТС-23м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
pevoons@gmail.com

БОЛЬШАКОВА
Кристина Евгеньевна
студент группы БИМ21-з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
krisbol2000@gmail.com

БОНДАРЕВ
Эдуард
студент группы ИКТИ-25м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
eddition@yandex.ru

БОНДАРЕНКО
Игорь Борисович
кандидат технических наук, доцент
кафедры информационных управляющих систем
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
igorlitmo@rambler.ru

БОНДАРЬ
Андрей Дмитриевич
студент группы ИКТС-22
Санкт-Петербургского
государственного университета
телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
bad0405@yandex.ru

БОРИСОВА
Анастасия Алексеевна
студент группы ЭБМ-31з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича

БОРОДКИН
Денис Юреьвич
студент группы РСО-21м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
denis.borodkin99@gmail.com

БОТАЛОВ
Андрей Алексеевич
студент группы ИСТ-231м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
andbotalovand@gmail.com

БОЧАРОВ
Дмитрий Николаевич
студенты группы ИСТ-341м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
dim.bocharov123@mail.ru

БРЕНЕВА
Екатерина Павловна
студент группы ИКТР-22
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, meetfead@mail.ru

БРИЗГАНОВ Евгений
Андреевич
студент группы ИСТ-331м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
brizganove@gmail.com

БУДАРИН
Макар Эдуардович
студент ИКТЗ-31м
Санкт-Петербургский государственный
университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
budarin.makar@gmail.com

БУЛЫГИН
Дмитрий Константинович
студент группы ИБС-12
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
bulygin.dk@gmail.com

БУСЫГИН
Константин Николаевич
доцент кафедры интеллектуальных систем и
защиты информации Санкт-Петербургского
государственного университета промышленных
технологий и дизайна, busyginkn@list.ru

БУТИКОВ
Заян Эрдниевич
студент группы ИКТО-07
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича, leviark@mail.ru

БЫКОВ
Максим Андреевич
студент группы ИБС-21
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
jstlktwo@gmail.com

БЫЛИНА
Мария Сергеевна
кандидат технических наук, доцент, заведующий
кафедрой фотоники и линий связи,
преподаватель базовой кафедры ВТС DWDM
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М.А.
Бонч-Бруевича, BylinaMaria@mail.ru

БЯКИНА
Александра Васильевна
студент группы РСМ-21з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
byakina2000@mail.ru

ВАСИЛЬЕВ
Артур Геннадьевич
студент группы РТ-21
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
artuk79406@gmail.com

ВАСИЛЬЕВ
Владимир Михайлович
студент группы РСО-21м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
vovanvas18@gmail.com

ВАСЬКОВ
Артём
студент группы 3-МД-16
Санкт-Петербургского государственного
университета промышленных технологий и
дизайна, vaskov.artem001@gmail.com

ВЕНКОВ
Владислав Дмитриевич
студент группы ИКТС-22
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
vladvenkov320@gmail.com

ВЕРБИЦКИЙ
Алексей Владимирович
заведующий лабораторией базовой кафедры
«Цифровое телевизионное и радиовещание»
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича

ВЕРБИЦКИЙ
Андрей Алексеевич
студент группы Р-31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
a.verbitskeey@gmail.com

ВЕРЛИКОВ
Никита Владимирович
студент группы ФП-31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
verlikov@internet.ru

ВЕСЕЛОВ
Даниил Алексеевич
студент группы ИСТ-241м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
daniil.veselov2012@yandex.ru

ВИННИКОВ
Семён Андреевич
студент группы ИКТЗ-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vinnikovsema@mail.ru

ВИНОГРАДОВ
Анатолий Эдуардович
студент группы ИСМ-11з
студент группы Р-12 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tolwin130394@mail.ru

ВИНОГРАДОВА
Наталия Алексеевна
студент группы ЭБМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nataliv000@gmail.com

ВИСАЛ
Инг
студент группы 4-МДА-7 Санкт-Петербургского государственного университета промышленных технологий и дизайна, jangful123@gmail.com

ВИТКОВА
Лидия Андреевна
кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, vitkova@comsec.spb.ru

ВЛАДИМИРОВ
Сергей Сергеевич
доктор технических наук, доцент, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimirov.opds@gmail.com

ВОРОБЬЕВ
Ярослав Владимирович
студент группы ИКТВ-03 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yaroslav.vorobev.02@mail.ru

ВОИНКОВ
Егор Борисович
студент группы ИКТК-01
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
voinkoveb@gmail.com

ВОЛКОВ
Владислав Дмитриевич
студент группы ИКТИ-25м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
vladislavvolkovn1@yandex.ru

ВОЛОШИНОВ
Денис Вячеславович
доктор технических наук, заведующий кафедрой
информатики и компьютерного дизайна Санкт-
Петербургского государственного университета
телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
denis.voloshinov@yandex.ru

ВОРОБЬЕВ
Артём Валерьевич
студент группы 4-МДА-7
Санкт-Петербургского государственного
университета промышленных технологий и
дизайна, 8cla77nitsa@gmail.com

ВОРОБЬЕВ
Олег Владимирович
кандидат технических наук, профессор,
заведующий кафедры радиосвязи и вещания
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М.А. Бонч-Бруевича, vorobievov@bk.ru

ВОРОБЬЕВА
Валерия Викторовна
научный сотрудник лаборатории квантовых
коммуникаций и лаборатории квантовых
процессов и измерений, сотрудник
подразделения лаборатории квантовой
информатики Санкт-Петербургский
национальный исследовательский университет
информационных технологий, механики и
оптики

ВОРОНИН
Никита Сергеевич
студент группы Р-21м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
sershantm@mail.ru

ВОРОНЦОВ
Андрей Анатольевич
студент группы ИКТЗ-21м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
vorontsov.andrey000@yandex.ru

ВОРОПАЕВ
Павел Валерьевич
студент группы ФП31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича

ВЫЖЛОВА
Ангелина Кирилловна
студент группы ИСТ-241м Санкт-
Петербургского государственного университета
телекоммуникаций им. проф. М. А. Бонч-
Бруевича, angelsurvivor13@gmail.com

ВЫШИНСКИЙ
Артём Алексеевич
студент группы ИКТС-23
Санкт-Петербургского
государственного университета
телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
aqwenteda@mail.ru

ГАБДУЛИНА
Алина Радиковна
студент группы ИБС-22
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-
Бруевича,lina.gabdulina.04@mail.ru

ГАБИТОВ
Георгий Денисович
студент группы ИКТС-21
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
gabitovg4@gmail.com

ГАЙЛИТ
Данил Дмитриевич
студент группы РТ-22м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
danil.gailit@gmail.com

ГАРИФУЛЛИН
Нияз Билалович
студент группы ИСМ-21з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
nick.comlink.spb2@mail.ru

ГАРМАТЮК
Валерия Вячеславовна
студент группы ИКБ-25
Санкт-Петербургского государственного
университета телекоммуникация
им. проф. М. А. Бонч-Бруевича,
garmatyuklerka@gmail.com

ГЕРБЕРСГАГЕН
Марк Юрьевич
студент группы ИСТ-212
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
3.333-392@mail.ru

ГЕТТО
Дмитрий Юрьевич
студент группы ИКТС-23
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича
dmitrijgetto2004@gmail.com

ГИЛЕВА
Дарья Андреевна
студент группы ИКТС-21
Санкт-Петербургского
государственного университета
телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
zhiza.tiara@gmail.com

ГНЕЗДИЛОВ
Дмитрий Александрович
студент группы РК-21
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
gdabony@gmail.com

ГОЛУБИН
Матвей Вячеславович
студент группы РСО-31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
golubinmv@yandex.ru

ГОМЕНИЦА
Вадим Александрович
студент группы ИКТФ-26м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
nazarnazarov676@gmail.com

ГОНЧАРОВ
Савелий Васильевич
студент группы ИСТ-241м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
saigon2000@inbox.ru

ГОРДЕЕВА
Александра Федоровна
студент группы ИКТС-23
Санкт-Петербургского
государственного университета
телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
alexgordeeva99@mail.ru

ГОРДЕЕВА
Арина Максимовна
студент группы ИКБ-23
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
ardeeva1920@gmail.com

ГРЕЧИШНИКОВ
Евгений Владимирович
доктор технических наук, профессор, профессор
кафедры интеллектуальных систем
автоматизации и управления Санкт-
Петербургского государственного университета
телекоммуникаций им. проф. М.А. Бонч-
Бруевича

ГРИБОВСКИЙ
Алексей Андреевич
студент группы ИСТ-341м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
lesha.kar@yandex.ru

ГРИГОРЬЕВА
Рината Григорьевна
студент группы ИСТ-211м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
honey.lottu@gmail.com

ГРИН Соня	студент группы БИ-21м Санкт-Петербургского государственного университета телекоммуникаций им. профессора М. А. Бонч-Бруевича
ГРОМОВ Владислав Витальевич	кандидат технических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, gromov.vladislav.vitalevich@gmail.com
ГРОХОЛЬСКИЙ Артём Викторович	студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artem.groh2110@yandex.ru
ГРУЗДЕВ Александр Сергеевич	студент группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, xbxfy@mail.ru
ГРУЗДЕВ Алексей Андреевич	студент группы ИСТ-341м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gruzdev.a.a26@mail.ru
ГУБАШЕВА Амина Анваровна	студент группы ЭБМ-31з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, aminka.gubasheva@mail.ru
ГУБИН Александр Николаевич	кандидат технических наук, доцент, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, ius@sut.ru
ГУДОЧКИНА Анна Романовна	студент группы 4-МДА-9 Санкт-Петербургского государственное университета промышленных технологий и дизайна, nazarova.name1@gmail.com

ГУЛЯЕВ
Руслан Сергеевич
студент группы ФП-31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
grulan526@gmail.com

ГУНИНА
Елена Викторовна
кандидат педагогических наук, доцент кафедры
информатики и компьютерного дизайна Санкт-
Петербургского государственного университета
телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
e.v.gunina@yandex.ru

ГУСЕНОВ
Саид Юсупович
студент группы 3-МД-16
Санкт-Петербургского государственного
университета Промышленных технологий и
дизайна, said.gusenov.2004@mail.ru

ГУЩИН
Роман Сергеевич
студент группы ИКТС-22
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, listoshek23@gmail.com

ДАНЯЕВА Татьяна
Васильевна
студент группы БИМ-21з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
st_tatianka@mail.ru

ДАЦЕНКО
Олег Валерьевич
студент группы ИСиТ-041
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
zubazheg@gmail.com

ДВОРОВОЙ
Андрей Васильевич
студент группы ИКТС-23
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
dvorsut13@gmail.com

ДЕГТЕВ
Фёдор Романович
студент группы ИКТС-21
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
fediadegtev@gmail.com

ДЕЛЛА
Корте Флавио
студент группы ИСТ-042
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
fvdellacorte@gmail.com

ДМИТРИЕВ
Сергей Сергеевич
студент группы 4-МДА-9
Санкт-Петербургского государственного
университета промышленных технологий и
дизайна, 2ssdmit@gmail.com

ДМИТРИЕВА
Ирина Николаевна
студент группы ИКТЗ-31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
renedmitrieva@yandex.ru

ДОБРАЯ
Олеся Павловна
студент группы Р-32м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
olesadobraa@gmail.com

ДОВГАЛЕВ
Федор Владимирович
студент группы БИМ-21з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
fedor.tvgu@gmail.com

ДОГАДАЕВ
Андрей Сергеевич
студент группы ИКТБ-37м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
a.dogadaeff2001@yandex.ru

ДОЛЯ Александра Дмитриевна — студент группы ИСТ-231М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, A9977007@yandex.ru

ДОМБРОВСКИЙ Роман Михайлович — студент группы ИКТБ-37М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, skillers-dea186@yandex.ru

ДОМОТЫРКО Вячеслав Станиславович — студент группы ИКТС-22 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, greenbaubab@bk.ru

ДРЕПА Владислав Евгеньевич — студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladikdrepa@mail.ru

ДУБАКОВ Александр Владимирович — студент группы РТ-22м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sanek-dubakov@mail.ru

ДУБОВИКОВ Лев Олегович — студент группы ИКТС-01 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, levdubovikov0808@gmail.com

ДУНАЕВ Николай Павлович — аспирант кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ndunaev@inbox.ru

ДУНИЧЕВ
Александр Петрович
студент группы ИБС-21
Санкт-Петербургского государственного университета телекоммуникаций им. профессора М. А. Бонч-Бруевича, vdidpd9@gmail.com

ДЮДИН
Антон Иванович
студент группы РМ-02
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, atos-svet33@mail.ru

ДЮСМЕТОВА Азалия Айдаровна
студент группы ИКБ-02
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dyusmetova_azaliya@mail.ru

ДЯТЧЕНКО
Анастасия Андреевна
студент группы ИКТЗ-21м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dyatchenko-a@kiszi.ru

ЕВСТАФЬЕВ
Михаил Викторович
студент группы ИБТС-31
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,aensidh0@gmail.com

ЕГОРОВ
Никита Андреевич
студент группы ИКТС-23
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Egorna1990@mail.ru

ЕГОРОВА
Марина Александровна
кандидат экономических наук, доцент кафедры управления и моделирования в социально-экономических системах Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egorova-mak@yandex.ru

ЕГОРОВА
Полина Юрьевна
студент группы ИКБ-22
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
egorovaPU@yandex.ru

ЕДЕМСКАЯ
Екатерина Дмитриевна
студент группы ИКТБ-28м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
ekaterina.edemskaya51@gmail.com

ЕЖУРОВ
Антон Павлович
студент группы ИСТ-241м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
aezhurov90@mail.ru

ЕЛАГИН
Василий Сергеевич
кандидат технических наук, доцент, заведующий
кафедрой инфокоммуникационных систем
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, elagin.vas@gmail.com

ЕЛИСЕЕВА
Елизавета Вадимовна
студент группы РСМ-21з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
lizeevallisssa@mail.ru

ЕМЕЛЬЯНЕНКО
Георгий Юрьевич
студент группы ИКТБ-38м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
gogoshanin2000@gmail.com

ЕРМАЧКОВА
Мария Владиславовна
студент группы 4-МДА-7
Санкт-Петербургского государственного
университета промышленных технологий и
дизайна, ermachkova.mari@bk.ru

ЕРЧУКОВ
Илья Игоревич
студент группы Р-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 1looha@mail.ru

ЖЕРТОВСКАЯ
Алина Андреевна
студент группы ИКБ-23 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alya.zhertovskaya@mail.ru

ЖИЛЯКОВ
Глеб Витальевич
студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zgv00@bk.ru

ЖИРЯКОВ
Владимир Петрович
студент группы РЦТ-03 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimir.zhiriakov@gmail.com

ЗАВЬЯЛОВ
Артём Андреевич
студент группы ИКБ-24 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pobedablok@gmail.com

ЗАГРЕБАЕВА
Надежда Михайловна
студент группы ЭБМ-11з, Институт непрерывного образования Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ), nzagrebaeva12@gmail.com

ЗАНОЗИН
Егор Витальевич
студент группы РМ-02 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egor.zanozin@gmail.com

ЗАРУБИН
Иван Максимович
студент группы РК-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivanzar.bonch@yandex.ru

ЗАХАРОВА Марина Михайловна — студент группы ИКБ-25 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, efizmor@gmail.com

ЗЕБЗЕЕВ Егор Алексеевич — студент группы ИКТЗ-21М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zebzeev.avis@gmail.com

ЗИКРАТОВ Игорь Алексеевич — доктор технических наук, профессор, декан факультета информационных систем и технологий, профессор кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, zikratov.ia@sut.ru

ЗЛОБИН Олег Николаевич — студент группы ИСТ-012 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, olegzlobin00@mail.ru

ЗОЛОТОРЁВА Анастасия Игоревна — студент группы ИКБ-25 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, miss.asyaZ@mail.ru

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 ИКТБ-38м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, juliatee777@gmail.com

ИГНАТЬЕВА
Дарья Александровна
студент группы ИКТЗ-21м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
miss.ignateva.14@mail.ru

ИЛЬИН
Ярослав Александрович
студент группы ИКТБ-38м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
jaroslav.ilin@gmail.com@mail.ru

ИСМАИЛОВ
Айхан Нураддинович
студент группы ИСТ-251м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
ayxan8911@mail.ru

КААДЗЕ
Никита Тамазович
студент группы ИКТО-07
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича

КАЗАНЦЕВ
Алексей Анатольевич
старший преподаватель кафедры защищенных
систем связи Санкт-Петербургского
государственного университета
телекоммуникаций им. проф. М.А. Бонч-
Бруевича, kazantsev.ikss@yandex.ru

КАЗАНЦЕВА
Анна Геннадьевна
кандидат технических наук, доцент кафедры
экологической безопасности телекоммуникаций
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М.А.
Бонч-Бруевича, Kazanutik@mail.ru

КАЛИМУЛЛИН
Азат Русланович
студент группы ИКТС-23
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
azat_kalimullin_2017@mail.ru

КАЛИМУЛЛИНА
Ольга Валерьевна
кандидат экономических наук, доцент кафедры управления и моделирования в социально-экономических системах Санкт-Петербургский государственный университет телекоммуникаций им. профессора М. А. Бонч-Бруевича

КАМУЕЖИ
Йури Гашпар
студент группы ИКТМ-22м
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
yuricamuegi@gmail.com

КАРАХАНОВА
Екатерина
Константиновна
студент группы ИКТГ-34м
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
k.karakhanova@yandex.ru

КАШИРИН
Павел Геннадьевич
студент группы ИКТС-22
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Baryshnikov101@yandex.ru

КИРИК
Дмитрий Игоревич
декан факультета радиотехнологий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, d_i_kirik@mail.ru

КИРИЛОВА
Диана Сергеевна
студент группы ИКТЗ-31м
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича, dianka-kirilova-2001@mail.ru

КИСЕЛЁВ
Виктор Павлович
студент группы ИСТ-251м
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Vkisel102@yandex.ru

КИСЛЯКОВ
Сергей Викторович
кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, s.v.kislyakov@gmail.com

КЛИМОВ
Тимофей Алексеевич
студент группы ИБС-21
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Nbvjatqrkbvjd2@mail.ru

КЛЫКОВ
Данила Дмитриевич
студент группы Р-31м
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
danilaklykov@gmail.com

КНИГИНИЦКИЙ
Егор Игоревич
студент группы ФП-21м
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
egor.knig@yandex.ru

КНЫШЕНКО
Сергей Сергеевич
студент группы ИКТС-21 Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Knyshenk0@gmail.com

КОВАЛЕВА
Александра Александровна
студент группы ИКТБ-38м Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
niktoto2002@mail.ru

КОВАЛЕНКО
Даниил Данилович
студент группы ИКТР-21
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
dankosteve@yandex.ru

КОЗЛОВА
Анастасия Алексеевна
студент группы ИКТУ-03
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
nastak452@yandex.ru

КОЛЕСНИКОВ
Михаил Сергеевич
студент группы ИКТ-35
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
mkolles26@gmail.com

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
кафедры конструирования и производства
радиоэлектронных средств Санкт-
Петербургского государственного университета
телекоммуникаций им. проф. М.А. Бонч-
Бруевича, agkolosko@mail.ru

КОЛЫБЕЛЬНИКОВ
Николай Юрьевич
студент группы ИКТС-01
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, ya.nikolai.kolyb@gmail.com

КОНАК
Владимир Евгеньевич
студент группы 3-МД-16
Санкт-Петербургского государственного
университета промышленных технологий и
дизайна, superliquid344@gmail.com

КОНДРАТЮК
Михаил Александрович
студент группы РК-32
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
mihak8993@gmail.com

КОНОПЛЁВА
Анастасия Владимировна
студент группы ЭП-21м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
konopleva1209@mail.ru

КОНТОРОВ
Владимир Федорович
студент группы ИБТС-31
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Kontorov22@mail.ru

КОНЬКОВ
Владимир Владимирович
студент группы ИКТБ-37м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М.А.Бонч-Бруевича,
No0boT2001@mail.ru

КОПП
Максим Юрьевич
студент группы ИСТ-232М
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича
koppmax03@gmail.com

КОПЫЛОВА
Юлия Владимировна
студент группы РСМ-21з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича, ulyalion@mail.ru

КОРОБЕЙНИКОВ
Александр Николаевич
студент группы ФП-02
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
korablik604@gmail.com

КОРОВИН
Константин Олегович
кандидат физико-математических наук,
заведующий кафедрой радиосистем и обработки
сигналов, доцент Санкт-Петербургского
государственного университета
телекоммуникаций им. проф. М.А. Бонч-
Бруевича, korovin.ko@sut.ru

КОРОЛЕВСКИЙ
Константин Юрьевич
студент группы ИСТ-212М
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
K-korolevskiy@mail.ru

КОРШУНОВ
Илья Дмитриевич
студент группы 3-МД-16
Санкт-Петербургский государственный
университет промышленных технологий и
дизайна, ilyakors2003@gmail.com

КОСТАНДОВ
Максим Кириллович
студент группы ИБТС-3
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
kmk.78rus@gmail.com

КОТОВ
Виктор Иванович
кандидат технических наук, доцент кафедры
управления и моделирования в социально-
экономических системах, Санкт-Петербургского
государственного университета
телекоммуникаций им. проф. М. А. Бонч-
Бруевича kotov-vi@yandex.ru

КОТОВ
Тимофей Алексеевич
студент группы ИКТС-22
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
kotoff201211@gmail.com

КОЧЕРЁЖКИНА
Ульяна Александровна
студент группы ЭП-31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
uliana.kch51@gmail.com

КРАВЕЦ
Елена Валентиновна
кандидат технических наук, доцент кафедры
радиосвязи и вещания, Санкт-Петербургского
государственного университета
телекоммуникаций им. проф. М.А. Бонч-
Бруевича, helen-kravetz@yandex.ru

КРАВЦОВА
Анастасия Алексеевна
студент группы ИСТ-232М
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, nastya-kravtcova21@mail.ru

КРАВЦОВА
Валерия Андреевна
студент группы ИКТЗ-31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
kravtsova_valeria@mail.ru

КРАХМАЛЕВ
Дмитрий Сергеевич
студент группы ИСТ-341м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
dpixdxd@yandex.ru

КРЕПАК
Владислав Викторович
студент группы РСО-31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
vkrep77@gmail.com

КРЕСТЬЯШИН
Никита Антонович
студент группы ИКТБ-28м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
gamer_enot@mail.ru

КУДИНОВ
Александр Сергеевич
студент группы ИКТС-23
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Sashakud205@gmail.com

КУЗЬМИН
Григорий Алексеевич
студент группы ИБТС-31
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
kuzmin.gk@gmail.com

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, kukunin.ds@sut.ru

КУЛАКОВ
Алексей Сергеевич
студент группы ИСТ-211м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kulakovalexey@hotmail.com

КУЛАКОВ
Евгений Михайлович
студент группы РСО-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, evgeniy.kulakov.2002@mail.ru

КУЛИКОВ
Сергей Павлович
старший преподаватель Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kulikov.sp@sut.ru

КУЛЬНАЗАРОВА
Анастасия Витальевна
доцент, кандидат политических наук, заместитель декана социальных цифровых технологий по воспитательной работе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kulnazarova.av@sut.ru

КУРМАНОВ
Илья Олегович
студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, iluhakurmanov@gmail.com

КУРНОСОВ
Валерий Игоревич
доктор технических наук, профессор кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университет Телекоммуникаций им. профессора М. А. Бонч-Бруевича, vi-kurnosov@mail.ru

КУТУЕВ
Тимур Тагирович
студент группы ИКТЗ-31м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Afanimmailab@gmail.com

ЛАВРОВ
Максим Николаевич
студент группы РТ-21м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Lavrov_mn@mail.ru

ЛАЗАРЕВ
Илья Владленович
студент группы ИКТС-23
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Lazarew2004@gmail.com

ЛАКОМКИНА
Елена Александровна
студент группы ИСМ-11з
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,
vip.lakomkina@mail.ru

ЛЕБЕДЕВ
Максим Павлович
студент группы РСО-31м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,
maxf003008@yandex.ru

ЛЁВКИНА
Лилия Сергеевна
Студент группы БИМ-213
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, llevkinaa@mail.ru

ЛЕВЧЕНКО
Владислава Витальевна
студент группы РСМ-21з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
levchenko_vladislava@bk.ru

ЛЕШУКОВА
Анастасия Михайловна
студент группы ИКТБ-28м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
n.leshukova98@mail.ru

ЛИКОНЦЕВ
Алексей Николаевич
кандидат технических наук, доцент кафедры
радиосистем и обработки сигналов Санкт-
Петербургского государственного университета
телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
likoncev.an@sut.ru

ЛИМОНОВ
Михаил Иванович
студент группы ИКБ-23
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича, mlimnov@mail.ru

ЛИСЕЦКИЙ
Андрей Петрович
студент группы ИБС-12
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
lisetskiy.ap@gmail.com

ЛИТВИНОВ
Владислав Леонидович
кандидат технических наук, доцент, доцент
кафедры информационных управляющих систем
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, vlad.litvinov61@gmail.com

ЛОБАНОВ
Кирилл Алексеевич
студент группы ИКТС-21
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-
Бруевича,kirieel24@gmail.com

ЛОБОДИНА
Елизавета Артемовна
студент группы 4-мда-9 Санкт-Петербургского государственного университета промышленных технологий и дизайна, jkzerz@mail.ru

ЛОГИНОВСКАЯ
Алена Николаевна
кандидат географических наук, доцент кафедры экологической безопасности телекоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aloginovskaja@bk.ru

ЛОНШАКОВ
Максим Андреевич
студент группы ИКТС-22 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, lonsakov66@gmail.com

ЛОПАТКИН
Кирилл Алексеевич
студент группы 3-МД-16 Санкт-Петербургского государственного университета промышленных технологий и дизайна, lopatkin23@inbox.ru

ЛОХОВ
Денис Александрович
студент группы ИКТИ-25м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, ldenis.17@bk.ru

ЛЮБАЩЕНКО
Тимофей Дмитриевич
студент группы ИКТЗ-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tima17.03@mail.ru

МАВРИЧЕВ
Вячеслав Константинович
студент группы ИСМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mavrichevvk@gmail.com

МАКАРОВ
Владислав Алексеевич
студент группы РК-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladmakarov2505@mail.ru

МАКАРОВ Леонид Михайлович	кандидат технических наук, доцент, доцент кафедры интеллектуальных систем автоматизации и управления Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, makarov.lm@sut.ru
МАКАРОВА Александра Константиновна	студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Alex-ecureuil@mail.ru
МАКИНА Милена Алексеевна	студент группы ЭБМ-31з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, makina.milena@mail.ru
МАКОВЧИК Дарья Вячеславовна	студент группы РМ-02 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dasha.makov4ik@yandex.ru
МАКСИМОВ Александр Максимович	студент группы РМ-02 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alex.maximov9@yandex.ru
МАКСИМОВА Анна Валерьевна	студент группы РТ-01 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maksimova16anya@gmail.com
МАКСИМОВА Серафима Вячеславовна	студент группы ИСТ-232М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, simamaximoff@gmail.com
МАЛАНИЯ Марк Тимурович	студент Санкт-Петербургского государственного университета промышленных технологий и дизайна, markmalaniya2015@mail.ru

МАЛЕЕВ
Демид Андреевич
студент группы ИСТ-232м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
demid.maleev@inbox.ru

МАЛКОВ
Тихон Александрович
студент группы ИСТ-232м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
tihon1240@gmail.com

МАЛЮГИНА
Ольга Валентиновна
студент группы БИМ 21-з
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, MalyuginaOV@yandex.ru

МАМОНОВ
Матвей Алексеевич
студент группы РЦТ-03
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
matveikamamonov@yandex.ru

МАРИИНСКАЯ
Александра Павловна
старший преподаватель кафедры иностранных и
русского языков Санкт-Петербургского
государственного университета
телекоммуникаций им. проф. М.А. Бонч-
Бруевича, a.marinskaya@mail.ru

МАРИНОВА
Виктория
Константиновна
студент группы ИКТС-91
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, vi.marinova@yandex.ru

МАРОЧКИН
Даниил Алексеевич
студент группы 4-МДА-9
Санкт-Петербургского государственного
университета промышленных технологий и
дизайна, town.kor@gmail.com

МАРТЫНЕНКО
Даниил Романович
студент группы ИКБ-21
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
dama,mart@mail.ru

МАСЮТИН
Михаил Дмитриевич
студент группы ИКТБ-38м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, capslock228322@gmail.com

МАТВЕЕВ
Егор Сергеевич
студент группы ИСТ-241м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yatutallo09@gmail.com

МАТВЕЕВА
Вероника Олеговна
студент группы БИН-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

МАТУКАС
Марюс Ромасович
студент группы Иктг-24м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maryusmatukas@mail.ru

МАХОРИН
Андрей Сергеевич
студент группы ИКТБ-38м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gadget2001@yandex.ru

МАШОШИН
Евгений Сергеевич
студент группы ИСТ-232м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pb@svyatmtk0.ru

МЕДВЕДЕВ
Дмитрий Сергеевич
студент группы ИСТ-211м, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ds1000one@gmail.com

МЕЛЬНИЧЕНКО
Александра
Александровна
студент группы ИКТК-01 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, llucidev@gmail.com

МИНАЕВ Никита Витальевич — студен группы ИКМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, inikitam98@gmail.com

МИНЕЕВА Варвара Дмитриевна — студент группы ИКТГ-24м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, varvaramineyeva@gmail.com

МИНОХОВ Кирилл Владимирович — студент группы ИБС-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, redblackdragon1246@gmail.com

МИРЗАГАЛИМОВ Булат Маратович — студент группы ИСТ-232м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, truebulat@yandex.ru

МИРЗАЛИЕВ Эмин Эдикович — студент группы 3-МД-16 Санкт-Петербуржского государственного университета промышленных технологий и дизайна, eminmirzaliev297@gmail.com

МИТИН Егор Олегович — студент группы ИКТС-23м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egor.mitin.2000@mail.ru

МИТРОФАНОВА Ксения Юрьевна — студент группы РСМ11з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ks_mitt@mail.ru

МИХАЙЛОВА Зоя Владимировна — студент группы РК-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, wzeymix@gmail.com

МИЦКЕВИЧ
Анатолий Андреевич
студент группы РК-01
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича, kuna2014@bk.ru

МИШКИНА
Диана Олеговна
студент группы БИМ-21з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Mishkina_d@mail.ru

МОКРОУСОВА
Ксения Сергеевна
студент группы 3145401/20101
Санкт-Петербургского политехнического
университета Петра Великого,
ksuha.kseniya@gmail.com

МОХАМАДИ
Раша
студент группы БИ-21м
Санкт-Петербургский государственный
университет телекоммуникаций
им. профессора М. А. Бонч-Бруевича

МУРАВЬЕВ
Максим Игоревич
студент группы 4-МДА-7
Санкт-Петербургского государственного
университета промышленных технологий и
дизайна, hayhaymuravey@gmail.com

МУСАЕВА
Татьяна Вагифовна
кандидат технических наук, доцент, доцент
кафедры информатика и компьютерный дизайн
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, neli_6868@mail.ru

НАДЕЖДА
Михайловна Загребаева
студент группы ЭБМ-11з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
nzagrebaeva12@gmail.com

НАЗАРОВ
Илья Викторович
студент группы ЭП-21м
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, ilnaz5@icloud.com

НАУМОВА
Татьяна Дмитриевна
студент группы 4-мда-9
Санкт-Петербургского государственного университета промышленных технологий и дизайна, naumovatd@gmail.com

НЕВ
Даниил Артемович
студент группы РТ-21м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nevdaiil3112@gmail.com

НЕФЕДОВ
Даниил Ильич
студент группы ИСТ232-м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ne.danyalll@gmail.com

НЕЧАЕВ
Андрей Александрович
студент группы ИКТБ-27м
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
lcme.nechaev@mail.ru

НИКИТИН
Юрий Александрович
кандидат технических наук, старший научный сотрудник, доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, yuriyan@list.ru

НИКИФОРОВ
Виталий Сергеевич
студент группы ИКТС-21
Санкт-Петербургского
государственного университета
телекоммуникаций им.
проф. М. А. Бонч-Бруевича
Nikiforov123@outlook.com

НИКИФОРОВ
Семён Сергеевич
студент группы ИКТИ-25м
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
semion1999@mail.ru

НИКОНОВ
Евгений Русланович
студент группы ИКТБ-27м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
NIKKSTUDIO3023@gmail.com

НОВИКОВ
Дмитрий Сергеевич
студент группы ИКТБ-38м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
frogy3228@gmail.com

НОВОРУССКИЙ
Владимир Валерьевич
студент группы РСМ-21з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
novorusskiyv@gmail.ru

ОВСЯННИКОВ
Егор Борисович
студент группы 2-МГ-56
Санкт-Петербургского государственного
университета
промышленных технологий и дизайна,
ovsiannickov.egor@yandex.ru

ОЛЕЙНИК
Артём Александрович
студент группы ИКТБ-37м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А.Бонч-Бруевича,
artem186oleynik@gmail.com

ОНОПРИЕНКО
Вячеслав Владиславович
студент группы РТ-01
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
slava_v_o@mail.ru

ОСИПОВ
Родион Владимирович
студент группы ИБС-23
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
rodion20049@mail.ru

ОСМАНОВ Джамалутдин Магомедмухтарович — студент группы ИКТС-23м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, dzamalutdinosmanov@gmail.com

ОХЛОПКОВА Юлия Владимировна — студент группы ИКБ-22 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, uliaohlopkova6538@gmail.com

ПАВЛЕНКО Александр Сергеевич — студент группы 4-МДА-9 Санкт-Петербургского государственного университета промышленных технологий и дизайна, Alex-Pavlenko-net-2013@yandex.ru

ПАВЛОВСКАЯ Анна Александровна — студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anna_pavll@mail.ru

ПАВЛОВСКИЙ Михаил Валентинович — студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anna_pavll@mail.ru

ПАВЛЮЧЕНКОВ Никита Андреевич — студент группы ИКТР-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pavlyuchenkov1509@mail.ru

ПАНКОВ Арсений Владимирович — студент группы 236А-23 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, k777tt@gmail.com

ПАНКОВА
Елизавета Анатольевна
студент группы ИКТС-91
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pankova.lizaveta@yandex.ru

ПАНФИЛОВ
Андрей Александрович
студент группы 2-МГ-56
Санкт-Петербургского государственного университета промышленных технологий и дизайна, andreypanfilov73@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

ПАСТУХОВ
Владислав Васильевич
студент группы ИКБ-04
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pastukhov_vlad2002@mail.ru

ПЕНЗОВСКАЯ
Елена Серегеевна
студент группы ИКБ-25
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, l.pes.0502@mail.ru

ПЕРЕВЫШКО
Александра Сергеевна
аспирант группы 231А-22
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, milashka-spaiki@yandex.ru

ПЕРМИНОВА
Яна Александровна
студент группы ИКТЗ-21м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, permino@inbox.ru

ПЕРЦЕВ
Даниэль Сергеевич
студент группы ИБС-21
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pdsnu@mail.ru

ПЕСТОВ
Игорь Евгеньевич
доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ip@sut.ru

ПЕТРИВ
Роман Богданови
старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, roman.petriv@mail.ru

ПЕТРОВ
Дмитрий Валерьевич
студент группы ИСМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, snowmandexter@gmail.com

ПЕТРОВ
Михаил Андреевич
студент группы ЭП-31м Санкт-Петербургского Государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, vbifvbif21@mail.ru

ПЕТРОВ Павел Евгеньевич
студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, petrulya_2000@mail.ru

ПЕТРОВ
Павел Сергеевич
студент группы ИКТС-03 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mrfreejgg@gmail.com

ПЕТРОВА
Татьяна Сергеевна
студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 9992125013@mail.ru

ПЕТРОВСКАЯ
Полина Эдуардовна
студент группы ИСМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pp1811@mail.ru

ПИЛИЩУКОВ Глеб Андреевич — студент группы ИСТ-341м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gleb-1800501@mail.ru

ПОБЕГАЛОВА Валерия Витальевна — студент группы ИСТ-232м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pobegalova.vv@gmail.com

ПОДЛЕВСКИХ Антон Павлович — студент группы РТ-22м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, podlevskikh.anton@gmail.com

ПОЛОЗЕНКО Иван Дмитриевич — студент группы ИКТС-22 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, v-polozenko@mail.ru

ПОЛУХИН Илья Алексеевич — студент группы ИКТС-22 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,polukhinjuja@yandex.ru

ПОЛЯКОВ Александр Иванович — студент группы Р-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича a.polak5555@gmail.com

ПОЛЯНИЧЕВА Анна Валерьевна — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, polyanicheva.av@sut.ru

ПОПКОВ
Святослав Витальевич
студент группы Р-31м
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, Slavik.Popkov@gmail.com

ПОПОВ
Александр
Александрович
студент группы Р-31м
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, UncleRainFace@yandex.ru

ПОПОВИЧ
Сергей Игоревич
студент группы РТ-22м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
sergpopowich@mail.ru

ПОПОНИН
Антон Сергеевич
инженер-программист ООО "Естественный
Интеллект", apoponin@naint.ru

ПОТОМАКО
Денис Олегович
студент группы ИКТБ-27м
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М.А.
Бонч-Бруевича, den.potomako@mail.ru

ПРАВДИН
Андрей Алексеевич
студент группы ИКПИ-01
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, andreypravdin52@gmail.com

ПРОНИЧЕВ
Владислав Дмитриевич
студент группы ИКТБ-37м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
nggajloy@gmail.com

ПРОХОРОВ
Иван Романович
студент группы ИСМ-11з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
zadiac_www@mail.ru

ПУГАЧ
Мария Степановна
студент группы РД-01
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.

Бонч-Бруевича, maashusik@ya.ru

ПУЧКОВ
Владимир Викторович — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, puchkov-81@bk.ru

ПЫЛАЕВ
Вадим Евгеньевич — студент группы ИКТО-07 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vadik.pylaev@mail.ru

РАКОВСКИЙ
Олег Владимирович — кандидат технических наук, доцент, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

РЕЗНИКОВ
Богдан Константинович — старший преподаватель кафедры фотоники и линий связи, преподаватель кафедры специальные средства связи, старший преподаватель кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, rznkff@net.sut.ru

РИДАЛЬ
Иван Викторович — студент группы ИСМ-11з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, neatsketch@gmail.com

РОДИОНОВ
Артем Леонидович — студент группы ИКПИ-02 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rodionov.artem.for.docs@gmail.com

РОМАНОВА
Алина Анатольевна — студент группы ИСТ-232м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aln.rom@mail.ru

РОМАНОВА
Екатерина Александровна
студент группы РТ-32м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
c.romanova712@gmail.com

РОМАНЮК
Егор Олегович
студент группы ИКТБ-27м
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, pomidorych2000@gmail.com

РУДЕНКО
Сергей Андреевич
студент группы ИКТБ-38м
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича,
rudenkosergeyandreevich01@mail.ru

РУФОВ
Максим Алексеевич
студент группы ИКТС-03
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, maxnator2@gmail.com

РЮТИН
Константин Евгеньевич
студент группы Р-22м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
ryutin.sut@gmail.com

РЯБИКОВ
Дмитрий Сергеевич
студент группы РТ-22м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
dmitryryabickov@yandex.ru

САЛЧАК
Батый Бакчапович
студент группы ИКТС-21
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
batyibatyi1707@gmail.com

САМАРИН
Владимир Васильевич
студент группы Р-12
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
samarin.vladimir163@gmail.com

САМОХИН
Григорий Андреевич
студент группы 4-МДА-9
Санкт-Петербургского государственного
университета промышленных технологий и
дизайна, grig.samoxin2002@yandex.ru

САРАЗОВА
Инна Александровна
студент группы 4-МДА-7
Санкт-Петербургского государственного
университета промышленных технологий и
дизайна, sarazova.inna04@mail.ru

САФРАНОВСКИЙ
Арсений Игоревич
студент группы РСО-31м Санкт-Петербургского
государственного университета
телекоммуникаций им. проф. М. А. Бонч-
Бруевича, asftwists@yandex.ru

САФРОНОВА Мария
Михайловна
студен Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича ,
Mashulya34555@gmail.com

СВЕТОВА
Анастасия Васильевна
студент группы ИКТГ-34м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
nastya_sv00@mail.ru

СЕВОСТЬЯНОВ
Владислав Андреевич
студент группы 236А-23
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, vlad08007@hotmail.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

СЕМЕНОВ Максим Эдуардович	студент группы ИКТС-22 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,ababadcdc@yandex.ru
СЕРАФИМОВИЧ Катарина Сергеевна	студент группы ИКТС-23 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, katarixa@mail.ru
СЕРГЕЕВ Николай Алексеевич	студент группы ИСТ-232м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, www_nick2690@mail.ru
СЕРЕДКИН Егор Вадимович	студент группы 3145401/20101 Санкт-Петербургского Политехнического Университета Петра Великого, surfacemtgs@gmail.com
СИНЕЛЬЩИКОВ Владимир Сергеевич	студент группы ИКТБ-38м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vov4kman@gmail.com
СИТНИКОВ Фёдор Антонович	студент группы ИБС-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fyodorsit@yandex.ru
СКАКУНОВ Игорь Рустамович	студент группы ИКТГ-24м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ighor.skakunov@mail.ru
СКОРОДУМОВ Никита Витальевич	студент группы 3-МД-16 Санкт-Петербургского государственного университета промышленных технологий и дизайна, snvwork11@gmail.com

СЛАВУЦКИЙ
Дмитрий Сергеевич
студент группы ИКТО-07
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
dimaslav2001@gmail.com

СЛЕПОГИН
Антон Юрьевич
студент группы ИКТФ-26м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
antoha0517@mail.ru

СЛЕСАРЕНКО
Валерия
студент группы ИСТ-331м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
titaniya348@gmail.com

СМИРНОВ
Дементий Петрович
студент группы РМ-01
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
dementiy.2002@gmail.com

СМИРНОВА
Алёна Алексеевна
студент группы ИКТГ-24м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
alena_a.smirnova@mail.ru

СМИРНОВА
Дина Андреевна
студент группы ФП-31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
sm.dina.a@yandex.ru

СМОРОДИН
Геннадий Николаевич
кандидат технических наук, доцент кафедры
информационных управляющих систем Санкт-
Петербургского государственного университета
телекоммуникаций им. проф. М.А. Бонч-
Бруевича, gsmorodin@gmail.com

СМОРОДИНА
Арина Геннадиевна
студент группы БМБ2304С
Национального исследовательского университета «Высшая школа экономики», arina.smorodina@gmail.com

СМУРОВ
Илья Александрович
студент группы ИКТБ-28м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ismurov@mail.ru

СОЛОВЬЕВ
Александр Сергеевич
студент группы ИКПИ-02
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, solovwork@ya.ru

СОЛОВЬЕВ
Артем Сергеевич
студент группы ИСМ-11з
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.solovev.add@gmail.com

СОЛОВЬЕВА
Дарья Евгеньевна
студент группы ИСТ-331м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, de.solov@mail.ru

СПИРИДОНОВ
Даниил Петрович
студент группы ИКТБ-38м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tank891000@gmail.com

СТАРИЦЫН
Никита Евгеньевич
студент группы РК-31м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, forbusiness2303@mail.ru

СТАРШЕВ
Роман Андреевич
студент группы ИКБ-24
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman.starshev@mail.ru

СТАЦЕНКО Евгений Александрович	студент группы РСО-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, radianc8@mail.ru
СТЕПАНОВ Александр Михайлович	студент группы ИКТИ-25м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, salex14082000@gmail.com
СТЕПАНОВ Максим Петрович	студент группы ИКТЗ-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mack.stepanow2001@gmail.com
СТЕПУРОВА Ульяна Игоревна	студент группы РСО-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ulianastepurova@mail.ru
СТРЕЛЬНИКОВ Валентин Максимович	студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vel4onok@mail.ru
СТУКАЛОВ Артем Николаевич	студент группы 3-МД-16 Санкт-Петербургского государственного университета промышленных технологий и дизайна, stukalov.artiom@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
СУРОВЕГИН Михаил Константинович	студент группы БИМ-11з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lokonosto@yandex.ru

СУХОМЛИНОВ
Даниил Игоревич
студент группы ИКТС-33м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
d.sukhomlinov.spb@gmail.com

СУЯРГУЛОВ
Иван Маратович
студент группы ИКТС-23
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-
Бруевича,suyargoolov@gmail.com

ТАКАН
Дмитрий Гарипович
студент группы ИБС-23
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
sdima8823@gmail.com

ТАЛАКИН
Евгений Николаевич
студент группы ИКТЗ-31м
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, tj91@bk.ru

ТАМБОВСКИЙ
Александр Николаевич
студент группы ИКТБ-37м
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М. А.
Бонч-Бруевича, tambovskii.aleksandr00@mail.ru

ТАРАСОВ
Владимир Анатольевич
старший преподаватель Санкт-Петербургского
государственного университета
телекоммуникаций им. проф. М. А. Бонч-
Бруевича. vat-liquidator@bk.ru

ТАРАСОВ
Владимир Владимирович
студент группы РК-31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
vovataradov16@gmail.com

ТАРАТЫНОВ
Иван Дмитриевич
студент группы ИКТБ-37м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
ivantar28@yandex.ru

ТАТАРЕНКОВ
Дмитрий Александрович — старший преподаватель кафедры телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, tatarenkov.da@sut.ru

ТИХОНОВ
Алексей Максимович — студент группы ИКТГ-24м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexeyushaki@yandex.ru

ТКАЧ
Глеб Александрович — студент группы ИКБ-23 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tkach.gleb@mail.ru

ТРЕЗОРОВ
Владислав Игоревич — студент группы ИКТЗ-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, trezorov.v.i@yandex.ru

ТРИАНДАФИЛИДИ
Иоанис Иванович — студент группы ИСТ-211м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mr.ioanis@gmail.com

ТУКМАЧЕВА
Марина Алексеевна — адъюнкт факультета подготовки кадров высшей квалификации Санкт-Петербургского университета государственной противопожарной службы МЧС России, mtukmacheva@mail.ru

ТУР
Виктор Сергеевич — студент группы 2-МГ-56 Санкт-Петербургского государственного университета промышленных технологий и дизайна, t1tusique@gmail.com

УЛЬЯНОВСКИЙ
Дмитрий Андреевич
студент группы ИБС-21
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
d1isikea@gmail.com

УПОРОВ
Михаил Евгеньевич
студент группы ЭП-31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
m.uporov@mail.ru

УРГАЛКИНА
Кристина Алексеевна
студент группы БИМ-21з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
k.urgalkina@mail.ru

УРСЕГОВ
Андрей Константинович
студент группы ИКТЗ-21М
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
aursegov000@gmail.com

УШАКОВ
Игорь Александрович
кандидат технических наук, доцент кафедры
защищенных систем связи Санкт-Петербургского
государственного университета
телекоммуникаций им. проф. М. А. Бонч-
Бруевича, ushakov.ia@sut.ru

УШАНЁВ
Кирилл Игоревич
студент группы ИБС-22
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-
Бруевича,kirill.u2003@mail.ru

УШКОВА
Ирина Геннадьевна
студент группы Р-22м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
ushkova.irina2015@yandex.ru

ФЕДОРОВ
Сергей Леонидович
кандидат технических наук, доцент кафедры телевидения и метрологии, заведующий кафедрой телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича, sergey.fedorov@sut.ru

ФЕДОРОВ
Павел Олегович
аспирант группы 236А-23 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pavel_lenin@mail.ru

ФЁДОРОВА
Алина Владимировна
начальник отдела аспирантуры и докторантуры, кандидат экономических наук, доцент кафедры информатики и компьютерного дизайна, fav111@yandex.ru

ФЕДОРОВА Екатерина Сергеевна
студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ek.chukina@yandex.ru

ФЕДОРОВА
Злата Анатольевна
студент группы ИКТ3-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, ZF_sweetday@mail.ru

ФЕДОРЧЕНКО
Елена Владимировна
кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича

ФИЛИПОВ
Александр Сергеевич
студент группы ИБС-23 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sasha.filipow2014@gmail.com

ФИЛИПОВ
Эдуард Олегович
студент группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, filipov.edick@gmail.com

ФИЛИППОВ
Феликс Васильевич
кандидат технических наук, доцент кафедры Информационных Управляющих Систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, 9000096@mail.ru

ФЛЕЙШМАН
Алексей Андреевич
студент группы ЭП-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевич, alex2zoro@mail.ru

ФОКИН
Григорий Алексеевич
доктор технических наук, доцент кафедры инфокоммуникационных систем, преподаватель кафедры РСиВ Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, harley_84@mail.ru

ФОМИЧЕВ
Виталий Артурович
студент группы 4-МДА-9 Санкт-Петербургского государственного университета промышленных технологий и дизайна, vitalifting2@mail.ru

ХАМЕД
Мохамед Махфуд
студент группа 4-МДА-7 Санкт-Петербургского государственного университета промышленных технологий и дизайна

ХАПСИРОКОВ
Валерий Асланович
студент группы ИСТ-231м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, valerykhapsirokov@gmail.com.

ХАЧАТРЯН
Армине Арамовна
студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, armine4.khachatryan@gmail.com

ХИМЕНКОВА
Дарья Андреевна
студент группы РМ-02
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
khimenkovad@gmail.com

ХОДАНОВИЧ
Александр Иванович
доктор педагогических наук, профессор кафедры
информационных управляющих систем Санкт-
Петербургского государственного университета
телекоммуникаций им. проф. М.А. Бонч-
Бруевича, akhodanovich@yandex.ru

ХОДОВ
Михаил Дмитриевич
студент группы ИКБ-25
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
miha-266@mail.ru

ЦВЕТКОВА
Ирина Юрьевна
студент группы ЭП-31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
IrinaTcvetkovaa@gmail.com

ЦИТРИН
Владислав
Александрович
студент группы ИКТС-23
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
vladushats@mail.ru

ЦЫГОНЯЕВА
Александра Юрьевна
кандидат философских наук, доцент кафедры
истории и регионоведения Санкт-Петербургского
государственного университета
телекоммуникаций им. проф. М. А. Бонч-
Бруевича, tau-85@mail.ru

ЧАХИР
Арина Александровна
студент группы 4-МДА-7
Санкт-Петербургского государственного
университета промышленных технологий и
дизайна, chahir.arina@yandex.ru

ЧЕМОДУРОВ
Данила Дмитриевич
студент группы ИКТС-22 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, danila.chemodurov@yandex.ru

ЧЕРНИК
Ярослав Вячеславович
студент группы ИКТБ-38м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, guronx@yandex.ru

ЧЕРНОВ
Игорь Николаевич
старший преподаватель кафедры радиосистем и обработки сигналов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,full41@bk.ru

ЧЕРНОВ
Максим Денисович
студент группы Р-12 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maksimantchernov@yandex.ru

ЧЕРНЫШОВ
Александр Сергеевич
студент группы ИСТ-241м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sanna-benelli@mail.ru

ЧЕРНЫШОВ
Артём Геннадьевич
кандидат технических наук, доцент кафедры Радиосвязи и Вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

ЧЕРНЫШОВА
Анастасия Владимировна
студент группы РТ-22м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Nastena-slastena0800@mail.ru

ЧЕСНОКОВ
Константин Эдуардович
студент группы ИСТ-041
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chesnokov078@gmail.com

ЧЕШКОВ
Константин Николаевич
студент группы ИСТ-231м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cheshcovkostya@gmail.com

ЧИЗИБА
Эндрю
студент группы ИКТБ-37м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chizandrew@yandex.ru

ЧУГРЕЕВА
Анастасия Сергеевна
студент группы ИСТ-232м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, larazimina08@gmail.com

ЧУПАХИН
Игорь Игоревич
студент группы ИБТС-31
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chu2106@inbox.ru

ЧУРЫНИНА
Марина Владимировна
студент группы ЭП-31м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, churynina92@mail.ru

ШАГИСУЛТАНОВ
Тимур Айратович
студент группы ИКТЗ-31м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shg.timur@gmail.com

ШАЙЕР
Адриан Владимирович
студент группы 4-МДА-7
Санкт-Петербургский государственный университет промышленных технологий и дизайна,ashayer02@gmail.com

ШАЛАГИНОВ
Михаил Николаевич
студент группы ИКТИ-25м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mishalgnv@gmail.com

ШАМИН
Максим Алексеевич
студент группы ИКБ-25
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxshamin@gmail.com

ШАНЕНКО
Даниил Евгеньевич
стувдент группы ИСМ-21з
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, danshanenko@gmail.com

ШАРАПОВА
Амина Халиловна
студент группы ИСТ-232м
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
sharapovaamina2@yandex.ru

ШВЕЦОВ
Федор Павлович
студент группы РТ-22
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича, F999964@mail.ru

ШВИДКИЙ
Артем Александрович
начальник НОЦ "Программно-определяемые системы" Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shvidkiy@sut.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

ШЕНХОРОВА Дарья Николаевна — студент группы ИКВТ-01 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dasha.shh52@gmail.com

ШЕРЕМЕТ Денис Николаевич — студент группы ИСТ-331м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, denchiksher@mail.ru

ШЕРЕМЕТ Никита Викторович — студент группы Р-32м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sidwavedata@gmail.ru

ШЕРСТОБИТОВ Александр Андреевич — студент группы ФП-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shbeetov@yandex.ru

ШЕСТАКОВ Александр Викторович — доктор технических наук, старший научный сотрудник, alexandr.shestakov01@yandex.ru

ШЕСТАКОВ Семён Михайлович — студент группы 4-мда-7 Санкт-Петербургского государственного университета промышленных технологий и дизайна, schestackov.semeon@yandex.ru

ШЕСТАКОВА Валерия Алексеевна — студент группы ИКТС-23м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича,shestalons@yandex.ru

ШЕСТАКОВА Виктория Артуровна — студент группы 4-МДА-9 Санкт-Петербургского государственного университета промышленных технологий и дизайна, 3243f6a8885@inbox.ru

ШИНГАРЕВА Алёна Николаевн — студент группы БИМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 12alena1212@gmail.com

ШИРОКОВ
Дмитрий Александрович
студент группы РСО-31м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
nutella2277@yandex.ru

ШИРОПАТИН Олег
Игоревич
студент группы ИСТ-241м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
shiropatin@gmail.com

ШИХОВ
Михаил Станиславович
студент группы ИКТС-23
Санкт-Петербургского
государственного университета
телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
mshikhov2005@gmail.com

ШИШКИНА
Виктория Юрьевна
студент группы ИКМ-32з
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича, vijka09@mail.ru

ШИШКИНА
Екатерина Тарасовна
студент группы ИСТ-041
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
ekaterina.23.10@mail.ru

ШИШОВ
Никита Максимович
студент группы ИСТ-331м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
advanture337@icloud.com

ШИЯН
Андрей Анатольевич
кандидат педагогических наук, доцент, доцент
кафедры информатики и компьютерного дизайна
Санкт-Петербургского государственного
университета телекоммуникаций им. проф. М.А.
Бонч-Бруевича, shiyan.aa@sut.ru

ШИЯН Павел Анатольевич — старший преподаватель кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shiyan.pa@sut.ru

ШИЯН Яна Андреевна — студент группы 3-МД-16 Санкт-Петербургского государственного университета промышленных технологий и дизайна, yanashiiiyan@gmail.com

ШОКОДЬКО Алексей Алексеевич — студент группы ИСТ–331м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Lexa-le@mail.ru

ШТЕРЕНБЕРГ Ольга Михайловна — аспирант группы 1001А-20 Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, vinogradova.ol@bk.ru

ШУВАЕВ Дмитрий Владимирович — студент группы 3-МД-16 Санкт-Петербургский государственный университет промышленных технологий и дизайна, Dimaskaa228@gmail.com

ШУМКОВА Евгения Станиславовна — студент группы БИМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shumkova.eva01@mail.ru

ЩЕГЛОВ Сергей Александрович — студент группы ИКТГ-24М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shew341@gmail.com

ЩЕГОЛЬСКИЙ Юлиан Евгеньевич — студент группы ИКТМ-32м Санкт-Петербургского университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, yulik.shchegolskiy@gmail.com

ЮГИН
Савва Дмитреевич
студент группы ИКТС-22
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
zavvayu8@gmail.com

ЮКЛУТОВ
Денис Александрович
студент группы ИКТС-01 Санкт-Петербургского
государственного университета
телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
denkam03@yandex.ru

ЮРОВА
Ульяна Сергеевна
студент группы ИКТЗ-31м Санкт-
Петербургского государственного университета
телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
u_yurova@mail.ru

ЯКУБОВИЧ
Сергей Александрович
студент группы ИКТБ-38м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
yakubovich2001@icloud.com

ЯКУБОВСКИЙ
Иван Александрович
студент группы 4-МДА-9
Санкт-Петербургский государственный
университет промышленный технологий и
дизайна, vanyayak2@mail.ru

ЯНДИЕВ
Ахмед Алаудинович
студент группы РТ-22м
Санкт-Петербургского государственного
университета телекоммуникаций
им. проф. М. А. Бонч-Бруевича, студент кафедры
РСиВ, alaudin.yandiev@mail.ru.

ЯСАФОВ
Иван Константинович
студент группы ИКТС-23
Санкт-Петербургского
государственного университета
телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
vyasafov@yandex.ru

ЯССЕР
Марк Владимирович
студент группы ИКТЗ-31м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yasser.mark@yandex.ru

ЯЦЫШИН
Илья Русланович
студент группы ЗР-31м
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, jblprow@gmail.com

ЯШКОВА
Анастасия Витальевна
студент группы РСМ-21з
Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anastasia.yashkova@bk.ru

всероссийская научно-методическая
конференция магистрантов и их руководителей

ПКМ

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