СПбГУТ)))

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

ПОДГОТОВКА ПРОФЕССИОНАЛЬНЫХ КАДРОВ В МАГИСТРАТУРЕ В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

ПКМ 2024

СБОРНИК ЛУЧШИХ ДОКЛАДОВ

Том 2

Санкт-Петербург
2025

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

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

ПОДГОТОВКА ПРОФЕССИОНАЛЬНЫХ КАДРОВ В МАГИСТРАТУРЕ В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ (ПКМ-2024)

3 декабря – 5 декабря 2024 года

Сборник лучших докладов

Том 2

Информационные технологии и программная инженерия

Кибербезопасность

Гуманитарные, экономические и экологические проблемы цифрового общества

СПб ГУТ)))

Санкт-Петербург

2025

УДК 621.39:004
ББК 32.74

Рецензент – доцент, доктор технических наук Н. С. Пщелко

Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации (ПКМ-2024). V Всероссийская научно-техническая и научно методическая конференция магистрантов и их руководителей. Сборник лучших докладов: в 2 т. / Под ред. А. Н. Бучатского; сост. И. Е. Скалецкая. СПб.: СПбГУТ., 2025.

ISBN 978-5-89160-359-2

Том 2. СПб.: СПбГУТ., 2025. 629 с.

ISBN 978-5-89160-361-5

Сборник содержит доклады, признанные лучшими по результатам работы научных направлений конференции ПКМ-2024. Тематика работ охватывает актуальные вопросы по направлениям: информационные технологии и программная инженерия; кибербезопасность; гуманитарные, экономические и экологические проблемы цифрового общества.

Доклады, не вошедшие в число лучших и не представленные в настоящем сборнике, размещены в материалах конференции ПКМ-2024 на сайте PKM.SUT.RU.

Издание рассчитано на студентов специалитета и бакалавриата, магистрантов, их руководителей, аспирантов, молодых ученых и преподавателей.

ISBN 978-5-89160-361-5 (Т. 2)
ISBN 978-5-89160-359-2

© Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», 2025

СОДЕРЖАНИЕ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММНАЯ ИНЖЕНЕРИЯ

3.1. Интеллектуальные коммуникационные технологии 9

Авдеева Т. М., Литвинов В. Л. Исследование технологий определения эмоционального состояния человека по изображению 9

Бондаренко И. Б., Заборовская Н. В., Якубова Н. Р. Подходы к оценке эффективности комплексирования средств при проектировании систем защиты информации 14

Карлина К. С. Текстовый анализ. Методики и подходы к исследованию неструктурированных данных 20

Колмаков А. Е., Литвинов В. Л. Технологии моделирования реалистичного поведения виртуальных персонажей 24

Копытова Е. В., Мавричев В. К., Петров Д. В., Филиппов Ф. В. Интерпретируемость результатов работы ML моделей и методы повышения прозрачности 30

Корнюшкин Д. А., Крылов А. А. Методы управления технологическими объектами при помощи нейросетевых регуляторов 35

Коровкина Е. В., Литвинов В. Л. Прогнозирование угроз информационной безопасности на основе анализа открытых данных 39

Крюков А. Н. Использование искусственного интеллекта в учебном процессе 43

Мамаев Е. А. Анализ использования искусственного интеллекта в цифровых двойниках телекоммуникационных сетей 46

Петров Д. В., Филиппов Ф. В. Обучение моделей YOLO для детекции трещин в стеклах обесточенных LCD панелей 51

Фирсов В. Н. Разработка метода детектирования неисправностей асинхронных электродвигателей с помощью машинного обучения 57

Чернобровкин С. В. Модель процесса доведения информации до подвижных носителей 61

3.2. Информационные технологии в дизайне 68

Андрианов Д. М. Адаптация модели Лотки-Вольтерры для моделирования взаимодействия туристов и природных ресурсов на экологических маршрутах 68

Беляев Б. Р., Диброва О. П., Дорохова Е. Ю., Мусаева Т. В. Исследование технологий рекомендательных систем 74

Боталов А. А. Применение GPT-4 в решении олимпиадных задач по математике для старшеклассников 79

Волошинов Д. В., Иваненко Е. А. Применение искусственного интеллекта в проектировании пользовательских интерфейсов 82

Гольдин И. И., Шиян А. А. Использование визуальных систем для мониторинга персонала и рабочих процессов 88
Громов А. В. Визуализация данных результатов моделирования и анализа пульсовых волн человека 93
Дорохова Е. Ю., Мусаева Т. В. Исследование нейросетевых моделей обработки и анализа изображений 96
Князева Е. В, Козлова А. Н. Современное проявление визуальных элементов стиля ар-нуво 101
Марушина М. Е. Кастомизация индивидуальных объектов в информационных системах 107
Мусаева Т. В., Никифоров П. А. Проблемы и метод восстановления 3D-модели разрушенного здания 112
Мусаева Т. В., Рамзаев К. К. Системы управления модулей подвижности на основе платформы Стюарта 116
Широков А. А., Шиян А. А. Система электронного документооборота на Blockchain 120

3.3. Программная инженерия 124

Березкин А. А., До Ф. Х., Киричек Р. В. Анализ техник предсказания кадров для уменьшения задержки в спутниковых каналах связи для потоковой передачи видео 124
Березкин А. А., Ченский А. А. Разработка программной системы мониторинга беспилотных воздушных судов на карте и тестирования источников данных 130

КИБЕРБЕЗОПАСНОСТЬ

4.1. Защищенные системы связи 136
Алькаттан С. Enhancing Application Security through Dynamic Binary Instrumentation 136
Чизиба Э. Integrated security in devops: design and implementation of automated security testing frameworks in devops pipelines 141
Алехин Р. В. Механизм эмуляции атаки типа Man in the Middle на узлы инфраструктуры 145
Альотум Ю. М. А. А. Метод одноразового пароля в механизме факторной аутентификации и возможность его использования в биометрической системе 150
Амалиев Х. С. Исследование типов моделей ассимиляционной памяти для выработки когнитивных функций систем защиты информации 156
Бирих Э. В., Сахаров Д. В., Теряев М. А. Разграничение доступа в облачных инфраструктурах распределенных ИСПДн 159
Бударный Г. С., **Манжула К. А.** Модель защиты ассимиляционной памяти в средах IoT 165
Бусыгин К. Н., Егоров И. М., Зурахов В. С., Чалова Е. И. Автоматизированные средства для поддержки разработки безопасных программных продуктов 170
Бусыгин К. Н., Егоров И. М., Зурахов В. С., Чалова Е. И. Ключевые моменты защиты корпоративной сетевой инфраструктуры 175

Бусыгин К. Н., Егоров И. М, Зурахов В. С., Чалова Е. И., Штеренберг С. И. Сетевые проблемы при создании кластера на основе LXC 181
Васильев И. Д. Реализация программной основы игры на платформе Unity 185
Виткова Л. А, Трофимов Е. А. К вопросам о защите ML-моделей в облачных инфраструктурах 190
Гречухин Д. Н. Анализ методов обработки естественного языка для улучшения обнаружения фишинга 194
Долуденко Б. В. Топология многообразий в анализе безопасности обфускации программ 198
Дюсметова А. А. Задачи защиты систем виртуализации 201
Иванов Р. А. Анализ сетевого трафика с использованием искусственного интеллекта 207
Камалова А. О., Пестов И. Е., Смирнов Д. Н. Особенности типовых архитектур облачных инфраструктур при обеспечении информационной безопасности 212
Кирилова Д. С. Квантово-устойчивая инфраструктура открытых ключей 216
Кулиныч Н. Д. Искусственный интеллект и машинное обучение в кибербезопасности 220
Левшун Д. С., Староверов А. И. Подход к оценке эффективности атак на отравление данных в моделях с активным обучением 224
Левшун Д. С., Щеголев Е. К. Анализ современного состояния исследований в области обнаружения уязвимостей исходного кода устройств интернета вещей 229
Марков А. С. Формирование системы защиты информации в мультисервисных сетях связи 234
Михайлов А. А. Разработка защищенного файлового хранилища для инстансов VMware vSphere 238
Пешкина В. В. О реализации совершенного линейного эквивалентного профиля двоичной последовательности 243
Поляничева А. В., Шулындина М. С. Анализ основных угроз уязвимостей WebRTC: от перехвата данных до DDoS-атак 248
Райлян Д. П. Методы и алгоритмы обеспечения безопасности данных для защиты от спама 252
Рубацкий Р. А. Российские сканеры уязвимостей как необходимость поддержания высокого уровня защиты сетевой инфраструктуры 256
Руденко С. А. Влияние расширенного использования IoT на безопасность беспроводных коммуникаций 260
Стародубцев В. И. Оптимизация мобильного интерфейса с помощью искусственного интеллекта 264
Талакин Е. Н. Анализ свойств децентрализованных рассинхронизированных пакетных нейросетевых программ в распределенной информационной системе 268
Тамбовский А. Н., Ушаков И. А. Архитектура сервиса сбора данных для обнаружения инсайдерских угроз в файловых системах Linux 273
Чистяков А. С. Автоматическое обновление сертификатов TLS 277
Чистяков А. С. Интеграция автоматического обновления TLS-сертификатов в контейнерные оркестраторы (Kubernetes) 282
Якобсон Д. А. Обеспечение безопасности Android-приложений, новые угрозы в OWASP Mobile Top 10 286

4.2. Информационная безопасность компьютерных сетей 292

Мано Г., Турусида Т., Хаддад М. Н. Exploring the role of canary tokens in detection and backdoor attacks in windows environments 292

Бабков И. Н., Сидельников А. С. Технические каналы утечки информации ПЭМИН в автоматизированной системе. Пассивные и активные средства защиты 296

Бенч М. Н., Косов Н. А. Тестирование эффективности DevSecOps процессов 300

Бирих Э. В., Сахаров Д. В., Травкина Е. А. Влияние применения файервола nftables на производительность сетевых взаимодействий в виртуализированной среде 305

Боднарчук К. М., Ильин Я. А., Ковцур М. М. Исследование зоны покрытия WLAN для повышения уровня информационной безопасности корпоративной сети 310

Борисенко И. И. Роль социальной инженерии и USB-устройств в моделировании сетевых атак 315

Борисенко И. И., Серегин И. А. Социальная инженерия как угроза информационной безопасности: анализ методов и способов защиты 320

Бударин М. Э., Лобащенко Т. Д., Никифоров А. В. Анализ характеристик современных протоколов виртуальных частных сетей и их безопасности 325

Винников С. А., Киструга А. Ю., Ковцур М. М. Исследование способов обнаружения атаки Evil Twin в сетях IEEE 802.11AX 330

Виткова Л. А., Лагутина С. В., Сахаров Д. В. Обнаружение информационных фейков: изменения и вызовы в пост-2022 период 334

Виткова Л. А., Прохорова М. В. Обзор и особенности использования процесса Detection Engineering в SIEM системах 337

Гаврилов П. Р. Методы минимизации ущерба при возможных инцидентах безопасности 341

Груздев А. С., Комаров Д. А. Социальные сети как инструмент социальной инженерии 345

Гугунишвили Л. Д., Левшун Д. С. Применение подхода к проектированию устройств на основе микроконтроллеров для объектов критически важной инфраструктуры к сетевому маршрутизатору 351

Денисов А. С., Пантюхин О. И., Родичев И. Д. Изучение аспектов применения машинного обучения в области информационной безопасности 356

Дзиговский В. А. Анализ актуальных угроз безопасности решений второго уровня блокчейн-сетей 361

Догадаев А. С., Косов Н. А. Руткиты ядра и анализ Turla 366

Домбровский Р. М. Косов Н. А. Реализация уязвимости Image Magic на Astra Linux 370

Дрепа В. Е., Ковцур М. М., Красников Д. А. Обзор актуальных Honeypot-решений с открытым исходным кодом 374

Журавлева А. С. Разработка метода формирования общего сетевого ключа в протоколе OWE в Wi-Fi сетях 380

Исмаилов Р. Р., Спицын М.А. Идея стратегии обнаружения угроз на базе концепции Detection Engineering 385

Калмыков А. А. Методы выявления вредоносного кода в репозиториях пакетных менеджеров для языков программирования 390

Ковцур М. М., Коренюгин Е. В., Яссер М. В. Разработка защищенного мобильного приложения для хранения данных для операционной системы Android 395

Козырева Н. И., Савин Е. А. Моделирование угроз информационной безопасности в сетях IoT на уровне устройства 400
Козырева Н. И., Теплов К. И. Моделирование угроз информационной безопасности в сетях IoT: атака через захват устройства 404
Конев А. Р., Косов Н. А. Исследование эффективности VPN на канальном уровне модели OSI 408
Коньков В. В., Красов А.В. Цифровые водяные знаки как метод защиты от реверс-инжиниринга в модулях ядра Linux 414
Косов Н. А., Филипов Э. О. Протокол OAuth: Грант «Код авторизации» как стандарт безопасной авторизации 419
Миноченков Н. С. Организация мониторинга, управления уязвимостями и расследования инцидентов с использованием многофункционального зонда на базе одноплатной вычислительной платформы 424
Нижлукченко И. Д. Проблемы обеспечения безопасности ОС на базе OpenSource решений 430
Новиков Д. С. Автоматизация тестирования безопасности веб-приложений: анализ преимуществ и возникающих проблем 434
Пимашин Е. Н. Сравнительный анализ мультиязычных парсеров программного кода на примере языков Python и JavaScript 438
Проничев В. Д., Ушаков И. А. Автоматизированный анализ изменений в сетевых конфигурациях устройств на основе нейронных сетей 443
Страйстар В. А., Ушаков И. А. Проблемы глубокого обучения для обнаружения внутренних нарушителей (инсайдеров) 449
Таратынов И. Д. Автоматизированная генерация трафика центров управления ВПО на примере фреймворка постэксплуатации Merlin 454
Федотовская А. Д. Анализ времени выполнения служебных запросов платформ больших данных для выявления аномалий и злоумышленников 460
Шиликов Д. А. Анализ комбинаций методов преобразования сигнала с физического датчика случайных чисел, основанного на кольцевых осцилляторах 465
Якубович С. А. Анализ угроз безопасности веб-приложений. Выявление причин возникновения современных уязвимостей и целей эксплуатации уязвимостей 470

ГУМАНИТАРНЫЕ, ЭКОНОМИЧЕСКИЕ И ЭКОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ЦИФРОВОГО ОБЩЕСТВА

5.1. Вопросы регионоведения и межкультурных коммуникаций в цифровую эпоху 474

Аверьянов М. А., Гехт А. Б. Краткий анализ деятельности Французского союза и Французского сообщества 474
Бондарь Н. А. От СБСЕ к ОБСЕ: краткий обзор трансформации организации 480
Гехт А. Б. Развитие международного контроля за применением технологий искусственного интеллекта на примере деятельности Консультативного органа ООН (КОИИ ООН) по искусственному интеллекту 486
Гехт А. Б., Капуков А. И. Анализ практического воплощения идейного наследия Рихарда Куденхове-Калерги 492
Иванова А. М. Особенности PR-продвижения космической политики РФ на современном этапе 496
Килина М. А., Цверианашвили И. А. Энвайронментализм в политической жизни современной Аргентины 501
Климентьев Е. Н., Патрушева Д. А. Мигранты как движущая сила технологического прогресса и экономического роста США 506

Неровный А. В., Яцышин И. Р. Эволюция внешней политики Канады в арктическом регионе при Джастине Трюдо 510
Окуджава А. Э. Евроатлантическая интеграция Грузии: содержание, динамика и перспективы 515
Полякова К. В. Экологические проблемы Арктического региона в восприятии живописи 520
Самбуров К. В. Транспортная подвижность населения регионов России на примере дальнего железнодорожного сообщения 526

5.2. Реклама и связи с общественностью в цифровом обществе 531

Желтова Е. П., Маршева Н. В. Стратегии обучения иноязычному академическому чтению для научно-исследовательской работы 531
Кривонос А. О., Кульназарова А. В. Продвижение фотоуслуг в цифровой сфере 538
Русова А. А., Щур С. Ю. Особенности взаимодействия инклюзивных брендов со своей аудиторией 542

5.3. Цифровая трансформация, инновации, бизнес 547

Аверина А. А. Интеграция инструментов искусственного интеллекта в управлении бизнес-процессами компании 547
Большакова К. Е. Исследование возможностей и перспектив цифровой трансформации автомобильного бизнеса 552
Иванов Н. А., Киселев Д. И., Сотников А. Д. Моделирование информационных процессов в инфокоммуникационных системах 558
Кваша Н. В., Шитиков И. Е. Феномен ограниченной рациональности теории принятия решений в концепции интеллектуальной экономики 564

5.4. Экология и формирование информационного пространства 570

Казанцева А. Г., Цветкова И. Ю. Исследование зависимости концентрации загрязняющих веществ от выбросов крупных предприятий на основе данных автоматизированной системы мониторинга г. Красноярска 570
Казанцева А. Г., Чурынина М. В. Обработка космических снимков с целью получения экологической информации 575
Лосева А. С. Анализ шумового загрязнения муниципального округа «Невский округ» с применением ГИС-технологий 580
Михтеева Е. Ю., Потапова И. А., Скобликова А. Л., Яковлева Т. Ю. Влияние дневного света на определение коэффициента ослабления для слабо замутненной атмосферы лидарными системами 585
Ожегов В. А. Исследование динамики развития городской застройки г. Сыктывкар 592
Пентегова В. В., Стурман В. И. Картографирование электромагнитных полей промышленной частоты в Красногвардейском районе Санкт-Петербурга 598
Пищугина А. Д. Учет наложения секторов базовых станций при экологическом мониторинге электромагнитных полей 603

Авторы статей 609

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММНАЯ ИНЖЕНЕРИЯ

3.1. Интеллектуальные коммуникационные технологии

УДК 004.855.5
ГРНТИ 28.23.37

ИССЛЕДОВАНИЕ ТЕХНОЛОГИЙ ОПРЕДЕЛЕНИЯ ЭМОЦИОНАЛЬНОГО СОСТОЯНИЯ ЧЕЛОВЕКА ПО ИЗОБРАЖЕНИЮ

Т. М. Авдеева, В. Л. Литвинов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Эмоции играют огромную роль в жизни человека и межличностном общении. Они могут быть выражены различными способами, однако наибольшей выразительностью обладает лицо человека. Распознавание эмоций у людей представляет собой актуальную задачу в области машинного обучения. В связи с этим важно изучение технологий, используемых для классификации эмоций. В данной статье рассмотрены основные подходы к распознаванию эмоций, датасеты и архитектуры.

эмоции, сверточные нейронные сети, датасет, архитектура

Эмоции представляют собой специфический класс психических процессов, отражающих субъективное отношение индивида к окружающему миру и самому себе. Они способствуют выживанию, обеспечивая быструю и экономичную реакцию на внешние воздействия.

Важно отметить, что индивидуальные особенности выражения эмоций могут варьироваться. Исследования американского психолога Пола Экмана, проведенные в 70-х годах XX века среди изолированных племен Папуа-Новой Гвинеи, показали, что ряд основных эмоций (гнев, страх, печаль, отвращение, презрение, удивление и радость) являются универсальными и понятными для людей любой культуры [1].

Определение эмоционального состояния человека по изображению лица является сложной задачей, которая может быть решена с помощью различных методов.

Традиционный подход основан на классификации ключевых точек лица (facial landmarks). Расположение точек привязывается к бровям, глазам, губам, носу и челюсти, что позволяет частично захватить мимику лица. Нормализованные координаты могут быть использованы в качестве входных данных для классификаторов, таких как SVM или Random Forest, для получения базовой оценки эмоции [2]. Важно отметить, что этот метод требует предварительного выравнивания положения лиц на изображении.

Однако, современные исследования показывают, что такой подход считается устаревшим. Ограниченность подхода, основанного только на координатах ключевых точек, заключается в потере важной визуальной информации. Глубокие сверточные сети продемонстрировали наилучшую эффективность в анализе визуальных данных, включая распознавание эмоций по лицу.

Использование методов «глубокого обучения» для распознавания эмоций обеспечивает более высокую точность, однако требует значительных вычислительных ресурсов.

В системах распознавания лиц, которые могут быть реализованы на основе алгоритма Виолы-Джонса, обратной сверточной нейронной сети (DNN) или детектора объектов с максимальным запасом (MMOD), исходное изображение обрабатывается для выделения области, содержащей лицо человека. Впоследствии исходное изображение преобразуется из цветового формата RGB или BGR в оттенки серого, чтобы уменьшить пространство объектов и повысить скорость работы классификатора эмоций. Область оттенков серого, идентифицируемая детектором лиц, затем нормализуется и передается в классификатор эмоций, который представляет собой обученную сверточную нейронную сеть (CNN) [3].

CNN выдает критерии, указывающие на интенсивность шести основных эмоций и состояние спокойствия.

Существуют различные датасеты для обучения сверточных нейронных сетей, классифицирующих эмоции. Рассмотрим наиболее популярные из них в таблице 1:

ТАБЛИЦА 1. Обобщающие данные о датасетах для обучения

Название	Количество изображений	Количество людей	Размер	Количество эмоций	Цветовая модель
FER2013 [4]	35 887 изображений	-	48x48	7	Gray
MMI [5]	2900 видео и 740 изображений	75	-	6	RGB
CKP [6]	593 изображений	123	640x490 и 640x480	7	RGB, Gray

Рассмотрим различные архитектуры сверточных нейронных сетей для классификации эмоций.

1. Resnet50

Название ResNet является сокращением от «Residual Network», что дословно переводится как «остаточная сеть».

Для решения проблемы внезапного снижения точности при увеличении глубины нейронной сети компания Microsoft разработала архитектуру ResNet, основанную на «быстрых соединениях с идентификатором». Данные соединения позволяют информации напрямую проходить через один или несколько слоев (см. рисунок 1), что значительно упрощает процесс обучения глубоких сетей и предотвращает проблему «исчезающего градиента» [7].

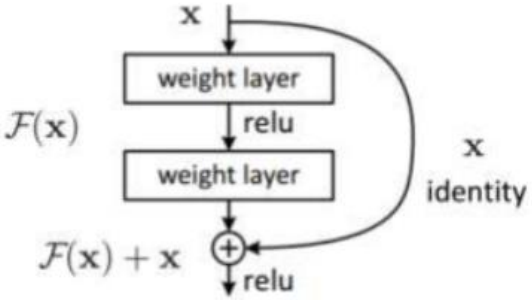


Рис 1. Остаточный блок

Достоинства сети ResNet:

– простота оптимизации (архитектура ResNet упрощает процесс настройки параметров модели);

– масштабируемость (увеличение глубины сети ResNet позволяет повысить точность предсказаний без существенного усложнения процесса обучения).

Архитектура сети представлена на рисунке 2:

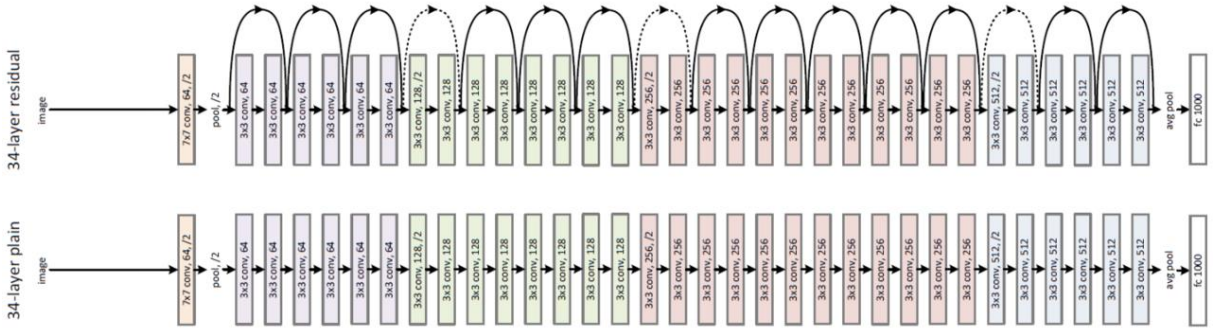


Рис. 2. Архитектура среды ResNet

2. GoogLeNet

В целях оптимизации вычислительных затрат в глубоких нейронных сетях (DNN) и повышения их эффективности был разработан модуль Inception (рис. 3), интегрированный в архитектуру сети GoogLeNet.

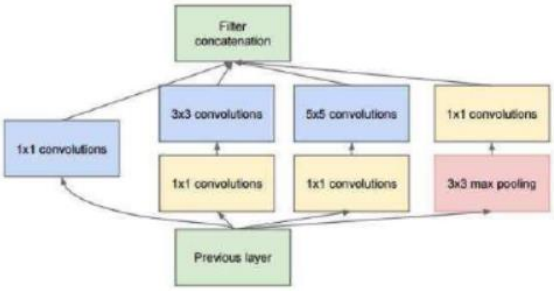


Рис. 3. Модуль Incertion

Несмотря на кажущуюся простоту параллельного соединения сверточных фильтров размеров "1x1", "3x3" и "5x5", ключевым преимуществом модуля Inception является использование сверточного слоя "1x1" для уменьшения объема обрабатываемых данных, что в конечном итоге способствует повышению производительности сети [8].

Нейронная сеть состоит из девяти таких блоков (рис. 4).

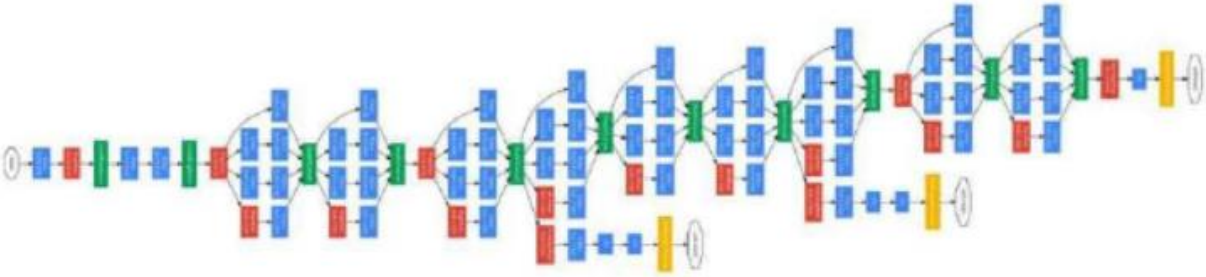


Рис. 4. Архитектура сети GoogLeNet

3. VGG16

VGG16 является улучшением сети AlexNet, в которой фильтры с большими ядрами (11x11 и 5x5) заменены несколькими фильтрами размером 3x3 (рисунок 5).

Несмотря на это улучшение, у VGG16 имеются существенные недостатки: длительный процесс обучения и значительное количество обучаемых параметров (около 138 миллионов) [9].

Тем не менее, благодаря своей простоте реализации, данная архитектура может служить хорошей основой для обучения. Следует отметить, что VGG16 изначально разрабатывалась для обработки изображений размером 224x224.

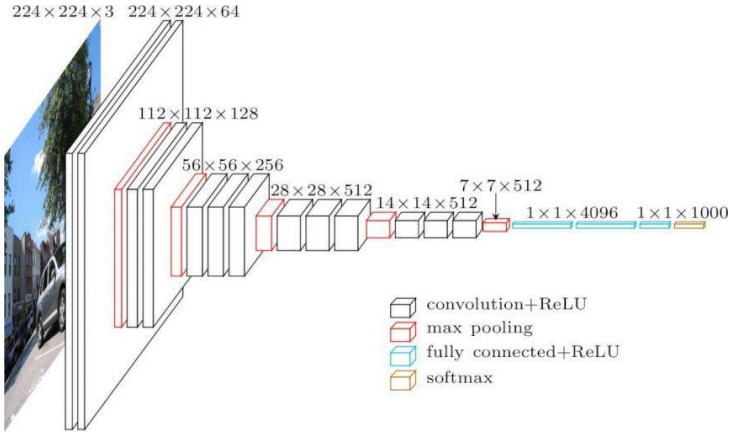


Рис. 5. Архитектура среды VGG16

Таким образом, для классификации эмоций по фотографии создают сверточные нейронные сети, для которых используются различные датасеты и архитектуры.

Список используемых источников

1. Экман П. Эволюция эмоций. СПб: Питер. 2020. 480 с.
2. Бойцев А. А. Детекция ключевых точек лица с помощью капсульных нейронных сетей // Научно-технический вестник информационных технологий, механики и оптики, 2023. Том 23. № 3.
3. Соболь Б. В. Эффективность применения различных спектральных признаков для классификации эмоций с помощью сверточной нейронной сети // Международный научно-исследовательский журнал, № 9 (147).
4. FER2013 Dataset: Papers with code. URL: https://paperswithcode.com/dataset/fer2013 (дата обращения 12.09.2024).
5. MMI Facial Expression Database. URL: https://mmifacedb.eu/ (дата обращения 10.10.2024).
6. CK+ Dataset: Papers with code. URL: https://paperswithcode.com/dataset/ck (дата обращения 01.10.2024).
7. Елисеев А. И. Решение задач глубокого обучения с использованием фреймворков Pytorch и Pytorch Lightning: учебное пособие / А. И. Елисеев, Ю. В. Минин, Ю. В. Кулаков. Тамбов: Издательский центр ФГБОУ ВО «ТГТУ». 2023.
8. GoogLeNet. URL: https://ai.google/research/pubs/pub43022 (дата обращения 06.09.2024).
9. VGG16 – нейросеть для выделения признаков изображений. URL: https://neurohive.io/ru/vidy-nejrosetej/vgg16-model/ (дата обращения 20.09.2024)

Avdeeva T., Litvinov V. **RESEARCH OF TECHNOLOGIES FOR CREATING NEURAL NETWORKS OF EMOTION CLASSIFICATION.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Emotions play a huge role in human life and interpersonal communication. They can be expressed in various ways, but the person's face has the greatest expressiveness. Recognizing emotions in humans is an actual task in the field of machine learning. In this regard, it is important to study the technologies used to classify emotions. This article discusses basic approaches to emotion recognition, the datasets and architectures used.

Key words: emotion, convolutional neural networks, dataset, architecture.

УДК 681.3
ГРНТИ 81.93.29

ПОДХОДЫ К ОЦЕНКЕ ЭФФЕКТИВНОСТИ КОМПЛЕКСИРОВАНИЯ СРЕДСТВ ПРИ ПРОЕКТИРОВАНИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

И. Б. Бондаренко, Н. В. Заборовская, Н. Р. Якубова
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Описан ряд подходов при решении задачи оценки эффективности комплексных систем защиты информации. Рассмотрены подсистемы комплексных систем, приведены характеристики качества, методы свертки компонент качества. Определены уровни защиты и соответствующие им стратегии защиты информации, а также выявлено соответствие вида компонента проектируемой системы уровням защиты конфиденциальной информации.

комплексная система защиты, средства защиты, комплексирование, защита информации, эффективность, показатели эффективности, компоненты качества, уровни защиты

При проектировании комплексных систем защиты информации (КСЗИ) наряду с проблемами обеспечения требуемых показателей защищенности вычислительных ресурсов в локальной вычислительной сети (ЛВС) предприятия необходима оценка эффективности применяемых средств защиты от несанкционированного доступа к циркулирующей в ЛВС информации. Задачами КСЗИ являются обеспечение: бесперебойного и безопасного функционирования систем, обнаружения и устранения угроз информационной безопасности в виде инцидентов, диагностики уязвимостей подсистем [1, 2].

Анализ эффективности осложняется необходимостью учета множества средств и методов защиты, применяемых в современных КСЗИ, а также вариативностью аппаратной архитектуры и профилей программных средств [3]. Также необходим учет имеющихся встроенных средств защиты, например, в операционных системах.

В КСЗИ входят следующие подсистемы: DLP (Data Loss Prevention) – для выявления и предотвращения утечки критичных данных на основе анализа исходящего трафика, IDS (Intrusion Detection System) / IPS (Intrusion Prevention System) – для предотвращения атак извне, SIEM (Security information and event management) – система для мониторинга за инцидентами, IDM (Identity

management) – комплекс для контроля за учетными записями и управления доступом к данным пользователей.

При вероятностном подходе оценки эффективности безопасности ее получают, используя модель, или проводя эксперименты на реальном объекте защиты. При этом КСЗИ рассматривается как совокупность взаимосвязанных компонентов, в том числе учитывается работа персонала, работа которых направлена на достижение определенной цели. Тогда эффективность КСЗИ будет определяться минимальным расхождением между запланированным и достигнутым уровнями защиты. При этом подходе эффективность средств, входящих в КСЗИ, определяется как совокупность свойств, каждое из которых количественно характеризуется числовой характеристикой или функцией достигнутого качества – показателем $y_i(t)$. В этом случае совокупность показателей качества состояния системы в момент времени t можно записать в следующем виде:

$$\mathbf{Y}(t) = (y_1(t), y_2(t), \ldots, y_n(t)).$$

Каждый показатель качества y_i образует пространство допустимых значений, свойства которых зависят от состава средств защиты, входящих в КСЗИ. Степень соответствия вектора $\mathbf{Y}(t)$ требованиям, предъявляемым к КСЗИ, и будет определять комплексный показатель вероятности достижения цели КСЗИ.

Из-за мнокритериальности требований к безопасности и сложности описания функционирования КСЗИ решение задачи оценки эффективности возможно с помощью:

– стохастических дифференциальных уравнений;

– разностных стохастических уравнений;

– методов анализа временных рядов;

– многомерного интегрирования совместной плотности распределения вероятности;

– последовательного интегрирования частных показателей эффективности.

Совокупность показателей качества **Y** содержит три группы компонент:

$$\mathrm{Y} = \mathrm{Y_R} \cup \mathrm{Y_З} \cup \mathrm{Y_T},$$

где $\mathbf{Y_R}$ – группа, характеризующая результативность работы КСЗИ; $\mathbf{Y_З}$ – группа показателей – затрат на работу КСЗИ; $\mathbf{Y_T}$ – вектор затрат времени для получения результатов работы КСЗИ.

Такое разделение на группы необходимо для проведения операции свертки разнородных показателей качества, которая возможна только внутри перечисленных групп.

В качестве показателей качества для определения эффективности комплексирования средств защиты используются следующие:

– количество успешно предотвращенных инцидентов;

– время, затрачиваемое КСЗИ на обнаружение угрозы и восстановление после ее проявления;

– степень соответствия КСЗИ стандартам и политикам безопасности;

– степень удовлетворенности пользователей работой КСЗИ;

– соотношение затрат на средства защиты, входящие в КСЗИ, к выгоде от ее использования.

Причем те же показатели качества характеризуют КСЗИ и в процессе ее эксплуатации.

При оценочном подходе оценки эффективности безопасности определяются исходя из политики безопасности, установленной законом РФ, и на основе анализа на соответствие имеющихся в КСЗИ механизмов защиты информации одному из семи классов защиты. Тем самым обеспечивается достаточность применяемых средств защиты по определенному классу защищенности информации, циркулирующей в сети предприятия. Определение необходимого уровня защищенности информации для предприятия осуществляется с помощью анализа рисков [4]. Различные конфигурации информационных систем являются причиной того, что угрозы и уязвимости имеют различный вес, что усложняет расчет суммарного риска при комплексировании средств защиты. Вдобавок к этому необходимо учитывать взаимосвязь факторов риска, сочетание которых может привести к значительному ущербу. Не будем останавливаться на методах анализа рисков, оценки ущерба и определения уровня потерь предприятия при реализации угроз, которые всесторонне рассмотрены в многочисленных источниках, например [5,6], в связи с ограниченностью размера статьи.

Отметим, что от уровня защиты, обеспечиваемого компонентами КСЗИ, зависит стратегия защиты информации (см. таблицу 1) [7]. Выделение темным цветом означает, что данный уровень должен быть обеспечен, а светлый – может быть.

Слабый уровень защиты информации в КСЗИ обеспечивается при применении серийно выпускаемых средств обработки информации с использованием общедоступных организационно-правовых мер.

Средний уровень защиты означает, что дополнительно необходимо использование средств разграничения доступа и управления защитой информации.

Верхний уровень защиты информации предполагает следующую градацию защит: слабая, средняя, сильная, очень сильная и особая. Компоненты сильной защиты в обязательном порядке должны образовывать комплекс, а в организационной структуре управления при этом должна функционировать служба защиты информации.

Очень сильная защита обеспечивается компонентами КСЗИ, когда система строится на основе типового проектирования с наличием непрерывного цикла защиты информации.

При особой защите компоненты разрабатываются по индивидуальному заказу, и организуется мандатный доступ к информации.

ТАБЛИЦА 1. Зависимость стратегии защиты конфиденциальной информации предприятия от уровня защиты компонентов КСЗИ

Уровень защиты	Стратегия защиты информации		
	Оборонительная	Наступательная	Упреждающая
Слабый (<= 0,5)			
Средний (0,5…0,75)			
Сильный (0,75…0,87)			
Очень сильный (0,87…0,93)			
Особый (>0,93)			

Для четырех уровней требуемой защищенности конфиденциальной информации: со слабой защитой (открытая информация), сильной защитой (гриф – конфиденциально), очень сильной защитой (строго конфиденциально) и особой защитой (особо конфиденциально) в таблице 2 приведены средства КСЗИ, разделенные по принципу действия на: пассивные, полуактивные и активные. Светлым выделены базовые средства, темным – допустимые.

Отметим, что средства для КСЗИ, применяемые для защиты на различных уровнях иерархии архитектуры вычислительных ресурсов предприятия, должны обеспечивать соответствующий уровень защиты типовых объектов (ПК, серверов, вычислительной сети предприятия, и т. д.).

ТАБЛИЦА 2. Соответствие вида компонента КСЗИ уровням защиты конфиденциальной информации

Уровни защиты	Компоненты (средства) КСЗИ		
	Пассивные	Полуактивные	Активные
Слабая защита	Допустимые / целесообразные	Допустимые / целесообразные в особых случаях	Допустимые / нецелесообразно
Сильная защита	Недопустимые	Допустимо/целесообразно	Допустимо / целесообразно в особых случаях
Очень сильная защита	Недопустимые	Допустимо / целесообразно в особых случаях	Допустимо / целесообразно обязательно в особых случаях
Особая защита	Недопустимые	Недопустимо	Обязательно

Экспериментальный подход заключается в организации соревновательного процесса между сотрудниками службы безопасности, часть из которых играют роль злоумышленников, пытающихся преодолеть систему защиты. В качестве аудиторов могут выступать специалисты компании или сотрудники сторонних организаций.

Проведенное исследование показало, что выбор подхода для определения состава компонент при проектировании комплексной системы защиты конфиденциальной информации зависит от множества требований и показателей, зависящих от вида производственной информации, количества уровней защиты и масштаба вычислительной сети. Таким образом, комплексирование аппаратных и программных средств защиты целесообразно осуществлять с учетом уровня защиты для проектирования эшелонированной системы защиты конфиденциальной информации с требуемыми характеристиками.

Список используемых источников

1. Ворона В. А. Комплексные (интегрированные) системы обеспечения безопасности / В. А. Ворона, В. А. Тихонов. М.: Гор. линия-Телеком, 2013. 160 с.
2. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие/ В. Ф. Шаньгин. М.: ФОРУМ: ИНФРА-М, 2022. 592 с.
3. Бондаренко И. Б., Раковский О. В., Мироненкова М. А., Крылов Д. А. Использование профилей сервисов защиты при разработке комплексных систем защиты информации с мягкой архитектурой // Фундаментальные и прикладные научные исследования: инноватика в современном мире. Сборник научных статей по материалам XIII Международной научно-практической конференции. Уфа: Изд. НИЦ Вестник науки, 2024. С. 29–33.

4. Громов Ю. Ю., Карасев П. И., Губсков Ю. А., Котюкова В. О. Оценка эффективности систем защиты информации и анализ рисков информационной безопасности в организации // Информационная безопасность, 2022. Т. 25. Вып. 2. С. 187–192.
5. Симонов С. Анализ рисков, управление рисками // Jet Info. 1999. № 1. С. 1–28.
6. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность/ С. А.Петренко, С. В. Симонов. М.: Академия АйТи: ДМК Пресс. 2018 384 с.
7. Сабанов А. Г. Многоуровневый анализ угроз безопасности процессов аутентификации // Вопросы защиты информации, 2014. № 1(104).

Bondarenko I., Zaborovskaya N., Yakubova N. **APPROACHES TO EVALUATING THE EFFECTIVENESS OF THE INTEGRATION OF TOOLS IN THE DESIGN OF INFORMATION SECURITY SYSTEMS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

A number of approaches to solving the problem of evaluating the effectiveness of integrated information security systems are described. The subsystems of complex systems are considered, quality characteristics, methods of convolution of quality components are given. The levels of protection and the corresponding information protection strategies have been determined, and the correspondence of the type of component of the designed system to the levels of protection of confidential information has been revealed.

Key words: comprehensive protection system, security tools, integration, information protection, efficiency, performance indicators, quality components, protection levels.

УДК 004.1082
ГРНТИ 00.77

ТЕКСТОВЫЙ АНАЛИЗ. МЕТОДИКИ И ПОДХОДЫ К ИССЛЕДОВАНИЮ НЕСТРУКТУРИРОВАННЫХ ДАННЫХ

К. С. Карлина
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В условиях популяции Artificial Intelligence (AL) и неограниченного потока текстовой информации, растет все большая необходимость в интеграции эффективных методик анализа неструктурированных данных. Текстовый анализ (ТА) выступает мощнейшим инструментом обработки и интерпретации текста. Совокупное применение вычислительных методов, позволяет выявлять практические знания и закономерности в тексте. Настоящая работа посвящена ключевым концепциям, таким как Distant Reading (DR), Corpus Linguistics (CL), Natural Language Processing (NLP) и Text Mining (TM). Автор приходит к выводу, что анализ текста с помощью новейших систем не только упрощает работу с большим объемом данных, но и позволяет принимать обоснованные решения на основе извлеченной информации.

текстовая аналитика, искусственный интеллект, неструктурированные данные, методы анализа текста

Текстовый анализ (ТА) относится к процессу изучения, обработки и интерпретации неструктурированных данных (текстовых материалов) для выявления практических знаний с использованием вычислительных методов [1, с. 217]. Неструктурированные данные (текст) могут включать: электронные письма, литературные тексты, письма, статьи, рекламу, официальные документы, контент социальных сетей, стенограммы и обзоры продуктов.

Практические знания относятся к идеям и шаблонам, используемым для классификации, сортировки, извлечения информации, определения отношений, выявления тенденций и принятия обоснованных решений.

Важно понимать, что текстовая аналитика не имеет ничего общего с текстовым анализом. В рассматриваемом контексте текстовый анализ относится к ручным методам изучения: внимательному чтению и качественному интерпретационному подходу. В то время как текстовая аналитика относится к количественному и вычислительному исследованию текста. Однако в этой работе, автор считает текстовый анализ и текстовую аналитику синонимами, беря во внимание всевозможные компьютерные, качественные или количественные методы анализа.

В то время как Distant Reading (DR), Corpus Linguistics (CL), Natural Language Processing (NLP) и Text Mining (TM) имеют общую цель использования текстовых данных, они все имеют весомые различия в своих подходах, методологиях и целях. Текстовый анализ можно рассматривать как общий термин, охватывающий другие типы анализа или подходов, упомянутые ранее. Далее мы рассмотрим подробнее данные подходы анализа, чтобы выделить их основные различия и связи с рассматриваемым «TA».

Distant Reading (DR) – подход к анализу (литературных) текстов, который впервые был разработан Франко Моретти Моретти. Он включает в себя анализ больших корпусов литературных текстов с использованием вычислительных методов для выявления широких закономерностей и тенденций [2, с. 18]. Distant Reading (DR) фокусируется на количественном анализе текстов, а не на качественном чтении. Это позволяет исследовать крупномасштабные закономерности и тенденции, которые было бы трудно различить с помощью традиционных методов исследования. «DR» – термин для приложений «TA», которые исследуют литературные и культурные тенденции путем анализа больших объемов текстовых данных. Напротив, чтение относится к традиционному методу подробного анализа текстов для интерпретации их значений. Хотя и «TA», и «DR» используют схожие вычислительные методы, они отличаются своими конечными прогнозами для достижения цели. Перспектива «DR» состоит в извлечении информации из текста без использования привычного редактирования, т.е. без чтения самих документов, а скорее сосредоточения на возникающих закономерностях в используемом языке [2, с. 21].

Corpus Linguistics (CL) Amador Moreno – отрасль лингвистики, которая включает в себя изучение языка с использованием больших массивов текста, именуемых как «корпуса» [3, с. 69]. Она направлен на анализ лингвистических явлений путем изучения закономерностей, частот слов и структур в корпусе. Корпусная лингвистика предоставляет эмпирические данные и понимание использования языка, вариаций и их изменений с течением времени.

Обработка естественного языка (NLP) Mitkov – область информатики, которая фокусируется на взаимоотношениях между компьютерами и привычным языком [4, с. 32]. Она фокусируется на разработке и оценке методов, которые направлены на систематизацию работы компьютеров с «пониманием», интерпретацией и генерацией человеческого языка

Ключевые аспекты «NLP» включают в себя понимание смысла и контекста текста или речи, извлечение информации из больших объемов неструктурированных данных и создание текста, приближенного к человеческому. Методы «NLP» используют «Machine Learning» и «Deep Learning» в различных приложениях:

– машинный перевод;
– распознавание речи;
– чат-боты;
– поиск информации и классификация текста.

Text Mining (TM) – область науки о данных, ориентированная на извлечение информации и идей из больших объемов неструктурированных текстовых данных [5, с. 112]. Text Mining (TM) основана на данных и обычно применяет автоматизированные методы без существенного контроля извне. Это позволяет эффективно обрабатывать обширные наборы текстовых значений с использованием методов «NLP», машинного обучения (ML) и статистики:

– классификация текста;
– кластеризация;
– анализ настроений;
– распознавание сущностей.

В настоящее время «TM» ассоциируется с набором больших данных, в среде которых ручной анализ непрактичен из-за массивного объема информации.

Текстовый анализ (TA) имеет более широкие возможности применения, чем Corpus Linguistics (CL) и Distant Reading (DR), поскольку он не ограничивается литературными текстами или пониманием языка. «TA» меньше фокусируется на разработке и тестировании вычислительных методов, как это происходит, к примеру, при обработке естественного языка (NLP). «TA» использует вычислительный анализ текста для решения широкого спектра тем, попадающих в сферу вычислительных гуманитарных исследований. Эта область представляет собой применение вычислительных методов в гуманитарных науках, с использованием изучения и анализа различных вопросов, связанных со знаниями о тексте в целом.

Список используемых источников

1. Бринк Х. Машинное обучение / Бринк Хенрик, Ричардс Джозеф, Феверолф Марк. СПб.: Питер. 2017. С. 336.
2. Иванько А. Ф., Сизова Ю. А. Нейронные сети: общие технологические характеристики // Научное обозрение. Технические науки, 2019. № 2. С. 17–23.
3. Петров И. В., Смирнова Е. Н. Применение нейронных сетей в обработке естественного языка // Вестник компьютерных и информационных технологий, 2021. № 5. С. 67–72.
4. Хобсон Л. Обработка естественного языка в действии / Хобсон Лейн, Ханнес Хапке, Коул Ховард.: пер. с англ. СПб.: Питер. 2020. С. 42.
5. Остроух А. В., Суркова Н. Е. Системы искусственного интеллекта: монография – Издательство «Лань». 2019. С. 228.

6. Томашевская В. С., Яковлев Д. А. Способы обработки неструктурированных данных // Russian Technological Journal, 2021. № 9 (1). С. 7–17.

Karlina K. **TEXT ANALYSIS. METHODS AND APPROACHES TO THE STUDY OF UNSTRUCTURED DATA.**

Saint Petersburg State University of Industrial Technologies and Design

In the context of the Artificial Intelligence (AL) population and unlimited flow of text information, there is a growing need to integrate effective methods for analyzing unstructured data. Text analysis (TA) is a powerful tool for processing and interpreting text. The combined use of computational methods allows us to identify practical knowledge and patterns in the text. This paper focuses on key concepts such as Distant Reading (DR), Corpus Linguistics (CL), Natural Language Processing (NLP), and Text Mining (TM). The author concludes that text analysis using the latest systems not only simplifies working with large amounts of data, but also allows us to make informed decisions based on the information extracted.

Key words: Text analytics, Artificial intelligence, Unstructured data, Text analysis methods

УДК 004.81
ГРНТИ 28.23.29

ТЕХНОЛОГИИ МОДЕЛИРОВАНИЯ РЕАЛИСТИЧНОГО ПОВЕДЕНИЯ ВИРТУАЛЬНЫХ ПЕРСОНАЖЕЙ

А. Е. Колмаков, В. Л. Литвинов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире возникает необходимость обеспечения реалистичного поведения виртуальных персонажей, к примеру, маскотов бренда. Существует множество способов решения этой проблемы, большинство из них имеет низкое отношение эффективности к затратам. Самым эффективным способом оказывается развивающаяся технология эмоционального ИИ (Emotional AI).

эмоциональный ИИ, виртуальный персонаж, моделирование поведения

Введение

Трехмерная анимация приобретает все большую популярность и продолжает развиваться. Она широко используется в различных сферах человеческой деятельности, таких как медицина, обучение, развлечения, реклама.

Актуальность исследования обусловлена ростом проникновения трехмерной графики в различные сферы деятельности потенциального Потребителя, а также постепенным развитием технологий виртуальной и дополненной реальностей. Качественная и реалистичная анимация персонажей играет важную роль в создании впечатляющих и запоминающихся образов, увеличивает прибыль с продаж продукции, использующей трехмерную графику, повышает уровень доверия и интереса к системам искусственного интеллекта [1].

Цель данной исследовательской работы заключается в изучении поведения виртуальных трехмерных персонажей. Для достижения этой цели необходимо решить следующие задачи:

– ввести понятие виртуального цифрового персонажа;

– исследовать существующие способы повышения реалистичности виртуальных персонажей;

– провести сравнение существующих способов повышения реалистичности виртуальных персонажей, выделить их достоинства и недостатки;

– выбрать наиболее простой и удобный, но в то же время действенный способ.

В данной работе подразумевается, что виртуальный персонаж – это компьютерная модель, способная взаимодействовать с пользователем в трехмерном пространстве. Такие агенты используются в различных областях, например, в играх, симуляторах, обучении и рекламе. Реалистичность характеризует степень доверия человека виртуальной модели разумного существа [2].

В данной работе опускаются философские и гуманистические аспекты замены человека виртуальными персонажами. Подразумевается, что виртуальный персонаж не является разумным существом [3].

Методы исследования включают в себя:

– анализ литературы и исследований в области виртуальной реальности, трехмерной графики и поведения персонажей;

– анализ и интерпретация полученных результатов.

Виртуальный цифровой персонаж

Виртуальный цифровой персонаж есть интерфейс для взаимодействия между человеком и системой поддержки принятия решений. Модель персонажа может быть любым маскотом того или иного бренда – хоть Колобком, хоть Микки Маусом. Модель персонажа может быть двухмерной, может быть трехмерной и обладать поведением, соответствующим ситуации. Она получает входной сигнал, демонстрируя заинтересованность в вопросе, передает его на обработку в «мозг» и возвращает ответ в формате живой речи и эмоций, применяя эмоциональный ИИ (Emotional AI).

Чтобы виртуальные персонажи выглядели реалистично и убедительно, используются различные методы, такие как поведенческое моделирование, искусственный интеллект и машинное обучение.

Поведенческое моделирование

Виртуальные персонажи должны уметь реагировать на окружающую среду и взаимодействовать с пользователем. Это достигается с помощью следующих методов.

1. Скрипты поведения. Персонажи выполняют заранее определенные действия в ответ на определенные условия.

2. Системы конечных состояний. Персонажи переходят между различными состояниями в зависимости от внутренних и внешних стимулов.

3. Алгоритмы планирования. Персонажи планируют свои действия наперед, что позволяет им выполнять более сложные задачи.

Искусственный интеллект

ИИ помогает создавать реалистичное поведение персонажей. Обозначим основные методы работы с ним.

1. Обучение с подкреплением. Персонажи учатся на собственном опыте, получая вознаграждение за правильные действия и наказание за ошибки.

2. Генетические алгоритмы. Эти алгоритмы используются для оптимизации поведения персонажей через эволюционные вычисления.

3. Нейронные сети. Позволяют персонажам распознавать сложные паттерны и принимать решения на основе больших объемов данных.

Моделирование эмоций и личности

Чтобы персонажи выглядели еще более реалистично, нужно учитывать их эмоции и личность:

– модели эмоций используются для симуляции эмоциональных реакций на разные события;

– моделирование личности, при этом персонажи наделяются уникальными чертами характера, которые влияют на их поведение.

Взаимодействие с окружающей средой

Виртуальные персонажи должны взаимодействовать с окружающей средой:

– физическое моделирование – персонажи должны подчиняться законам физики;

– социальное взаимодействие – учитываются взаимоотношения между персонажами и их взаимодействие в социальных ситуациях.

Сравнительный анализ технологий

В таблице 1 указаны достоинства и недостатки данных технологий.

ТАБЛИЦА 1. Достоинства и недостатки технологий моделирования реалистичных виртуальных персонажей

Технология	Достоинства	Недостатки
Скрипты поведения	– Простота реализации: легко создается и настраивается разработчиками. – Предсказуемость: поведение персонажа легко контролируется	– Ограниченность: персонажи действуют строго по заранее определенному сценарию, что может показаться неестественным. – Отсутствие адаптивности: не могут реагировать на непредвиденные ситуации
Системы конечных состояний	– Гибкость: персонажи могут переходить между состояниями в зависимости от условий	– Сложность: с увеличением числа состояний управление может стать сложным

Технология	Достоинства	Недостатки
	– Упрощение отладки: легко тестировать и отлаживать каждое состояние отдельно	– Трудоемкость: требует значительных усилий для создания и поддержания множества состояний
Алгоритмы планирования	– Интеллект: позволяют персонажам принимать сложные решения. – Адаптивность: персонажи могут планировать свои действия в зависимости от ситуации	– Ресурсоемкость: высокие требования к вычислительным ресурсам. – Непредсказуемость: могут возникать неожиданные решения, которые не всегда соответствуют задумке разработчиков
Обучение с подкреплением	– Самообучение: персонажи улучшают свое поведение с опытом. – Адаптивность: способность учиться и адаптироваться к новым ситуациям	– Сложность настройки: требует большого количества данных и времени для обучения. – Непредсказуемость: не всегда можно точно предсказать поведение персонажа
Генетические алгоритмы	– Оптимизация: позволяют находить наиболее удачные решения для сложных задач. – Эволюционность: могут со временем улучшаться	– Сложность реализации: требуют серьезных знаний в области эволюционных алгоритмов. – Ресурсоемкость: требуют серьезных вычислительных ресурсов
Нейронные сети	– Распознавание паттернов: Способность распознавать сложные закономерности и принимать решения. – Гибкость: подходят для широкого круга задач	– Требования к данным: необходимы большие объемы данных для обучения. – Сложность настройки: трудоемкий процесс настройки и оптимизации
Модели эмоций	– Глубина взаимодействия: персонажи могут выражать эмоции, что делает их более человечными. – Улучшение пользовательского опыта: реалистичные эмоции способствуют вовлечению пользователя в процесс	– Сложность моделирования: трудно создать реалистичные модели эмоций, которые точно отражают человеческие чувства. – Аппаратные ресурсы: высокие требования к вычислительным ресурсам для обработки эмоциональных реакций в реальном времени
Моделирование личности	– Уникальность: каждый персонаж может иметь свою уникальную личность, что делает взаимодействие с ними более интересным. – Реализм: персонажи с разными личностями действуют по–разному, что добавляет реализма в виртуальные миры	– Сложность разработки: требует глубокого понимания психологии и поведения для создания правдоподобных личностей. – Трудоемкость: значительные усилия для разработки и настройки каждой уникальной личности
Физическое моделирование	– Реализм: персонажи подчиняются законам физики, что делает их движения и взаимодействие с окружающей средой правдоподобными. – Интерактивность: позволяет персонажам взаимодействовать с объектами и элементами окружения	– Высокие вычислительные затраты: требует значительных ресурсов для расчета физических взаимодействий в реальном времени. – Сложность моделирования: трудно обеспечить корректное моделирование всех аспектов физического взаимодействия

Технология	Достоинства	Недостатки
Социальное взаимодействие	– Правдоподобие: персонажи могут взаимодействовать друг с другом, что создает ощущение живого мира. – Динамика: возможность создания сложных социальных сценариев и взаимодействий	– Сложность: трудно создать реалистичные социальные взаимодействия, учитывая множество факторов и нюансов. – Зависимости: необходимо учитывать множество переменных и условий, что усложняет разработку

Анализируя все вышеперечисленные методы, можно сделать вывод, что использование мыслительных моделей на основе специальных алгоритмов является наиболее затратной стороной вопроса и представляет высокую вычислительную сложность, и к тому же весьма избыточно. С другой же стороны, моделирование социальное обладает сложностью с научной точки зрения - необходимо учесть чрезвычайно много аспектов и нюансов. Физическое моделирование в данном случае имеет мало смысла, поскольку виртуальные персонажи не обязаны быть анатомически реалистичными, многие из них являются продукцией творчества мультипликаторов, которые создают своих героев скорее под стать плюшевым игрушкам, нежели биологически точным органическим существам. Это в свою очередь повышает продаваемость виртуального персонажа [4].

Наиболее впечатляющие результаты может дать моделирование эмоций и личности. Эти технологии способны создать виртуальных персонажей, которые не только реалистичны с точки зрения внешнего поведения, но и могут эмоционально взаимодействовать с пользователем, что значительно усиливает доверие к виртуальным персонажам. Ключевое слово здесь - «значительно».

Например, исследование, проведенное в 2020 году, показало, что люди, которые взаимодействуют с роботами, обладающими эмоциональным интеллектом, чувствуют больше доверия и комфорта по сравнению с теми, кто взаимодействует с роботами без таких способностей. Это связано с тем, что роботы с эмоциональным интеллектом могут лучше понимать и реагировать на эмоции людей, что делает взаимодействие более естественным [5].

Таким образом, следует усиливать эмоциональный интеллект виртуального персонажа, чтобы обеспечить наиболее точное взаимодействие человека с искусственным интеллектом.

Список используемых источников

1. Уракова Е. А. Агентное моделирование в компьютерной графике и играх // Вестник Московского университета. Серия 15: Вычислительная математика и кибернетика, 2019. № 4. С. 28–34.

2. Дмитриева Е. С., Гельман В. Я., Зайцева К. А., Орлов А. М. Оценка связи восприятия эмоциональной интонации речи с компонентами эмоционального интеллекта, 2012. Т. 9. № 1. С. 126–134.
3. Щербаков М. Г. Эмоциональный интеллект как элемент системы искусственного интеллекта: этические и правовые вопросы // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки, 2022. №3. URL: https://cyberleninka.ru/article/n/emotsionalnyy-intellekt-kak-element-sistemy-iskusstvennogo-intellekta-eticheskie-i-pravovye-voprosy (дата обращения 04.11.2024).
4. Мамина Р. И., Пирайнен Е. В. Эмоциональный искусственный интеллект как инструмент взаимодействия человека и машины // Дискурс, 2023. №9 (2). С. 35-51. URL: https://doi.org/10.32603/2412-8562-2023-9-2-35-51 (дата обращения 20.10.2024).
5. Хрисанфова Е. Эмоциональный ИИ: кто и зачем распознает эмоции в России и за рубежом. URL: https://rb.ru/longread/emotion-ai/ (дата обращения 20.10.2024).

Kolmakov A., Litvinov V. **TECHNOLOGIES FOR SIMULATING VIRTUAL CHARACTERS REALISTIC BEHAVIOR.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the modern world, there is a need to ensure realistic behavior of virtual characters, for example, brand mascots. There are many ways to solve this problem, most of them have a low cost-effectiveness ratio. The most effective way is the developing technology of emotional AI.

Key words: Emotional AI, virtual character, behavior modeling.

УДК 004.891.3
ГРНТИ 28.23.02

ИНТЕРПРЕТИРУЕМОСТЬ РЕЗУЛЬТАТОВ РАБОТЫ ML МОДЕЛЕЙ И МЕТОДЫ ПОВЫШЕНИЯ ПРОЗРАЧНОСТИ

Е. В. Копытова, В. К. Мавричев, Д. В. Петров, Ф. В. Филиппов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается интерпретируемость ML моделей, описывается ее влияние на уровень доверия пользователей к основанным на них системам. Анализируются пост-объяснительные методы LIME и SHAP. Уделяется внимание этическим аспектам и правовому регулированию. Описываются основные факторы, влияющие на восприятие ИИ, в том числе баланс между интерпретируемостью и производительностью моделей.

интерпретируемость, методы объяснимого ИИ, LIME, SHAP, прозрачность, этические аспекты

С развитием искусственного интеллекта (ИИ) и внедрением его в различные отрасли, встал серьезный вопрос доверия пользователей к подобным системам [1]. Ключевым фактором, влияющим на уровень доверия, является способность ИИ-системы объяснить свои решения. Проблема интерпретируемости особенно сложных моделей машинного обучения привлекает все больше внимания исследователей и разработчиков, поскольку отсутствие факторов, по которым было принято то или иное решение, может заставить пользователя усомниться в качестве выводов, что в свою очередь затрудняет интеграцию ИИ в критически важные области науки.

Способность ИИ-системы объяснить пользователю причины принятия решений называется интерпретируемостью [2], данной особенностью отличаются современные ML модели. Не понимая выводов модели, причин определенных решений, пользователи могут сомневаться в ее справедливости и точности, ведь ошибочные решения могут привести к серьезным последствиям и убыткам.

Так в 2024 году вопросы регулирования и интерпретируемости ИИ начали находить свое отражение в правовом поле, например:

– *Евросоюз,* март 2024 года принят первый в мире закон, регулирующий разработку и применение ИИ. Документ классифицирует риски и устанавливает требования к системам ИИ в зависимости от их категории. Например, системы, которые подвержены подсознательному манипулированию и биомет-

рической классификации людей на основе чувствительных характеристик, отнесены к недопустимым рискам и запрещены;

– *США,* подписан указ о безопасном, надежном и заслуживающем доверия развитии и использовании ИИ. Документ охватывает восемь направлений политики и направлен на обеспечение новых стандартов безопасности и надежности ИИ, защиту конфиденциальности американцев, продвижение равенства и гражданских прав, защиту интересов потребителей и рабочих, а также стимулирование инноваций и конкуренции [3];

– *Китай,* приняты временные меры, предусматривающие ответственность разработчиков ИИ за генерируемый контент. Введен запрет на контент, подрывающий социалистические ценности или подстрекающий к свержению государственного строя. Разработчики в ответе за персональные данные пользователей, а также за соблюдение прав на интеллектуальную собственность;

– *Российская Федерация,* готовит законопроект регулирования в сфере ИИ. Документ должен определить ответственность за разработку систем ИИ и создаваемый с их помощью контент и исключить использование технологии мошенниками;

– *ООН,* запуск инициативы «ИИ для всеобщего блага» (AI for Good);

– *ОЭСР,* приняты руководящие принципы управления системами ИИ.

Интерпретируемость модели [4], ни что иное, как способность понять взаимосвязь между переменными и то, как они влияют на прогноз. Простые модели, например такие как линейная регрессия, обычно интерпретируются проще, чем более сложные модели, такие как нейронные сети. Интерпретируемость помогает не только пользователям, но и разработчикам и регуляторам, позволяя им выявить и устранить возможные ошибки или предвзятость в работе модели [5].

Производительность модели влияет на точность и качество прогнозов. При сравнении различных моделей нужно выбирать именно ту, которая лучше справится с такими метриками, как «средняя квадратичная ошибка» (MSE) и «средняя абсолютная ошибка» (MAE).

Равновесие между интерпретируемостью и производительностью в машинном обучении (ML) заключается в следующем: более сложные модели обычно имеют более точные предсказания. Но у этого есть и своя цена - снижение интерпретируемости того, по причине чего были сделаны те или иные прогнозы, а также возможное повышение сложности ввода в эксплуатацию. Как показало исследование [6], опубликованное в сентябре 2024 года, строгого компромисса между эффективностью прогнозирования и интерпретируемостью модели для табличных данных - нет. Например, обобщенные адди-

тивные модели (GAMS) обладают свойствами для захвата сложных нелинейных закономерностей, оставаясь при этом полностью интерпретируемыми [7].

Не стоит забывать и про этические аспекты. Одной из главных этических проблем, связанных с использованием ИИ-систем – вопрос ответственности за ошибки. Когда модель не может объяснить, почему было принято то или иное решение, это ставит под сомнение прозрачность процесса, а также затрудняет определение зон ответственности за ошибочные выводы.

Многие модели машинного обучения могут быть подвержены предвзятости, что может привезти к дискриминационным решениям. Особенно это может быть критичным в таких областях, как найм на работу или кредитование. Интерпретируемость позволяет выявить подобные предвзятости и принять меры для их устранения. Без возможности объяснить решения ИИ предвзятость может остаться незамеченной, что в свою очередь может нарушить этические принципы справедливости. Есть и обратная сторона медали, слишком высокая прозрачность может привести к манипуляциям, если пользователи понимают, как именно модель принимает решения, они могут намеренно изменять вводные данные и влиять на получение выгодных результатов для них результатов. То есть при формировании модели перед разработчиком ставится задача по нахождению баланса между прозрачностью и защитой от манипуляций.

Методы повышения интерпретируемости

В первую очередь стоит обратить внимание на два главных метода увеличения прозрачности принимаемых моделями решений LIME (Local Interpretable Model-agnostic Explanations) и SHAP (SHapley Additive exPlanations) [8]. Популярность методов заключается в том, что они используются для объяснения решений сложных моделей машинного обучения. Использование данных методов позволяет понять, почему модель сделала то или иное предсказание, что в свою очередь помогает повысить интерпретируемость и доверие пользователей к ИИ-системам.

LIME – метод, позволяющий объяснять предсказания любой модели путем создания интерпретируемой локальной аппроксимации для каждого конкретного случая. Достигается это благодаря генерации более простой модели, обученной на небольшом наборе данных, близких к точке предсказания, для объяснения конкретного предсказания.

Метод LIME очень полезен в случаях, когда требуется понять, почему модель сделала конкретное предсказание для конкретного набора входных данных. Например, в случае медицинских приложений LIME может показать, какие признаки пациента оказали наибольшее влияние на диагноз, предложенный ИИ.

Метод SHAP основан на теории игр и использует значения Шепли для трактовки вклада каждого входного признака в итоговое предсказание модели. SHAP предлагает математически обоснованный подход к интерпретируемости, который может быть применен как для локальных, так и для глобальных объяснений. Метод SHAP позволяет увидеть, как каждый входной признак влияет на конечное предсказание модели. SHAP особенно полезен для понимания не только отдельных предсказаний, но и общего поведения модели.

Подведя итог, следует выделить основные плюсы и минусы обоих методов, которые для удобства представлены в таблице 1.

ТАБЛИЦА 1. Преимущества и недостатки методов LIME и SHAP

Метод	Преимущества	Недостатки
LIME	Локальная интерпретируемость: объясняет отдельные предсказания	Предоставляет только локальные объяснения, не отражая глобальное поведение модели
	Подходит для любой модели (независим от архитектуры)	Результаты могут быть нестабильны в зависимости от выбора данных для аппроксимации
	Простота и гибкость применения на разных типах данных (текст, изображения, таблицы)	Иногда слишком упрощает модель, что может искажать истинные причины предсказаний
	Быстрое вычисление на небольших наборах данных	
SHAP	Обеспечивает как локальные, так и глобальные объяснения поведения модели	Высокие вычислительные затраты, особенно для сложных моделей
	Теоретически обоснованное распределение вклада признаков, что делает его выводы более справедливыми и точными	Может быть медленным при расчете объяснений для большого числа признаков или сложных моделей
	Универсальность: подходит для объяснения как отдельных предсказаний, так и общей интерпретируемости модели	

Заключение

Интерпретируемость является важнейшим аспектом, напрямую влияющим на доверие пользователей к ИИ-системам. Пост-объяснительные методы, такие как LIME и SHAP, помогают улучшить интерпретируемость сложных ML моделей, повышая прозрачность и давая пользователям возможность понять и проверить решения, принимаемые искусственным интеллектом.

Важно помнить, что для успешного внедрения ИИ-систем в критические области нужно обеспечить не только высокую производительность, но и баланс между интерпретируемостью, точностью, справедливостью и ответственностью, что в результате повысит доверие пользователей и улучшит принятие перспективных технологий. Необходимо помнить, что ИИ-системы также необходимо защитить от возможных противоправных манипуляций.

Список используемых источников

1. Копытова Е. В., Мавричев В. К., Петров Д. В., Филиппов Ф. В. Проблемы этики в области искусственного интеллекта // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб, СПбГУТ, 2024. С. 399–402. EDN BKTUDO.
2. Интерпретируемый ИИ, или как я научился перестать беспокоиться и доверять ИИ // skine.ru URL: https://skine.ru/articles/368914/ (дата обращения 16.10.2024).
3. What to Expect in Evolving U.S. Regulation of Artificial Intelligence in 2024. URL: https://www.foley.com/insights/publications/2023/12/us-regulation-artificial-intelligence-2024/ (дата обращения 16.10.2024).
4. Interpretability in Machine Learning: An Overview // The Gradient URL: https://thegradient.pub/interpretability-in-ml-a-broad-overview/ (дата обращения 16.10.2024).
5. Zachary C. Lipton the Mythos of Model Interpretability 6 Mar 2017. URL: https://arxiv.org/pdf/1606.03490 (дата обращения 16.10.2024).
6. Дашков А. А., Нестерова Ю. О. Построение доверия при использовании искусственного интеллекта // E-Management, 2021. №2. URL: https://cyberleninka.ru/article/n/postroenie-doveriya-pri-ispolzovanii-iskusstvennogo-intellekta (дата обращения 16.10.2024).
7. Challenging the Performance-Interpretability Trade-off: An Evaluation of Interpretable Machine Learning Models Sven Kruschel, Nico Hambauer, Sven Weinzierl, Sandra Zilker, Mathias Kraus, Patrick Zschech 22 Sep 2024 URL: https://arxiv.org/pdf/2409.14429v1 (дата обращения 16.10.2024).
8. LIME и SHAP // Хабр URL: https://habr.com/ru/companies/otus/articles/779430/ (дата обращения 16.10.2024).

Kopytova E., Mavrichev V., Petrov D., Philippov F. **INTERPRETABILITY OF ML MODELS RESULTS AND METHODS OF INCREASING TRANSPARENCY.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The interpretability of ML models is considered, its impact on the level of user trust in systems based on them is described. The post-explanatory methods LIME and SHAP are analyzed. Attention is paid to ethical aspects and legal regulation. The main factors influencing the perception of AI are described, including the balance between interpretability and model performance.

Key words: interpretability, explainable AI methods, LIME, SHAP, transparency, ethical aspects.

УДК 681.5
ГРНТИ 28.23.25

МЕТОДЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ОБЪЕКТАМИ ПРИ ПОМОЩИ НЕЙРОСЕТЕВЫХ РЕГУЛЯТОРОВ

Д. А. Корнюшкин, А. А. Крылов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время нейросетевые регуляторы непрерывной адаптации успешно внедряются в системы управления технологическими объектами. Современные объекты и их системы управления достигли предельного уровня сложности и сделали невозможным использование успешно применяемых ранее методов. Нейросетевые регуляторы призваны устранить существующие проблемы в системах управления и повысить уровень статических и динамических характеристик объекта.

искусственные нейронные сети, методы обучения, нейросетевые регуляторы непрерывной адаптации, адаптация

Необходимость разработки и внедрения новых методов управления технологическими объектами возникла из-за отсутствия возможности производить точные измерения и расчеты параметров системы, и нелинейных характеристик оборудования, автоматизированных нейросетевых систем управления техническими объектами с нелинейными и неопределенными характеристиками [1]. Данную проблему можно решить при помощи систем на базе искусственного интеллекта, которые подходят для решения проблем, как в статических, так и в динамических системах.

Нейросетевые регуляторы непрерывной адаптации подходят динамически изменяющимся системам, потому что они позволяют:

– по результатам получения данных в ходе даже первого эксперимента позволяют производить оптимальную исходную настройку регулятора;

– производить вычисления в условиях, когда динамические подсистемы объекта находятся в переходном состоянии, что в свою очередь, позволяет нейросетевому регулятору и системе управления адаптироваться и активировать необходимый сценарий работы.

Рассмотрим наиболее популярные методы работы нейросетевых регуляторов.

1. Метод непрерывной адаптации нейросетевого регулятора. Данный метод характеризуется функционированием нейронной сети с отсутствием замкнутого цикла между нейронами и однонаправленной передачей информации от конкретных входов к концертным выходам.

2. Метод синтеза адаптивного подчиненно-нейронного регулирования. Данный метод характеризуется системой управления с наличием обратной связи, причем количество контуров управления с обратной связью, соотнесено с множеством контролируемых параметров. То есть каждый контур обратной связи формируется для контроля предопределенного параметра. Для синтезирования итогового результата, контуры обратной связи имеют логическую взаимосвязь.

3. Метод адаптации по обнаружению ресинхронизации или обнаружения противоречий. Для предопределенного набора параметров не в аварийной ситуации метод предполагает отсутствие изменений нейронных сетей, однако, при наличии отклонений предопределенного уровня, изменяет функционирование блока управления объекта.

Как правило, математические модели для проектируемого объекта являются весьма упрощенными. Предопределить заранее количество параметров для расчетов является достаточно трудоемкой операцией. Если количество параметров сравнительно мало, то модель становится слишком упрощенной и результат может существенным образом отличаться от полученных эксплуатационных характеристик реального объекта. Для избыточного количества математических моделей характерно существенное усложнение алгоритмов [2]. Решением для выбора оптимального количества параметров является использование нейросетевых регуляторов. Полученная система не только использует оптимальное количество параметров, отсекая неизменяемые или слабо изменяемые, но и получает данные с реально существующего объекта управления, фактически не применяемую его математическую модель [3].

Сложность управления динамическими подсистемами объекта по заданным сценариям обусловлена следующими факторами:

1. Невозможность точно узнать, являются ли полученные параметры регулятора оптимальными. Для получения наиболее оптимальных параметров регулятора требуется повторять процесс оптимизации несколько раз и с выбором наилучшего результата;

2. Трудоемкость в составлении обучающей выборки. При составлении обучающей выборки необходимо корректно подобрать подходящий идентифицирующий процесс;

3. Необходимость переобучения. Если по сравнению с ошибкой на тренировочных данных, на валидационной модели ошибка уменьшается, то нейронная сеть корректно переобучилась.

4. Перерегулирование. Система в любом положении стремиться свести к минимуму параметр рассогласования, а методом устранения данной проблемы является увеличение управляющего воздействия.

5. Возможность наличия недопустимых управляющих сигналов. Набор управляющих сигналов может сказаться, как на повышенном электропотреблении, так и в выводе приборов и устройств за границы их корректной работы.

Для исключения вышеперечисленных ошибок и недопустимости работы необходимо перейти к активации сценариев при помощи нейронных сетей. Активация сценариев работы при помощи нейронных систем имеет множество вариаций развития событий и режимов функционирования оборудования [4]. Так же реализуемая система предлагает различные варианты по улучшению режимов работы оборудования на объекте. Основными параметрами, над улучшением которых работает система, являются, увеличение скорости реакции, повышение уровня безопасности, экономия электроэнергии [5]. Данные расчеты производятся в «режиме сна». Система выполняет расчет сценариев с целью оптимизации предыдущих сценариев и с прогнозированием результатов, и предложений новых сценариев по результатам накопленных результатов интегрально накопленных предыдущих периодов.

Расчет оптимизации режимов переключения, предложенных оператору для принятия новых сценариев работы в качестве:

– основного режима;

– одного из вариантов, не являющимся приоритетным;

– варианта требующего накопления статистики и дальнейшего использования.

Например, для работы различных сценариев, предложенных при помощи нейросетевого регулятора для типового спортивного комплекса, в том числе, должно зависеть от типа запланированных мероприятий, прогноза погоды, полученного от локальной и ряда внешних метеостанций, вида спорта, проводимого на объекте исследования, в зависимости от того, в тренировочном или официальном формате проходит событие, от количества проданных билетов, а также от фактического количества зрителей на трибунах.

В случае если система регистрирует неисправности в работе оборудования, которые не превышают критических значений, приводящих к поломкам и остановки системы в целом, то активируется сценарий о возникновении дефекта в конкретном узле или агрегате [6]. Данные действия позволяют как скорректировать работу системы, так и назначить ремонт или замену конкретного узла во время следующей плановой остановки.

У каждого оборудования на объекте существует заданный производителем объем повреждений, по достижению которого оборудование полностью выходит из строя [7, 8]. Данные критических параметров хранятся в «модели угроз». Система так же анализирует данные, полученные в ходе эксплуатации оборудования на объекте и определяет значения, при которых систему необходимо либо дублировать устройством схожим по его функционалу, либо, при

заранее выявленной угрозе, минимизировать ущерб функционированию объекта.

Заключение

Проведенные исследования показали, что внедрение метода непрерывной адаптации нейросетевого регулятора для системы управления технологическим объектом, который характеризуется наличием динамически изменяющихся подсистем позволили устранить существующие проблемы управления и избежать рассогласования в режимах работы, позволяет устранить существующую проблему управления, как отдельно взятых подсистемах, так и для всего комплекса в целом.

Список используемых источников

1. Феофилов С. В. Анализ методов обучения искусственной нейронной сети /С. В. Феофилов, Д. Л. Хапкин // Сборник конференции XVIII Всероссийской научно-технической конференции студентов, магистрантов, аспирантов и молодых ученых «Техника XXI века глазами молодых ученых и специалистов». Тула: изд. ТулГУ, 2020. С. 88–96.
2. Хапкин Д. Л. Синтез гарантированно устойчивых нейросетевых регуляторов с оптимизацией качества переходного процесса / Д. Л. Хапкин, С. В. Феофилов, А. В. Козырь // Известия ТулГУ. Технические науки, 2022. № 12. С. 128–133.
3. Зацаринный А. А., Сучков А. П. Информационное взаимодействие в распределенных системах ситуационного управления. М.: ТОРУС ПРЕСС, 2021. 268 с.
4. Воевода А. А. Расчет регулятора для многоканального объекта с нестационарными параметрами, содержащего звенья запаздывания / А. А. Воевода, В. И. Шипагин // Системы анализа и обработки данных, 2022. № 1 (85). С. 7–24.
5. Бобобеков К. М., Воевода А. А., Шипагин В. И. Полиномиальный метод синтеза автоматического управления для одноканальных и многоканальных объектов: монография. – Душанбе: ТТУ им. М.С. Осими, 2021. 192 с.
6. Белов А. М., Белов М. П. Применение нейронных сетей в электроприводных системах насосных агрегатов // Междунар. конф. по мягким вычислениям и измерениям. СПбГЭТУ «ЛЭТИ», 2022. Т. 1. С. 91–94.
7. Шолтанюк С.В. Влияние гиперпараметров нейронной сети на ее численную обусловленность // Цифровая трансформация, 2020. № 1. С. 43–50.
8. Сиддиков И. Х., Каландаров П. И., Ядгарова Д. Б., Исматуллаев Х. Н. Алгоритм адаптации параметров нейро-нечеткого регулятора на основе метода разности площадей // Математическое и программное обеспечение в промышленной и социальной сферах. 2021. Т. 9. № 1.

Kornyushkin D., Krylov A. **METHODS OF CONTROLLING TECHNOLOGICAL OBJECTS USING NEURAL NETWORK REGULATORS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

At present, neural network regulators of continuous adaptation are successfully implemented in control systems of technological objects. Modern objects and their control systems have reached the ultimate level of complexity and made it impossible to use the previously successfully applied methods. Neural network regulators are designed to eliminate the existing problems in control systems and improve the level of static and dynamic characteristics of the object.

Key words: Artificial neural networks, learning methods, continuous adaptation neural network regulators, adaptation.

УДК 004.056.5
ГРНТИ 81.93.29

ПРОГНОЗИРОВАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ АНАЛИЗА ОТКРЫТЫХ ДАННЫХ

Е. В. Коровкина, В. Л. Литвинов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается актуальные вопросы информационной безопасности в условиях активного использования открытых данных для анализа угроз. Рассмотрены основные подходы к прогнозированию угроз, включая методы сбора и обработки информации из открытых источников. Приведен анализ рисков, связанных с потенциальной утечкой и манипуляцией данными, а также предложены меры для повышения уровня защищенности информации в условиях постоянно изменяющихся угроз. Особое внимание уделено техническим и аналитическим аспектам использования OSINT (Open Source Intelligence) в информационной безопасности.

информационная безопасность, открытые данные, OSINT, прогнозирование угроз, анализ рисков

С развитием цифровых технологий использование открытых данных (OSINT) для анализа информационных угроз стало необходимым компонентом современной системы информационной безопасности. Многочисленные исследования показывают, что своевременное и точное прогнозирование угроз позволяет организациям предотвращать инциденты, связанные с утечками данных и внешними атаками [1]. Однако процесс анализа открытых данных содержит в себе ряд рисков и требует особого подхода к их интерпретации и защите.

В рамках данного исследования раскрываются ключевые методы прогнозирования угроз информационной безопасности на основе OSINT, включая этапы сбора, анализа и классификации данных. В статье представлены практические рекомендации по организации системы прогнозирования угроз, ориентированной на идентификацию паттернов и потенциальных угроз на ранних стадиях. На основе собранных данных создается структурированный процесс обработки информации, включающий применение технологий автоматического анализа, машинного обучения и методов интеллектуальной обработки текста.

Методы прогнозирования угроз на основе OSINT предполагают использование различных источников данных, таких как социальные сети, форумы, блоги и информационные порталы [2]. В условиях постоянно растущего объ-

ема данных системы информационной безопасности требуют эффективного инструментария для мониторинга и анализа информации. Ниже перечислены основные этапы обработки данных для прогнозирования угроз.

1. Сбор информации из открытых источников. Применяются автоматизированные скрипты и API для сбора данных с платформ ВКонтакте, HeadHunter и других ресурсов.

2. Классификация и фильтрация данных. Использование алгоритмов для отсеивания нерелевантной информации и фокусировка на ключевых темах и пользователях, представляющих интерес.

3. Анализ данных для выявления паттернов и угроз. Применение методов машинного обучения и обработки естественного языка (NLP) для обнаружения аномалий и трендов, потенциально указывающих на угрозы.

4. Прогнозирование и моделирование. Использование собранных данных для предсказания вероятных угроз на основе анализа исторических данных и текущих тенденций.

Таблица 1 представляет собой сводную характеристику различных угроз информационной безопасности, идентифицированных в процессе анализа открытых данных, а также соответствующих методов их предотвращения.

ТАБЛИЦА 1. Характеристка угроз информационной безопасности

Тип угрозы	Источник данных	Метод обнаружения	Рекомендуемые меры
Нарушение конфиденциальности	Социальные сети	Поиск ключевых слов, мониторинг упоминаний	Ограничение доступа, настройка фильтров
Утечка корпоративной информации	Сайты вакансий и форумы	Сравнение контента с базой данных, отслеживание ключевых тем	Усиление мониторинга, обучение сотрудников
Целевая фишинговая атака	Электронные рассылки, блоги	Анализ текстов, распознавание аномалий	Уведомления, автоматическое блокирование подозрительных сообщений
Дезинформация	Социальные сети, блоги	Сравнение данных из разных источников	Факт-чекинг, использование проверенных источников
Вредоносное ПО	Файлообменники, форумы	Анализ файлов, поиск сигнатур	Установка антивирусных решений, контроль доступа

Прогнозирование угроз на основе OSINT позволяет своевременно реагировать на угрозы информационной безопасности, используя актуальные дан-

ные из открытых источников [3]. Анализ угроз информационной безопасности требует комплексного подхода, который включает мониторинг данных, автоматизированную обработку информации и применение современных технологий защиты данных.

Применение методов машинного обучения, включая кластеризацию данных и выявление аномалий, способствует выявлению новых угроз. Так, регулярный анализ данных о вакансиях позволяет обнаруживать утечки информации о внутренних процессах компании. Аналогично, мониторинг социальных сетей позволяет оперативно выявлять случаи утечки конфиденциальной информации и целевые фишинговые атаки, направленные на ключевых сотрудников.

Введение таких мер, как контроль доступа и регулярное обучение сотрудников, позволяет минимизировать риск утечек данных и повысить осведомленность о методах социальной инженерии, используемых злоумышленниками. Таким образом, OSINT-технологии играют важную роль в современной системе информационной безопасности, позволяя своевременно выявлять потенциальные угрозы и предупреждать кибератаки.

Прогнозирование угроз информационной безопасности на основе анализа открытых данных становится неотъемлемой частью эффективной системы защиты. Система, использующая OSINT, требует постоянного мониторинга данных и применения инновационных методов анализа [4]. Только интеграция передовых технологий анализа данных с грамотной политикой безопасности позволит компании оставаться защищенной в условиях растущего числа информационных угроз. Современные методы OSINT позволяют организациям своевременно выявлять потенциальные угрозы и, таким образом, минимизировать риски, связанные с утечками и искажением информации.

Список используемых источников

1. Батоев В. Б. О технологии поиска по открытым источникам «OSINT» в оперативно-розыскной деятельности. URL: https://cyberleninka.ru/article/n/o-tehnologii-poiska-po-otkrytym-istochnikam-osint-v-operativno-rozysknoy-deyatelnosti (дата обращения 04.11.2024).
2. Использование OSINT в раскрытии и расследовании преступлений. URL: https://cyberleninka.ru/article/n/ispolzovanie-osint-v-raskrytii-i-rassledovanii-prestupleniy (дата обращения 04.11.2024).
3. Информационная безопасность: современные реалии. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-sovremennye-realii (дата обращения 04.11.2024).
4. Ageeva V., Novokhrestov A., Kholodova M. Threats to the information system in the physical environment and cyberspace // arxiv.org. URL: https://arxiv.org/abs/2012.02511 (дата обращения 04.11.2024).

Korovkina E., Litvinov V. **FORECASTING INFORMATION SECURITY THREATS BASED ON OPEN DATA ANALYSIS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article addresses the current issue of information security in the context of actively using open data for threat analysis. The main approaches to threat forecasting are considered, including methods for collecting and processing information from open sources. An analysis of risks associated with potential data leaks and manipulation is provided, along with proposed measures to enhance information protection in a constantly evolving threat landscape. Special attention is given to the technical and analytical aspects of using OSINT (OpenSource Intelligence) in information security.

Key words: information security, open data, OSINT, threat forecasting, risk analysis.

УДК 378.146
ГРНТИ 14.35.09

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УЧЕБНОМ ПРОЦЕССЕ

А. Н. Крюков
Рязанский государственный радиотехнический университет им. В. Ф. Уткина

Искусственный интеллект может составлять планы и конспекты, формулировать вопросы для тестов и развернутого ответа, описывать принципы действия радиотехнических устройств и временные диаграммы.

учебный процесс, ChatGPT, PhD Mentor, вопросы тестов

Универсальный бот ChatGPT хорошо знает школьную программу, может сформулировать тему занятия, структурировать материал, сделать к нему пояснения, написать вопросы. У него есть доступ к контенту, он способен конспектировать учебники и научные статьи, грамотно вести диалог, анализировать ответы, выявлять и анализировать ошибки, развивать критическое мышление [1]. Бесплатная версия приводит ссылки на платный, иностранный или недоступный контент при наличии открытого отечественного [2].

Согласно результатам опросов, педагоги используют его чаще, чем учащиеся, для адаптации учебных программ, генерации видеозаписей лекций, индивидуализации обучения, моделирования сложных радиотехнических процессов.

МГУ разрешил студентам использовать ИИ для написания ВКР при условии проверки на ошибки и галлюцинации нейронной сети [3].

С целью оценки целесообразности использования искусственного интеллекта в учебном процессе кафедры радиотехнических устройств автором были произведены тестирования возможностей бесплатной версии ChatGPT.

Задав PhD Mentor ChatGPT [4] на русском языке задание - написать статью на тему «Использование искусственного интеллекта в учебном процессе» - автор получил план и список источников, в которых рассмотрены направления решения и отсутствуют конкретные результаты. Предложение описать примеры использования ИИ в подготовке радиоинженеров и привести ссылки на источники вызвало описание симуляторов и программно-аппаратных комплексов, не содержащих элементов ИИ, но предоставляющих интерфейсы для их интеграции. Зарубежные источники из списка сгенерированной статьи google.com [5] не найдены, и на сайтах журналов, в которых якобы напеча-

таны, не содержатся. С платной подпиской ChatGPT Plus ИИ может искать актуальную информацию в интернете, а не только в своей базе данных.

Затем PhD Mentor ChatGPT [4] был задан вопрос: может ли он составить в Micro-Cap v8 [6] модель синхронного транзисторного выпрямителя, на который получен положительный ответ. Полученный после уточнений, изменений и дополнений файл *.cir модели не работал, не содержал марок использованных транзисторов, координат соединительных линий, параметров трансформатора и многого другого, имел объем 1,2 кбит против 22 кбит рабочей модели, составленной автором. При этом текстовые описания принципиальной схемы синхронного транзисторного выпрямителя, принципа ее действия и временных диаграмм работы были корректны.

Составление тестов в Moodle [7] к текстам лекций требует формулировки неправильных ответов, которые бы для не подготовленного студента выглядели, как правильные, и занимает много времени преподавателя. Загрузив в PhD Mentor ChatGPT [3] текст лекции в формате *.txt, автор в течение часа диалога с несколькими перезагрузками получил 20 вопросов с правильными и не правильными ответами в формате «множественный выбор», при котором из 7 ответов (A-G) нужно отметить несколько правильных вариантов. Формулировки (а в ряде случаев и правильность) ответов требуют исправлений, опыт можно считать удачным.

Защита отчетов по лабораторным работам предполагает как развернутые ответы преподавателю по существу в классе, так и ответы на тесты. В PhD Mentor ChatGPT была загружена методическая разработка для выполнения лабораторной работы «Исследование передатчика энергии» в формате *.txt (в форматах *.docx, *.pdf тоже можно, но изображения бесплатная версия не анализирует), после чего ему было предложено составить как вопросы тестов, так и задать вопросы по существу. Полученные вопросы и ответы на них после исправления можно использовать для защиты отчетов.

Если необходимо анализировать графики или медицинские снимки, задавать вопросы по фото задачи из учебника, потребуется доступ к Dall-E 3 [8], также включающийся при платной подписке.

Список испольуемых источников

1. Погодин Н. Искусственный интеллект в образовании: перспективы и примеры использования. URL: https://media.foxford.ru/articles/neyroseti-v-obrazovanii (дата обращения 04.11.2024).

2. Как пользоваться ChatGPT в России? URL: https://journal.tinkoff.ru/chatgpt-in-russia/ (дата обращения 04.11.2024).

3. Реморенко И. М., Сулейманов Р. С. Искусственный интеллект в образовании: перспективы и вызовы для ректоров и преподавателей URL: https://rectorspeaking.ru/iskusstvennyj-intellekt-v-obrazovanii (дата обращения 03.11.2024).
4. PhD Mentor on the GPT Store. Virtual mentor for PhD research, wtiting and data analysis. URL: https://chatgpt.com/g/g-XXErl79U4-phd-mentor (дата обращения 04.11.2024).
5. Google – крупнейшая в мире поисковая система URL: https://www.google.com/ (дата обращения 04.11.2024).
6. Micro-Cap v8 – SPICE-совместимый симулятор аналоговых и цифровых схем. URL: https://en.wikipedia.org/wiki/Micro-Cap, https://kazus.ru/programs/download/16513/?ysclid=m336i2wvz2427443434 (дата обращения 04.11.2024).
7. Welcome to the Moodle community. URL: https://moodle.org/ (дата обращения 04.11.2024).
8. DALL·E 3 understands significantly more nuance and detail than our previous systems, allowing you to easily translate your ideas into exceptionally accurate images. URL: https://openai.com/index/dall-e-3/ (дата обращения 04.11.2024).

Kryukov A. **USING ARTIFICIAL INTELLIGENCE IN THE EDUCATIONAL PROCESS.**

Ryazan State Radio Engineering University named after V. F. Utkin

Artificial intelligence can make plans and summaries, formulate questions for tests and a detailed answer, describe the principles of operation of radio engineering devices and time diagrams.

Key words: learning Process, ChatGPT, PhD Mentor, Test questions.

УДК 004.896
ГРНТИ 49.01.75

АНАЛИЗ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЦИФРОВЫХ ДВОЙНИКАХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

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

Статья посвящена анализу применения искусственного интеллекта в цифровых двойниках телекоммуникационных сетей. С этой целью был произведен обзор научных работ для выявления сфер применения, проблем и методов их решения, а также текущих тенденций в данном направлении. На основании обзора сделан вывод о целесообразности использования существующих и разрабатываемых решений.

цифровые двойники, GAI, управление сетями связи, 6G

В связи с развитием телекоммуникаций и появлением новых, более требовательных услуг, сети становятся сложнее и функциональнее. Это требует наличия инструмента, который бы позволял оценивать производительность сети, оптимизировать ее работу в реальном времени и управлять ею.

Одним из таких перспективных инструментов являются цифровые двойники сети.

Цифровые двойники сети (ЦД) – это виртуальные копии реальных сетей мобильной связи, которые в реальном времени отражают их состояние и помогают эффективно управлять ими.

ЦД используют модели данных для точной эмуляции работы сети и предлагают адаптивные стратегии управления. В отличие от симуляторов, ЦД взаимодействуют с реальной сетью, обеспечивая динамическое отображение ее состояния [1].

Цифровые двойники состоят из трех основных модулей [2]:

1. Модуль эмуляции статуса. Отражает текущее состояние физической сети, используя данные, собранные из нее.

2. Модуль абстракции характеристик данных. Извлекает полезную информацию из данных о состоянии сети (например, распределение трафика) и помогает отслеживать изменения в сети.

3. Модуль принятия сетевых решений. Генерирует решения по управлению сетью, которые передаются контроллеру для реализации.

Из-за сложности современных беспроводных сетей трудно создать единого цифрового двойника для всей беспроводной сети. Распространенным решением этого является сегментация беспроводной сети и создание ЦД для конкретных сетевых компонентов, чтобы соответствовать индивидуальным целям. Методологии моделирования для этих цифровых близнецов настраи-

ваются в зависимости от архитектуры и функциональности соответствующих сетевых элементов.

С приходом 6G цифровые двойники сетей сталкиваются с новыми вызовами: сложность, масштабируемость и неоднородность сетей значительно возрастают.

Три ключевые области, требующие усовершенствований [3]:

1. Физическо-цифровое моделирование. Традиционные методы моделирования становятся слишком сложными и затратными для 6G. ИИ-модели предлагают более гибкий и автоматизированный подход.

2. Физико-цифровая синхронизация. Масштаб и сложность 6G сетей требуют новых стратегий передачи данных для поддержания синхронизации между физической и цифровой сетью. ИИ может помочь решить эту проблему.

3. Возможность нарезки. 6G сети будут иметь большее разнообразие сетевых структур и сценариев использования. ИИ-методы, такие как глубокое обучение, могут помочь в настройке и управлении этими структурами в цифровых двойниках.

Новая ветвь искусственного интеллекта (ИИ), генеративный ИИ (GAI), фокусируется на создании новых экземпляров данных, анализе корреляции данных и решении проблем оптимизации, что может помочь улучшить эмуляцию состояния сети, абстракцию характеристик данных и принятие сетевых решений в ЦД, тем самым удовлетворяя растущие требования цифровых двойников беспроводных сетей 6G.

В таблице 1 [2] представлены четыре модели GAI, которые могут быть использованы в цифровых двойниках сетей мобильной связи.

ТАБЛИЦА 1. Модели GAI, применяемые в сетях мобильной связи

Модель	Функции	Характеристики	Метрики
GAN	– создание изображений; – расширение набора данных	– генератор; – дискриминатор	– пиковое отношение сигнал/шум; – структурное сходство
GT	– понимание и создание текст;а – извлечение признаков	– позиционное кодирование	– оценка общего понимания языка
VAE	– обучение признакам; – шумоподавление	– вероятностная графическая модель; – вариационный вывод	– среднеквадратическая ошибка; – расхождение Кульбака–Лейблера
GDM	– генерация условий; – принятие решений	– обратная диффузия; – Марковский переход	– временная когерентность; – качество интерполяции

Генеративная состязательная сеть (GAN): генерирует синтетические данные, похожие на реальные, что решает проблему нехватки данных для обучения ЦД.

Генеративный трансформатор (GT): помогает ЦД понимать намерения пользователей и анализировать данные, обеспечивая более точное управление сетью.

Вариационный автоэнкодер (VAE): выделяет важные признаки из данных сети и восстанавливает их, что полезно для моделирования сложных сетевых процессов.

Генеративная модель диффузии (GDM): моделирует процесс управления сетью, позволяя повысить эффективность обучения и принятия решений ЦД.

Варианты применения генеративных технологий ИИ [3, 4]:

1. Генеративное дополнение данных для цифрового двойника. Метод моделирования на основе данных для цифровых двойников сетей связи требует большое количество ресурсов для работы. Распространенным решением является аугментация данных – метод, который повышает как качество, так и количество данных за счет создания новых образцов из существующих с помощью модели GAN. Применение генеративного дополнения данных предлагает реальное решение путем создания разнообразных синтетических сетевых данных, таких как поведение пользователей и модели трафика на основе собранных реальных данных. Генеративное дополнение данных увеличивает не только объем, но и разнообразие данных беспроводных сетей, тем самым облегчая обучение моделей цифровых двойников беспроводных сетей и позволяя оценивать потенциальные риски в сетях 6G.

2. Генеративная передача для цифрового двойника. Цифровые двойники беспроводных сетей могут использовать диффузионную модель для улучшения процесса передачи данных. Модель диффузии включает в себя две основные фазы: процесс прямой диффузии, который постепенно вводит шум в данные до тех пор, пока они не достигнут заданного уровня шума, и процесс обратного шумоподавления, который постепенно устраняет шум до тех пор, пока данные не вернутся в исходное положение. Это позволяет диффузионной модели эффективно обучаться на основе сильно зашумленных данных и генерировать образцы высокой точности.

После тщательного обучения энкодер служит генеративным передатчиком для синхронизации цифровых двойников беспроводной сети 6G.

3. Генеративный ИИ как цифровые двойники. Помимо помощи в создании цифровых двойников сама модель генеративного искусственного интеллекта может служить цифровым двойником. Эти генеративные модели вос-

производят поведение физических сетей, предлагая более эффективную альтернативу трудоемким решениям, управляемым моделями.

4. Генеративное обучение на основе моделей для цифрового двойника. Чтобы справиться с различными сценариями и гетерогенными сетевыми структурами в 6G возможность срезки также должна быть задействована в цифровых двойниках. Можно создать настраиваемые цифровые двойники для различных срезов с помощью обучения на основе генеративных моделей. Используя знания из хорошо обученной исходной задачи, передача обучения помогает цифровому двойнику беспроводной сети 6G избежать обучения генеративных моделей ИИ с нуля и ускорить адаптацию к новым, но похожим сценариям.

5. Генеративное управление сетью моделями ИИ. Существенное улучшение производительности сети и операционной эффективности после интеграции сетевого цифрового двойника с генеративным искусственным интеллектом (таблица 2).

ТАБЛИЦА 2. Сравнение показателей производительности сети

Показатель	До интеграции	После интеграции
Задержка (мс)	100	70
Использование полосы пропускания (%)	75	90
Частота ошибок (%)	5	1,5
Точность прогнозирования (%)	80	95

Помимо преимуществ использование искусственного интеллекта в цифровых двойниках сетей связи сопряжено с техническими трудностями:

– массивное кэширование и вычислительные затраты: поскольку модели GAI обычно имеют большие размеры и сложную структуру нейронной сети, сложно напрямую развернуть модели GAI на узлах на границе сети с ограниченными возможностями кэширования и вычислений. Решением данной проблемы могут стать облегченные GAI модели;

– масштабируемость и эффективность моделей: для моделей GAI разного размера большие модели GAI обычно обеспечивают более высокую производительность обработки данных, но при этом потребляют больше сетевых ресурсов. Использование адаптивного механизма выбора моделей GAI поможет справиться с этой проблемой;

– надежная обработка данных для обеспечения устойчивости сети: поскольку сложность моделей GAI может привести к непредсказуемой и необъективной эмуляции состояния, абстрагированию характеристик и принятию

сетевых решений в ЦД, возникает проблема разработки надежного механизма обработки данных для повышения устойчивости сети;

– конфиденциальность и безопасность данных: поскольку генеративный искусственный интеллект предполагает обширные манипуляции и генерацию данных, обеспечение конфиденциальности и безопасности данных в цифровых двойниках имеет первостепенное значение. Разработка надежных механизмов защиты данных, одновременно обеспечивающих сложные функциональные возможности генеративного ИИ, остается серьезной проблемой;

– возможности обработки данных в реальном времени: задержка в обработке данных и принятии решений является решающим фактором для сетевых операций. Расширение возможностей обработки интегрированных цифровых двойников в реальном времени с помощью генеративного искусственного интеллекта, особенно в условиях больших объемов данных и быстрой динамики сети, является сложной задачей [2].

Таким образом, в данной работе был проведен анализ применения искусственного интеллекта в цифровых двойниках телекоммуникационных сетей. На основании обзора можно сделать вывод о том, что использование цифрового двойника в сетях следующего поколения с моделями генеративного ИИ является целесообразным, однако для полноценного функционирования существующие решения либо не подходят, либо требуют существенной доработки.

Список используемых источников

1. Lin X., Kundu L., Dick C., Obiodu E., Mostak T. 6G Digital Twin Networks: From Theory to Practice. URL: https://arxiv.org/pdf/2212.02032 (дата обращения 15.11.2024).
2. Huang X., Yang H., Zhou C., Shen X., Zhuang W. When Digital Twin Meets Generative AI: Intelligent Closed-Loop Network Management. URL: https://arxiv.org/pdf/2404.03025 (дата обращения 15.11.2024).
3. Tao Z., Xu W., Huang Y., Wang X., You X. Wireless Network Digital Twin for 6G: Generative AI as A Key Enabler. URL: https://arxiv.org/html/2311.17451v2#S2 (дата обращения 15.11.2024).
4. Muhammad K., David T., Nassisid G., Farus T. Integrating Generative AI with Network Digital Twins for Enhanced Network Operations. URL: https://arxiv.org/html/2406.17112v1#bib (дата обращения 15.11.2024).

Mamaev E. **ANALYZING THE USE OF ARTIFICIAL INTELLIGENCE IN DIGITAL TWINS OF TELECOMMUNICATION NETWORKS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article is devoted to analysing the application of artificial intelligence in digital twins of telecommunication networks. For this purpose, a review of scientific works was carried out to identify areas of application, problems and methods of their solution, as well as current trends in this direction. Based on the review, the conclusion is made about the feasibility of using existing and developing solutions.

Key words: GAI, digital twins, communication network management, 6G.

УДК 004.891.3
ГРНТИ 28.23.15

ОБУЧЕНИЕ МОДЕЛЕЙ YOLO ДЛЯ ДЕТЕКЦИИ ТРЕЩИН В СТЕКЛАХ ОБЕСТОЧЕНЫХ LCD ПАНЕЛЕЙ

Д. В. Петров, Ф. В. Филиппов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследуется дообучение моделей однопроходных детекторов семейства YOLOv8 для решения задачи обнаружения и сегментации трещин дисплеев на фотографиях обесточенных LCD-панелей, полученных с помощью камеры, чувствительной к ближнему ИК-спектру. Анализируется влияние различных гиперпараметров на метрики полученных моделей. Описывается сбор, разметка и аугментация датасета изображений, произведенные в условиях производственного предприятия.

компьютерное зрение, искусственный интеллект, анализ изображений, детекция объектов, семантическая сегментация, YOLOv8, OpenCV, Embedded платформы, ИК-камеры, промышленность

Производство потребительской электроники в РФ, а именно телевизоров и мониторов с жидкокристаллическими (LCD – Liquid Crystal Display) на момент написания данной работы (Ноябрь 2024 года) представляет собой по большей части крупноузловую финальную сборку из ключевых компонентов, произведенных за рубежом (в основном в Китае) [1]. При этом LCD-панели достаточного размера в России не производится, а в процессе поставки из-за рубежа существенно повышается риск повреждений. Трещины в стеклах LCD-панелей, как правило, не обнаружимы до момента включения, ввиду конструкционных особенностей (натяжение поляризационной пленки, многослойная структура), что делает невозможным получение компенсаций от поставщика в ходе рекламации брака.

Согласно собранной производственной статистике, только 3 % таких дефектов были распознаны людьми, при том, что перед производством досконально осматривается каждая панель.

В предыдущей статье была выдвинута и экспериментально подтверждена гипотеза о том, что данный дефект виден на изображениях, полученных посредством ИК-чувствительной камеры с прямой ИК подсветкой [2]. Ближний ИК-диапазон (от 700 нм до 1400 нм) при этом оказался особенно полезен для просвечивания тонких материалов. Физика процесса заключается в том, что длинные волны инфракрасного света могут проникать в материалы на боль-

шую глубину, чем волны видимого света. Это свойство используется для выявления внутренних структур и дефектов в материалах. ИК-камеры способны фиксировать различия в пропускании и отражении инфракрасного света, что позволяет обнаруживать трещины и другие аномалии.

Основная цель проведенного исследования состоит в разработке модели, подходящей для автоматизированной детекции трещин на фотографиях обесточенных LCD-панелей, полученных с помощью камеры, чувствительной к ближнему ИК-спектру. При этом первостепенно важно в принципе обнаружить трещину и не допустить попадания бракованной панели на производственную линию, точность определения положения и полнота выявления дефектной области играют второстепенные роли.

Сбор, разметка и аугментация изображений

Для сбора изображений был собран стенд из платформы Raspberry Pi 5 8GB и MIPI CSI камеры Waveshare OmniVision OV5647 с Fisheye объективом, поддержкой ночного зрения и подсветкой из двух ИК (850нм). Стенд был собран на стальной пластине с термопадами (для отвода тепла от камеры и подсветки) и креплением под фотоаппаратный штатив. Собранный стенд продемонстрирован на рисунке 1.

Рис. 1. Стенд

Всего было собрано и размечено 1200 изображений, из них 417 с трещинами. Разметка проводилась в среде CVAT, выделением областей (точки, ограничивающие области), так как из таких аннотаций можно получить 2 датасета для обучения моделей для задачи сегментации и детекции после несложных преобразований. На изображениях размечались области:

– LCM_Display – дисплей, на котором возникают искомые трещины. Он хорошо заметен и будет обнаружен с высокой вероятностью, что в дальнейшем можно использовать для ограничения области поиска трещин

– LCM_Crack – трещина на дисплее LCM панели.

Датасеты собирались с равномерным распределением изображений с трещинами по train и val выборкам.

Ко всем изображениям в собранном датасете и их аннотациям были применены аугментации: *HorizontalFlip(p=0.5), VerticalFlip(p=0.5), RandomRotate90(p=0.5), RandomBrightnessContrast(p=0.5), GaussNoise(p=0.5), Blur(p=0.5), CLAHE(p=0.5)*. Это позволило расширить датасет с 1200 до ~7400 изображений. Результаты проверки продемонстрированы на рисунке 2.

Всего из полученных изображений были собраны 4 датасета:

1. Для задачи сегментации из оригинальных данных;
2. Для задачи сегментации из расширенных данных:
3. Для задачи детекции из оригинальных данных;
4. Для задачи детекции из расширенных данных.

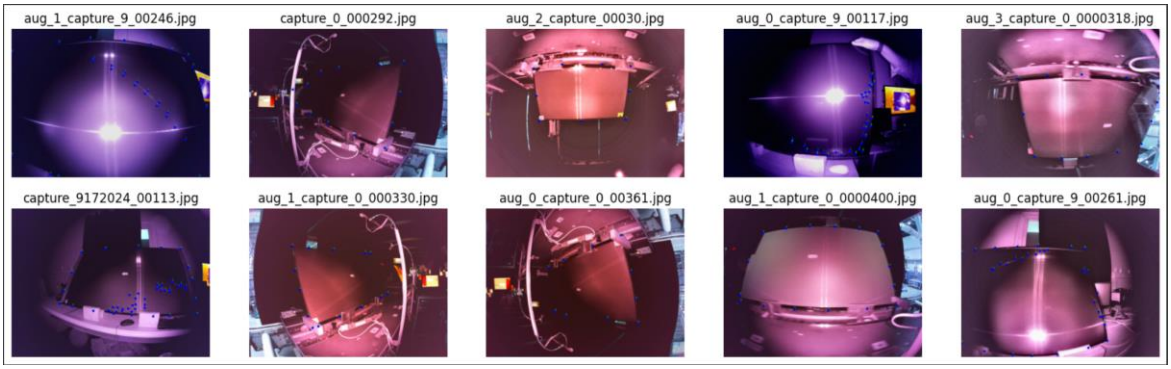


Рис. 2. Проверка аугментаций

Проверка аннотаций к каждому датасету производилась посредством выведения 5 рандомных изображений из train и val выборок с отрисовкой на них ограничивающих точек, соответственно измененным файлам аннотаций, пример изображен на рисунке 3.

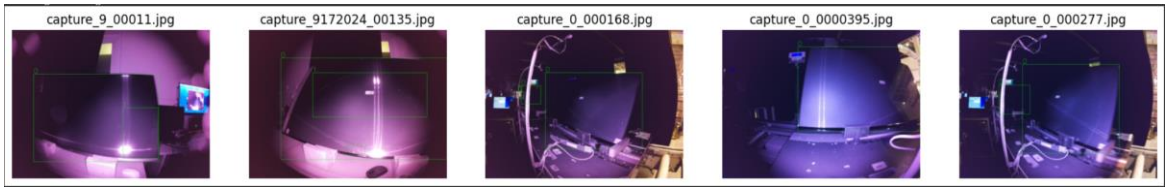


Рис. 3. Проверка аннотаций, преобразованных для задачи детекции

Выбор и обучение моделей

В ходе проведенного эксперимента предобученная на COCO модель YOLOv8s показала наилучшие результаты – позволяла в инференсе на Raspberry Pi 5 обрабатывать и визуализировать в среднем примерно 20 кадров в секунду, т.е. результат распознавания был виден почти в реальном времени.

Для исследования были выбраны модели YOLOv8s-seg и YOLOv8s-det для задач сегментации и детекции соответственно. Размер ‘S’ был выбран так как такие модели хорошо конвертируются в формат NCNN и прекрасно рабо-

тают на Raspberry Pi 5, показывая при этом сравнимый с большими моделями mAP.

На каждом из четырех полученных датасетов были дообучены по 2 модели YOLOv8s с разными размерами бэтчей и кол-вом эпох. Оптимизатор, lr и momentum к нему ULTRALYTICS при обучении подбирает автоматически, поэтому влияние этих параметров не исследовалось. Визуализация обучения двух лучших моделей представлена на рисунке 4.

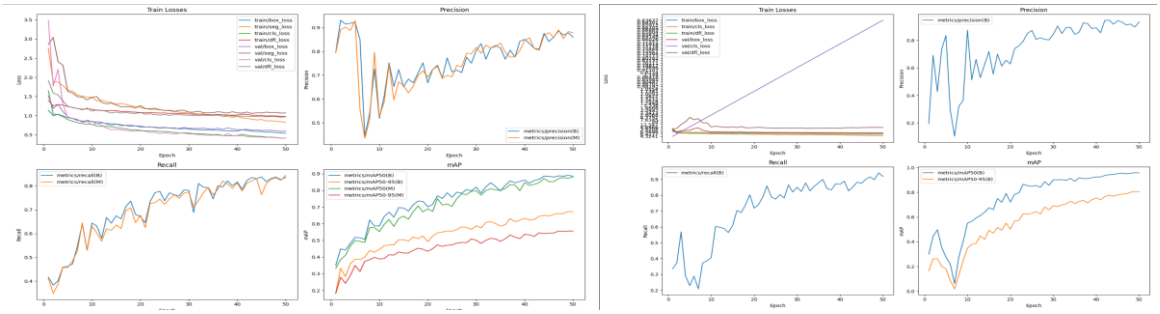


Рис. 4. Обучение двух лучших из полученных моделей

Оценка результатов

В рамках оценки результатов обучения моделей, были проведены 2 проверки: на известных и неизвестных моделям данных. При проверке на известных размеченных данных производился подсчет на скольких из 417 размеченных изображений каждая модель засечет трещину. Для оценки модели была введена метрика Detection rate, являющаяся частным случаем F1 меры для этой задачи. Результаты проверки представлены в таблице 1.

ТАБЛИЦА 1. Сравнение полученных моделей на известных данных

Model	Train image qty	Epochs	Batch size	Detected	Detection rate
Detection (original)	958	50	16	412	98.8 %
	958	50	64	414	99.3 %
Detection (augmented)	4958	50	16	411	98.6 %
	4958	50	64	411	98.6 %
Segmentation (original)	958	50	16	403	96.6 %
	958	20	64	388	93.0 %
Segmentation (augmented)	5754	20	16	389	93.3 %
	5754	20	64	396	95.0 %

В рамках проверки на неизвестных данных, результаты работы моделей были оценены визуально на 15 неразмеченных изображениях. На некоторых из них представлены уникальные LCM, с существенно отличающимися от прочих диагональю и коэффициентами отражения/преломления наклеенной на стекло пленки. Результаты оценки представлены в таблице 2.

ТАБЛИЦА 2. Сравнение полученных моделей на известных данных

Model	Train image qty	Epochs	Batch size	Detected	Detection rate
Detection (original)	958	50	16	14	93 %
	958	50	64	14	93 %
Detection (augmented)	4958	50	16	14	93 %
	4958	50	64	14	93 %
Segmentation (original)	958	50	16	13	86.7 %
	958	20	64	12	80.0 %
Segmentation (augmented)	5754	20	16	11	73.3 %
	5754	20	64	11	73.3 %

Заключение

Все полученные модели YOLO показали себя неплохо. При проверке на имеющихся размеченных и не размеченных наборах данных, с помощью лучшей из полученных моделей удалось обнаружить от 93 % до 99 % трещин. Лучший результат показала модель детекции, обученная на оригинальных данных при использовании более крупных бэтчей. Худший результат при этом у аугментированных моделей - от 73 % до 95 %. Визуальная проверка, представленная на рисунке 5, показала, что даже если моделям не хватало Confidence для определения трещины, они не считали поврежденный участок частью дисплея.

Рис. 5. Результаты сегментации

Несмотря на то, что эти результаты значительно выше, чем 3 %, которые, могут быть обнаружены людьми, он может и должен быть улучшен. Таким образом дальнейшая работа с моделями семейства YOLOv8 и их оценка в рам-

ках поставленной задачи целесообразна. Для этого требуются существенно больше размеченных изображений с трещинами.

Список используемых источников

1. Электроника: производство и торговля // XVIII конференция ассоциации ратэк москва, 26 октября 2023 года. Материалы конференции. URL: http://ratek.org/wp-content/uploads/2023/10/RATEK-obshhaya.pdf (дата обращения 18.05.2024).
2. Петров Д. В., Филиппов Ф. В. Разработка системы анализа изображений и распознавания объектов для контроля качества в производстве // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб, СПбГУТ, 2024.

***Petrov D., Philippov F.* YOLO MODELS TRAINING FOR CRACK DETECTION IN POWERED OFF LCD SCREENS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This paper Investigates the pre-training of single-pass detector models of the YOLOv8 family to solve the problems of display crack detection and segmentation in photos of depowered LCD panels captured with a near-infrared-sensitive camera. The influence of various hyperparameters on the metrics of the resulting models is analyzed. The acquisition, partitioning and augmentation of the image dataset, performed in a production facility environment, is described.

Key words: Computer vision, artificial intelligence, image analysis, object detection, semantic segmentation, YOLOv8, OpenCV, Embedded platforms, IR cameras, industry.

УДК 004.891.3
ГРНТИ 20.53.19

РАЗРАБОТКА МЕТОДА ДЕТЕКТИРОВАНИЯ НЕИСПРАВНОСТЕЙ АСИНХРОННЫХ ЭЛЕКТРОДВИГАТЕЛЕЙ С ПОМОЩЬЮ МАШИННОГО ОБУЧЕНИЯ

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

В докладе рассматривается возможность разработки программного обеспечения для диагностики неисправностей асинхронных электродвигателей. Система использует дискретное преобразование Фурье для анализа измеренных токов, после чего метрики обрабатываются с помощью искусственного интеллекта. Программа выдает предположения о возможных неисправностях, что способствует своевременному ремонту и предотвращению простоев. Обсуждаются преимущества повышения надежности оборудования и снижения затрат на обслуживание, а также сложности, связанные с отсутствием датасетов в данной предметной области.

асинхронные электродвигатели, преобразование Фурье, машинное обучение

В современном мире электротехническое оборудование играет ключевую роль в производственных процессах. Особенно важными и широко используемыми являются асинхронные трехфазные электродвигатели, которые приводят в движение различные механизмы и оборудование. Однако, как и любое техническое устройство, электродвигатели подвержены износу и выходу из строя, что может привести к непредвиденным простоям и проблемам в производственном процессе.

Возможные неисправности асинхронных электродвигателей могут существенно влиять на характеристики потребляемых токов. Например, межвитковое замыкание приводит к увеличению тока в одной из фаз по сравнению с двумя другими. Это происходит из-за смещения обмоток, механической вибрации и ударов, что вызывает изменение сопротивления и, как следствие, изменение тока.

Аналогично, обрыв обмотки или замыкание обмотки на корпус также приводят к изменению токов. В случае обрыва обмотки ток по другим фазам будет повышен, что может привести к перегреву и повреждению двигателя. Замыкание обмотки на корпус может вызвать короткое замыкание и пожар, если не обеспечена должная электрическая защита [1].

Механические неисправности, такие как износ подшипников или повреждение крыльчатки обдува, также влияют на токи. Износ подшипников увеличивает механическую вибрацию и шум, что может привести к перегреву и падению производительности двигателя. Повреждение крыльчатки обдува может вызвать перегрев двигателя из-за недостаточного охлаждения.

Подобные неисправности асинхронных электродвигателей могут диагностироваться с применением метода гармонического анализа, который позволяет выявить изменения в потребляемых токах [2].

Для диагностики необходимо измерить токи и напряжения по всем фазам с помощью вольтметров и трансформаторов тока. Показания с датчиков (вольтметров и трансформаторов тока) снимаются регистрирующим устройством, которое преобразует аналоговые сигналы в дискретные данные через АЦП. Высокая частота дискретизации обусловлена промышленной частотой электрического тока, что позволяет точно фиксировать изменения в сигналах и выявлять признаки неисправностей с помощью дискретного преобразования Фурье [3].

Дискретное преобразование Фурье раскладывает измеренные сигналы на гармонические составляющие, что позволяет выявить изменения в частотном спектре, характерные для различных типов неисправностей.

Полученные данные вместе с другой необходимой информацией, такой как технические характеристики с шильдика асинхронного двигателя, можно обработать с помощью машинного обучения. Машинное обучение позволяет создать интеллектуальную систему, которая будет анализировать данные и выдавать предположения о возможных неисправностях.

Машинное обучение использует алгоритмы для построения моделей, которые предсказывают возможные неисправности на основе данных. Эти модели могут быть обучены на больших объемах данных, что позволяет им выявлять скрытые закономерности и аномалии [4].

Преимущества машинного обучения:

1. Быстрое и автоматическое выявление аномалий. Машинное обучение позволяет быстро и автоматически выявлять аномалии в данных, что ускоряет процесс диагностики.

2. Высокая точность. Алгоритмы машинного обучения могут достигать высокой точности в предсказании неисправностей, особенно при наличии достаточного объема данных для обучения.

3. Универсальность. Машинное обучение применимо к широкому спектру электрических систем, что делает его универсальным инструментом для диагностики асинхронных электродвигателей.

Интеллектуальная система, созданная на основе машинного обучения, будет анализировать полученные данные и выдавать предположения о возможных неисправностях, что значительно повысит эффективность диагностики и обслуживания асинхронных двигателей.

Для реализации данной системы необходимо преодолеть одну сложность – отсутствие необходимых датасетов. Предлагается дополнительно разработать программное обеспечение (ПО), способное эмулировать различные неисправности. Это ПО будет использоваться на этапе, когда данные уже внесены в таблицу после преобразования Фурье вместе с информацией с шильдиков.

Дополнительно можно развернуть сервис с веб-интерфейсом, где пользователи смогут вносить информацию с шильдиков через формы и загружать таблицы с замерами токов и напряжений. Сервис будет выдавать предположения о возможных неисправностях и запрашивать обратную связь от пользователей о правильности предположений.

Такая информация будет использоваться для дальнейшего постепенного дообучения системы. Со временем система сможет стать довольно точной и эффективной в диагностике асинхронных двигателей.

Преимущества такого подхода:

1. Эмуляция неисправностей. ПО для эмуляции неисправностей позволит создать необходимые данные для обучения системы, даже если реальные данные отсутствуют.

2. Веб-сервис. Веб-сервис с формами для ввода данных и обратной связью позволит собирать данные от пользователей, что способствует постепенному дообучению системы и повышению ее точности.

3. Постоянное улучшение. Система будет постоянно улучшаться благодаря обратной связи от пользователей и возможности дообучения на новых данных, что делает ее более точной и надежной с течением времени.

Таким образом, сочетание эмуляции неисправностей, веб-сервиса и постепенного дообучения позволит создать эффективную и точную систему диагностики асинхронных двигателей.

Заключение

Реализация предложенной системы с использованием эмуляции неисправностей, веб-сервиса и постоянного дообучения позволит создать высокоточную и надежную систему диагностики асинхронных двигателей. Это значительно повысит эффективность обслуживания и ремонта электрических систем, что в конечном итоге приведет к снижению затрат и повышению надежности оборудования.

Список используемых источников

1. Основные неисправности электродвигателя. URL: https://mirprivoda.ru/articles/osnovnye-neispravnosti-elektrodvigatelya/ (дата обращения 20.10.2024).
2. Беляев П. В., Головский А. П. Диагностика неисправностей асинхронных двигателей на ранних стадиях повреждения // Динамика систем, механизмов и машин, 2020. Том 8, №3. С. 16–23.
3. Самородов А. В., Баширов М. Г., Чурагулов Д. Г., Абдуллин А. А. Разработка программно-аппаратного комплекса для оценки технического состояния машинных агрегатов с электрическим приводом // Нефтегазовое дело, 2012. № 6. С. 10–20.
4. Сальников С. В., Солодкий Е. М., Вишняков Д. Д., Юдин Р. Ю., Петроченков А. Б. Диагностика асинхронного двигателя на основе машинного обучения. Сборник материалов XXVI Международной конференции по мягким вычислениям и измерениям (SCM-2023). Санкт-Петербург. 24 – 26 мая 2023 г. СПб.: СПбГЭТУ «ЛЭТИ». ISBN 978-5-7629-3198-4. С. 295–300.

Firsov V. **DEVELOPMENT OF A METHOD FOR DETECTING FAULTS OF ASYNCHRONOUS ELECTRIC MOTORS USING MACHINE LEARNING.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The report examines the possibility of developing software for diagnosing faults in asynchronous electric motors. The system uses discrete Fourier transform to analyze measured currents, after which the metrics are processed using artificial intelligence. The program provides suggestions about possible faults, which contributes to timely repairs and prevention of downtime. The advantages of increasing equipment reliability and reducing maintenance costs, as well as the challenges associated with the lack of datasets in this subject area, are discussed.

Keywords: Asynchronous electric motors, Fourier transform, machine learning

УДК 004.624
ГРНТИ 49.37.29

МОДЕЛЬ ПРОЦЕССА ДОВЕДЕНИЯ ИНФОРМАЦИИ ДО ПОДВИЖНЫХ НОСИТЕЛЕЙ

С. В. Чернобровкин
Военная академия связи им. Маршала Советского Союза С. М. Буденного

С развитием технологий возрастают объемы информации, передаваемые в интересах принятия решения должностными лицами. В связи с этим имеет смысл обеспечить доведение информации путем фрагментации исходного объема передаваемых данных с целью повышения вероятности своевременного ее доведения до должностных лиц. Для решения задачи предлагается модель процесса доведения информации.

передача данных, фрагментация данных, вероятность своевременного доведения

Из анализа конфликтов последних лет видно, что широкое применение таких средств разведки, как беспилотные летательные аппараты (БПЛА) и средств поражения, как высокоточное оружие (ВТО), позволяет достигать необходимых результатов при минимальных потерях среди личного состава и военной техники.

Все более важное значение приобретают военно-политические и технологические аспекты развития силовых структур Российской Федерации, нацеленные на переход на качественно новый, инновационный уровень управления войсками и оружием [1].

При доведении больших объемов информации в течении длительного времени верность воздействий различного рода на систему доведения информации возрастает. При таких воздействиях на систему доведения происходит сбой в обмене информации, что в свою очередь приводит к необходимости повторной загрузки информации. Тем самым время доведения информации возрастает, что в свою очередь отрицательным образом сказывается на выполнении поставленных задач.

Целью настоящей работы является разработка варианта модели процесса доведения информации, который основан на методах фрагментации информации, и, как следует, с большей вероятностью своевременной доставки за счет уменьшения времени на передачу одного фрагмента по сравнению с блоком исходных данных.

Постановка задачи:

$A=\{a_i\}$ – множество серверов хранения;

$N=\{n_g\}$ – множество требуемых ресурсов;

$B=\{b_o\}$ – множество объемов ресурсов;

$L=\{l_j\}$ – множество получателей;

$t_{треб} \leq 70$ мин;

$C=\{c_h\}$ – множество пропускных способностей каналов связи;

$R=\{r_{ab}\}$ – множество фрагментов информации;

$RTT=\{rtt_{ij}\}$ – множество круговых задержек при передаче между узлами a_i и l_j (бит/с);

$U=\{u_{a\}}$– множество алгоритмов доведения информации в тракте;

$DV=\{dv_e\}$ – множество воздействий на сеть передачи данных.

Допущения и ограничения:

1. Внутренний нарушитель отсутствует;
2. Рассматривается тракт доведения в закрытой сети передачи данных.

Требуется разработать:

M – модель процесса доведения информации

$$M = f(A, C, R, \mathrm{RTT}, \mathrm{DV}, S(x))$$

S(x) =f (L, B, N) – показатели системы доведения информации.

С целью разработки модели процесса доведения информации предлагается решать задачу с целевой функцией вероятности своевременной доставки блока данных. В качестве оптимизируемых параметров будет рассматриваться количество фрагментов блока данных, на которые данный исходный блок фрагментируется и распределение этих фрагментов по необходимому числу источников данных информации.

Этапы разработки модели [2–5]:

1. Оптимизация размера фрагмента;
2. Оптимизация распределения фрагментов, назначаемых для передачи источниками информации.

Исходными данными 1-го этапа является анализ вероятностно-временных характеристик при заданных:

L_1 – объем информационной части блока;

c – контрольная сумма.

Исходя из длины информационной части блока и контрольной суммы получим объем информационной части блока данных с учетом контрольной суммы

$$V_1 = L_1 + c$$

Таким образом, необходимо определить оптимальное количество фрагментов s, для которого обеспечивается максимум вероятности своевременной доставки блока.

Предлагается пересчитать вероятность своевременной доставки блока к вероятности своевременной доставки фрагмента, найти вероятность своевременной доставки (функцию распределения вероятности времени доставки) фрагмента и найти оптимальное количество фрагментов [3–5]

$$Q = (1 - p)^n \tag{1}$$

где Q – вероятность неправильного приема блока;

p – количество символов;

n – количество символов.

Из выражения вероятности правильного приема сообщения, состоящего из *p* символов, получим, что при фрагментации блока данных на *s* фрагментов, формула (1) будет иметь следующий вид [4, 5]

$$Q(s) = (1 - p)^{1s}. \tag{2}$$

Исходя из (1) и (2), получим

$$P_{v(s)} = 1 - (1 - p)^{V(s)V_1}. \tag{3}$$

$P_{v(s)}$ – вероятность неправильного приема фрагмента.

Исходя из исходных данных получим размер информационной части фрагмента по формуле

$$L(s) = \frac{L_1}{s} \tag{4}$$

Тогда, общая длина фрагмента составит

$$L_{sc} = L(s) + c. \tag{5}$$

Исходя из формулы (4) размер блока, состоящего из s фрагментов

$$V(s) = s(L(s) + c) = L_1 + \text{sc}. \tag{6}$$

Относительное чистое время передачи s фрагментов (т. е. всего блока)

$$t_s = \frac{V(s)}{V_1} s.$$

Допустимое время, отводимое на переспросы, вычисляется по формуле

$$t_k = t - \frac{V(s)}{V_1} s.$$

где t – время передачи блока данных без учета деструктивных воздействий.

Вероятность передачи фрагментов за s шагов рассчитывается с помощью вероятностно-временных графов [4–6] и представлена на рис. 1.

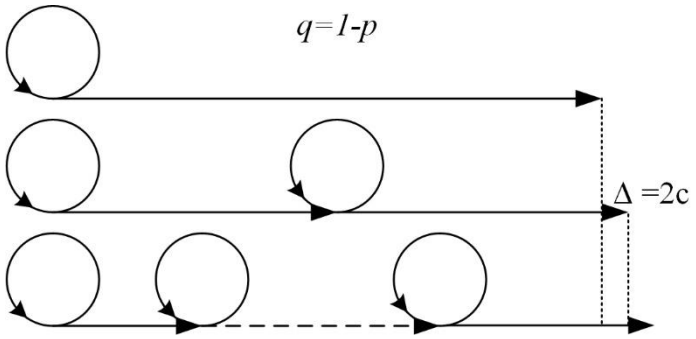


Рис. 1. Вероятностно-временной граф передачи блока данных

Здесь $q = (1-p)^{V(s)V_1}$ – вероятность успешной передачи фрагмента,

n – количество фрагментов блока информации.

Соответственно, p – это вероятность переспроса фрагмента.

Для передачи одного фрагмента (т. е. перехода на один шаг вправо за время k)

$$\Pr\{j = k\} = \mathrm{q}\mathrm{p}^k.$$

При этом, функция распределения вероятности имеет вид:

$$\Pr\{T_1 \le t = t_s + t_k\}$$

$$\Pr\{T_1 \le t\} = 0 \text{ при } t \le t_s$$

$$\Pr\{T \le t\} = \sum_{j=1}^{k} p(1-q)^k \text{ при } t \ge t_s, \text{ где } k = \mathrm{Int}(t - \frac{V(s)}{V} s).$$

При большом s

$$k = \mathrm{Int}(t - \frac{V(s)}{V} s).$$

Функция распределения вероятности времени передачи s фрагментов определяется сверткой полученных функций. В связи с большой вычислительной сложностью полученных сверток будем вычислять через математическое ожидание времени передачи пакета m и дисперсию σ^2, аппроксимируя суммарное распределение Гауссовским распределением.

В связи с дискретными значениями количества шагов s производящая функция вероятности времени передачи фрагмента имеет вид [4]:

$$\chi(z) = \mathrm{q}z(1 + \mathrm{p}z + p^2 z^{2+} \ldots) = \frac{\mathrm{q}z}{1 - \mathrm{p}z}$$

Из производящей функции получим математическое ожидание времени передачи фрагмента [5]:

$$m = x'(1) = q(p + 2p^2 + 3p^3 + \ldots) = \frac{q(1-\mathrm{p}z) + \mathrm{p}\mathrm{q}z}{(1-\mathrm{p}z)^2} = \frac{q}{(1-\mathrm{p}z)^2}|_{z=1} = \frac{1}{q}$$

$$\sigma^2 = m_2 - m_1^2$$

где m_2 – второй момент.

Принцип вычисления второго момента [4, 5]:

$$m_2 = (\chi'(z)z)'|_{z=1}$$

$$\chi'(z) = \frac{q}{(1-\mathrm{pz})^2}, z\chi'(z) = \frac{\mathrm{qz}}{(1-\mathrm{pz})^2}$$

$$[z\chi'(z)]' = q\frac{(1-\mathrm{pz})^2 + 2p(1-\mathrm{pz})z}{(1-\mathrm{pz})^4} = q\frac{(1-\mathrm{pz}) + 2\mathrm{pz}}{(1-\mathrm{pz})^3} = q\frac{1+\mathrm{pz}}{(1-\mathrm{pz})^3} m_2 = (\chi'(z)z)'|_{z=1}$$
$$= q\frac{1+p}{(1-p)^3} = \frac{1+P_{V(s)}}{(1-P_{V(s)})^2}$$

Исходя из (4), (5), (6) получим дисперсию через моменты времени передачи фрагмента

$$\sigma^2 = m_2 - m_1^2 = \frac{1+p}{q^2} - \frac{1}{q^2} = \frac{P_{V(s)}}{(1-P_{V(s)})^2}$$

Исходя из полученных выражений для вычисления математического ожидания и дисперсии передачи блока от количества фрагментов, получим

$$m(s) = V(s)\frac{L_{\mathrm{sc}}}{V_1}\frac{1}{(1-P_{V(s)})^{V(s)V_1}}$$

$$\sigma^2(s) = V^2(s)\left[\frac{L_{\mathrm{sc}}}{V_1}\right]^2 \frac{P_{V(s)}}{(1-P_{V(s)})^2}$$

$$\sigma(s) = V(s)\frac{L_{\mathrm{sc}}}{V_1}\sqrt{\frac{P_{V(s)}}{(1-P_{V(s)})^2}}$$

Таким образом, функция распределения вероятности времени передачи s фрагментов примет вид

$$\Pr\{T(s) \le t\} = F\left(\frac{t - \frac{L_{\mathrm{sc}}}{V_1} - m(s)}{\sigma(s)}\right) \quad (6)$$

Аппроксимируя (6) Гауссовским распределением для заданного t, находим оптимальное значение s.

Рассмотренный пример для моделирования состояний дает возможность пошагово определять значения индикаторов состояния, что позволяет получать наблюдения за числовыми значениями вероятности своевременной доставки.

Для примера реализации работы модели были использованы различные вероятности своевременной доставки исходного объема информации Рд.

В качестве единицы измерения времени t своевременной доставки (рис. 2, 3) при данном подходе используется время передачи блока данных без учета

деструктивных воздействий с учетом пропускной способности сети передачи данных.

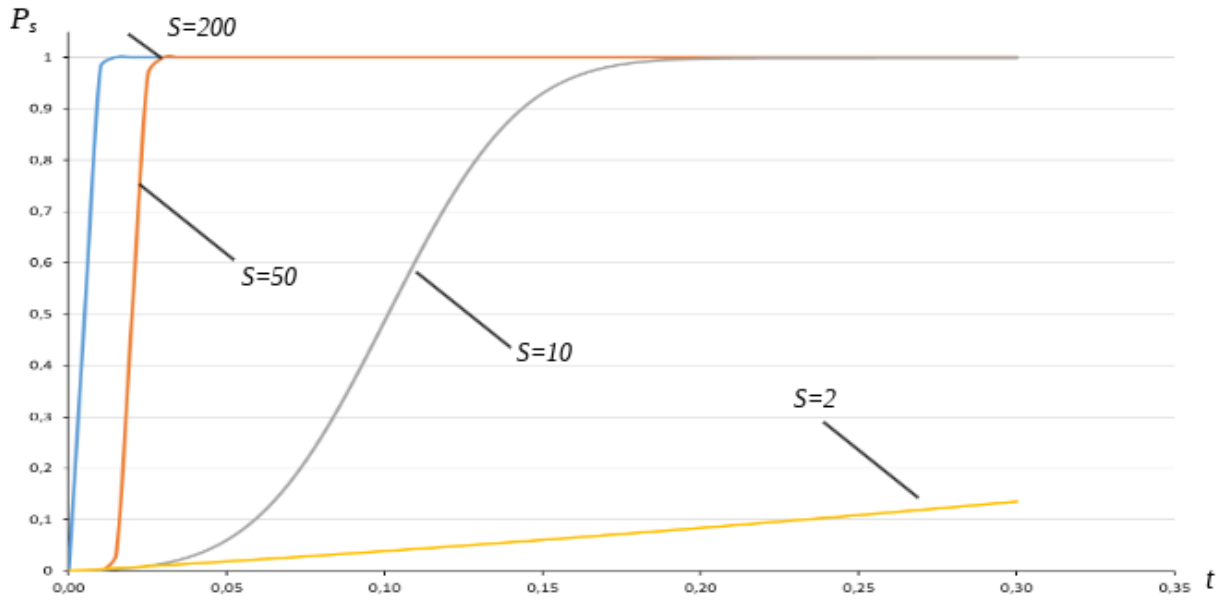


Рис. 2. Результаты моделирования –график зависимости значений своевременной доставки от количества фрагментов при $P_д = 0,9$

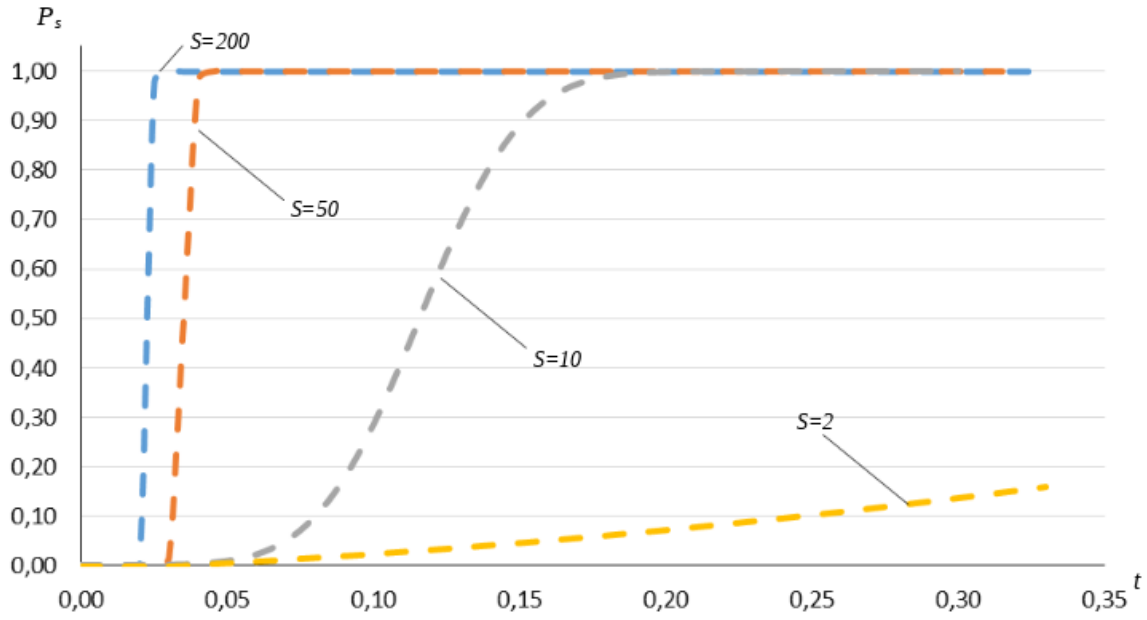


Рис. 3. Результаты моделирования –график зависимости значений своевременной доставки от количества фрагментов при $P_д = 0,5$

Выводы

Из анализа работы полученной математической модели процесса доведения информации до подвижных носителей, можно сделать вывод, что при передаче больших и сверхбольших объемов информации (при несопоставимой разнице в объемах контрольных сумм и фрагмента передаваемых данных) в

интересах планирования применения объектов специального назначения, процесс фрагментации блока данных на фрагменты, позволяет существенно повысить вероятность своевременной доставки объемов информации, необходимой для планирования применения объектов специального назначения.

Все это позволяет сделать вывод о целесообразности использования разработанной модели для математического описания стохастического процесса доведения информации, имеющего место в системе доведения информации до подвижных носителе.

В работе предложен подход к повышению своевременности доведения информации больших объемов за счет фрагментации исходного объема информации. Показана возможность повышения вероятности своевременного доведения информации при применении модели процесса доведения информации.

Список используемых источников

1. Концепция развития информационных и телекоммуникационных технологий Вооруженных Сил Российской Федерации на период до 2025 года. М.: МО РФ, 2015. 16 с.
2. Захаров А. И., Основы передачи данных. Санкт-Петербург, Военная академия связи, 1985. С. 19–41.
3. Хедми А. Таха, Исследование операций. СПб.: Издательский дом «Вильямс», 2016.
4. Вентцель Е. С., Теория вероятностей. М.: Издательский дом «Академия», 2003.
5. Чуднов А. М. Монография. Математические основы моделирования, анализа и синтеза систем. СПб.; Военная академия связи, 2021.
6. Богатырев В. А., Богатырев С. В. Своевременность обслуживания в многоуровневых кластерных системах поэтапным уничтожением просроченных запросов // Вестник компьютерных и информационных технологий, 2017. № 2. С. 28–35.

Chernobrovkin S. **INFORMATION DELIVERY PROCESS MODEL TO MOBILE MEDIA.**

Military Academy of Communications named after
Marshal of the Soviet Union S. M. Budyonny

With the development of technology, the amount of information transmitted for decision making by officials is increasing. In this regard, it makes sense to provide information delivery by fragmenting the initial volume of transmitted data in order to increase the probability of its timely delivery to officials. To solve the problem, we propose a model of the information dissemination process.

Key words: data transfer, data fragmentation, likelihood of timely communication.

3.2. Информационные технологии в дизайне

УДК 004.9
ГРНТИ 20.15.05

АДАПТАЦИЯ МОДЕЛИ ЛОТКИ-ВОЛЬТЕРРЫ ДЛЯ МОДЕЛИРОВАНИЯ ВЗАИМОДЕЙСТВИЯ ТУРИСТОВ И ПРИРОДНЫХ РЕСУРСОВ НА ЭКОЛОГИЧЕСКИХ МАРШРУТАХ

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

В данном исследовании рассматривается воздействие туризма на экосистемы экологических троп и предлагается адаптация модели Лотки-Вольтерры для анализа динамики туристической нагрузки. Система дифференциальных уравнений используется для прогнозирования изменений численности туристов и состояния природных ресурсов. На основе моделирования предложены рекомендации по управлению туристическим потоком для минимизации ущерба и поддержания устойчивости экосистем. Результаты исследования могут быть полезны при проектировании экологических маршрутов и разработке стратегий устойчивого туризма.

туризм, экологические тропы, модель Лотки-Вольтерры, устойчивость экосистем, управление туризмом, устойчивое развитие, экологические маршруты, моделирование, туристический поток

Туризм оказывает немаловажное воздействие на природную среду и экосистемы, значительное влияние оказывается и в зонах экологических троп, где на небольших территориях концентрируется большая плотность посетителей. Понимание динамики взаимодействия туристов и природных ресурсов становится важным фактором для устойчивого управления экологическими маршрутами и сохранения природного ресурса.

Одним из способов количественной оценки рассматриваемого взаимодействия является адаптация модели Лотки-Вольтерры [1] в рамках моделирования процессов на экотропах. Первоначально модель предназначалась для описания взаимодействия типа «хищник»-«жертва». В рамках данной работы

адаптируем модель для анализа динамики туристической нагрузки на природные ресурсы, для прогнозирования устойчивости экосистем и в дальнейшем разработать меры по регулированию туристического потока, минимизирую ущерб и поддерживая экологический баланс.

Актуальность данной работы связана с растущим воздействием туризма на экосистемы экологических троп, что тем самым создает риск изнеможения природных ресурсов в условиях повышенного потока туристов.

Цель статьи – использование модели Лотки-Вольтерры для моделирования взаимодействия туристов и экосистемы с целью минимизации негативного воздействия [2]. Целью применения модели является выявления условий, при которых туристический поток не превышает способность экосистем экологических маршрутов к их восстановлению. Данное исследование поможет разработчикам экологических маршрутов и специалистам в области туризма, прогнозировать и регулировать допустимые нагрузки на природные территории, минимизировать их деградацию и предложить меры для устойчивого использования природных ресурсов.

Модель Лотки-Вольтерры описывается взаимодействие двух популяций: «хищников» и «жертв» [3]. В данной работе эти популяции интерпретируются как численность туристов – X(t), которая отражает изменение численности туристов во времени. Рост числа туристов может быть обусловлен привлекательностью маршрута, инфраструктурой или информационной наполненностью. Количество доступных природных ресурсов – Y(t) в зоне экологической тропы, которая отражает состояние природных ресурсов (биоразнообразие, состояние почвы, растительности и т.д.), количество может уменьшаться под воздействием туризма, но имеет способность к восстановлению. Динамика взаимодействия этих переменных может быть выражена системой дифференциальных уравнений (1):

$$\frac{dX}{dt} = X(\alpha - \beta Y) + \frac{c}{X}$$

$$\frac{dY}{dt} = Y(-\gamma + \delta X) + \frac{d}{Y} \qquad (1)$$

где α – коэффициент естественного роста туристов в условиях доступности природных ресурсов;

β – коэффициент убыли туристов вследствие сокращения природных ресурсов;

γ – коэффициент естественного убывания ресурсов экосистемы;

δ – коэффициент восстановления ресурсов под воздействием умеренной туристической нагрузки;

c и d – дополнительные параметры, отражающие внешние влияния на численность туристов и ресурсов соответственно.

Предложенная система уравнений может быть использована для моделирования различных сценариев воздействия туризма на экосистемы.

Экологическая карта маршрутов представляет собой визуализацию того, как распределяются туристы на разных участках маршрута, а также показывает влияние туристического потока на природные ресурсы. В рамках данной работы произведем моделирование на реальном экологическом маршруте, с гипотетическими исходными данными.

Для построения карты выделим несколько ключевых параметров:

– зоны с высокой туристической активностью – это участки маршрута, где поток туристов наиболее интенсивен. В данных зонах экосистема подвержена воздействию в наибольшей степени, и ее состояние может ухудшаться быстрее;

– зоны с высоким потенциалом восстановления – это участки маршрута, где экосистема способна к быстрому восстановлению даже при наличии умеренного туристического потока;

– уязвимые зоны – это места, где даже незначительное увеличение количества туристов может привести к существенному ухудшению состояния экосистем (например, редкие виды растений).

Экологическая карта маршрутов представлена на рисунке 1.

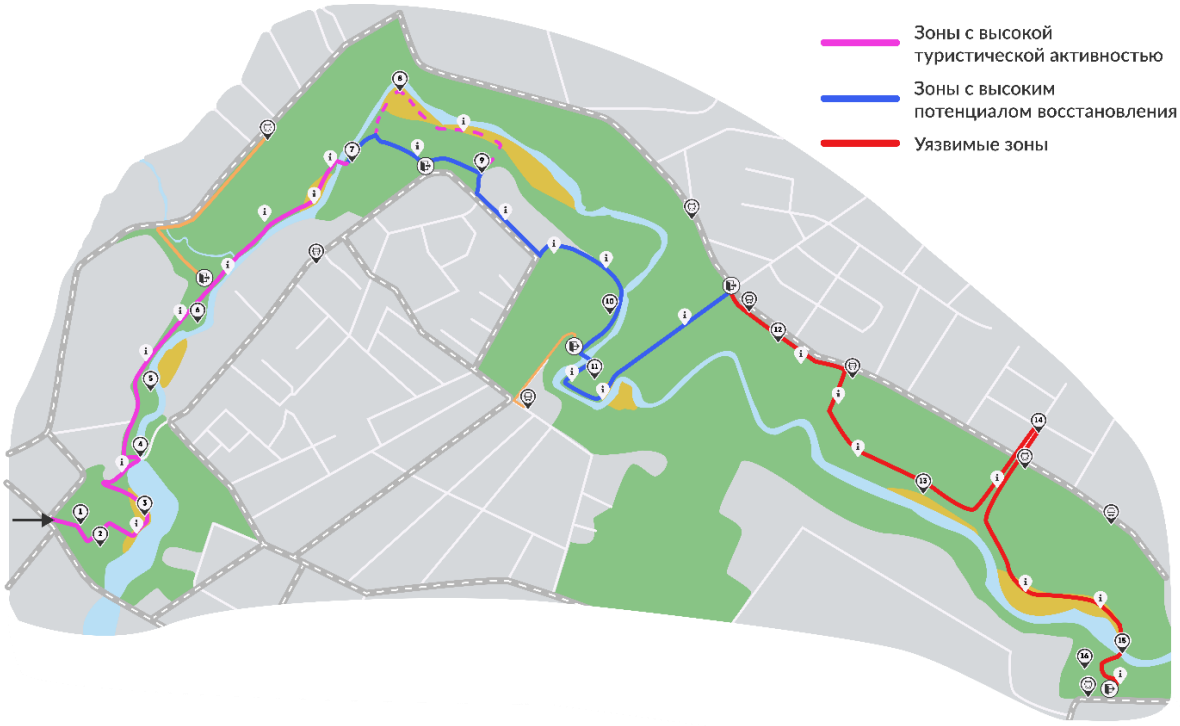


Рис. 1. Экологическая карта маршрутов

Для моделирования на разных участках выбраны следующие значения начальных параметров: $X_0 = 5$ (численность туристов) и $Y_0 = 10$ (начальная доступность ресурсов), временной интервал моделирования составляет один год (365 дней) с дискретизацией по дням, $\alpha = 0.25$, $\beta = 0.3$, $\gamma = 0.7$, $\delta = 0.14$.

Для решения систем дифференцированных уравнений используем численный метод Рунге-Кутты, реализованный в библиотеке *solve_ipv* из пакета *scipy* в Python [4].

На рисунке 2 можно увидеть фазовый портрет системы, как будут меняться природные ресурсы в зависимости от заданных начальных условий. По горизонтальной оси отложены размер природных ресурсов, по вертикали – количество посетителей.

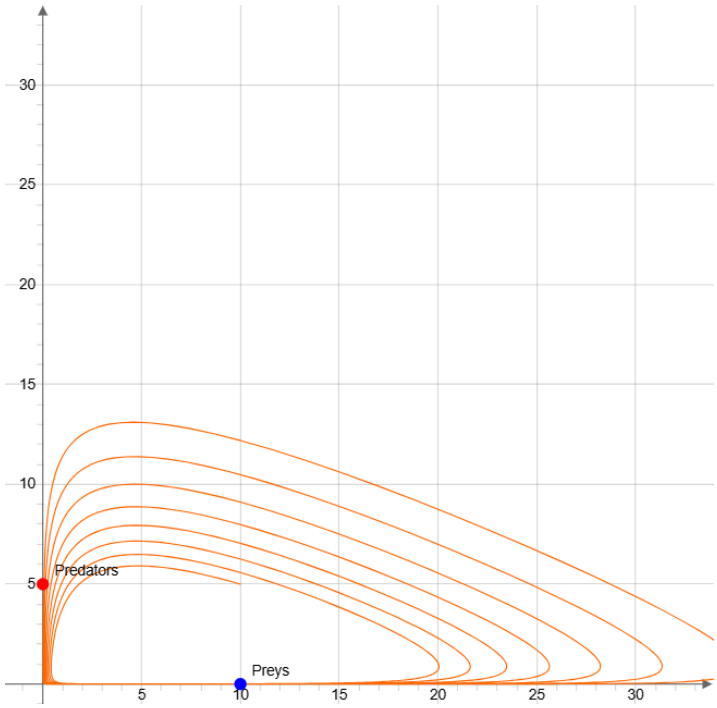


Рис. 2. Фазовый портрет системы

На графике видны спиралевидные траектории, постенно затухающие и приближающиеся к стационарному значению. Это говорит о достижении состояния устойчивого равновесия, где количество ресурсов и туристов становится стабильным, но на начальных этапах наблюдается колебательная динамика, со временем система стабилизируется, что отражает способность экосистемы саморегулироваться и восстанавливаться под влиянием туристов. Полученные результаты подтверждают что полученная модель может быть полезна для прогнозирования устойчивости экосистемы при различных сценариях, в зависимости от параметров α, β, γ, δ.

Произведем расчеты для всех участков экологического маршрута и запишем в таблицу 1.

ТАБЛИЦА 1. Результаты моделирования

Участок маршрута	Начальная численность туристов X0	Начальное состояние ресурсов Y0	Количество туристов через T дней	Состояние ресурсов через T дней	Рекомендации
Участок 1	200	700	230	600	Ввести меры по охране экосистемы
Участок 2	100	500	150	400	Ограничить поток туристов
Участок 3	50	300	80	180	Можно увеличить поток туристов

Полученные данные позволяют глубже понять, как взаимодействуют туристы и ресурсы экосистемы на разных участках маршрута, что способствует разработке рекомендаций по управлению туристическими потоками. На основе представленной модели можно прогнозировать, как будут изменяться численность туристов и доступность природных ресурсов в зависимости от интенсивности системы, однако модель имеет некоторые ограничения, например, не учитывает ряд факторов, таких как сезонные колебания туристической активности, влияние других видов рекреационной деятельности и климатические изменения. В будущем улучшение модели может включать интеграцию более сложных экологических параметров. Развитие описанного подхода откроет новые возможности для проектирования экологически устойчивых маршрутов, минимизации ущерба природе и сохранения уникальных экосистем для будущих поколений.

Список используемых источников

1. Лотка А. Дж. Элементы физической биологии. М.: Наука, 1967.
2. Kignsland S. Alfred J. Lotka and the origins of theoretical population ecology. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC4534218/pdf/pnas.201512317.pdf (дата обращения 05.10.2024).
3. Минаев В. А. Математическая модель «хищник – жертва» в системе информационной безопасности / В.А. Минаев, М.П. Сычев, Е.В. Вайц, Ю.В. Грачева // Информация и безопасность. 2016. № 19 (3). С. 397–400.
4. Медоев Т. Г. Моделирование живучести войсковой группировки на марше в условиях возможного соприкосновения с противником / Т. Г. Медоев, М. А. Чурсина // Актуальные

проблемы защиты и безопасности: труды XXII Всероссийской научно-практической конференции РАРАН, Санкт-Петербург, 01–04 апреля 2019 года. Том 1. СПб: Российская академия ракетных и артиллерийских наук, 2019. С. 343–349.

Andrianov D. **ADAPTATION OF THE LOTKA-VOLTERRA MODEL FOR SIMULATION OF INTERACTION OF TOURISTS AND NATURAL RESOURCES ON ECOLOGICAL ROUTES.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This study examines the impact of tourism on the ecosystems of ecological trails and proposes the adaptation of the Lotka-Volterra model to analyze the dynamics of the tourist load. A system of differential equations is used to predict changes in the number of tourists and the state of natural resources. Based on the simulation, recommendations are proposed for managing the tourist flow to minimize damage and maintain the sustainability of ecosystems. The results of the study can be useful in the design of ecological routes and the development of sustainable tourism strategies.

Key words: tourism, ecological trails, Lotka-Volterra model, ecosystem sustainability, tourism management, sustainable development, ecological routes, modeling, tourist flow.

УДК 004.891
ГРНТИ 20.23.25

ИССЛЕДОВАНИЕ ТЕХНОЛОГИЙ РЕКОМЕНДАТЕЛЬНЫХ СИСТЕМ

Б. Р. Беляев, О. П. Диброва, Е. Ю. Дорохова, Т. В. Мусаева
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье проводится анализ различных типов рекомендательных систем, используемых в работе современных цифровых платформ. Описаны методы коллаборативной фильтрации, обработки естественного языка и аудиомоделей, позволяющие улучшить точность и релевантность рекомендаций. Особое внимание уделено механизмам обработки данных, повышающим качество персонализированных рекомендаций.

рекомендательные системы, коллаборативная фильтрация, обработка естественного языка, аудиомодель, персонализированные рекомендации, цифровые платформы.

Рекомендательные системы играют важную роль в современных цифровых сервисах, помогая пользователям сократить время на поиск товаров, услуг или контента и повышая вероятность обнаружения новых объектов, способных их заинтересовать, благодаря чему повышается лояльность пользователей и удовлетворенность взаимодействием с веб-сервисами.

Рекомендации могут быть персонализированными и неперсонализированными. В первом случае система использует информацию о пользователе, во втором – популярные или сопутствующие товары. В зависимости от типа рекомендательной системы пользователь видит разные рекомендации [1].

Рекомендательные системы делятся на следующие типы: коллаборативная фильтрация, фильтрация на контенте, фильтрация на знания.

Метод коллаборативной фильтрации строится на истории оценок как конкретного пользователя, так и других людей [2]. Используется два типа входных данных: множество объектов интереса и множество пользователей. Отношения между ними чаще всего выражаются при помощи оценок, выставленных пользователями. Например, первый пользователь купил на маркетплейсе товары *A, B, C*, а второй – *B, C, D*. Тогда система, основываясь на данных, предложит первому пользователю купить товар *D*, а второму – товар *A*. Здесь действует принцип накопления знаний: чем больше единиц контента просматривает пользователь, тем точнее становятся рекомендации. Принцип работы метода коллаборативной фильтрации представлен на рис. 1.

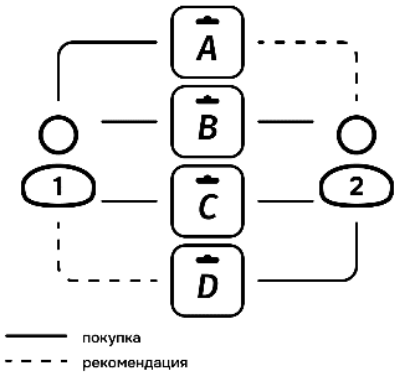


Рис. 1. Принцип работы метода коллаборативной фильтрации

Фильтрация на контенте подбирает менее персонализированные рекомендации, так как данные системы пропускают этап знакомства с пользователем. Пользователю предлагаются объекты, похожие на те, которыми он интересовался до этого. В процессе анализа собирают любые полезные данные: жанр, производитель, конкретные функции и так далее [3]. Например, онлайн-кинотеатр «IVI» выстраивает рекомендации по жанрам, странам-производителям фильмов, актерам, съемочной группе. Принцип работы метода фильтрации на контенте представлен на рис. 2.

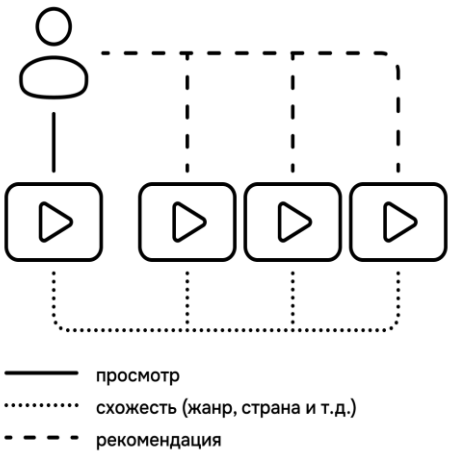


Рис. 2. Принцип работы метода фильтрации на контенте

В системе, основанной на знаниях, рекомендации строятся на основе предметной области, а не отдельных объектов. Системы изучают и производят анализ взаимосвязей между различными объектами, а также учитывают дополнительную информацию, относящуюся к индивидуальным данным конкретного пользователя [4]. Используются фильтры для отсечения нерелевантных товаров и создания предложений, таких как «Покупают вместе». Например, при покупке телефона система предлагает сопутствующие товары, что

способствует увеличению покупок и прибыли компании. Пример подборки «Вместе с этим товаром покупают» представлен на рис. 3.

Рис. 3. Пример подборки «Вместе с этим товаром покупают»

На сегодняшний день рекомендательные системы внедрены практически в каждый веб-сервис. Для разбора выбран Spotify, стриминговый музыкальный сервис, который обрел большую популярность по за счет качественных и точных рекомендаций. Один из плейлистов – «Открытия недели», персональная подборка из 30 новых для слушателя песен, которые, как считает сервис, с высокой вероятностью понравятся пользователю. Популярность подобных рекомендаций побудила Spotify вложить больше ресурсов в разработку алгоритмов создания плейлистов [5]. Пример плейлиста «Открытия недели» представлен на рис. 4.

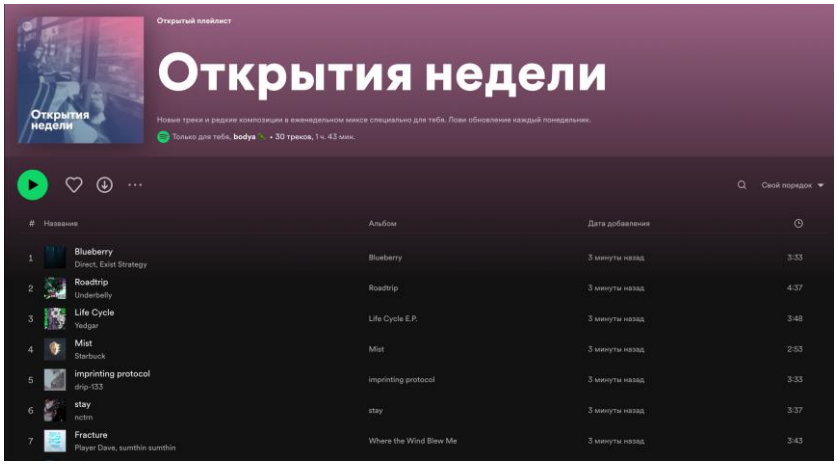


Рис. 4. Пример плейлиста «Открытия недели»

Для «Открытий недели» сервис использует три модели: коллаборативную фильтрацию, обработку естественного языка и аудиомодели.

Коллаборативная фильтрация работает хорошо и по одиночке, но в Spotify улучшили систему для повышения точности рекомендаций. База данных строится на основе косвенных откликов – количество прослушиваний и история действий пользователя (сохранение песни, посещение страницы артиста и так далее).

Обработка естественного языка (ОЕЯ) – способность компьютера понимать человеческую речь. База данных для данной модели строится из тексто-

вой информации о треке, новостях, статьях, упоминаниях в блогах и так далее. Алгоритмы Spotify постоянно исследуют интернет и ищут любые тексты о конкретной музыке, для понимания того, что говорят о той или иной песне.

Допустим, у песни только 50 прослушиваний, что слишком мало для коллаборативный фильтрации. При этом песня нигде не обсуждалась в интернете, никакой информации о ней нет, поэтому и модель ОЕЯ пропустит ее. Здесь на помощь и приходит модель аудиофайлов, которая учитывает даже никому не известные треки. Пример работы представлен на рис. 5.

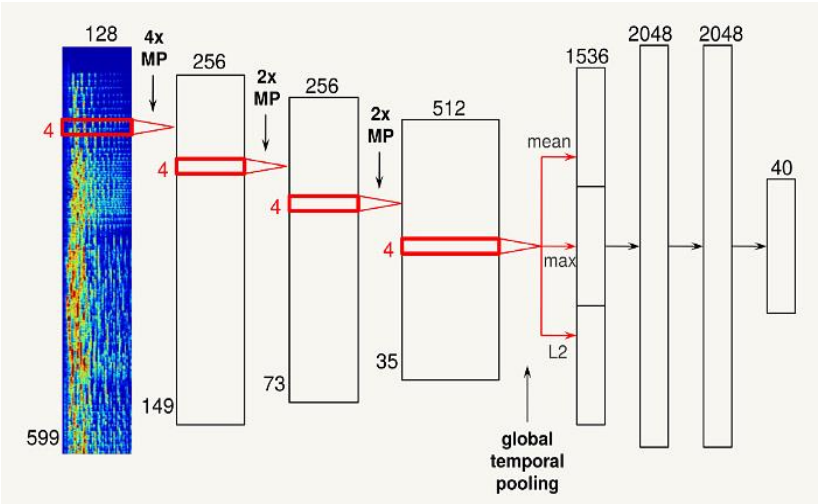


Рис. 5. Пример работы аудиомодели

В модели используется сверточная нейросеть, которая имеет четыре сверточных слоя и три плотных узких слоя. Проходы сквозь слои – временная частота аудиофрагментов, которые на выходе соединяются в спектрограмму. В итоге получается некое «понимание» песни, которое включает в себя размер песни, гармонию, темп и громкость.

Считывание ключевых характеристик определенных песен помогает Spotify понять различия между треками. После завершения работы всех трех алгоритмов пользователи получают свои «Открытия недели», пользующиеся спросом у слушателей.

Рекомендательные системы, будучи одним из ключевых инструментов современных цифровых платформ, оказывают значительное влияние на взаимодействие пользователей с сервисами.

Коллаборативная фильтрация, фильтрация на контенте и фильтрация на знания имеют сильные и слабые стороны. Коллаборативная фильтрация предлагает точные рекомендации на основе похожих предпочтений других пользователей, но требует больших объемов данных, что может затруднить рекомендации новых или редких треков. Фильтрация на контенте использует характеристики самих объектов, что снижает зависимость от данных о поведе-

нии пользователей, но иногда ограничивает учет индивидуальных вкусов. Фильтрация на знаниях обеспечивает высокую точность, анализируя взаимосвязи между объектами и контекстные данные, но ее настройка требует значительного объема информации и сложных правил, что может ограничивать ее гибкость.

Например, для поиска музыкальных предпочтений лучше всего подходит метод, улучшающий коллаборативную фильтрацию. Данный подход позволяет учитывать как индивидуальные вкусы, так и характеристики музыкальных треков, связи между жанрами и стилями, что обеспечивает наиболее точные и разнообразные рекомендации.

Различные методы рекомендаций позволяют компаниям повышать точность и релевантность предложений. Совершенствование данных систем способствует повышению лояльности и удовлетворенности пользователей.

Список используемых источников

1. Рекомендательные системы: что это и как работает алгоритм рекомендаций. URL: https://mindbox.ru/journal/education/rekomendatelnye-sistemy/ (дата обращения 06.11.2024).
2. Андреева Я. А. Сравнительный анализ рекомендательных систем и методов оценки их качества / Я. А. Андреева, К. А. Василевский // Международный журнал информационных технологий и энергоэффективности, 2022. Т. 7. № 4-1 (26). С. 59–66.
3. Рекомендательные системы: как помочь пользователю найти то, что ему нужно? URL: https://vc.ru/marketing/152926-rekomendatelnye-sistemy-kak-pomoch-polzovatelyu-nayti-to-chto-emu-nuzhno (дата обращения 07.11.2024).
4. Что такое рекомендательные системы и как они работают. URL:https://skillbox.ru/media/code/chto_takoe_rekomendatelnye_sistemy_i_kak_oni_rabotayut / (дата обращения 07.11.2024).
5. Откуда Spotify знает, что нам нравится? URL: https://i-m-i.ru/post/how-spotify-works (дата обращения 09.11.2024).

Belyaev B., Dibrova O., Dorokhova E., Musaeva T. **STUDY OF TYPES OF RECOMMENDER SYSTEMS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article analyzes various types of recommendation systems used in modern digital platforms. It describes methods of collaborative filtering, natural language processing, and audio models that improve recommendation accuracy and relevance. Special attention is given to data processing mechanisms that enhance the quality of personalized recommendations.

Key words: recommendation systems, collaborative filtering, natural language processing, audio model, personalized recommendations, digital platforms.

УДК 004.832
ГРНТИ 28.23.37

ПРИМЕНЕНИЕ GPT-4 В РЕШЕНИИ ОЛИМПИАДНЫХ ЗАДАЧ ПО МАТЕМАТИКЕ ДЛЯ СТАРШЕКЛАССНИКОВ

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

В настоящее время наблюдается повышенный интерес к исследованиям применения нейронных сетей в различных сферах науки, включая как творческие, так и технические области знаний. Данное исследование анализирует результат работы нейронной сети Generative Pre-trained Transformer 4 в решении олимпиадных задач по математике для учеников старших классов, проводимых в России за учебный 2023-2024 год. Результаты работы нейронной сети оказались следующими: в половине задач она справилась с поиском и обоснованием решения.

нейронные сети, математика, применение нейронных сетей, GPT-4

Нейронные сети представляют собой важнейший компонент современных научных и технологических исследований [1] и оказывают значительное влияние на развитие наук, в том числе математику. В последние годы, благодаря интенсивному развитию аппаратных ресурсов и методов глубокого обучения, нейронные сети стали доступны широкому кругу пользователей, в том числе школьникам.

Целью данной работы является проведение анализа использования нейронных сетей при решении математических задач школьных олимпиад, проводимых разными организациями в 2023-2024 учебный год в России.

Для исследования выбраны олимпиады, включенные в Перечень олимпиад для школьников [2]. Поскольку база данных нейронной сети GPT-4 на момент исследования ограничивается октябрем 2023 года, информации о прямом решении приведенных задач в ней не содержится. Существуют тесты [3], которые проверяли работу GPT-4 в математических задачах. Согласно им (рис. 1), нейронная сеть решает 52.9 % задач, схожих по структуре с олимпиадными задачами для старшеклассников.

	GPT-4	GPT-3.5
Undergraduate level knowledge *MMLU*	86.4% 5-shot	70.0% 5-shot
Graduate level reasoning *GPQA, Diamond*	35.7% 0-shot CoT	28.1% 0-shot CoT
Grade school math *GSM8K*	92.0% 5-shot CoT	57.1% 5-shot
Math problem-solving *MATH*	52.9% 4-shot	34.1% 4-shot

Рис. 1. Результаты тестов рассматриваемых нейронных сетей в математике

В таблице 1 приведены результаты работы нейронной сети в решении трех заключительных этапов олимпиад: «Высшая проба» для учеников одиннадцатых и десятых классов, «50-я Всероссийская математическая олимпиада школьников» для учеников одиннадцатых классов.

ТАБЛИЦА 1. Результаты работы нейронной сети GPT-4 в решении олимпиадных задач по математике для старшеклассников

Название олимпиады, этап, класс	Общее количество задач	Количество решенных задач	Ожидаемое количество набранных баллов / общее количество баллов	Время выполнения этапа олимпиады нейронной сетью / ограничение по времени на этап	Ожидаемое место в конкурсном списке / общее число участников
«Высшая проба» 2023/2024, заключительный этап, 11 класс	6	6	50/100	15 минут/240 минут	136/775
«Высшая проба» 2023/2024, заключительный этап, 10 класс	6	3	20/100	15 минут/240 минут	159/387
«50-ая Всероссийская математическая олимпиада школьников», заключительный этап, 11 класс	8	2	10/50	18 минут/240 минут	Данные отсутствуют

У балловой оценки решения каждого задания существуют ряд критериев, которые оцениваются экзаменаторами, поэтому при оценке каждой работы возникает фактор субъективности: критерии не всегда полные, а в каких-то

заданиях отсутствуют вообще. Из-за этого при заполнении таблицы вписывался минимальный балл, который получила бы нейронная сеть при выполнении заданий, в соответствии с пояснением критериев организаторов. Всего решено 11 из 20 задач, которые можно поделить на две категории: алгебраические и геометрические. Основные проблемы нейронная сеть демонстрировала в решении геометрических задач – при правильных ответах, ход решения в большинстве задач оказался спутанных или нелогичным.

На всероссийской математической олимпиаде нейронная сеть набрала 10 баллов, справившись с двумя заданиями из восьми. На олимпиаде «Высшая проба» для одиннадцатых классов нейронная сеть справилась лучше 82 % участников, для десятых классов – лучше 59 %.

По результатам исследования можно заключить, что нейронная сеть GPT-4 способна интерпретировать задачи на естественном языке в математические, после чего решать их – даже те, которые считаются сложными для учеников старших классов школы. Нейронная сеть решила 55 % олимпиадных задач, выдав верные ответы и корректно обосновав решения.

Для составителей олимпиад рекомендуется учитывать этот фактор при подготовке задач и способов принятия экзаменов. Дальнейшие исследования по теме могут включать сравнительные результаты по выполнению аналогичных задач с другими видами (версиями) нейронных сетей.

Список используемых источников

1. Зубричев Н. В. Обзор областей применения нейросетей / Н. В. Зубричев, Ф. А. Ащепков // Концепция динамического равновесия в новых технологиях: сборник статей Международной научно-практической конференции, Казань, 22 октября 2017 года. Казань: Общество с ограниченной ответственностью "ОМЕГА САЙНС", 2017. С. 33–36.
2. Приказ Министерства науки и высшего образования Российской Федерации от 28.08.2023 № 823 "Об утверждении перечня олимпиад школьников и их уровней на 2023/24 учебный год" (Зарегистрирован 28.09.2023 № 75362).
3. Gpt4 comparison to anthropic Opus on benchmarks. URL: https://community.openai.com/t/gpt4-comparison-to-anthropic-opus-on-benchmarks/726147 (дата обращения 01.11.2024).

Botalov A. **APPLICATION OF GPT-4 IN SOLVING COMPETITIONS MATHEMATICS PROBLEMS FOR HIGH SCHOOL STUDENTS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Currently, there is an increased interest in research on the application of neural networks across various scientific fields, including both creative and technical domains. This paper analyzes the performance of the Generative Pre-trained Transformer 4 neural network in solving mathematics competition problems for high school students conducted in Russia during the 2023-2024 academic year. The neural network's results showed that it successfully found and justified solutions for half of the tasks.

Key words: neural networks, mathematics, application of neural networks, GPT-4.

УДК 004.85; 004.056
ГРНТИ 05.13.10

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОЕКТИРОВАНИИ ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСОВ

Д. В. Волошинов, Е. А. Иваненко
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Актуальность работы обусловлена стремительным развитием технологий искусственного интеллекта (ИИ) и их возрастающим влиянием на проектирование пользовательских интерфейсов. Создание более интуитивно-понятных и персонализированных интерфейсов стимулирует поиск новых подходов к их проектированию. Рассмотрены имеющиеся решения в проектировании интерфейсов с использованием искусственного интеллекта.

искусственный интеллект, пользовательские интерфейсы, персонализация, прогнозная аналитика, автоматизация

В условиях стремительной цифровизации всех сфер жизни происходит активное исследование новых методов взаимодействия человека с расширяющимся цифровым пространством. Искусственный интеллект становится одним из ключевых двигателей этой эволюции, особенно в сфере проектирования пользовательских интерфейсов.

Искусственный интеллект в проектировании интерфейсов представляет собой совокупность технологий, которые автоматизируют и улучшают процесс создания пользовательских интерфейсов. ИИ может помогать дизайнерам в различных задачах. Однако, несмотря на ряд преимуществ, использование искусственного интеллекта в проектировании интерфейсов сопряжено с некоторыми вызовами. Например, отсутствие достаточного количества специалистов, компетентных в использовании искусственного интеллекта в дизайне интерфейсов, ограничивает широкое внедрение этих технологий.

Одной из ключевых тенденций в применении искусственного интеллекта в проектировании пользовательских интерфейсов является персонализация [1].

Персонализация – это использование данных о пользователе для создания уникального опыта взаимодействия с интерфейсом. Персонализация позволяет привлечь и удержать пользователей, особенно если продукт ориентирован на разные целевые аудитории. Однако традиционные методы персонализации часто оказываются трудоемкими и не всегда успешными [2]. Требуется тщательное сегментирование пользователей, чтобы предложить им функции, которые будут действительно ценны для них.

Искусственный интеллект радикально меняет этот подход, открывая новые перспективы и возможности. Стоит отметить, что искусственный интеллект обладает способностью анализировать большие объемы данных о пользователях с высокой скоростью, что позволяет командам дизайнеров глубоко понимать потребности клиентов и точно настраивать продукты под их индивидуальные требования. Результат – высоко персонализированный пользовательский интерфейс.

Примером является программа The Grid, которая анализирует содержание страницы и предлагает целесообразное расположение элементов с помощью интеллектуальных алгоритмов, учитывая размер и тип элементов, их важность и целевую аудиторию [3]. Более того, The Grid может учитывать данные о предпочтениях пользователя и персонализировать компоновку страницы для каждого пользователя, делая ее более релевантной и удобной. Например, для пользователя, который в основном использует мобильное устройство, The Grid может предложить более компактную компоновку, чтобы упростить навигацию и обеспечить интуитивно-понятный просмотр на малом экране. В то же время, для пользователя, который использует компьютер, The Grid может предложить более широкую компоновку с большим количеством информации.

Другой важной тенденцией является прогнозная аналитика. Прогнозная аналитика – это использование искусственного интеллекта для предсказания будущего поведения пользователя на основе анализа его прошлых действий. Прогнозная аналитика позволяет оптимизировать расположение элементов на странице, предлагать релевантные предложения и увеличить вероятность желаемых действий пользователя. К примеру, Attention Insight генерирует тепловые карты и визуализирует зоны максимального внимания, что дает ценную информацию о юзабилити интерфейса, что представлено на рис. 1.

Рис. 1. Тепловая карта мобильного приложения кофейни

Более того, искусственный интеллект помогает перевести прогнозную аналитику на новый уровень. Алгоритмы могут получать доступ к данным о клиентах из разных источников [4], что позволяет системе дизайна предвидеть, какой путь взаимодействия будет использовать пользователь, и соответствующим образом корректировать его. Что, несомненно, приводит к повышению качества обслуживания клиентов и улучшению их взаимодействия с продуктом.

В дополнение к персонализации и прогнозной аналитике, искусственный интеллект также автоматизирует многие рутинные задачи в проектировании интерфейсов, освобождая дизайнеров от монотонной работы и позволяя им сосредоточиться на более творческих задачах, например, на разработке новых концепций и решений. Искусственный интеллект может автоматизировать следующие процессы: создание прототипов, тестирование юзабилити и генерация контента. Примером такой автоматизации является программа Usketch, которая позволяет пользователю рисовать скетчи прототипа прямо на экране устройства, а искусственный интеллект превращает эти скетчи в реалистичные прототипы с четкими элементами интерфейса.

Помимо вышеупомянутых тенденций стоит обратить внимание на способность искусственного интеллекта анализировать восприятие цветов, шрифтов и предлагать оптимальные решения для улучшения визуального дизайна. Программа Procreate, доступная для iPad, является ярким примером такого инструмента. Система позволяет конвертировать изображения, фотографии или рисунки в готовые палитры, содержащие гармонично сочетающиеся цвета [5]. Таким образом, значительно упрощается процесс подбора цветовых сочетаний, особенно для дизайнеров, которые не являются профессиональными колористами.

Проблема обосновывается тем, что в условиях стремительного развития цифровых технологий и растущего объема данных искусственный интеллект становится неотъемлемой частью процесса проектирования современных пользовательских интерфейсов [6], что, в свою очередь, способствует повышению качества и уровня взаимодействия с цифровыми продуктами. Это подчеркивает актуальность рассматриваемой темы.

Чтобы определить направления дальнейших исследований необходимо проанализировать уже имеющиеся решения в проектировании интерфейсов с использованием искусственного интеллекта.

В настоящее время многие компании внедряют в свои продукты искусственный интеллект для проектирования пользовательских интерфейсов, анализ функционала программ приведен в таблице 1.

ТАБЛИЦА 1. Анализ использования ИИ в проектировании интерфейсов

Название программы	Предназначение ИИ	Функции
Procreate (iPad)	AI для анализа восприятия цвета и шрифта	Преобразует изображения, фотографии или рисунки в готовые цветовые палитры, упрощая подбор гармоничных сочетаний
Adobe Color	AI для анализа восприятия цвета и шрифта	Создает цветовые палитры на основе анализа введенных параметров
Coolors.co	AI для анализа восприятия цвета и шрифта	Генерирует цветовые палитры на основе изображений или ключевых слов
Palette.fm	AI для анализа восприятия цвета и шрифта	Предлагает цветовые палитры, основанные на популярных стилях дизайна
Usketch	AI для автоматизации прототипирования	Позволяет пользователю рисовать скетчи прототипа прямо на экране устройства, а искусственный интеллект превращает эти скетчи в реалистичные прототипы с четкими элементами интерфейса
Figma	AI для автоматизации прототипирования	Может использовать ИИ для автоматической генерации элементов интерфейса, таких как кнопки, формы и текстовые поля
Adobe XD	AI для автоматизации прототипирования	Предлагает инструменты для автоматической генерации прототипов на основе схем и данных о пользователях
Attention Insight	AI для прогнозной аналитики внимания пользователя	Создает тепловые карты для визуализации зоны максимального внимания пользователя
The Grid	AI для персонализации интерфейса	Анализирует содержание страницы и предлагает оптимальное расположение элементов с учетом размера, типа и важности элементов, а также целевой аудитории
UXPin Merge	AI для персонализации интерфейса	Позволяет создавать персонализированные интерфейсы на основе данных о пользователях и для генерации вариантов компоновки и стиля

Анализ показал, что текущие версии программ не в полной мере удовлетворяет разнообразные потребности пользователей, обусловленные возрастными, гендерными и другими факторами.

Дальнейшее развитие ИИ в проектировании интерфейсов требует интеграции более сложных алгоритмов персонализации, способных учитывать не только демографические данные, но и динамические поведенческие паттерны пользователей в контексте их взаимодействия. Необходимо совершенствова-

ние прогнозной аналитики на основе многоканальных данных для более точного предсказания поведения пользователей и предложения релевантных функций. Ключевым направлением является повышение интеллектуальности автоматизации процессов проектирования, включая использование генеративных моделей ИИ и систем юзабилити-тестирования.

Таким образом, несмотря на развивающееся направление применения искусственного интеллекта в дизайне, многие компании и дизайнеры отказываются от использования ИИ в проектировании интерфейсов, поскольку считают его слишком сложным и требующим специальных навыков. Это ограничивает широкое внедрение ИИ-технологий и задерживает развитие проектирования интерфейсов дизайна в целом.

Исходя из вышесказанного, искусственный интеллект не заменяет человеческую мысль и креативность, а скорее становится мощным инструментом, который помогает дизайнерам реализовать свои идеи более успешно и инновационно. В развивающемся обществе искусственный интеллект будет продолжать влиять на то, как дизайнеры создают свою продукцию, формируя будущее проектирования интерфейсов.

Список используемых источников

1. Милкова Э. Г. Современные тренды в развитии искусственного интеллекта. URL: https://cyberleninka.ru/article/n/sovremennye-trendy-v-razvitii-iskusstvennogo-intellekta (дата обращения 10.11.2024).
2. Number of mobile app downloads worldwide from 2016 to 2022. URL: https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/ (дата обращения 11.11.2024).
3. Малашук Е. В. Инструменты ИИ в веб-дизайне: области применения и методы использования // Инновационная наука. 2023. № 10–1. URL: https://cyberleninka.ru/article/n/ instrumenty-ii-v-veb-dizayne-oblasti-primeneniya-i-metody-ispolzovaniya (дата обращения 10.11.2024).
4. Абалуев Р. Н., Шацкий В. А., Картечина Н. В. Подходы к проектированию модуля Web-интерфейса для подсистемы машинного обучения // Наука и образование, 2022. № 1. URL: https://cyberleninka.ru/article/n/podhody-k-proektirovaniyu-modulya-web-interfeysa-dlya-podsistemy-mashinnogo-obucheniya (дата обращения 14.11.2024).
5. Зубкова Т. М., Тагирова Л. Ф., Тагиров В. К. Прототипирование адаптивных пользовательских интерфейсов прикладных программ с использованием методов искусственного интеллекта // Научно-технический вестник информационных технологий, механики и оптики, 2019. № 4. URL: https://cyberleninka.ru/article/n/prototipirovanie-adaptivnyh-polzovatelskih-interfeysov-prikladnyh-programm-s-ispolzovaniem-metodov-iskusstvennogo-intellekta (дата обращения 12.11.2024).
6. Зубкова Т М., Наточая Е Н. Проектирование интерфейса программного обеспечения с использованием элементов искусственного интеллекта // Программные продукты и си-

стемы, 2017. № 1. URL: https://cyberleninka.ru/article/n/proektirovanie-interfeysa-programmnogo-obespecheniya-s-ispolzovaniem-elementov-iskusstvennogo-intellekta (дата обращения 12.11.2024).

Voloshinov D., Ivanenko E. **APPLICATION OF ARTIFICIAL INTELLIGENCE IN USER INTERFACE DESIGN.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The relevance of the work is due to the rapid development of artificial intelligence (AI) technologies and their increasing influence on the design of user interfaces. The creation of more intuitive and personalized interfaces stimulates the search for new approaches to their design. Available solutions in designing interfaces using artificial intelligence are reviewed.

Key words: Artificial intelligence, user interfaces, personalization, predictive analytics, automation.

УДК 004.22
ГРНТИ 62.03.01

ИСПОЛЬЗОВАНИЕ ВИЗУАЛЬНЫХ СИСТЕМ ДЛЯ МОНИТОРИНГА ПЕРСОНАЛА И РАБОЧИХ ПРОЦЕССОВ

И. И. Гольдин, А. А. Шиян
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе рассматриваются вопросы внедрения визуальных подходов к мониторингу для улучшения восприятия персоналом данных. Особое внимание уделяется тому, как такие системы помогают отслеживать статус сотрудников, повысить прозрачность рабочих процессов. Вопросы интеграции с корпоративными платформами, улучшения координации внутри команды и повышения производительности также являются важными аспектами.

визуальные системы мониторинга, адаптивность системы, оптимизация ресурсов, прогнозирование и аналитика, нестандартные схемы визуализации

В современных компаниях с увеличением объема информационных ресурсов растет потребность в инструментах для оперативного отслеживания и управления статусами сотрудников. Одной из таких технологий становятся визуальные системы мониторинга, которые в реальном времени отображают текущие задачи, занятость и прогресс работы персонала. Эти системы помогают координировать рабочие процессы и выявлять узкие места в управлении, что особенно актуально в условиях высокой интенсивности работы и необходимости быстрого принятия решений. Благодаря этим системам информация о статусах сотрудников становится доступной и наглядной, что позволяет менеджерам и коллегам быстро ориентироваться в загрузке персонала и готовности к новым проектам. Например, мониторинг активности сотрудников помогает более точно распределять задачи и предотвращать перегрузки, делая управление гибче и снижая риск простоев.

Такие системы легко интегрируются с корпоративными платформами, включая CRM, ERP и другие инструменты управления проектами, что позволяет адаптировать их под задачи конкретной компании. Визуальные системы мониторинга находят применение в разных отраслях. В ИТ-компаниях они отображают прогресс работы команд разработчиков и помогают менеджерам видеть общую картину загрузки сотрудников. В производственных и логистических компаниях такие системы способствуют улучшению координации между командами и более точному распределению ресурсов. Помимо повы-

шения прозрачности и управляемости, такие системы помогают сократить затраты, связанные с неэффективной организацией труда.

Они ускоряют процесс принятия решений, уменьшают количество простоев и позволяют избежать спешных перераспределений задач. В перспективе такие решения могут быть дополнены предиктивной аналитикой, которая будет прогнозировать возможные трудности и предлагать рекомендации по повышению эффективности. Развитие технологий искусственного интеллекта позволяет этим платформам автоматически адаптироваться к изменениям и оптимизировать задачи на основе данных, что делает визуальные системы перспективным инструментом для повышения эффективности и вовлеченности сотрудников в рабочий процесс. Для графических систем мониторинга важным фактором являются интуитивность и удобство восприятия. Простые и понятные схемы помогают пользователям легко ориентироваться в статусах коллег, не отвлекаясь на сложные интерфейсы. Цветовые индикаторы и значки, указывающие состояния сотрудников («занят», «свободен», «выполняет задачу»), упрощают восприятие данных. Также такие схемы должны быть адаптивными, чтобы соответствовать требованиям конкретной компании и ее специфике.

Интеграция с корпоративными системами, такими как CRM и ERP, обеспечивает актуальность данных и их автоматическое обновление. Не менее важна аналитическая функция этих систем. Они должны не только отображать текущие статусы сотрудников, но и предоставлять прогнозы, чтобы менеджеры могли заранее предвидеть задержки или перегрузки. Такой аналитический компонент помогает точнее планировать и распределять ресурсы, делая управление более взвешенным и эффективным. Одним из ключевых аспектов является безопасность данных. Системы должны обладать высоким уровнем защиты и ограничивать доступ к информации, чтобы соблюдать конфиденциальность. Это исключает несанкционированный доступ к данным о рабочих процессах и персональных сведениях сотрудников.

Кроме того, визуальные системы мониторинга могут положительно влиять на корпоративную культуру и коммуникации [1]. Прозрачность работы позволяет сотрудникам видеть загруженность коллег и развивает осознанный подход к планированию. Такие системы также помогают новым сотрудникам быстрее адаптироваться, предоставляя наглядную информацию о задачах и статусах, что ускоряет их включение в рабочий процесс и облегчает взаимодействие с командой.

Применение визуализации данных сотрудников на предприятиях связи

На предприятиях связи, где работа часто требует координации многочисленных специалистов и команд, визуализация данных становится важным эле-

ментом управления. Ниже рассмотрены несколько практических аспектов использования таких систем в отрасли связи:

1. Для предприятий связи, занимающихся установкой и техническим обслуживанием оборудования, особое значение приобретает мониторинг полевых сотрудников. Визуальные системы позволяют оперативно отслеживать их местоположение, статус задач и степень загрузки. На карте можно в реальном времени видеть, какие сотрудники находятся в активной зоне и готовы принять новый заказ, что оптимизирует распределение рабочих заданий и снижает время ожидания клиентов;

2. В условиях, когда сотрудники предприятия связи выполняют многоэтапные проекты, визуализация данных помогает управлять не только текущее распределение задач, но и учет производительности в долгосрочной перспективе. Системы мониторинга позволяют анализировать время, затраченное на выполнение различных этапов проекта, и сопоставлять его с плановыми показателями. В результате руководство получает возможность более эффективно планировать ресурсы, минимизировать временные затраты и повышать общую производительность команды.

Одним из решений для мониторинга и управления рабочим временем сотрудников является Monitask (рис 1). Эта платформа позволяет вести учет рабочего времени и активности сотрудников, фиксируя использование приложений и веб-сайтов. Monitask поддерживает прозрачность в управлении командой, предоставляя данные для анализа продуктивности каждого сотрудника и выявления возможных узких мест в процессе работы. Это позволяет руководителям оптимизировать рабочие процессы и повышать общую эффективность команды, особенно в условиях удаленной работы.

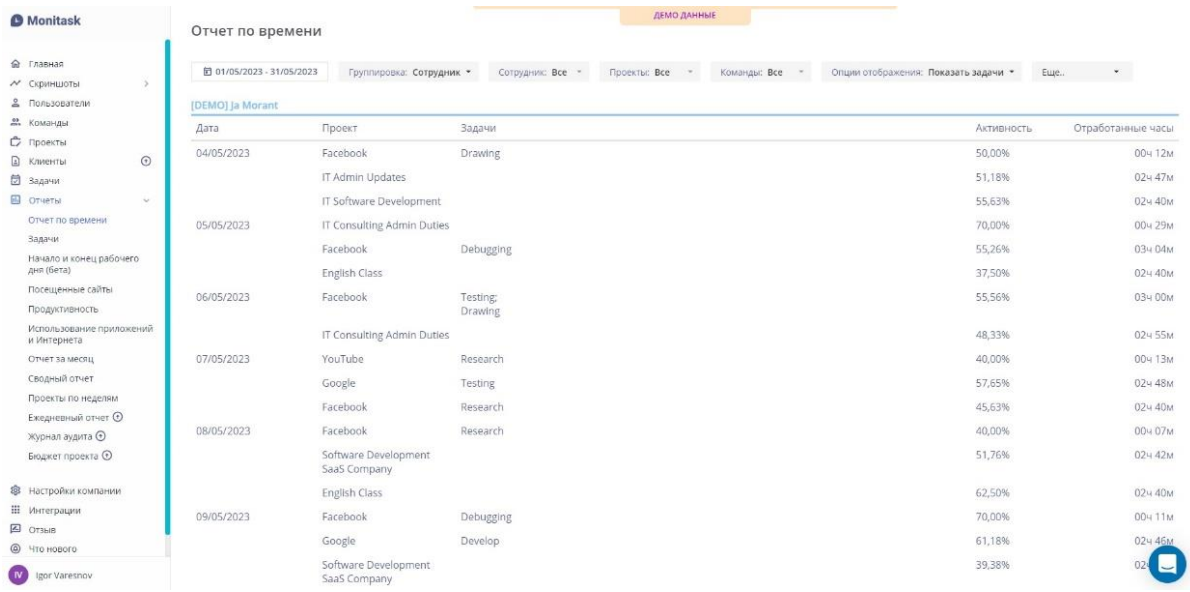


Рис. 1. Интерфейс Monitask, системы учета рабочего времени и контроль сотрудников

Продолжая обсуждение возможностей визуализации данных о сотрудниках, стоит отметить альтернативный подход – использование схемы Лиц Чернова и других подобных карт, которые иллюстрируют данные мониторинга персонала на предприятии. Такие схемы, по своей структуре и визуальным характеристикам, выделяются на фоне традиционных диаграмм и графиков. Лица Чернова представляют собой особую визуализацию данных, где состояние и вовлеченность сотрудников можно отобразить через эмоциональные выражения, похожие на лица, и различные графические элементы. Это позволяет интуитивно воспринимать информацию о рабочей нагрузке, активности и удовлетворенности персонала, не углубляясь в числовые данные.

В отличие от стандартных графических интерфейсов, эти визуальные схемы акцентируют внимание на интуитивности и эмоциональном восприятии [2]. Если представить ход выполнения проекта, обозначив все этапы при помощи нестандартных схем, то этот подход облегчит анализ больших объемов данных (рис. 2) ведь человек быстрее замечает и различает эмоциональные образы, чем анализирует цифры и графики. Например, в схемах Лиц Чернова различные эмоции могут отражать уровни стресса или удовлетворенности, а цветовая палитра – интенсивность загрузки сотрудников.

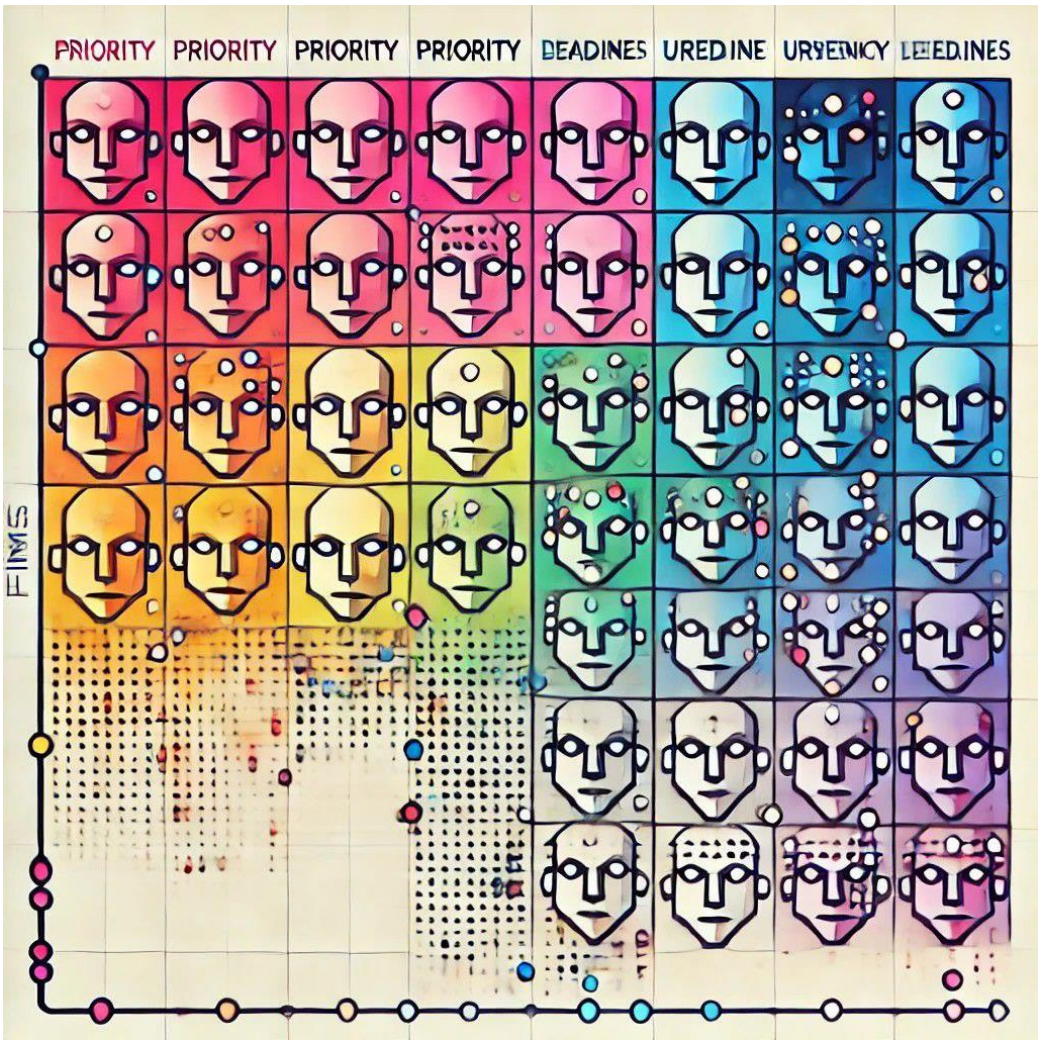


Рис. 2. Альтернативные визуальные схемы

Использование альтернативных схем представления в современных системах визуализации данных и мониторинга сотрудников позволяет по-новому воспринять объемные данные. Применение таких решений становится стандартом для компаний, стремящихся к повышению эффективности быстроты восприятия информации для сотрудников. В результате, внедрение визуальных систем учета и мониторинга способствует, упрощению этапов рабочего процесса.

Список используемых источников

1. Кузнецов В. П., Сидоров Н. А. Современные методы мониторинга сотрудников в корпоративных структурах // Журнал информационных технологий, 2022. Т. 19. № 4. С. 98–104. ISSN 2450-2341.
2. Новикова И. Н., Михайлов Д. К. Визуализация рабочих процессов и управление задачами сотрудников // Вестник технологий управления, 2021. Т. 16. № 5. С. 214–220. ISSN 2587-5665.

***Goldin I., Shiyan A*. USING VISUAL SYSTEMS FOR MONITORING PERSONNEL AND WORK PROCESSES.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This paper discusses the implementation of visual approaches to monitoring to improve staff perception of data. Special attention is paid to how such systems help to track the status of employees and increase the transparency of work processes. Issues of integration with corporate platforms, improving coordination within the team and improving productivity are also important aspects.

Key words: visual monitoring systems, system adaptability, resource optimization, forecasting and analytics, non-standard visualization schemes.

УДК 51-76
ГРНТИ 28.17.19

ВИЗУАЛИЗАЦИЯ ДАННЫХ РЕЗУЛЬТАТОВ МОДЕЛИРОВАНИЯ И АНАЛИЗА ПУЛЬСОВЫХ ВОЛН ЧЕЛОВЕКА

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

Все чаще математическое моделирование применяется для исследования работы сложных систем. К таким системам относится и кровеносная система человека. Артериальная пульсовая волна является источником информации о ее здоровье. В работе рассматриваются вопросы повышения качества визуализации результатов моделирования таких волн для оценки состояния кровеносной системы и отслеживания негативных изменений.

визуализация данных, математическое моделирование, пульсовые волны, кровеносные сосуды

В настоящее время неотъемлемой частью научных исследований различных явлений и процессов на ряду с экспериментальной деятельностью является математическое моделирование [1]. Его применяют в физике, биологии и многих других областях науки. Математическая модель позволяет описать реальный объект с помощью математических соотношений, а компьютерное моделирование дает возможность проанализировать и предсказывать работу комплексных систем в различных условиях.

Одной из таких систем является кровеносная система человека. Негативные изменения в ее состоянии в силу возраста, неправильного образа жизни и перенесенных заболеваний серьезно отражаются на здоровье и являются одной из главных причин смертности (после COVID-19) [2]. Поэтому врачи и исследователи обращают особое внимание на исследование этой системы.

Существуют различные модели для описания работы сердечно-сосудистой системы [3]. Компьютерное моделирование позволяет отразить динамику работы системы. На рис. 1 представлен пример результата визуализации моделирования, где видна сеть артериальных сосудов и наполнение кровью их на этой сети и вблизи. Однако качество визуализаций и отсутствие необходимых пояснений часто затрудняет исследователям использовать модели для своих задач.

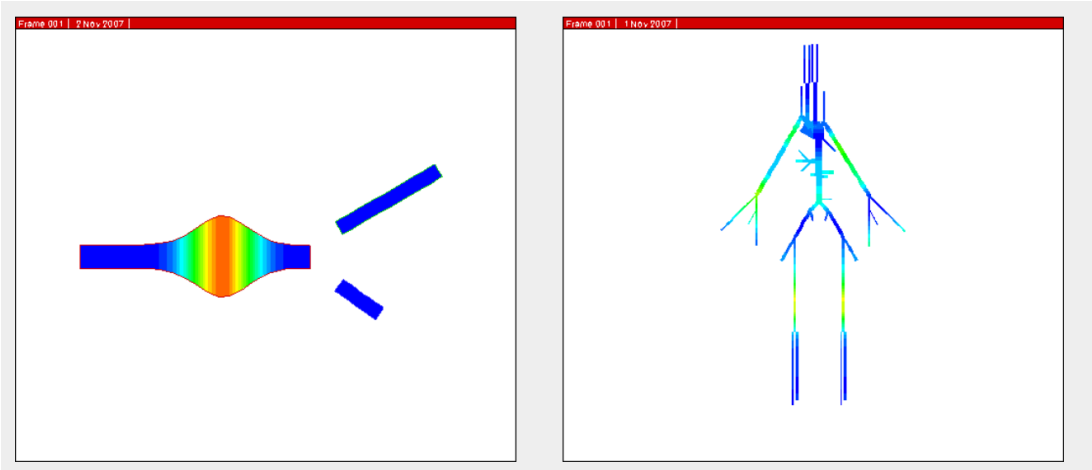


Рис. 1. Пример визуализации результатов моделирования работы кровеносной системы.

Для оценки состояния сердечно-сосудистой системы по результатам моделирования оцениваются различные величины [4, 5], из которых достаточно важной является пульсовая волна. Это распространяющаяся по артериям волна повышенного давления, вызванная выбросом крови из левого желудочка сердца в период систолы. С помощью прибора – пульсоксиметра, эту волну можно зарегистрировать в различных участках тела (чаще всего на пальце руки). Рис. 2 содержит типичную форму пульсовой волны в таком месте.

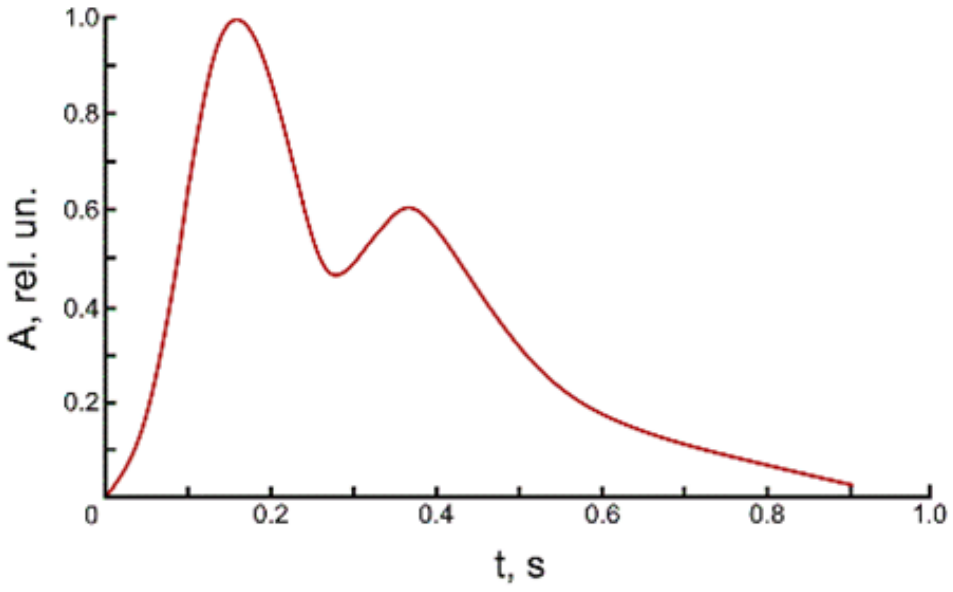


Рис. 2. Типичная форма пульсовой волны у человека, регистрируемая на пальце руки

Существуют различные программные пакеты для анализа пульсовых волн [6], однако эти средства существуют зачастую сами по себе, принимая на вход сигнал волны в дискретной форме. Осуществление анализа пульсовых волн в реальном времени и визуализация результатов моделирования позволит более ясно оценить работу кровеносной системы, а также помочь ученым

внести улучшения в математическую модель для повышения точности прогнозирования нарастания негативных изменений в ней.

Поэтому в работе рассматривается модель Nektar1D [7] на базе которой осуществляется моделирование, визуализация данных и анализ полученных пульсовых волн. Были смоделированы пульсовые волны условно здоровых людей различного возраста, проведено сравнение с датасетом от людей с отклонениями в работе сердечно-сосудистой системы и в удобной форме визуализированы результаты анализа.

Список используемых источников

1. Неймарк Ю. И. Математическое моделирование как наука и искусство: Учебник. Н. Новгород: Изд-во Нижегородского госуниверситета, 2010. 420 с.
2. Timmis A., Vardas P., Townsend N., Torbica A., Katus H., De Smedt D., Gale C. P., Maggioni A. P., Petersen S. E., Huculeci R., Kazakiewicz D., de Benito Rubio V., Ignatiuk B., Raisi-Estabragh Z., Pawlak A., Karagiannidis E., Treskes R., Gaita D., Beltrame J. F., McConnachie A. European Society of Cardiology: cardiovascular disease statistics 2021 // European Heart Journal. 2022. № 43 (8). PP. 716–799.
3. Boileau, E., Nithiarasu P., Blanco P. J., Müller L. O., Fossan F. E., Hellevik L. R., Donders W. P., Huberts W., Willemet M., Alastruey J. A benchmark study of numerical schemes for one-dimensional arterial blood flow modelling // International journal for numerical methods in biomedical engineering. 2015. № 31 (10). 10.1002/cnm.2732.
4. Vargas J. M., Bahloul M. A., Laleg-Kirati T-M. A learning-based image processing approach for pulse wave velocity estimation using spectrogram from peripheral pulse wave signals: An in silico study // Front. Physiol. 2023. № 14. 1100570
5. Alastruey J., Charlton P. H., Bikia V., Paliakaite, B. Hametner B., Bruno, R. M., Mulder M. P., Vennin S., Piskin S., Khir A. W., Guala, A. Mayer C. C., Mynard J., Hughes, A.D., Segers P., Westerhof B. E. Arterial pulse wave modeling and analysis for vascular-age studies: a review from VascAgeNet // American Journal of Physiology-Heart and Circulatory Physiology. 2023. 325 (1). H1-H29.
6. Charlton P. H., Harana J. M., Vennin S., Li Y., Chowienczyk P., Alastruey J. Modeling arterial pulse waves in healthy aging: a database for in silico evaluation of hemodynamics and pulse wave indexes // American Journal of Physiology-Heart and Circulatory Physiology. 2019. 317 (5). H1062-H1085.
7. Nektar1D: A numerical code for solving the 1-D equations of blood flow in arterial networks. URL: http://haemod.uk/nektar (дата обращения 15.11.2024).

Gromov A. **VISUALIZATION OF DATA FROM MODELING AND ANALYSIS OF HUMAN PULSE WAVES.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Mathematical modeling is increasingly used to study the operation of complex systems. The human circulatory system is one of such systems. The arterial pulse wave is a source of information about its health. The paper examines issues of improving the quality of visualization of the results of modeling such waves to assess the state of the circulatory system and track negative changes.

Key words: data visualization, mathematical modeling, pulse waves, blood vessels.

УДК 004.932.2
ГРНТИ 28.23.37

ИССЛЕДОВАНИЕ НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ ОБРАБОТКИ И АНАЛИЗА ИЗОБРАЖЕНИЙ

Е. Ю. Дорохова, Т. В. Мусаева
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С развитием технологий в области искусственного интеллекта сверточные нейронные сети стали ключевым инструментом для анализа и обработки изображений. В статье представлены принципы работы и особенности архитектуры сверточных нейронных сетей, которые широко используются для задач распознавания, сегментации и детекции, что важно для выявления и классификации дефектов. Рассмотрены особенности современных архитектур, таких как ResNet, которая решает проблемы обучения глубоких сетей, и U-Net, созданная для точной сегментации. Обзор демонстрирует возможности сверточных нейронных сетей для повышения точности и надежности производственных процессов.

нейросетевые модели, обработка изображений, анализ данных, дефекты

С развитием технологий искусственного интеллекта и машинного обучения сверточные нейронные сети стали инструментом для решения множества задач в различных отраслях.

Одним из направлений их применения является обработка изображений и анализ данных, с целью диагностики на наличие дефектов поверхностей изделий разного назначения и структуры.

Методы, рассматриваемые в статье, являются актуальными и востребованными, позволяют:

– выявлять и классифицировать дефекты;

– автоматизировать процессы диагностики и контроля качества.

Применение методов нейросетевых технологий позволит улучшить в производственных процессах такие критерии, как:

– скорость;

– точность;

безопасность.

Сверточные нейронные сети разработаны для анализа и обработки изображений. Данные сети построены на основе сверточных слоев для автоматического извлечения признаков из входных данных [1], и позволяют моделям извлекать характеристики изображения, такие как края, текстуры и формы.

Классическая архитектура сверточной нейронной сети позволяет решать задачи распознавания объектов, сегментации изображений и обнаружения дефектов, что является особенно актуально в промышленных применениях.

Сверточные нейронные сети широко используются в задачах распознавания объектов, классификации изображений, детекции и сегментации изображений. Сегментация изображения – разбиение изображения на множество покрывающих его областей. Сегментация применяется во многих областях, например, в производстве для индикации дефектов при сборке деталей [2].

У сверточных нейросетей имеется два основных типа слоев – свертка и пулинг.

Рассмотрим алгоритм работы каждого из этих слоев.

Сверточный слой, или слой свертки, – ключевой элемент, который помогает нейросети выделить только важную информацию, отфильтровав лишние детали, такие как границы, линии или фон. Данный слой предназначен для обнаружения различных признаков изображения: форм, текстур и цветов. Нейросеть на каждом уровне самостоятельно находит и оптимизирует нужные признаки для распознавания.

В основе работы сверточных слоев лежат фильтры (или ядра свертки) – матрицы небольшого размера, чаще всего 3×3 пикселя. Фильтры помогают выявлять значимые элементы, такие как края и контуры. Процесс проходит в несколько этапов:

1. Фильтр последовательно перемещается по изображению, как сканер;
2. На каждом участке значения фильтра умножаются на соответствующие значения пикселей, после чего результаты суммируются;
3. Полученная сумма записывается в новую матрицу, которая называется картой признаков;
4. Процесс повторяется для всех возможных положений фильтра на изображении.

В итоге получается карта признаков, содержащая информацию о присутствии и расположении обнаруженных элементов, что позволяет сети анализировать и распознавать изображение. Принцип работы сверточного слоя представлен на рис. 1.

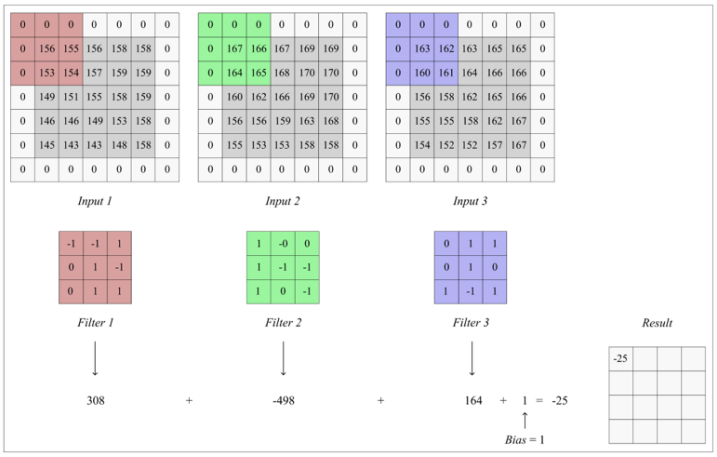


Рис. 1. Принцип работы сверточного слоя

После сверточного слоя следует пулинговый слой. Исходное изображение делится на блоки, для каждого из которых вычисляется некоторая функция. Чаще всего используется функция максимума (*max pooling*) или взвешенного среднего (*weighted average pooling*). Обучаемых параметров у данного слоя нет [3]. Основные цели пулингового слоя:

– уменьшение изображения, чтобы последующие свертки оперировали над большей областью исходного изображения;

– увеличение инвариантности выхода сети по отношению к малому переносу входа;

– ускорение вычислений.

После этого сверточный слой можно применить снова и повторить процесс несколько раз, чтобы постепенно выделять более сложные признаки изображения. Например, на первых этапах нейросеть может распознать контуры цветка, а затем – его форму и оттенки. Пример операции пулинга представлен на рис. 2.

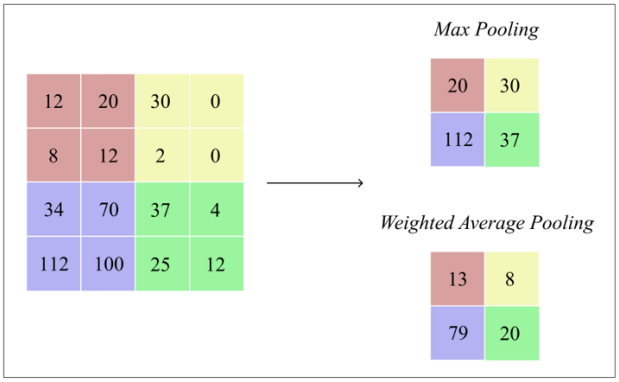


Рис. 2. Пример операции пулинга

Работу сверточных нейросетей можно сравнить со зрительным восприятием человека: сначала распознается общее, а затем, слой за слоем, частное [4].

Рассмотрим архитектуры *ResNet* и *U-Net*, с целью определения их возможностей для решения задач опознавания дефектов и диагностики.

Архитектура *ResNet* использует остаточные связи для более глубокого анализа данных, что помогает избежать эффекта затухания градиента. Архитектура использует концепцию *«skipconnections»* или *«residualconnections»*, позволяющих передавать информацию непосредственно от одного слоя к другому, минуя промежуточные слои, что позволяет обучать более глубокие сети с лучшей производительностью [5]. Это свойство позволяет применять сверточные нейросети для сложных изображений, где требуются детализированные признаки.

Архитектура *U-Net*, изначально созданная для медицинских задач, сегодня успешно применяется в дефектоскопии, где требуется точная сегментация. Благодаря своей *U*-образной форме сеть эффективно работает даже при ограниченном количестве обучающих данных, что часто бывает в промышленных условиях. Архитектура состоит из стягивающего пути для захвата контекста и симметричного расширяющегося пути, который позволяет осуществить точную локализацию [6].

Другой важный аспект сверточных нейронных сетей – возможность гибкой настройки слоев и их параметров для различных применений. Например, с помощью различных комбинаций сверточных и пулинговых слоев можно создавать модели, подходящие для обработки изображений с разными уровнями детализации.

Таким образом, сверточные нейронные сети представляют собой инструмент для автоматизации диагностики и контроля качества, обеспечивая точное и быстрое выявление и классификацию дефектов. Рассмотренные архитектуры *ResNet* и *U-Net* обладают преимуществами для решения таких задач:

– ResNet за счет остаточных связей позволяет строить глубокие сети, что делает ее пригодной для анализа сложных изображений с детализированными признаками, благодаря чему справляется с задачами, где требуется многоуровневое распознавание и точная передача информации между слоями;

– U-Net имеет высокую точность в сегментации и локализации дефектов, даже в условиях ограниченного набора данных, что делает ее подходящей для промышленности, где точное выявление дефектов является приоритетом;

– гибкость сверточных нейронных сетей позволяет адаптировать комбинации сверточных и пулинговых слоев для обработки изображений разного уровня сложности и детализации, что расширяет возможности их применения.

Список используемых источников

1. Калгина И. С. Интеллектуальные информационные системы: учеб. пособие. Чита: ЗабГУ, 2023. 123 с.

2. Обзор алгоритмов сегментации. URL:https://habr.com/ru/companies/intel/articles/266347/ (дата обращения 07.11.2024).

3. Сверточные нейронные сети. URL: https://neerc.ifmo.ru/wiki/index.php?title=Сверточные_нейронные_сети (дата обращения 07.11.2024).

4. Гайд по работе сверточных нейронных сетей. URL: https://blog.skillfactory.ru/gayd-po-rabote-svertochnyh-neyronnyh-setey/#:~:text=Сверточные % 20нейронные % 20сети % 20обычно % 20применяются,классификация % 2C % 20детекция % 20и % 20сегментация % 20изображений (дата обращения 08.11.2024).

5. Практическое применение моделей YOLO и ResNet для обнаружения нежелательных предметов на фотографиях. URL:https://habr.com/ru/articles/761200/ (дата обращения 08.11.2024).
6. U-Net: нейросеть для сегментации изображений. URL:https://neurohive.io/ru/vidy-nejrosetej/u-net-image-segmentation/ (дата обращения 08.11.2024).

***Dorokhova E., Musaeva T.* STUDY OF NEURAL NETWORK MODELS OF IMAGE PROCESSING AND ANALYSIS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

With the development of technologies in the field of artificial intelligence, convolutional neural networks have become a key tool for image analysis and processing. The paper presents the operating principles and architecture features of convolutional neural networks, which are widely used for recognition, segmentation and detection tasks, which are important for defect detection and classification. The features of modern architectures, such as ResNet, which addresses deep network training problems, and U-Net, designed for accurate segmentation, are reviewed. The review demonstrates the potential of convolutional neural networks to improve the accuracy and reliability of manufacturing processes.

Key words: neural network models, image processing, data analysis, defects.

УДК 7.036
ГРНТИ 18.11

СОВРЕМЕННОЕ ПРОЯВЛЕНИЕ ВИЗУАЛЬНЫХ ЭЛЕМЕНТОВ СТИЛЯ АР-НУВО

Е. В. Князева, А. Н. Козлова
Санкт-Петербургский государственный политехнический университет имени Петра Великого

В наше время многие дизайнеры используют визуальные элементы стиля ар-нуво в создании проектов. Стиль зародился в конце XIX века как результат обращения к различным историческим эпохам. Период ар-нуво продлился недолго, но смог сформировать основополагающие принципы, которых придерживаются сейчас. В данной статье рассматривается история возникновения, особенности визуальных элементов ар-нуво и их проявление в современной информационной среде.

стиль, ар-нуво, искусство, визуальные элементы, информационная среда

На протяжении истории человечества существовало множество художественных стилей: готика, возрождение, барокко, рококо, классицизм, ар-нуво, романтизм и другие. Авторы статьи рассматривают стиль ар-нуво, который господствовал в мире в «переломное» время конца XIX – начала XX веков. Сегодня он вызывает большой интерес, что отчасти связано с созвучностью этого периода современным процессам в обществе. На рубеже XIX – XX веков отношение к ар-нуво было противоречивым и сам период был коротким, поэтому сегодня требуется реабилитация и переоценка его роли в искусстве, культуре и, в частности, информационной среде XXI века. Также это тема эстетизации среды человека, большого внимания к женственным образам, которые занимали особое место в конце XIX – начала XX веков [1].

Стиль – это понятие, которое отражает совокупность характерных приемов, систему изобразительно-выразительных средств, единой образной системы произведения, общность формы, содержания, иконографии, мировоззрения [2]. На формирование стиля ар-нуво повлиял культурно-художественный духовный кризис рубежа столетий, вызванный потребностью в появлении нового изобразительного языка и нового стиля, пришедшего на смену классицизму. Необходимость перемены проявлялась в развитии технологий, перехода от классической типографики к модернистской и выхода Японии в мир как культурного феномена.

Художественные особенности стиля ар-нуво строятся на элементах романтизма, склонности к стилизации и обращении к смыслам символизма, а также интерпретации античности, Средневековья, Возрождения, культур Азии и Востока.

Термин «ар-нуво» впервые появился в 1880-х годах в бельгийском журнале «L`Art Moderne» и в переводе означал «новый стиль». На 80-90-е годы XIX века пришелся его рассвет, распространяясь по странам Европы, в каждой из них он имел свое название: в Англии «Модерн стайл», в Франции «Ар-нуво», в Италии «Либерти», в Германии «Югендстиль», в Австрии «Сецессион» в России «Модерн». Ар-нуво объединял самые разные сферы искусства: живопись, архитектуру, графику, скульптуру и др. Важное место среди произведений этого стиля занимали журналы. В них разрабатывали и размещали новинки книжной графики, публиковали творчество мастеров. Ярким представителем журналистики в Англии стал Обри Берсли. Во Франции в живописи, графике, плакате наибольшее влияние оказали Э. Грассе, А. Муха. В Германии в оформлении журналов участвовали такие графики немецкого модерна, как Г. Фогелер, Т. Хайне, О. Экман. В России в 1898 году в Петербурге начал выходить журнал «Мир искусства», во главе которого находились А. Бенуа и С. Дягилев (рис. 1) [2].

Рис. 1. Фронтиспис для журнала «Мир искусств», К.Сомов, 1901 г.

В работах мастеров на ряду с исключительно оптимистичными образами присутствовали циклы рождения жизни, увядания и смерти, мотивы умирания, безысходности, отчаяния. В стиле ар-нуво есть ощущение ва-саби – японской концепции, которая подчеркивает, что природа несовершенна и ее эле-

гантность и чувственность следует ценить, а не стремиться к совершенству или индустриализации. Художники хотели подчеркнуть не только декоративную сущность предмета, но и наполнить его символическим содержанием, новым смыслом.

Стилевым принципом этого периода является использование орнаментики в работах художников. В основе лежит органическая природа: животные, птицы, стебли растений и цветы, например, ирисы, цикламены, каштаны, линии, а также мотивы морской волны, лебединая шея, томные женские фигуры с распущенными волосами, плавно переходящими в орнаментальные украшения. Делается акцент на воспроизведение чувственных плавных форм, использование декоративных изогнутых линий. Контуры имеют приоритет над цветом (рис. 2) [3, 4].

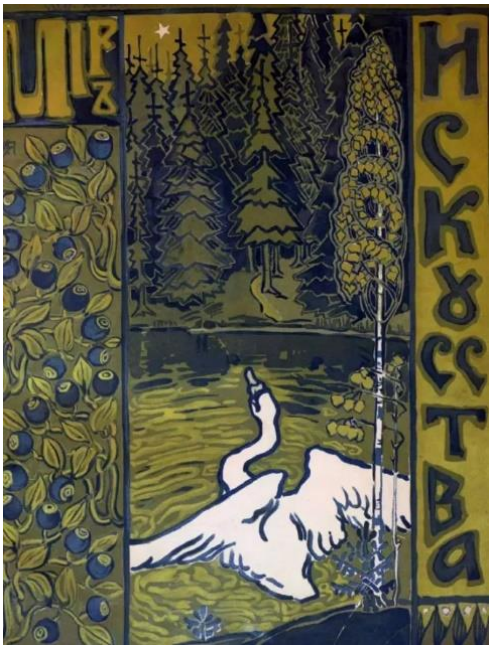


Рис. 2. Обложка журнала «Мир искусства»,
Мария Якунчикова, цветная литография, линогравюра, 1898 г.

Стилизация и плоскостность изображения стали одними из основополагающих понятий ар-нуво. Мастер фиксировал обобщенные впечатления от предмета, придавая ему новую цельность восприятия. Детали образа менялись, складывались, гиперболизировались, не теряя узнаваемости, но приобретая особую эстетизацию форм. Формообразование предметов в свою очередь имело сходство с натурой, имитируя природные объекты, в связи с чем появлялась динамика, движение и саморазвитие. Главным графическим элементом стиля ар-нуво является плавная изогнутая линия. Один из ярких примеров этой особенности – вышивка «Цикламен» или «Удар бича» Германа Обриста (рис. 3) [2].

Рис. 3. «Цикламен» («Удар бича»), Герман Обрист, вышивка, 1895 г.

В XXI веке роль стиля ар-нуво в формировании искусства и дизайна возрастает. Во многом этому способствует развитие компьютерных технологий и информационной среды. Информационная среда – это часть информационного пространства, ближайшее внешнее по отношению к индивиду информационное окружение, совокупность условий, в которых непосредственно протекает его деятельность [5].

Сегодня дизайнеры обращаются к стилю ар-нуво для придания продукту элитарности и аутентичности. Визуальные элементы, стилизация, вложение в работы смысла, стремление вызвать эмоции у зрителя является основополагающим в проектировании тех или иных предметов интерьера, одежды, печатной и цифровой продукции, которые присутствуют в информационной среде. Например, визуальные элементы используются на упаковках косметики, парфюмерии, кондитерских изделий, плакатов, афиш театров, отражая фирменный стиль. Декоративные шрифты и изогнутые формы, продолжают присутствовать в современной типографике, особенно в дизайне логотипов (рис. 4). Они помогают создать запоминающийся и элегантный образ бренда [6].

Рис. 4. Логотип для ботанического бренда Flora the Roman, S. Kitanovic

На рис. 5 представлен фрагмент сайта с иллюстрациями, выполненными в векторной графике. Сайт разработан для создания проектов по графическому дизайну, в нем использованы визуальные элементы стиля ар-нуво с различными вариантами орнаментов. Декоративность стиля ар-нуво находит проявление в современной типографике, например, при разработке шрифтов или визуальной айдентике.

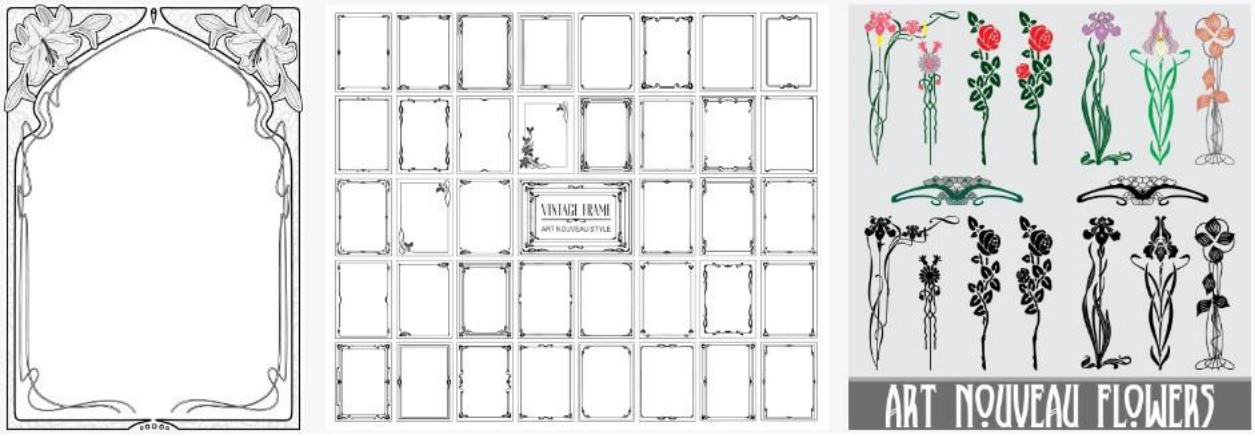


Рис. 5. Визуальные элементы в стиле ар-нуво векторной графике, Vector Stock

В заключение можно сделать вывод, что, впитывая в себя отличительные черты других стилей и эпох, стиль ар-нуво обобщает эстетический опыт человечества, синтезируя художественные традиции Запада и Востока. Современное направление стиля продолжает развиваться, обогащаться новыми формами в информационной среде XXI века и проявляться в создании гармоничного утонченного и обладающего индивидуальностью продукта, образ которого остается в памяти пользователя.

Список используемых источников

1. Патрикеева М. М. Женский образ в изобразительном искусстве стиля модерн: автореф. дис. канд. культурологии: 27.12.05 / Патрикеева Марина Михайловна. СПб., 2005. 18 с.
2. Завьялова А. Н. Культурные основания стиля модерн: автореф. дис. канд. культурологии: 15.11.03 / Завьялова Анна Николаевна. СПб., 2003. 24 с.
3. Фон Арб-Кнорозок Т. Ю. Орнамент в художественной практике декоративно-прикладного искусства второй половины XIX века: автореф. дис. канд. искусствоведения: 23.09.02 / Фон Арб-Кнорозок Татьяна Юрьевна. СПб., 2002. 18 с.
4. Харди У. Путеводитель по стилю ар-нуво: пер. с англ. М.: ОАО Издательство «Радуга», 1999. 128 с.
5. Пронина Л.А. Современная информационная среда как новая форма бытия человека // Аналитика культурологии, 2005. № 2 (4). С. 135–143.
6. Субботина Н. О. Феномен искусства: модерн как источник вдохновения в современной рекламе // Альманах теоретических и прикладных исследований рекламы: электрон. науч.

журн. 2014. № 2 С. 124–135. URL: https://cyberleninka.ru/article/n/fenomen-iskusstva-modern-kak-istochnik-vdohnoveniya-v-sovremennoy-reklame/viewer (дата обращения 12.10.24).

Knyazeva E., Kozlova A. **A MODERN MANIFESTATION OF THE VISUAL ELEMENTS OF THE ART NOUVEAU STYLE.**

The Peter the Great Saint Petersburg State Polytechnic University

Nowadays, many designers use visual elements of the Art Nouveau style in creating projects. The style originated at the end of the XIX century as a result of the appeal to various historical epochs. The Art Nouveau period did not last long, but it was able to form the fundamental principles that are adhered to now. This article examines the history of the emergence, the features of the visual elements of Art Nouveau and their manifestation in the modern information environment.

Key words: style, art Nouveau, art, visual elements, information environment.

УДК 004.9
ГРНТИ 20.53.01

КАСТОМИЗАЦИЯ ИНДИВИДУАЛЬНЫХ ОБЪЕКТОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

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

Сегодня все большую популярность получают сервисы для создания индивидуальных товаров. Равно как и растет количество людей, которые желают приобрести что-то специально для себя, соответствующее их конкретным критериям и имеющее часть их собственной личности. Данная статья рассматривает понятие кастомизации индивидуальных объектов пользователя, особенности кастомизации и использование информационных систем в этой сфере.

кастомизация, информационные системы, кастомизированные продукты, производство

На данный момент в мире, когда информационные технологии стремительно развиваются, многие сферы из реальной жизни перешли в интернет-пространство, где получают свое уникальное распространение. Совместно с их развитием в интернете, также становится популярной тенденция на стремление пользователей к проявлению своей индивидуальности и индивидуализации своих объектов обладания. Каждый хочет заявить не только о своей принадлежности к определенной группе, но также о своей неповторимой и многогранной личности.

Такое направление, как кастомизация появилось относительно недавно, но приобрело достаточно большую популярность. Прежде чем перейти к разбору особенностей данной сферы, разберем сам термин подробнее.

Кастомизацией называют процесс создания продукта, который подразумевает его соответствие индивидуальным запросам и потребностям пользователя. Тишкова Е.М. в своей статье [1], считает основной задачей подобного подхода к созданию объектов – создание у потребителя ощущения уникальности работы, словно она производится только для него и удовлетворения его личных запросов. Данный способ производства эффективно повышает востребованность продукта для конкретного человека, делая из обычного продукта, эксклюзивный товар. Вовлечение покупателя в процесс создания, повышает его интерес к продукту и лояльность к производителю. Вместе с этим соответ-

ственно растет конкурентоспособность товара, за счет его значимости для единоличного покупателя.

Данный термин очень легко принять за синоним понятия персонализация, однако, исходя из данных статьи Е. А. Жолнерчик [2], стоит понимать, что персонализация – является процессом создания продукта, подходящего под потребности и желания некоторой группы, которые собраны на основе персональных данных, без участия группы непосредственно. В то время как, кастомизация предполагает, что покупатель становится полноправным участником производства чего-то абсолютно нового и созданного лично для удовлетворения его потребностей.

В современном мире кастомизация широко представлена в самых разных областях, таких как:

– полиграфия. Все чаще полиграфические объекты делаются на заказ для конкретного человека с учетом его требований и пожеланий или даже разработкой индивидуального дизайна;

– пищевая продукция. Часто может подвергаться изменениям в зависимости от особенностей потребителя, например, в ресторанах или при заказе онлайн;

– автомобили и транспорт. Покупателям предоставляется выбор в модификациях внешнего вида и функциональности их будущих авто и транспорта;

– одежда и аксессуары. Область предоставляет большой пласт для творчества и выполнения даже самых странных и необычных запросов покупателей;

– сфера электронных технологий и услуг. Кастомизация также получает большое развитие, за счет легкости кастомизации и внедрения, как массовых, так и индивидуализированных объектов;

– образовательные платформы. Нередко для достижения большей эффективности обучения, образовательные программы и учебные материалы адаптируют под отдельных учеников.

Как можно заметить, кастомизация как явление появляется в довольно широком круге областей, однако со временем, под влиянием стремления пользователей к индивидуализации, этот список будет быстро пополняться.

Кастомизация, как лишь относительно новая область развития, пришла к нам от понятия массовой кастомизации – когда имея определенный продукт для потребителя, при помощи небольших атрибутов его делают более персонализированным, но тем не менее он остается объектом потребления некоторой группы, а не конкретного человека. Для того, чтобы рассмотреть ее наиболее полно, может поспособствовать понимание нескольких важных особенностей данной сферы. В своей статье М. А. Всякий [3] как раз приводит некото-

рые из них. Проанализировав его высказывания и дополнив их, в том числе информацией из статьи Г. Л. Азоева [4], получилось выявить следующие особенности кастомизации:

1. Основной группой населения, которая прибегает к кастомизации – являются молодые взрослые от 25 до 35 лет. Это объясняется тем, что это часть населения, которая достаточно долго взаимодействует с сетью и чувствует себя уверенно не только при совершении покупок, но и при участии в процессе создания продукта. Вследствие чего способы кастомизации должны быть направлены конкретно на эту группу потребителей;

2. Необходимость сбора и обработки информации, полученной от заказчика продукта, для чего требуется развитая информационная структура связи с покупателем и система, которая способна хранить большие объемы данных, анализировать их и составлять заказы в порядке очередности, учитывая при этом особенности товара и пожелания заказчика;

3. Производство самого продукта. Сложность заключается в том, что не все нынешнее производство рассчитано на выполнение специализированных заказов, а вместо этого больше направлено на создание больших партий продукта, направленного на удовлетворение большинства населения;

4. Существование нескольких типов кастомизации:

– *адаптивный тип*, предполагает массовое производство продукта, который в будущем может быть трансформирован непосредственно руками покупателя;

– *совместный тип*, используется в случаях, когда пользователь может испытывать трудности в самостоятельном выборе необходимых ему вариантов, тогда внедряется возможность диалога с продавцом-производителем для нахождения идеального решения;

– *косметический тип*, применяется в ситуациях, когда на фоне общего удовлетворения продуктом заказчик не испытывает такого же удовлетворения от внешнего вида товара и желает изменить некоторые его характеристики;

– *транспарентный тип*, клиент не узнает напрямую о том, что его товары или оказываемые ему услуги индивидуальны, специально с учетом его личных предпочтений, но компания, все равно выполняет действия по индивидуализации.

5. Существование нескольких методов кастомизации, в рамках которых реализуются типы кастомизации:

– *экспертная кастомизация*, потребности покупателей предварительно прогнозируются и тщательно изучаются, а для создания продукта, удо-

влетворяющего желания узкой группы пользователей, заранее определяется степень его индивидуализации;

– *модульная кастомизация*, предполагает создания некоторого количества компонентов, из которых состоит продукт и которые пользователь может самостоятельно выбрать;

– *смешанная кастомизация*, является слиянием двух вышеперечисленных методов, когда некоторые характеристики продукта выделяются и для индивидуализации самим производителем, а другие выбираются клиентом самостоятельно;

– *внешняя кастомизация*, представляет собой минимальные внешние изменения продукта, такие как изменение цвета или упаковки.

Как упоминалось ранее, особую роль в кастомизации сейчас играет развитие электронных технологий и услуг, а также необходимость сбора и обработки информации от заказчика. Именно с такими задачами способны стравится информационные системы, они способны анализировать большие объемы информации о предпочтениях пользователей.

Так, Г. Л. Азоев, в своей статье [4] о технологиях кастомизации, упоминает два способа привлечения информационных систем в процесс кастомизации:

– создание программного обеспечения или модулей информационной системы, которые будут выступать в роли конфигуратора продукта. При помощи них пользователь самостоятельно сможет принять решения о модификации продукта, настраивать его характеристики и увидеть результат еще до непосредственного создания товара и не прибегая к помощи компании-производителя;

– создание программного обеспечения для связи между клиентом и производителем, где они смогут совместно делать выводы и принимать решения о персонализации продукта.

Помимо этого, существует еще способ внедрения информационных систем в сферу кастомизации, а именно использование их способности к повышению эффективности и популярности услуги не только крупных производств, но и индивидуальных предпринимателей. Так при помощи интернета и социальных сетей они могут продуктивно заниматься поиском аудитории, которая была бы заинтересована в их работе, а также идей и материалов для будущих проектов.

Также информационные системы могут расширять возможности функциональности, например, при помощи подключения сторонних сервисов (сервисы оплаты, управления данными, сотрудничество с поставщиками) и добавления новых плагинов и модулей для удовлетворения специфических требо-

ваний заказчика. Отдельным преимуществом использования информационных систем является их способность к созданию и настройке пользовательских интерфейсов и возможность персонализации контента и рекомендаций. При использовании подобных интерфейсов, каждый пользователь может адаптировать систему под себя, а индивидуально собранная система рекомендаций подскажет какие товары в теории захотел бы приобрести покупатель.

В заключение, хотелось бы снова упомянуть, что кастомизация – термин, пришедший от массовой кастомизации, но значащий для отдельного человека намного больше, чем для группы потребителей. В рамках производства она позволяет из товаров, в которых нуждаются большие группы людей, создавать уникальные решения, ориентированные на пожелания конкретного заказчика. Это может выделить компанию среди конкурентов, помочь в привлечении внимания новых клиентов и выстраивания позитивных эмоциональных связей как с индивидуальным предметом обладания, так и с компанией-производителем. Однако стоит помнить об особенностях внедрения кастомизации в производство, а также особую роль информационных систем в организации процесса кастомизации от взаимодействия с потребителем до создания и распространения продукта. В общем, можно сделать вывод, что кастомизация является очень перспективным в развитии направлением и в скором времени начнет приобретать все большую популярность в разнообразных сферах производства.

Список используемых источников

1. Тишкова Е. М., Страукас Я. С. Эволюция и сущность процесса кастомизации // Аллея науки, 2017. Т. 5, № 16. С. 615–620.
2. Бизнес. Образование. Экономика: Междунар. науч.-практ. конф., Минск, 7–8 апр. 2022 г. : сб. ст. / редкол.: В. В. Манкевич [и др.]. Минск: Институт бизнеса БГУ, 2022. С. 261–264.
3. Всякий М. А., Стрижанов И. А. Особенности организации кастомизированного производства // ЭКОНОМИНФО. 2011. №15. URL: https://cyberleninka.ru/article/n/osobennosti-organizatsii-kastomizirovannogo-proizvodstva (дата обращения 14.11.2024).
4. Азоев, Г. Л. Технологии кастомизации / Г. Л. Азоев, В. С. Старостин // Маркетинг. 2013. № 1 (128). С. 86-102. EDN RWXLYR.

Marushina M. CUSTOMIZATION OF INDIVIDUAL OBJECTS IN INFORMATION SYSTEMS.

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Today, services for creating individual products are becoming increasingly popular. Just as the number of people who want to buy something specifically for themselves, corresponding to their specific criteria and having a part of their own personality, is growing. This article examines the concept of customization of individual user objects, the features of customization and the use of information systems in this area.

Key words: customization, information systems, customized products, production.

УДК 004.946
ГРНТИ 28.17.33

ПРОБЛЕМЫ И МЕТОД ВОССТАНОВЛЕНИЯ 3D-МОДЕЛИ РАЗРУШЕННОГО ЗДАНИЯ

Т. В. Мусаева, П. А. Никифоров
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время значимым является вопрос восстановления утраченных объектов исторического культурного наследия, в том числе и в виртуальном цифровом 3D формате. В данной статье рассматриваются существующие проблемы, методы их воспроизведения в виртуальном пространстве. На основе анализа и сделанных выводов предлагается метод, который позволит значительно улучшить точность и качество 3D-моделей разрушенных зданий, несмотря на ограниченность исходных данных.

3D-моделирование, фотограмметрия, цифровая реставрация, машинное обучение, историческая архитектура, визуализация, текстурирование, объекты культурного наследия, виртуальная реальность

В соответствии с законом РФ N 73-ФЗ 25 июня 2002 года объекты культурного наследия (памятники истории и культуры) народов Российской Федерации представляют собой уникальную ценность для всего многонационального народа Российской Федерации и являются неотъемлемой частью всемирного культурного наследия. В Российской Федерации гарантируется сохранность объектов культурного наследия (памятников истории и культуры) народов Российской Федерации в интересах настоящего и будущего поколений многонационального народа Российской Федерации [1].

В соответствии с данными Всероссийского общества охраны памятников истории и культуры «ежегодные утраты составляют 150-200 памятников» [2].

Цель исследования в рамках статьи – выявление ключевых проблем при реконструкции 3D-моделей разрушенных зданий и разработка методологии, повышающей качество воспроизведения в виртуальном пространстве.

При воссоздании цифровой 3D-модели разрушенного здания на основе старых фотографий возникает ряд сложных проблем, требующих комплексного подхода и использования самых современных технологий.

К таким проблемам относятся: формат исходных данных, нехватка ракурсов, нехватка данных о масштабах и пропорциях здания, сложность передачи текстуры и материалов, разрушение и утрата отдельных частей строения.

Старые фотографии (далее – фотографии), часто единственные доступные визуальные материалы, могут быть низкого качества, с нечеткими дета-

лями и искажениями из-за технических ограничений прошлых камер, что делает практически неразличимыми важные архитектурные элементы, такие как декоративные украшения фасадов, текстуры и отделка. Эти детали играют важную роль в создании исторически точной модели, так как именно они придают зданию уникальность и узнаваемость.

Фотографии чаще всего запечатлевают только фасад здания или его наиболее привлекательные стороны, оставляя другие стороны здания вне кадра. Это приводит к тому, что архитектурные особенности задних и боковых фасадов, внутренние дворы и другие скрытые зоны остаются неизвестными. В случае разрушенного здания такие пробелы невозможно восполнить фотографиями самого объекта, поэтому художнику приходится восстанавливать утраченные детали по аналогичным зданиям того же периода или реконструировать их, основываясь на исторических описаниях. Это, в свою очередь, создает риск внесения в модель элементов, не соответствующих оригинальному проекту, что снижает историческую точность.

Изображения на фотографиях редко содержат масштабные ориентиры или какие-либо измерения, что затрудняет восстановление точных размеров. Восстановление пропорций становится возможным только через трудоемкий анализ масштабирующих элементов, если их размеры известны. Перспективные искажения на старых фотографиях усложняют процесс создания достоверной геометрии, так как для исправления таких ошибок требуются специализированные методы, такие как фотограмметрия.

Здания исторических периодов, как правило, использовали определенные строительные материалы (текстуру), которые сложно воспроизвести без доступа к исходным текстурам. На фотографиях текстуры материалов зачастую плохо различимы, что делает их точное воспроизведение трудной задачей. Это особенно актуально, когда речь идет о выцветших поверхностях, повреждениях от времени или мелких элементах декора.

Также существуют сложности, связанные с разрушенными и утраченными частями здания. Разрушенные конструкции могут иметь значительные деформации, и их исходная форма часто бывает неопределенной. В таких случаях приходится принимать решения на основе симметрии здания или искать схожие архитектурные объекты для ориентировки. Также, каждый элемент здания может обладать уникальными особенностями, характерными только для данного сооружения, что затрудняет точную реконструкцию.

В воссоздании разрушенного здания важны знания и навыки в различных областях – от архитектуры и истории до цифровой обработки изображений. Без комплексного подхода, который включает методы фотограмметрии, цифровой реставрации и использование нейросетей для улучшения качества изображений, точно воспроизвести здание практически невозможно.

Методология воссоздания 3D-модели разрушенного здания на основе старых фотографий основывается на использовании современных технологий – фотограмметрия, машинное обучение, анализ аналогичных архитектурных объектов.

Первый шаг в процессе – это сбор всех доступных материалов, включая фотографии, чертежи, карты и архивные документы, больше различных видов изображений для компенсирования возможных недостающих ракурсов и деталей. Затем тщательный анализ этих изображений для выявления перспективных искажений, пропорций и видимых архитектурных элементов, выявления возможных недостатков данных, выделения отдельных частей строения, которые будут нуждаться в реконструкции на основе аналогичных объектов.

Далее, следует этап восстановления масштаба и пропорций здания. Часто фотографии не содержат масштабных ориентиров, для этого используются известные размеры элементов (например, окно). Фотограмметрия на основе нескольких изображений помогает точно восстанавливать геометрию здания и исправлять перспективные искажения, что является важным шагом для получения точных пропорций. С помощью этого метода создаются трехмерные точки и пространственные координаты, которые помогают воссоздать объем здания, даже если исходные фотографии были сделаны под различными углами.

На следующем этапе происходит моделирование. Сначала создается базовая структура здания, используя полученные размеры и координаты. Эта модель представляет собой «черновой» вариант, который позже уточняется и детализируется. Здесь важно работать с крупными архитектурными блоками, такими как стены, крыша и основные колонны. В дальнейшем добавляются более мелкие элементы, такие как окна, двери, карнизы и другие архитектурные украшения. Если информация о некоторых деталях отсутствует или недостаточно точна, используется анализ аналогичных зданий той же эпохи и стиля, что помогает восполнить недостающие элементы.

Реконструкция разрушенных частей здания представляет собой одну из самых сложных задач, поскольку восстановление утраченных элементов требует знания архитектурных особенностей и структуры подобных объектов. В этом случае, следует полагаться на симметрию оставшихся частей здания или применить элементы, характерные для аналогичных сооружений того времени. В случае, если разрушенные части не могут быть точно воссозданы, используются исторические и архитектурные гипотезы, которые могут предложить специалисты в этой области.

Создание текстур и материалов – это следующий важный этап. Воссоздание материалов, таких как, например, камень, основано на исследовании внешнего вида строительных материалов, используемых в здании. Если фотографии не предоставляют достаточно четких текстур, применяется технология

машинного обучения, например, нейросети для улучшения разрешения старых фотографий, что позволяет выявить больше деталей, а также для генерации текстур, близких к оригинальным. Процесс создания текстур включает в себя не только их визуальное воспроизведение, но и настройку их состояния, например, износа или повреждений, что придает зданию аутентичность.

Важное значение имеет историческая точности модели, правильное воспроизведение архитектурных элементов, сохранение атмосферы здания.

В заключение, на финальном этапе проводится верификация модели и ее тестирование. Это может включать в себя проверки на точность масштаба, а также проекцию модели с тех же ракурсов, что и на фотографиях, для оценки ее соответствия оригиналу. Этот этап также включает консультации с экспертами для дополнительной проверки исторической достоверности и корректности воссоздания элементов. Модель, после проверки и уточнений, может быть использована для дальнейших исследований, образовательных целей или интеграции в виртуальную реальность для сохранения культурного наследия.

Предложенный метод позволит значительно улучшить точность и качество 3D-моделей разрушенных зданий, несмотря на ограничения исходных данных. Использование фотограмметрии способствует корректировке перспективных искажений и восстановлению пропорций на основе доступных фотографий, а анализ аналогичных зданий помогает восполнить недостающие архитектурные элементы. Применение технологий машинного обучения для улучшения разрешения изображений и генерации текстур повышает детализацию и историческую достоверность модели.

Список используемых источников

1. Федеральный закон об объектах культурного наследия народов российской федерации. https://www.consultant.ru/document/cons_doc_LAW_37318/ (дата обращения 04.12.2024).
2. Всероссийское общество охраны памятников истории и культуры https://voopik.ru/our-heritage/status-cultural-heritage/ (дата обращения 04.12.2024).
3. Меженин А. В. Технологии разработки 3D-моделей. Университет ИТМО. 2018.
4. Сергеева В. С. Проблемы применения методов 3d-моделирования и 3d-печати в науке и производстве. Нижегородский Государственный педагогический университет имени Козьмы Минина. 2021.

Musaeva T., Nikiforov P. **PROBLEMS AND METHOD OF RESTORATION OF A DESTROYED BUILDING IN A 3D MODEL.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Currently, the issue of restoring lost objects of historical cultural heritage, including in digital 3D format, is significant.
This article discusses the problems and methods for solving them in virtual space. Based on the analysis, conclusions are drawn. This method allows for a significant increase in the accuracy and quality of 3D models of destroyed buildings, despite the limited initial data.

Key words: 3D modeling, photogrammetry, digital restoration, machine learning, historical architecture, visualization, texturing, cultural heritage, virtual reality.

УДК 004.42
ГРНТИ 28.17.23

СИСТЕМЫ УПРАВЛЕНИЯ МОДУЛЕЙ ПОДВИЖНОСТИ НА ОСНОВЕ ПЛАТФОРМЫ СТЮАРТА

Т. В. Мусаева, К. К. Рамзаев
Санкт-Петербургский государственный университет телекоммуникаций им проф. М. А. Бонч-Бруевича

Платформа Стюарта, или гексапод, представляет собой механизм с шестью степенями свободы, который широко применяется в авиационных и автомобильных тренажерах, военных симуляторах и индустрии развлечений. Программное обеспечение для управления такими платформами существенно упрощает настройку и управление симуляцией для пользователя, обеспечивая интуитивный интерфейс и доступ к настройкам, позволяющим гибко адаптировать параметры движений.

В статье рассматриваются существующие решения для управления платформой Стюарта, а также анализируются их особенности. Внимание уделено программным продуктам лидеров рынка, таких как «ForceSeatPM» от компании «Motion Systems», ПО «SimTools» и ПО «Brunner». Также уделено внимание перспективам разработки веб-ориентированных интерфейсов, которые могут повысить удобство работы, кроссплатформенность и доступность подобных решений для широкой аудитории.

платформа Стюарта, гексапод, программное обеспечение управления, настройка симуляции, «ForceSeatPM», «Brunner», пользовательский интерфейс, веб-интерфейсы

Платформа Стюарта находит применение в различных областях, включая тренажеры для авиации, автомобилестроения, военных симуляторов, а также в индустрии развлечений. Эффективное управление движением платформы требует специализированного программного обеспечения, обеспечивающего точный контроль и настройку различных параметров.

Пользовательский интерфейс – важная часть программного обеспечения для управления платформами Стюарта.

Для успешного использования таких программ требуются следующие ключевые элементы интерфейса:

– основной экран управления – отображает основные показатели системы, такие как положение платформы, угол наклона и текущие настройки, что позволяет пользователю легко отслеживать состояние симуляции;

– инструменты диагностики и контроля состояния – включают в себя возможность проверки состояния платформы, отслеживание ошибок, а также доступ к журналу ошибок и уведомлений;

– модули настройки движения – интерфейс для настройки параметров движений платформы, включая амплитуду, скорость и плавность движения;

– настройки и калибровка – позволяют калибровать систему под конкретные требования симуляции или условия эксплуатации. Для этого предусмотрены такие функции, как настройка вибрации, коррекция углов наклона и калибровка положения.

Существующие решения для управления платформой Стюарта

1. «ForceSeatPM» от компании «Motion Systems»

«ForceSeatPM» – это специализированное программное обеспечение, разработанное компанией «Motion Systems», предназначенное для управления движением платформ типа гексапод. Этот софт используется для ряда моделей платформ, таких как PS-6TM-150 и PS-6TM-550.

«ForceSeatPM» обеспечивает комплексную систему настройки и диагностики, включающую следующие функции:

– диагностика платформы – отслеживание технического состояния платформы в реальном времени;

– конфигурация компенсации движения – позволяет подстроить движения под конкретные требования симуляции, уменьшая вибрации и улучшая плавность работы;

– настройка подключения и интеграция с играми – ПО поддерживает настройку подключения для совместимости с симуляционными играми и тренажерами;

– кинематический анализ – позволяет точно рассчитывать движение платформы, основываясь на текущем положении и желаемом результате.

«ForceSeatPM» совместимо исключительно с платформами от «Motion Systems» и имеет интуитивно понятный интерфейс, предназначенный для специалистов и пользователей, знакомых с основными принципами работы платформы. Программное обеспечение активно используется в тренажерах для авиации, автомобильных симуляторах и развлекательных системах [1].

2. Программное обеспечение от компании «Brunner»

Компания «Brunner» разработала собственное ПО для управления платформами гексапод, например, для модели 6DOF Motion 1000. В отличие от «ForceSeatPM», ПО от «Brunner» ориентировано на гибкость и более широкий спектр настройки движений, что делает его востребованным в симуляторах

военного назначения, автомобильных и авиационных тренажерах, а также в тестовых лабораториях.

Основные характеристики этого ПО:

– настройка кинематических параметров – позволяет пользователям настраивать параметры движения для конкретных условий симуляции;

– опции индивидуализации – пользователи могут адаптировать движения в зависимости от массы и положения симуляционного объекта;

– интеграция с различными платформами – ПО от «Brunner» поддерживает множество типов тренажеров, что делает его универсальным решением.

Пользовательский интерфейс ПО от «Brunner» включает функциональные элементы для точной настройки параметров движения и интуитивно понятное меню для управления и диагностики системы [2].

3. Motion for SimTools

«SimTools» – это программный пакет, который позволяет настраивать и управлять движением платформ Стюарта в реальном времени, особенно в симуляторах для гоночных игр и авиасимуляторов. Он поддерживает широкий спектр симуляторов и игр, а также позволяет интегрировать пользовательские параметры движения.

Основные функции:

– Motion for SimTools позволяет пользователю создавать уникальные профили для разных типов симуляторов, таких как автомобильные гонки или полеты. Профили можно изменять в зависимости от интенсивности и скорости движений;

– ПО имеет интеграцию с VR-шлемами, что усиливает эффект погружения, корректируя движения платформы в зависимости от положения пользователя в виртуальном пространстве;

– ПО предоставляет гибкие инструменты для управления амплитудой и скоростью движения, что позволяет создавать реалистичную симуляцию перегрузок.

«SimTools» является примером интуитивного интерфейса с широкими возможностями настройки, что делает его удобным для использования как в любительских, так и профессиональных симуляторах [3].

Современные решения для управления платформой Стюарта включают в себя широкий спектр программных продуктов с разнообразными возможностями настройки и управления. «ForceSeatPM», ПО от «SimTools» и ПО от «Brunner» представляют собой заметные примеры программного обеспечения, предоставляющего пользователям интуитивные интерфейсы и мощные

инструменты для настройки движения. Проанализировав существующие решения, можно сделать вывод, что внедрение веб-приложений в данную область способно еще больше расширить функциональность и удобство таких систем, обеспечивая гибкость и кроссплатформенность. Это, в свою очередь, позволит разрабатывать отечественные симуляторы с конкурентоспособными возможностями.

Веб-приложения представляют собой современное решение для управления тренажерами, основанными на платформе Стюарта. Основные преимущества веб-приложений:

1. Кроссплатформенность – пользователи могут получить доступ к ПО из любого браузера, что устраняет зависимость от операционной системы и повышает доступность;
2. Быстродействие и обновляемость – веб-приложения легко обновляются, что позволяет оперативно добавлять новые функции и исправлять ошибки;
3. Расширенные возможности интерфейса – в веб-приложениях можно интегрировать сложные графические элементы и адаптивные панели для улучшения визуализации данных [4].

Список используемых источников

1. MotionSystems: сайт. URL: https://motionsystems.pl/ (дата обращения 5.11.2024)
2. BRUNNER: сайт. URL: https://www.brunner-innovation.swiss (дата обращения 5.11.2024)
3. SimTools: сайт. URL: https://simtools.us/ (дата обращения 5.11.2024)
4. Рамзаев К. К., Мусаева Т. В. Модуль подвижности на основе платформы Стюарта // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. Том 2. С. 501–505

Musayeva T., Ramzaev K. **MOBILITY MODULE CONTROL SYSTEMS BASED ON THE STEWART PLATFORM.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The Stewart platform, or hexapod, is a six-degree-of-freedom mechanism that is widely used in aviation and automotive simulators, military simulators, and the entertainment industry. The software for managing such platforms greatly simplifies the setup and management of the simulation for the user, providing an intuitive interface and access to settings that allow flexible adaptation of motion parameters. The article examines the existing solutions for managing the Stewart platform, as well as analyzes their features. Attention is paid to software products of market leaders such as "ForceSeatPM" from Motion Systems, SimTools software and Brunner software. Attention is also paid to the prospects of developing web-oriented interfaces that can improve the usability, cross-platform compatibility and accessibility of such solutions to a wide audience.

Key words: Stewart platform, hexapod, control software, simulation setup, "ForceSeatPM", "Brunner", user interface, Web interfaces.

УДК 005.92
ГРНТИ 20.17.17

СИСТЕМА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРТА НА BLOCKCHAIN

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

В настоящее время системы электронного документооборота становятся все более актуальнее благодаря оптимизации внутренних процессов компаний. Цифровая документация проще поддается анализу и обработке, что приводит к экономии ресурсов и времени. Электронные системы удобны в эксплуатации, позволяя получать доступ к файлам дистанционно. Мы предлагаем применять технологию блокчейн для управления документооборотом, гарантируя безопасность, прозрачность и эффективность – эти качества делают ее подходящим инструментом для решения различных задач.

система, электронный документооборот, blockchain, защита

Блокчейн представляет собой непрерывно цепочку блоков, организованных по определенным правилам и содержащих информацию [1]. Эта технология находит применение во многих сферах благодаря тому, что она позволяет перейти от централизованной системы учета данных к децентрализованной, обеспечивающей безопасность, целостность и конфиденциальность хранения информации [2].

Блокчейн – это не только криптовалюта и не только ISEO – международная поисковая система оптимизации. Технология блокчейн используется в широком смысле для обеспечения безопасности хранения, использования, извлечения и фиксации любого рода информации. Blockchain – это цепочка блоков, которую мы встраиваем в документооборот для защиты информации. В этой цепочке выдерживается строгая последовательность.

Использование этой технологии исключает возможность скрытых манипуляций, а также будет видно все изменения в реестре. Было принято решение создать отдельные цепочки блокчейнов для каждого документа в документообороте, чтобы обеспечить максимальную изоляцию данных и избежать проблемы с масштабируемостью. Новые документы добавляются в систему как независимые блокчейны.

Идентификаторы строк в базе данных – это уникальное значение, которое присваивается каждой строке таблицы, для ее идентификации. Идентификаторы строк играют важнейшую роль в обеспечении уникальности и точного учета документов. Они представляют собой уникальные значения, которые

присваиваются каждой записи, связанной с документом, для ее однозначной идентификации. Это позволяет эффективно управлять информацией в сложных системах, где большое количество документов требует строгой структуризации.

В документообороте идентификаторы строк позволяют избежать путаницы между документами, даже если у них схожие атрибуты, такие как названия, авторы или даты создания. Например, если система хранит версии одного и того же документа, уникальный идентификатор каждой версии помогает точно определить, какая из них является актуальной или связана с конкретным процессом.

Идентификаторы также используются для создания связей между документами и их атрибутами. Благодаря уникальным идентификаторам такие связи становятся прозрачными и управляемыми, что упрощает поиск информации и обработку документов в рамках рабочих процессов. Кроме того, идентификаторы строк играют ключевую роль в масштабируемости документооборота. В системах с большим объемом данных они позволяют эффективно индексировать документы, ускоряя операции поиска, фильтрации и обработки. Это особенно актуально для организаций, где документооборот включает десятки тысяч записей, распределенных по разным отделам или филиалам.

Таким образом, в системах документооборота идентификаторы строк обеспечивают уникальность записей, упрощают управление связями между данными, способствуют сохранению целостности и прозрачности информации, а также поддерживают эффективную работу с большими объемами документов.

Такие идентификаторы позволяют эффективно управлять данными и упрощать поиск информации. Современные базы данных используют идентификаторы строк, которые можно упорядочить по времени внесения записей. В системе у каждого документа имеется два вида идентификаторов:

Внутренний идентификатор создается на основе timestamp. Timestamp это числовое значение, которое фиксирует конкретный момент времени, выраженный в секундах. Использование timestamp решает множество проблем, связанных с фиксацией, обработкой, анализом данных, а также идентификацией и формированием цепочки.

Внешний идентификатор предназначен для идентификации документов в общедоступных источниках.

Поскольку основной принцип работы блокчейна заключается в строгом контроле изменений и сохранении целостности данных, включение всех возможных атрибутов при построении каждого звена цепочки обеспечивает максимальную надежность структуры. Такой подход позволяет наиболее точно

отражать состояние всей цепи, сохраняя ее прозрачность и непротиворечивость. В базовой реализации предложено преобразовывать каждый атрибут в строку и объединять их в одну общую строку, что упрощает процесс создания уникальных хэш-сумм.

Использование конкатенации строк как основы для формирования хэшей предоставляет дополнительные возможности для защиты данных. Ключевым моментом является порядок объединения строк, регистр символов, а также использование разделителей. Эти факторы обеспечивают уникальность и стабильность результата. Любое изменение в исходной строке немедленно отражается на хэш-сумме, делая любую попытку несанкционированного изменения данных легко обнаруживаемой. Для этого в системе предусмотрен отдельный атрибут в реестре документов, где хранятся рассчитанные хэш-суммы. Однако из-за хаотичной структуры хранения записей в базе данных сами по себе хэш-суммы теряют смысл без строгой сортировки. Особое место в цепочке занимает "генезис-блок", первая запись, не содержащая хэш-суммы. Именно этот блок служит отправной точкой для всей структуры блокчейна, задавая стандарт для последующих блоков. Это позволяет избежать разночтений при обработке данных и упрощает первичную настройку системы.

В предлагаемом подходе к формированию цепочки данные, используемые для расчета хэш-суммы, формируются на основе следующих правил: в качестве разделителя строк используется точка с запятой, порядок объединения атрибутов соответствует их расположению в реестре, а исходный регистр строк сохраняется. Эти правила позволяют поддерживать последовательность и стабильность цепочки. Дополнительно возможно использование временных меток (timestamp) для записи времени создания блока. Это делает цепочку не только защищенной, но и позволяет фиксировать порядок внесения изменений, что важно для аудита.

При добавлении нового документа алгоритм проверяет существующую цепочку и формирует новое звено. Это решение эффективно, так как позволяет за один проход по реестру как проверить целостность, так и создать хэш нового блока. Генезис-блок рассчитывает свою хэш-сумму без учета предыдущих звеньев, так как они отсутствуют. Для всех последующих звеньев алгоритм сравнивает рассчитанные хэши с хэшами предыдущих блоков. Если соответствие найдено, хэш текущего блока сохраняется в атрибуте нового звена. В случае, если хэш текущего блока не совпадает с ожидаемым, возвращается пустое значение и внутренний идентификатор документа, который не прошел проверку. Это позволяет оперативно выявлять и устранять проблемы, сохраняя целостность всей цепочки.

Таким образом, предложенная система эффективно поддерживает целостность блокчейна, оперативно выявляет любые нарушения, предотвращает

их распространение и предоставляет дополнительные возможности для анализа и защиты данных. Это делает ее универсальным инструментом для работы с документами в условиях повышенных требований к безопасности (рисунок 1).

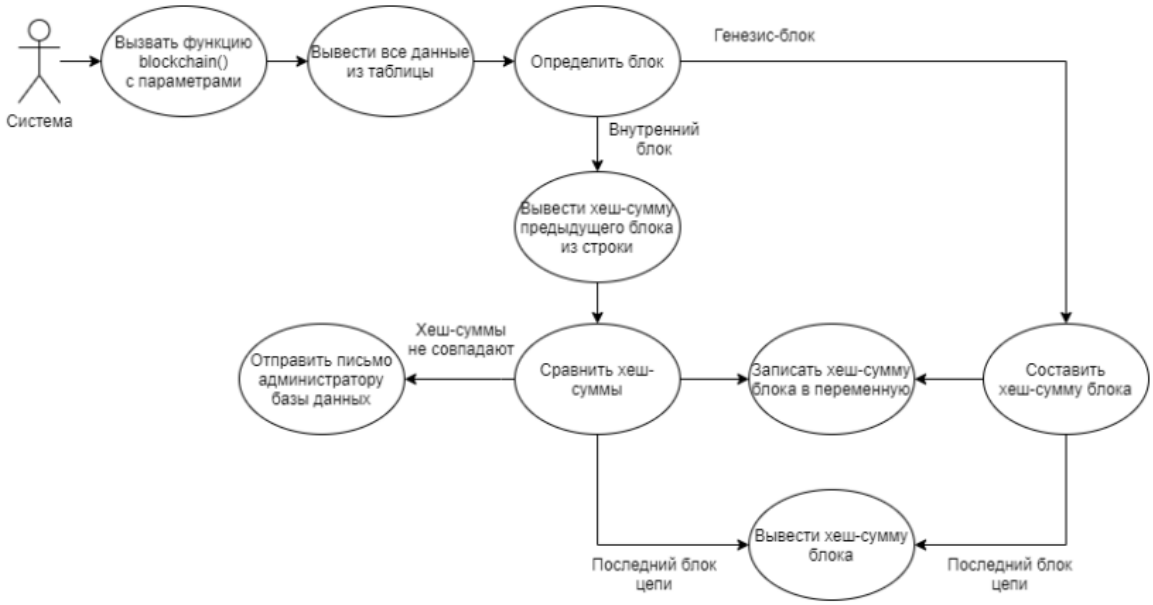


Рис. 1. Диаграмма принципа Blockchain’а в системе документооборота

В заключение можно сказать, что использование блокчейна для системы документооборота позволяет сделать ее более надежной и безопасной. Блокчейн защищает документы от подделки благодаря своей уникальной структуре. В настоящее время мы разрабатывает систему электронного документооборота на основе blockchain технологии, которая имеет функции визуализации статусов документов посредствам их динамической кодификации.

Список используемых источников

1. Пескова О. Ю., Половко И. Ю., Захарченко А. Д. Применение блокчейн-технологий в системах электронного документооборота: анализ и программная реализация // Инженерный вестник Дона. №3. 2019. URL: http://ivdon.ru/ru/magazine/archive/n3y2019/5801
2. Лелу Л. Блокчейн от А до Я: все технологии десятилетия. М.: Бомбора, 2018. 249 с.

***Shirokov A., Shiyan A.* ELECTRONIC DOCUMENT MANAGEMENT SYSTEM ON THE BLOCKCHAIN.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Currently, the electronic document management system is becoming more and more relevant. This is due to the optimization of processes within organizations. Digital documents are easier to analyze and process, which can save money and time. Electronic document management is easy to use, allows you to access documents from anywhere in the world. We propose using blockchain technology for document management, ensuring security, transparency and cost–effectiveness - all this makes it an urgent solution for modern business tasks and government services.

Key words: system, electronic document management, blockchain, protection.

3.3. Программная инженерия

УДК 004.896
ГРНТИ 49.33.29

АНАЛИЗ ТЕХНИК ПРЕДСКАЗАНИЯ КАДРОВ ДЛЯ УМЕНЬШЕНИЯ ЗАДЕРЖКИ В СПУТНИКОВЫХ КАНАЛАХ СВЯЗИ ДЛЯ ПОТОКОВОЙ ПЕРЕДАЧИ ВИДЕО

А. А. Березкин, Ф. Х. До, Р. В. Киричек
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В системах спутниковой связи задержка является серьезной проблемой, особенно для таких приложений, как потоковая передача видео, которые требуют быстрой передачи данных и четких изображений. Алгоритмы предсказания кадров предлагают эффективное решение, снижая необходимость в передаче данных в реальном времени и позволяя предсказывать кадры для уменьшения задержки. Основными темами данного обзора и сравнительного анализа методов предсказания кадров являются рекуррентные нейронные сети (RNN), генеративные состязательные сети (GAN) и модели диффузии. Для оценки этих моделей используются такие метрики, как обученное перцептивное сходство изображений (LPIPS), пиковое отношение сигнал/шум (PSNR) и индекс структурного сходства (SSIM). Наши результаты демонстрируют преимущества и недостатки каждой модели с точки зрения снижения задержки при сохранении качества изображения.

задержка, спутниковые системы связи, предсказание кадров, генеративные состязательные сети, диффузионные модели

Введение

В системах спутниковой связи задержка является серьезной проблемой, особенно при потоковой передаче видео. Качество видео страдает из-за длительных времен передачи сигнала, вызванных большим расстоянием между спутниками и наземными станциями. Каждая секунда задержки имеет критическое значение в этих приложениях для обеспечения стабильной передачи видео.

Одним из способов снижения задержки является использование техник предсказания кадров. Эти методы, используя текущие кадры для предсказания следующих, минимизируют задержку и объем данных, которые необходимо передать, при этом сохраняя хорошее качество изображения. В данной работе

рассматривается эффективность различных техник предсказания кадров, таких как RNN [1], GAN и модели диффузии [2], с использованием метрик SSIM, PSNR и LPIPS. Целью является оценка преимуществ и недостатков моделей для определения того, какие из них лучше всего подходят для снижения задержки без потери качества изображения в системах спутниковой связи.

Обзор процесса предсказания кадров

Полный процесс предсказания, от ввода видео до предсказания кадров, передачи через спутниковые каналы связи и конечного отображения пользователю, показан на рисунке 1. Сначала модель получает исходные кадры видео, что позволяет ей распознавать временные зависимости между кадрами, на основе которых строятся последующие предсказания. Затем система снижает зависимость от передачи данных в реальном времени и обеспечивает более плавное воспроизведение видео, используя одну из выбранных моделей (RNN, диффузионная модель [3] или GAN [4]) для предсказания следующего кадра на основе предыдущих. На третьем этапе предсказанные кадры передаются через спутниковые каналы связи и затем отображаются. Снижение зависимости от постоянной передачи данных помогает уменьшить задержку.

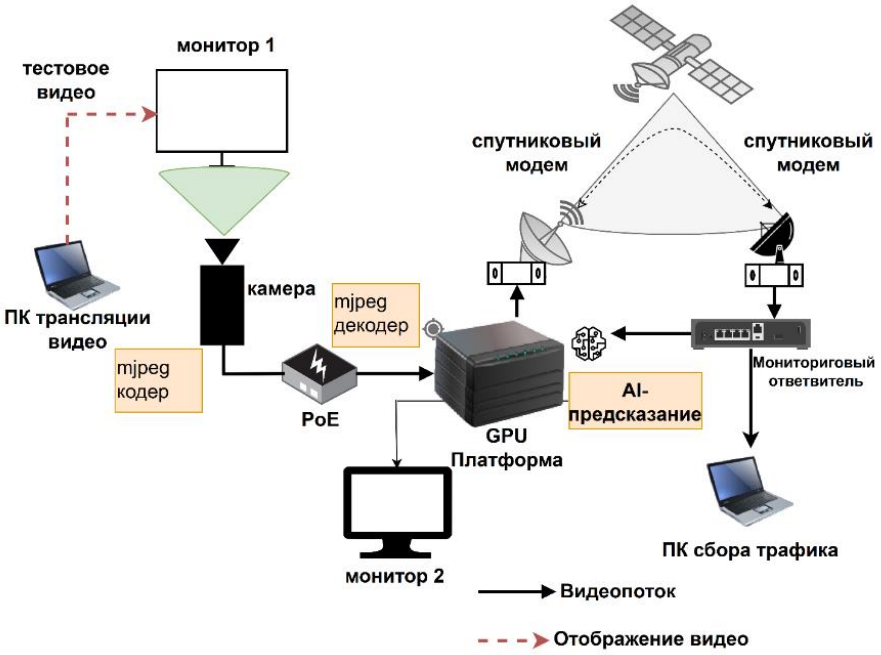


Рис. 1. Подробная последовательность процесса прогнозирования следующего кадра при передаче данных по спутниковому каналу

В этой статье мы сравним и оценим методы прогнозирования следующего кадра видеоданных на основе различных моделей, таких как модель диффузии, GAN и RNN.

Общие методы, используемые для прогнозирования следующего кадра

Прогнозирование следующего кадра очень подходит для модели RNN, поскольку оно часто работает с данными временных рядов [5]. Благодаря архитектуре RNN можно находить зависимости и ассоциации между соответствующими кадрами данных. Однако RNN часто сталкиваются с проблемами исчезновения градиентов и ограниченной памяти, что приводит к разработке лучших версий, таких как GRU и LSTM.

GAN [6] – популярная модель, используемая для создания реалистичных изображений. Он состоит из двух частей: дискриминатора и генератора, которые работают вместе для создания фактического изображения. Однако обучение GAN требует много ресурсов и предъявляет очень высокие требования к оборудованию.

Модель диффузии – это один из методов, который помогает создавать данные изображения для постепенного удаления шума из изображения. Однако вычислительные затраты довольно высоки, но при этом получаются качественные изображения, и это особенно важно в процессе обеспечения соответствия между задержкой и качеством получаемого изображения в тех случаях, когда вычислительные ресурсы недоступны.

Некоторые критерии для сравнения

Задержка является одним из параметров для оценки эффективности каждого метода в задаче прогнозирования следующего кадра. Среди перечисленных выше моделей модели диффузии и GAN могут вызывать большие задержки из-за высоких вычислительных затрат. Что касается модели RNN [7] и ее вариантов, таких как LSTM и GRU, задержка может быть ниже.

Второй фактор – это вычислительные ресурсы, необходимые для прогнозирования следующего кадра, что также является важным параметром для оценки эффективности каждой модели. GAN и диффузионные модели потребуют больше вычислительных ресурсов, в то время как для RNN требования к вычислительным ресурсам достаточны, но не должны быть слишком большими.

Другие факторы, такие как SSIM, PSNR и LPIPS, которые отражают качество выходного кадра, также являются одними из факторов, помогающих оценить эффективность каждой доступной модели. Модели GAN и диффузии дадут лучшие результаты, чем RNN и ее варианты. Однако требования к вычислительным затратам довольно велики, поэтому их необходимо учитывать.

Анализ методов, связанных с предсказанием следующего кадра

Оценивать и сравнивать эффективность методов и техник прогнозирования следующего кадра на основе ряда параметров, таких как задержка, вычис-

лительная сложность и качество сгенерированного кадра. В таблице 1 показано подробное сравнение существующих исследований с использованием различных методов, таких как RNN, GAN и диффузионная модель.

ТАБЛИЦА 1. Сравнения методов предсказания кадров

Статья	Метод	Уменьшение задержки	Вычислительная сложность	Качество восстановления	Комментарий
[1]	PredRNN	Низкая задержка благодаря последовательной обработке	Средняя (требует значительных ресурсов для обучения)	Высокое качество при предсказании пространственно-временных данных	Предлагает лучшие результаты в реальных условиях, но требует значительных вычислительных ресурсов
[2]	MCVD	Средняя задержка из-за итеративного подхода	Высокая, требует много вычислений для диффузионных шагов	Высокое качество восстановления, хотя иногда может быть нестабильным	Эффективен для создания высококачественных кадров, но ограничен вычислительными ресурсами
[3]	Диффузионные модели для предсказания видео	Средняя задержка из-за итеративного подхода	Очень высокая, особенно для больших видеоданных	Отличное качество изображений, особенно для длинных последовательностей	Хорошо подходит для создания высококачественных видео, но требует мощных вычислительных ресурсов
[4]	GAN для интерполяции кадров видео	Низкая задержка при использовании оптимизированных архитектур	Высокая, но ниже, чем у диффузионных моделей	Отличное качество кадров, но иногда не хватает стабильности	Подходит для улучшения видео, но требует значительных вычислительных мощностей
[5]	Предсказание видео для удаленного мониторинга	Низкая задержка благодаря предсказанию кадров	Средняя, подходит для реального времени	Среднее качество, но эффективно для мониторинга	Идеально для приложений в реальном времени, где важна скорость, хотя качество может быть не всегда на высшем уровне
[6]	Ретроспективный Cycle GAN	Средняя задержка из-за двустороннего обучения	Высокая, но эффективность повышается с улучшением модели	Хорошее качество при предсказаниях в замкнутых системах	Обещающий подход для улучшения качества видео, но требует многократных итераций
[7]	PredRNN с пространственно-временными LSTM	Низкая задержка, эффективно работает с временными зависимостями	Средняя, подходит для задач с большим объемом данных	Высокое качество для данных с временными зависимостями	Отлично подходит для обработки данных с временной зависимостью, но требует значительных ресурсов для обучения

Задержка, вычислительные требования и качество генерации следующего кадра являются важными факторами для сравнения методов и методов прогнозирования следующего кадра. Модель GAN и модель диффузии требуют большого объема математической обработки, поэтому задержка довольно велика и оказывает большое влияние на приложения реального времени. RNN и ее варианты имеют меньшую вычислительную сложность, чем две другие модели, поэтому подходят для сред с ограниченной вычислительной мощностью.

Модели GAN и диффузии обеспечивают эффективность процесса прогнозирования следующего кадра, но вычислительные затраты высоки, поэтому их необходимо учитывать во время использования. Однако модели GAN и диффузии создают кадры более высокого качества. Модели и варианты RNN имеют более низкое качество реконструкции кадров, но более стабильную задержку, что делает их более подходящими для реальных приложений.

Заключение

В этой статье мы сравнили некоторые популярные методы, используемые для прогнозирования следующего кадра, на основе ряда критериев сравнения, таких как задержка, требования к вычислительным ресурсам и качество создания кадра. Результаты показывают, что RNN и ее варианты имеют достаточно низкие требования к задержке и вычислительным ресурсам, что делает их пригодными для практического применения. Модели GAN и диффузии создают кадры лучшего качества, однако требуют больших вычислительных ресурсов, чем RNN и ее варианты. По времени выполнения RNN лучше, чем две другие модели.

Научная статья подготовлена в рамках прикладных научных исследований СПбГУТ, регистрационный номер 1023031600087-9-2.2.4;2.2.5;2.2.6;1.2.1;2.2.3 в ЕГИСУ НИОКТР.

Список используемых источников

1. Wang Y. et al. Predrnn: A recurrent neural network for spatiotemporal predictive learning // IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022. Vol. 45. №. 2. PP. 2208–2225.
2. Voleti V., Jolicoeur-Martineau A., Pal C. Mcvd-masked conditional video diffusion for prediction, generation, and interpolation // Advances in neural information processing systems, 2022. Vol. 35. PP. 23371–23385.
3. Höppe T. et al. Diffusion models for video prediction and infilling //arXiv preprint arXiv:2206.07696. 2022.

4. Tran Q. N., Yang S. H. Efficient video frame interpolation using generative adversarial networks // Applied Sciences, 2020. Vol. 10. №. 18. PP. 6245.
5. Sato T. et al. Compensation of communication latency in remote monitoring systems by video prediction // IEICE Transactions on Communications. 2024.
6. Kwon Y. H., Park M. G. Predicting future frames using retrospective cycle gan //Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019. PP. 1811-1820.
7. Wang Y. et al. Predrnn: Recurrent neural networks for predictive learning using spatiotemporal lstms // Advances in neural information processing systems, 2017. Vol. 30.

Berezkin A., Do Ph. H., Kirichek R. **ANALYSIS OF FRAME PREDICTION TECHNIQUES TO REDUCE DELAY IN SATELLITE COMMUNICATION CHANNELS FOR VIDEO STREAMING.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In satellite communication systems, latency is a major problem, particularly for applications like video streaming that need fast data transfer and crisp pictures. By lowering the need for real-time data transmission and enabling frame prediction to reduce latency, frame prediction algorithms provide an efficient option. Recurrent neural networks (RNNs), generative adversarial networks (GANs), and diffusion models are the main topics of this paper's review and comparative study of frame prediction techniques. Metrics including learning perceptual image similarity (LPIPS), peak signal-to-noise ratio (PSNR), and structural similarity index (SSIM) are used to assess these models. Our findings demonstrate each model's advantages and disadvantages in terms of lowering latency without sacrificing image quality.

Key words: Latency, satellite communication systems, frame prediction, generative adversarial networks, diffusion models.

УДК 004.422:004.054
ГРНТИ 20.53.21, 28.27.27, 50.41.25

РАЗРАБОТКА ПРОГРАММНОЙ СИСТЕМЫ МОНИТОРИНГА БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ НА КАРТЕ И ТЕСТИРОВАНИЯ ИСТОЧНИКОВ ДАННЫХ

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

Беспилотные воздушные суда в последние годы находят активное применение в различных сферах. Вместе с тем они могут представлять угрозу для инфраструктурных объектов и граждан вследствие нештатных ситуаций при их полетах и целенаправленных враждебных действий со стороны недружественных государств. Обеспечение безопасности в сфере беспилотных воздушных судов требует их правового регулирования, идентификации, мониторинга и подавления. Приблизиться к решению третьей проблемы позволяет настоящая работа. Представляемая в ней программная система позволяет производить мониторинг перемещения беспилотных воздушных судов и проводить тестирование источников данных о них.

беспилотный летательный аппарат, дрон, тестирование, визуализация на карте, программное обеспечение, радар, мониторинг

В последние годы беспилотные воздушные суда (далее – БВС) активно применяются во многих сферах [1–3]. Они позволяют: существенно повысить эффективность ведения сельского хозяйства [1–3]; обеспечивать контроль строительных площадок [1]; составлять карты [3]; проводить мониторинг экологической обстановки [3]; доставлять продукты и медикаменты лицам, оказавшимся в зоне стихийных и антропогенных бедствий [1, 3]. Вместе с тем БВС предоставляют широкие возможности по атакам на инфраструктуру и совершению террористических актов на территории сопредельных государств [4]. Это активно используется недружественными государствами по отношению к Российской Федерации и представляет значительную угрозу национальной безопасности. Таким образом, возникает проблема обеспечения безопасности в сфере БВС. В этом выделяют несколько направлений:

1. Правовая регуляция использования гражданских БВС. В 2017 году была установлен обязательный государственный учет БВС взлетной массы от 250 грамм до 30 кг [5]. На 2024 год минимальная взлетная масса БВС для регистрации составляет 150 грамм. Регулируются зоны, в которых полет беспилотных летательных аппаратов ограничен или запрещен [6];

2. Технические аспекты идентификации БВС. Выделяется два подхода: идентификация официально зарегистрированных БВС и прочих неопознанных. В первом случае используются такие подходы, как RFID-метки и отправка данных с бортовой прибор системы идентификации (БПСИ) на специальные системы идентификации [7]. Во втором случае данные подходы неприменимы в связи с тем, что с БВС не отправляется никаких идентификационных данных. Для идентификации таких БВС используются радиолокационные и оптические методы;

3. Технические аспекты мониторинга БВС. Если при идентификации осуществляется получение идентификатора БВС и характеристик, таких как координат местонахождения, высоты, скорости и курсового угла, то при мониторинге эти данные должны быть предоставлены заинтересованным лицам и службам в виде понятном человеку;

4. Подавление БВС, осуществляющих несанкционированный полет. Для этого применяется средства радиоэлектронной борьбы (РЭБ) и средства физического уничтожения БВС.

В настоящей работе рассматривается третье направление.

Потребность в системе мониторинга БВС возникла в ходе ведущихся на данный момент в СПбГУТ практических научных исследований по разработке системы идентификации БВС на базе архитектуры цифровых объектов (DOA – Digital Objects Architecture). Изначально для тестирования системы применялся программный эмулятор БВС [7], который отправлял данные в систему идентификации, и система мониторинга полетной обстановки FlyDrone [8]. Тем не менее, система FlyDrone, которая на тот момент предназначалась именно для демонстративных целей, стала на продолжительный срок недоступна. Соответственно, осуществление тестирования системы идентификации оказалось затруднено, ввиду чего потребовалась альтернативная система. К ней были выдвинуты следующие требования.

1. Возможность локального развертывания. Она не должна быть явно зависима от внешних программных интерфейсов (API), в доступе к которым возможны перебои.

2. Возможность добавления поддержки новых систем идентификации БВС и форматов данных. Данное требование обусловлено тем, что в ходе практических научных исследований форматы данных меняются.

3. Возможность использования системы через сеть Интернет. Демонстрация работоспособности систем идентификации и мониторинга БВС должна быть доступна при доступе к сети Интернет вне зависимости от географического положения.

4. Данная система должна быть отечественным программным обеспечением. Это делается во избежание утечек данных в недружественные страны.

5. Возможность просмотра активных БВС на карте и их данных.

7. Возможность проведения нагрузочного тестирования источников данных, являющихся системами идентификации БВС. Данное требование возникает из необходимости оценки их ограничений по использованию.

8. Ограничение прав доступа к подсистемам карты и тестирования.

Существует ряд программных систем, предоставляющих широкие возможности по мониторингу БВС: просмотр положения БВС, управление полетами, запрос разрешений на полеты над населенными пунктами, просмотр зон запрета и ограничения полета [8, 9]. К таким системам относятся FlyDrone [8] и Небосвод [9] Тем не менее, они не удовлетворяют первому требованию. Альтернативные программные средства, такие как [10, 11], не удовлетворяют ряду других вышеуказанных требований. В связи с этим было принято решение о разработке собственной программной системы мониторинга БВС.

Программная система «БВС-монитор DOA» (рис. 1), рассматриваемая в данной работе, представляет собой веб-приложение на языке программирования Python на фреймворке Django версии 5. В качестве планировщика задач используется Django Background Task 4, а библиотеки интерактивных карт – OpenLayers.

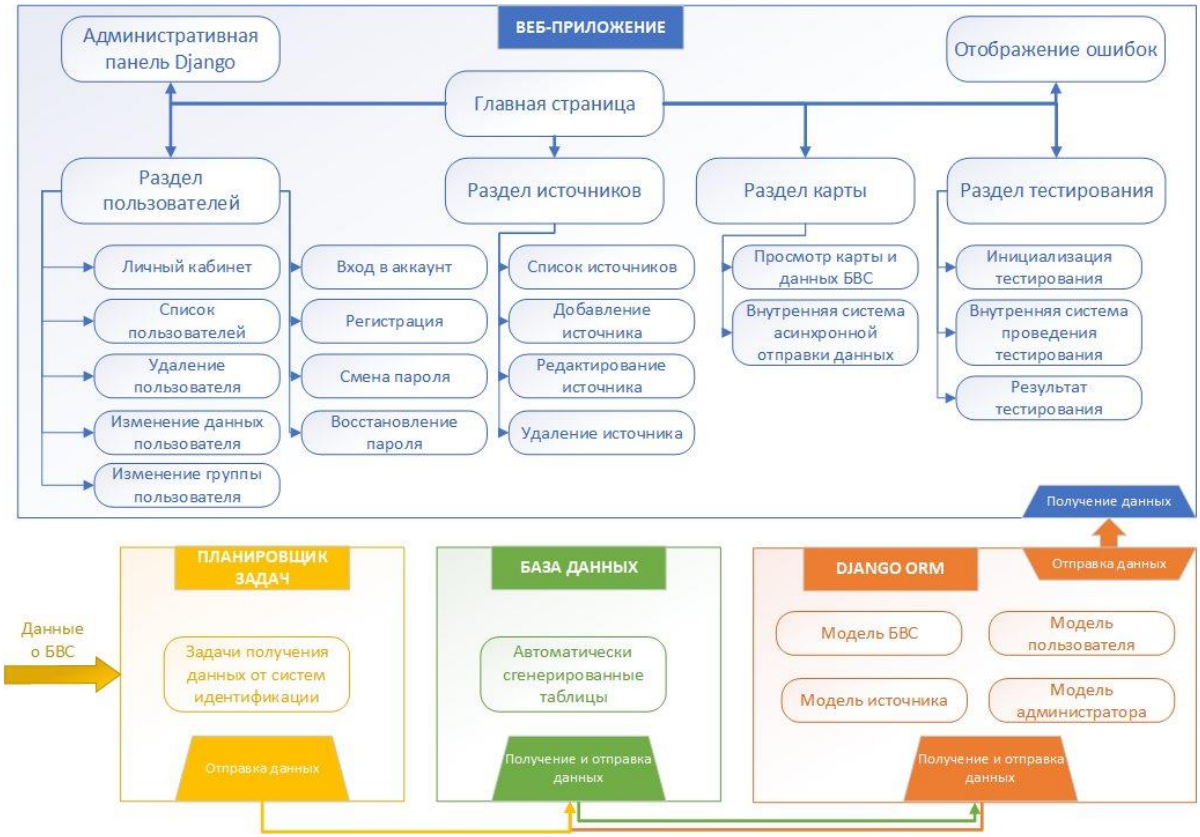


Рис. 1. Структурная схема программной системы «БВС-монитор»

Для разграничения доступа определено четыре группы пользователей: гость, пользователь, техник и администратор (таблица 1). Отдельно выделены суперпользователи, имеющие доступ к административной панели Django. Каждая группа следующего уровня имеет все права групп предыдущего уровня и дополнительные.

ТАБЛИЦА 1. Группы пользователей

Группа	Уровень	Права
Гость	0	Доступ к своему личному кабинету
Пользователь	1	+ Доступ к карте
Техник	2	+ Доступ к источникам + Доступ к тестированию
Администратор	3	+ Доступ к данным других пользователей + Доступ к списку пользователей + Доступ к редактированию и удалению пользователей + Доступ к изменению групп пользователей
Суперпользователь	4	+ Доступ к административной панели Django, дающей подробные данные о сайте и возможности управления им

В качестве карты используется OpenStreetMap (рис. 2) с приведенными в соответствие с Конституцией границами Российской Федерации. При испытаниях было выявлено, что 1000 БВС на карте успешно отображаются.

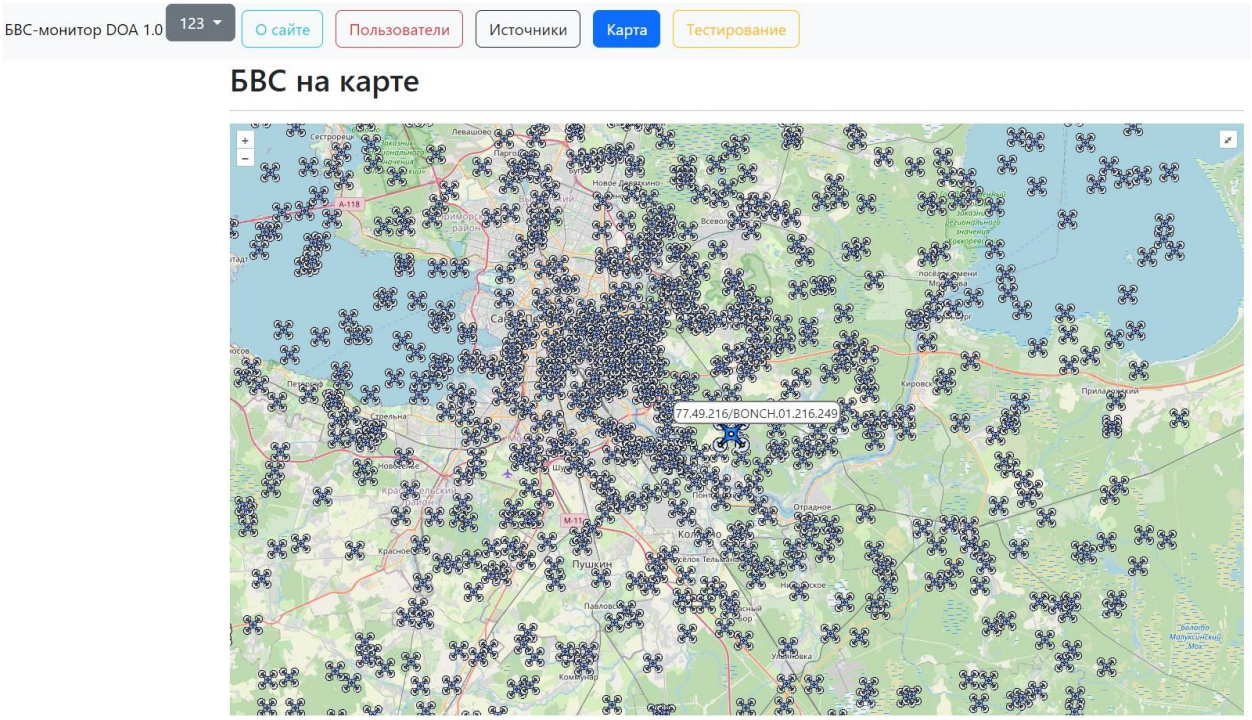


Рис. 1. Пример просмотра БВС на карте в системе «БВС-монитор»

Исходные параметры нагрузочного тестирования источников: тестируемая система, период запросов (мс), время тестирования (мс).

Результирующие параметры: среднее время ожидания (мс), процент корректных кодов ответов (%), процент корректных ответов (%). Под процентом корректных кодов ответов понимается процент запросов, коды HTTP-ответов которых равны 200. Под процентом корректных ответов понимает процент запросов, ответы на которые содержат данные в поддерживаемом формате. На текущий момент поддерживается один формат: FlyDrone-радар, но присутствует функциональная возможность добавления других.

Таким образом, была выполнена разработка программной системы, удовлетворяющей поставленным требованиям. Она дает пользователям возможности: отслеживания перемещения БВС по карте, получения данных по ним и выполнения тестирование систем идентификации БВС. Несмотря на то, что изначально данная система создавалась для тестирования, при интеграции с соответствующими системами она может использоваться для мониторинга полетов БВС.

Список используемых источников

1. Mohsan S. A. H., Othman N. Q. H., Li Y. Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends // Intelligent Service Robotics. 2023. Vol. 16. №. 1. PP. 109–137.
2. Shakhatreh H., Sawalmeh A. H., Al-Fuqaha A., Dou Z., Almaita E., Khalil I. Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges // IEEE Access, 2019. Vol. 7. PP. 48572–48634.
3. Nawaz H., Ali H.M., Massan S. Applications of unmanned aerial vehicles: a review // Tecnol. Glosas InnovaciÓ Apl. Pyme. Spec, 2019. Vol. 2019. PP. 85–105.
4. Тикшаев В. Н., Барвиненко В. В. Проблема борьбы с беспилотными летательными аппаратами и возможные пути ее решения // Военная мысль. 2021. №1.
5. Горовой В. В. Правовые аспекты регулирования полетов беспилотных летательных аппаратов в Российской Федерации // Вестник Академии права и управления. 2018. № 2 (51).
6. Постановление Правительства Российской Федерации от 21.06.2023 № 1016 «О внесении изменений в Федеральные правила использования воздушного пространства Российской Федерации и признании утратившим силу отдельных положений постановления Правительства Российской Федерации от 03.02.2020 № 74».
7. Ченский А. А., Березкин А. А. Разработка программного обеспечения для нагрузочного тестирования систем идентификации и мониторинга беспилотных летательных аппаратов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024.
8. Ивашов Н. Беспилотье в России: маркетплейс как драйвер отрасли // Технологии безопасности жизнедеятельности, 2023. № 2. С. 72–74.

9. Свидетельство о государственной регистрации программы для ЭВМ № 2022666202 Российская Федерация. Программное обеспечение для организации полетов БВС «Небосвод»: № 2022664724 : заявл. 09.08.2022 : опубл. 26.08.2022 / А. Н. Хрипунов; заявитель Общество с ограниченной ответственностью НИЦ «Аэроскрипт».
10. Зарипов Г. С. Система мониторинга за беспилотными летательными аппаратами в нижнем воздушном пространстве / Г. С. Зарипов, А. В. Ким, Д. А. Евсевичев // Актуальные проблемы физической и функциональной электроники : Материалы 23-й Всероссийской молодежной научной конференции, Ульяновск, 20–22 октября 2020 года. Ульяновск: Ульяновский государственный технический университет, 2020. С. 82–83.
11. Itkin M., Kim M., Park Y. Development of cloud-based UAV monitoring and management system // Sensors, 2016. Vol. 16. №. 11 P. 1913.

Berezkin A., Chenskiy A. **DEVELOPMENT OF A SOFTWARE SYSTEM FOR UNMANNED AIRCRAFT VEHICLES MONITORING ON THE MAP AND DATA SOURCES TESTING.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the last years, unmanned aircraft vehicles have been actively used in various spheres. At the same time, they may pose a threat to infrastructure objects and citizens due to emergency situations in the flights and deliberate hostilities from the unfriendly states. In order to enforce security in this sphere, it is necessary to identify and monitor unmanned aircraft vehicles. The present work approaches the second problem. It presents a software system that allows the user to monitor the movements of unmanned aircraft vehicles and test the data sources.

Key words: unmanned aircraft vehicle, drone, testing, map visualization, software, radar, monitoring.

КИБЕРБЕЗОПАСНОСТЬ

4.1. Защищенные системы связи

УДК 004.056.53
ГРНТИ 81.93.29

ENHANCING APPLICATION SECURITY THROUGH DYNAMIC BINARY INSTRUMENTATION

S. Alkattan
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

As mobile and desktop applications on platforms like Android and Windows become increasingly vulnerable to runtime attacks, a robust security solution is essential. Traditional static security methods often fall short in detecting sophisticated, dynamic attacks, motivating the use of Dynamic Binary Instrumentation (DBI) for real-time threat mitigation. This paper presents a cross-platform DBI-based security framework utilizing Frida, DynamoRIO, and Pin to enhance security on Android and Windows applications. The framework demonstrates effective detection and mitigation of runtime threats, including memory corruption, code injection, and control flow manipulation, with manageable performance trade-offs.

DLL Injection, Security Mechanisms, DBI, Anomaly Detection

1. INTRODUCTION

The rise in the number of digital applications on Android and Windows platforms has increased their exposure to security threats. This is because these widely used platforms are the main targets for attackers looking to exploit application vulnerabilities due to their popularity. Techniques such as code injection, buffer overflow, and control flow manipulation are commonly used to compromise the system. Although static analysis and signature-based detection methods were originally used to secure highly vulnerable applications, these methods typically occur at runtime. They fail to handle sophisticated attacks [1]. Dynamic Binary Instrumentation (DBI) offers an attractive alternative by enabling real-time code inspection, thus providing a proactive approach to mitigate runtime threats during runtime.

2. BACKGROUND AND RELATED WORK

2.1 Dynamic Binary Instrumentation (DBI)

Dynamic binary analysis is a technique used to analyze and modify application code while it is running. This provides significant benefits for security monitoring and attack prevention. Dynamic binary analysis tools such as Frida and DynamoRIO for Android or Pin for Windows allow real-time tooling to be inserted into application's binary without changing the source code, this capability is particularly useful for detecting runtime anomalies in code execution and control flow. It is a frequent vector of attacks [2]. Dynamic binary analysis facilitates interception of system calls. Memory allocation function and other critical operations that lead to memory corruption. Unauthorized code injection. At the same time, against threats such as control tampering, detection is completed [3].

2.2 Related Work

Previous studies have investigated the potential of DBI for platform-specific security. For example, Han et al. [4] used Frida on Android to monitor runtime behavior and detect malicious code injection, while Johnson Kim [5] demonstrated a control flow protection implementation on Windows using DynamoRIO. Although these studies provide valuable insights into the security of Android and Windows and these environments, cross-platform approaches remain largely unexplored. This paper contributes to this area by presenting an integrated DBI-based framework that addresses security challenges on both platforms. It builds on the strengths of previous work.

3. Proposed Framework

The proposed framework is based on DBI to examine Android (using Frida) and Windows (using DynamoRIO and PIN) applications and consists of three main components:

– *Runtime Instrumentation:* The framework inserts a hook into important system functions to monitor and record runtime behavior. Frieda for Android blocks system calls and memory allocation functions, while on Windows it monitors memory management operations on DynamoRIO or Pin allowing early detection of malicious behavior.

– *Anomaly Detection:* The system continuously monitors application behavior. It identifies changes from normal operation. Abnormal behavior, such as unauthorized memory access patterns or unexpected system calls, triggers immediate notification and activation of a security response.

– *Attack Mitigation:* Detecting the attack stops, or holds dynamic execution. Changes the control path or blocks memory access to prevent further intrusion. This proactive approach provides important protection against runtime threats that bypass usual security mechanisms.

3.1 Memory Exploit Mitigation

Memory-related attacks such as buffer overflow and use-of-free vulnerabilities. As is common in Android and Windows operating systems, our framework checks memory allocation tasks (such as malloc and free on Windows, and VirtualAlloc and HeapAlloc on Android) for buffer usage. Detecting overflow prevents unauthorized memory modification. Intervening by adding a warning to prevent buffer overflow attempts when buffer overflow detection is attempted. The efficiency of usage is reduced [6].

3.2 Dynamic Code Loading Protection

Dynamic code loading is often used to inject malicious payloads at runtime. Check code loading mechanisms, such as DexClassLoader on Android and LoadLibrary on Windows, to ensure that only authorized code runs. Unauthorized or suspicious code will be blocked. Prevent dangerous injection. For example, on Windows, the framework intercepts attempt to load unauthorized DLLs, stopping the injection before any code can be executed [7].

3.3 Control Flow Integrity (CFI)

Control Flow Integrity is essential for maintaining the correct execution flow of an application, particularly as attackers' often try to hijack control flow to execute arbitrary code. The framework monitors indirect jumps and function pointers to detect changes from the expected control flow. Using DynamoRIO on Windows, the framework intercepts any attempt to manipulate the control flow, blocking unauthorized execution paths and ensuring application integrity [8].

4. FRAMEWORK VALIDATION AND SECURITY ANALYSIS

4.1 Theoretical Security Benefits

The proposed DBI-based framework offers significant theoretical advantages by enabling real-time monitoring and threat response across Android and Windows platforms. Unlike static analysis methods, DBI-based instrumentation detects runtime threats, providing timely interventions for memory corruption, code injection, and control flow manipulation. This framework prevents unauthorized memory

and control flow modifications, thus effectively mitigating common runtime threats [9].

4.2 Hypothetical Case Scenarios

To illustrate the practical application of the framework, consider the following scenarios:

– *Memory Corruption Prevention:* In an Android application with a buffer overflow vulnerability, Frida's monitoring of malloc and free detects an overflow and blocks it, stopping the attack from compromising application memory.

– *Dynamic Code Injection Blocking:* On Windows, an attacker tries to inject malicious code through an unauthorized DLL. The framework, using DynamoRIO, intercepts the attempt to load this DLL via LoadLibrary, preventing malicious code from executing and compromising the application.

4.3 Expected Performance Considerations

DBI inevitably adds some runtime overhead due to its continuous monitoring functions. Studies on tools such as Frida and DynamoRIO indicate a typical overhead of 10–15 %, a manageable impact for security-sensitive applications such as banking, healthcare, and communications [10]. Future optimizations could focus on minimizing this overhead, making the framework viable for performance-critical environments.

5. CONCLUSION AND FUTURE WORK

This paper presents a cross-platform DBI-based framework for enhancing application security on Android and Windows. By leveraging tools like Frida and DynamoRIO, the framework effectively detects and mitigates runtime threats, such as memory exploits, code injection, and control flow hijacking, with an acceptable performance impact.

References

1. Seshadri A., Luk M., Qu N., et al. SecVisor: A tiny hypervisor to provide lifetime kernel code integrity for commodity Oses // ACM SIGOPS Operating Systems Review, 2008. № 41 (6). PP. 335–350.

2. Nethercote N., Seward J. Valgrind: A framework for heavyweight dynamic binary instrumentation // ACM Sigplan Notices, 2007. № 42 (6). PP. 89–100.

3. Srivastava A., Giffin J. Efficient monitoring of dynamically-typed programs for security // Journal of Computer Security, 2012. № 18 (1). PP. 1-25.

4. Han J., Lee K., Shin D. Runtime anomaly detection for Android malware using dynamic instrumentation // International Journal of Mobile Security, 2020. № 16 (2). PP. 241–259.

5. Johnson A., Kim J. Control-flow integrity for Windows applications using DBI // Journal of Information Security Research, 2019. № 17 (3). PP. 89–102.
6. Chen P. M., Noble B. D. When virtual is better than real: Performance and consistency in real-time scheduling // Journal of the ACM, 2001. № 49 (3). PP. 24–47.
7. Kiriansky V., Bruening D., Amarasinghe S. Secure execution via program shepherding // 11th USENIX Security Symposium, 2002.
8. Abadi M., Budiu M., Erlingsson Ú., Ligatti J. Control-flow integrity principles, implementations, and applications // ACM Transactions on Information and System Security (TISSEC), 2005. № 13 (1). P. 4.
9. Zhang M., Sekar R. Control flow integrity for COTS binaries // 22nd USENIX Security Symposium, 2013.
10. Nethercote N., Seward J. Valgrind: A framework for heavyweight dynamic binary instrumentation // ACM Sigplan Notices, 2007. № 42 (6). PP. 89–100.

***Алькаттан С.* ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ПРИЛОЖЕНИЙ С ПОМОЩЬЮ ДИНАМИЧЕСКОГО ДВОИЧНОГО ИНСТРУМЕНТАРИЯ.**

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

Поскольку мобильные и настольные приложения на таких платформах, как Android и Windows, становятся все более уязвимыми для атак во время выполнения, необходимо надежное решение безопасности. Традиционные статические методы безопасности часто не справляются с обнаружением сложных динамических атак, что мотивирует использование Dynamic Binary Instrumentation (DBI) для смягчения угроз в реальном времени. В этой статье представлена кроссплатформенная инфраструктура безопасности на основе DBI, использующая Frida, DynamoRIO и Pin для повышения безопасности приложений Android и Windows. Эта инфраструктура демонстрирует эффективное обнаружение и смягчение угроз во время выполнения, включая повреждение памяти, внедрение кода и манипулирование потоком управления, с управляемыми компромиссами производительности.

Ключевые слова: внедрение DLL, механизмы безопасности, DBI, обнаружение аномалий.

УДК 004.056.53
ГРНТИ 81.93.29

INTEGRATED SECURITY IN DEVOPS: DESIGN AND IMPLEMENTATION OF AUTOMATED SECURITY TESTING FRAMEWORKS IN DEVOPS PIPELINES

A. Chiziba
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

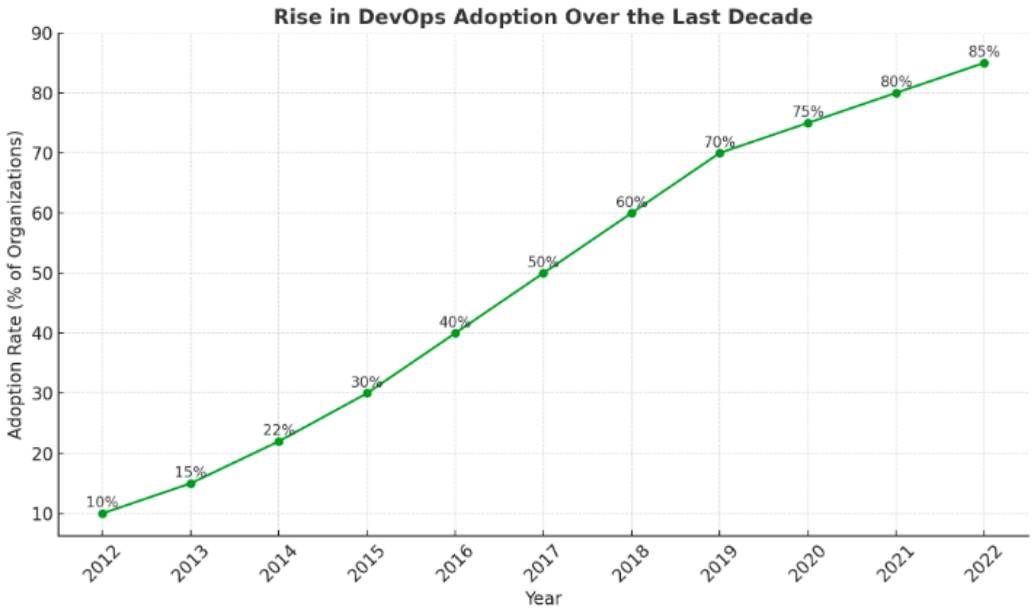
There has been a rapid increase in the number of applications and services that are being deployed through DevOps pipelines by individuals, organizations and companies e.g using tools like Gitlab, Jenkins, etc. This increase in deployment speed has highlighted the need to include security checks into the DevOps workflows; there is also the constant threat of exploitation that has cause organizations to adopt automatic security checks that include automatic vulnerability scanning, real-time monitoring and secrets management. These security features are mainly integrated directly into the DevOps pipeline.

DevOps Security, Automated Security Testing, OpenSource Security Tools, Static Code Analysis, CI/CD Pipelines, Dynamic Code Analysis, SonarQube, GitGuardian, TruffleHog, Pytest.

The use of DevOps practices has been rapid and has changed how individuals and organizations build, deploy and maintain software applications, a good example is how updates are pushed to mobile applications without disturbing service to the users. By combining development and operation principles, DevOps allows collaboration, speeds up delivery cycles and ensures that updates to software have passed tests before they are published to production. This enables updates to be made frequently while not affecting the quality and stability [1] of the applications.

Another major factor that has increased the use of DevOps practices is the need to automate software deployment. Automated testing of software and continuous deployment reduce manual effort and ensure that there is a consistent outcome since there is minimal human intervention to cause errors. In addition to that, there are now affordable cloud services (e. g. DigitalOcean, Heroku, Netlify) that support DevOps practices and provide documentation and support for setup. To further simplify the use of DevOps, there are tools like Docker [2] and Kubernetes [3] that enable containerization and orchestration of containers respectively.

This shift to automated DevOps practices has indeed led to an increase in the rate of deployment of applications and services. This, however has also introduced new challenges, particularly in ensuring that there are thorough security checks throughout the development cycle. The image (Img. 1) below highlights the increase in software deployment done through DevOps pipelines over the last decade.



Img. 1. DevOps adoption over a 10year Period

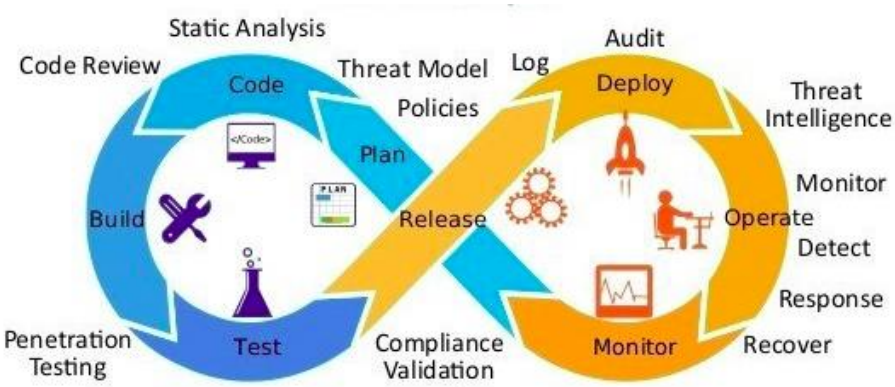
There has also been a steady increase in cyber-attacks that target web applications and this has caused online services to integrate security measures into DevOps and the development cycle of software. With that in mind, modern DevOps practice has evolved to Development Security and Operations (DevSecOps) [4]. DevSecOps has a security focus approach that includes security checks throughout the development and deployment pipeline.

Some of the checks that have high priority in DevSecOps, along with their descriptions are listed in table 1.

TABLE 1. Common security checks in DevOps environments and their descriptions

Security Check	Description
Role-Based Access Control (RBAC)	Enforcing least-privilege access in DevOps tools, repositories, and cloud environments to prevent unauthorized actions by restricting access based on roles
Continuous Vulnerability Scanning	Using tools like SonarQube or Trivy within CI/CD pipelines to automatically scan code, container images, and dependencies for vulnerabilities before deployment
Automated Input Validation	Integrating static code analysis tools into CI/CD pipelines to detect and remediate vulnerabilities like SQL injection or XSS during development
Real-Time Monitoring and Logging	Enable monitoring tools like Prometheus and centralized logging solutions such as ELK or Grafana Loki to detect anomalies in real-time and streamline incident response
Automated Patch Management	Using infrastructure-as-code (IaC) tools like Ansible or Terraform to deploy updates and security patches across environments automatically, minimizing downtime and ensuring compliance
Secure Authentication Mechanisms	Implementing secure and automated identity management solutions, such as OAuth, multi-factor authentication (MFA), or secrets management tools, to control access to applications and pipelines.

With the proper security checks put in place in the DevOps environment, organizations can balance rapid development and deployment with strong application security. The image (Img. 2) below shows the different stages of a DevOps lifecycle and how security testing and audits happen during each of those stages.



Img. 2. Stages of Security Analysis in DevOps

This is research will focus on designing and implementing a framework that allow automation of security testing in DevOps environments and their pipelines. It is separated into three main connect components: Static and Dynamic Code Analysis, Secrets Management, and CI/CD integration [5].

The Static and Dynamic Code Analysis component, which is the first one, will be developed for code analysis and will use source code from SonarQube and Semgrep. SonarQube will be used because it supports multiple programming languages and Semgrep supports writing customizable rules for identifying vulnerabilities. The effectiveness of the developed component will be tested on code bases with known vulnerabilities. This will enable us to judge the accuracy of the component also determine the integration complexity. The results of the tests will also help to redefine some rules that lead to false positives and also add rules that can detect improper storage of API keys.

The second component is Secrets Management, the main goal of this component is to detect sensitive data that is exposed in the code-base. This can include API keys, passwords and connection strings. The component will be built on top of GitGuardian and TruffleHog, these will help in detecting hard-coded secrets and issue alerts if secrets are exposed in the code before the application is deployed. To see the effectiveness of the component, it will be tested by introducing exposed secrets into the code and checking the detection rates, efficiency, and the overall impact on performance.

The final component involves CI/CD integration, this will handle combining all tools into one framework that will enable continuous development and automated security development at every stage of the software development and deployed. The framework will be developed using Python-based tools and will also use pytest to

automate unit testing. The security testing stages will cover code scanning, secrets detection and assessment of vulnerabilities to ensure that issues are discovered and resolved before the code is deployed. The main goal of the integrated framework is to help automated security testing and providing alerts to help inform developers and the security team if there are issues that need to be addressed.

The framework will be tested in real work environments that include large code-bases so that it's performance and reliability can be assessed. These tests will mainly focus on determining accuracy, reducing false positive alerts, and the overall performance. The aim of the research is to deliver an automated security testing framework that easy to use, efficient and can be integrated into existing DevOps workflows so that organizations can adopt better security practices in DevSecOps.

References

1. DevOps LifeCycle: Definition, Key Components, Best Practices. URL: https://katalon.com/resources-center/blog/devops-lifecycle (дата обращения 11.11.2024).
2. Docker. URL: https://www.docker.com/ (дата обращения 12.11.2024).
3. Kubernetes Documentation. URL: https://kubernetes.io/ (дата обращения 12.11.2024).
4. What is DevSecOps? URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-devsecops (дата обращения 15.11.2024).
5. CI/CD: The what, why, and how. URL: https://github.com/resources/articles/devops/ci-cd (дата обращения 15.11.2024).

***Чизиба Э.* ИНТЕГРИРОВАННАЯ БЕЗОПАСНОСТЬ В DEVOPS: ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ АВТОМАТИЗИРОВАННЫХ ФРЕЙМВОРКОВ ДЛЯ ТЕСТИРОВАНИЯ В КОНВЕЙЕРАХ DEVOPS.**

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

Наблюдается быстрый рост числа приложений и сервисов, которые развертываются через конвейеры DevOps отдельными лицами, организациями и компаниями, например, с использованием таких инструментов, как Gitlab, Jenkins и т. д. Это увеличение скорости развертывания выявило необходимость включения проверок безопасности в рабочие процессы DevOps; также существует постоянная угроза эксплуатации, которая заставила организации внедрить автоматические проверки безопасности, включающие автоматическое сканирование уязвимостей, мониторинг в реальном времени и управление секретами. Эти функции безопасности в основном интегрированы непосредственно в конвейер DevOps.

Ключевые слова: безопасность DevOps, автоматизированное тестирование безопасности, инструменты безопасности с открытым исходным кодом, статический анализ кода, конвейеры CI/CD, динамический анализ кода, SonarQube, GitGuardian, TruffleHog, Pytest.

УДК 004.62
ГРНТИ 20.15.05

МЕХАНИЗМ ЭМУЛЯЦИИ АТАКИ ТИПА MAN IN THE MIDDLE НА УЗЛЫ ИНФРАСТРУКТУРЫ

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

В современном мире, где информация является одним из самых ценных активов, защита от атак типа «человек посередине» становится особенно актуальной. Атаки ARP-спуфинга представляют собой распространенный и опасный метод, используемый злоумышленниками для перехвата и манипуляции сетевым трафиком. С ростом использования беспроводных сетей и удаленной работы, уязвимости в сетевой безопасности стали более заметными, что делает необходимость в защите от подобных атак критически важной.

информационная безопасность, сетевая безопасность, эмуляция атаки, атака типа «Man in the Middle», ARP-спуфинг

Атаки типа «человек посередине» (MITM, “Man In The Middle”) представляют собой метод взлома, при котором злоумышленник перехватывает и, иногда, модифицирует коммуникацию между двумя сторонами, ничего не подозревающими о вмешательстве. Эти атаки могут происходить в различных контекстах – от частных сетей до публичных Wi-Fi, и могут использоваться для кражи данных, внедрения вредоносного ПО или осуществления других злонамеренных действий.

Атака MITM включает действия злоумышленника, который помещается между двумя сторонами, которые пытаются общаться друг с другом. Это может происходить на разных уровнях: на уровне сетевого протокола, на уровне приложения и даже на уровне физического подключения. При успешной атаке злоумышленник может перехватывать, читать, изменять или подделывать сообщения между сторонами, что ставит под угрозу целостность и конфиденциальность данных [1].

Классифицировать атаки этого типа можно следующим образом:

– ARP Spoofing (атакующий отправляет поддельные ARP-ответы, чтобы связать свой MAC-адрес с IP-адресом другого устройства в локальной сети);

– DNS Spoofing (атакующий изменяет записи DNS, чтобы перенаправить жертву на поддельный сервер);

– SSL Stripping (злоумышленник разрывает зашифрованное HTTPS-соединение, заменяя его на незащищенное HTTP-соединение);

– Wi-Fi eavesdropping (на публичных сетях Wi-Fi злоумышленник может создать поддельную точку доступа, чтобы перехватывать трафик пользователей, подключающихся к этой сети [2]);

– Session Hijacking (атакующий может перехватить сессию пользователя, используя похищенные куки или токены аутентификации, что позволяет ему получить доступ к учетным записям жертвы);

– Email Interception (злоумышленник может перехватывать электронные письма, модифицировать их и отправлять от имени жертвы, создавая ложное впечатление о легитимности сообщений).

Проведение атаки такого типа может повлечь за собой серьезные риски и угрозы, в числе которых угроза конфиденциальности, модификация данных, финансовые потери, репутационные риски, правовые последствия, а также внедрение вредоносного ПО [3].

В рамках данного исследования будет проводится анализ угроз проведения подвида атаки MITM на основе ARP-спуфинга. ARP-спуфинг – это тип атаки, который использует уязвимость протокола ARP для перехвата сетевого трафика, передаваемого между устройствами в локальной сети. В результате этого трафик может быть перехвачен, изменен или перенаправлен злоумышленником.

В рамках анализа атаки с использованием ARP-спуфинга можно выделить следующие этапы проведения атаки:

1. Сканирование сети;
2. Отправка поддельных ARP-ответов;
3. Перенаправление трафика;
4. Перехват и модификация трафика.

Последствия такой атаки могут быть выражены в перехвате данных, манипуляции данными, отказом в обслуживании целевого хоста атаки, внедрения вредоносного ПО.

Базовый стенд для эмуляции атаки представлен на рисунке 1.

Для эмуляции атаки собрана следующая топология: имеются две виртуальные машины, объединенные между собой в локальную сеть. Виртуальная машина с операционной системой Ubuntu является целевым узлом для проведения атаки. Виртуальная машина с Kali Linux является атакующим узлом [4]. Для эмуляции атаки достаточно установить следующее программное обеспечение на атакующую машину: Ettercap и Wireshark.

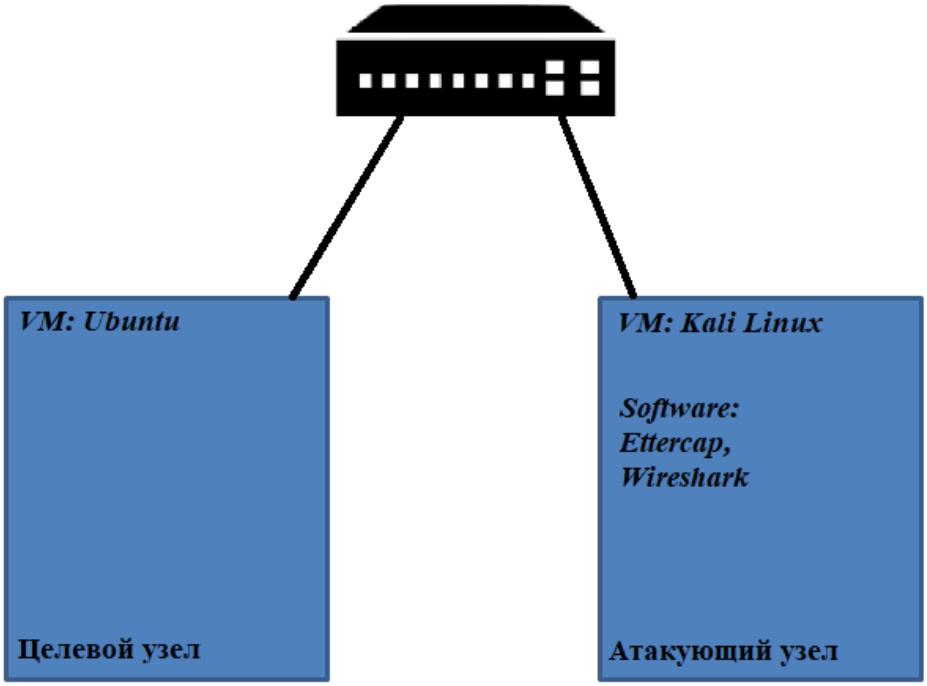


Рис. 1. Схема экспериментального стенда

Ettercap – это инструмент для перехвата и анализа сетевого трафика, который часто используется для атак типа «человек посередине», а также для ее подвидов, таких как ARP-спуфинг [5]. Этот инструмент позволяет пользователю следить за данными, проходящими через сеть, а также модифицировать и управлять этим трафиком [6].

Wireshark – это один из самых популярных и мощных инструментов для анализа сетевого трафика. Это приложение с открытым исходным кодом предназначено для захвата и детального анализа данных, проходящих через сеть, и используется как специалистами по сетям, так и исследователями безопасности [7].

Ход эксперимента проводится в несколько этапов.

Первый этап – «Подготовка». Он включает в себя настройку окружающей среды, присвоение виртуальным машинам адресации из одной подсети, а также установку необходимого программного инструментария на атакующий узел, а именно – Ettercap и Wireshark.

Второй этап – «Запуск Ettercap». С помощью команды «*sudo ettercap -G*» происходит запуск утилиты от имени суперпользователя на атакующем узле. Выбирается сетевой интерфейс через меню «*Sniff*», оснастку «*Unified Sniffing*».

Третий этап – «Сканирование сети». Действием «*Scan for hosts*» меню «*Hosts*» начинается сканирование активных узлов в сети. После того, как сканирование будет завершено необходимо в меню «Hosts», оснастке «Manage hosts» записать IP-адрес целевой машины и шлюза.

Четвертый этап – «Настройка эмуляции атаки». В качестве значений «*Target 1*» и «*Target 2*» выбираются адреса целевой машины и шлюза. В меню «*MITM*», оснастке «*Arp poisoning*» выбирается отметка «*Sniff remote connections*». На этом этапе начинается атака с подменой адресации шлюза на адрес атакующего узла в сторону трафика от целевого узла атаки.

Пятый этап – «Отслеживание трафика». Запускается Wireshark с помощью команды «*sudo wireshark*», с целью инициировать процесс сбора информации от имени суперпользователя. Выбирается конкретный сетевой интерфейс для отслеживания.

Финальный этап – «Отслеживание и анализ». В режиме реального времени анализируются захваченные пакеты с помощью утилиты Wireshark. По окончании атаки утилита Ettercap выключается с помощью внутренней команды «*Stop sniffing*».

Выводы, которые стоит заключить о ходе эксперимента, заключаются в демонстрации уязвимости в сети. Атака демонстрирует, как легко злоумышленник может подменить ARP-таблицы и перехватить трафик, если сеть не защищена. Злоумышленник может получить доступ ко всей информации, передаваемой в сети, включая пароли и конфиденциальные данные, что подчеркивает риски. С помощью Ettercap атака легко осуществима и эффективна, что показывает, что даже с минимальными техническими знаниями злоумышленник может перехватить и манипулировать сетевым трафиком. Все устройства в локальной сети могут стать мишенью, что делает защиту особенно критичной для организаций и пользователей.

ARP-спуфинг – это серьезная угроза для локальных сетей, поэтому важно принимать меры для защиты от этой уязвимости. Для обеспечения соответствующего уровня безопасности необходим грамотный и гибридный подход к защите данных. Настройка статических ARP-записей, как сценарий противодействия ARP-спуфингу предотвратит изменение ARP-кэша через поддельные ARP-ответы. Однако это может быть затруднительным при наличии большого числа устройств и может потребовать постоянного обновления. Использование протоколов шифрования также является составляющей для противодействия подобным атакам. Использование виртуальных частных сети (VPN) для шифрования трафика сделает данные, передаваемые через сеть, недоступными для злоумышленников, даже если они смогут перехватить трафик [8]. Использование соответствующих систем, таких как IDS (Системы предотвращения вторжений) позволят осуществлять мониторинг трафика и предотвращать подобные вторжения в сеть предприятия [9]. Защита от ARP-спуфинга требует многоуровневого подхода, учитывающего как технические, так и образовательные меры.

Список используемых источников

1. Штеренберг С. И., Ушаков И. А., Скорых М. А. исследование проблем построения доверенной среды передачи. 2024.
2. Волкогонов В. Н. и др. Анализ безопасности wi-fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 270-275.
3. Гельфанд А. М. Модель угроз конфиденциальности, целостности и доступности при передаче сообщения // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия. Т. 1. С. 5–9.
4. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инраструктуры // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2020. № 4. С. 72–76.
5. Цветков А. Ю., Рузманов Е. Ю. Рассмотрение методов тестирования на проникновение для анализа защищенности компании // ББК 3 П27, 2021. С. 57.
6. Ершова Т. В., Цветков А. Ю. Выбор метода проведения аудита информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 480-483.
7. Скорых М. А., Израилов К. Е., Башмаков А. В. Задачаориентированное сравнение средств анализа сетевого трафика // Теория и практика обеспечения информационной безопасности, 2021. С. 103–107.
8. Пестов И. Е., Кошелева С. А. Способы защиты от атаки «человек посередине» (MITM) // Инновационные решения социальных, экономических и технологических проблем современного общества, 2021. С. 116–118.
9. Пестов И. Е. и др. Разработка программно-аппаратной системы контроля и управления доступом // Эргодизайн, 2020. № 1 (7). С. 19–24.

Alekhin R. THE MECHANISM FOR EMULATING A “MAN IN THE MIDDLE ATTACK” ON INFRASTRUCTURE NODES.

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the modern world, where information is one of the most valuable assets, protection against man-in-the-middle attacks is becoming especially relevant. ARP spoofing attacks are a common and dangerous method used by attackers to intercept and manipulate network traffic. With the increasing use of wireless networks and remote work, network security vulnerabilities have become more visible, which makes the need to protect against such attacks critically important.

Key words: Information Security, Network Security, Attack Emulation, "Man in the Middle" type attack, ARP spoofing.

УДК 004.056.53
ГРНТИ 81.93.29

МЕТОД ОДНОРАЗОВОГО ПАРОЛЯ В МЕХАНИЗМЕ ФАКТОРНОЙ АУТЕНТИФИКАЦИИ И ВОЗМОЖНОСТЬ ЕГО ИСПОЛЬЗОВАНИЯ В БИОМЕТРИЧЕСКОЙ СИСТЕМЕ

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

Безопасность в интернете становится последней важной проблемой наряду с широким применением технологии. Слабость какой-либо части приводит к фатальному результату для всей системы безопасности. Поэтому системы безопасности требуют тщательной разработки и взаимной координации в каждом элементе. Была изучена и интегрирована с биометрической системой система генерации случайного одноразового пароля для повышения безопасности и защиты пользовательских данных.

одноразовый пароль, факторы аутентификации, биометрическая система, отпечаток пальца, MFA

Одноразовый пароль (OTP) – это пароль, который действителен только для одного сеанса входа или транзакции в компьютерной системе или другом цифровом устройстве [1]. OTP избегают ряда недостатков, связанных с традиционной (статической) аутентификацией на основе паролей; ряд реализаций также включают двухфакторную аутентификацию, гарантируя, что одноразовый пароль требует доступа к чему-то, что есть у человека (например, к небольшому брелоку-брелку со встроенным в него калькулятором OTP, или к смарт-карте или определенному мобильному телефону), а также к чему-то, что человек знает (например, к PIN-коду). Самое важное преимущество, которое решается с помощью OTP, заключается в том, что, в отличие от статических паролей, они не уязвимы для атак с повторным воспроизведением [2, 3]. Это означает, что потенциальный злоумышленник, которому удастся записать OTP, который уже использовался для входа в службу или для проведения транзакции, не сможет злоупотребить им, поскольку он больше не будет действительным. Исследования показывают, что сочетание метода генерации одноразового пароля с биометрией образует железные ворота, через которые сложно проникнуть из-за баллистической природы этих измерений [4].

Фактор аутентификации

1. Однофакторная аутентификация

Наиболее популярным методом аутентификации является комбинация имени пользователя и пароля.

Одним из основных недостатков однофакторной аутентификации является вместо использования надежных паролей многие люди выбирают простые. Фишинговые атаки могут быть вызваны чрезвычайно простыми паролями, такими как имя пользователя, дата рождения и т. д. Пароли больше не являются достаточными для защиты данных, к которым осуществляется доступ и которые передаются через Интернет, из-за их многочисленных недостатков [1, 5, 6].

2. Двухфакторная аутентификация

Повышает безопасность за счет интеграции фактора личного владения, который может включать в себя безопасный токен, использующий одноразовый пароль (OTP), с репрезентативными данными (комбинация имени пользователя и пароля), может быть получен из трех различных видов групп факторов: Фактор владения: предмет, принадлежащий пользователю, например, мобильный телефон. Фактор знания: все, что знает пользователь, например, пароль. Биометрический фактор – это аспект поведения пользователя или биометрии [1, 5].

3. Многофакторная аутентификация (MFA)

MFA обычно включает в себя уникальные биологические характеристики пользователя, такие как сканирование отпечатков пальцев или радужной оболочки глаза, поскольку они часто очень точны при их создании и использовании [4]. Это способ предложить повышенный уровень безопасности для защиты безопасности компьютерного оборудования и других жизненно важных служб от несанкционированного доступа путем объединения по крайней мере трех типов учетных данных [5].

Одноразовый пароль (One-Time Password, OTP) – это способ аутентификации, при котором пользователю выдается уникальный пароль, который можно использовать только один раз для входа в систему или подтверждения личности [6].

Этот метод обеспечивает дополнительный уровень безопасности, так как пароль действителен только в течение одного сеанса входа. Когда он использован, он больше не действителен, что делает его невозможным для повтор-

ного использования злоумышленниками. Это автоматически сгенерированная числовая или буквенно-цифровая строка символов, которая аутентифицирует пользователя для одной транзакции или сеанса входа [4]. Одноразовые пароли усиливают существующие системы идентификации и паролей, добавляя в них динамически генерируемые идентификационные данные. Токены OTP генерируют PIN синхронно или асинхронно, это зависит от их поставщика. Синхронные токены для создания одноразового пароля используют приватный ключ пользователя и текущее время.

Механизм одноразового пароля

1. Запрос кода: когда пользователь пытается войти в учетную запись или совершить транзакцию, система запросит одноразовый пароль (OTP) в качестве дополнительного шага проверки [2, 3].

2. Отправить код: после запроса система отправит OTP-код на устройство, зарегистрированное пользователем. Способы доставки могут быть через SMS, электронную почту или специальные приложения аутентификации [2, 4, 5].

3. Проверка кода: пользователям будет предложено ввести полученный OTP-код в предоставленную колонку. Затем система проверит, является ли введенный код правильным или нет [2, 3].

4. Доступ одобрен: если введенный код совпадает с отправленным системой, то доступ к учетной записи или транзакции будет одобрен. Однако, если код неправильный или недействительный, доступ будет отклонен [3].

Создание и распределение OTP

Специфика конкретных алгоритмов OTP сильно различается. Ниже приведен список нескольких методов создания OTP:

1. На основе синхронизации времени между сервером аутентификации и клиентом, предоставляющим пароль (OTP действительны только в течение короткого периода времени) [2, 5].

2. Использование математического алгоритма для генерации нового пароля на основе предыдущего пароля (OTP фактически представляют собой цепочку и должны использоваться в предопределенном порядке) [2, 5].

3. Использование математического алгоритма, где новый пароль основан на вызове (например, случайном числе, выбранном сервером аутентификации или данными транзакции) и/или счетчике [5].

Биометрия: это отрасль науки, которая занимается количественными исследованиями популяции и ее разнообразия на основе измерений характери-

стик биологических организмов. Такие расследования направлены на классификацию и описание лиц и могут использоваться для проверки или идентификации людей для защиты различных ресурсов, отличают его от других методов отсутствием необходимости запоминать пароль или другие предметы и символы, позволяющие получить доступ к ресурсам, повышенная безопасность (позволяет использование биометрических данных для защиты от некоторых атак, таких как фишинг), и их невозможно забыть или потерять [7]. Существует две подкатегории биометрии: физиологическая биометрия и поведенческая биометрия. В физиологической биометрии для подтверждения идентификации используются физические черты тела человека, такие как лицо, отпечатки пальцев, вены или радужная оболочка глаз. Физиологическая биометрия и поведенческая биометрия могут использоваться с фактором одноразового пароля либо путем генерации случайного пароля на основе этих измерений, либо с использованием его в качестве дополнительного фактора, поскольку этот процесс считается многофакторной аутентификацией [6, 7, 8].

Создание паролей-ключей с использованием характеристик отпечатков пальцев

Поскольку механизм одноразового пароля также является программой, он запрограммирован на случайность, но случайность нарушается через определенный промежуток времени, и пароли становятся предсказуемыми, поэтому механизмы одноразовых паролей имеют недостаток, заключающийся в необходимости обмена модулями токенов OTP через определенный промежуток времени. Чтобы преодолеть такие недостатки, есть исследование, представляющее метод создания ключей одноразового пароля в клиентах OTP с использованием характеристик отпечатков пальцев, а на рисунке 1 показан процесс создания ключа пароля. Из характеристик этого исследования, на которые следует обратить внимание, следует обратить внимание на то, что токен OTP не располагается на сервере OTP, а находится на стороне клиента OTP для снижения накладных расходов сервера OTP. Процесс создания ключа пароля начинается с того, что пользователь сканирует свой отпечаток пальца, как показано в (a) рисунка 6. Отсканированный отпечаток пальца не используется для аутентификации. Диапазон этого исследования начинается после завершения процесса аутентификации и не связан с аутентификацией. Однако еще одним преимуществом является то, что его можно использовать вместе с другой системой аутентификации. Существующие системы аутентификации могут быть добавлены к этому исследованию для создания нового сильного токена OTP. Как показано в (b) рисунка 6, клиент OTP может использовать отпечаток пальца пользователя для извлечения информации о его характери-

стиках. (c) рисунка 6 показывает процесс случайного выбора точек характеристик простого числа с помощью извлеченной информации о характеристиках отпечатка пальца. (d) рисунка 6 показывает процесс создания комбинации перестановки с использованием выбранного простого числа по порядку, а (e) рисунка 6 показывает создание ключей OTP с использованием циклической перестановки. (d) рисунка 6 создает временные бесконечные ключи пароля OTP для одного сеанса. Бесконечные временные пароли OTP могут быть созданы, поскольку он использует характеристики циклической перестановки [3, 4].

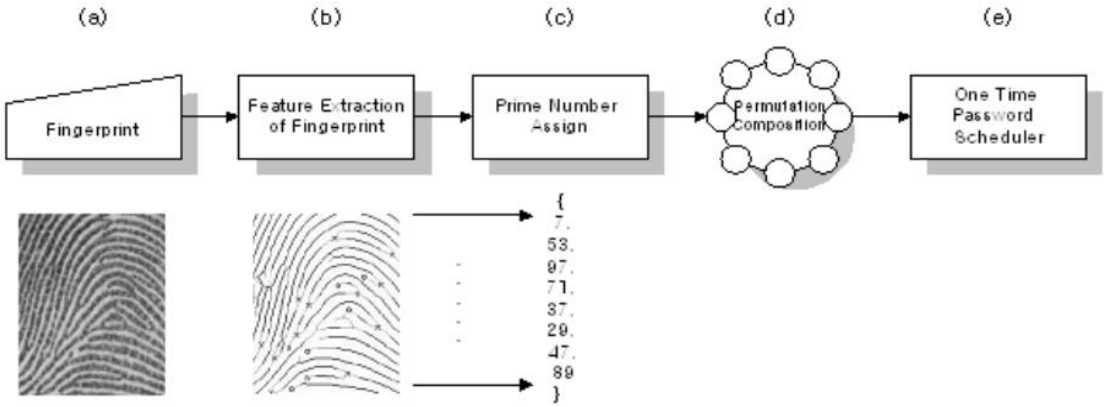


Рис. 6. Парольный ключ процесс создания OTP

Список используемых источников

1. Maria P., Leandros M., Nick A. Modern Authentication Methods: A Comprehensive Survey // IntechOpen. 2022. № 2. PP. 1–24.

2. Devendra K. One Time Password Security Security System // International Journal of Advance Research and Development, 2020. № 2. PP. 40–46.

3.Chun Y. H., Shang P. M., Kuan T. C. Using one-time passwords to prevent password phishing attacks // Journal of Network and Computer Applications, 2022. № 34. PP. 1292–1301.

4. Varasiddhi J. G., Yashwanth P. V., Srinidhi V. B., Ramesh T. K. Smart Door Using Biometric NFC Band and OTP Based Methods // International Conference for Emerging Technology (INCET), 2020. № 3. PP. 60–64.

5. Swagatam B., Hafizul I. Quantum-attack-resilience OTP-based multi-factor mutual authentication and session key agreement scheme for mobile users // Computers and Electrical Engineering, 2024. № 119. PP. 1120–1141.

6. Красов А. В., Альотум Ю., Ушаков И. А. Аутентификация и идентификация пользователя с использованием биометрической динамики нажатия клавиш на основе «манхэттенского и евклидовского расстояния» // Вестник, 2023. № 4. С. 49–56.

7. Alotoum Y. M. A. A. Biometric and behavioral authentication and soft biometrics using keystroke and mouse dynamics // ICAIT. 2023. № 1. PP.70–75.

8. Альотум Ю. М. А. А., Пешков А. И. Пат. 2024664769 Свидетельство о государственной регистрации программы для ЭВМ Российская Федерация. Программа по многофакторной аутентификации пользователей на основе биометрических динамических методов. – № 2024663318: заявл. 11.06.2024; опубл. 24.06.2024.

Alotoum Y. M. A. A. **ONE-TIME PASSWORD METHOD IN FACTOR AUTHENTICATION MECHANISM AND ITS POSSIBLE USE IN BIOMETRIC SYSTEM.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Internet security is becoming the latest important issue along with the widespread use of technology. Weakness of any part leads to fatal result for the whole security system. Therefore, security systems require careful development and mutual coordination in each element. Random one-time password generation system has been studied and integrated with biometric system to enhance security and protect user data.

Key words: One-time password, Authentication factors, Biometric system, Fingerprint, MFA.

УДК 004.42
ГРНТИ 20.11.00

ИССЛЕДОВАНИЕ ТИПОВ МОДЕЛЕЙ АССИМИЛЯЦИОННОЙ ПАМЯТИ ДЛЯ ВЫРАБОТКИ КОГНИТИВНЫХ ФУНКЦИЙ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Х. С. Амалиев
Санкт-Петербургский Государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Системы защиты информации приобретают все большее значение в свете стремительного роста объемов данных и возрастания числа угроз безопасности. В данной ситуации ассимиляционная память и связанные с ней модели становятся основополагающими для формирования когнитивных функций, которые необходимы для обеспечения надежной безопасности.

Цель данной работы – изучить различные типы моделей ассимиляционной памяти и исследовать их применение в современных системах защиты информации.

ассимиляционная память, защита информации, системы защиты информации

Виды моделей ассимиляционной памяти

Нейронные сети. Нейронные сети, включая сверточные (CNN) и рекуррентные (RNN), широко используются для анализа больших объемов данных в сфере информационной безопасности. Их ключевая особенность – способность распознавать сложные закономерности, что делает их эффективным инструментом для своевременного выявления угроз и аномалий в динамических системах [1].

Сверточные сети демонстрируют высокую результативность при анализе визуальной информации или графиков сетевой активности, помогая обнаруживать вредоносные программы. В то же время рекуррентные сети идеально подходят для обработки временных последовательностей данных.

Индуктивные модели. Модели, основанные на индуктивных подходах, играют важную роль в автоматическом выявлении структур и закономерностей внутри данных. Эти инструменты ценны для систем, работающих в условиях изменчивой среды, где требуется быстрое распознавание новых угроз. Алгоритмы индуктивного обучения помогают моделировать пользовательское поведение, что дает возможность обнаруживать аномальные действия и потенциальные атаки.

Машинное обучение. Методы машинного обучения, такие как деревья решений и алгоритмы опорных векторов, активно применяются в задачах клас-

сификации сетевых событий. Эти подходы отличаются способностью быстро идентифицировать известные угрозы и адаптироваться к новым типам атак при наличии достаточного объема обучающих данных [2].

Анализ лучших и слабых сторон

В рамках исследования были выделены наиболее успешные и наименее эффективные примеры использования ассимиляционной памяти для обеспечения безопасности информации.

Успешные. К числу наиболее успешных примеров относятся глубокие нейронные сети, которые благодаря обучению на больших данных демонстрируют способность оперативно реагировать на новые угрозы и предоставлять точные прогнозы. Ансамблевые методы, такие как Random Forest, также показывают высокую точность в классификации сетевых аномалий.

Слабые. Наименее эффективными оказались простейшие классификационные модели, такие как Naive Bayes, которые не справляются с многосложными задачами, включающими широкий спектр данных и возможных угроз [3]. Кроме того, модели, обученные на нерепрезентативных данных, часто оказываются неэффективными, что увеличивает риск успешных кибератак.

Основные направления исследования

В исследовании будут использоваться модели нейронных сетей с акцентом на следующие аспекты.

Адаптивность. Это свойство, отражающее способность сети подстраиваться под новые входные данные. Планируется применять комбинированные подходы, объединяющие сильные стороны различных архитектур для повышения уровня адаптации.

Производительность. Особое внимание будет уделено эффективности работы сетей при анализе больших массивов данных. Разрабатываются подходы, минимизирующие затраты вычислительных ресурсов при сохранении высокой точности.

Создание тестовых сценариев. Разработка критериев оценки эффективности моделей в различных условиях станет одним из ключевых этапов. При этом будут рассмотрены методы проверки и подтверждения достоверности полученных результатов.

Изучение разнообразных моделей ассимиляционной памяти открывает новые горизонты для улучшения защиты данных, а также их интеграции с передовыми подходами в обработке больших данных.

Осознание сильных и слабых сторон разных подходов не только позволит усовершенствовать текущие системы безопасности, но и создаст более эффективные стратегии для защиты данных в будущем.

В дальнейшем исследование будет сосредоточено на оптимизации применения ассимиляционной памяти, что поможет в более эффективном обнаружении и предотвращении угроз в цифровом пространстве.

Список используемых источников

1. Штеренберг С. И. Разработка методологии защиты системы искусственного интеллекта в распределенных информационных системах / С. И. Штеренберг // Вестник СибГУТИ. 2023. Т. 17, № 3. С. 78-86. DOI 10.55648/1998-6920-2023-17-3-78-86.
2. Ушаков И. А. Безопасность передачи данных в территориально распределенных информационных системах в офтальмологии на базе отечественного оборудования / И. А. Ушаков, Р. И. Дементьев, Д. Я. Держко // Офтальмохирургия. 2022. № S4. С. 108-114. DOI 10.25276/0235-4160-2022-4S-108-114.
3. Штеренберг, С. И. Разработка методики внедрения скрытой подписи кода в Gitlab / С. И. Штеренберг, Ю. С. Данилова // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. № 3. С. 44-49. DOI 10.46418/2079-8199_2022_3_6.

Amaliev H. **STUDY OF TYPES OF ASSIMILATION MEMORY MODELS FOR DEVELOPING COGNITIVE FUNCTIONS OF INFORMATION SECURITY SYSTEMS**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Information security systems are gaining increasing importance in light of the rapid growth in data volumes and the rise in cyber threats. In this context, assimilation memory and related models become fundamental for the development of cognitive functions essential for ensuring reliable security.

The purpose of this work is to study various types of assimilation memory models and explore their applications in modern information security systems.

Key words: assimilation memory, information security, security systems.

УДК 004.056
ГРНТИ 81.93.29

РАЗГРАНИЧЕНИЕ ДОСТУПА В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ РАСПРЕДЕЛЕННЫХ ИСПДн

Э. В. Бирих, Д. В. Сахаров, М. А. Теряев
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире облачные технологии занимают центральное место в обеспечении гибкости, масштабируемости и эффективности информационных систем персональных данных (ИСПДн). Существенным элементом управления облачной инфраструктурой становится безопасность, особенно в контексте надежной идентификации и аутентификации пользователей и вычислительных узлов. Разграничение доступа к защищенным зонам и поддержание высокого уровня доступности представляют собой ключевые задачи для любой облачной среды распределенных ИСПДн.

облачная инфраструктура, системы идентификации, информационная безопасность

Введение. В условиях стремительного прогресса информационных технологий облачные решения становятся важной составляющей инфраструктуры множества организаций, предоставляя им гибкость, возможность масштабирования и высокую эффективность. Все это относится к обеспечению ИСПДн. Одной из основных задач управления облачными системами является обеспечение ИБ, особенно в аспекте надежной идентификации пользователей. Обеспечение защищенного доступа к жизненно важным ресурсам и поддержание высокого уровня доступности остаются приоритетными задачами для каждой облачной платформы.

Цель работы. Предложить надежную идентификацию пользователей в распределенных ИСПДн и рассчитать эффективность ее общей производительности и доступности (OPA), вероятность которого должна превышать значение 0,9.

Решение. В основе облачной инфраструктуры лежат аппаратные и программные ресурсы, которые объединяются благодаря виртуализации. Эта технология дает возможность разделять физические ресурсы на множество независимых виртуальных машин, каждая из которых функционирует как отдельный ресурс.

Основными элементами облачной инфраструктуры являются вычислительные мощности (предоставление виртуальных машин или контейнеров), хранилище данных (облачные базы данных, распределенное хранение), сете-

вые компоненты (балансировщики нагрузки, сетевые протоколы) и программное обеспечение, которое управляет распределением и выделением ресурсов.

Централизованная система представляет собой модель, в которой управление и обработка данных сосредоточены в одном месте или через единый центральный узел. В такой архитектуре центральный сервер отвечает за хранение данных и управление сетевыми функциями, в то время как подключенные клиенты или терминалы в основном осуществляют ввод и вывод информации. Это означает, что все пользовательские данные находятся в одном месте, что упрощает контроль доступа и управление безопасностью. [1, 2]

Централизованные системы применяют различные методы шифрования и другие технологии безопасности для защиты конфиденциальности данных. Благодаря этой структуре они способны обеспечивать высокий уровень защиты, эффективно противодействуя потенциальным угрозам безопасности информации [3–5].

Тем не менее, централизованная модель имеет и свои недостатки. Один из основных недостатков – это уязвимость к отказам центрального узла. Если центральный сервер выходит из строя, вся система может стать недоступной, что может привести к серьезным потерям данных и ухудшению качества предоставляемых услуг. Кроме того, централизованные системы могут испытывать трудности с масштабируемостью, поскольку нагрузка на центральный узел увеличивается с ростом числа пользователей и объема обрабатываемой информации. Это может потребовать дополнительных ресурсов и изменений в инфраструктуре для поддержания стабильной работы.

С точки зрения безопасности, несмотря на высокий уровень защиты конфиденциальности, централизованные системы привлекают внимание киберпреступников. Сосредоточение данных в одном месте может иметь серьезные последствия в случае успешной атаки, так как злоумышленники могут получить доступ к большому объему информации.

Таким образом, хотя централизованные системы предлагают значительные преимущества в управлении данными и обеспечении конфиденциальности, важно также учитывать и эффективно управлять их потенциальными рисками и недостатками. Это требует комплексного подхода к безопасности, включающего технические, организационные и процессные меры для обеспечения надежной и безопасной работы таких систем в различных условиях.

Децентрализованная система представляет собой модель управления и организации, в которой вычислительные ресурсы и процессы распределены между несколькими узлами, не зависящими от центрального управляющего узла. Это контрастирует с централизованными системами, где все данные обрабатываются и хранятся в одном месте. Среди преимуществ таких систем

можно выделить устойчивость к сбоям, равномерное распределение нагрузки и улучшенную масштабируемость.

Каждый узел в такой системе имеет возможность проверять и фиксировать данные, что способствует созданию надежной структуры, где данные остаются доступными даже при сбоях или атаках на отдельные элементы. Тем не менее, вопросы конфиденциальности могут оставаться проблемой [6, 7].

Для того чтобы создать универсальную облачную инфраструктуру, можно соединить две системы идентификации, централизованную и децентрализованную, чтобы получить облачную инфраструктуру с возможностью [8, 10]:

– гибкой масштабируемости;

– настройки зон с повышенной безопасностью и низкими требованиями к безопасности;

– оптимизировать затраты ресурсов;

– единого входа;

– централизованного управление доступом;

– делегированием нагрузки на узлы.

Такая гибридная инфраструктура, представленная на рисунке 1, позволяет более эффективно защищать данные и контролировать доступ к ним, обеспечивая при этом высокую степень надежности и устойчивости к сбоям и атакам.

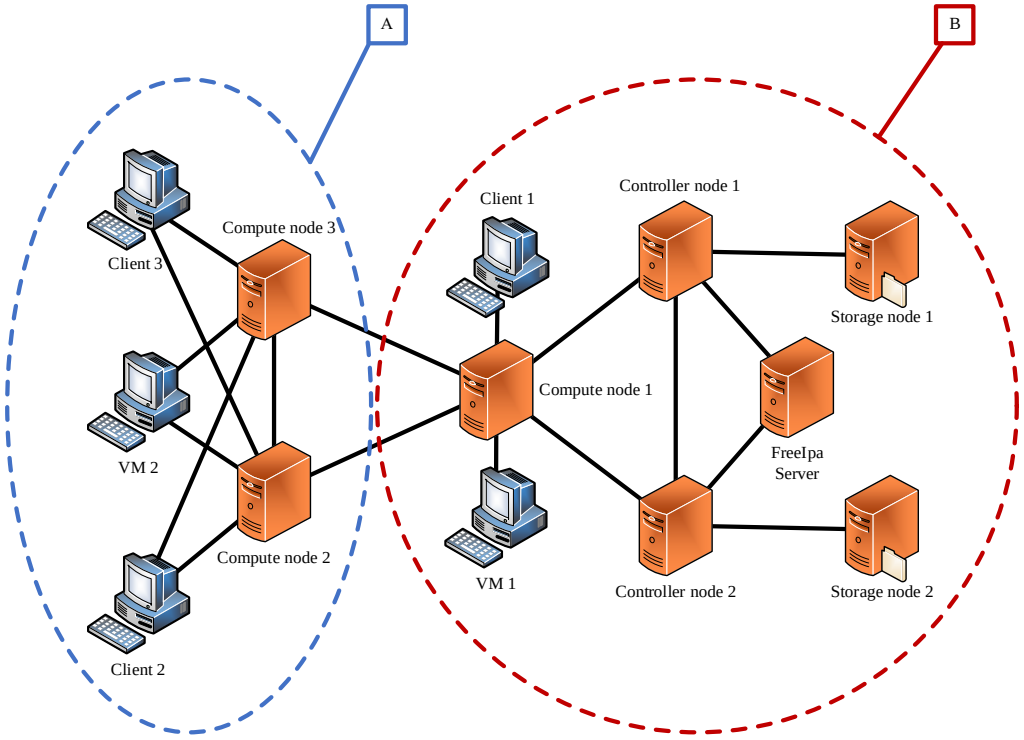


Рис. 1. Схема реализации облачной инфраструктуры

Зона А представляет собой область с низкими требованиями к безопасности, где применяется децентрализованная система. В то время как Зона Б характеризуется повышенными стандартами безопасности и использует централизованный подход.

Централизованная система обеспечивает строгие политики безопасности и удобный контроль, что облегчает администрирование, мониторинг и соблюдение нормативных требований [10,11]. Это особенно актуально для организаций, которым необходимо придерживаться жестких стандартов безопасности и регулярно проходить аудиты.

Децентрализованная система, с другой стороны, позволяет быть более гибкой и масштабируемой, что необходимо для быстрого адаптирования к изменениям технологической среде. Это позволяет легко интегрировать новые приложения и сервисы без необходимости в значительных изменениях архитектуры системы. Кроме того, такая структура повышает устойчивость к сбоям, так как распределенные компоненты снижают риски, связанные с выходом из строя отдельного узла, обеспечивая непрерывность работы даже в случае локальных сбоев.

Расчет эффективности. Для оценки эффективности облачной инфраструктуры мы применяем формулу OPA, которая учитывает три основных параметра: время безотказной работы, индекс производительности и эффективность затрат [12].

Общая производительность и доступность вычисляется по формуле 1:

$$OPA = \frac{Uptime * Performancew_Index}{Cost_Efficiency} \quad (1)$$

где Uptime – процент времени, когда система доступна и работает без сбоев (в долях от 1), Performance_Index – средняя производительность системы, измеряемая в ответном времени на запросы или скорости обработки данных (безразмерная величина), Cost_Efficiency – эффективность затрат, измеряемая как соотношение стоимости облачных услуг к предоставляемым ресурсам и производительности (безразмерная величина).

Рассматривая систему, состоящую из централизованной и децентрализованной систем, мы получим следующие данные:

– Uptime = 0.98 (система доступна 98 % времени);

– Performance_Index = 0.82 (максимальная производительность составляет 82 %);

– Cost_Efficiency = 0.74 (эффективность затрат 74 %).

Тогда расчет будет следующим:

$$OPA = \frac{0.98 * 0.82}{0.87} = \frac{0.8036}{0.87} = 0.92 \quad (2)$$

Значение OPA = 0.92 указывает на хорошую общую производительность и доступность облачной инфраструктуры. Значение выше 0.9 говорит о требуемом уровне производительности и доступности по сравнению с затратами. Значения ниже 0.9 могут свидетельствовать о необходимости улучшений в производительности, доступности и повышении затрат [12].

Метрика OPA объединяет ключевые показатели для формирования комплексной оценки эффективности облачной инфраструктуры. Она отличается простотой в расчетах и интерпретации, что делает ее полезным инструментом для управления и оптимизации облачных ресурсов.

Вывод. В результате создания гибридной облачной инфраструктуры возможно достижение требуемой безопасности, надежности и гибкости в защите ИСПДн, с обеспечением экономической эффективности и простоты администрирования. При этом расчетная эффективность материальных затрат составляет 0.74 %, а значение OPA – 0.92. Это делает возможным более эффективное управление идентификацией, доступом к ресурсам и обеспечивает устойчивость к будущим изменениям и потребностям. Такой подход рекомендуется для внедрения распределенных ИСПДн в облачные среды, где необходимы высокий уровень защиты и доступности. Цель работы достигнута.

Работа выполнена при финансовой поддержке «Грант ИБ МТУСИ» 2022 г. №10/22-к. Соглашение № 40469-10/2022-к от 30.06.2022г. в СПбГУТ им.проф. М.А.Бонч-Бруевича.

Список используемых источников

1. Barkat A., Dos Santos A. D., Ho T. T. N. Open stack and cloud stack: Open-source solutions for building public and private clouds // 2014 16th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing. IEEE, 2014. С. 429–436.
2. Миняев А. А., Красов А. В., Сахаров Д. В. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2020. № 1. С. 29–33. DOI 10.46418/2079-8199_2020_1_5. EDN ULHTJK.
3. Наседкин П. Н. Облачные технологии в рамках сервисной модели оказания услуг по информационной безопасности / П. Н. Наседкин // Молодая наука Сибири, 2019. № 2 (4). С. 41–47. EDN BDNAGK.
4. Штеренберг С. И. Методика построения поисковой системы для примитивной программы адаптивного действия // Наукоемкие технологии в космических исследованиях Земли, 2015. Т. 7. № 4. С. 52–57.
5. 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. № 2. С. 40–46.

6. Гельфанд А. М., Пестов И. Е., Смирнов Д. Н., Чумаков И. В. Преимущества Использования централизованной и децентрализованной системы индентификации для повышения уровня безопасности облачной инфраструктуры // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 235–237. EDN WAZGCE.
7. Андрианов В. И., Виткова Л. А., Сахаров Д. В. Исследование алгоритма защиты общедоступных персональных данных в информационных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2016. С. 227–231.
8. 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. VII Международная научно-техническая и научно методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 191–195.
9. Виткова Л. А., Денисов Е. И., Сахаров Д. В., Ушаков И. А. Вопросы формирования безопасной информационной системы на основе технологии децентрализованных сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 174–179.
10. Бирих Э. В., Виткова Л. А., Левин М. В., Чмутов М. В. Развитие стандартов и руководств в сфере облачных технологий // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. С. 92–95.
11. Minyaev A. A., Krasov A. V., Saharov D. V. The method and methodology of efficiency assessment of protection system of distributed information systems / // 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT 2020, Brno, 05–07 октября 2020 года. Brno: Institute of Electrical and Electronics Engineers, 2020. PP. 291–295. DOI 10.1109/ICUMT51630.2020.9222451. EDN KAGNKZ.
12. Бухарин В. В., Липатников В. А., Сахаров Д. В. Метод управления информационной безопасностью организации на основе процессного подхода // Информационные системы и технологии? 2013. № 3 (77). С. 102–109.

Birikh E., Sakharov D., Teryaev M. **ACCESS RESTRICTION IN CLOUD INFRASTRUCTURES.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the modern world, cloud technologies play a key role in ensuring flexibility, scalability and efficiency of information systems. One of the important aspects of cloud infrastructure management is security, in particular, reliable identification and authentication of users and computing nodes. Separating access to high-security zones and ensuring high levels of availability are critical tasks for any cloud environment.

Key words: cloud infrastructure, identification systems, information security.

УДК 004.738.5
ГРНТИ 81.93.29

МОДЕЛЬ ЗАЩИТЫ АССИМИЛЯЦИОННОЙ ПАМЯТИ В СРЕДАХ IOT

Г. С. Бударный, К. А. Манжула
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

В статье рассматривается модель защиты ассимиляционной памяти в средах IoT. Были рассмотрены преимущества для IoT систем с учетом использования подобных моделей, а также пункты, которые необходимы для реализации данных преимуществ. Приведена схема взаимодействия механизмов модели защиты ассимиляционной памяти, разработаны структуры ассимиляционной памяти для сред IoT.

IoT, модель защиты, ассимиляционная память, нейроаналогии, базы данных, базы знаний

Модель защиты ассимиляционной памяти в средах IoT является очень перспективной задачей, так как данная тема имеет малое количество исследований на данный момент, но при этом несет множество преимуществ для Iot систем за счет пунктов, приведенных ниже.

1. Репликация и кластеризация. Репликация и кластеризация являются важными компонентами, за счет которых возможно упорядочивать, нормализовать и агрегировать большие массивы данных, что способствует оптимизации и увеличению производительности IoT систем в сфере работы с большими данными [1].

2. Оценка взаимодействия компонентов. Данный параметр позволяет в ассимиляционной памяти выстраивать принцип противодействия угрозам, включающим в себя нарушения ИБ любого вида, так как именно данный этап служит для приведения сведений о поступающих атаках.

3. Формирование когнитивной области интеллектуальной IDS. Оно необходимо для результата моделирования защиты ассимиляционной памяти в среде IoT. Именно в когнитивной области будет происходить принятие решений, как о картах НС в целом, так и их дальнейшем формировании в частности. Далее будет происходить выработка правил обеспечения работоспособности уже децентрализованной ПНП в РИС [2].

Для самостоятельного принятия самостоятельных решений, которые будут ориентированы на борьбу с направленными атаками, интеллектуальной IDS необходимы полученные и уже накопленные оценки. Также важной зада-

чей является полноценный уход от использования оператора (человека), что даст сильный толчок, так как позволит полноценно уйти от такой проблемы, как человеческий фактор [3] , но при этом самым главным аспектом, который будет противодействовать данной задаче является то, что происходит по сути только учет новых факторов формирования хранения и обработки информации, а модель защиты ассимиляционной памяти не может существовать отдельно [4].

Таким образом мы должны наблюдать следующие свойства.

1. Способность к обучению. Первостепенным параметром является возможность к самостоятельному обучению, алгоритмы работы должны перестраиваться для наиболее эффективного обнаружения угроз, для чего и нужна способность к самостоятельному обучению [5].

2. Высокие способности к анализу и последующей обработке информации. В выявлении угрозы не менее важным фактором является время, поэтому очень важно чтобы IDS могла быстро анализировать и обрабатывать большие объемы информации, что позволит более оперативно реагировать на появление угрозы.

3. Детектирование новых угроз. Система должна быстро выявлять не только знакомые, но и новые типы угроз, что позволит также сократить временной интервал реакции.

4. Высокий уровень адаптивности. Помимо того, что система обязана быстро выявлять новые типы угроз, она также обязана в максимально короткий срок адаптироваться к изменениям как в условиях, так и видах угроз, что напрямую содействует повышению эффективности защиты информации [2].

5. Эффективность взаимодействия с другими узлами системы. Этот ключевой параметр необходим для правильной работы системы, так как только при наличии способности к координации и совместной работе с другими компонентами информационной системы можно говорить о обеспечении общей безопасности системы [4].

Для визуального восприятия взаимодействия узлов ниже приведена примерная схема взаимодействия механизмов модели защиты ассимиляционной памяти (рис. 1).

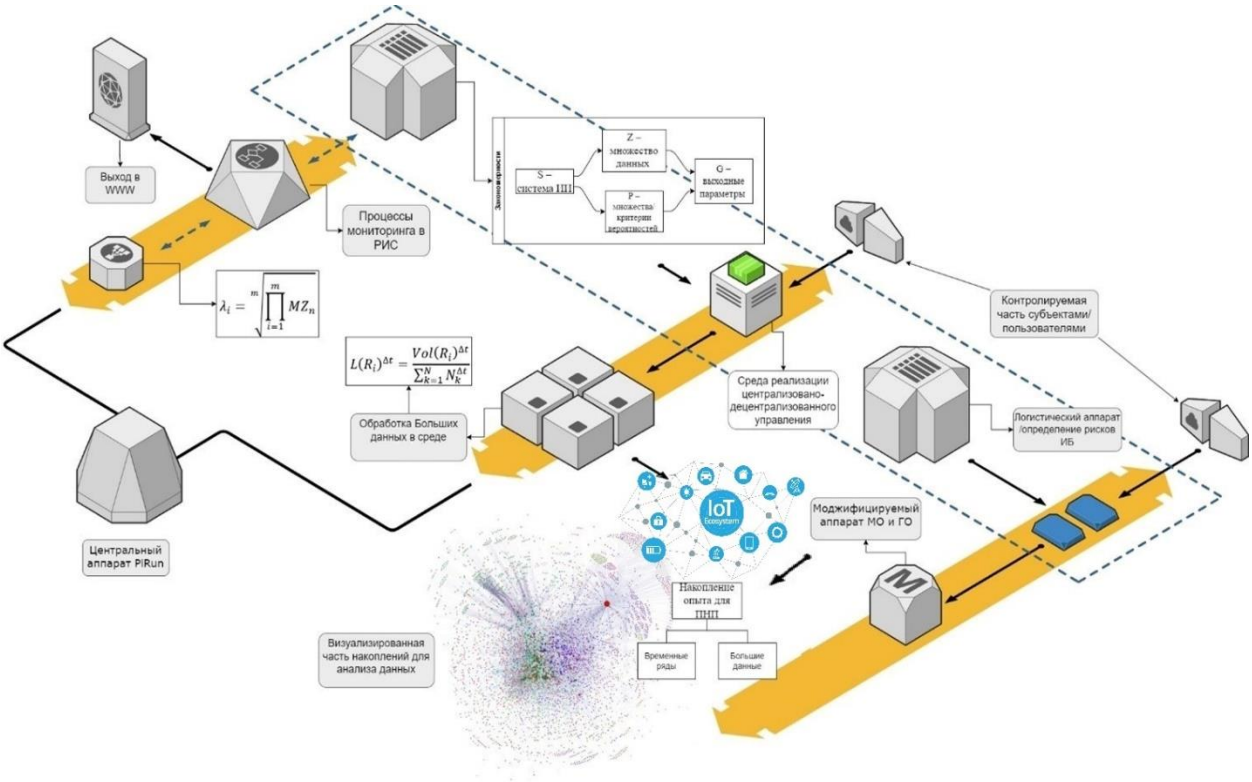


Рис. 1. Схема взаимодействия механизмов модели защиты ассимиляционной памяти

Когда идет разговор о ассимиляционной памяти важной частью является математический аспект данного вопроса, но так как на данный момент для него не существует стандартизированного решения [3] ниже представлена таблица (таблица 1) структур ассимиляционной памяти в средах IoT для схемы взаимодействия механизмов модели защиты ассимиляционной памяти (рисунок 1). Первый столбец таблицы несет информацию о предложенных ID, второй вносит такое понятия, как нейроанология – аналогия, которая наблюдается в нейронной памяти IoT систем, а третий несет в себе описание структуры в интеллектуальной IDS.

Таблица – 1 структуры ассимиляционной памяти в средах IoT

ID	Нейроалогия	Структура в интеллектуальной IDS
ATR	Доступность	Иерархичный доступ к ресурсам
NAS	Запоминание	Создание и сохранение ПА
SID	Специфичность	Отношение между ПА и ПО
INT	Целостность	Целостность ПО
DISID	Дискретность	Доступ к ПО
DEVM	Развитие	Параметры МО
DEVG		Параметры ГО
OOR	Открытость	Открытость ресурсов
RIS	Возможность обмена и взаимодействия между нейронами	Взаимодействие с рабочими компонентами РИС
DTR	Обмен данными путем нейроимпульсов	Перенос информации
VR	Изменчивость	Потенциальные изменения переносимых данных
CopYR	Распространение	Механизмы копирования и распространения информации
KIIS	*Отсутствует*	Набор механизмов для внутреннего изменения структур
RISDTN	Взаимодействия с различными отделами памяти	Взаимодействие на уровне сетей передачи данных
AAT	Импульсность	Реакции на атаки и угрозы
TimeID	*Отсутствует*	Отметка времени захвата пакета
DTime	*Отсутствует*	Продолжительность потока
BPSTime	*Отсутствует*	Числовой показатель байт в потоке
PPSTime	*Отсутствует*	Числовой показатель пакетов в потоке
AVP	*Отсутствует*	Средний размер пакета
MinPP	*Отсутствует*	Минимальная длина пакета
MaxPP	*Отсутствует*	Максимальная длина пакета
APP	*Отсутствует*	Средняя длина пакета
ATPP	*Отсутствует*	Среднее значение длины активности потока
ASPP	*Отсутствует*	Допустимое отклонение активности потока (секунды)
ASPPMax	*Отсутствует*	Верхняя метка активности потока
ASPPMin	*Отсутствует*	Нижняя метка активности потока
AMean	*Отсутствует*	Время простоя потока
ASdtime	*Отсутствует*	Стандартное отклонение времени простоя потока
STMax	*Отсутствует*	Верхняя метка простоя потока
STMin	*Отсутствует*	Нижняя метка простоя потока
NAA	*Отсутствует*	Отметка типа потока (стандартный поток/атака)

Заключение

Данное исследование направлено на получение компонентов для НС-структур. Имеет смысл в наполнении сведений БД и БЗ. В ходе разработки были спроектированы сами структуры имеющие дальнейшее применение в ассимиляционной модели организации памяти НС структур. Результатом исследования будет являться условный уход от границ между БД и БЗ, что происходит за счет минимизации переходов и ускоренной обработки запросов. Так же в дальнейшем рассмотрение данного тезиса послужит надежной средой для изучения свойств BigData и SmallData.

Список используемых источников

1. Гельфанд А. М., Казанцев А. А., Красов А. В., Орлов Г. А. Оценка рисков и угроз безопасности в среде "умный дом" // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Том 1. С. 316–321. EDN HIGZYQ.
2. Гельфанд А. М., Казанцев А. А., Красов А. В., Орлов Г. А. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Том 1. С. 321–326. EDN GYBXPT.
3. Калинин М. О. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения / М. О. Калинин, С. И. Штеренберг // Интеллектуальные технологии на транспорте. 2018. № 3 (15). С. 47–54. EDN MITIHZ.
4. Красов А. В., Ягудин И. Р. Анализ активных сетевых атак: arp-spoofing и dns-spoofing // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. Том 1. С. 520–526.
5. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности: учебное пособие. СПб.: СПбГУТ, 2012. 396 с.

Bydarniy G., Manzhula K. **AN ASSIMILATION MEMORY PROTECTION MODEL IN IOT ENVIRONMENTS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article discusses the model of assimilation memory protection in IoT environments. The advantages for IoT systems were considered, taking into account the use of such models, as well as the points that are necessary to implement these advantages. The scheme of interaction of the mechanisms of the assimilation memory protection model is presented, the structures of assimilation memory for IoT environments are developed.

Key words: IoT, protection model, assimilation memory, neuroanalogies, databases, knowledge bases.

УДК 004.056; 004.413
ГРНТИ 81.93.29

АВТОМАТИЗИРОВАННЫЕ СРЕДСТВА ДЛЯ ПОДДЕРЖКИ РАЗРАБОТКИ БЕЗОПАСНЫХ ПРОГРАММНЫХ ПРОДУКТОВ

К. Н. Бусыгин, И. М. Егоров, В. С. Зурахов, Е. И. Чалова
Санкт-Петербургский государственный университет промышленных технологий и дизайна

Перед командой разработки нового программного продукта в настоящее время стоит не только традиционная задача по выстраиванию процессов качественной реализации требуемого пользователям функционала, но и процессов, поддерживающих высокий уровень информационной безопасности получившегося решения, на что расходуется большая доля сил сотрудников. Для снятия нагрузки предлагается ряд инструментов автоматизации процессов безопасности, заимствованных из методики DevSecOps, таких как SAST, DAST, SCA, Secret Detection, WAF, RASP.

проектирование и разработка ПО, информационная безопасность, DevSecOps

Обеспечение безопасности разрабатываемого нового программного комплекса ставит перед разработчиками задачи выявления и нейтрализации уязвимостей информационной безопасности [1] на протяжении всего жизненного цикла (ЖЦ) продукта. Подход к обеспечению безопасности должен носить комплексный и системный характер, что подразумевает даже при высоком уровне автоматизации процессов создания ПО непосредственное активное участие сотрудников в выполнении множества обязательных процедур, в свете чего переложение рутинных задач информационной безопасности на специализированное программное обеспечение становится особенно актуальным.

Вне зависимости от модели жизненного цикла ПО, применяемой командой разработки, полезно перенять некоторые лучшие методики для использования в проекте. В процессе работы над созданием продукта можно выделить следующие обобщенные этапы, которые в различных моделях ЖЦ могут быть по-своему представлены во времени и деталях реализации, но суть которых неизменна [2]:

1) определение потребности клиента в некоторой функциональности;

2) определение функциональных и нефункциональных требований к продукту, составление графика работ;

3) построение архитектуры проекта, используемых технологий, кодирование, построение интеграций, дебаг;

4) разработка системы тестирования продукта, тестирование выполнения функциональных и нефункциональных требований, приемочное тестирование;

5) доставка продукта пользователю, работа с обратной связью, вывод из эксплуатации.

Система безопасной разработки продукта должна прорабатываться с самого первого этапа и органично вписываться в основной конвейер разработки. В настоящее время хорошо проявившей себя и зрелой методикой проявил себя DevSecOps [3], опыт автоматизации операций которого можно частично распространить на другие модели проектирования ПО. Согласно этой методике, на каждом обобщенном этапе можно выделить, например, следующие способы обеспечения безопасности:

1) Threat Intelligence, исследование инцидентов в индустрии;

2) моделирование угроз, управление рисками, определение требований регулирующих органов;

3) изучение требований, стандартов и лучших практик, сканирование уязвимостей зависимостей, ревью безопасности кода, статический анализ кода;

4) динамический анализ кода, тестирование на проникновение;

5) Threat Intelligence, поддержка клиентов, управление уязвимостями, Web-Application Firewall и Runtime Application Self-Protection.

Из приведенных способов в данной работе будут выбраны и рассмотрены те, которые помогут автоматизировать часть работы по созданию и развитию безопасного программного продукта. Для создания последнего используется широкий ряд технологий, но здесь внимание будет уделено только серверной части продукта, на которую ляжет основная нагрузка по обеспечению информационной безопасности. Языком реализации выбран Java, база данных – PostgreSQL, для построения конвейера развертывания – GitLab.

Конвейер включает стандартные этапы разработки программ, которые дополняются дополнительными этапами, настроенными на запуск инструментов, реализующих следующие технологии [4]:

– SAST;
– DAST;
– SCA;
– Secret Detection;
– WAF;
– RASP.

Далее будут приведены краткие характеристики перечисленных методов и их инструментальные альтернативы.

SAST (static application security testing) – это процесс тестирования «белого ящика» приложения на наличие ошибок и уязвимостей в исходном коде. В процессе работы такие инструменты на первом этапе строят обобщенную модель кода, например, абстрактное синтаксическое дерево (причем это позволяет инструменту поддерживать разные языки программирования), а на втором производится поиск дефектов путем применения различных семантических, структурных и прочих правил («из коробки» или заданных вручную) к смоделированному коду.

Статический анализ может находить такие дефекты как:

– скрытые уязвимости;
– логические ошибки;
– ошибки архитектуры;
– дефекты реализации;
– «мертвый» код;
– наличие «закладок»;
– отклонение от стандартов кодирования.

Инструментов статического анализа создано множество, универсальные или под конкретные языки и платформы. Средства отечественного изготовления поставляют такие компании как Positive Technologies (PT Application Inspector) и PVS-Studio.

Очень удобной возможностью является встраивание технологии в среду разработки в виде плагина, как, например, SpotBugs, который используется для аудита Java кода.

GitLab поддерживает SAST для проектов на Java, используя собственный Advanced SAST analyzer.

DAST (Dynamic application security testing) – методика тестирования «черного ящика», которая позволяет определить уязвимости и слабости работающего приложения посредством отправки ему пакетов данных с потенциально вредоносной нагрузкой. Инструменту необходимо предоставлять экземпляр запущенного приложения в тестовой среде, максимально приближенной к боевой, иначе будет увеличиваться риск ложных срабатываний.

Методика позволяет обнаружить такие недостатки как:

– недекларированное поведение;
– утечки памяти;
– ошибки валидации данных;
– ошибки аутентификации;
– недостатки конфигурации сервера;
– возможность переполнения буфера;
– уязвимость к SQL-инъекции и т. д.

Инструменты этого класса не привязаны к языку или платформе, на которой ведется разработка продукта, потому как опираются на стандарты определения API и особенности используемых инфраструктурных компонентов. Среди представителей – AppScan, BurpSuit, Acunetix, известный и распространенный OWASP ZAP. GitLab имеет хорошую интеграцию с последним или через отдельный настроенный этап конвейера в Ultimate версии, или через подробную документацию по настройке.

IAST (Interactive Application Security Testing) сочетает в себе преимущества предыдущих технологий, предоставляя возможность тестирования методом «серого ящика», что повышает точность динамического анализа с помощью дополнительного анализа исходного кода приложения, выполняющегося в данный момент.

Представители, например, Synopsys Seeker, Veracode Interactive Analysis, Checkmarx CxIAST, Contrast Assess, PT Application Inspector.

SCA (Software composition analysis, контроль open-source) – набор технологий, которые анализируют зависимости приложения от сторонних компонентов и выявляют среди них устаревшие, открытые к известным уязвимостям и эксплойтам.

Может применяться для:

– контроля библиотек в зависимостях (транзитивных в том числе);

– нахождения известных уязвимостей в open-source;

– определения лицензионных ограничений;

– мониторинга новых уязвимостей в зависимостях.

Существует множество проприетарных в основном облачных решений (например, CodeScoring, Sonatype, Nexus, WhiteSource). Для начала разработки и построения первоначального конвейера может подойти OWASP Dependency-Check – бесплатная версия инструмента. GitLab предоставляет собственный Dependency Scanning для подписки Ultimate.

Secret Detection – технология анализа кода приложения, предотвращающая раскрытие аутентификационных данных для доступа к сторонним сервисам (или информирующая об этом факте) при опубликовании кода приложения в репозиторий системы контроля версий. Чаще всего инструмент предоставляется как часть конвейера развертывания приложения.

GitLab предоставляет возможность безвозмездного использования этой технологии.

RASP (Runtime Application Self-Protection) – это технология, которая использует инструментацию времени исполнения для распознавания и предотвращения компьютерных атак, получая необходимую для работы информа-

цию от работающего приложения. Нет большого различия этой RASP и IAST, в основном в этапе жизненного цикла времени работы инструмента.

Может использоваться для:

– предотвращения эксплуатации уязвимостей в реальном времени;

– завершения пользовательской сессии в случае угрозы;

– завершения работы всего приложения в критичных случаях;

– уведомления персонала или пользователя о тревогах.

Среди известных инструментов для экосистемы Java можно выделить Hdiv Protection, Waratek, Veracode Runtime Protection, Imperva RASP, Contrast Security. На российском рынке подобные решения предлагают Positive Technologies и Код Безопасности.

Для схожих целей использован Web Application Firewall (WAF) и Web Application and API Protection (WAAP), отличие которого в том, что он не так сильно связан с приложением, а используется в качестве посредника безопасности, и может быть расположен на другой вычислительной машине. В качестве примера можно привести CloudGuard AppSec от Check Point, продукты от Wallarm. На российском рынке также представлены Positive Technologies и Код Безопасности.

Корректное использование приведенных технологий и инструментов может повысить уровень защищенности разрабатываемого приложения на всех этапах жизненного цикла посредством автоматизации ряда задач информационной безопасности.

Список используемых источников

1. ГОСТ Р 56939–2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования». М.: Стандартинформ, 2018.
2. ГОСТ Р ИСО/МЭК 12207–2010 «ПРОЦЕССЫ ЖИЗНЕННОГО ЦИКЛА ПРОГРАММНЫХ СРЕДСТВ». М.: Стандартинформ, 2011.
3. Каждая третья российская компания уже строит процессы безопасной разработки. URL: https://www.securitylab.ru/analytics/532833.php (дата обращения 11.11.2024).
4. Derek Fisher. Application Security Program Handbook. NY: Manning Publications Co, 2022. 297 p.

Busygin K., Egorov I., Zurakhov V., Chalova E. **AUTOMATED TOOLS TO SUPPORT THE DEVELOPMENT OF SECURE SOFTWARE PRODUCTS.**

Saint Petersburg State University of Industrial Technologies and Design

The team of developing a new software product currently faces not only the traditional task of building processes for the high-quality implementation of the functionality required by users, but also processes that support a high level of information security of the resulting solution, which consumes a large proportion of employees' efforts. To relieve the load, a number of security process automation tools are offered, borrowed from the DevSecOps methodology, such as SAST, DAST, SCA, Secret Detection, WAF, RASP.

Key words: software engineering, software development, information security, DevSecOps.

УДК 621.396.99
ГРНТИ 81.93.29

КЛЮЧЕВЫЕ МОМЕНТЫ ЗАЩИТЫ КОРПОРАТИВНОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

К. Н. Бусыгин, И. Н. Егоров, В. С. Зурахов, Е. И. Чалова
Санкт-Петербургский государственный университет промышленных технологий и дизайна

Требования по защите сетевой инфраструктуры крупной компании постоянно модернизируются в современном мире, это влечет за собой обновление ПО и сетевой аппаратной инфраструктуры. Однако, ключевые моменты остаются неизменными в течение относительно продолжительных периодов.

защита сетевой инфраструктуры, ИБ, корпоративные системы, пользовательский доступ

Введение

Обеспечение непрерывной работы критически важных систем и минимизация рисков атак на корпоративную сеть – это ключевые задачи для отдела информационной безопасности (ИБ) в любой компании. Одним из наиболее эффективных подходов к решению этих вопросов является ограничение полномочий пользователей систем.

С точки зрения ИБ, критически важные системы обладают двумя основополагающими свойствами – целостностью и доступностью, от которых зависит их бесперебойная работа. Для защиты корпоративной сети от атак необходимо снижать «поверхность атаки», сокращая количество устройств и сетевых сервисов, доступных извне, и обеспечивая защиту тех систем и сервисов, которым такой доступ действительно нужен, например, веб-сервисов, шлюзов, роутеров и рабочих станций. В частности, компьютеры пользователей, подключенные к интернету, представляют собой один из основных векторов атак на корпоративную сеть.

Для эффективной защиты критически важных систем от несанкционированных изменений и снижения возможности атак на корпоративную сеть необходимо выполнить следующие шаги:

1. Определить объекты (оборудование, системы, бизнес-приложения, важные документы и т. д.), требующие защиты в корпоративной сети.

2. Описать бизнес-процессы компании и, исходя из них, установить уровни доступа к защищаемым объектам.

3. Обеспечить уникальность учетных записей для каждого субъекта (пользователя или корпоративного приложения).

4. Максимально ограничить доступ субъектов к объектам, то есть установить четкие права доступа в рамках бизнес-процессов.

5. Убедиться, что все действия субъектов с объектами логируются, а логи надежно хранятся.

В современных корпоративных сетях ситуация выглядит следующим образом:

– все важные корпоративные документы хранятся в централизованном формате, в общих папках на одном из серверов компании, например, на сервере с функцией контроля содержания документов;

– доступ к критически важным системам ограничен только для администраторов. Это позволяет им, в случае сбоя, оперативно подключаться к системе удаленно и устранять неполадки;

– в некоторых случаях администраторы могут использовать общую учетную запись, что создает определенные риски;

– учетные записи рядовых сотрудников имеют минимальные права «обычного пользователя», однако, при необходимости, они могут быстро получить права локального администратора.

Технически, защита критических систем значительно проще, чем защита рабочих станций. Это связано с тем, что изменения в бизнес-процессах происходят редко, регламенты остаются стабильными, и можно детально проработать все аспекты безопасности. В отличие от этого, рабочее окружение пользователей характеризуется хаосом: процессы меняются стремительно, и вместе с ними меняются требования к безопасности.

К тому же, многие пользователи относятся с недоверием или даже негативом к ограничениям, даже если они не затрагивают их рабочие процессы. В результате, традиционный подход к защите пользователей зачастую строится на принципе «лучше пропустить вредоносное ПО, чем заблокировать что-то полезное».

В прошлом году компания Avecto провела исследование уязвимостей программного обеспечения Microsoft и сделала вывод: «Отказ от использования прав локального администратора может снизить риски эксплуатации 92 % критических уязвимостей». Этот вывод выглядит разумным, однако стоит отметить, что Avecto не проводила непосредственное тестирование уязвимостей, а лишь проанализировала данные из Microsoft Vulnerability Bulletin 2023.

Тем не менее, действительно очевидно, что вредоносное ПО, работающее без прав администратора, не сможет выполнять ряд критических действий: устанавливать драйвера, создавать или изменять файлы в защищенных ката-

логах (%systemdrive %, %windir %, %programfiles % и других), изменять системные настройки и, что особенно важно, использовать привилегированные функции API.

Однако на практике отсутствие прав администратора не создает значительных преград ни для вредоносного ПО, ни для хакеров, проникающих в корпоративные сети. Во-первых, в любой системе можно найти множество уязвимостей, которые позволяют получить необходимые права – вплоть до уровня ядра. Во-вторых, существуют угрозы, которые можно реализовать даже с привилегиями обычного пользователя.

На следующей схеме представлены возможные векторы атак, которые не требуют наличия прав администратора. Именно на них мы и сфокусируемся в дальнейшем [1], схема представлена на рис. 1.

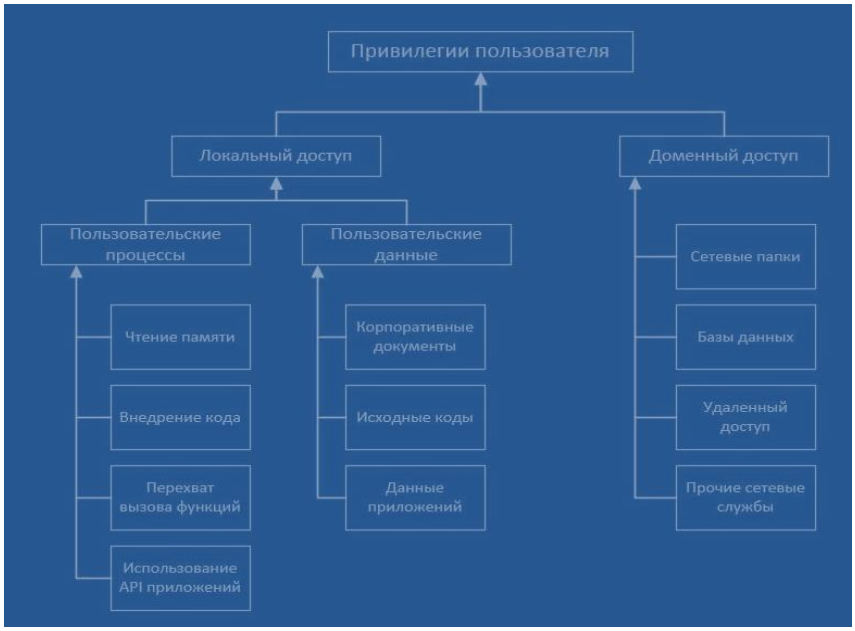


Рис. 1. Пользовательский доступ

Локальные атаки

Злоумышленники, обладая стандартными правами пользователя, могут получить полный доступ к памяти всех процессов, запущенных под этой учетной записью. Это создает идеальные условия для внедрения вредоносного кода, который позволяет удаленно управлять системой через бэкдоры, перехватывать ввод с клавиатуры с помощью кейлогеров и модифицировать содержимое браузера. Хотя большинство антивирусных программ блокируют попытки внедрения неизвестного кода, злоумышленники часто используют более хитрые методы. Один из таких приемов – внедрение бэкдоров и кейлогеров через плагины и расширения браузера. Для установки плагина достаточно обычных прав пользователя, и его код может выполнять практически те же функции, что и полноценный троян – управлять браузером, логировать

ввод данных, перехватывать трафик и взаимодействовать с веб-сервисами, что открывает двери для фишинга [2].

Офисные приложения, такие как почтовые клиенты и мессенджеры, также представляют интерес для злоумышленников. Они могут атаковать других пользователей в сети, используя фишинг и социальную инженерию. Злоумышленники могут получить доступ к таким программам, как Outlook, The Bat, Lync и Skype, не только внедряя вредоносный код, но и через API и локальные сервисы.

Кроме того, данные, хранящиеся на компьютере, могут представлять огромную ценность для атакующих. Злоумышленники активно ищут корпоративные документы, файлы с паролями, зашифрованные данные и цифровые ключи (SSH, PGP и т. д.). Если на компьютере имеются исходные коды, они могут попытаться внедрить туда свой вредоносный код, что создаст дополнительные риски.

В современном цифровом мире важно осознавать эти угрозы и принимать меры по защите своих систем и данных. Игнорирование локальных атак может привести к серьезным последствиям, как для отдельных пользователей, так и для организаций в целом.

Доменные атаки: угроза для корпоративной безопасности

В корпоративном сегменте учетные записи большинства пользователей зависят от доменной авторизации, что обеспечивает удобный доступ к различным сетевым службам. Однако именно эта удобство может обернуться серьезной угрозой. Механизмы Windows Authentication позволяют пользователям автоматически подключаться к ресурсам без необходимости повторной проверки логина и пароля. Это создает уязвимость: если злоумышленник получает доступ к учетной записи зараженного пользователя с правами на доступ к корпоративной базе данных, он может без труда воспользоваться этими правами [3].

Благодаря доменной авторизации злоумышленник также получает доступ ко всем сетевым папкам и дискам, а также к внутренним ресурсам интранета. В некоторых случаях это может привести к доступу к другим рабочим станциям в том же сегменте сети, что значительно увеличивает масштабы атаки.

Кроме того, в корпоративной сети часто функционируют различные сетевые службы, такие как удаленный доступ, FTP, SSH, TFS, GIT и SVN. Даже если для доступа к этим ресурсам используются отдельные учетные данные, злоумышленник может легко их использовать в процессе работы пользователя, во время активной сессии.

Таким образом, важно осознавать потенциальные риски, связанные с доменной авторизацией, и принимать меры для защиты корпоративных данных.

Защита рабочих станций: эффективный подход к безопасности

Обеспечить высокий уровень безопасности на рабочих станциях, лишив пользователей прав администратора, представляется крайне сложной задачей. Хотя установка антивирусного программного обеспечения может повысить защиту, этого недостаточно для решения относительного количества проблем. Для достижения надежной безопасности рекомендуется использовать технологию контроля приложений (Application Control), которая включает три ключевых элемента:

1. Режим «Запрещено по умолчанию» (Default Deny). Этот режим позволяет запускать и устанавливать только те программы, которые одобрены администратором. При этом администратору не нужно добавлять каждое конкретное приложение в список разрешенных. Существует множество инструментов, которые позволяют автоматически включать в этот список все программы, подписанные доверенными сертификатами, или полученные из надежных источников, а также записанные в базе данных Allow_listing, предоставляемой поставщиком защитного ПО.

2. Контроль доверенных приложений. Этот элемент ограничивает функции разрешенного ПО только теми возможностями, которые необходимы для его работы. Например, браузер может создавать сетевые соединения, но не должен иметь доступа к памяти других процессов, подключаться к сетевым базам данных или сохранять файлы на общие ресурсы. Такой подход минимизирует риски и защищает систему от несанкционированного доступа.

3. Контроль установки обновлений. Система позволяет безопасно обновлять программное обеспечение на рабочих станциях в условиях режима «Запрещено по умолчанию», что снижает риск заражения через механизмы обновления. Это обеспечивает актуальность и безопасность ПО без ущерба для системы [4].

Кроме перечисленных возможностей, продукты, использующие технологию Application Control, предлагают ряд дополнительных полезных функций. К таким функциям относятся инвентаризация программного обеспечения, контроль за установленными в сети приложениями, а также сбор журналов событий, которые могут оказаться незаменимыми в случае расследования инцидентов.

Это сочетание технологий обеспечивает пользователям все необходимое для работы. В случае необходимости, они могут легко получить доступ к дополнительным ресурсам. В то же время, возможности злоумышленников, по-

лучивших несанкционированный доступ к защищенной системе, остаются крайне ограниченными. Таким образом, мы достигаем идеального баланса между гибкостью и безопасностью в защите корпоративной сети.

Список используемых источников

1. Статистика отрасли: Министерства цифрового развития, связи и массовых коммуникаций РФ. URL: https://digital.gov.ru/ru/pages/statistika-otrasli/ (дата обращения 06.11.2024).
2. Авдошин С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности: учебное пособие/ С. М. Авдошин, А. А. Савельева, В. Сердюк. М.: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. 431 с. URL: https://ipr-smart.ru/102070.
3. Анисимов А. А. Менеджмент в сфере информационной безопасности: учебное пособие / А. А. Анисимов. 4-е изд. М.: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. 210 с. ISBN 978-5-4497-2408-3. Цифровой образовательный ресурс IPR SMART. URL: https://www.iprbookshop.ru/133946.html (дата обращения 11.11.2024).
4. Фаронов А. Е. Основы информационной безопасности при работе на компьютере: учебное пособие / А. Е. Фаронов. 4-е изд. М.: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. 154 с. ISBN 978-5-4497-2418-2. Цифровой образовательный ресурс IPR SMART. URL: https://www.iprbookshop.ru/133957.html (дата обращения 11.11.2024).

Busygin K., Egorov I., Zurakhov V., Chalova E. **KEY POINTS TO PROTECTING CORPORATE NETWORK INFRASTRUCTURE.**

Saint Petersburg State University of Industrial Technologies and Design

The requirements for protecting a large company's network infrastructure are constantly being modernized in the modern world, which entails updating software and network hardware infrastructure. However, key points remain unchanged for relatively long periods.

Key words: network infrastructure protection, information security, corporate systems, user access.

УДК 621.396.99
ГРНТИ 20.15.05

СЕТЕВЫЕ ПРОБЛЕМЫ ПРИ СОЗДАНИИ КЛАСТЕРА НА ОСНОВЕ LXC

К. Н. Бусыгин, И. М. Егоров, В. С. Зурахов, Е. И. Чалова, С. И. Штеренберг
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В статье рассматриваются проблемы сетевого взаимодействие контейнеров в кластере Линукс-контейнеров, отдельное внимание следует уделить настройке и конфигураци сетевого стека. Проблемы в сетевом взаимодействии контейнеров, объединенных в вычислительный кластер, как правило, распространены если говорить о Линукс-контейнере, а не о технологии в общем.

виды сетевого взаимодействия, проблемы конфигурации сети, виртуальные сетевые устройства

Введение

В настоящее время технология контейнеризации стали неотъемлемой частью разработки и развертывания приложений. Одним из наиболее популярных решений в этой области является Линукс-контейнеры. Создание кластеров на основе контейнеров Линукс-контейнеров предоставляет множество преимуществ, но реализация сетевого взаимодействия является достаточно трудоемким процессом и может привести к различным сетевым проблемам, которые могут затруднить настройку и эксплуатацию кластера.

Объекты сетевого взаимодействия в кластере

Основными объектами сетевого взаимодействия в lxc, как и в других решениях является сетевой мост, по сути представляется виртуальным устройством. Контейнеры подключаются к виртуальному мосту на хосте, что позволяет им общаться друг с другом и с внешними сетями [1]. Следующая технология по популярности это сеть NAT (Network Address Translation) механизм позволяющий преобразовывать ip адреса для пакетов следующих транзитом, Контейнеры здесь получают внутренние IP-адреса, а внешний доступ к ним осуществляется через IP-адрес хоста с помощью NAT. Данный метод также популярен в связи организацией сетевого взаимодействия по протоколу ipv4.[2] Конечно следует уделить внимание пространству имен для сетей Namespace Networking, представляющих изоляцию систем ресурсов, Сетевое

оборудование, стеки протоколов ipv4 ipv6, таблица маршрутизации, firewall номера портов и прочее [3], в данном случае контейнеры можно сделать полностью изолированными. И оверлейная сеть Overlay Networks: используются для связи контейнеров в разных хостах через виртуальные сети.

Сетевые проблемы

Сетевые проблемы в кластерах LXC могут серьезно повлиять на производительность и доступность приложений. Выявленные причины показаны в таблице 1, правильно настроенное сетевое взаимодействие контейнеров в кластере позволяет повысить отказоустойчивость и безопасность.

ТАБЛИЦА 1. Базовые сетевые проблемы конфигурации

Тип	Симптомы	Причины	Решение
Проблемы с конфигурацией сети	Контейнеры не могут взаимодействовать друг с другом или с внешними системами	Контейнеры могут использовать различные режимы сетевой настройки (например, bridged, veth и т.д.), и неправильная конфигурация может привести к тому, что контейнеры не смогут взаимодействовать друг с другом или с внешней сетью	Возможно использования режима bridge, который позволяет контейнерам получать IP-адреса из одной и той же подсети, что упрощает взаимодействие. Необходимо настроить сетевой интерфейс на хосте и указать его в конфигурации контейнеров. /etc/network/interfaces
IP-адресация	Конфликтующие IP-адреса или недоступность контейнеров	Контейнеры могут получать одинаковые IP-адреса из-за неправильной конфигурации DHCP. Неправильное определение и несоответствие подсетей	Используйте статическую настройку IP-адресов или корректно настройте DHCP-сервер, чтобы предотвратить конфликты. Обязательно проверяйте, что каждое устройство находится в уникальной подсети и имеет свой уникальный адрес
Брандмауэр и NAT	Контейнеры не могут получить доступ к сервисам, работающим на хосте	Настройки брандмауэра, такие как iptables, могут блокировать трафик между контейнерами или между контейнерами и внешним миром. Как исходящий, так и входящий трафик	Проверьте настройки iptables и убедитесь, что необходимые правила прописаны для разрешения трафика между контейнерами. Возможно, потребуется создать правила разрешения трафика и трафика NAT для контейнеров
Отсутствие маршрутизации между контейнерами	Контейнеры не взаимодействуют	Если контейнеры находятся в разных сетях, они могут не иметь возможности взаимодействовать друг с другом без соответствующих правил маршрутизации	Убедитесь, что маршруты между сетями настроены правильно, и используйте маршрутизаторы или правила iptables для их соединения.

DNS-проблемы	Контейнеры не могут разрешать имена хостов, что мешает подключению к необходимым сервисам	Контейнеры могут не разрешать DNS-имена других контейнеров или внешних устройств, что затрудняет взаимодействие	Обеспечьте наличие корректных DNS-серверов. Это можно сделать, добавив настройки DNS в конфигурации контейнера или установив DNS-сервер (например, dnsmasq) для Убедитесь, что файл /etc/resolv.conf настроен в каждом контейнере и указывает на корректные DNS-серверы
Проблемы при использовании VLAN	Не настроить транковый порт и маршрут	Если вы используете VLAN для разделения трафика, могут возникнуть сложности с настройкой VLAN для контейнеров	Убедитесь, что физический интерфейс хоста правильно настроен для работы с VLAN, и что соответствующие VLAN-теги корректно добавлены к контейнерам
Балансировка нагрузки	Неправильное распределение запросов, где одни контейнеры перегружены, а другие простаивают	Неправильные настройки балансировщика нагрузки. Ограниченные алгоритмы распределения трафика (например, использование толькоROUND Robin без учета текущей нагрузки на контейнеры)	Используйте более сложные алгоритмы балансировки нагрузки, такие какLeast Connections или IP Hash, чтобы учитывать текущее состояние контейнеров. -Настройте мониторинг текущей нагрузки на контейнеры, чтобы балансировщик мог динамически изменять распределение трафика в зависимости от загруженности
Низкая производительность сети	Высокие задержки или медленное соединение между контейнерами	Ограниченная пропускная способность сетевого интерфейса. - Неоптимизированные настройки MTU (Maximum Transmission Unit)	Проверьте использование сетевых ресурсов с помощью инструментов, таких как iftop или nload. Попробуйте оптимизировать настройки MTU для максимизации пропускной способности, особенно если вы используете туннелирование или VPN
Безопасность сетевого взаимодействия	Возникновение непредвиденных соединений или утечек данных	Неправильно настроенные правила брандмауэра. Уязвимости в сетевой архитектуре	Используйте инструменты управления сетевой безопасностью, такие как iptables или ufw, для настройки правил доступа к контейнерам. Рассмотрите использование VPN для создания защищенных туннелей между контейнерами, особенно если они должны обмениваться конфиденциальной информацией

Сетевые проблемы при создании кластера на основе LXC могут быть вызваны неправильной конфигурацией, отсутствием маршрутизации, проблемами с разрешением имен и другими факторами. Правильная настройка сети, а также использование подходящих инструментов и библиотек могут помочь преодолеть эти сложности и обеспечить стабильную работу LXC-кластера.

Рассмотренные основные сетевые проблемы при объединении контейнеров в кластер помогают определить ту или иную сетевую проблему, особое внимание следует уделять балансировки.

Список используемых источников

1. Сетевой мост. URL: https://en.wikipedia.org/wiki/Network_bridge (дата обращения 06.11.2024).
2. NAT Network Address Translation «преобразование сетевых адресов. URL: https://ru.wikipedia.org/wiki/NAT (дата обращения 06.11.2024).
3. Межсетевой экран. URL: https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%8D%D0%BA%D1%80%D0%B0%D0%BD (дата обращения 06.11.2024).

Busygin K., Egorov I., Zurakhov V., Chalova E. Shterenberg S. **NETWORK ISSUES CREATING AN LXC-BASED CLUSTER.**

Saint Petersburg State University of Industrial Technologies and Design

The article discusses the problems of network interaction of containers in the Linux cluster of containers, special attention should be paid to the configuration and configuration of the network stack. Problems in the network interaction of containers combined into a computing cluster are usually common if we talk about Linux container and not about technology in general.

Key words: types of network interaction, network configuration problems, virtual network devices.

УДК 004
ГРНТИ 20.53.01

РЕАЛИЗАЦИЯ ПРОГРАММНОЙ ОСНОВЫ ИГРЫ НА ПЛАТФОРМЕ UNITY

И. Д. Васильев
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В работе исследуются особенности новой высокопроизводительной архитектуры, которая позволяет управлять большим объемом данных. Статья рассматривает важность оптимизации широкой компонентной системы в Unity, особенности работы с графикой и шейдерами. Затрагивается использование уникальных инструментов при работе с анимацией объектов, а также инструменты для сетевого взаимодействия.

индустрия игровых развлечений, компонентно-ориентированная архитектура, графика, шейдерграф, анимация, сетевое взаимодействие.

Введение в проблематику разработки

Сегодня игровой девелопмент на платформе Unity является популярным направлением для R&D в области интерактивных медиа и индустрии игровых развлечений. Unity не только предлагает мощные инструменты для создания сложных 3D и 2D игр, но и формирует уникальную экосистему для инди-разработчиков и крупных студий. Однако, за широкими возможностями и интуитивно понятным UI скрывается целый пласт технических нюансов, требующих углубленного понимания архитектурных паттернов, принципов управления ресурсами, алгоритмов физического взаимодействия и оптимизации игровых процессов. Рассмотрим исследование концептов, связанных с программной основой на Unity, акцентируя внимание на современных методах оптимизации и использования компонентной архитектуры для достижения производительности.

Архитектура и компонентная модель Unity

Unity изначально базируется на Component-based архитектуре, далее CBA, что позволяет рассматривать каждый элемент игры как набор взаимозависимых и взаимозаменяемых компонентов. В этой парадигме каждый GameObject – это объект-контейнер, который способен получать функциональные характеристики за счет добавления компонентов [1]. Однако для грамотного проектирования недостаточно просто использовать готовые компо-

ненты. Важно выстроить структуру так, чтобы соблюсти баланс между функциональностью и производительностью. На высоком уровне программирования на Unity следует избегать частого использования методов Update() в каждом компоненте, так как это может привести к перегрузке процессора, особенно на мобильных устройствах и слабых ПК [2]. Вместо этого стоит прибегнуть к асинхронным методам, таким как корутины, которые выполняются в отдельном потоке и могут запускаться по таймеру.

Для разработки на Unity основным инструментом для создания игровой логики остается класс MonoBehaviour, который обрабатывает жизненный цикл объекта и является базой для всех компонентов [2]. Тем не менее, использование большого количества MonoBehaviour-компонентов на различных объектах может привести к перегрузкам в сборщике мусора, так как каждый объект при уничтожении оставляет фрагменты, которые необходимо очищать. Современные методы минимизации затрат памяти включают в себя использование пула объектов (Object Pooling), что позволяет не уничтожать объекты, а повторно их использовать, экономя ресурсы на их создании.

Также стоит отметить, что Unity не предоставляет встроенной поддержки для многопоточной обработки в MonoBehaviour, что ограничивает возможности масштабирования для проектов, где необходимо обрабатывать большое количество параллельных событий. Это особенно актуально для open-world игр с большим количеством NPC или сложной физикой.

В последнее время Unity активно развивает новую архитектуру – Entity-Component-System (ECS), которая, в отличие от MonoBehaviour, позволяет управлять большим количеством объектов (Entities) с высокой степенью оптимизации. ECS разделяет игру на три основных модуля:

1. Entities – данные, не обладающие функциональностью.
2. Components – наборы данных, описывающих поведение или состояние.
3. Systems – логика, которая обрабатывает объекты и компоненты.

Этот подход устраняет проблему множественного вызова Update() и позволяет обрабатывать данные партиями, что приводит к значительному ускорению и снижению нагрузки на процессор. ECS работает на основе Data-Oriented Technology Stack (DOTS), который использует возможности кэширования данных в процессоре и поддерживает многопоточность, что является прорывом в области оптимизации.

Применение ECS в игровых проектах особенно полезно для реализации массовых сцен с большим количеством объектов, таких как противники в стратегии или элементы в симуляторах. Несмотря на это, ECS требует от разработчика более высокого уровня абстракции и знаний в области низкоуровнего программирования, что усложняет его внедрение в инди-проектах.

На уровне производственного управления ресурсами Unity включает в себя такие важные аспекты, как загрузка и выгрузка ресурсов, использование

ассетов и оптимизация текстур и моделей. Asset Bundles – это наборы ресурсов, которые могут загружаться из сети или диска, позволяя динамически загружать и выгружать элементы без необходимости полного перезапуска приложения. Этот подход используется для оптимизации размеров финального билда и управления памятью. Asset Bundles позволяют загружать ресурсы на лету, что важно для игр с открытым миром или большими картами, где необходимо загружать ресурсы только для активной части карты, минимизируя при этом затраты на память.

Object Pooling – еще одна методология управления ресурсами, заключающаяся в предварительном создании и хранении объектов, которые часто создаются и уничтожаются. В играх-шутерах, где персонаж выпускает большое количество снарядов, каждое создание и уничтожение снаряда может быть заменено на возврат в пул объектов [3]. Этот подход уменьшает частоту вызова garbage collector и позволяет экономить ресурсы.

Оптимизация при работе с компонентами и графикой

Реализация ИИ также требует отдельного рассмотрения, так как использование стандартных методов, таких как NavMesh, значительно упрощает задачу передвижения NPC по сложным картам. Однако для создания более реалистичного поведения следует использовать поведенческие деревья или finite-state machines (FSM), которые позволяют моделировать сложные сценарии поведения персонажей и событий [4].

Необходимо оптимизировать все физические взаимодействия, особенно при работе с Rigidbody компонентами, так как каждое взаимодействие занимает объем ресурсов, и чрезмерное их использование может привести к сбоям или падению FPS.

В условиях расширения возможностей графики и роста ресурсоемкости игр, растут и вычислительные требования. Оптимизация охватывает аспекты рендеринга, управление частотой кадров и использование шейдеров.

Существует широкий набор стандартных шейдеров, таких как Surface и Unlit, которые обеспечивают базовый уровень графической проработки и сильно не влияют на производительность, но в проектах, требующих высокодетализированной графики, разрабатываются кастомные шейдеры, используя язык ShaderLab и HLSL [5].

Применение более сложных шейдеров увеличивает нагрузку на GPU, что приводит к снижению производительности, особенно на мобильных платформах и VR-устройствах. Для устранения таких тонкостей, разрабатываются Lightmaps, представляющие собой предвычисленное освещение, сохраняемое в виде текстур, что значительно разгружает GPU при рендеринге сложных сцен. Однако из-за ограничений лайтмапинга, таких как фиксированное осве-

щение, приходится искать баланс между динамическими источниками света и предрасчитанными текстурами.

На уровне кода также применяются методы, снижающие нагрузку на процессор. Unity предоставляет инструменты для профилирования, такие как Profiler и Frame Debugger, позволяющие разработчику отслеживать процессы и выявлять наиболее ресурсоемкие функции. Это особенно полезно при разработке мобильных приложений, где оптимизация становится первостепенной задачей из-за ограниченных возможностей устройств.

Управление состояниями объектов и сетевое взаимодействие

Unity базируется на использовании анимационных систем, таких как Animator и Animation. Аниматор контролирует иерархию анимационных состояний, что позволяет моделировать сложные анимационные переходы и события, которые меняют поведение объектов в зависимости от действий игрока или изменений игровой среды. Создание плавных переходов между анимациями – важный аспект при разработке игр, требующих реализма. Анимация движения персонажа может быть интегрирована с системой физики, чтобы соответствовать реальным законам инерции и силы трения.

Для создания продвинутых анимаций в Unity можно использовать Inverse Kinematics (IK), которая позволяет моделировать движения конечностей персонажей в зависимости от положения объекта, делая их более реалистичными. При использовании IK персонаж сможет адаптировать походку под неровные поверхности или наклоняться, чтобы достичь заданной точки. Несмотря на значительные преимущества, IK является вычислительно затратной, поэтому ее следует применять лишь в необходимых случаях и тщательно оптимизировать.

Unity также предоставляет возможности для создания многопользовательских игр благодаря встроенным инструментам для сетевого взаимодействия, таким как UNet и Mirror. Использование сетевого слоя требует от разработчика знания принципов клиент-серверной архитектуры и асинхронного обмена данными. Сетевые игры нуждаются в низкой задержке и высокой синхронизации, что требует применения специальных методов, таких как interpolation и extrapolation для предсказания движения объектов на стороне клиента и создания иллюзии плавного взаимодействия [6]. Такой подход позволяет минимизировать эффект лагов, обеспечивая более комфортный геймплей для игроков.

Особенно актуальна проблема синхронизации анимации и звука, так как их несинхронное воспроизведение может нарушить атмосферу игры. Unity позволяет использовать Timeline для интеграции аудиовизуальных элементов и синхронизации сцен. Timeline является инструментом для нарезки и управ-

ления временными секциями, что позволяет комбинировать звуковые и визуальные эффекты с точной временной привязкой, что важно для квестов или нарративных сцен, требующих глубокого погружения.

Процесс разработки игр в Unity представляет собой комплекс задач, требующих глубоких знаний в областях программирования, оптимизации и проектирования пользовательского опыта. Unity предоставляет мощный инструментарий для работы с графикой, анимацией, сетевым взаимодействием и искусственным интеллектом, однако для создания действительно качественного продукта необходимо понимать фундаментальные принципы и ограничения каждой из этих областей. Комбинируя различные подходы и техники, можно достигнуть высокого уровня производительности, не теряя в качестве остальных аспектов.

Список используемых источников

1. Юниверс Г. Основы работы с физическими движками в игровой платформе Unity. URL: https://unity.com/ru/resources/physics-engine (дата обращения 05.11.2024).
2. Макаров А.В., Смирнов П.Ю. Программные основы разработки интерактивных приложений в среде Unity // Программирование и компьютерные технологии, 2021. Т. 16. № 2. С. 34–41.
3. Джонсон К., Фрэнклин Л. Real-Time Game Optimization Techniques // International Journal of Game Development, 2019. Vol. 8. № 3. P. 110–122.
4. Мартинес Э. М., Смит Дж. Интеграция AI-алгоритмов в игровую логику: Unity ML-Agents // Game Technologies and AI Research, 2020. Vol. 6. № 1. P. 89–101.
5. Уайт Дж. Специфика разработки шейдеров для высокопроизводительных приложений // Journal of Computer Graphics and Applications, 2018. Vol. 14. № 2. P. 75–83.
6. Хан С. В. Методы и средства оптимизации графических процессов в 3D-играх на базе Unity // Научные исследования и разработки: информационные и телекоммуникационные технологии, 2022. Т. 14. № 4. С. 56–63.
7. Ли Г. Реализация сетевых взаимодействий в многопользовательских играх на Unity. URL: https://developer.unity.com/ru/networking (дата обращения 05.11.2024).
8. Миньков Н. Г., Лебедев А. С. Методы синхронизации и рендеринга в Unity: вопросы производительности // Вестник программной инженерии и систем, 2023. Т. 20. № 1. С. 102–108.
9. Поляк И. Ю. Разработка игр в Unity: особенности и лучшие практики. URL: https://gameunity.ru/bestpractices (дата обращения 05.11.2024).
10. Браун Д., Харрис Л. Exploring Physics-Based Simulations in Unity // Simulation in Interactive Games, 2021. Vol. 9. № 4. P. 45–52.

Vasilyev I. **IMPLEMENTATION OF THE SOFTWARE FRAMEWORK OF THE GAME ON THE UNITY PLATFORM.**

Saint Petersburg State University of Industrial Technology and Design

This article explores the features of a new high-performance architecture that enables management of large volumes of data. The article examines the importance of optimizing Unity's extensive component-based system, along with the specifics of working with graphics and shaders. It also addresses the use of unique tools for object animation and tools for network interaction.

Key words: game entertainment industry, component-oriented architecture, graphics, shader graph, animation, network interaction.

УДК 004.896
ГРНТИ 28.23.01

К ВОПРОСАМ О ЗАЩИТЕ ML-МОДЕЛЕЙ В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ

Л. А. Виткова, Е. А. Трофимов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Модели машинного обучения играют ключевую роль в современных облачных системах, помогая в анализе больших данных, в автоматизации процессов и в предсказании событий. Однако с ростом частоты использования ML-моделей в облачных инфраструктурах возникает необходимость защиты этих моделей от различных атак и уязвимостей. Защита моделей машинного обучения – это актуальная задача, включающая в себя защиту наборов данных для обучения, конфиденциальности, а также предотвращение несанкционированного доступа и манипуляций.

ML-модели, облачная инфраструктура, угрозы для искусственного интеллекта.

Модели машинного обучения играют ключевую роль в современных облачных системах, помогая в анализе больших данных, в автоматизации процессов и в прогнозировании. Однако с ростом частоты использования ML-моделей в облачных инфраструктурах возникает необходимость защиты этих моделей от различных атак и уязвимостей. Защита моделей машинного обучения (ML) в облачных средах имеет свои уникальные особенности, обусловленные распределенной инфраструктурой, масштабируемой и динамичной природой облаков. Задача защиты моделей машинного обучения в облачных вычислениях требует применения многоуровневой стратегии. [1]

Облачная многослойная архитектура состоит из различных уровней: аппаратная инфраструктура, цифровая платформа и программное обеспечение, каждый из которых требует отдельного подхода к безопасности. Модель может быть уязвима на каждом из этих уровней.

В список наиболее распространенных конфигураций облачных инфраструктур входит:

– SaaS («Software as a Service») – предполагает аренду конкретного программного обеспечения;

– PaaS («Platform as a Service») – предполагает использование облачного сервиса для разработки нового программного обеспечения;

– IaaS («Infrastructure as a Service») – предполагает полную аренду информационной инфраструктуры.

Наиболее распространенной конфигурацией является SaaS. В его случае на удаленном сервере развертывается экземпляр необходимого программного обеспечения, для него выделяются ресурсы, а пользователь получает доступ не к самому серверу, а к интерфейсу прикладного ПО. Таким образом клиент напрямую получает решение своей задачи, не сталкиваясь с необходимостью настраивать рабочее место, систему и оборудование. [2]

Атаки на ML-модели в облачных средах

Далее в статье рассматриваются угрозы и атаки, с которыми сталкиваются системы машинного обучения. Как показано на рис. 1, на сегодняшний день угрозы безопасности на протяжении жизненного цикла систем машинного обучения можно разделить на пять категорий: 1) Отравление обучающего набора; 2) Бэкдор в обучающем наборе; 3) Атаки на конкурирующие примеры; 4) Кража модели; 5) Восстановление конфиденциальных данных обучения (включая атаку на инверсию модели). Первые две атаки происходят во время обучения, в то время как последние три атаки происходят во время эксплуатации. [3] Так же стоит учитывать, что совместное использование ресурсов в облачных средах часто предполагает мультиарендность, когда несколько клиентов используют одну и ту же инфраструктуру. Это создает потенциальные риски для утечки данных и компрометации модели, если защита изоляции между арендаторами нарушена. Злоумышленники могут попытаться использовать боковые каналы или атаки через виртуализацию для доступа к чужим данным и моделям.

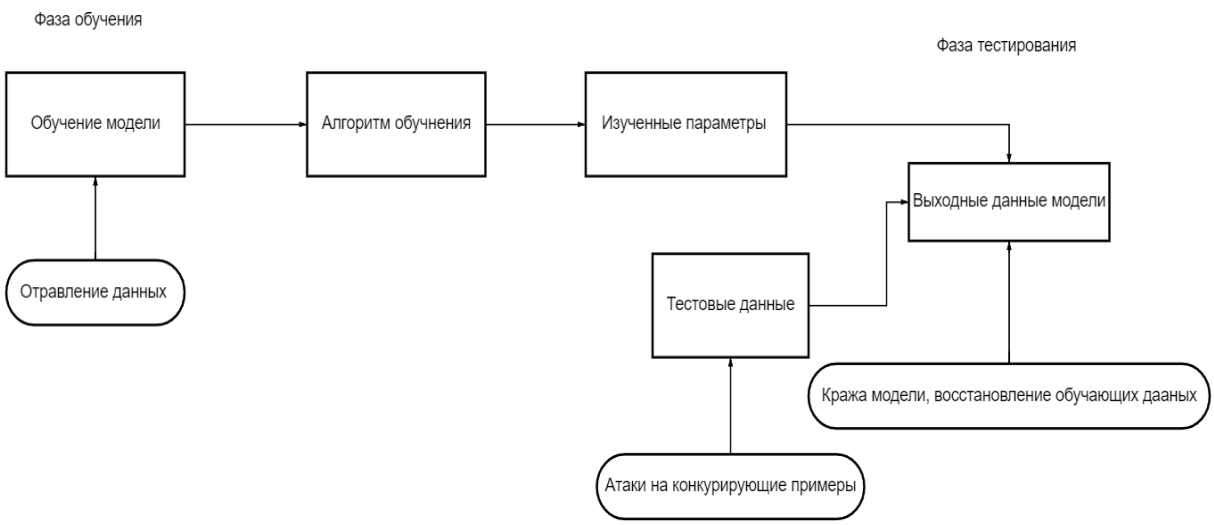


Рис. 1 Атаки на ML системы

Стратегии защиты ML-моделей

Для защиты самих моделей машинного обучения в облачных инфраструктурах рекомендуется применять комплексные стратегии, охватывающие как этап обучения, так и этап эксплуатации.

Обеспечение чистоты и достоверности данных, используемых для обучения, достигается посредством мониторинга источников данных и анализа на наличие аномалий в самих наборах данных.

Дифференциальная приватность представляет собой метод, который добавляет шум к данным или результатам модели, предотвращая тем самым извлечение конфиденциальной информации. Даже если злоумышленник получает доступ к модели, данные пользователей остаются защищенными. [4]

Для защиты модели от атак, основанных на специально разработанных входных данных, применяется adversarial training. Этот подход включает обучение модели на данных, содержащих примеры атак, что позволяет модели «научиться» распознавать и корректно обрабатывать такие входы.

Также контроль доступа к модели является важнейшей мерой защиты. Необходимо ограничить количество пользователей, имеющих доступ к модели или возможность ее модификации. Это достигается посредством многофакторной аутентификации и ролевых политик доступа.

Для предотвращения таких атак, как угон модели или отказ в обслуживании, необходимо внедрить системы мониторинга, отслеживающие использование модели. Необычная активность, например, слишком частые запросы или внезапные изменения в результатах, могут служить индикаторами атаки. [5]

Использование механизмов шифрования при передаче и хранении данных модели является обязательной мерой для защиты от атак. Это включает в себя шифрование всех взаимодействий между облаком и пользователями.

Эффективные решения для защиты ML в облаке включают использование изолированных виртуальных машин и контейнеров для защиты модели от компрометации.

Для предотвращения кражи модели необходимо ограничить количество запросов, которые могут быть отправлены к ней, и внедрить механизм защиты от чрезмерного использования. Также можно применять методы мониторинга активности пользователей и фильтрацию запросов.

Один из подходов к защите модели состоит в обфускации (маскировании) архитектуры модели и скрытии деталей ее работы. Это снижает вероятность того, что злоумышленник сможет восстановить структуру модели и повторить ее поведение.

Таким образом, защита моделей машинного обучения в облачных инфраструктурах требует комплексного подхода, включающего защиту данных, мониторинг активности, ограничение доступа и контроль над API. Уязвимости, возникающие из-за масштабируемости и открытого доступа к облачным сервисам, должны быть учтены в стратегиях безопасности, чтобы обеспечить надежную работу ML-моделей и предотвратить атаки.

Список используемых источников

1. Ogeti P., Fadnavis N. S., Patil G. B., Padyana U. K., Rai H. P. Benefits and Challenges of Deploying Machine Learning Models in the Cloud. 2024. С. 1–3.
2. Пестов И. Е. Методика автоматизированного противодействия несанкционированным воздействиям на инстансы облачной инфраструктуры с использованием безагентного метода сбора метрик. 2020. С. 21–29.
3. Xue M., Yuan C., Wu H., Zhang Y., Liu W. Machine Learning Security: Threats, Countermeasures, and Evaluations. 2020. С. 2–21.
4. Papernot N., Abadi M., Erlingsson U., Goodfellow I., Talwar K. Semi-Supervised Knowledge Transfer for Deep Learning from Private Training Data // Proceedings of the International Conference on Learning Representations (ICLR). 2016. С. 2–21.
5. MLSecOps: Protecting AI/ML Lifecycle in Telecom. URL: https://www.everythingrf.com/Whitepapers/details/5346-mlsecops-protecting-the-ai-ml-lifecycle-in-telecom (дата обращения 02.11.2024).

Vitkova L., Trofimov E. **QUESTIONS ABOUT THE PROTECTION OF ML MODELS IN CLOUD INFRASTRUCTURES.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Machine learning models play a key role in modern cloud systems, helping in big data analysis, process automation, and event prediction. However, with the increasing frequency of using ML models in cloud infrastructures, it becomes necessary to protect these models from various attacks and vulnerabilities. Protecting machine-learning models is an urgent task, including protecting training datasets, privacy, and preventing unauthorized access and manipulation.

Key words: ML models, cloud infrastructure, threats to artificial intelligence.

УДК 004.056.5
ГРНТИ 81.93.29

АНАЛИЗ МЕТОДОВ ОБРАБОТКИ ЕСТЕСТВЕННОГО ЯЗЫКА ДЛЯ УЛУЧШЕНИЯ ОБНАРУЖЕНИЯ ФИШИНГА

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

Растущая распространенность фишинговых атак представляет собой серьезную угрозу для глобальной кибербезопасности. По мере того, как методы фишинга эволюционируют, они все чаще обходят традиционные методы обнаружения, используя психологические уловки и языковые особенности для введения пользователей в заблуждение.

NLP, машинное обучение, защита информации

Судя по статистике Positive Technologies за I квартал 2024 года, количество инцидентов с распространением ВПО выросло на 19 %. Более, чем в половине случаев (51 %), распространение происходило через электронную почту [1].

На данный момент чаще всего используются стандартные методы обнаружения фишинга, которые представлены в ТАБЛИЦЕ 1.

ТАБЛИЦА 1. Традиционные методы обнаружения фишинга

Анализ URL	Изучение структуры, домена и путей URL-адресов для выявления вредоносных ссылок
Проверка черных списков	Проверка ссылок и адресов электронной почты по известным черным спискам фишинговых доменов
Анализ контента	Исследование структуры страницы, метаданных и поведения скриптов
Анализ электронной почты	Проверка заголовков писем, IP-адресов отправителя и ключевых слов

В данный момент повсеместно внедряются системы машинного обучения и искусственного интеллекта. Решением данной проблемы можем быть использование NLP для выявления фишинга.

Обработка естественного языка (NLP) – это междисциплинарная область исследований, лежащая на стыке информатики, лингвистики и искусственного интеллекта. Основной задачей NLP является разработка алгоритмов и моделей, которые позволяют компьютерам интерпретировать, анализировать и генерировать человеческий язык таким образом, чтобы обеспечивать качественное взаимодействие между человеком и машиной [2].

Существующие методы анализа текста с помощью NLP [3] представлены на рис. 1.

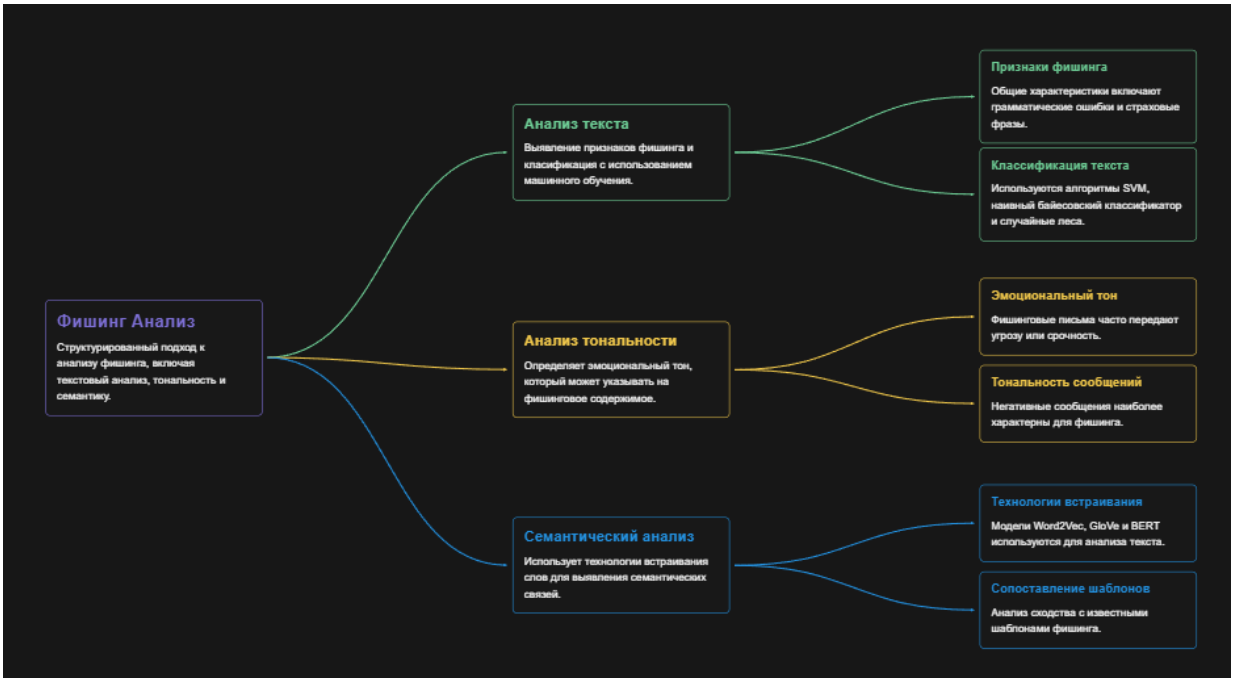


Рис. 1. Методы анализа текста с помощью NLP

Эффективность методов NLP для обнаружения фишинга представлена на рис. 2.

Рис. 2. Эффективность методов NLP для обнаружения фишинга

Представление системы обнаружения, в основе которого лежит NLP [4], показано на рис. 3.

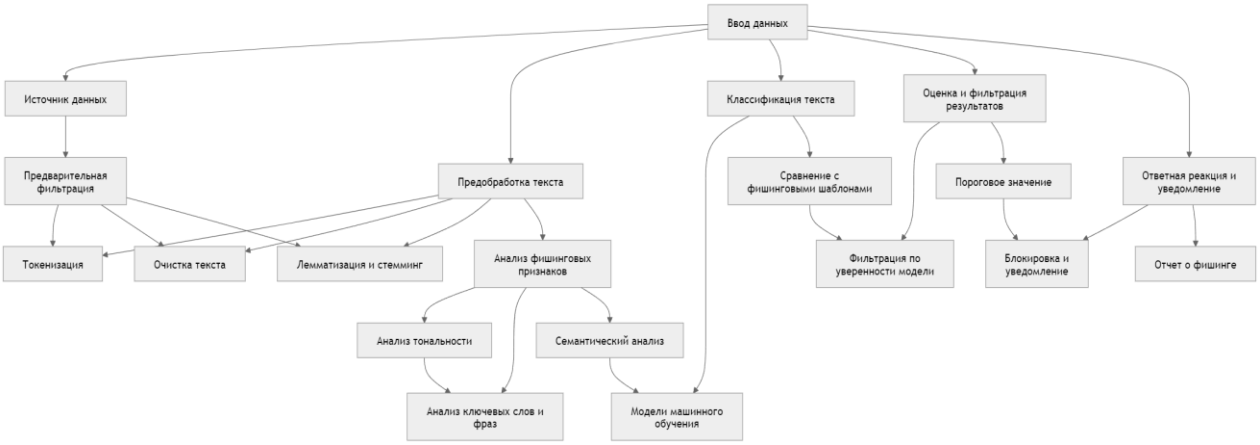


Рис. 3. Схема архитектуры системы обнаружения фишинга на основе NLP

Улучшение существующих методов NLP

Обработка сложных языковых структур: разработка моделей, способных анализировать сложные предложения для лучшего обнаружения сложных фишинговых сообщений.

Расширение обучающих данных: увеличение объема и разнообразия наборов данных, включение многоязычных и мультидиалектных примеров, что позволит повысить адаптивность NLP-моделей.

Оценка производительности в реальных условиях: создание тестовых сред для оценки точности моделей NLP в условиях реального времени [5].

Краткое резюме выводов

Методы NLP улучшают обнаружение фишинга за счет анализа текстовых, семантических и тональных аспектов сообщений, обеспечивая значительное улучшение по сравнению с традиционными методами. Каждый из подходов NLP – анализ текста, определение тональности и семантический анализ – имеет свои сильные стороны, хотя все еще существуют ограничения в обработке сложных и многоязычных фишинговых сообщений.

Направления будущих исследований

Для дальнейшего усиления обнаружения фишинга будущие исследования должны сосредоточиться на разработке NLP-методов, устойчивых к манипуляциям и адаптируемых к изменяющимся угрозам. Интеграция NLP с комплексными системами безопасности может открыть путь к более продви-

нутым и адаптивным системам обнаружения фишинга, способным защитить пользователей в глобальном масштабе.

Список используемых источников

1. Positive Technologies: больше половины успешных атак с использованием вредоносного ПО начинаются с фишинга URL: https://dsmedia.pro/company/ptsecurity/analytics/positive-technologies-bolshe-poloviny-uspeshnyh-atak-s-ispolzovaniem-vredonosnogo-po-nachinajutsja-s-fishinga (дата обращения 05.11.2024).
2. NLP and Education: using semantic similarity to evaluate filled gaps in a large-scale Cloze test in the classroom. URL: https://arxiv.org/abs/2411.01280 (дата обращения 06.11.2024).
3. Thoughtful Adoption of NLP for Civic Participation: Understanding Differences Among Policymakers. URL: https://arxiv.org/abs/2410.22937 (дата обращения 07.11.2024).
4. The Handbook of Computational Linguistics and Natural Language Processing. URL: https://onlinelibrary.wiley.com/doi/book/10.1002/9781444324044#page=291 (дата обращения 08.11.2024).
5. Application of NLP-based models in automated detection of risky contract statements written in complex script system. URL: https://www.sciencedirect.com/science/article/abs/pii/S0957417424021638 (дата обращения 09.11.2024).

Grechukhin D. **ANALYSIS OF NATURAL LANGUAGE PROCESSING TECHNIQUES TO IMPROVE PHISHING DETECTION.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The growing prevalence of phishing attacks poses a serious threat to global cybersecurity. As phishing techniques evolve, they increasingly evade traditional detection methods by using psychological tricks and linguistic features to mislead users.

Key words: NLP, machine learning, information security.

УДК 517.972.8
ГРНТИ 27.19.19

ТОПОЛОГИЯ МНОГООБРАЗИЙ В АНАЛИЗЕ БЕЗОПАСНОСТИ ОБФУСКАЦИИ ПРОГРАММ

Б. В. Долуденко
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В современном мире обфускация программного обеспечения становится важным инструментом для защиты данных и предотвращения реверс-инжиниринга. Однако с ростом сложности обфускации возникает необходимость в новых подходах к оценке безопасности таких программ. Одним из таких подходов является использование методов топологии многообразий для анализа измененной структуры программного кода. Топологические инварианты и концепции, такие как гомотопия и гладкие многообразия, могут помочь оценить устойчивость обфусцированных программ к анализу и атакам, затрудняя или делая невозможным восстановление исходного кода.

гомотопия, обфускация кода, топология многообразий, анализ безопасности

Современные информационные технологии значительно изменили мир и предоставили новые возможности для хранения и обмена данных, а также для создания программного обеспечения. Но с развитием технологий возрастает и число угроз, которые направлены на нарушение безопасности информации. Одной из таких угроз является реверс-инжиниринг программ, вследствие чего, от разработчиков требуется применение современных методов защиты, например, обфускация кода. Обфускация, в свою очередь, усложняет анализ программного кода и защищает его от несанкционированного доступа.

Однако с ростом сложности обфускации возникает и необходимость в новых подходах для оценки ее безопасности. В настоящее время один из самых перспективных – метод топологии многообразий, применяемый для анализа изменений в структуре программы, произведенных обфускацией. Такой подход открывает новые возможности для повышения устойчивости программ к атакам, таких как реверс-инжиниринг.

Обфускация программного кода является процессом, при котором исходный код программы изменяется так, чтобы усложнить его понимание для анализирующего код объекта. Существует множество техник обфускации, таких как изменение потока управления, распараллеливание процессов, добавление мертвого кода или изменение логики работы программы [1].

Цель обфускации – это не просто защита от несанкционированного доступа, но также и создание дополнительных сложностей для атакующих, это позволяет затруднить анализ программы и ее последующую деобфускацию.

Но, несмотря на эффективные методы защиты, традиционные способы анализа безопасности обфусцированных программ, такие как статический и динамический анализ кода, часто недостаточны. Поэтому для более глубокого понимания изменений, вызванных обфускацией, и как они влияют на безопасность программного обеспечения, нужно использовать более сложные методы, например, математические подходы.

Топология многообразий – это одна из областей математики, которая изучает геометрические и пространственные свойства объектов, не изменяющихся при непрерывных преобразованиях. В контексте программного кода многообразия рассматриваются, как абстрактные структуры, являющиеся разными реализациями одной и той же программы. Когда программа подвергается обфускации, ее структура изменяется, но функциональность остается той же [2].

Методы топологии позволяют моделировать изменения в структуре программы, как топологическое преобразование. Это позволяет не только более точно оценить, как сильно изменилась структура программы после обфускации, но и понять, как эти изменения влияют или могут повлиять на ее безопасность. Важным инструментом для анализа являются топологические инварианты, такие как гомология и когомология. Инварианты позволяют выявить изменения, произошедшие в структуре программы, и оценить, трудность восстановления исходного кода атакующим.

Топологические инварианты играют важную роль в анализе защищенных программ. Инварианты – характеристики объекта, которые не изменяются при топологических преобразованиях. В контексте анализа программного кода инварианты можно использовать для оценки изменения структуры программы после ее обфускации [3].

1. Гомология и когомология: концепции помогающие анализировать структуру программы на основе графа зависимостей. В случае обфускации можно использовать гомологию для оценки изменения структуры потока управления и выявления возможных скрытых фрагментов кода. Когомология может быть полезна для анализа того, как изменения в коде могут повлиять на его поведение в различных условиях, так как она является более «сильным» инвариантом.

2. Гомотопия: концепция, описывающая, как одно топологическое пространство может быть непрерывно преобразовано в другое. Гомотопия может быть использована для оценки сложности восстановления исходной программы атакующим, после обфускации. Если исходная программа и обфусцированная версия могут быть связаны через гомотопическое преобразование, это может свидетельствовать тому, что восстановление исходного кода является возможным.

Использование топологических методов для анализа обфусцированных программ имеет несколько важных преимуществ. Топология предоставляет возможность:

1. Оценить изменения в структуре программы, то есть, применяя методы топологии, можно детально анализировать, как обфускация изменяет структуру программы, а также предсказать, как эти изменения могут повлиять на ее устойчивость к атакам;

2. Выявить скрытые уязвимости, применение топологических инвариантов может помочь обнаружить скрытые уязвимости в обфусцированном коде, которые, в свою очередь, могут быть использованы для деобфускации;

3. Моделировать атаки и защиту, топология позволяет моделировать возможные атаки на программы после обфускации, оценивая, насколько трудно атакующему восстановить исходный код, а также разрабатывать методы защиты на основе этих оценок.

Использование методов топологии многообразий в анализе обфускации программ является перспективным подходом для повышения безопасности программного обеспечения. Топологические инварианты и концепции, такие как гомотопия и гомология, позволяют сильней и более углубленно понять изменения в структуре программы, после ее обфускации, а также оценить ее устойчивость к реверс-инжинирингу. Такие методы могут стать важным инструментом для создания более защищенных программ и улучшения алгоритмов анализа безопасности.

Список используемых источников

1. Красов А. В., Зуев И. П., Карельский П. В., Радынская В. Е., Гераськина В. С. Алгоритмы и методы защиты программного кода на базе обфускации // Вестник информационной безопасности. 2020. Т. 15. № 4. С. 12–25.
2. Баранов В. В., Крибель А. М., Лаута О. С., Нечепуренко А. П. Применение метода топологического преобразования стохастических сетей для оценки эффективности средств защиты // Вестник Военной академии связи им. С. М. Буденного. 2017. Т. 34. № 6. С. 45–58.
3. Емельянов С. В., Коровин С. К., Бобылев Н. А. и др. Гомотопии экстремальных задач // Математические методы в экономике и управлении. 2001. Т. 33. № 4. С. 332–343.

Doludenko B. **TOPOLOGY OF MANIFOLDS IN THE ANALYSIS OF OBFUSCATION SECURITY OF SOFTWARE.**

Saint Petersburg State University of Industrial Technologies and Design

In the modern era, code obfuscation has become a crucial method for safeguarding software and preventing reverse engineering. As obfuscation techniques grow in complexity, there is an increasing need for advanced approaches to assess the security of obfuscated programs. One promising approach involves the application of manifold topology to analyze the transformed structure of program code. By leveraging topological invariants and concepts such as homotopy and smooth manifolds, it is possible to evaluate the robustness of obfuscated programs against reverse engineering and code analysis, making it significantly more challenging to recover the original code.

Key words: homotopy theory, code obfuscation, manifold topology, security analysis.

УДК 004.056.53
ГРНТИ 20.51.19

ЗАДАЧИ ЗАЩИТЫ СИСТЕМ ВИРТУАЛИЗАЦИИ

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

Современные виртуализированные среды стали неотъемлемой частью ИТ-инфраструктур, обеспечивая гибкость и масштабируемость для бизнес-задач. Однако виртуализация несет в себе уникальные риски, которые требуют особого подхода к безопасности, обеспечению отказоустойчивости и резервированию. Статья рассматривает основные угрозы для виртуальных систем, начиная от аппаратных сбоев и сетевых коммуникаций до специфических рисков, связанных с гипервизором, виртуальными машинами и их сетевой инфраструктурой.

виртуализация, гипервизор, аутентификация, виртуальная машина

Преимущества виртуализации

Виртуализация позволяет объединить различные вычислительные ресурсы в централизованную инфраструктуру, что значительно упрощает администрирование и масштабирование [1]. Этот подход повышает эффективность использования оборудования, снижает эксплуатационные расходы, упрощает резервное копирование и восстановление данных. В дополнение к этому, изоляция виртуальных машин и приложений создает барьер для распространения атак: в случае взлома воздействие ограничивается только одним приложением на одной операционной системе. При грамотной настройке виртуальная среда также обеспечивает удобный доступ к системе для пользователей без раскрытия им критической информации. В случае заражения виртуальной машины, ее можно оперативно откатить к «чистому» состоянию, существовавшему до инцидента, что ускоряет восстановление работоспособности [2]. Более того, за счет сокращения количества физического оборудования виртуализация упрощает инфраструктуру, снижая затраты на эксплуатацию и улучшая физическую безопасность – меньше устройств означает меньше потенциальных точек доступа, а также меньшую потребность в центрах обработки данных. В совокупности эти аспекты делают виртуализацию привлекательной для компаний, стремящихся к повышению безопасности и оптимизации управления ресурсами. Однако с широким распространением виртуальных сред появляется и новый уровень угроз, что делает вопрос безопасности виртуализации критически важным.

К защите виртуальных инфраструктур относится как защита отдельных виртуальных машин, так и гипервизоров: защита от несанкционированного доступа к информации, утечки данных и разных атак, использующих уязвимости или вредоносный код. Эти меры помогают поддерживать целостность и безопасность данных и ресурсов, что особенно важно в виртуализированных средах, где любое нарушение может затронуть множество систем и сервисов одновременно. На рисунке 1 представлен пример схемы обеспечения безопасности виртуальной инфраструктуры.

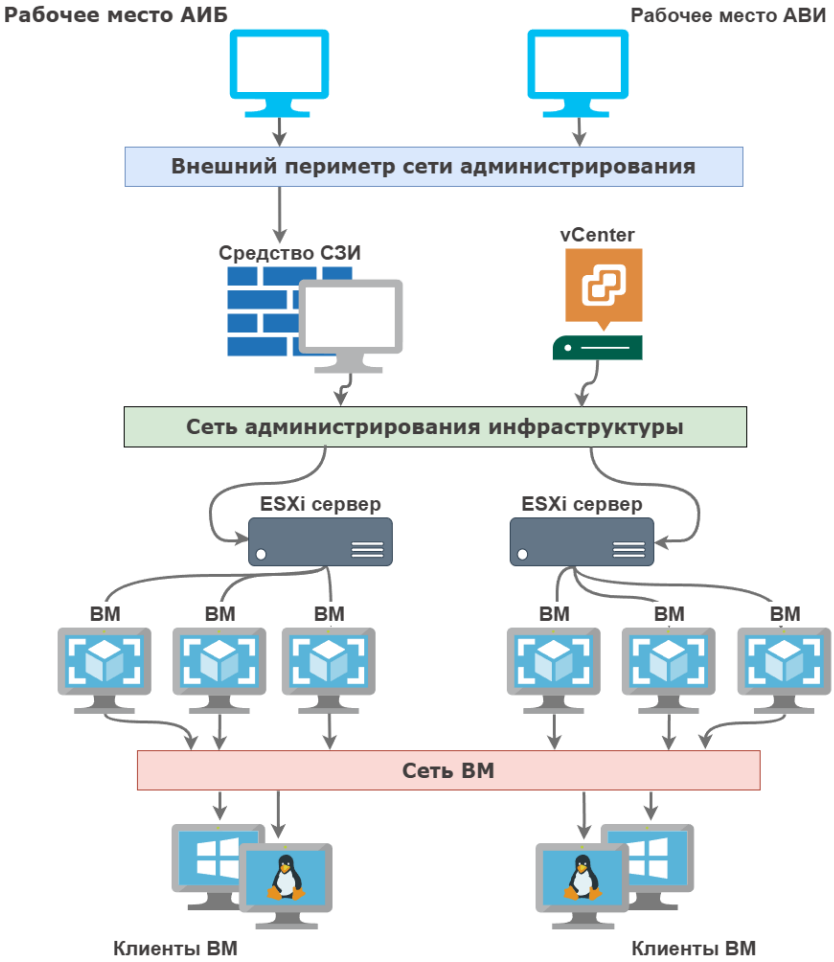


Рис. 1. Схема обеспечения безопасности виртуальной инфраструктуры

Задачи защиты систем виртуализации

Задачи защиты систем виртуализации подразделяются в зависимости от типов угроз. Каждая из которых требует детального анализа и проработки механизмов противодействия:

– основные задачи защиты систем виртуализации;
– управление доступом и разграничение доступа;
– обеспечение целостности и конфиденциальности данных;
– отказоустойчивость и резервирование.

Основные задачи защиты систем виртуализации

Предотвращение угроз хостовой системе и нарушения работы аппаратных компонентов: сбой в работе хоста, связанный с его аппаратными частями может привести к нарушению функционирования всех запущенных на нем виртуальных машин. Аппаратные сбои, такие как отказы процессоров, памяти или дисков, могут иметь разрушительные последствия для виртуализированных систем.

Также ВМ, работающие на сервере виртуализации, могут быть связаны виртуальными каналами передачи данных, которые эмулируют реальные телекоммуникационные сети. При переносе вычислительных ресурсов в виртуальное пространство важно сохранить все коммуникации на прежнем уровне, обеспечивая соответствие существующим условиям коммутации и маршрутизации, а также эффективную фильтрацию трафика [3].

Одним из основных рисков остается использование плохо защищенных виртуальных машин с некорректными настройками безопасности. Уязвимости, такие как слабые пароли или отсутствие актуальных патчей, делают их легкой мишенью для злоумышленников. Также важно учитывать риски сетевых атак между виртуальными машинами, так как вирусные заражения или другие формы атак могут быстро распространяться по всей инфраструктуре, нарушая работу системы. Для предотвращения таких угроз требуется внедрение сетевой изоляции, регулярный мониторинг и контроль за настройками безопасности виртуальных машин.

Управление доступом и контроль

Одной из важнейших задач защиты виртуализированных систем является управление доступом и контроль за действиями пользователей в виртуальной среде. Эффективные меры защиты включают многоуровневую аутентификацию и строгий контроль доступа, которые минимизируют риск несанкционированного проникновения и помогают защитить ключевые компоненты, такие как гипервизор и консоль управления виртуальными машинами.

Виртуальные среды также требуют системы мониторинга, способной в реальном времени обнаруживать аномалии и потенциальные угрозы. Такие системы анализируют сетевые подключения, процессы и действия, выявляя подозрительную активность, которая может указывать на угрозы безопасности, такие как попытки несанкционированного доступа или изменение параметров виртуальных машин [4].

Обеспечение целостности и конфиденциальности данных

Некачественное разграничение доступа или нарушение правил безопасности может привести к утечке данных и компрометации всей инфраструктуры. Несанкционированный доступ к сети хранения образов виртуальных машин (ВМ) создает серьезные риски, позволяя злоумышленникам получить доступ к критически важным данным и управлению системой, что может привести к сбоям и утечкам.

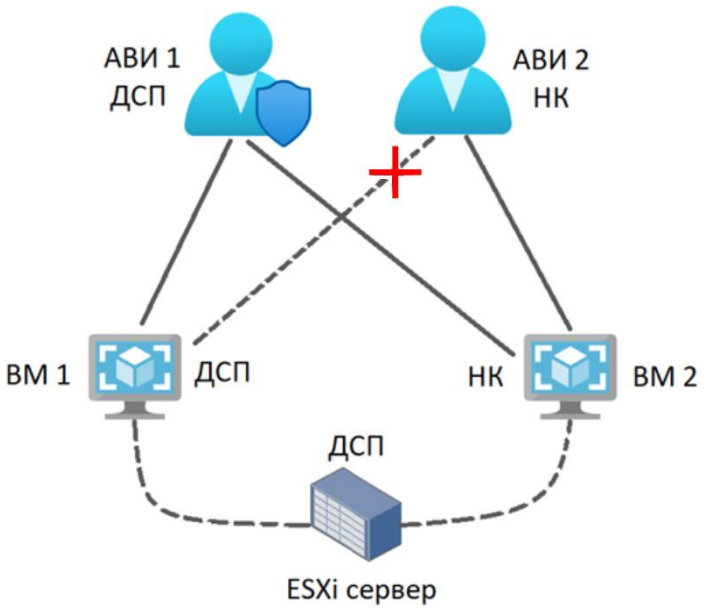


Рис. 2. Пример обеспечения конфиденциальности данных

Неконтролируемый рост числа ВМ без должного управления и мониторинга может привести к значительным нагрузкам на инфраструктуру, усложняя процессы безопасности и увеличивая вероятность уязвимостей. Помимо этого, несанкционированный доступ к консоли управления виртуальными машинами или их настройкам создает угрозу перехвата управления. Злоумышленники, получившие доступ к конфигурациям, могут изменить настройки или получить доступ к конфиденциальным данным, что ставит под угрозу безопасность всей виртуальной среды.

Виртуализированные среды часто содержат конфиденциальные данные, включая персональную информацию. Для защиты этих данных необходимо строгое разграничение прав доступа, шифрование информации и соблюдение требований законодательства по защите персональных данных. Нарушение конфиденциальности данных может повлечь за собой юридические и репутационные риски, поэтому важно уделять внимание обеспечению безопасности на каждом этапе управления данными.

Образы ВМ, содержащие конфиденциальные данные, могут быть подвержены несанкционированному копированию или искажению, что создает угрозу безопасности [3]. Пример разграничения конфиденциальной информации представлен на рисунке 2. Уничтожение или повреждение носителей данных с образами ВМ может привести к потере информации и отказу в доступе к виртуальным машинам. Чтобы минимизировать такие риски, важно использовать надежное резервное копирование и механизмы контроля целостности данных, такие как хэш-суммы и цифровые подписи.

Виртуальные машины, содержащие данные разных уровней конфиденциальности, должны быть изолированы для предотвращения утечек информации в случае компрометации одной из ВМ. При миграции данных между ВМ необходимо применять шифрование, чтобы исключить риск перехвата.

Отказоустойчивость и резервирование

Отказоустойчивость и резервирование являются важнейшими аспектами обеспечения надежности и стабильности виртуализированных систем [4]. Одной из серьезных угроз для работы виртуальных машин (ВМ) является неисправность сетевых коммуникаций [2]. Поскольку виртуализированные среды сильно зависят от сетевой инфраструктуры для обмена данными и управления ВМ, сбои в работе сети могут привести к потере доступа к ВМ, а также к нарушению работы всех сервисов, работающих на виртуализированных платформах. В случае отказа ключевых сетевых компонентов, таких как маршрутизаторы, коммутаторы или серверы виртуализации, весь процесс виртуализации может быть приостановлен, что приведет к серьезным проблемам в организации бизнеса.

Заключение

Виртуальные среды обеспечивают гибкость и масштабируемость, но при этом они уязвимы к различным видам атак и техническим сбоям, поскольку множество виртуальных машин работают на общем аппаратном оборудовании под управлением гипервизора, он является одной из ключевых точек безопасности, поэтому основное внимание уделяется его защите, а также поддержанию его надежной изоляции от других элементов системы.

Таким образом эффективная защита виртуальных машин предполагает не только обеспечение их изоляции друг от друга и от гипервизора, но и контроль доступа, регулярное обновление ПО и мониторинг безопасности. Использование многоуровневой аутентификации, разграничения доступа, разделения сети на сегменты позволяет сократить риск несанкционированного доступа.

Важнейшим элементом обеспечения безопасности является управление доступом и аудит всех действий в виртуализированной среде. Виртуальные сети, которые связывают виртуальные машины, также подвержены угрозам. Защита сетевой инфраструктуры требует применения механизмов шифрования, изоляции сетевых сегментов и регулярного мониторинга трафика. Важнейшим элементом обеспечения безопасности является управление доступом и аудит всех действий в виртуализированной среде.

Список используемых источников

1. Virtualization Security – защита виртуализации. URL: https://cloudnetworks.ru/inf-bezopasnost/virtualization-security/ (дата обращения 02.11.2024).
2. Средство защиты информации vGate R2. Руководство администратора. https://www.securitycode.net/upload/iblock/522/vGate %20R2 %20vSphere %20- %20Руководство %20администратора %20- %20Установка, %20настройка %20и %20эксплуатация.pdf (дата обращения 02.11.2024).
3. Угрозы ИБ систем виртуализации и современные средства защиты. URL: https://lib.itsec.ru/articles2/Oborandteh/ugrozy-ib-sistem-virtualizatsii-i-sovremennye-sredstva-zaschity (дата обращения 02.11.2024).
4. Печенкина А. В., Селифанов В. В. Системы обеспечения безопасности, применяемые при использовании технологии виртуализации // Интерэкспо Гео-Сибирь. 2019. № 2. С. 150–158 (дата обращения 07.11.2024).

***Dyusmetova A.* TASKS OF PROTECTION OF VIRTUALIZATION SYSTEMS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Modern virtualized environments have become an integral part of OT infrastructures, providing flexibility and scalability for business tasks. However, virtualization carries unique risks that require a special approach to security, fault tolerance, and redundancy. The article examines the main threats to virtual systems, ranging from hardware failures and network communications to specific risks associated with the hypervisor, virtual machines and their network infrastructure.

Key words: Virtualization, hypervisor, authentication, virtual machine.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ СЕТЕВОГО ТРАФИКА С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

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

Статья посвящена рассмотрению вопросов, связанных с анализом сетевого трафика. Описывается актуальность и имеющиеся проблемы. Рассматривается необходимость анализа сетевого трафика и его основные методы. Изучается потенциал использования искусственного интеллекта в решении задач анализа сетевого трафика, а также проблемы, с которыми можно столкнутся при его использовании.

информационная безопасность, компьютерные сети, анализ сетевого трафика, нейронные сети, машинное обучение, искусственный интеллект

Современный мир неразрывно связан с информационными технологиями. Цифровые сети стали неотъемлемой частью нашей жизни, обеспечивая связь, доступ к информации, управление ресурсами и многое другое. Использование сетевых технологий передачи данных давно стало основой коммуникации человечества. Нарушение работы сети приводит к угрозам потери важных данных, остановке бизнес-процессов и ряду других проблем. Также нельзя забывать, что любому устройству, работающему в локальной вычислительной сети, потенциально угрожают атаки со стороны злоумышленников.

Для диагностики и защиты сетевых ресурсов, необходимо обеспечить своевременное обнаружение состояний сети, приводящих в последствии к нарушениям в ее работе, уничтожению, изменению или утечке информации, возникающих вследствие отказов, случайных сбоев или являющихся результатом получения злоумышленником несанкционированного доступа к сетевым ресурсам, вторжения сетевых червей, вирусов и других угроз информационной безопасности. Своевременное обнаружение таких состояний даст возможность устранить их причину, а также предотвратить потенциальные последствия [1].

Одним из вариантов отслеживания работоспособности сети и предотвращения нарушения ее работы является анализ сетевого трафика. Анализ трафика в рамках информационной безопасности способствует обнаружению вторжений, перегрузок сети или других внутренних и внешних аномалий, основные виды которых представлены на рисунке 1.

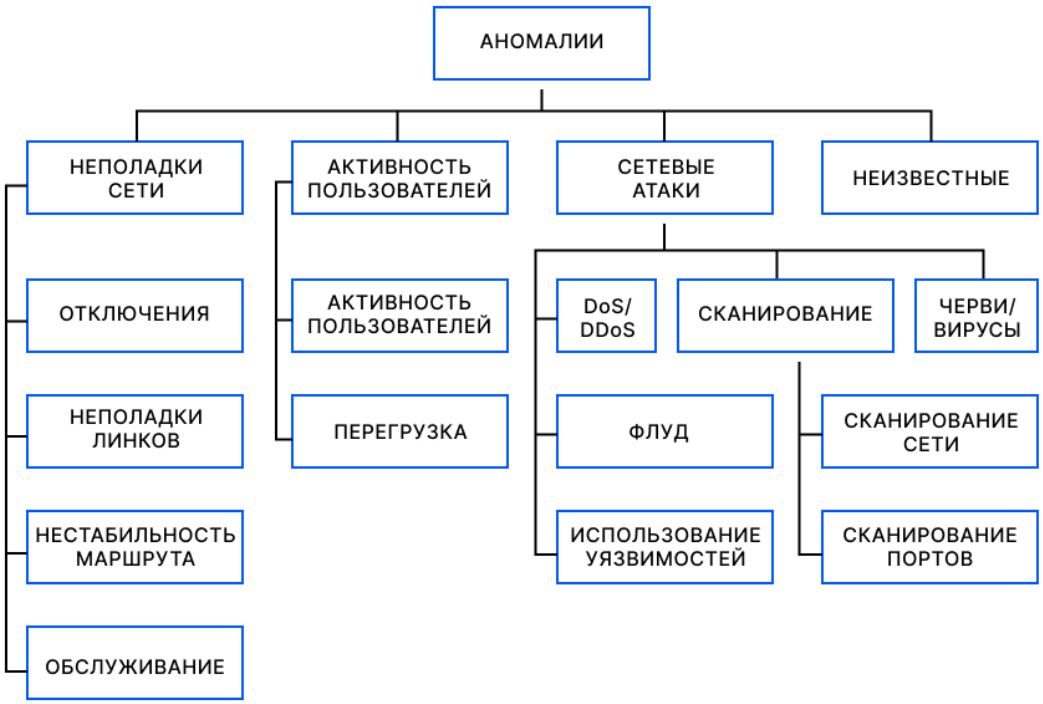


Рис. 1. Виды аномалий в сети

Для решения задач мониторинга и анализа трафика используются различные системы, такие как межсетевые экраны, антивирусы и системы обнаружения вторжений.

Основные методы, использующиеся для анализа сетевого трафика основаны на сравнении с известными шаблонами (сигнатурами) и обнаружении аномалий для нахождения нелегитимных действий и предотвращения вторжений в сеть [1].

Анализ на основе сигнатур. Данный метод основан на создании сигнатур или уникальных шаблонов, соответствующих известным сценариям действия вредоносного программного обеспечения, вирусов или других атак. Когда сетевой трафик соответствует заданной сигнатуре, на него устанавливается метка для дальнейшей проверки или блокировки.

Обнаружение аномалий. Методы анализа, которые используются для выявления аномального состояния сети основываются на отклонении значений от некоторого нормального состояния. Такие отклонения показывают изменения сети, которые могут сигнализировать о технических неполадках или об атаках злоумышленников на сетевые ресурсы. Такой подход дает возможность находить как известные аномалии трафика, так и новые типы. Методы анализа должны корректно и с достаточной точностью определять нормальное состояние сети и отклонения от него для недопуска ложных срабатываний или игнорирования аномалий. Алгоритмы обнаружения аномалий создаются на основе статистического анализа, машинного обучения или других методах. Методы, основанные на обнаружении аномалий, являются более перспектив-

ными. Их ключевая особенность – возможность обнаружения новых атак без знания их сигнатур.

С ростом скоростей и объемов трафика, а также с растущей сложностью методов реализации атак, становится труднее анализировать трафик обычными методами, поэтому использование искусственного интеллекта для анализа сетевого трафика становится все более актуальным и перспективным. С помощью искусственного интеллекта можно автоматизировать процессы анализа, находить сложные закономерности в сетевом трафике, выявлять новые и неизвестные угрозы и адаптироваться к изменениям в поведении злоумышленников [2].

Первые исследования в области применения искусственного интеллекта в задачах анализа сетевого трафика были посвящены машинному обучению. Машинное обучение дало возможность классифицировать трафик и идентифицировать различные типы протоколов и приложений. При этом алгоритмам машинного обучения необходимы признаки классифицируемых примеров, на основе которых будет приниматься решение. Это заложило основу для более сложных подходов, включая обнаружение аномалий, когда модели искусственного интеллекта обучались выявлять отклонения от нормального поведения сети, потенциально указывающие на вредоносную активность. Метод глубокого обучения, усложненное машинное обучения, также включает в себя обучение нейронных сетей на больших объемах данных, чтобы выявлять закономерности и делать прогнозы [3]. Эти нейронные сети можно использовать для задач анализ сетевого трафика.

Нейронные сети могут использоваться в информационной безопасности для различных задач, таких как обнаружение вторжений, анализ безопасности сети, идентификацию пользователей, а также классификацию и анализ сетевого трафика. Также обучение позволяет нейронным сетям находить аномалии и атаки, которые могут оказаться сложными для обнаружения с помощью стандартных методов [4]. Эти достижения привели к разработке систем обнаружения вторжений на базе искусственного интеллекта, которые могут выявлять угрозы и реагировать на них в режиме реального времени, повышая безопасность и устойчивость сети.

В качестве недостатков использования методов машинного обучения и нейронных сетей можно выделить недостаточное количество данных для обучения [5]. Существуют уже готовые наборы данных для обучения, такие как NIMS 2007, CICIDS 2018, CICIDS 2017, UGR-16, NSL-KDD 2009, Kyoto 2006, KDD Cup 1999 и другие [6]. Краткое описание указанных датасетов приведено в таблице 1.

Таблица 1. Описание готовых датасетов

Название датасета	Объем	Описание	Вид трафика	Аномалии
NIMS 2007	10 ГБ	Сетевой трафик, собранный за 2 месяца в американском университете	HTTP, FTP, DNS, TCP, UDP	DDoS, SYN Flood, Port Scan, Botnet
CICIDS 2018	78 ГБ	Создан для моделирования современного сетевого трафика, включая атаки на веб-приложения, криптомайнинг, ботнеты	HTTP, HTTPS, DNS, TCP, UDP	DDoS, Brute Force, SQL Injection, XSS, Cryptojacking
CICIDS 2017	2.5 ГБ	Сетевой трафик, собранный с помощью Cisco NetFlow	HTTP, HTTPS, DNS, TCP, UDP	DDoS, Botnet, Web Attack, Infiltration
UGR-16	20 ГБ	Сетевой трафик, записанный в университете в Испании	HTTP, HTTPS, DNS, TCP, UDP	DDoS, Brute Force, SQL Injection, XSS
NSL-KDD 2009	4.5 ГБ	Подмножество KDD Cup 1999, сбалансированное по количеству экземпляров каждого класса атак	TCP, UDP, ICMP	DDoS, Probe, R2L, U2R
Kyoto 2006	2 ГБ	Сетевой трафик, записанный в университете в Японии	TCP, UDP	DDoS, Probe, R2L, U2R
KDD Cup 1999	4.9 ГБ	Сетевой трафик, записанный в военном центре США	TCP, UDP, ICMP	DDoS, Probe, R2L, U2R

Однако следует учитывать, что применение готовых наборов данных не всегда эффективно и для конкретной сети может потребоваться собрать собственный набор.

Также надо упомянуть, что натренированная для определенных условий нейронная сеть может давать ложные срабатывания при использовании с другим трафиком. Таким образом, необходимо проводить грамотное тестирование таких систем перед внедрением их в сеть для решения боевых задач.

Использование методов искусственного интеллекта для обеспечения сетевого анализа находится в активной стадии развития. Несмотря на то, что достигнуты определенные успехи в этом направлении, исследования в этой области продолжаются для решения существующих проблем и поиска новых методов. Это включает в себя улучшение интерпретируемости и объяснимости, а также решение проблемы нехватки данных в определенных контекстах сетевой безопасности. Несмотря на проблемы, потенциал использования искусственного интеллекта для анализа сетевого трафика остается крайне высоким и требует дальнейшего исследования.

Список используемых источников

1. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Под ред. профессора О. И. Шелухина. М.: Горячая линия–Телеком, 2016. 220 с.
2. Шелухин О. И., Ерохин С. Д., Полковников М. В. Технологии машинного обучения в сетевой безопасности. Горячая линия–Телеком, 2021. 353 с.
3. Скрыпников А. В. Использование методов машинного обучения при решении задач информационной безопасности / А. В. Скрыпников, В. В. Денисенко, И. А. Саранов // Вестник Воронежского института ФСИН России. 2020. №4. С. 69–73. EDN MYVNUV
4. Симаворян С. Ж., Симонян А. Р., Попов Г. А., Улитина Е. И. Общая концепция выявления вторжений неизвестного типа на основе нейронных сетей» // Программные системы и вычислительные методы. 2021. №4. С.23-45. DOI: 10.7256/2454-0714.2021.4.37072
5. Чаругин В. В., Чесалин А. Н. Анализ и формирование наборов данных сетевого трафика для обнаружения компьютерных атак // International journal of open information technologies. 2023. Т. 11. № 6. С. 100–106. EDN: HZDNHW
6. Гетьман А. И., Горюнов М. Н., Мацкевич А. Г., Рыболовлев Д. А. Методика сбора обучающего набора данных для модели обнаружения компьютерных атак. Труды ИСП РАН, 2021. Т. 33 (5). С. 83–104. DOI: 10.15514/ISPRAS–2021–33(5)–5

Ivanov R. **NETWORK TRAFFIC ANALYSIS USING ARTIFICIAL INTELLIGENCE.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article is devoted to the consideration of issues related to the analysis of network traffic. The relevance and existing problems are described. The necessity of analyzing network traffic and its main methods are considered. The potential of using artificial intelligence in solving network traffic analysis problems is considered, as well as the problems that can be encountered when using it.

Key words: information security, computer networks, network traffic analysis, neural networks, machine learning, artificial intelligence.

УДК 004.056
ГРНТИ 81.93.29

ОСОБЕННОСТИ ТИПОВЫХ АРХИТЕКТУР ОБЛАЧНЫХ ИНФРАСТРУКТУР ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. О. Камалова, И. Е. Пестов, Д. Н. Смирнов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

В статье рассматриваются аспекты безопасности трех основных моделей облачных услуг: инфраструктура как услуга, платформа как услуга и программное обеспечение как услуга. Облачные сервисы требуют особого внимания к вопросам безопасности из-за уникальных рисков, связанных с каждой моделью. Комплексный подход к безопасности, включая технологии, процессы и обучение пользователей, поможет эффективно защищать данные в облачных сервисах.

IaaS, SaaS, PaaS, облачная инфраструктура, архитектура облачных инфраструктур

Облачная инфраструктура – это совокупность аппаратных и программных ресурсов, составляющих облако [1]. Поставщики облачных услуг обслуживают глобальные центры обработки данных с тысячами компонентов ИТ-инфраструктуры: серверы, физические устройства хранения данных и сетевое оборудование. Они настраивают физические устройства с использованием всех типов конфигураций операционной системы и устанавливают другие типы программного обеспечения, необходимого для запуска приложения.

Виды архитектур облачных инфраструктур

IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service) и SaaS (Software-as-a-Service) являются тремя наиболее популярными типами облачных услуг [2]. Их иногда называют моделями облачных услуг или моделями облачных вычислений.

IaaS (инфраструктура как услуга) представляет собой доступ по требованию к облачным физическим и виртуальным серверам, хранилищам и сетям (т. е. серверной ИТ-инфраструктуре) для запуска приложений и рабочих нагрузок в облаке.

Примеры на российском рынке:

– CloudMTS;
– SberCloud;
– VK Cloud;
– Yandex Cloud.

PaaS (платформа как услуга) представляет собой доступ по требованию к полной, готовой к использованию, облачной платформе для разработки, запуска, обслуживания и управления приложениями.

Примеры на российском рынке:

– SberCloud;

– VK Cloud;

– Yandex Cloud.

SaaS (программное обеспечение как услуга) представляет собой доступ по требованию к готовому к использованию, размещенному в облаке прикладному программному обеспечению.

Примеры:

– электронная почта;

– облачные хранилища данных;

– CRM-системы, учетные системы;

– приложения для планирования и постановки задач;

– сервисы онлайн-встреч;

– системы электронного документооборота;

– платформы для создания сайтов, интернет-магазинов;

– офисные программы.

Многие организации используют несколько одного видов облачных инфраструктур для работы, а большинство крупных предприятий используют все три.

Безопасность типовых архитектур облачных инфраструктур

Безопасность систем, использующих облачные сервисы, требует разделения ответственности между клиентом (владельцем конечной системы) и провайдером (владельцем облачной инфраструктуры). Это разделение зависит от модели облачных сервисов. В таблице 1 представлено разделение ответственности за обеспечение безопасности, где X – зона ответственности провайдера, пустая ячейка – зона ответственности клиента.

ТАБЛИЦА 1. Разделение ответственности за обеспечение безопасности

Параметр сравнения	IaaS	PaaS	SaaS
Управление доступом к данным			
Безопасность приложений			X
Безопасность ОС		X	X
Сетевая безопасность (Overlay)		X	X
Резервирование		X	X

Параметр сравнения	IaaS	PaaS	SaaS
Шифрование		X	X
Логи аудита	X	X	X
Безопасность хранилища данных и оборудования	X	X	X
Сетевая безопасность (Underlay)	X	X	X
Физическая безопасность и катастрофоустойчивость	X	X	X

Во всех четырех ситуациях только клиент контролирует и управляет правами доступа. Остальная ответственность зависит от модели.

Безопасность в облачных сервисах IaaS, PaaS и SaaS обеспечивается с помощью различных методов и технологий.

Шифрование данных: данные передаются между клиентом и облачным провайдером в зашифрованном виде, что снижает риск утечки информации;

Аутентификация и авторизация: пользователи должны пройти процедуру аутентификации (ввод логина и пароля) и авторизации (подтверждение прав доступа к ресурсам) перед использованием облачных сервисов;

Многофакторная аутентификация: использование нескольких факторов аутентификации, таких как пароль, токен, биометрические данные или SMS-код, повышает уровень безопасности;

Резервное копирование и восстановление данных: клиенты могут создавать резервные копии своих данных и восстанавливать их в случае потери или повреждения;

Мониторинг и аудит: облачные провайдеры отслеживают активность пользователей и ресурсов, а также предоставляют отчеты о работе системы для анализа и улучшения безопасности [3,4];

Соблюдение стандартов и сертификация: облачные провайдеры должны соблюдать определенные стандарты безопасности, такие как ISO 27001, PCI DSS и другие, и иметь соответствующие сертификаты [5];

Использование межсетевых экранов и виртуальных частных сетей (VPN): для защиты данных и приложений от внешних угроз используются брандмауэры и VPN, которые обеспечивают шифрование трафика и контроль доступа к ресурсам;

Регулярное обновление программного обеспечения: клиенты и облачные провайдеры должны регулярно обновлять программное обеспечение и операционные системы для устранения уязвимостей и повышения безопасности;

Обучение персонала: облачные провайдеры должны проводить обучение своего персонала по вопросам безопасности, чтобы сотрудники могли выявлять и предотвращать возможные угрозы.

Заключение

Каждая модель облачных сервисов требует индивидуального подхода к безопасности. При разработке стратегии защиты важно учитывать особенности каждой модели облачных сервисов: инфраструктура, доступ к данным, управление правами доступа и потенциальные угрозы. Комплексный подход к обеспечению безопасности включает использование инструментов для мониторинга и предотвращения атак, внедрение процессов управления безопасностью, а также регулярное обучение сотрудников и пользователей основным навыкам в области информационной безопасности. Это позволит значительно снизить риски утечки данных и обеспечить надежную защиту информации в облаке.

Список используемых источников

1. Красов А. В., Левин М. В., Фостач Е. С. Проблемы обеспечения безопасности облачных вычислений // Информационная безопасность регионов России (ИБРР-2017): Материалы конференции, Санкт-Петербург, 01–03 ноября 2017 года. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2017. С. 520–522.
2. Алехин Р. В., Красов А. В., Макарова А. Д., Орлов Г. А. Облачные сервисы. Принцип работы, классификация и модели обслуживания // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2022. Том 1. С. 70–74.
3. Гельфанд А. М., Косов Н. А., Красов А. В., Орлов Г. А. Защита для распределенных отказов в обслуживании в облачных вычислениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Том 1. С. 329–334.
4. Красов А. В., Ягудин И. Р. Анализ активных сетевых атак: arp-spoofing и dns-spoofing // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. Том 1. С. 520–526.
5. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности: учебное пособие. СПб.: СПбГУТ, 2012. 396 с.

Kamalova A., Pestov I., Smirnov D. **SECURITY FEATURES OF TYPICAL CLOUD INFRASTRUCTURE ARCHITECTURES.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article considers the security aspects of three main models of cloud services: IaaS (infrastructure as a service), PaaS (platform as a service) and SaaS (software as a service). Cloud services require special attention to security issues due to the unique risks associated with each model. A comprehensive approach to security, including technologies, processes and user training, will help to effectively protect data in cloud services.

Key words: IaaS, SaaS, PaaS, cloud infrastructure, cloud infrastructure architecture.

УДК 004.056.55
ГРНТИ 81.93.29

КВАНТОВО-УСТОЙЧИВАЯ ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ

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

В условиях стремительного роста объемов персональных данных и конфиденциальной информации вопросы их защиты приобретают первостепенное значение в обеспечении цифровой безопасности. Инфраструктура открытых ключей является основным инструментом для обеспечения конфиденциальности, подлинности и целостности данных. Однако с появлением квантовых вычислений традиционные криптографические алгоритмы, используемые в инфраструктуре открытых ключей, сталкиваются с новыми угрозами. В данной работе рассматривается переход на квантово-устойчивую криптографию, которая обеспечивает защиту от атак квантовых компьютеров. Приводится обзор современных квантово-устойчивых алгоритмов и анализируется их интеграция в существующие системы инфраструктуры открытых ключей, включая такие аспекты, как эффективность, совместимость и стандартизация.

квантовые компьютеры, криптографические средства защиты информации, информационная безопасность, алгоритмы шифрования

С развитием квантовых вычислений традиционные криптографические методы, такие как RSA и эллиптические кривые (ECC), становятся уязвимыми перед атаками, которые способны реализовать квантовые компьютеры. Эти технологии могут сломать алгоритмы, защищающие коммуникации, аутентификацию и данные в системах инфраструктуры открытых ключей (Public Key Infrastructure, PKI). Квантово-устойчивая криптография (Post-Quantum Cryptography, PQC) призвана обеспечить безопасность в условиях квантовых угроз, предлагая альтернативные алгоритмы, которые устойчивы к атакам с использованием квантовых компьютеров.

PKI является основным компонентом современных систем безопасности, обеспечивая криптографические механизмы для шифрования, цифровых подписей и проверки подлинности. Ключевыми элементами традиционной PKI являются:

– центры сертификации (Certificate Authorities, CA), которые выдают цифровые сертификаты;

– ключи и сертификаты: публичные ключи хранятся и управляются с помощью цифровых сертификатов, которые обеспечивают привязку ключа к субъекту;

– протоколы безопасности: протоколы, такие как TLS/SSL, зависят от криптографических алгоритмов, таких как RSA и ECC.

Угроза квантовых компьютеров заключается в том, что они могут использовать алгоритмы, такие как алгоритм Шора, для эффективного решения задач факторизации и дискретного логарифмирования, на которых основана безопасность RSA и ECC. Таким образом, атака на традиционную PKI с использованием квантовых компьютеров может привести к взлому сертификатов и подделке цифровых подписей [1].

Квантово-устойчивая криптография разрабатывается для обеспечения безопасности даже в условиях появления квантовых вычислений. В инфраструктуре открытых ключей это означает использование квантово-устойчивых криптографических алгоритмов для ключевого обмена, цифровых подписей и шифрования данных. Такие алгоритмы должны сохранять стойкость как против классических, так и квантовых атак [2].

Алгоритмы на основе решеток (Lattice-based cryptography) – одним из ключевых преимуществ решеточной криптографии является ее устойчивость к атакам с использованием квантовых компьютеров. Алгоритмы, такие как Crystals-Kyber и Crystals-Dilithium, уже рассматриваются для стандартизации в рамках программы NIST и могут использоваться для квантово-устойчивого обмена ключами и создания цифровых подписей. Подробнее об алгоритмах приведено в таблице 1.

ТАБЛИЦА 1. Алгоритмы на основе решеток

Алгоритм	Пояснение
Crystals-Kyber	Алгоритм основан на задаче обучения с ошибками (Learning with Errors, LWE) и предназначен для защиты передачи симметричных ключей
Crystals-Dilithium	Алгоритм является одной из перспективных схем цифровых подписей и основан на решении сложных задач на решетках

Кодово-зависимые алгоритмы (Code-based cryptography) – одним из известных алгоритмов этого класса является Classic McEliece, основанный на исправлении ошибок и кодах Гоппы. Этот алгоритм считается устойчивым к квантовым атакам, так как основан на сложной задаче декодирования случайного линейного кода. Основным преимуществом McEliece является высокая степень безопасности, но его недостаток заключается в больших размерах публичных ключей, что создает проблемы с хранением и передачей данных.

Многочленные алгоритмы (Multivariate polynomial cryptography) – эти алгоритмы основываются на решении систем многочленов над конечными полями. Примером является Rainbow, который используется для цифровых подписей. Многочленные алгоритмы могут обеспечить высокую стойкость к квантовым атакам, но их производительность и эффективность требуют дальнейших улучшений.

Хеш-основанная криптография (Hash-based cryptography) – алгоритмы, такие как SPHINCS+, используют хеш-функции для создания квантово-устойчивых схем цифровых подписей. Хеш-основанные схемы отличаются высокой безопасностью, однако их недостатком являются большие размеры подписей, что может усложнить их использование в некоторых системах [3].

Создание квантово-устойчивой инфраструктуры открытых ключей требует модификации ключевых компонентов инфраструктуры открытых ключей.

Для успешного внедрения квантово-устойчивой криптографии в инфраструктуру открытых ключей необходимо внести ряд ключевых изменений, которые представлены в таблице 2.

ТАБЛИЦА 2. Изменяемые компоненты инфраструктуры открытых ключей

Объект	Изменение	Последствия
Ключевой обмен	Традиционные методы обмена ключами, такие как Диффи-Хеллман или алгоритмы на основе эллиптических кривых, должны быть заменены на квантово-устойчивые решения, такие как Crystals-Kyber или NTRUEncrypt	При установлении защищенного соединения вместо традиционного алгоритма Диффи-Хеллмана используется Crystals-Kyber для безопасного обмена симметричными ключами, которые будут использоваться для шифрования данных
Цифровые подписи	Криптографические алгоритмы RSA и ECDSA, могут быть заменены на Crystals-Dilithium, Falcon или SPHINCS+, которые обеспечивают защиту от атак с использованием квантовых компьютеров	Вместо использования RSA или ECDSA для подписи сертификатов и сообщений применяется квантово-устойчивая схема, например, Crystals-Dilithium. Это обеспечивает защиту цепочек доверия и подлинности данных
Управление сертификатами	Центры сертификации должны переходить на квантово-устойчивые цифровые подписи для создания и управления сертификатами	Центры сертификации начинают выдавать квантово-устойчивые сертификаты, подписанные алгоритмами, такими как Falcon или SPHINCS+. Такой переход позволит повысить устойчивость системы к квантовым атакам

Однако, несмотря на множественные положительные аспекты, которые последуют после повсеместного применения данной технологии, специали-

сты могут столкнуться с рядом проблем, таких как совместимость, производительность, стандартизация и масштабируемость.

Использование квантово-устойчивой инфраструктуры открытых ключей неотъемлемая часть эволюции ИТ-сферы. Несмотря на многочисленные проблемы, с которыми придется столкнуться исследователям и разработчикам, которые занимаются информационной безопасностью, переход на новую ступень защиты уязвимых данных необходим не только большим корпорациям и государственным организациям, но и небольшим предприятиям, обрабатывающим персональные данные, технологическую и конфиденциальную информацию.

Поэтапное внедрение квантово-устойчивых алгоритмов совместно с использованием гибридных схем помогут разработать криптографические системы, способные противостоять квантовым атакам, а также минимизировать риски.

Список используемых источников

1. Глозштейн, Д. А. Обеспечение безопасности инфраструктуры открытых ключей в условиях развития квантовых компьютеров / Д. А. Глозштейн // Вопросы обеспечения безопасности в киберпространстве: Материалы II Всероссийской научно-технической конференции, Махачкала, 10–11 мая 2024 года. Махачкала: Типография ФОРМАТ, 2024. С. 148–153. EDN NVFCIO.
2. Султан К. Б. Изучение возможностей и ограничений квантово-устойчивых криптографических алгоритмов / К. Б. Султан // Научный аспект, 2023. Т. 20, № 5. С. 2490–2500. EDN NVMKUF.
3. Гавриков И. В. Обзор квантово-устойчивых криптографических алгоритмов / И. В. Гавриков // Дни науки КФУ им. В. И. Вернадского: V научно-практическая конференция профессорско-преподавательского состава, аспирантов, студентов и молодых ученых. Сборник тезисов участников. Секция «Бизнес-информатика и математическое моделирование», Симферополь, 29 октября 2019 года. Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2019. С. 17–19. EDN OAZPHO.

***Kirilova D.* QUANTUM-STABLE PKI.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the context of the rapid growth of personal data and confidential information, the issues of their protection are of paramount importance in ensuring digital security. The public key infrastructure is the main tool for ensuring confidentiality, authenticity and integrity of data. However, with the advent of quantum computing, traditional cryptographic algorithms used in public key infrastructure are facing new threats. In this paper, we consider the transition to quantum-stable cryptography, which provides protection against attacks by quantum computers. An overview of modern quantum-stable algorithms is provided and their integration into existing public key infrastructure systems is analyzed, including aspects such as efficiency, compatibility and standardization.

Key words: quantum computers, cryptographic information security tools, information security, encryption algorithms.

УДК 004.89
ГРНТИ 20.15.05

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ В КИБЕРБЕЗОПАСНОСТИ

Н. Д. Кулиныч
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В последние годы искусственный интеллект и машинное обучение стали неотъемлемыми инструментами в области кибербезопасности, обеспечивая новые возможности для защиты информационных систем от все более сложных угроз. Данная работа посвящена анализу применения ИИ и МО в кибербезопасности, включая их роль в обнаружении и предотвращении кибератак, анализе угроз, а также в автоматизации процессов реагирования на инциденты.

машинное обучение, искусственный интеллект, кибератака, безопасность

Современный мир полностью зависит от информационных технологий и цифровых средств обмена информацией. Однако по мере того, как связи между обществом и экономикой становятся все более зависимым и от них, растут и угрозы кибербезопасности. Кибертаки, утечка данных и киберпреступность представляют серьезную угрозу для организаций и государств.

В последние время термин «искусственный интеллект» (ИИ) стал одним из самых популярных в СМИ.

Искусственный интеллект – это способность компьютерной системы или машины реализовывать задачи, имитируя человеческий интеллект. Искусственный интеллект обычно подразделяют на три категории: Слабый искусственный интеллект (NarrowAI), Сильный искусственный интеллект (GeneralAI) и Суперинтеллект (Superintelligence).

Слабый искусственный интеллект. Применяется для решения только одной конкретной задачи и выдачи данных. Эти системы не обладают общим пониманием или сознанием, они только могут выполняют запрограммированные функции. Слабый ИИ является самым распространенным типом ИИ на сегодняшний день и используется в различных сферах.

Сильный искусственный интеллект. Этот вид ИИ новый. Способен мыслить, принимать решение как человек.

Суперинтеллект. Вид машинного интеллекта, опережающий человеческий разум, он решает любую задачу лучше человека. Этого вида искусственного интеллекта пока еще нет.

Искусственный интеллект - широкая область, включающая в себя множество методик, из которых машинное обучение можно рассматривать как средство для реализации ИИ.

По своей сути машинное обучение – это инструмент для всех трех типов ИИ. Машинное обучение обычно определяется как использование алгоритмов для анализа огромных массивов данных и обучения компьютеров распознаванию закономерностей и выявлению ценной информации без человеческого задействования [1]. Модели МО могут предсказывать будущее поведение киберугрозы на основе имеющихся данных, позволяя организациям своевременно реализовывать меры безопасности и уменьшать вероятность успешных результатов в атаках на ситемы, а также обучаться на данных предыдущих атак.

Кибербезопасность – это одна из самых актуальных проблем современного мира. Количество киберугроз растет с каждым годом, а традиционные методы защиты становятся все менее эффективными. Искусственный интеллект может стать эффективным средством в борьбе с киберугрозами.

Искусственный интеллект находит широкое применение в области кибербезопасности для улучшения защиты информационных систем:

– системы обнаружения вторжений (IDS) используют машинное обучение для обнаружения аномалий в сетевом трафике;

– системы предотвращения вторжений (IPS) используют машинное обучение для блокирования известных угроз;

– антивирусные программы используют машинное обучение для обнаружения вредоносного ПО;

– системы управления уязвимостями (VMS), которые используют машинное обучение для обнаружения и устранения уязвимостей в системах.

Благодаря мощным возможностям автоматизации и анализа данных ИИ используется для точного и быстрого анализа больших объемов данных [2]. Системы ИИ используют полученные знания о прошлых угрозах для обнаружения похожих атак в будущем, даже если сама схема атаки изменилась. Безусловно, ИИ имеет множество преимуществ в области кибербезопасности.

1. Быстрое реагирование на определение киберугроз. Некоторые решения безопасности, такие как SIEM или XDR, регистрируют тысячи событий, указывающих на предполагаемое аномальное поведение. Хоть и большинство этих событий безвредны, некоторые из них являются критически опасными, и риск пропустить потенциальную киберугрозу может быть внушающим. ИИ помогает выявлять поистине важные инциденты.

Оно также помогает обнаружить поведение, которое не выглядеть опасным, но в применении с другими действиями сигнализирует на вероятно допустимую угрозу безопасности [3].

2. Упрощение отчетности. Утилиты, использующие искусственный интеллект, могут получать информацию от нескольких источников данных для создания простых отчетов, которыми специалисты по безопасности могут легко пользоваться в своих организациях.

3. Выявление уязвимости. ИИ помогает находить потенциальные риски такие, как незащищенные конфиденциальные данные, устаревшие операционные системы, облачные приложения, неизвестные устройства.

Несмотря на высокую точность, ИИ системы совершают ошибки. Они могут неправильно воспроизводить данные, что приводит к ложным оповещениям о возможных угрозах. Например, алгоритм МО может неверно интерпретировать нормальную активность как подозрительную, что приводит к чрезмерному использованию ресурсов при ложных срабатываниях, поэтому требуется постоянный контроль и настройка систем ИИ, чтобы свести к минимуму такие риски.

Причины ложных срабатываний:

1. Некорректные данные для обучения. Недостаточное количество данных или низкое качество данных может привести к неправильному обучению модели;

2. Плохая настройка моделей. Некорректная настройка параметров может стать причиной высокой частоты ложных срабатываний;

3. Изменение поведения системы. ИИ может воспринимать нормальные изменения в поведении системы или пользователей как аномалии, что может приводить к ложным срабатываниям.

В заключение, можно утверждать, что искусственный интеллект и машинное обучение произвели революцию в области кибербезопасности, предоставляя новые инструменты и возможности для обнаружения, предотвращения угроз и реагирования на кибератаки. Эти технологии позволяют организациям результативно защищать данные в условиях нарастающих и все более изощренных киберугроз, благодаря способности к постоянному обучению и адаптации. Однако использование искусственного интеллекта и ML требует внимательного подхода, включая баланс между их преимуществами и недостатками, а также решение таких проблем, как качество данных и конфиденциальность. С учетом постоянного развития кибербезопасности, искусственный интеллект и машинное обучение будут играть ключевую роль в поддержке защищенности современной цифровой среды.

Список используемых источников

1. В чем разница между машинным и глубоким обучением? URL: https://aws.amazon.com/ru/compare/the-difference-between-machine-learning-and-deep-learning/ (дата обращения 30.11.2024).
2. ИИ в кибербезопасности: трансформация обнаружения и предотвращения угроз. URL: https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/ (дата обращения 01.11.2024).
3. Искусственный интеллект в информационной безопасности: добро или зло. URL: https://b-152.ru/iskusstvennyj-intellekt-v-ib (дата обращения 03.11.2024).

***Kulinych N.* ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN CYBERSECURITY.**

Saint Petersburg State University of Industrial Technologies and Design

In recent years, artificial intelligence and machine learning have become integral tools in the field of cybersecurity, providing new opportunities to protect information systems from increasingly complex threats. This paper analyzes the application of AI and ML in cybersecurity, including their role in detecting and preventing cyberattacks, analyzing threats, and automating incident response processes.

Key words: machine learning, artificial intelligence, cyber attack, security.

УДК 004.056.5
ГРНТИ 81.93.29

ПОДХОД К ОЦЕНКЕ ЭФФЕКТИВНОСТИ АТАК НА ОТРАВЛЕНИЕ ДАННЫХ В МОДЕЛЯХ С АКТИВНЫМ ОБУЧЕНИЕМ

Д. С. Левшун, А. И. Староверов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С развитием и внедрением активного обучения в системах с использованием искусственного интеллекта, важность надежности и безопасности моделей выходит на первый план. Активное обучение, в отличие от привычных методов, позволяет модели динамически выбирать наиболее информативные данные, что особенно эффективно при ограниченном объеме обучающей выборки. Недостатком таких систем является подверженность угрозе отравления данных, которая может снизить их производительность. В данной работе представлен подход к оценке эффективности атак на отравление данных в моделях с активным обучением, ориентированный на изучении поведения модели в зависимости от степени искажения и применения отравления меток как типа атаки.

состязательные атаки, анализ уязвимостей, машинное обучение, безопасность, отравление данных, набор данных

Атаки, направленные на отравление данных, используемых для обучения, представляют собой одну из серьезных угроз для моделей машинного обучения. Особенно уязвимыми к таким атакам являются модели с активным обучением [1], где модель периодически обновляется на новых данных, предоставляемых пользователями, автоматически выбранных из потоков данных или подготовленные тренерами. Активное обучение используется для повышения эффективности классификации в задачах, где данных недостаточно или они требуют значительных затрат на разметку.

Активное обучение позволяет моделям улучшать свои результаты, используя данные, которые поступают в процессе их эксплуатации или подготовленные для дополнительного обучения. Но такой подход делает модели более уязвимыми к атакам, поскольку любые изменения в новых данных могут напрямую повлиять на их результативность, показатели и поведение. Например, добавление искаженных или специально подобранных данных может привести к снижению точности модели или, в худшем случае, к неверным классификациям, что потенциально может причинить значительный вред [2].

Первым шагом является определение целей атаки, поскольку тип атаки определяет выбор подходов к ее оценке. Атаки на отравление данных можно разделить на целевые и общие. Целевые атаки направлены на изменение по-

ведения модели в отношении конкретных примеров или классов, например, чтобы заставить модель ошибочно классифицировать определенные данные. Общие атаки, в свою очередь, стремятся снизить общую производительность модели, делая ее менее эффективной по всем задачам [3]. В контексте активного обучения важно учитывать, что модель может обновляться на новых данных в процессе эксплуатации, что делает ее особенно уязвимой к атаке, так как даже небольшие изменения могут со временем значительно повлиять на ее показатели и производительность в целом.

Второй шаг заключается в создании отравленных данных или порче существующих, которые затем добавляются в обучающий набор модели. Существует множество методов отравления данных, включая добавление ложных меток, искажение признаков или подмену данных. Ложные метки подразумевают преднамеренные изменения меток, чтобы модель ошибочно классифицировала примеры. Искажение признаков представляет собой манипуляцию значениями признаков, чтобы усложнить обучение модели. Подмена данных включает в обучающий набор примеры, созданные для достижения определенного поведения модели. Отравление может быть выполнено одномоментно, добавляя сразу большой объем искаженных данных, а может быть постепенно, что делает атаку менее заметной и более эффективной в долгосрочной перспективе.

Третьим шагом, основании собранных данных проводится анализ устойчивости модели к различным уровням отравления. Если метрики резко падают даже при небольшом проценте отравленных данных, это свидетельствует о высокой уязвимости модели. Если же метрики будут оставаться стабильными до определенного уровня загрязнения, модель можно считать устойчивой к данной атаке. Этот анализ позволяет сделать выводы о том, насколько модель подвержена влиянию отравленных данных и в каких случаях атака может быть наиболее эффективной.

В работе подчеркивается особое влияние отравления данных на конечные показатели модели. Также исследуется влияние различных уровней отравления данных на примере модели с активным обучением. В качестве объекта исследования была выбрана модель PassiveAggressiveClassifier библиотеки scikit-learn, которая применяется для задач классификации с высокими требованиями к скорости обучения [4]. Набор данных, использованный в данном исследовании, был взят из репозитория UCI Machine Learning (Internet Firewall Data, 2019), в котором проводилось исследование классификации журналов межсетевых экранов, проведенное Ertam и Kaya (2018). Меткой был выбран столбец “Action”, представляющей собой 3 категории: “drop”, “deny” и “allow”, их количество и процентное соотношение представлено в таблице 1.

ТАБЛИЦА 1. Набор данных для проведения анализа

Label	Count	Part
Allow	37439	65.4871
Drop	11635	20.3516
Deny	8042	14.0668
Reset-both	54	0.0945

Для адекватной оценки эффективности атаки необходимо выбрать подходящие метрики, которые помогут определить, насколько атака повлияла на модель. В данном случае использовались такие метрики, как Precision, Recall, F1 Score и ROC-AUC. Precision измеряет точность предсказаний модели в положительных классах, показывая долю корректных предсказаний среди всех положительных. Recall измеряет полноту модели, показывая, насколько хорошо она выявляет все положительные примеры. F1 Score – это гармоническое среднее Precision и Recall, которое полезно, когда важно учитывать и точность, и полноту. ROC-AUC отражает способность модели различать положительные и отрицательные классы. Эти метрики помогут оценить, как атаки на отравление данных влияют на различные аспекты работы модели, и дают целостное представление о ее устойчивости к манипуляциям.

На рис. 1 показано изменение значений метрик модели при увеличении процента отравленных данных. Мы использовали отравление меток (label flipping) как вид атаки на модель. Этот вид искажения данных заключается в преднамеренном изменении целевых меток (labels) для части обучающих данных, чтобы модель обучалась на искаженных примерах. Из графика видно, что при росте уровня отравления происходит постепенное снижение всех четырех метрик, что свидетельствует о высокой чувствительности модели к искажению данных. Особенно заметно резкое падение показателей уже при 0,5 % и второе заметное снижение в диапазоне 1–5 %. Самой стойкой оказалась метрика ROC-AUC, так как она оценивает способность модели различать между классами по всей кривой, а не на основе фиксированного порога. Это делает его более устойчивым к искажениям, связанным с изменением меток данных, поскольку влияние отдельных ошибочных меток смягчается при интегральной оценке.

Эти результаты согласуются с выводами других исследований [5], которые так же приходят к выводу, что модели активного обучения особенно уязвимы к отравлению данных. Подобные атаки могут привести к значительным искажениям предсказаний, что потенциально опасно для критически важных приложений.

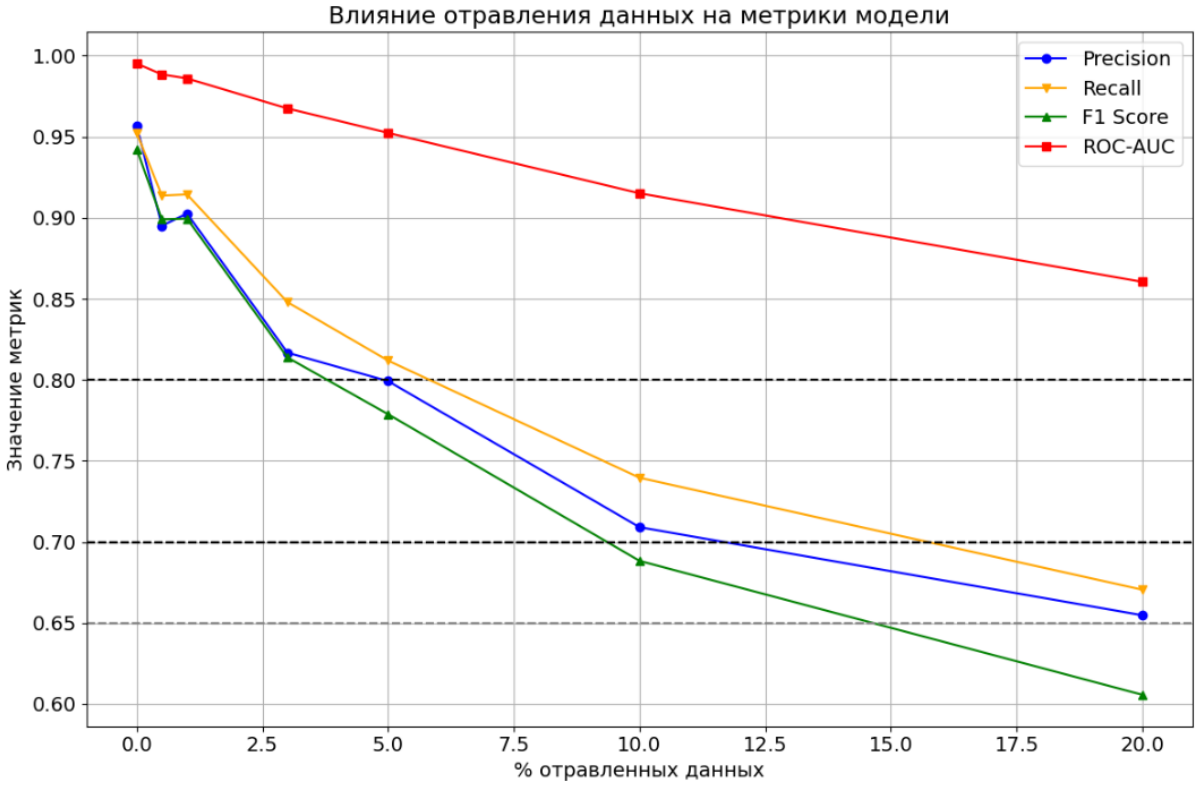


Рис. 1. Влияние отравления данных на метрики модели

Результаты экспериментов продемонстрировали и согласуются с другими исследованиями, что даже незначительное количество отравленных данных может значительно снизить точность и надежность модели, особенно в контексте активного обучения. PassiveAggressiveClassifier оказался весьма чувствительным к добавлению испорченных данных, что может объясняться его особенностями и ориентацией на быструю адаптацию к новым данным.

Это исследование подчеркивает важность разработки устойчивых методов защиты для моделей с активным обучением. К возможным мерам защиты можно отнести внедрение алгоритмов обнаружения аномалий и автоматическое удаление подозрительных данных. Будущие исследования в этой области необходимо сосредоточить на усовершенствовании методов фильтрации данных и использовании более сложных моделей, устойчивых к атакам на отравление, а также разработки алгоритмов обнаружения аномалий и постоянного их совершенствования.

Список используемых источников

1. Levshun D., Tushkanova O., Chechulin A. Two-Model Active Learning Approach for Inappropriate Information Classification in Social Networks // International Journal of Information Security, 2023. Vol. 22. № 6. PP. 1921–1936.

2. Levshun D., Tushkanova O., Chechulin A. Active Learning Approach for Inappropriate Information Classification in Social Networks // Proceedings of the 30th Euromicro International Con-

ference on Parallel, Distributed and Network-Based Processing (PDP 2022). Institute of Electrical and Electronics Engineers Inc., 2022. PP. 283–289.
3. Li M., Wong K. Resilience of Passive-Aggressive Classifiers to Data Poisoning in Active Learning // Information Security Issues. Computer Systems, 2021. № 3. PP. 22–30.
4. Smith J., Johnson K. Impact of Label Poisoning Attacks in Active Learning Systems // Information Technology and Security, 2020. Vol. 6. № 1. PP. 90–99.
5. Yong T., Zhou L., Wu P. Sequential data poisoning attacks in the context of active learning // Journal of Information Technology, 2022. Vol. 15. № 7. PP. 65–74.

Levshun D., Staroverov A. **AN APPROACH TO ASSESSING THE EFFECTIVENESS OF DATA POISONING ATTACKS IN MODELS WITH ACTIVE LEARNING.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

With the development and implementation of active learning in machine learning and artificial intelligence systems, the importance of model reliability and security comes to the forefront. Unlike traditional methods, active learning allows the model to dynamically select the most informative data for training, which is particularly effective when the training dataset is limited. However, there are also challenges: such systems are vulnerable to data poisoning attacks, which can reduce their accuracy and reliability. This paper presents an approach to evaluating the effectiveness of data poisoning attacks on models using active learning, focusing on studying the model's behavior depending on the degree of distortion and the use of label poisoning as a type of attack.

Key words: adversarial attacks, vulnerability analysis, machine learning, security, data poisoning, dataset

УДК 004.056.5
ГРНТИ 81.93.29

АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ ИССЛЕДОВАНИЙ В ОБЛАСТИ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ ИСХОДНОГО КОДА УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

Д. С. Левшун, Е. К. Щеголев
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С развитием Интернета вещей устройства стали уязвимыми для широкого спектра атак, что требует новых методов защиты. В работе представлен обзор существующих подходов и методов обнаружения уязвимостей в исходном коде устройств Интернета вещей. Рассматриваются ключевые вызовы, такие как сложность доступа к прошивке, ограниченность ее эмуляции и необходимость использования передовых методов анализа, включая фаззинг и автоматизированный анализ кода. Обсуждаются возможности и ограничения современных методов машинного обучения, а также направления для будущих исследований в области безопасности Интернета вещей.

Интернет вещей, анализ уязвимостей, машинное обучение, безопасность, исходный код, набор данных

С ростом числа устройств Интернета вещей (Internet of Things, IoT), которое, по прогнозам, достигнет 39,6 млрд подключенных устройств по всему миру к 2033 году (рис. 1) [1], сильно увеличивается потребность в надежной защите исходного кода [2, 3]. Выявление уязвимостей на ранних этапах разработки становится критически важным для предотвращения серьезных инцидентов, таких как утечки данных и DDoS-атаки [4].

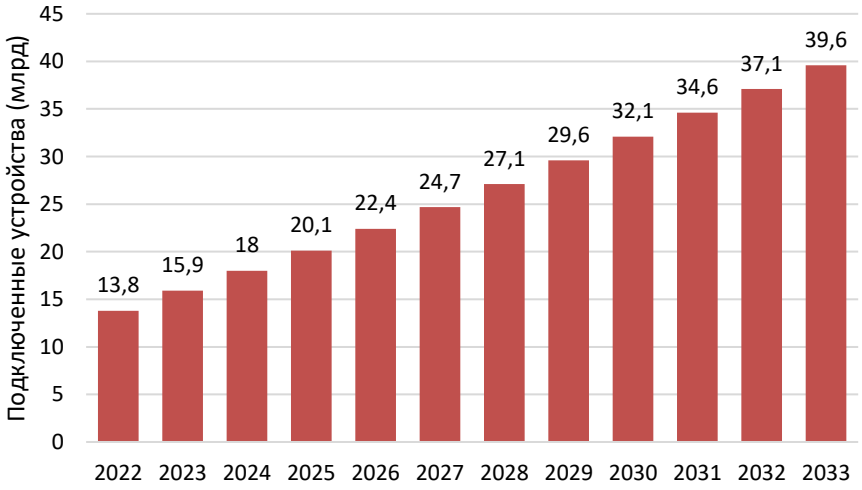


Рис. 1. Количество подключений Интернета вещей (IoT) по всему миру с 2022 по 2023 год, с прогнозом на 2024–2033 годы

Прошивка устройств Интернета вещей часто содержит уязвимости, которые могут быть использованы злоумышленниками для получения несанкционированного доступа и управления устройствами. В работе [5] подчеркивается особая важность анализа прошивок для своевременного выявления и устранения уязвимостей до их эксплуатации в реальных условиях. Среди методов анализа – эмуляция прошивок, автоматизированный анализ кода и сетевой фаззинг, которые помогают исследователям обнаруживать слабые места. Однако сложности с доступом к прошивкам и их эмуляцией затрудняют полноценный анализ безопасности. Методы машинного обучения стали популярным инструментом для улучшения выявления уязвимостей, однако остается много проблем, связанных с высокой сложностью кода и разнообразием уязвимостей [6]. Традиционные методы, такие как статический (SAST) и динамический (DAST) анализ, не всегда могут обеспечить полное покрытие, что снижает их эффективность для сложных IoT-систем. Методы AST (Abstract Syntax Tree) и машинное обучение, включая Random Forest (RF), Convolutional Neural Network (CNN) и Recurrent Neural Network (RNN), продемонстрировали успешные результаты в выявлении уязвимостей, особенно в IoT-среде, где безопасность кода имеет важное значение [7].

В ходе исследования существующих работ, был проведен анализ результатов, полученных для различных моделей машинного обучения на разных наборах данных, связанных с уязвимостями IoT. Результаты этого анализа представлены в таблице 1.

Существующие наборы данных, такие как DiverseVul и IoTvulCode, играют ключевую роль в обучении и оценке моделей для обнаружения уязвимостей в IoT-коде. DiverseVul охватывает множество уязвимостей и различных типов CWE, что делает его наиболее полным на данный момент [8]. IoTvulCode предлагает более специализированные выборки для IoT-устройств, что полезно для специфических сценариев анализа уязвимостей на низкоуровневых операционных системах IoT-устройств [9]. Использование таких наборов данных позволяет моделям более эффективно выявлять уязвимости, поскольку они обеспечивают разнообразие и дают возможность тренировать алгоритмы на примерах, близких к реальной эксплуатации устройств. Исследования показали, что модели на основе AST и текстового анализа уязвимостей с использованием больших языковых моделей (Large Language Model, LLM) могут превосходить графовые нейронные сети (Graph Neural Networks, GNN) и другие структурные модели, если обучены на обширных и качественных данных.

Модель iDetect продемонстрировала высокую точность в выявлении уязвимостей в IoT-системах, используя RF как классификатор. Использование

подходов, основанных на машинном обучении, позволяет достигать высоких показателей точности при анализе уязвимого кода IoT. Сравнительный анализ показал, что iDetect в сочетании с дополнительными инструментами, такими как Cppcheck, FlawFinder и RATS, успешно обнаруживает конкретные типы CWE в коде, что делает его полезным для анализа кода на C и C++. Однако необходимо дальнейшее развитие методов для улучшения обобщающей способности решений и снижения частоты ложноположительных срабатываний. Эти вопросы остаются вызовом для исследователей и разработчиков, работающих в области машинного обучения и анализа безопасности программного обеспечения IoT.

ТАБЛИЦА 1. Точность классификации различных моделей для наборов данных, связанных с IoT

Набор данных	Используемые модели	Результаты (точность классификации, %)	
		Бинарная классификация	Многоклассовая классификация
IDetect	RF	99	96,8
	CNN	95,8	94
	RNN	95,7	85,6
IoTvulCode	RNN	99,1	99
	LSTM	-	98,8
	CNN	96,2	98,9
Devign, ReVeal, BigVul, CrossVul, CVEFixes + DiverseVul	Семейство GNN (ReVeal)	85,88	-
	Семейство RoBERTa (RoBERTa, CodeBERT, GraphCodeBERT)	94,19-95,59	-
	Семейство GPT-2 (GPT-2 Base, CodeGPT, PolyCoder)	92,73-95,06	-
	Семейство T5 (T5 Base, CodeT5 Small, CodeT5 Base, NatGen)	94,91-96,16	-

Существующие модели могут испытывать трудности при обработке ранее не встречавшегося кода из-за высокой специфики данных, на которых они обучались, что ставит под сомнение их универсальность и применимость в новых проектах и IoT-средах. Большие языковые модели с дополнительными задачами предобучения, адаптированными к особенностям кода, представляют

собой перспективное направление для улучшения результатов анализа, так как они способны учитывать как синтаксическую, так и семантическую составляющие кода. Например, CodeT5 и другие LLM продемонстрировали высокие результаты при анализе крупных наборов данных, таких как DiverseVul и CVEFixes, тем самым показывая способность более точно выявлять уязвимости, особенно в коде для IoT [10].

Таким образом, современные методы анализа уязвимостей с использованием машинного обучения и специализированных наборов данных значительно улучшают результаты анализа исходного кода IoT, но требуют дальнейшего развития для более широкого спектра задач. Перспективными направлениями являются совершенствование методов генерализации, снижение ложных срабатываний и использование более глубоких языковых моделей для повышения точности и универсальности анализа.

Список используемых источников

1. Number of Internet of Things (IoT) connected devices worldwide // Statista. URL: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (дата обращения 02.11.2024).
2. Levshun D., Kotenko I., Chechulin A. The application of the methodology for secure cyber–physical systems design to improve the semi-natural model of the railway infrastructure // Microprocessors and Microsystems, 2020. P. 103482.
3. Levshun D., Kotenko I., Chechulin A. The Integrated Model of Secure Cyber-Physical Systems for Their Design and Verification // Studies in Computational Intelligence, 2020. Vol. 868. PP. 333–343.
4. Kim, H.-H., & Yoo, J. Analysis of security vulnerabilities for IoT devices // Journal of Information Processing Systems, 2022. Vol. 18. № 4. PP. 489–499.
5. Feng S., Zhu S., Han C.-L., Zhou W., Wen S., Xiang Y. Detecting Vulnerability on IoT Device Firmware: A Survey // IEEE/CAA Journal of Automatica Sinica, 2023. Vol. 10. № 1. PP. 25–41.
6. Krishnamoorthy G., Sistla S. M. Exploring machine learning intrusion detection: Addressing security and privacy challenges in IoT – A comprehensive review // Journal of Knowledge Learning and Science Technology, 2023. Vol. 2. № 2. PP. 115–130.
7. Al-Boghdady A., El-Ramly M., Wassif K. iDetect for vulnerability detection in Internet of Things operating systems using machine learning // Scientific Reports, 2022. Vol. 12. PP. 17086.
8. Chen Y., Ding Z., Alowain L., Chen X., Wagner D. DiverseVul: A New Vulnerable Source Code Dataset for Deep Learning Based Vulnerability Detection // RAID '23, 26th International Symposium on Research in Attacks, Intrusions and Defenses. Hong Kong, 2023. P. 15.
9. Bhandari G. P., Assres G., Gavric N., Shalaginov A., Grønli T.-M. IoTvulCode: AI-enabled vulnerability detection in software products designed for IoT applications // International Journal of Information Security, 2024. Vol. 23. PP. 2677–2690.
10. Fazeli A. Machine Learning-Based Automated Vulnerability Classification in C/C++ Software: магистерская дис. / Fazeli Artin. Линчепинг, 2024. 52 с.

Levshun D., Shchegolev E. **ANALYSIS OF THE CURRENT STATE OF RESEARCH IN VULNERABILITY DETECTION OF SOURCE CODE FOR INTERNET OF THINGS DEVICES.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

With the rapid development of the Internet of Things, devices have become vulnerable to a wide range of attacks, necessitating innovative protection methods. This work provides an overview of existing approaches and methods for detecting vulnerabilities in the firmware of IoT devices. Key challenges, such as limited firmware access, emulation complexity, and the necessity for advanced analysis methods like fuzzing and automated code analysis, are discussed. The paper also highlights the potential and limitations of modern machine learning techniques and future research directions in IoT security.

Key words: Internet of Things, vulnerability analysis, machine learning, security, source code, dataset.

УДК 004.056
ГРНТИ 50.41.23

ФОРМИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В МУЛЬТИСЕРВИСНЫХ СЕТЯХ СВЯЗИ

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

С развитием технологий связи и увеличением числа пользователей в различных областях жизнедеятельности возникает необходимость в обеспечении безопасности и конфиденциальности данных в мультисервисных сетях. Эти сети, поддерживающие множество различных типов сервисов, таких как голосовая связь, видеоконференции, передача данных, электронная почта, становятся объектами различных угроз. Целью данной статьи является описание ключевых аспектов формирования системы защиты информации в мультисервисных сетях связи, а также предложенная модель реализации такой системы, обеспечивающая надежную защиту как на уровне физической инфраструктуры, так и на уровне приложений.

мультисервисные сети, защита информации, SDN, NFV, шифрование данных, VoIP, видеоконференции, передача данных

Мультисервисные сети связи (MSN) на данный момент предлагают широкий спектр функциональных возможностей, включая голосовой и визуальный обмен, передачу данных и утилиты, специфичные для предприятия [1]. Это повышает вероятность того, что сеть может столкнуться с угрозами безопасности и онлайн-опасностями. В таких системах сложно гарантировать защиту информации, поскольку для различных служб могут потребоваться отдельные протоколы безопасности, а архитектура сети может быть смешанной и изменчивой. Пример реализации МСС представлен на рисунке 1.

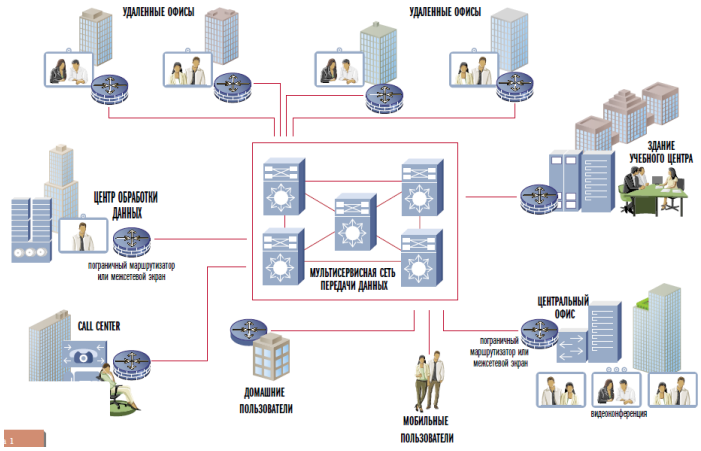


Рис. 1. Пример реализации мультисервисной сети

Обеспечение безопасности в мультисервисных сетях связи должно включать не только защиту от внешних угроз (например, атак хакеров), но и защиту от внутренних угроз, таких как утечка данных, а также соответствовать нормативным требованиям в области защиты персональных данных и конфиденциальной информации [2].

Структурная схема мультисервисной сети включает три уровня: ядро сети, уровень распределения и уровень доступа. Ядро отвечает за скорость и надежность передачи основного трафика. Уровень распределения выполняет маршрутизацию, фильтрацию и установление правил доступа к ядру. Уровень доступа соединяет конечные устройства с основной сетью.

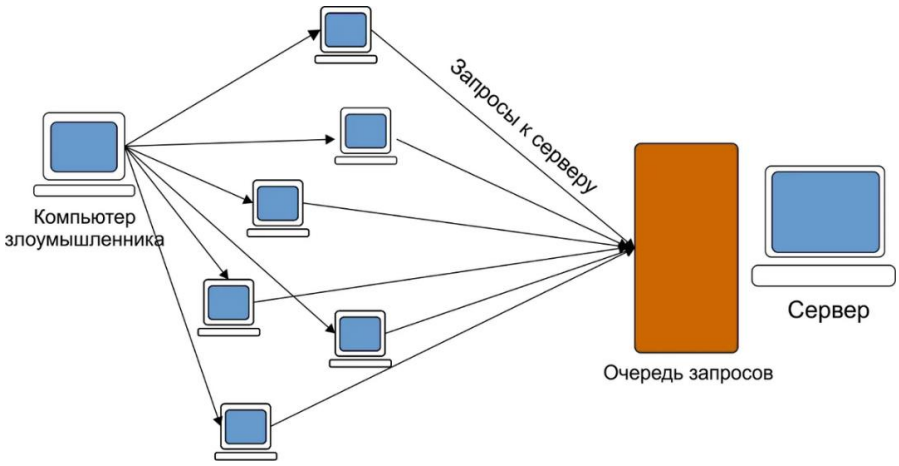


Рис. 2. Схема DoS-атаки

МСС состоит из ключевых компонентов, включая магистраль на основе технологий IP/MPLS (высокоскоростная сеть передачи данных на основе коммутации пакетов), которая поддерживает виртуальные частные сети (VPN) и обеспечивает отказоустойчивость. Сервисные узлы предоставляют различные услуги пользователям, а клиентские устройства, такие как Ethernet-коммутаторы и IP-телефоны, обеспечивают взаимодействие с сетью.

Однако МСС подвержены угрозам безопасности. Одной из серьезных является неавторизованный доступ, который может привести к перехвату данных и изменению конфигурации. Также существуют угрозы конфиденциальности и атаки типа «отказ в обслуживании» (DoS), которые могут блокировать работу критически важных сервисов. На рисунке 2 представлен принцип работы DoS-атаки [3].

Манипуляции с трафиком, такие как изменение или подделка данных, могут иметь серьезные последствия, особенно в системах управления и финансовых операциях. Уязвимости в протоколах IP, MPLS и SIP создают возможности для атак. Для надежной защиты информации в мультисервисных сетях необходим комплексный подход, включающий несколько ключевых принципов [4].

Во-первых, многоуровневая защита, охватывающая все уровни сетевой архитектуры, создает многослойную защиту, усложняющую задачу злоумышленникам. Во-вторых, шифрование данных критически важно для конфиденциальности и предотвращает несанкционированный доступ.

В-третьих, аутентификация и авторизация с использованием сильных механизмов контроля доступа защищают критически важные ресурсы [3].

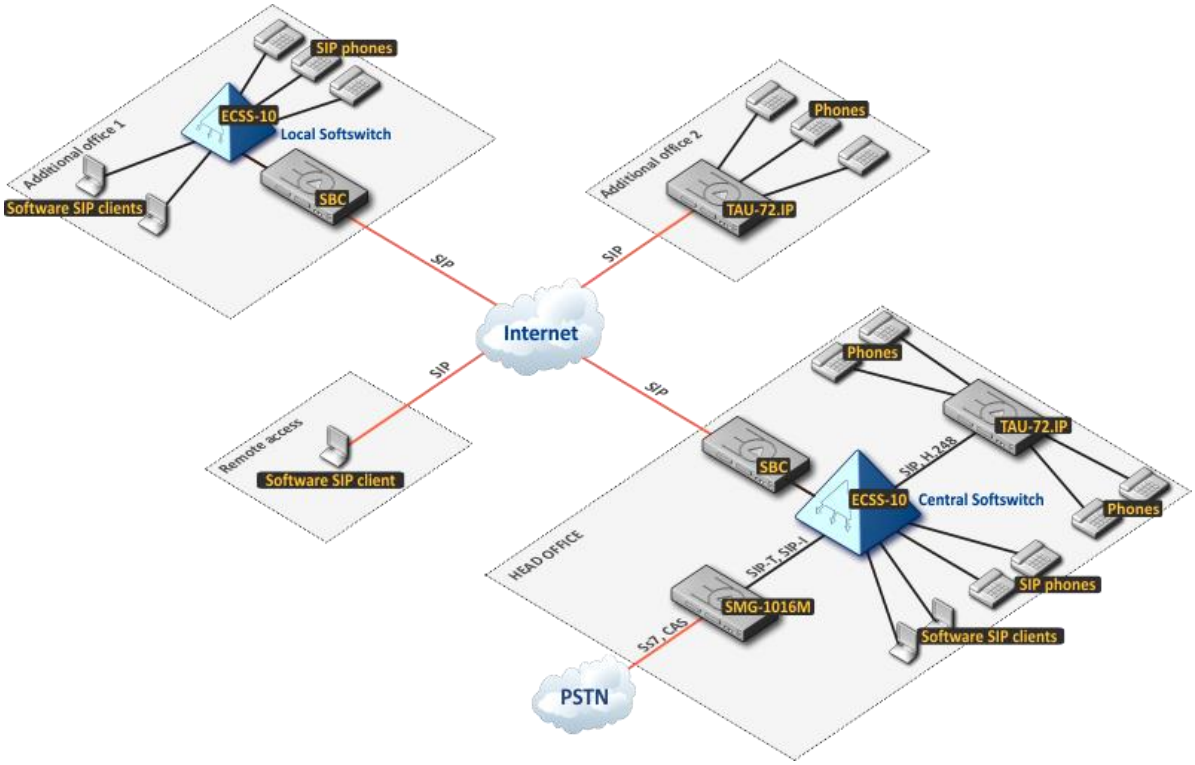


Рис. 3. Схема структуры МСС компании Eltex

Крупные организации, такие как банки и телекоммуникационные компании, активно используют мультисервисные сети для оптимизации бизнес-процессов. Примером является компания Eltex, которая предлагает интегрированные решения для передачи данных, голосовой связи и видеосервиса. На рисунке 3 представлена реализация построения структуры сеть и основных компонентов. Использование оборудования Eltex позволяет значительно улучшить качество обслуживания клиентов и снизить затраты на связь. Кроме того, Eltex разрабатывает и внедряет системы безопасности, такие как решения на основе технологии IPSec и VPN, для защиты данных и обеспечения надежной работы сервисов [5]. Eltex демонстрирует, как мультисервисные сети способствуют повышению конкурентоспособности компаний на рынке.

Таким образом, система защиты информации в мультисервисных сетях должна быть гибкой, масштабируемой и адаптируемой к новым угрозам. Внедрение технологий SDN (программно-определяемые сети) и NFV (виртуализация сетевых функций), которые активно поддерживаются Eltex, открывает возможности для создания комплексных решений, обеспечивающих за-

щиту данных и надежную работу сервисов. Безопасность сети требует не только применения современных технических средств, но и организации процессов управления инцидентами и обновления политик безопасности. Формирование эффективной системы защиты информации является многогранной задачей, требующей междисциплинарного подхода и обеспечивающей высокий уровень защищенности данных и бесперебойную работу сервисов связи, что является приоритетом для компании Eltex.

Список используемых источников

1. Сетевые технологии: Основы и применение / А. А. Петров. СПб.: Издательство "Питер", 2019. 256 с.
2. Программно-определяемые сети: Принципы и технологии / Н. Н. Смирнов. Казань: Издательство "Казанский университет", 2022. 300 с.
3. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // В сборнике: Региональная информатика "РИ-2018". Материалы конференции, 2018. С. 570–571.
4. Защита информации в мультисервисных сетях / М. М. Кузнецов. Новосибирск: Издательство "Сибирское образование", 2023. 150 с.
5. Проектирование локальных мультисервисных сетей: Учебное пособие. / О. Г. Шерстнева. Екатеринбург: УрТИСИ ФГОБУ ВПО «СибГУТИ», 2012. 112 с.

***Markov A.* FORMATION OF INFORMATION SECURITY SYSTEM IN MULTISERVICE COMMUNICATION NETWORKS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

With the development of communication technologies and the increasing number of users in various areas of activity, there arises a need to ensure the security and confidentiality of data in multiservice networks. These networks, supporting a variety of service types such as voice communication, video conferencing, data transmission, and email, become targets for various threats. The purpose of this article is to describe the key aspects of forming an information security system in multiservice communication networks, as well as to propose a model for implementing such a system that provides reliable protection at both the physical infrastructure level and the application level.

Key words: multiservice networks, information security, SDN, NFV, data encryption, VoIP, video conferencing, data transmission.

УДК 004.056.52
ГРНТИ 20.53.17

РАЗРАБОТКА ЗАЩИЩЕННОГО ФАЙЛОВОГО ХРАНИЛИЩА ДЛЯ ИНСТАНСОВ VMWARE VSPHERE

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

В данном докладе рассматривается разработка защищенного файлового хранилища для инстансов платформы VMware vSphere. Созданное решение позволяет безопасно передавать файлы на виртуальные машины и с них в условиях работы под управлением гипервизора VMware ESXi. Проведено тестирование работоспособности программы, результаты которого показали соответствие решения поставленным целям по обеспечению безопасности и конфиденциальности данных.

информационная безопасность, VMware vSphere, виртуализация, файловое хранилище

Виртуализация является важным аспектом современных корпоративных и облачных инфраструктур, однако защита данных в этих средах требует использования дополнительных методов. Для обеспечения безопасности данных, хранимых на виртуальных машинах *VMware vSphere*, был разработано защищенное файловое хранилище, предотвращающее кибератаки и утечки данных.

Защищенное файловое хранилище предназначено для работы с инстансами *VMware vSphere* и обеспечивает передачу и загрузку файлов на виртуальные машины. Главная цель решения – защита от распространенных атак, таких как атака «человек посередине» (рисунок 1), которая представляет собой тип кибератаки, когда злоумышленник внедряется в канал связи и получает возможность перехватывать или изменять данные [1].

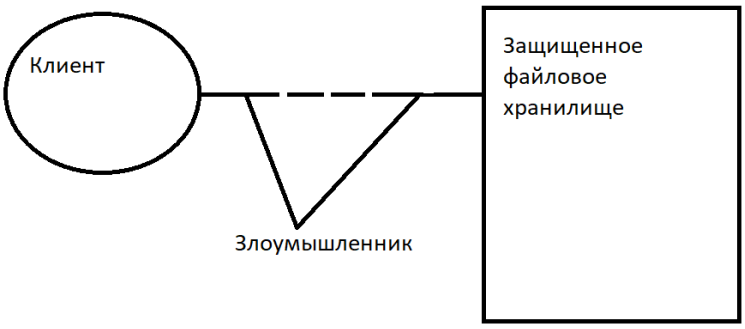


Рис. 1. Схема атаки «человек посередине»

Подключение к виртуальным машинам осуществляется через сервер *VMware vCenter*, с поддержкой операционных систем, таких как *Microsoft Windows 10*. Программа поддерживает *VMware vSphere* версии 7.0 и *VMware ESXi 7.0* и требует ввода *IP*-адреса сервера, логина и пароля администратора, которые шифруются симметричным ключом и хранятся в отдельном защищенном файле [2]. В основе шифрования данных используется библиотека *Cryptography* с алгоритмом *Fernet*, который реализует симметричное шифрование. Симметричное шифрование предполагает использование единого ключа для шифрования и дешифрования данных, что обеспечивает высокую скорость обработки и надежность защиты [3].

Для защиты аутентификационных данных, таких как логин и пароль, реализованы функции:

generate_key(): создает или считывает ключ для шифрования данных. Ключ сохраняется в защищенном файле *secret.key*, который должен быть доступен только программе и защищен от несанкционированного доступа.

encrypt_data(data, key): шифрует данные с использованием симметричного ключа.

decrypt_data(encrypted_data, key): дешифрует данные для использования в программе.

Такой подход позволяет безопасно передавать данные на виртуальные машины, предотвращая утечку в случае перехвата информации третьими лицами.

Программа включает несколько функций для валидации данных, предотвращая ввод неправильных данных и возможные вредоносные атаки:

– *validate_server_address(address)* – проверка формата адреса сервера;

– *validate_path(path)* – проверка пути на запрещенные последовательности;

– *validate_password(password)* – проверка сложности пароля;

– *validate_username(username)* – проверка корректности имени пользователя.

Функции программы включают:

– *on_vm_selected(event)* – обработка события выбора виртуальной машины;

– *get_vm(vm_name)* – получение объекта виртуальной машины;

– *connect_to_vcenter()* – проверка введенных данных, шифрование пароля и подключение;

– *load_vm_list()* – загрузка списка виртуальных машин и отображение их для выбора.

При успешном подключении пользователь может передавать и скачивать файлы с виртуальной машины. В случае ошибки доступа или отсутствия нужных прав программа выводит сообщение об ошибке.

Программа включает *SSL*-сертификаты для защиты соединения между клиентом и сервером, что гарантирует безопасность при передаче данных. Пользователь может указать путь к сертификату, если он не установлен в системе. Программа ведет журнал всех действий, указывая временные метки, что упрощает диагностику и позволяет отслеживать действия.

Программа фиксирует каждое действие пользователя в журнале, указывая временную метку для каждой операции. Функция *log_event(message)* записывает в журнал события, такие как подключение к виртуальной машине, передача и скачивание файлов. Журналирование позволяет отслеживать историю действий, что значительно облегчает диагностику и позволяет быстро определить источник ошибок или некорректных операций. Это особенно полезно при проведении аудитов безопасности и расследовании инцидентов [4]. Графический интерфейс программы представлен ниже (рисунок 2).

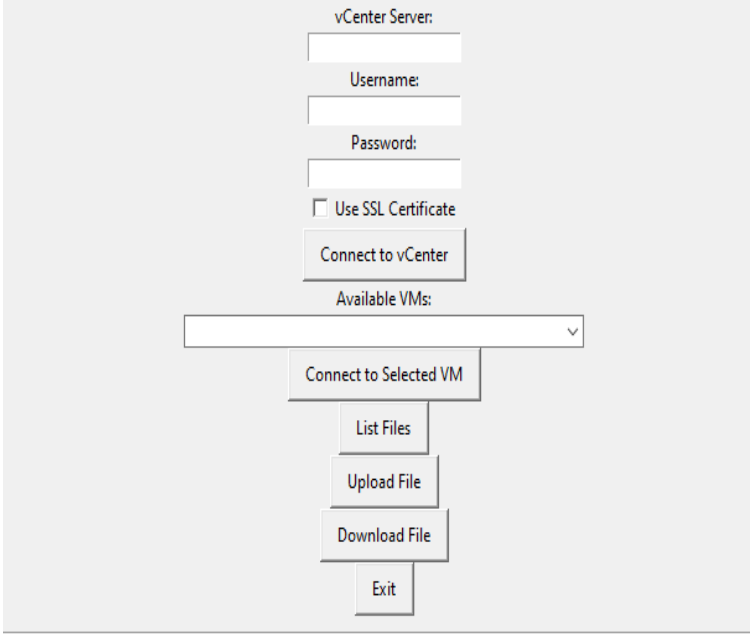


Рис. 2. Графический интерфейс программы

Для тестирования защищенного файлового хранилища был подготовлен экспериментальный стенд, состоящий из гипервизора *VMware ESXi*, сервера *vCenter* и инстанса *Windows 10*.

Целью теста была проверка передачи и скачивания файла. При запуске программы и вводе IP-адреса сервера и аутентификационных данных пользователю отображается список виртуальных машин. После подключения можно

просмотреть файлы в хранилище (рисунок 3), а затем загрузить и скачать файл с проверкой его целостности по хеш-сумме.

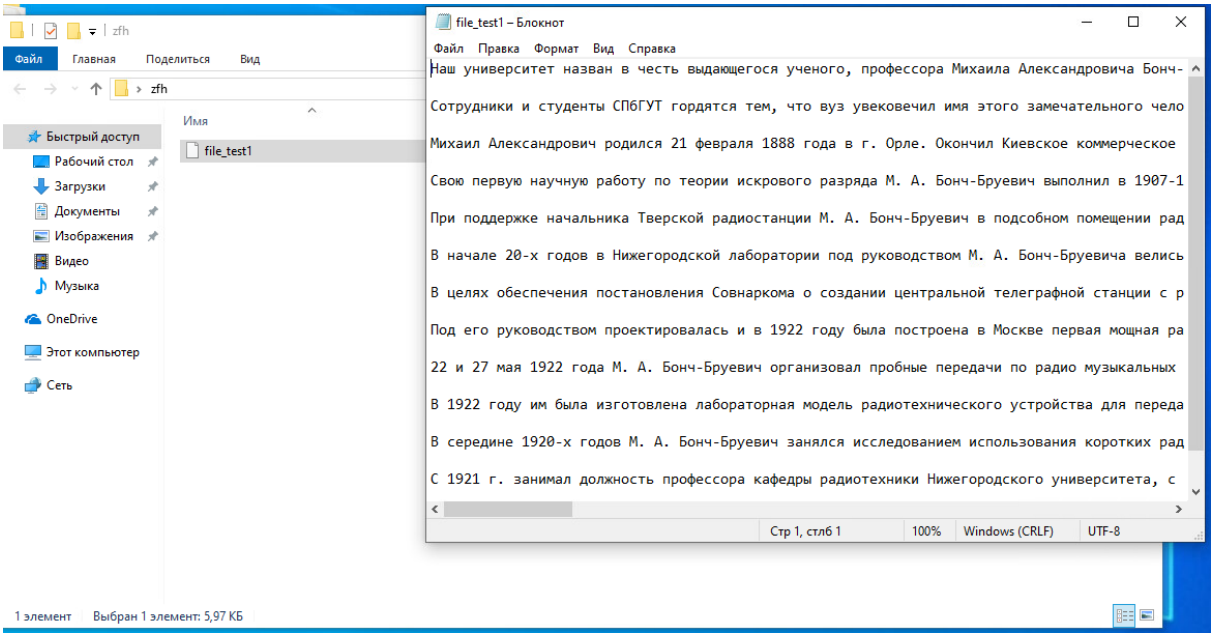


Рис. 3. Файл в хранилище

После завершения передачи и скачивания файл был открыт на локальном устройстве, и результат показал полное совпадение содержимого с исходным файлом (рисунок 4), что подтвердило корректность и безопасность процесса передачи данных. Это также продемонстрировало надежность механизма шифрования и целостность данных при передаче.

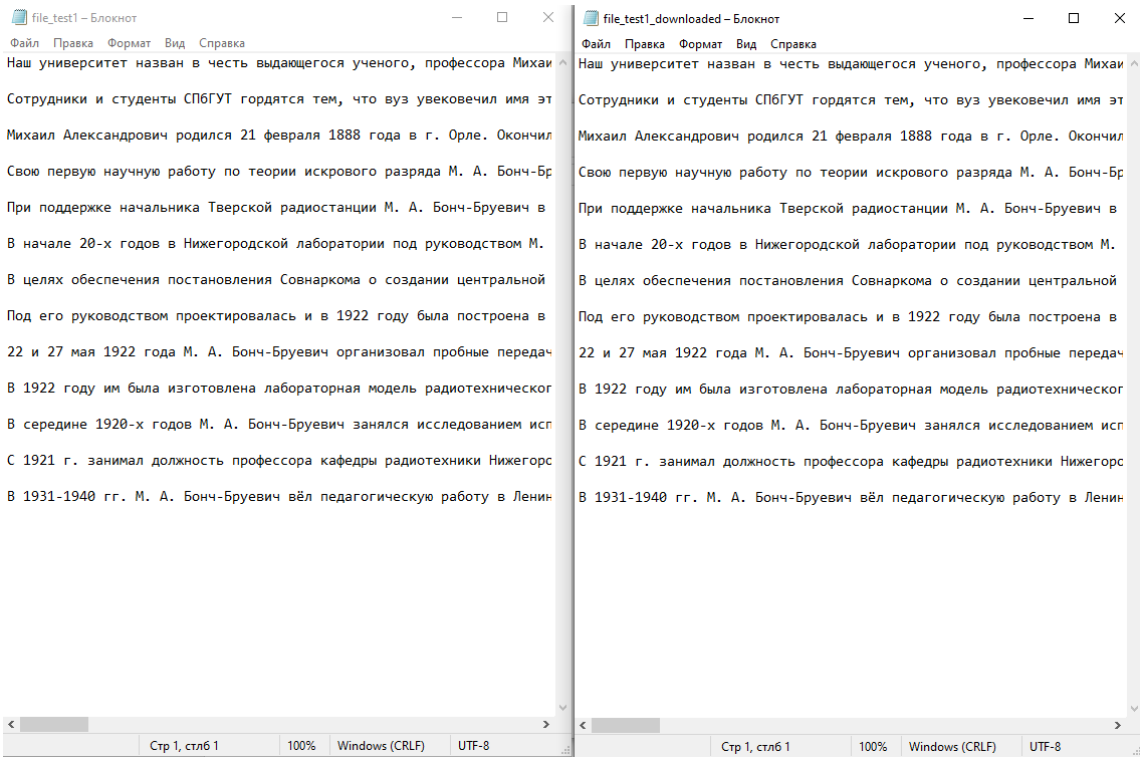


Рис. 4. Сверка файлов

Проведенное тестирование подтвердило эффективность разработанного защищенного файлового хранилища для *VMware vSphere*. Программа обеспечивает надежную защиту данных, их конфиденциальность и доступность, а также устойчивость к распространенным кибератакам. Решение ориентировано на использование в корпоративных средах, где требуется защита критически важных данных в виртуальных средах.

Список используемых источников

1. Сергеев Ю. К. Анализ угроз безопасности виртуальных информационных систем // Вестник Российского государственного гуманитарного университета, 2011. № 13. С. 160–170.
2. Антоненко В. А., Смелянский Р. Л., Ермилов А. А., Романов А. Р., Пинаева Н. М., Плакунов А. В. Платформа управления виртуальными сетевыми функциями С2 // Информационные технологии, 2018. Т. 24. № 3. С. 165–173.
3. ГОСТ Р 56938-2016. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения; введ. 2017 – 06 – 01. – Приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 г. № 457-ст.
4. Матвеев В. А., Цирлов В. Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2014 г. // Вопросы кибербезопасности, 2013. № 1(1). С. 61–64

***Mikhailov A.* SECURE FILE STORAGE FOR VMWARE VSPHERE INSTANCE.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This report discusses the development of secure file storage for VMware vSphere platform instances. The created solution allows to securely transfer files to and from virtual machines under the VMware ESXi hypervisor. Testing of the program performance was carried out, the results of which showed the compliance of the solution with the set goals to ensure data security and confidentiality.

Key words: Information security, VMware vSphere, virtualization, file storage.

УДК 004.056.55
ГРНТИ 81.93.29

О РЕАЛИЗАЦИИ СОВЕРШЕННОГО ЛИНЕЙНОГО ЭКВИВАЛЕНТНОГО ПРОФИЛЯ ДВОИЧНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

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

В статье рассматривается один из возможных способов повышения стойкости последовательности посредством использования нелинейного узла усложнения, принцип работы которого основан на понятии совершенного линейного эквивалентного профиля последовательности, а также производится оценка статистических свойств сформированной последовательности.

псевдослучайные последовательности, генераторы псевдослучайных последовательностей, линейная эквивалентная сложность, профиль линейной сложности, нелинейные узлы усложнения

Под линейной эквивалентной сложностью (ЛЭС) L_N последовательности $a_0, a_1, \ldots, a_{N-1}$ понимается минимальная длина линейного рекуррентного регистра (ЛРР), способного сгенерировать эту последовательность [1]. Одним из показателей качества шифрующей гаммы является профиль ее линейной сложности, который определяется, как зависимость ЛЭС последовательности от ее длины.

Линейный эквивалентный профиль (ЛЭП) называется совершенным, если он близок к математическому ожиданию ЛЭП чисто случайной последовательности. Совершенный профиль линейной сложности колеблется около линии $N/2$.

Полная характеристика всех двоичных последовательностей с совершенным линейным эквивалентным профилем была сформулирована в работе [2]. Было показано, что двоичная последовательность a имеет совершенный профиль линейной сложности тогда и только тогда, когда:

$$\begin{cases} a_0 = 1; \\ a_{2i} = a_{2i-1} \oplus a_{i-1}, \ i \geq 1. \end{cases} \quad (1)$$

Значения нечетных позиций $2i$-1 могут быть сформированы произвольно.

Рассмотрим генератор, состоящий из линейного рекуррентного регистра и нелинейного узла усложнения (НУУ), формирующего шифрующую гамму по правилу (1), используя при этом в качестве нечетных позиций значения с выхода ЛРР (рис. 1).

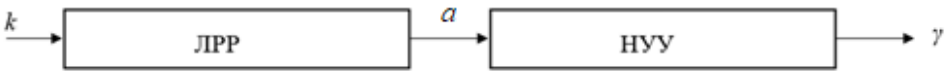


Рис. 1. Генератор гаммы с совершенным профилем линейной сложности

Если обозначить a_0, a_1, … выходную последовательность, формируемую ЛРР, а γ_0, γ_1, … – последовательность символов гаммы, то закон, по которому происходит формирование гаммы в данном генераторе, можно описать следующим образом:

$$\begin{cases} \gamma_0 = 1; \\ \gamma_{2i-1} = a_{i-1}; \\ \gamma_{2i} = \gamma_{2i-1} \oplus \gamma_{i-1}, \ i \geq 1. \end{cases} \quad (2)$$

График линейной сложности L для последовательности длиной $N = 100$, сформированной по правилу (2) представлен на рисунке 2.

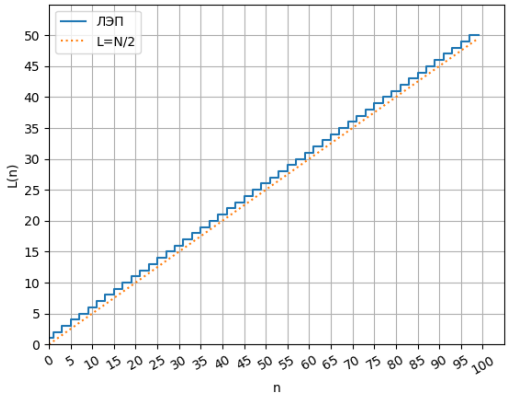


Рис. 2. Совершенный профиль линейной сложности

При формировании гаммы предложенным генератором возникает несколько проблем:

– во-первых, требуемый объем памяти для хранения промежуточных результатов, используемых для вычисления очередного четного символа гаммы, накладывает ограничения на длину генерируемой гаммы;

– во-вторых, нечетные элементы создаются ЛРР и, следовательно, НУУ никак не влияет на их криптографическую стойкость.

Одним из подходов к сокращению требуемой памяти может быть использование нескольких запусков генератора и применение в качестве гаммы объединения полученных последовательностей. Начальные заполнения ЛРР, формирующего нечетные элементы гаммы, при различных запусках должны различаться, иначе получаемые с выхода генератора последовательности будут повторяться. Поэтому для формирования начального заполнения ЛРР после перезапуска генератора использовался еще один ЛРР.

Для исключения недостатка, связанного с отсутствием усложнения нечетных элементов гаммы, возможны следующие варианты:

– выбор из генерируемой последовательности только четных позиций;

– использование генератора с перемежением;

– использование генератора с наложением.

В первом случае из исходных отрезков последовательности выбираются четные позиции, после чего итоговая гамма формируется только из выбранных значений. Таким образом, шифрующая гамма будет состоять только из элементов, которые вычислялись по правилу (1).

Вырабатываемая таким генератором последовательность будет иметь ЛЭП, допустимо отклоняющийся от совершенного, а ее линейная сложность будет расти до определенного предела (рис. 3).

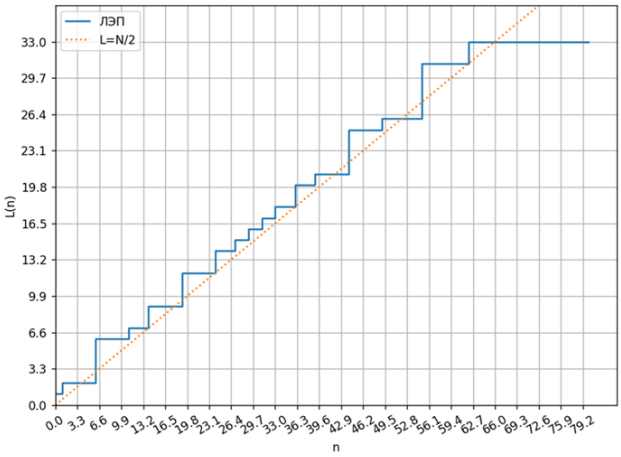


Рис. 3. График линейной сложности L для последовательности длиной $n = 81$, сформированной $N = 9$ запусками алгоритма при длине накопителя $M = 17$

Еще одним подходом может быть соединение двух предложенных ранее генераторов с выборкой позиций, формируемых по правилу (1), и использование в качестве четных позиций итоговой гаммы выходных элементов первого генератора, а в качестве нечетных – выходных элементов второго генератора. Схема генератора с перемежением последовательностей представлена на рисунке 4.

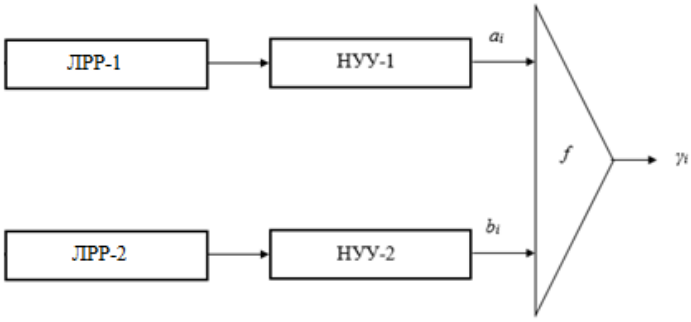


Рис. 4. Генератор гаммы с перемежением

Помимо схемы с перемежением значений двух исходных последовательностей возможна модификация генератора, в котором значения этих последовательностей накладываются друг на друга таким образом, что нечетные позиции последовательности a_i складываются с четными позициями последовательности b_i, а четные – с нечетными.

Для моделирования работы исследуемого генератора были выбраны линейные рекуррентные регистры, задаваемые следующими примитивными полиномами:

$$\text{ЛРР-1: } h_3(x) = x^4 + x^3 + 1,$$

$$\text{ЛРР-2: } h_4(x) = x^{10} + x^3 + 1.$$

Графики ЛЭП для предложенных генераторов приведены на рисунке 5.

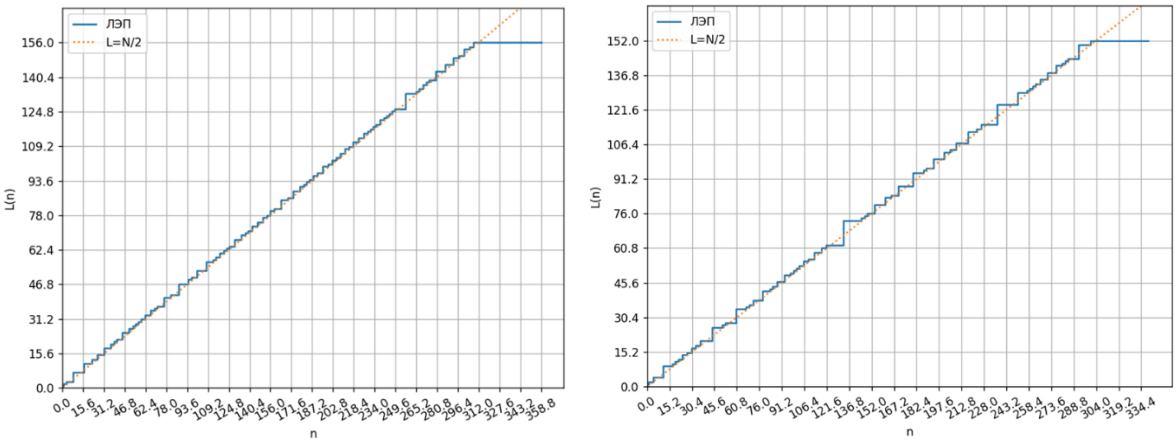


Рисунок 5 – Линейная сложность последовательности, сформированной 20 запусками алгоритма при длине накопителя $M = 17$: а) для генератора с перемежением; б) для генератора с наложением

Также было проведено исследование некоторых статистических свойств генерируемых последовательностей, а именно: свойство баланса, свойство серий, периодичность и автокорреляционная функция (АКФ). Результаты представлены в таблице 1, а также на рисунке 6.

ТАБЛИЦА 1. Исследование статистических свойств генерируемых последовательностей

	Генератор с одним формирующим ЛРР	Генератор с перемежением	Генератор с наложением
Амплитуда нарушения баланса	36	61	33
Свойство серий	не выполняется	не выполняется	не выполняется
Период	1596	не определился	не определился

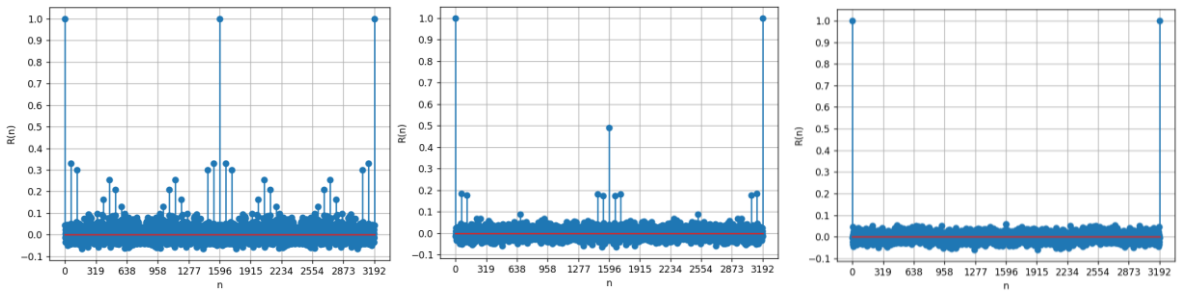


Рисунок 6 – График АКФ последовательности, сформированной:
а) генератором с одним формирующим ЛРР при длине накопителя $M = 455$ символов из четных элементов; б) генератором с перемежением при длине накопителя $M = 227$;
в) генератором с наложением при длине накопителя $M = 228$.

По результатам оценки статистических свойств и линейной эквивалентной сложности выходных последовательностей, формируемых тремя исследуемыми генераторами, можно сделать следующие выводы:

1. Генераторы, построенные на основе двух параллельных схем с нелинейными узлами усложнения, имеют в 4,5 раза большую линейную сложность по сравнению с генератором, состоящим только из одного генерирующего ЛРР;

2. Все три генератора формируют последовательности с линейным профилем, допустимо отклоняющимся от совершенного;

3. Наилучшими статистическими свойствами обладает генератор с наложением последовательностей. Его АКФ на рассмотренной длине выходной последовательности не имеет выбросов, что совпадает с АКФ чисто случайной последовательности.

Таким образом, исследуемый НУУ позволяет повысить ЛЭС последовательности, однако в работе проводилась оценка лишь некоторых ее статистических свойств. Применение данного НУУ в реальных криптосистемах требует проведения дополнительных исследований и не исключает использования традиционных узлов усложнения.

Список используемых источников

1. Поточные шифры. Результаты зарубежной открытой криптологии. М.: 1997 г. – 389 с. Не опубликовано.
2. Wang M. Z., Massey J. L. “The characteristics of all binary sequences with perfect linear complexity profiles,” paper presented at Eurocryp’86, Linkoping, Sweden, May 20-22, 1986.

Peshkina V. **REALIZATION OF A PERFECT LINEAR COMPLEXITY PROFILE OF A BINARY SEQUENCE.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article discusses one of the possible ways to increase the stability of a sequence by using a nonlinear complication node, the operating principle of which is based on the concept of a perfect linear equivalent profile of a sequence, and also evaluates the statistical properties of the generated sequence.

Key words: pseudorandom sequences, pseudorandom sequence generators, linear equivalent complexity, linear complexity profile, nonlinear complication nodes.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ ОСНОВНЫХ УГРОЗ УЯЗВИМОСТЕЙ WEBRTC: ОТ ПЕРЕХВАТА ДАННЫХ ДО DDOS-АТАК

А. В. Поляничева, М. С. Шулындина
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире популярность набирает WebRTC, но мало кто знает, что данная технология подвержена различным угрозам и атакам. В данной статье рассмотрим основные угрозы и уязвимости, а также предложим меры обеспечения безопасности при использовании WebRTC в реальных условиях.

WeRTC, угрозы, уязвимости, перехват данных, STUN/TURN, ICE, конфиденциальность, DDoS

WebRTC (Web Real-Time Communication) – это технология, позволяющая Web-приложениям и мобильным приложениям обмениваться аудио, видео и данными в режиме реального времени без использования промежуточных серверов. Данная технология широко используется в видеоконференциях, VoIP-сервисах и онлайн-играх, обеспечивая пользователям удобство и минимальные задержки [1].

Однако, несмотря на плюсы, которыми обладает WebRTC, эта технология также имеет определенные риски безопасности при использовании. Рассмотрим основные угрозы и уязвимости WebRTC, от перехвата данных до атак типа DDoS (распределенная атака на отказ в обслуживании). Для наглядности результаты всех уязвимостей и угроз приведены в таблице 1 [2].

ТАБЛИЦА 1. Основные угрозы и уязвимости WebRTC

Название угрозы/ уязвимости	Описание угрозы/уязвимости	Примеры атак
Перехват данных MITM (Man-in-the-Middle)	Атака "человек посередине", при которой злоумышленник, находясь между клиентом и сервером, перехватывает и изменяет передаваемые данные	– Перехват медиа-трафика, что может привести к утечке личных данных пользователей. – Замена медиа-потока, приводящая к искажению контента

Название угрозы/ уязвимости	Описание угрозы/уязвимости	Примеры атак
Уязвимости в протоколах STUN/TURN (Session Traversal Utilities for NAT/Traversal Using Relays around NAT)	Уязвимости в протоколах, используемых в установлении соединений в WebRTC, позволяют устройствам находить свой публичный IP-адрес и обходить NAT	– Использование открытых STUN серверов для атак на сети, что может привести к утечке IP-адреса и отслеживанию активности пользователя в сети. – Атаки на TURN серверы могут привести к утечке конфиденциальной информации
Риски при открытии порта через ICE	ICE используется для установления соединения между клиентами, что требует динамической передачи открытых портов между узлами через NAT	– Открытие портов на стороне клиента, что позвонит злоумышленнику получить доступ к внутренним сервисам пользователя. – Использование устаревших методов ICE позволяет злоумышленнику обходить защитные механизмы и тем самым получить доступ к данным пользователя
Утечка IP-адреса	Угроза утечки реального IP-адреса пользователя, даже при использовании VPN.	– Прямой обмен данными между клиентами, обходящий VPN-туннель [3]. – Злоумышленник использует STUN сервер для получения реального IP-адреса пользователя, даже при использовании VPN
DDoS-атаки через TURN-серверы	Злоумышленники могут перегружать TURN-серверы, отправляя большое количество запросов.	– Отказ в обслуживании (DoS) на TURN-серверы. – Злоумышленник находит и использует открытые TURN серверы для отправки запросов на целевые IP-адреса, тем самым создавая большую нагрузку на сеть

Рассмотрим основные меры обеспечения безопасности при использовании WebRTC.

1. Перехват данных (Man-in-the-Middle - MITM):

– использование современных алгоритмов шифрования и защиты передачи данных;

– настройка серверов для обязательной валидации сертификатов;

– использование HTTPS и других стандартов защиты при передаче сигнализации.

2. Уязвимости в реализации протоколов STUN/TURN:

– защита TURN-серверов с помощью механизмов аутентификации и авторизации [4];

– ограничить доступ к STUN-серверам с использованием фильтрации IP-адресов и аутентификации;

– внедрять защиту от DDoS-атак на серверном уровне;

– использование надежных STUN/TURN серверов.

– настройка брандмауэра для блокировки несанкционированных запросов к STUN и TURN серверам;

– регулярно проводить обновления и проводить аудит обновления и аудит безопасности.

3. Риски при открытии порта через ICE:

– ограничение открытых портов на устройствах и использование «ограниченного» ICE-соединения;

– применение строгих политик безопасности в сетевых конфигурациях и реализации ICE.

4. Атаки на конфиденциальность через утечку IP-адреса:

– блокировка WebRTC через настройки браузера или использование расширений, блокирующих WebRTC;

– использование сервисов, которые гарантируют скрытие реального IP-адреса, например, специальные VPN с защитой от утечек WebRTC.

– отключение WebRTC (Пользователи могут отключить WebRTC в настройках браузера или использовать расширения, которые блокируют его работу.

5. DDoS-атаки через TURN-серверы:

– ограничение количества подключений к TURN-серверам (или создание ACL-списков);

– настройка строгой аутентификации для доступа к TURN-серверам, чтобы только авторизованные пользователи могли их использовать;

– внедрение фильтрации и ограничения по IP-адресам.

WebRTC представляет собой мощную и удобную технологию для обмена данными в реальном времени, но при этом она сопряжена с рядом угроз и уязвимостей, которые могут быть использованы злоумышленниками для перехвата данных, осуществления DDoS-атак и других видов вмешательства в процесс коммуникации [5]. Для обеспечения безопасности WebRTC важно соблюдать лучшие практики защиты данных, правильно настраивать серверы и протоколы, а также своевременно обновлять клиентские приложения и браузеры.

Список используемых источников

1. Johnston A. B. WebRTC: APIs and RTCWeb Protocols of the HTML5 Real-Time Web / Johnston, A. B.: O'Reilly Media, Inc., 2016. 161 p.
2. Типовые уязвимости веб-приложений. Банк данных угроз. URL: https://bdu.fstec.ru/webvulns (дата обращения 10.11.2024).
3. Singh V. WebRTC Security and Privacy // IEEE Communications Surveys & Tutorials, 2020. № 22 (3). PP. 1234–1256.
4. Singh V. WebRTC Security: A Comprehensive Overview // Journal of Cyber Security Technology? 2021. № 5 (2). PP. 89–105.
5. Kumar A., Gupta R. Analyzing Vulnerabilities in WebRTC // International Journal of Information Security, 2022. № 21 (4). С. 345–367.

Polyanicheva A., Shulyndina M. **ANALYSIS OF THE MAIN THREATS OF WEBRTC VULNERABILITIES: FROM DATA INTERCEPTION TO DDOS ATTACKS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the modern world, WebRTC is gaining popularity, but few people know that this technology is subject to various threats and attacks. In this article, we will look at the main threats and vulnerabilities, as well as propose security measures when using WebRTC in real conditions.

Key words: WeRTC, threats, vulnerabilities, data interception, STUN/TURN, ICE, privacy, DDoS.

УДК 004.056
ГРНТИ 81.93.29

МЕТОДЫ И АЛГОРИТМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ ДЛЯ ЗАЩИТЫ ОТ СПАМА

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

Одной из наиболее актуальных угроз в защите данных является спам, а число атак данного типа растет ежегодно рекордными темпами. В связи с этим повышается значимость инструментов, способных обеспечить безопасность данных для защиты от спама. В рамках настоящей статьи проводится рассмотрение наиболее актуальных и эффективных методов и алгоритмов, нацеленных противодействию спаму.

спам, рассылка, информационная безопасность, защита данных, мошенник, алгоритм защиты

Вопросы информационной безопасности и защиты данных в 2024 году особенно актуальны из-за продолжающейся цифровизации, роста объемов данных и увеличения числа киберугроз [1]. Организации и частные лица сталкиваются с возрастающим риском утечек данных, атак на критическую инфраструктуру и других форм киберпреступлений, которые могут привести к значительным финансовым и репутационным потерям. Среди таких угроз одной из наиболее актуальных проблем остается спам, который стал ключевой угрозой безопасности и источником мошенничества в цифровой среде [2]. Актуальность данной проблемы подтверждается статистическими данными, которые свидетельствуют о 12 %-ом росте числа кибератак в период с 2022 по 2023 годы (рис. 1). Так, по последнему аналитическому отчету компании «РТК-Солар» число кибератак во втором квартале 2023 года составило свыше 325 000 инцидентов.

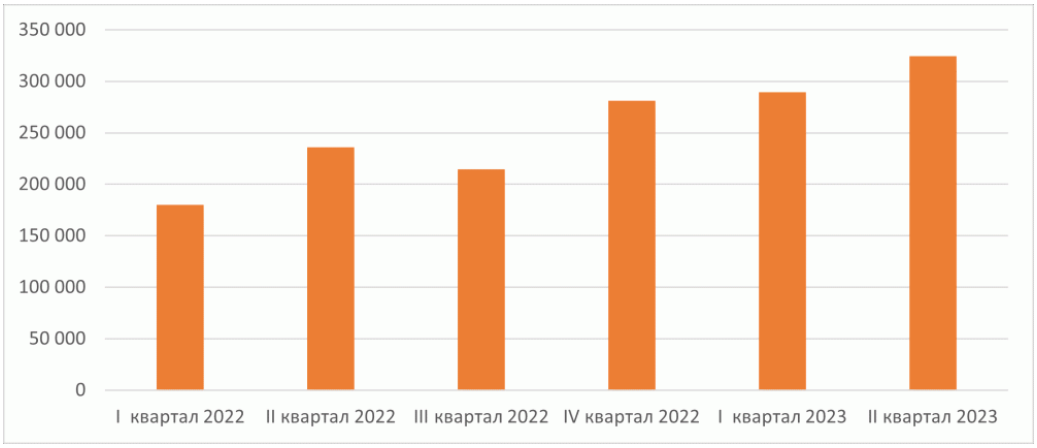


Рис. 1. Динамика роста числа кибератак 2022-2023 гг.

Спам представляет собой нежелательные или несанкционированные сообщения, чаще всего рекламного характера, которые рассылаются массово через электронную почту, социальные сети и мессенджеры. Помимо раздражающего фактора для пользователей, спам несет более серьезные риски [3]. Он может содержать вредоносные ссылки или вирусы, которые активируются при нажатии, а также фишинговые схемы, направленные на кражу персональных данных. Последствия распространения спама могут включать утечку конфиденциальной информации, заражение устройств вирусами и снижение производительности системы [4]. Такие угрозы требуют от компаний и пользователей повышения уровня информационной гигиены, установки современных фильтров и внедрения эффективных стратегий кибербезопасности, чтобы минимизировать риски и сохранить цифровое пространство безопасным. Так, согласно отчету компании «Positive Technologies» число утечек информации из организаций увеличилось с 47 % до 56 % в период с 2022 по 2023 годы, что во многом объясняется участившимися спам-атаками.

ТАБЛИЦА 1. Методы и алгоритмы защиты от спам-атак

№	Инструмент	Состав	Результат
1	Байесовский фильтр	Работает по принципу вероятностного анализа текста, оценивая вероятность того, что сообщение является спамом на основе ключевых слов и фраз, часто встречающихся в спам-сообщениях	Повышение точности классификации спама и снижение ложных срабатываний
2	Черные списки (Blacklist)	Использует базы данных известных источников спама, блокируя сообщения от IP-адресов, которые замечены в рассылке нежелательных сообщений	Предотвращение входа спама от источников, ранее замеченных в подозрительной активности
3	Методы машинного обучения (Machine Learning)	Использует базы данных известных источников спама, блокируя сообщения от IP-адресов, которые замечены в рассылке нежелательных сообщений	Адаптация к новым видам спама и более точное распознавание
4	Фильтрация на основе сигнатур (Signature-based Filtering)	Работает, сравнивая содержимое входящих сообщений с известными шаблонами спама	Быстрое обнаружение известных типов спам-атак, однако менее эффективно для новых типов угроз
5	Контентные фильтры (Content Filters)	Осуществляют анализ содержимого и ссылок в сообщениях на наличие подозрительных и вредоносных элементов, таких как фишинговые ссылки и вирусы	Предотвращение атак с использованием ссылок, защищая пользователей от переходов по вредоносным URL

В условиях продолжающегося роста числа кибератак и спам-угроз в 2024 году все более актуальным становится направление развития и применение методов и алгоритмов для защиты данных. Эти алгоритмы позволяют эффективно отслеживать, фильтровать и блокировать нежелательные сообщения и попытки несанкционированного доступа, предотвращая утечку данных и защищая устройства и сети. Алгоритмы защиты от спама по своему устройству и принципу работы могут различаться, начиная от простых фильтров, основанных на анализе ключевых слов, до сложных механизмов машинного обучения, которые обучаются на поведении пользователей и выявляют спам на основе динамических и контекстных факторов [5]. Автором в табл. 1 отражены наиболее эффективные методы и алгоритмы обеспечения безопасности данных для защиты от спама. Представленные методы и алгоритмы позволяют не только блокировать спам, но и постоянно адаптироваться к новым угрозам, обеспечивая надежную защиту данных и устройств от кибератак.

При этом особый интерес на момент 2024 года в вопросах защиты от спам-атак представляет развитие методов и алгоритмов искусственного интеллекта, поскольку традиционные методы фильтрации часто недостаточно эффективны против сложных и адаптивных атак, которые используют динамическое изменение контента и техники обхода. Искусственный интеллект позволяет адаптировать защитные меры, анализируя и классифицируя новые виды угроз в режиме реального времени, что делает его эффективным инструментом в противодействии современным спам-угрозам [6]. Для защиты от спама применяются различные методы и алгоритмы искусственного интеллекта, такие как машинное обучение и глубокое обучение, которые позволяют анализировать большие объемы данных и выявлять шаблоны поведения, характерные для спам-сообщений. Так, например, нейронные сети могут обучаться на больших наборах данных, чтобы различать спам от легитимных сообщений с высокой точностью. Метод обработки естественного языка (NLP) используется для анализа текста, помогая распознать фишинговые элементы, обманчивые фразы и вредоносные ссылки, что повышает способность фильтров выявлять замаскированные угрозы.

Помимо этого, алгоритмы классификации, такие как деревья решений и случайные леса, могут анализировать различные параметры сообщений - их структуру, частоту отправки и паттерны поведения отправителя, что позволяет идентифицировать подозрительные сообщения, даже если они не содержат традиционных признаков спама. Эти интеллектуальные инструменты улучшают защиту данных, предоставляя способность обучаться на меняющихся данных, адаптироваться к новым угрозам и защищать пользователей от сложных спам-атак, которые обходят классические фильтры.

Таким образом, основной целью представленной статьи являлось выполнение анализа относительно методов и алгоритмов обеспечения безопасности

данных для защиты от спама. В статье рассмотрены как традиционные подходы, такие как байесовская фильтрация и использование черных списков, так и инновационные методы на основе технологий искусственного интеллекта, включая машинное обучение, обработку естественного языка и классификацию данных. Современные алгоритмы ИИ продемонстрировали высокую адаптивность и гибкость, что делает их крайне эффективными для борьбы с динамическими и сложными видами спам-атак. Особую ценность в условиях 2024 года представляют алгоритмы глубокого обучения, нейронные сети и методы анализа естественного языка, которые способны распознавать скрытые угрозы, анализировать контекст сообщений и выявлять новые паттерны поведения в спам-атаках. Эти алгоритмы значительно превосходят традиционные методы, предлагая более точную и актуальную защиту, адаптированную к текущим и меняющимся угрозам. В заключение необходимо подчеркнуть необходимость продолжения разработки прикладных решений, использующих представленные в рамках настоящей статьи алгоритмы и методы, что позволит улучшить качество защиты от спам-атак и укрепить информационную безопасность в условиях роста киберугроз.

Список используемых источников

1. Частикова В. А., Козачек К. В. Обзор актуальных проблем основных методов фильтрации спама и анализ их эффективности // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки, 2021. №3 (286). С. 98–106.
2. Какорин И. А. Основные методы защиты конфиденциальной информации // Международный журнал гуманитарных и естественных наук, 2023. № 2-2 (77). С. 22–24.
3. Гафаров Р. И., Акбархужаев С. А. Применение двухуровневой модели для фильтрации спам-сообщений в электронной почте // Вестник науки и образования, 2020. № 11-2 (89). С. 40–44.
4. Плахина Е. А. К вопросу об информационной безопасности в сети интернет // Известия ТулГУ. Технические науки, 2020. № 12. С. 342–345.
5. Горюнова Д. А., Кузьмина Е. С. Обнаружение спама в электронной почте на основе машинного обучения: сравнение функциональной разработки и комплексных методов // Экономика и социум, 2024. № 6-1 (121). С. 1592–1597.
6. Козлова Н. Ш., Довгаль В. А. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки, 2023. № 3 (326). С. 65–72.

Raylyan D. **DATA SECURITY METHODS AND ALGORITHMS TO PROTECT AGAINST SPAM.**

Saint Petersburg State University of Industrial Technologies and Design

One of the most pressing threats to data protection is spam, and the number of attacks of this type is growing at a record pace each year. In this regard, the importance of tools that can ensure data security to protect against spam is increasing. This paper examines the most relevant and effective methods and algorithms aimed at countering spam.

Key words: spam, mailing, information security, data protection, fraudster, defense algorithm.

УДК 004.056
ГРНТИ 81.93.29

РОССИЙСКИЕ СКАНЕРЫ УЯЗВИМОСТЕЙ КАК НЕОБХОДИМОСТЬ ПОДДЕРЖАНИЯ ВЫСОКОГО УРОВНЯ ЗАЩИТЫ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Р. А. Рубацкий
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В статье рассмотрены причины необходимости и варианты защиты сетевой инфраструктуры с помощью автоматических сканеров угроз с помощью российского программного обеспечения.

сканеры уязвимостей, информационная безопасность компьютерных систем, БДУ ФСТЭК

Число кибератак во всем мире увеличивается от года к году, а развитие цифровизации увеличивает количество компьютерных систем в разы. По результатам исследования JupirterOne [1], за 2023 год количество ресурсов, участвующее в бизнес-процессах, увеличилось на 133 %, в то же время развитие искусственного интеллекта позволяет злоумышленникам получить более совершенное оружие взлома, и снижает уровень квалификации злоумышленника. Соответственно нагрузка на специалистов информационной безопасности возрастает и единственным путем противостоять злоумышленникам является автоматизация поиска возможных угроз.

Начиная с 2022 года, число кибератак на российские сервера резко возросло, что поспособствовало пониманию, что целью для атаки может быть кто угодно. В конце 2022 года Positive Technologies провели опрос среди представителей IT-компаний [2], госсектора, кредитно-финансовых организаций, и промышленных компаний. Согласно нему, по сравнению с 2020 годом доля компаний, не использующих специализированное программное обеспечение для работы с уязвимостями, сократилось с 26 % до 11 %. Так же изменилось и отношение к иностранному программному обеспечению: 50 % – что уже используют российское ПО, а 18 % респондентов сообщило, что планируют переход с иностранных продуктов на отечественное программное обеспечение.

Одним из инструментов борьбы с угрозами выступают автоматические сканеры уязвимостей. В России их использование необходимо не только для самостоятельной проверки инфраструктуры, но и для выполнения требований регуляторов PCI SSC, ФСТЭК России.

Сканеры уязвимостей представляют собой программные инструменты для поиска уязвимостей в информационной инфраструктуре. Благодаря им возможно найти уязвимости в операционных системах, сетевых ресурсах, веб-сервисах. Анализ распространяется как на внутренние, так и внешние угрозы. Основная задача сканера – поиск и выявление уязвимостей в системах, моделирование возможных атак, возможность заблокировать доступ к уязвимости до того момента как злоумышленник сможет ее использовать.

Использование данных инструментов позволяет поддерживать высокий уровень информационной безопасности, сокращать время на поиск угроз, а также исключить человеческих фактор.

Принцип работы автоматизированных сканеров уязвимостей [3]:

1. Сканирование сети. Проводится полная инвентаризация узлов, находящихся в сети, идентификация подключенных устройств и их параметры.

2. Сканирование портов. Проверяются все возможные открытые порты, анализируется сетевые сервисы и протоколы.

3. Идентификация уязвимостей. На основе банка данных угроз производится поиск уязвимых мест в конфигурациях устройств, операционных систем и приложений.

4. Анализ безопасности. При возможностях программ выполняется проверка на угрозы веб-сервисов, систем управления базами данных. Проверка на пароли по умолчанию, или даже производится проверка по базе данных утечки паролей.

5. Создание отчета. Должен содержать не только список угроз, но и рекомендации по их устранению.

Процесс поиска уязвимостей может быть как пассивным, так и активным. Активное сканирование подразумевает взаимодействие с системами напрямую, пассивное сканирует сетевой трафик и анализирует данные без непосредственного взаимодействия с системами.

Не маловажно то, что сканер угроз должен быть сертифицирован в государственных структурах и соответственно работать со своевременно обновляемой базой данных угроз.

На российском рынке представлены несколько систем сканеров уязвимостей [4].

– XSpider – компания «Positive Technologes»;
– MaxPatrol 8 - компания «Positive Technologes»;
– RedCheck – компания «АЛТЭКС-СОФТ»;
– ScanOVAL - компания «АЛТЭКС-СОФТ» по инициативе ФСТЭК;
– ревизор сети – ООО «Профиль защиты»»
– сканер ВС-6 – НПО «Эшелон».

Все данные системы сертифицированы ФСТЭК и имеют поддержку стандартов ФСТЭК и ГОСТ.

Рассмотрим основные функции данных систем.

1. XSpider и MaxPatrol 8 две системы от одной фирмы. Отличие в том, что XSpider более упрощенная форма сканера угроз и существует для быстрого выявления уязвимостей в сетевых структурах. MaxPatrol же предназначен для обеспечения контроля защищенности и соответствия стандартам безопасности информационных систем.

2. MaxPatrol 8 – одна из самых функциональных программ. Имеет собственный сканер разработки Positive Technologes, проводит комплексный анализ в сложных системах, включая Windows, Linux, Unix, сетевое оборудование Cisco, Juniper, Huawei. Так же работает с системами виртуализации Hyper-V, VMware, Ngnix и другими, серверами веб-приложений IBM WebSphere, Oracle, WebLogic и ERP-системами SAP и 1С.

В сканере присутствует анализ веб-приложений с поиском уязвимостей SQL-инъекций и межсайтовое выполнение сценариев XSS. Так же программа способна проверять СУБД, анализировать сетевые настройки, проверять на пароли по умолчанию, права и привилегии пользователей и позволяет управлять обновлениями. Есть интеграция с банком угроз безопасности ФСТЭК.

3. RedCheck – так же одна из самых функциональных программ. Использует сканер nmap со скриптами NSE. Обладает поддержкой поиска уязвимостей в системах семейства Windows, Linux, сетевого оборудования Cisco, Huawei, Check Point и других. Поиск угроз в веб-приложениях, контроль конфигураций и оценка соответствия их стандартам безопасности. Проведение аудита СУБД, аудита парольной политики, инвентаризация сети для получения информации об аппаратных и программных средствах. Так же присутствует аудит SCADA систем.

4. ScanOVAL разработан по инициативе ФСТЭК. Работает только под управлением семейства Windows. Сканер осуществляет поиск угроз, сведения о которых находятся в банке данных угроз безопасности информации ФСТЭК России. Использует XML-файлы с OVAL описаниями уязвимостей, выполненными со стандартом «The OVAL Language Specification».

5. Ревизор сети. Работает с Windows и Linux, способен искать угрозы, включенные в банк данных угроз ФСЭК России, и международных базах. Так же может включать в свой отчет результаты, полученные с использованием сетевого сканера nmap. Основные функции: проверка уязвимостей Windows, Linux, СУБД, средств виртуализации, проверка учетных записей для узлов сети с подбором паролей, сбор дополнительной информации об ОС Windows.

6. Сканер ВС-6 осуществляет комплексный анализ защищенности. Позволяет проводить тесты на проникновение и осуществлять анализ конфигураций различных узлов. База угроз обновляется еженедельно, так же осуществ-

лена поддержка банка данных угроз ФСТЭК. Сканер позволяет проводить инвентаризацию сети, сетевой и локальный анализ стойкости паролей, перехват и анализ сетевого трафика, анализ беспроводных сетей, аудит комплекса настроек Astra Linux и средств защиты. Дополнительно есть возможность поиска остаточной информации и гарантированную очистку через многократные затирания файлов по стандартам ГОСТ, BSI, FIPS, DoD.

Выводы

В связи с увеличением числа угроз безопасности сетевой инфраструктуре необходимым действием является автоматизация ручного труда и как следствие использование автоматических сканеров поиска угроз. Так же с невозможностью более безопасно использовать иностранное программное обеспечение, необходим переход на российское ПО.

Использование автоматического сканера угроз позволяет освободить достаточно времени сотрудников информационной безопасности, при своевременном обновлении исключить возможность пропуска угрозы, обеспечить быстрое реагирование на новые угрозы и содержать сетевую инфраструктуру с высоким уровнем безопасности. Так же на российском рынке программного обеспечения содержится достаточное количество сертифицированных продуктов. Выбор только по соотношению цена-качество, однако экономить на собственной безопасности не стоит.

Список используемых источников

1. Positive Technologes: Автономные SOC: будущее мониторинга ИБ и реагирования на инциденты. URL: https://www.ptsecurity.com/ru-ru/research/analytics/autonomous-socs-future-of-cybersecurity-monitoring-and-incident-response/#id1 (дата обращения 09.11.2024).
2. Positive Technologes: Как изменилась работа с уязвимостями в 2022 году. URL: https://www.ptsecurity.com/ru-ru/research/analytics/kak-izmenilas-rabota-s-uyazvimostyami-v-2022-godu/?utm_source=pt&utm_medium=cpm&utm_campaign=VM-analytics22&utm_content=product-Xspider (дата обращения 09.11.2024).
3 SecurityLab: Российские сканеры уязвимостей: обзор технологий и решений URL: https://www.securitylab.ru/blog/personal/paragraph/354220.php?ref=123 (дата обращения 09.11.2024).
4. Anti-Malware: Сканеры уязвимостей – обзор мирового и российского рынков. URL: https://www.anti-malware.ru/analytics/Market_Analysis/Vulnerability-scanners-global-and-Russian-markets (дата обращения 09.11.2024).

Rubatskiy R. **RUSSIAN VULNERABILITY SCANNERS AS A NECESSITY TO MAINTAIN A HIGH LEVEL OF NETWORK INFRASTRUCTURE PROTECTION.**

Saint Petersburg State Institute of Industrial Technologies and Design

The article discusses the reasons for the need and options for protecting network infrastructure using automatic threat scanners using Russian software.

Key words: Vulnerability scanners, information security of computer systems, FSTEC BDU.

УДК 004.75
ГРНТИ 20.15.05

ВЛИЯНИЕ РАСШИРЕННОГО ИСПОЛЬЗОВАНИЯ IOT НА БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ КОММУНИКАЦИЙ

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

Данная статья посвящена изучению влияния расширенного использования Internet of Things (IoT) на безопасность беспроводных коммуникаций. В контексте современного развития технологий IoT, все больше устройств становятся подключенными к Интернету, создавая не только новые возможности, но и угрозы для безопасности. В статье обсуждаются основные аспекты, связанные с безопасностью беспроводных коммуникаций в контексте расширенного использования IoT. Анализируются потенциальные уязвимости и угрозы, с которыми возможно столкнуться при использовании беспроводных коммуникаций, а также предлагаются методы и рекомендации для обеспечения безопасности в данной области.

IoT, безопасность, беспроводные коммуникации, уязвимости, атаки, шифрование, блокчейн, аутентификация, авторизация, контроль доступа, обнаружение аномалий, искусственный интеллект

Расширенное использование Интернета вещей (IoT) предоставляет множество преимуществ и новых возможностей в различных сферах жизни, начиная от домашней автоматизации и заканчивая промышленными процессами. Однако, использование IoT имеет ряд уязвимостей и потенциальных угроз безопасности [1, 2].

Одной из основных проблем, возникающих при эксплуатации IoT, является уязвимость сетевых устройств. Каждое подключенное устройство может стать точкой входа, которой могут воспользоваться злоумышленники, чтобы получить несанкционированный доступ к важной информации, перехватить коммуникации или взломать устройства для своих целей [3, 4].

Для защиты беспроводных соединений IoT необходимо применять современные методы и технологии. Одной из таких технологий является блокчейн. Блокчейн предлагает децентрализованную систему хранения данных, которая обеспечивает прозрачность, непрерывность и целостность информации. В контексте беспроводных коммуникаций блокчейн может использоваться для создания доверенности и обеспечения целостности данных, например, для за-

писи и проверки логов устройств IoT, что позволяет отслеживать и проверять все изменения данных и выявлять возможные атаки или вмешательства.

Еще одним важным инструментом для обеспечения безопасности беспроводной связи является искусственный интеллект. С помощью алгоритмов машинного обучения и анализа данных, искусственный интеллект может автоматически обнаруживать аномалии и возможные угрозы в сети. Например, системы машинного обучения могут анализировать сетевой трафик и идентифицировать необычное поведение устройств или несанкционированную активность. Это позволяет активно реагировать на возможные атаки и предупреждать о возможных угрозах.

Однако, несмотря на преимущества использования блокчейна и искусственного интеллекта, они также имеют свои ограничения. Блокчейн требует высокой вычислительной мощности для выполнения операций. Искусственные нейронные сети требуют больших объемов входных данных и значительного времени для обучения и оценки трафика.

Также важно принимать во внимание вопросы приватности и конфиденциальности при обработке и передаче данных в беспроводных сетях IoT. С увеличением количества подключенных устройств и объема генерируемых данных возникает угроза нарушения приватности и утечки конфиденциальной информации. Поэтому необходимо разработать эффективные механизмы защиты данных и создать стандарты приватности и безопасности, которые должны соблюдаться при использовании беспроводных IoT коммуникаций.

Каждое использование IoT должно быть сопровождено соответствующими мерами безопасности, чтобы защитить беспроводные коммуникации от возможных атак и угроз. Технологии, такие как блокчейн и искусственный интеллект, могут играть важную роль в обеспечении безопасности системы, но требуют дальнейшего развития и исследований, чтобы стать полностью эффективными и надежными решениями. Ключевыми аспектами являются учет ограничений и вызовов, а также обеспечение приватности и конфиденциальности данных [5].

Существуют различные методы обеспечения эффективной защиты беспроводных коммуникаций:

1. Одним из основных методов является шифрование данных. Шифрование обеспечивает конфиденциальность и целостность передаваемой информации путем преобразования ее в зашифрованный вид, который может быть расшифрован только с помощью ключа. Однако, не все алгоритмы и протоколы достаточно надежны, некорректно выбранный или уязвимый шифровальный алгоритм может привести к успешному взлому системы. Поэтому, при выборе метода шифрования необходимо учитывать его надежность.

2. Вторым методом является аутентификация и авторизация устройств. При аутентификации проводится проверка подлинности идентификаторов устройств. Авторизация устанавливает права доступа и полномочия для каждого устройства. Данный метод защиты помогает предотвратить несанкционированный доступ.

3. Третий метод – контроль доступа, который позволяет управлять тем, какие устройства и какие данные имеют доступ к сети. Можно использовать различные техники контроля доступа, такие как механизмы идентификации, сетевые уровни фильтрации и виртуальные частные сети.

4. Четвертый метод – обнаружение аномалий, которое заключается в мониторинге поведения системы и обнаружении необычных или подозрительных активностей. Этот метод основан на анализе и сравнении данных с базовыми параметрами и моделями поведения системы. При обнаружении аномалии принимаются соответствующие меры для предотвращения атаки или несанкционированного вмешательства.

Каждый из приведенных способов обеспечения безопасности имеет свои преимущества и ограничения. Шифрование данных обеспечивает конфиденциальность, но может увеличить нагрузку на систему. Аутентификация и авторизация гарантируют безопасность, но требуют дополнительных ресурсов для проверки подлинности и принятия решений. Контроль доступа и обнаружение аномалий требуют постоянного мониторинга и настройки, но могут быть эффективны при предотвращении несанкционированного доступа и обнаружении атак [6].

Для обеспечения безопасности в устройствах IoT необходимо сочетать различные методы и алгоритмы, адаптировать их к специфическим потребностям системы, что позволит минимально нагружать вычислительные ресурсы системы. Это может быть достигнуто использованием легковесных алгоритмов шифрования, уникальных идентификаторов устройств, биометрических данных или двухфакторной аутентификации; настройкой ограничений доступа к определенным функциям устройства или установкой политик доступа для различных пользователей; созданием алгоритмов машинного обучения, которые анализируют паттерны поведения устройств и выявляют отклонения от нормы [7].

Список используемых источников

1. Штеренберг С. И., Виткова Л. А., Просихин В. П. Методика применения концепции адаптивной саморазвивающейся системы // Информационные технологии и телекоммуникации, 2014. Т. 2. № 4. С. 126–133.

2. Гельфанд А. М., Казанцев А. А., Красов А. В., Орлов Г. А. Оценка рисков и угроз безопасности в среде «Умный Дом» // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 316–321.
3. Косов Н. А., Гельфанд А. М., Лаптев А. А. Анализ темных данных для обеспечения устойчивости информационных систем от нарушения конфиденциальности или несанкционированных действий // Colloquium-Journal, 2019. № 13-2 (37). С. 100–103.
4. Красов А. В., Гельфанд А. М., Коржик В. И., Котенко И. В., Петрив Р. Б., Сахаров Д. В., Ушаков И. А., Шариков П. И., Юркин Д. В. Построение доверенной вычислительной среды. СПб.: СПбГУТ, 2019. 108 с.
5. Кривец А. С., Штеренберг С. И. Анализ систем искуственного интелекта применяемых для работы систем обнаружения вторжений // Технологии информационного общества. Сборник трудов XVIII Международной отраслевой научно-технической конференции. М., 2024. С. 99–101.
6. Казанцев А. А., Манжула К. А., Пестов И. Е., Шкляев Г. В. Проблемы кибербезопасности iot устройств // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 386–389.
7. Штеренберг С. И., Пестов И. Е., Гельфанд А. М., Катасонов А. И., Бударный Г. С. Программа расчета защищенности модели машинного обучения и построения нейронной сети на основе данной модели. Свидетельство о регистрации программы для ЭВМ RU 2024663124, 04.06.2024. Заявка от 21.05.2024.

Rudenko S. **THE IMPACT OF THE EXPANDED USE OF IOT ON THE SECURITY OF WIRELESS COMMUNICATIONS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article is devoted to the study of the impact of the extended use of the Internet of Things (IoT) on the security of wireless communications. In the context of the modern development of IoT technologies, more and more devices are becoming connected to the Internet, creating not only new opportunities, but also security threats. The article discusses the main aspects related to the security of wireless communications in the context of the expanded use of IoT. Potential vulnerabilities and threats that may be encountered when using wireless communications are analyzed, as well as methods and recommendations for ensuring security in this area are proposed.

Key words: IoT, security, wireless communications, vulnerabilities, attacks, encryption, blockchain, authentication, authorization, access control, anomaly detection, artificial intelligence.

УДК 004.8
ГРНТИ 20.51.23

ОПТИМИЗАЦИЯ МОБИЛЬНОГО ИНТЕРФЕЙСА С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В. И. Стародубцев
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В данной работе рассматриваются методы оптимизации мобильного интерфейса с использованием технологий искусственного интеллекта, таких как машинное обучение, обработка естественного языка и компьютерное зрение. Описаны подходы к предсказанию пользовательских действий и персонализации интерфейса, адаптация интерфейса с учетом условий окружающей среды и улучшение удобства использования с помощью голосовых помощников. Приведены примеры успешного применения ИИ компаниями Google и Yandex, что позволяет сократить время выполнения задач пользователями и повысить удовлетворенность их взаимодействием с приложениями.

искусственный интеллект, машинное обучение, мобильные интерфейсы, персонализация UX, обработка естественного языка (NLP), компьютерное зрение, адаптивный интерфейс, пользовательский опыт (UX)

В последние годы мобильные устройства стали неотъемлемой частью жизни большинства людей, предоставляя доступ к огромному количеству приложений и веб-сайтов. Однако растущий объем информации и функциональных возможностей требует эффективных интерфейсов, которые обеспечивают удобство и интуитивное взаимодействие пользователей. Проблема адаптации интерфейсов к разнообразным потребностям пользователей, их предпочтениям и характеристикам устройства стала одной из основных задач, стоящих перед разработчиками. Технологии искусственного интеллекта (ИИ) предоставляют уникальные возможности для оптимизации интерфейсов, позволяя повысить эффективность и персонализировать взаимодействие [1].

Цель данной работы – исследовать и описать методы оптимизации мобильного интерфейса с помощью ИИ, а также рассмотреть успешные примеры внедрения таких решений. Мы сосредоточим внимание на подходах, использующих машинное обучение, обработку естественного языка и методы компьютерного зрения для улучшения взаимодействия пользователя с мобильными устройствами.

Многие исследователи подчеркивают значимость улучшения UX (User Experience) мобильных приложений через внедрение ИИ. Одним из популярных подходов является использование машинного обучения для прогнозиро-

вания пользовательского поведения и автоматической настройки интерфейсов в реальном времени. Например, алгоритмы, которые анализируют привычки пользователей и адаптируют интерфейс в соответствии с их предпочтениями.

Исследования показывают, что персонализация интерфейса может значительно сократить количество действий, необходимых для выполнения задачи, и улучшить общую удовлетворенность пользователей. Современные системы, такие как рекомендательные движки и чат-боты, применяют ИИ для анализа данных о поведении пользователя, предоставляя персонализированные рекомендации. В данной статье мы рассмотрим, как подобные методы могут использоваться для мобильных интерфейсов.

Машинное обучение для предсказания действий пользователя

Методы машинного обучения помогают уменьшить количество действий и время, которое пользователь тратит на выполнение определенных задач. Такие технологии позволяют адаптировать интерфейсы под индивидуальные задачи пользователя, что делает использование приложений более простым и интуитивно понятным [2].

Например, в приложение для электронной коммерции можно использовать машинное обучение, для сбора статистического анализа, как ведет себя пользователь. На основе собранных данных, интерфейс автоматически показывает персональный порядок отображения на главной странице.

Предварительные исследования в области пользовательского опыта (UX) показывают, что адаптивные интерфейсы, которые основываются на машинном обучении, способны уменьшить затрачиваемое время и повысить удовлетворенность пользователей примерно на 25 %.

Обработка естественного языка для интерфейсов с голосовым управлением

Технологии обработки естественного языка (NLP) находят широкое применение в голосовых интерфейсах, что создает более удобное и доступное взаимодействие пользователя с приложением. Это особенно актуально в тех случаях, когда стандартные методы общения с приложением становятся затруднительными [3].

Например, в банковских приложениях, голосовые помощники могут выполнять такие задачи, как переводы денег или просмотр конкретной информации, при этом нет необходимости нажимать кнопки или использовать меню. Благодаря NLP пользователи могут сократить количество действий, необходимых для выполнения конкретной задачи, до 40 %, что позволяет сделать приложение намного проще и удобнее для использования.

Компьютерное зрение для адаптивного отображения интерфейса

Компьютерное зрение позволяет сделать интерфейсы более удобными, подстраиваясь под определенные условия, например освещение или местоположение пользователя. Благодаря таким технологиям, интерфейс может изменять автоматически цветовую схему или расположение элементов на экране, для того, чтобы элементы на экране стали более видимыми, а взаимодействие пользователя с приложением более комфортнее [4].

Например, тоже самое приложение для чтения новостей. В нем можно использовать анализ освещения вокруг пользователя, чтобы автоматически изменять яркость экрана в зависимости от освещения. Это позволит уменьшить нагрузку на глаза и сделать использование приложения на более комфортным. Такие маленькие изменения значительно повышают удобство для пользователей. Внедрение таких технологий может повысить видимость на 30 %, а также снизить нагрузку на зрение пользователя.

Крупные компании, такие как Google и Yandex, также используют искусственный интеллект для улучшения интерфейсов своих мобильных приложений. Эти технологии помогают сделать их приложения более удобными и понятными для пользователей. Например, в сервисах YouTube и Google Maps технологии машинного обучения анализируют поведение пользователей и на основе этого предсказывают их действия. Данный подход сокращает время на то, чтобы пользователь искал какую-нибудь информацию, а также ускоряет выполнение задач примерно на 20 %, что в последствии повышает комфорт и удовлетворенность пользователей [5].

Персонализация интерфейса и голосовые помощники Yandex активно использует ИИ для персонализации интерфейсов и интеграции голосового помощника «Алиса» в свои приложения. Обработка естественного языка позволяет пользователям взаимодействовать с интерфейсом с помощью голосовых команд, что особенно удобно для выполнения банковских операций и поиска информации. Согласно внутренним исследованиям Yandex, внедрение голосового помощника сократило количество действий пользователей на 35 %, улучшив удобство использования и сделав приложение более доступным для широкого круга пользователей [6].

Таким образом, применение ИИ для оптимизации мобильных интерфейсов открывает новые возможности для повышения удобства и эффективности взаимодействия пользователей с приложениями. Перспективные направления дальнейших исследований включают в себя разработку более сложных алгоритмов, способных адаптироваться к изменениям в поведении пользователей, и улучшение методов обработки естественного языка для более точной и естественной работы с голосовыми командами.

Искусственный интеллект позволяет автоматизировать многие аспекты интерфейса, что делает его персонализированным и динамическим, что особенно важно в современном мире, где мобильные устройства стали неотъемлемой частью повседневной жизни.

Список используемых источников

1. Рассел С., Норвиг П. Искусственный интеллект: современный подход. М.: Вильямс, 2006. 1408 с.
2. Жуков И. В., Герасимов С. В. Машинное обучение: методы и алгоритмы. М.: Бином, Лаборатория знаний, 2018. 432 с.
3. Бахтин М. А., Ханевский М. В. Обработка естественного языка и голосовые интерфейсы. СПб.: Питер, 2020. 256 с.
4. Ильин А., Окулов А., Невзоров И. Компьютерное зрение и глубокое обучение. М.: ДМК Пресс, 2019. 368 с.
5. Google AI. Understanding context with BERT. Google AI Blog, 2021. URL: https://ai.google-blog.com/2021/05/understanding-context-with-bert.html (дата обращения 06.11.2024).
6. Yandex. Развитие голосового помощника Алиса. Yandex Company Blog, 2022. URL: https://yandex.ru/blog/company/alisa (дата обращения 06.11.2024).

***Starodubtsev V.* OPTIMIZING THE MOBILE INTERFACE USING ARTIFICIAL INTELLIGENCE.**

Saint Petersburg State University of Industrial Technologies and Design

This paper examines methods for optimizing mobile interfaces using artificial intelligence technologies, such as machine learning, natural language processing, and computer vision. It describes approaches to predicting user actions and personalizing the interface, adapting the interface to environmental conditions, and improving usability with the help of voice assistants. Examples of successful AI implementation by companies like Google and Yandex are provided, demonstrating how AI can reduce task completion time for users and enhance their satisfaction with application interactions.

Key words: Artificial intelligence, machine learning, mobile interfaces, UX personalization, natural language processing (NLP), computer vision, adaptive interface, user experience (UX).

УДК 004.056.53
ГРНТИ 81.93.29

АНАЛИЗ СВОЙСТВ ДЕЦЕНТРАЛИЗОВАННЫХ РАССИНХРОНИЗИРОВАННЫХ ПАКЕТНЫХ НЕЙРОСЕТЕВЫХ ПРОГРАММ В РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

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

В современном мире информационные технологии составляют значимую часть повседневной жизни. Оптимизируют многие процессы, ускоряют обмен данными и повышают качество коммуникации. Одним из ключевых компонентов информационных технологий является искусственный интеллект (ИИ), который активно используется в различных сферах жизни, таких как наука, образование, транспорт и так далее. Все это требует анализа и обработки больших объемов данных, в данном случае рационально использовать распределенные системы, которые обеспечивают высокую производительность, отказоустойчивость, безопасность и удобство использования.

машинное обучение, искусственный интеллект, многослойные нейронные сети, обмен данными и инженерия

Нейронная сеть – это метод обучения (написания) компьютерной программы, основанный на принципах работы человеческого мозга. В искусственных нейронных сетях простейшие процессоры выполняют функции нейронов, а нейронные связи передают данные в виде числовых значений от одного нейрона к другому. Существует три основных типа нейронов:

1. Входные нейроны – получают большой объем информации, такой как тексты, изображения и данные из баз.

2. Скрытые нейроны – занимаются обработкой полученных данных.

3. Выходные нейроны – формируют ответ, после обработки данных, на поставленный вопрос или задачу.

Два американских ученых Уоррен Маккаллок (англ. Warren Sturgis McCulloch) и Уолтер Питтс (англ. Walter Pitts) в 1943 году впервые смоделировали процессы, происходящие в человеческом мозге, и разработали модель искусственного нейрона, основанную на математической логике. А в 1958 году американский нейрофизиолог Фрэнк Розенблатт (англ. Frank Rosenblatt) создал первую однослойную модель нейросети, получившую название «Перцептрон» [1].

Перцептрон представляет собой математическую (компьютерную) модель восприятия информации мозгом человека. Состоит из трех элементов: поступающие от датчиков сигналы передаются ассоциативным элементам, а затем – реагирующим элементам. Перцептроны позволяют создавать ассоциации между входными стимулами и требуемой реакцией на выходе.

Уже тогда ИИ могли распознавать простые образы и обучаться на основе подкрепления. Перцептрон задумывался как искусственный аналог человеческого нейрона и обучался с помощью корректировки «весов» на основе обратной связи. «Веса» – это параметры (коэфиценты), которые влияют на входной сигнал и принятие решений в нейронной сети. Если перцептрон давал правильный ответ, параметры не корректировали. Если неправильный – «веса» изменяли, пока ИИ не выдаст точный результат. Идеи, заложенные в Перцептрон, до сих пор играют ключевую роль в развитии современных моделей.

Главное отличие нейросети от обычной компьютерной программы это способность к обучению и самостоятельному переобучению. Поэтому результат работы нейросетей, хоть и имитируют то, что уже создано человеком, но не являются копиями. Например, обучив нейросеть на произведениях одного писателя, на выходе мы получим новое произведение с сюжетными линиями и персонажами, но с узнаваемым стилем автора.

Проблема

На сегодняшний день нейросети не превосходят мозг человека, они не разумны, и не способны реагировать на нестандартные ситуации. Они обрабатывают большое количество данных, но не отличают лож от правды. Нейросети обучены на массиве данных, подготовленных за определенный период, которые не учитывают новую информацию без участия человека и корректировки так называемых «весов», как следствие они могут работать с ошибками [2].

Основные характеристики

Обработка данных. Способны обрабатывать большие объемы данных, но ограничены информацией, на которой были обучены.

Ложная информация. Не могут различить достоверные и недостоверные данные, что приводит к ошибкам в результатах.

Реакция на нестандартные ситуации. Работают по заранее заданным алгоритмам и не могут адаптироваться к новым условиям без дополнительного обучения.

Участие человека. Для корректной работы необходимо участие человека для обучения нейросети, анализа результатов для уменьшения ошибок.

Децентрализованные рассинхронизированные пакетные нейросетевые программы

Децентрализованные рассинхронизированные ПНП представляют собой сложные системы, которые используют распределенные вычисления для обработки данных. Эти программы работают на основе множества распределенных узлов, каждый из которых выполняет свою часть вычислений независимо от других и обладают основными характеристиками.

Децентрализация. Вычисления распределены между несколькими узлами, что обеспечивает устойчивость системы к сбоям и повышает общую производительность.

Рассинхронизация. Узлы работают асинхронно, что позволяет им выполнять задачи в своем собственном режиме и времени, независимо от других узлов.

Пакетная обработка. Данные обрабатываются пакетами, что помогает более эффективно использовать ресурсы и минимизировать задержки.

Преимущества:

1. Высокая отказоустойчивость. В случае сбоя одного или нескольких узлов, система продолжит функционировать благодаря другим.

2. Масштабируемость. Добавление новых узлов увеличивает производительность системы без необходимости корректировки всей архитектуры.

К недостаткам можно отнести:

1. Сложность управления. Децентрализация требует более сложного управления и координации между узлами.

2. Задержки. Рассинхронизация приводит к задержкам в обработке данных.

3. Безопасность. Для обеспечение безопасности данных в системе требуется применения шифрования и дополнительных других мер защиты.

Таким образом, децентрализованные рассинхронизированные пакетные нейросетевые программы представляют собой мощные и гибкие инструменты для обработки данных, которые эффективны для обучения нейронных сетей в распределенных информационных системах с ограниченными ресурсами.

Свойства децентрализованных рассинхронизированных пакетных нейросетевых программ включают:

1. Ковариантный сдвиг. Проблема, возникающая из-за изменения пропорций элементов в обучающих данных, что замедляет процесс обучения модели. Это приводит к нестабильности и снижению точности модели.

2. Внутренний ковариантный сдвиг. Проблема, связанная с изменением распределения входных данных для каждого узла скрытых слоев при обновлении параметров предыдущего слоя. Это взывает расхождения в обучении между различными узлами сети.

3. Пакетная нормализация. Алгоритм устранения внутреннего ковариантного сдвига, который реализует наиболее быструю сходимость моделей, независимость обучения слоев нейронов и возможность использования более высокой скорости. Она нормализует входные данные для каждого пакета данных, что ускоряет процесс обучения и улучшает производительность модели.

Дополнительные свойства:

1. Адаптивная стратегия усреднения. Позволяет проводить распределенное обучение с разными параметрами подключения сети и вычислительной производительностью.

2. Глобальная аккумуляция градиентов. Обеспечивает эффективное накопление информации о ошибках для всех узлов сети. Это синхронизирует обучение между узлами и поддерживает целостность модели.

3. Проектирование специализированной системы. Учитывает особенности постановки задачи и позволяет обучать нейронные сети под конкретные требования и условия.

Для повышения стабильности, скорости и эффективности обучения нейронных сетей используется Пакетная нормализация (batch normalization).[4] Этот алгоритм, который используется для повышения производительности и стабильности нейронных сетей. Основные причины, почему он применяется:

1. Повышение стабильности обучения. Помогает стабилизировать процесс обучения, уменьшая внутренние ковариационные сдвиги в данных. Это особенно полезно в глубоких нейронных сетях, где ковариационные сдвиги всегда приводят к нестабильности и замедлению системы.

2. Улучшение скорости обучения позволяет быстрее сходиться к оптимальным параметрам, что ускоряет процесс обучения, так как имеют более предсказуемое распределение, что облегчает градиентный спуск.

3. Предотвращение переобучения. Так как данные более независимы от их исходного масштаба и распределения. Это позволяет нейронным сетям лучше обобщать и применять полученные знания к новым данным.

4. Улучшение интерпретируемости. Нормализованные данные легче интерпретировать, что используется для аудита работы нейронных сетей.

5. Устойчивость к изменениям в архитектуре. Пакетная нормализация может быть применена к различным архитектурам нейронных сетей.

Заключение

Децентрализованные рассинхронизированные пакетные нейросетевые программы в распределенных информационных системах обладают преимуществами, такими как устойчивость к сбоям, масштабируемость и гибкость. Что делает их мощным инструментом для решения самых сложных задач в области машинного обучения и искусственного интеллекта, особенно в условиях большого объема данных и распределенных вычислений.

Однако, такие системы имеют ряд недостатков и проблем, таких как необходимость постоянного участия человека в корректировке весов, синхронизации и постоянном обучении на новых данных.

Децентрализованные рассинхронизированные пакетные нейросетевые программы представляют собой перспективное направление для развития информационных технологий, но требуют тщательного подхода к их использованию и управлению, необходимо учитывать их особенности и разрабатывать стратегии для минимизации ошибок и повышения точности результатов.

Список используемых источников

1. Ховард Дж., Гуггер С. Глубокое обучение с fastai и PyTorch: минимум формул, минимум кода, максимум эффективности. СПб.: Питер, 2022. 624 с.
2. Рашид Т. Создаем нейронную сеть.: Пер. с англ. СПб.: ООО «Альфа-книга», 2017. 272 с.
3. Уорр К. Надежность нейронных сетей: укрепляем устойчивость ИИ к обману. СПб.: Питер, 2021. 272 с.
4. Бурков А. Инженерия машинного обучения / пер. с англ. А.А. Слинкина. М.: ДМК пресс, 2022. 306с.

Talakin E. **ANALYSIS OF THE PROPERTIES OF DECENTRALIZED, DESYNCHRONIZED, PACKET-BASED NEURAL NETWORK PROGRAMS IN A DISTRIBUTED INFORMATION SYSTEM.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This research focuses on the analysis of the properties of decentralized, desynchronized, packet-based neural network programs in a distributed information system. The study explores the characteristics and performance of these programs, highlighting their advantages and challenges in real-world applications.

Key words: machine learning, artificial intelligence, multilayer neural networks, data exchange and engineering.

УДК 004.056
ГРНТИ 81.93.29

АРХИТЕКТУРА СЕРВИСА СБОРА ДАННЫХ ДЛЯ ОБНАРУЖЕНИЯ ИНСАЙДЕРСКИХ УГРОЗ В ФАЙЛОВЫХ СИСТЕМАХ LINUX

А. Н. Тамбовский, И. А. Ушаков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе представлена архитектура сервиса сбора данных, предназначенного для обнаружения инсайдерских угроз в файловых системах Linux. Сервис специализируется на сборе сырых данных из различных инструментов, основанных на современных методах, таких как логирование, мониторинг, изоляция процессов, контроль целостности и ограничение привилегий. Собранные данные нормализуются и отправляются на внешний сервер, например, в систему SIEM, для дальнейшего анализа и реагирования. Предлагаемая архитектура обеспечивает гибкое и масштабируемое решение для эффективного обнаружения инсайдерских угроз.

информационная безопасность, инсайдерские угрозы, сервис сбора данных, linux, siem, Journald, Syslog, Inotify, Auditd, SELinux, AppArmor, Tripwire, RBAC

Введение

В современном цифровом мире информационные технологии являются фундаментом деятельности большинства организаций. С увеличением объема данных и усложнением информационных систем возрастает и число потенциальных угроз безопасности. Одной из наиболее серьезных и сложных для обнаружения является инсайдерская угроза – действия сотрудников или лиц с легальным доступом к системам, которые могут умышленно или случайно нанести вред организации.

Обнаружение таких угроз в файловых системах Linux требует системного подхода и использования специализированных инструментов для сбора и передачи данных в системы управления информационной безопасностью, такие как «Security Information and Event Management (далее – SIEM) [1]. В данной статье предлагается архитектура сервиса сбора данных, который интегрирует различные методы и инструменты безопасности для централизованного сбора сырых данных. Это позволяет эффективно обнаруживать инсайдерские угрозы и своевременно реагировать на них.

Актуальность

Инсайдерские угрозы стали одной из наиболее серьезных проблем для современных организаций. С увеличением объема ценной информации

внутри компаний растет и мотивация для сотрудников или лиц с легальным доступом к системам совершать неправомерные действия. Обладая привилегированным доступом и глубоким пониманием внутренних процессов, инсайдеры способны скрывать свои действия и обходить стандартные меры защиты, что значительно усложняет их обнаружение. В этом контексте разработка специализированного сервиса сбора данных для обнаружения инсайдерских угроз в файловых системах Linux приобретает особую актуальность.

Требования

Для решения поставленной задачи был сформирован следующий список требований:

– удобство настройки и обслуживания сервиса;
– стандартные протоколы и форматы данных для передачи информации;
– защита собранных данных;
– гибкость в изменении используемых методов;
– поддержка различных дистрибутивов Linux [2].

Основная часть

В основе сервиса лежит использование различных методов и инструментов мониторинга и безопасности, что представлено на рис. 1.

Рис. 1. Архитектура сервиса сбора данных для обнаружения инсайдерских угроз в файловых системах Linux

К общей архитектуре сервиса относятся следующие методы:

– логирование;

– мониторинг;

– изоляция процессов;

– контроль целостности;

– ограничение привилегий;

– сбор данных.

Каждый из этих методов поддерживается специализированными инструментами, обеспечивающими эффективное выполнение соответствующих функций.

Для простоты предлагается рассмотреть сценарий, в котором все описанные методы и инструменты взаимодействуют для предотвращения потенциальной угрозы [3].

От учетной записи (далее – УЗ) выполняется попытка несанкционированного изменения файла, содержащего конфиденциальную информацию. УЗ не имеет соответствующих привилегий, поэтому файл не удается изменить. Происходит попытка обхода ограничений через скрипт получения доступа к файлу. Далее следуют попытки изменения системных файлов конфигурации. Дальнейшие действия подвергаются постоянной регистрации. Установленные политики безопасности приводят к полной блокировке УЗ.

Методы сервиса выполняются в следующем порядке.

1. Логирование. Инструменты [4] используются для регистрации попыток доступа. Предлагается использовать API инструмента JournalD.

2. Мониторинг. Системные вызовы, попытками доступа. Это включает идентификатор пользователя (UID) и задействованные процессы. Данные отправляются в сервис сбора через API инструмента Inotify.

3. Изоляция процессов. Блокируются вторичные попытки запуска вредоносного скрипта приложений, лог события отправляется с сервис сбора.

4. Контроль целостности. Критичные файлы обладают метками, что обеспечивает защиту от попыток компрометации.

5. Ограничение привилегий. Подход снижает риски нарушения конфиденциальности файлов. Механизм блокирует запрос и фиксирует событие отказа в логах. Через API передается факт нарушения с сервис сбора при настройке автоматический мер по блокировке пользователя критически важна.

Существует несколько направлений для дальнейших исследований. Расширение интеграции с новыми инструментами мониторинга, логирования и анализа позволит охватить более широкий спектр потенциальных угроз и повысить адаптивность системы. Оптимизация производительности сервиса

важна для снижения нагрузки на систему при обработке большого объема данных, особенно в условиях высокой интенсивности событий.

Заключение

Таким образом, обнаружение инсайдерских угроз в файловых системах Linux достигается сбором данных из различных источников. Данная архитектура сервиса централизует сбор данных для отправки в системы реагирования. В результате корреляции возрастает точность мониторинга, что приводит к улучшению безопасности системы.

Список используемых источников

1. 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. № 4. С. 25–33.
2. Многообразие Linux-дистрибутивов // habr. URL: https://habr.com/ru/companies/lanit/articles/562484/ (дата обращения 01.11.2024).
3. Виткова Л. А., Иванов А. И. Обзор актуальных угроз и методов защиты в сфере облачных вычислений // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 115–130.
4. journald вместо syslog // habr. URL: https://habr.com/ru/companies/lanit/articles/562484/ (дата обращения 05.11.2024).

Tambovskii A., Ushakov I. **ARCHITECTURE OF A DATA COLLECTION SERVICE FOR DETECTING INSIDER THREATS IN LINUX FILE SYSTEMS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This paper presents the architecture of a data collection service designed to detect insider threats in Linux file systems. The service specializes in collecting raw data from various tools based on modern methods, such as logging, monitoring, process isolation, integrity control, and privilege restriction. The collected data is normalized and sent to an external server, such as a SIEM system, for further analysis and response. The proposed architecture provides a flexible and scalable solution for effective insider threat detection.

Key words: information security, insider threats, data collection service, linux, siem, Journald, Syslog, Inotify, Auditd, SELinux, AppArmor, Tripwire, RBAC.

УДК 004.056
ГРНТИ 81.93.29

АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ СЕРТИФИКАТОВ TLS

А. С. Чистяков
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В статье рассматривается проблема автоматизации обновления сертификатов TLS, необходимых для обеспечения безопасности веб-сайтов и сервисов. Обсуждаются основные методы автоматизации, такие как использование протокола ACME, инструмента Certbot и интеграции с оркестраторами контейнеров (например, cert-manager для Kubernetes). Приведены ключевые преимущества автоматизации: снижение риска человеческих ошибок, повышение безопасности и экономия времени. Также обсуждаются возможные ограничения и риски, связанные с зависимостью от внешних сервисов и некорректной конфигурацией. В заключении подчеркивается важность автоматизации в управлении сертификатами и необходимость тщательной настройки систем для предотвращения возможных сбоев.

автоматизация TLS, ACME протокол, Certbot, обновление сертификатов, безопасность веб-сайтов, сертификаты X.509, Kubernetes cert-manager, цифровые сертификаты, управление сертификатами, защита данных

Введение

Сертификаты TLS (Transport Layer Security) играют ключевую роль в обеспечении безопасности веб-сайтов и интернет-сервисов. Они подтверждают подлинность сервера и шифруют данные между клиентом и сервером, защищая их от перехвата. Однако один из значительных вызовов для администраторов – это необходимость регулярного обновления сертификатов, так как истекший сертификат может привести к отключению сервиса или утечке данных. В последние годы разработаны методы автоматического обновления сертификатов, что упрощает управление сертификатами и уменьшает вероятность ошибок, связанных с истечением срока действия.

TLS обеспечивает возможность безопасного закрытия соединения.

Когда действительно получено оповещение о закрытии, а реализация показывает, что нет. Дальнейшие данные будут получены по этому соединению. TLS реализации должны инициировать обмен оповещениями о закрытии до закрытия соединения. Реализация TLS может после отправки оповещения о закрытии «закройте соединение», не дожидаясь, пока одноранговый узел отправить его оповещение о закрытии, генерируя «неполное закрытие». Обра-

тите внимание, что реализация, которая делает это, может выбрать повторное использование сеанса.

Это следует делать только тогда, когда приложение знает (обычно путем обнаружения границ HTTP-сообщений), что он получил все данные сообщения, которые его интересуют [1].

Эта статья представляет обзор технологий и подходов к автоматизации обновления сертификатов TLS.

Методы автоматического обновления сертификатов TLS

Существует несколько подходов к автоматизации обновления сертификатов TLS. Одним из наиболее известных решений является протокол ACME (Automated Certificate Management Environment), разработанный некоммерческой организацией Let's Encrypt. Этот протокол автоматизирует процесс выдачи, проверки и обновления сертификатов, устраняя необходимость вручную взаимодействовать с центром сертификации (CA).

ACME-протокол взаимодействует с центрами сертификации и веб-серверами для автоматической проверки домена и выпуска сертификатов. Сервер делает запрос на получение сертификата, ACME-провайдер (например, Let's Encrypt) проверяет, является ли заявитель владельцем домена, используя вызов HTTP-01 или DNS-01. При успешной проверке сертификат автоматически выдается и устанавливается на сервер. Примером использования ACME является инструмент Certbot, который поддерживает автоматическое обновление сертификатов на большинстве популярных веб-серверов, таких как Apache и Nginx [2].

В современных системах, таких как Kubernetes, автоматизация обновления сертификатов может быть интегрирована в оркестраторы контейнеров. Например, инструмент cert-manager для Kubernetes автоматизирует запрос и обновление сертификатов в кластерах Kubernetes. Этот процесс интегрируется с механизмами балансировки нагрузки и проксирования, что делает автоматическое обновление незаметным для пользователей.

Решения, такие как Ansible, Chef и Puppet, также поддерживают автоматизированное обновление сертификатов. Эти системы могут автоматически загружать и применять новые сертификаты, интегрируясь с ACME-сервисами [3].

Результаты и преимущества автоматизации

Автоматизация обновления сертификатов TLS предоставляет несколько важных преимуществ:

1. Человеческий фактор, как правило, является основной причиной ошибок при управлении сертификатами, таких как забывание о сроках действия сертификатов. Автоматизация сводит этот риск к минимуму.

2. Периодическое обновление сертификатов уменьшает шансы использования устаревших или скомпрометированных сертификатов.

3. Ручное управление сертификатами требует времени и ресурсов, особенно в больших инфраструктурах. Автоматизация значительно снижает затраты на администрирование.

В случае компрометации сертификата автоматизированные системы могут быстро обновить его без необходимости долгих процедур [4].

Обсуждение

Несмотря на преимущества автоматизации обновления сертификатов TLS, существует несколько ограничений и потенциальных рисков. Одним из таких рисков является зависимость от внешних сервисов, таких как Let's Encrypt, что может привести к проблемам при недоступности их серверов. Более того, автоматические системы могут столкнуться с конфликтами при некорректной конфигурации сервера, что приведет к простоям [5].

Другой проблемой может стать нехватка гибкости в настройках автоматизированных систем для особых сценариев. Например, в некоторых организациях может потребоваться использование сертификатов, которые не поддерживаются автоматизированными системами (например, сертификаты с особыми требованиями к шифрованию или подписанию) [6].

Также важным аспектом является настройка своевременных уведомлений об ошибках. В случае, если система автоматического обновления сталкивается с проблемой, важно, чтобы администратор был немедленно оповещен и смог вмешаться вручную.

Протокол TLS предоставляет встроенный механизм для согласования версий между конечными точками, потенциально поддерживающими разные версии TLS.

TLS 1.x и SSL 3.0 используют совместимые сообщения ClientHello. Серверы также могут обрабатывать клиентов, пытающихся использовать будущие версии TLS, пока формат ClientHello остается совместимым и есть по крайней мере одна версия протокола, поддерживаемая как клиентом, так и сервером. Предыдущие версии TLS использовали номер версии уровня записи (TLSPlaintext.legacy_record_version и TLSCiphertext.legacy_record_version) для различных целей. Начиная с TLS 1.3, это поле устарело. Значение TLSPlaintext.legacy_record_version должно игнорироваться всеми реализациями. Значение TLSCiphertext.legacy_record_version включено в дополнитель-

ные данные для снятия защиты, но МОЖЕТ быть в противном случае проигнорировано или МОЖЕТ быть проверено на соответствие фиксированному постоянному значению. Согласование версий выполняется только с использованием версий рукопожатия (ClientHello.legacy_version и ServerHello.legacy_version, а также расширений ClientHello, HelloRetryRequest и ServerHello "supported_versions"). Чтобы максимизировать взаимодействие со старыми конечными точками, реализации, которые согласовывают использование TLS 1.0-1.2, должны устанавливать номер версии уровня записи на согласованную версию для ServerHello и всех записей последующих [7].

Заключение

Автоматизация обновления сертификатов TLS – это важный шаг в обеспечении безопасности и надежности веб-сервисов. Она значительно уменьшает риск сбоев из-за истечения срока действия сертификатов и снижает нагрузку на администраторов. Протоколы, такие как ACME, и инструменты, такие как Certbot и cert-manager, предоставляют мощные решения для автоматизации процесса обновления сертификатов в различных инфраструктурах.

Однако, как и любое автоматизированное решение, такие системы требуют тщательной настройки и мониторинга для предотвращения сбоев, и возможных уязвимостей. В дальнейшем автоматизация в области управления сертификатами будет продолжать развиваться, предлагая все более гибкие и безопасные решения для различных сценариев использования.

TLS не зависит от протокола приложения; протоколы более высокого уровня могут быть прозрачно наложены поверх TLS. Однако стандарт TLS не определяет, как протоколы добавляют безопасность с TLS; как инициировать рукопожатие TLS и как интерпретировать обмененные сертификаты аутентификации оставлены на усмотрение разработчиков и реализаторов протоколов, работающих поверх TLS.

Список используемых источников

1. Barnes R., Hoffman-Andrews J., McCarney D., and Kasten J. RFC 8555: Automated Certificate Management Environment (ACME), 2020. URL: https://tools.ietf.org/html/rfc8555 (date accessed 24.10.2024).
2. Margolis D., Brotman A., Ramakrishnan B., Jones J., Risher M. RFC 8460: SMTP TLS Reporting, 2018. URL: IETF Datatracker. Available at: https://tools.ietf.org/html/rfc8460 (date accessed 24.10.2024).
3. Eff.org. Welcome to the Certbot Documentation! Certbot 2.11.0, 2014. URL: https://certbot.eff.org/docs/ (date accessed 24.10.2024).
4. Cert-manager. (n.d.). URL: https://cert-manager.io/docs/ (date accessed 24.10.2024).

5. Tsai E., et al. CERTainty: Detecting DNS Manipulation at Scale Using TLS Certificates // Proceedings on Privacy Enhancing Technologies. 2023. № 3. PP. 122–137.
6. Butun I., et al. Hardware Security of Fog End-Devices for the Internet of Things // Sensors, 2020. Vol. 20. № 20. PP. 5729, doi.org/10.3390/s20205729.
7. Rescorla E. RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3. // IETF Datatracker, 2018, tools.ietf.org/html/rfc8446. (date accessed: 24.10.2024).

Chistyakov A. **AUTOMATIC RENEWAL OF TLS CERTIFICATES.**

Saint Petersburg State University of Industrial Technologies and Design

This article addresses the issue of automating the renewal of TLS certificates, which are essential for securing websites and services. The paper discusses key automation methods, including the use of the ACME protocol, the Certbot tool, and integration with container orchestrators like cert-manager for Kubernetes. The primary advantages of automation are highlighted, such as reducing human error risks, improving security, and saving time. Potential limitations and risks are also discussed, including dependency on external services and misconfiguration. The conclusion emphasizes the importance of automation in certificate management and the need for careful system configuration to prevent potential failures.

Key words: TLS automation, ACME protocol, Certbot, certificate renewal, website security, X.509 certificates, Kubernetes cert-manager, digital certificates, certificate management, data protection.

УДК 004.056
ГРНТИ 81.93.29

ИНТЕГРАЦИЯ АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ TLS-СЕРТИФИКАТОВ В КОНТЕЙНЕРНЫЕ ОРКЕСТРАТОРЫ (KUBERNETES)

А. С. Чистяков
Санкт-Петербургский государственный университет промышленных технологий и дизайна

В статье рассматривается проблема управления TLS-сертификатами в контейнерных оркестраторах, таких как Kubernetes, и подчеркивается значимость автоматизации этого процесса. Представлен обзор инструмента cert-manager, способного обеспечивать автоматический запрос и обновление сертификатов в контейнерных инфраструктурах. Описаны ключевые преимущества интеграции cert-manager для безопасности и управления в кластерах Kubernetes, а также приведены примеры практического применения. Сделан акцент на актуальности автоматизированного подхода к управлению сертификатами для уменьшения нагрузки на администраторов и повышения операционной эффективности контейнерных сред.

Kubernetes, TLS-сертификаты, cert-manager, автоматизация, безопасность, контейнерные оркестраторы, управление сертификатами

Введение

Современные контейнерные среды требуют высокой степени автоматизации для эффективного управления инфраструктурой, обеспечивающей отказоустойчивость и безопасность. Kubernetes, как одна из наиболее популярных платформ для оркестрации контейнеров, позволяет развертывать и управлять масштабируемыми кластерами приложений, где каждая составляющая должна соответствовать высоким требованиям безопасности и оперативности. Одной из ключевых задач становится управление TLS-сертификатами для шифрования данных и защиты от внешних угроз.

В крупных инфраструктурах вручное обновление и управление сертификатами часто оказывается трудоемким и подверженным ошибкам. Особенно это касается масштабируемых и динамических сред, таких как Kubernetes, где требуется гибкий и автоматизированный подход. Без автоматического обновления сертификатов организации рискуют столкнуться с простоями и уязвимостями, вызванными истекшими сертификатами. Для решения данной проблемы многие компании внедряют инструменты автоматизации, такие как cert-manager, предназначенные специально для Kubernetes [1–2].

Интеграция cert-manager с Kubernetes

Cert-manager – это мощное средство для управления сертификатами, специально разработанное для работы с Kubernetes. Этот инструмент позволяет настроить процесс автоматического получения, обновления и управления сертификатами, что значительно упрощает поддержание безопасности в кластере. Cert-manager использует протокол ACME (Automatic Certificate Management Environment), который применяется для безопасного взаимодействия с центрами сертификации (ЦС) и автоматического выпуска сертификатов.

Cert-manager работает поэтапно, начиная с формирования запроса сертификата, который отправляется на сервер центра сертификации (CA) для получения сертификата. Затем cert-manager отслеживает сроки действия сертификатов, автоматически обновляя их при необходимости, что минимизирует риск простоя и необходимости ручного вмешательства. Более того, он поддерживает несколько источников, таких как Let's Encrypt и коммерческие центры сертификации, что позволяет гибко управлять сертификатами в соответствии с требованиями конкретной инфраструктуры.

Использование cert-manager существенно сокращает необходимость участия администратора, так как инструмент интегрируется с Kubernetes через Custom Resource Definitions (CRD), обеспечивая автоматизированное получение сертификатов для различных сервисов в кластере, таких как веб-приложения и API-серверы.

Автоматизация обновления TLS-сертификатов в контейнерных инфраструктурах приносит значимые преимущества. Во-первых, постоянное обновление сертификатов гарантирует непрерывную работу сервисов, так как cert-manager самостоятельно инициирует обновление, исключая остановку работы приложений из-за истечения срока действия сертификата. Централизованное управление сертификатами позволяет унифицировать контроль в кластере, обеспечивая их получение из единого источника и избегая разрозненного управления. Кроме того, автоматическое обновление исключает риск использования устаревших сертификатов, что особенно важно для соблюдения таких стандартов безопасности, как GDPR и HIPAA.

Автоматизация с помощью cert-manager снижает нагрузку на DevOps-команды, освобождая инженеров от необходимости постоянного мониторинга сертификатов. Благодаря поддержке различных источников, cert-manager также гибко адаптируется к различным корпоративным требованиям, позволяя интеграцию с различными центрами сертификации для более гибкого управления в соответствии с потребностями организации.

Практическое применение и примеры

Cert-manager активно применяется в контейнерных средах, позволяя DevOps-командам упростить управление сертификатами. Примером успешного использования cert-manager является его внедрение в кластеры, обслуживающие крупные e-commerce платформы, где требуется постоянная поддержка безопасности пользовательских данных. Также cert-manager применяют компании, предоставляющие финансовые услуги, где критично соблюдать строгие требования безопасности.

Благодаря cert-manager DevOps-инженеры могут автоматизировать запросы сертификатов и их обновление, избавляя команду от необходимости вручного вмешательства и минимизируя риск ошибок, связанных с человеческим фактором. Это позволяет инженерам сосредоточиться на задачах разработки и поддержке инфраструктуры, что значительно повышает эффективность всей команды.

В дополнение к этому cert-manager можно настроить для работы с такими источниками, как Let’s Encrypt, что делает его удобным решением для малого и среднего бизнеса, которым необходимы бесплатные и автоматизированные сертификаты для защиты своих сервисов. Cert-manager также успешно интегрируется с NGINX и другими сетевыми сервисами, что позволяет автоматизировать защиту веб-сервисов без сложных настроек [3–5].

Заключение

Автоматизация обновления TLS-сертификатов стала критическим компонентом для крупных контейнерных инфраструктур, таких как Kubernetes. Использование cert-manager предоставляет гибкость и надежность, позволяя организациям эффективно управлять сертификатами без значительных временных затрат. Это снижает нагрузку на DevOps-команды и обеспечивает непрерывную защиту данных, что важно для современных динамических приложений.

Таким образом, cert-manager стал одним из ведущих инструментов для управления сертификатами в Kubernetes, сочетая возможности автоматического обновления, централизованного управления и интеграции с различными ЦС. Внедрение cert-manager способствует повышению безопасности, улучшает управляемость и позволяет организациям уверенно использовать масштабируемые контейнерные инфраструктуры, соответствуя требованиям безопасности и стандартам индустрии.

Список используемых источников

1. Pourzandi M., Gordon D., Yurcik W. and Koenig G. A. Clusters and security: distributed security for distributed systems // CCGrid 2005. IEEE International Symposium on Cluster Computing and the Grid, 2005. Cardiff, UK, 2005. Vol. 1, PP. 96–104, doi: 10.1109/CCGRID.2005.1558540.
2. Burns B., Grant B., Oppenheimer D., Brewer E., Wilkes J. Borg, Omega, and Kubernetes: Lessons learned from three container-management systems over a decade // ACM Queue, 2016. Vol. 14 (1). PP. 70–93. doi: 10.1145/2898442.2898444.
3. Let's Encrypt Documentation. URL: https://letsencrypt.org/docs/ (дата обращения 02.11.2024).
4. Cert-manager Documentation. URL: https://cert-manager.io/docs/ (дата обращения 02.11.2024)/
5. Kubernetes Documentation. URL: https://kubernetes.io/docs/concepts/cluster-administration/certificates/ (дата обращения 02.11.2024).

Chistyakov A. **INTEGRATION OF AUTOMATED TLS CERTIFICATE RENEWAL IN CONTAINER ORCHESTRATORS (KUBERNETES).**

Saint Petersburg State University of Industrial Technologies and Design

The article addresses the problem of managing TLS certificates in container orchestrations such as Kubernetes and highlights the importance of automating this process. Presented a review of the cert-manager tool, which can provide automatic request and update of certificates in container infrastructures. The key benefits of integrating cert-manager for security and management in Kubernetes clusters are described, as well as examples of practical applications. Emphasis was placed on the relevance of the automated approach to certificate management to reduce the burden on administrators and improve the operational efficiency of container environments.

Keywords: Kubernetes, TLS certificates, cert-manager, automation, security, container orchestrators, certificate management.

УДК 004.056.57
ГРНТИ 20.53.01

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ANDROID-ПРИЛОЖЕНИЙ, НОВЫЕ УГРОЗЫ В OWASP MOBILE TOP 10

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

В данном докладе рассматривается перечень новых уязвимостей из OWASP Mobile Top 10 2024. Проведен анализ уязвимостей и их потенциального влияния на безопасность мобильных приложений, что позволило определить наиболее критические угрозы для разработчиков и пользователей. Предложенные в работе рекомендации помогают минимизировать риски, связанные с этими угрозами, и способствуют созданию более защищенных мобильных решений.

OWASP Top 10, безопасность мобильных устройств, Android, уязвимость

Рынок Android-приложений стремительно растет: в 2023 году пользователи Google Play скачали 111,3 миллиарда мобильных приложений. Уязвимости в Android-приложениях могут затронуть миллионы пользователей, что подчеркивает критическую важность тестирования безопасности.

Многие современные фреймворки, такие как React Native, Flutter и Kivy, упрощают разработку мобильных приложений для Android, используя различные языки программирования и технологии. Однако быстрый рост популярности Android приводит к тому, что разработчики сосредотачиваются на функциональности, пренебрегая аспектами безопасности.

OWASP (Open Web Application Security Project) – некоммерческая организация, поддерживающая безопасность программного обеспечения через открытую модель сообщества. OWASP Top 10 представляет собой рейтинг и рекомендации по устранению наиболее критических рисков безопасности мобильных приложений, основанные на опыте и консенсусе специалистов по безопасности со всего мира. Риски классифицируются по частоте, серьезности и возможному влиянию, помогая разработчикам интегрировать меры защиты и минимизировать известные угрозы. В таблице 1 представлено сравнение уязвимостей из списков 2016 и 2024 годов.

ТАБЛИЦА 1. Сравнение уязвимостей 2016 и 2024 года

OWASP-2016	OWASP-2024-Release	Comparison Between 2016-2024
M1: Improper Platform Usage	M1: Improper Credential Usage	New
M2: Insecure Data Storage	M2: Inadequate Supply Chain Security	New
M3: Insecure Communication	M3: Insecure Authentication / Authorization	Merged M4 & M6 into M3
M4: Insecure Authentication	M4: Insufficient Input/Output Validation	New
M5: Insufficient Cryptography	M5: Insecure Communication	Moved from M3 to M5
M6: Insecure Authorization	M6: Inadequate Privacy Controls	New
M7: Client Code Quality	M7: Insufficient Binary Protections	Merged M8 & M9 into M7
M8: Code Tampering	M8: Security Misconfiguration	Rewording (M10)
M9: Reverse Engineering	M9: Insecure Data Storage	Moved from M2 to M9
M10: Extraneous Functionality	M10: Insufficient Cryptography	Moved from M5 to M10

В ходе обновления списка, в нем появились новые уязвимости M1, M2, M4, M6, некоторые уязвимости были перераспределены или объединены. Это отражает изменение приоритетов в области мобильной безопасности и адаптацию к новым угрозам. Например, уязвимость M1: Improper Credential Usage описывает ситуации, когда мобильные приложения неправильно обрабатывают учетные данные, например, имена пользователей, пароли, токены аутентификации или ключи API [1]. На рисунке 1 можно увидеть пример неправильного хранения данных в приложении “BugBazzar”. В исходном коде представлены критически важные учетные данные, такие как Google API Key, Google App ID, и пароль (*hardc0d3d_passw0rd*), хранящиеся в файле *strings.xml* в открытом виде.

```
<string name="google_api_key">AIzaSyDOx8mTnKN6LiCVh7bCjAvGqrx4QCd9AHk</string>
<string name="google_app_id">1:135771924448:android:57eab34c35a3088fdbad85</string>
<string name="google_crash_reporting_api_key">AIzaSyDOx8mTnKN6LiCVh7bCjAvGqrx4QCd9AHk</string>
<string name="google_storage_bucket">bugbazaar-cb1a1.appspot.com</string>
<string name="hardc0d3d_passw0rd">BugBazaarSeccool</string>
<string name="hello_blank_fragment">Hello blank fragment</string>
```

Рис. 1. Уязвимость Improper Credential Usage

Хранение конфиденциальной информации внутри приложения делает его уязвимым для атак реверс-инжиниринга. Например, утечка ключей google_api_key позволяет выполнять ложные запросы или получать доступ к чувствительным данным. Сохранение паролей в открытом виде повышает риск несанкционированного доступа к учетным записям и системным ресурсам.

Чтобы предотвратить уязвимость Improper Credential Usage, нужно избегать жесткого кодирования учетных данных в приложении. Вместо этого рекомендуется хранить секреты с помощью выделенной системы управления секретами (HashiCorp Vault) или облачного сервиса (Azure Key Vault). Также следует внедрять многофакторную аутентификацию (MFA) для повышения уровня безопасности. Необходимо регулярно обновлять и проверять учетные данные, чтобы минимизировать риск их утечки. Шифрование данных учетных записей как в состоянии покоя, так и при передаче помогает защитить их от перехвата и утечек данных.

Уязвимость M2: Inadequate Supply Chain Security связана с недостаточной защитой цепочек поставок, которые используются для загрузки и использования сторонних библиотек, SDK и других зависимостей в мобильных приложениях [2]. Если приложение или его зависимость загружаются из ненадежных источников или не проверяются на подлинность, это может привести к выполнению вредоносного кода, который был внедрен в эти библиотеки. Примером такого типа уязвимости может быть ситуация, когда мобильное приложение загружает сторонние файлы или зависимости через небезопасные каналы, без проверки их подлинности или целостности. На рисунке 2 изображен пример того, как приложение загружает файл с HTTP-сервера. В содержимом файла включена строка “Bonch1”, после обнаружения этой строки выполняет вредоносный код, который создает дополнительный файл malicious_output.txt с вредоносным содержимым.

```
Загружаем файл с: http://localhost:8000/malicious-file.txt
Файл загружен: C:\PrivacyLabJava\VulnerableApp\downloaded_file.txt
Содержимое файла: This is a harmless text file.
Bonch1
More content after the exploit trigger.

Найдено 'Bonch1'. Выполняем вредоносный код...
Вредоносный код выполняется...
```

Рис. 2. Уязвимость Inadequate Supply Chain Security

Для защиты от уязвимости необходимо загружать внешние зависимости только через защищенные каналы (HTTPS) и проверять их целостность с помощью цифровых подписей и контрольных сумм. Следует ограничить дове-

ренные источники загрузки и использовать инструменты, такие как Snyk или OWASP Dependency-Check, для выявления уязвимостей в сторонних библиотеках.

Уязвимость M4: Insufficient Input/Output Validation связана с отсутствием проверки или неправильной проверкой данных, получаемых от пользователя, или данных, отправляемых и получаемых от внешних источников. Эта уязвимость позволяет проводить атаки, а именно: SQL-инъекции, межсайтовые скриптовые атаки (XSS) и атаки с использованием произвольных данных [3].

В приложении “BugBazzar” присутствует уязвимость, которая позволяет провести XSS атаку. Разрешение выполнения JavaScript через *webView.getSettings().setJavaScriptEnabled(true);* без должной проверки источников открывает возможность внедрения вредоносного кода. Также URL, передаваемый через Intent в константе AppConstants.KEY_WEBVIEW_URL, не проверяется, это позволяет злоумышленнику подменить легитимный адрес на вредоносный.

Команда *adb shell am start -n com.Bugbazaar/.ui.TermsAndConditionsActivity -e webViewUrl “http://192.168.33.1:8099/xss.html”* запускает TermsAndConditionsActivity в приложении Bugbazaar, передавая URL через параметр webViewUrl. Этот URL указывает на страницу с XSS-скриптом, в результате чего приложение загружает этот адрес в WebView, результат показан на рисунке 3.

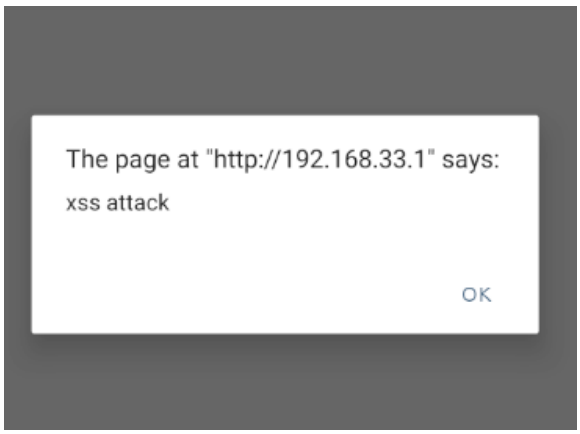


Рис. 3. Уязвимость Insufficient Input/Output Validation

Для предотвращения XSS-атак необходимо экранировать пользовательский ввод перед его выводом на веб-страницу, чтобы предотвратить выполнение вредоносных скриптов. Например, специальные символы <, >, и &, следует заменять на их HTML-эквиваленты *(<, >* и *&)*. Также нужно использовать безопасные методы вывода данных, такие как *TextView.setText()* в Android, которые автоматически экранируют ввод. Дополнительно следует использовать Content Security Policy (CSP) для ограничения источников скрип-

тов и внедрять библиотеки для проверки и очистки данных, полученных от пользователя или внешних источников [4].

Уязвимость M6: Inadequate Privacy Controls относится к недостаточному обеспечению конфиденциальности данных пользователей в мобильных приложениях. Для демонстрации работы была написана простая Java-программа (*InadequatePrivacyDemo.java*).

Эта программа устанавливает HTTP-соединение с локальным сервером и передает конфиденциальные данные (логин и пароль) в открытом виде. Для примера, программа отправляет *username=dima* и *password=jakobson* на сервер без какой-либо защиты. Отсутствие шифрования создает серьезную уязвимость, так как данные легко перехватить при помощи анализа сетевого трафика.

Мы создали простой сервер на Python, чтобы принять данные от Java-программы. Этот сервер работал на локальной машине и прослушивал входящие соединения на порту 8099.

На снимке экрана, представленного на рисунке 4, было видно, что передаваемые данные можно легко прочитать в незашифрованном виде.

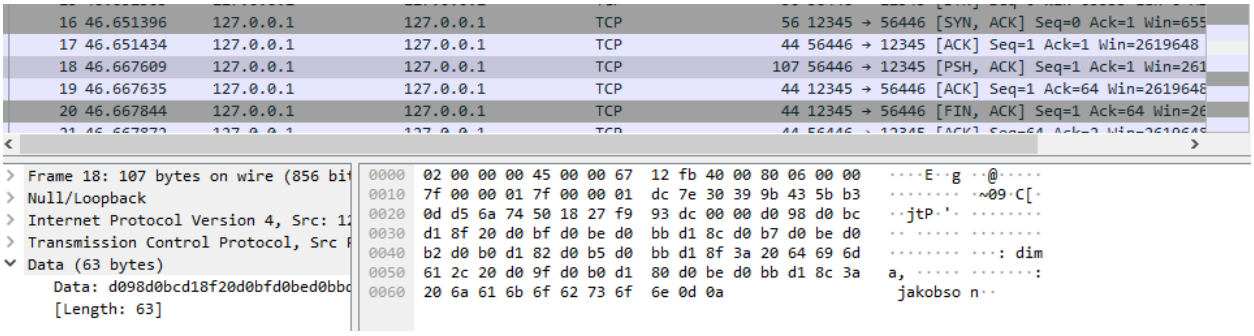


Рис. 4. Уязвимость Inadequate Privacy Controls

Для предотвращения уязвимости Inadequate Privacy Controls требуется соблюдать строгие практики минимизации данных, необходимо собирать и хранить только те данные пользователей, которые нужны для выполнения функции приложения. Например, если приложение собирает только адрес электронной почты для отправки уведомлений, оно не должно запрашивать и хранить номера телефонов пользователей.

В Android можно использовать встроенные средства шифрования, такие как Android Keystore для безопасного хранения криптографических ключей, AES для шифрования данных в покое и File-Based Encryption (FBE) для защиты данных на уровне файловой системы [5]. Для передачи данных рекомендуется использовать Network Security Configuration для настройки безопасных HTTPS-соединений. Эти методы помогают защитить конфиденциальность

пользователей и соответствовать требованиям Федерального закона № 152-ФЗ «О персональных данных».

Проведенный анализ новых уязвимостей из OWASP Mobile Top 10 подтвердил важность интеграции мер безопасности на всех этапах разработки. Обнаруженные уязвимости: неправильное использование учетных данных, недостаточная защита цепочки поставок, ошибки в валидации данных и недостаточные меры для обеспечения конфиденциальности, могут привести к серьезным угрозам для безопасности пользователей. Рекомендации, приведенные в статье, могут быть полезны разработчикам и организациям, стремящимся минимизировать риски и соответствовать требованиям безопасности в мобильной разработке.

Список используемых источников

1. Петрив Р. Б. Атаки на ОС Windows с помощью внедрения кода в легитимное по и методы их обнаружения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. Том 4. С. 813–819.
2. Сафин Л. К., Чернов А. В., Александров Я. А., Трошина К. Н. Исследование информационной защищенности мобильных приложений // Вопросы кибербезопасности, 2015. Т. 4. С. 28–37.
3. Домбровский Р. М., Петрив Р. Б. Анализ уязвимостей ядра и оценка эффективности средств защиты операционных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. Т. 4. С. 657–661.
4. Цыганенко Н. П. Статический анализ кода мобильных приложений как средство выявления его уязвимостей // ТРУДЫ БГТУ 2015. Том 6. Физико-математические науки и информатика. С. 200–203.
5. Коромыслов К. Е., Красов А. В., Ушаков И. А. Разработка модели угроз Android-приложений, свойственных ошибкам разработчика // I-methods, 2022. Т. 2.

***Jakobson D.* SECURING ANDROID APPLICATIONS: NEW THREATS IN THE OWASP MOBILE TOP 10.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This report examines the list of new vulnerabilities from the OWASP Mobile Top 10 2024. An analysis of the vulnerabilities and their potential impact on the security of mobile applications has been conducted, allowing for the identification of the most critical threats for developers and users. The recommendations provided in the report help minimize the risks associated with these threats and contribute to the development of more secure mobile solutions.

Key words: OWASP Top 10, mobile device security, Android, vulnerability.

4.2. Информационная безопасность компьютерных сетей

УДК 004.056.53
ГРНТИ 81.93.29

EXPLORING THE ROLE OF CANARY TOKENS IN DETECTION AND BACKDOOR ATTACKS IN WINDOWS ENVIRONMENTS

G. Mano, D. Turusida, M. N. Haddad
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Canary tokens play an important role in alerting administrators when certain files or system resources are accessed. While effective in many cases, the interaction between canary tokens and backdoor attacks remains an area of significant interest, especially as attackers employ advanced evasion tactics to evade detection systems.

canary tokens, backdoor, windows, Remote Access Tools (RATs), evasion techniques

Detecting unauthorised access and preventing persistent intrusions are key challenges for system administrators in modern cybersecurity. Canary tokens - decoy files or system resources designed to alert administrators when accessed - have gained prominence as an early warning mechanism [1]. These tokens, when accessed by an attacker, immediately alert system administrators and provide critical insight into the nature of the intrusion, including attacker behaviour, IP addresses and token names. The use of deception technologies, such as canary tokens, has been extensively studied in recent years [2, 3], but their interaction with backdoor attacks remains less explored.

Backdoor attacks, often using Remote Access Tools (RATs) such as Meterpreter, have evolved significantly. Attackers often evade traditional detection methods by using payload obfuscation and privilege escalation techniques [4]. Integrating canary tokens into detection systems is an effective countermeasure, but its success is not guaranteed against sophisticated evasion strategies [3].

A Canary Token is like motion sensors for your networks [1], computers and clouds. When an attacker interacts with the Canary token, such as opening a file or clicking a link, the token registers the activity and triggers an alert with the intruder's IP address, date, token name, etc.

Tokens can vary in format and complexity. In this study, we used several types of Canary tokens, including PDF and MS Word tokens, to demonstrate their effectiveness in detecting unauthorised access. When accessed, these tokens inform administrators of the attacker's IP address, the time of access and the specific resource accessed. Canary tokens have been deployed and successfully implemented in multiple industry use cases. These case studies highlight the effectiveness of canary tokens as an early warning system and a valuable tool in improving cybersecurity [5].

In the practical work conducted for this study, we created and monitored several canary tokens to observe how attackers interacted with these tokens. Figure 1 shows an instance where an MS Word document with a token was triggered by unauthorized access. This figure highlights the importance of canary tokens in providing immediate feedback about potential intrusions.

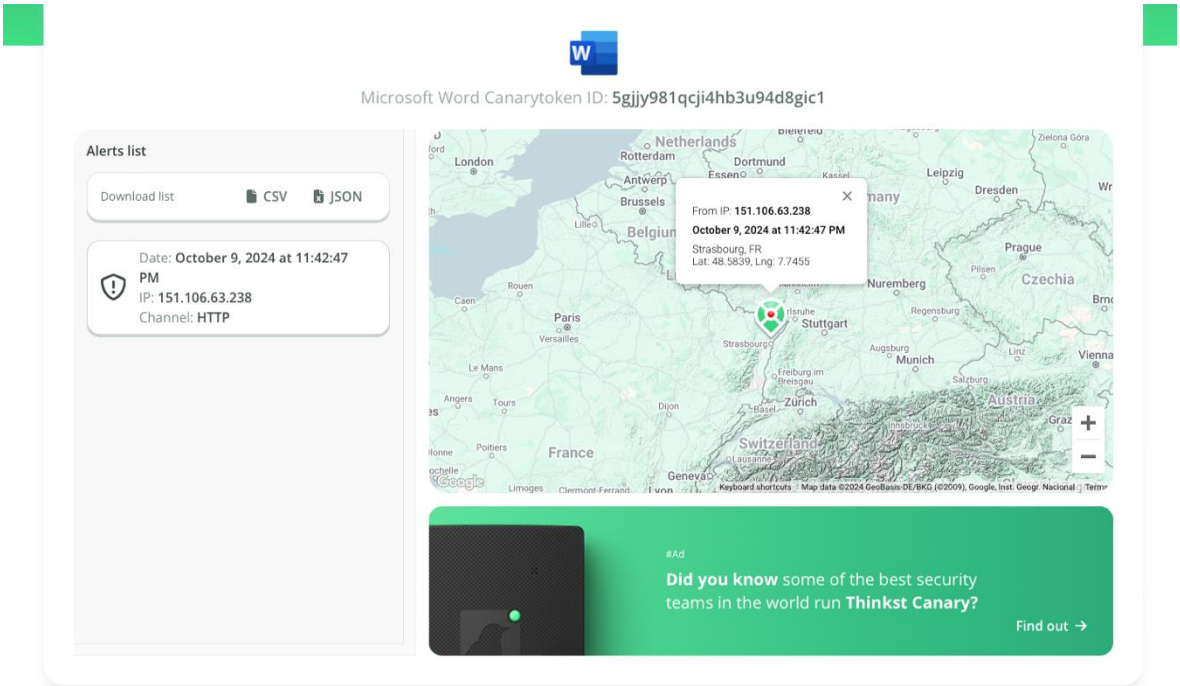


Fig. 1. Shows a canary token that was triggered when a MS Word document was accessed, providing more insight into the incident

The backdoor attack is one of the most threatening aspects that businesses face in the present times. An attacker, through hidden access points into systems, bypasses every layer of security and manages unauthorized entry into sensitive areas [6]. These attacks can take many forms, including Remote Access Tools (RATs) like Meterpreter, web shells, or custom malware that exploits specific system vulnerabilities. The primary goal of these backdoors is to enable attackers to maintain control of a system while avoiding traditional detection methods.

Despite the usefulness of canary tokens in identifying unauthorized access, backdoor attacks often employ a variety of evasion techniques to circumvent these defenses. For example, attackers may use payload obfuscation to disguise the nature

of their malicious code, or use privilege escalation to gain administrative access without triggering canary tokens. In addition, sophisticated malware may be able to access token-protected resources without alerting the monitoring system, as demonstrated by advanced RATs that can remain undetected even after accessing canary token files. This is consistent with previous studies showing how attackers use advanced evasion techniques to hide their presence on compromised systems [3].

Figure 2 shows a scenario where we used the Meterpreter session to access MS Word document and PDF files without triggering Canary tokens. The figure illustrates the limitations of relying solely on Canary tokens to detect sophisticated backdoor intrusions.

As shown, while Canary tokens can alert administrators to unauthorized access, backdoor attacks are constantly evolving and attackers are becoming more adept at evading detection systems. Therefore, it is imperative that detection mechanisms such as Canary tokens are constantly refined and adapted to stay ahead of these emerging threats.

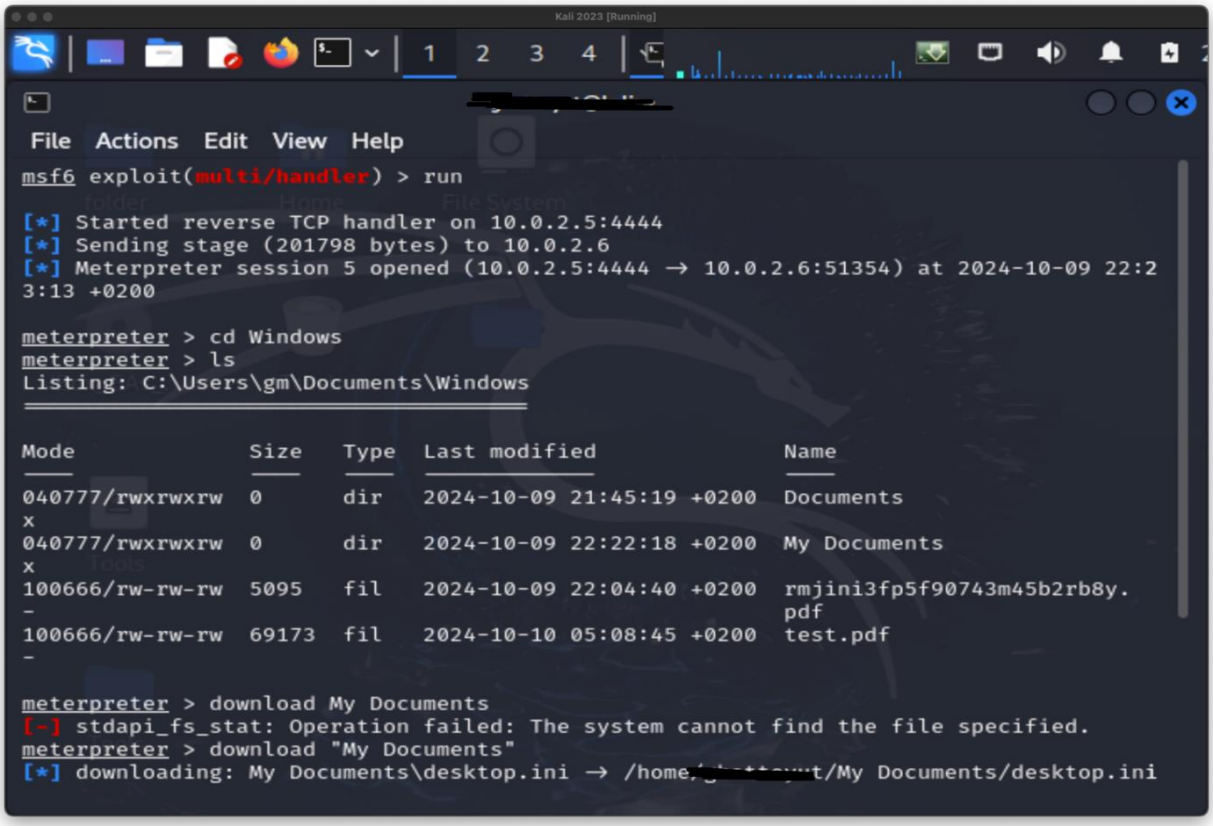


Figure 2. Shows a meterpreter session used to gain access to MS Word and PDF files without triggering Canary Tokens.

By strategically placing these bait tokens throughout various systems, organizations can detect and respond to threats in real-time, safeguarding their sensitive data and strengthening their overall security posture. However, their effectiveness is compromised by the techniques attackers use to evade detection, as demonstrated

by the use of an advanced RAT that was able to access not only the folder containing the Canary tokens, but also other files such as the token file of the MS Word document.

This research highlights the need for continuous adaptation of security tools such as Canary Tokens to ensure that they evolve with the tactics and techniques employed by advanced cybercriminals. Future research should explore further refinements in token deployment and the development of more robust methods to counter backdoor evasion.

References

1. CanaryTokens Documentation. URL: https://docs.canarytokens.org/guide/ (date of reference: 05.11.2024).
2. Srinivasa S., Pedersen J., Vasilomanolakis E. Towards systematic honeytoken fingerprinting. 2020. 10.1145/3433174.3433599.
3. Tal Arieh Be'ery and Itai Grady. Systems and methods for the detection of advanced attackers using client side honeytokens. US, 2020. Patent 10,609,048.
4. Casey P., Topor M., Hennessy E., Alrabaee S., Aloqaily M., Boukerche A. Applied Comparative Evaluation of the Metasploit Evasion Module. 2019. 10.1109/ISCC47284.2019.8969663.
5. Canary token – The Ultimate Tool for Detecting and Monitoring Cyber Attacks. URL: https://canariasacross.com/blog/canary-token-the-ultimate-tool-for-detecting-and-monitoring-cyber-attacks (date of reference: 05.11.2024).
6. What are Backdoor Attacks? Types & Examples. URL: https://www.sentinelone.com/cybersecurity-101/threat-intelligence/backdoor-attacks/ (date of reference: 06.11.2024).
7. Aslan Ö., Aktug S., Ozkan M., Yılmaz A., Akin E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, 2023. № 12. PP. 1–42. 10.3390/electronics12061333.

Мано Г., Турусида Д., Хаддад М. Н. **ИЗУЧЕНИЕ РОЛИ ТОКЕНОВ CANARY В ОБНАРУЖЕНИИ АТАК НА БЭКДОРЫ В СРЕДАХ WINDOWS.**

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

Canary токен играют важную роль в оповещении администраторов о доступе к определенным файлам или системным ресурсам. Несмотря на эффективность во многих случаях, взаимодействие между Canary Tokens и атаками с использованием бэкдоров по-прежнему представляет значительный интерес, особенно с учетом того, что злоумышленники применяют передовые тактики уклонения от систем обнаружения.

Ключевые слова: токены Canary, бэкдор, Windows, средства удаленного доступа (RAT), методы обхода.

УДК 004.056
ГРНТИ 20.53.31

ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ПЭМИН В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ. ПАССИВНЫЕ И АКТИВНЫЕ СРЕДСТВА ЗАЩИТЫ

И. Н. Бабков, А. С. Сидельников
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В автоматизированных системах технические каналы утечки информации представляют серьезную угрозу безопасности данных. К основным каналам побочных электромагнитных излучений и наводок относятся непреднамеренные излучения оборудования, которые могут быть перехвачены злоумышленниками. Для защиты от таких утечек используются активные средства, включающие создание помех и пассивные, включающие экранирование, фильтрацию сигналов. Эффективное сочетание этих методов минимизирует риск утечки информации и повышает общую защищенность системы.

информационная безопасность, техническая защита информации, ПЭМИН, автоматизированные системы, пассивная защита, активная защита

Под защитой информации понимается деятельность, направленная на предотвращение утечек данных и несанкционированного доступа. Выделяют множество технических каналов утечки информации, из которых одной из серьезнейших угроз является утечка через канал побочных электромагнитных излучений и наводок (далее – ПЭМИН), создаваемые техническими средствами. Эти излучения существуют в диапазоне от нескольких герц до полутора гигагерц и могут быть перехвачены злоумышленником [1].

Для защиты информации от утечки по техническим каналам применяются различные методы, которые можно разделить на пассивные и активные средства защиты информации (далее – СЗИ). Оба метода выполняют основную функцию, однако важно учитывать их недостатки, например, пассивные методы могут снижать удобство работы с оборудованием, в то время как активные методы могут накладывать дополнительные требования на обучение персонала.

Пассивный метод включает экранирование источников излучения. Это может быть достигнуто с помощью экранированных шкафов, помещений, а также использования поглощающих материалов. Основным недостатком является высокая стоимость создания экранированных помещений.

К пассивным СЗИ относятся поглощающие и экранирующие материалы, а также экранированные помещения, камеры и другие сооружения [2]. Применение пассивных методов защиты может быть более предпочтительным, чем активных, так как генераторы шума, входящие в состав активных СЗИ, могут оказывать негативное влияние на организм человека из-за высокого уровня электромагнитного и шумового излучения. Пассивные методы, в свою очередь, не оказывают отрицательного воздействия и, более того, в ряде случаев могут обеспечить комфортные условия, снижая уровень посторонних звуков в помещении. При высоком уровне экранирования оборудования и помещений использование активных средств безопасности может быть излишним. Экранирование защищает устройства, отдельные зоны или помещения целиком. Для защиты сетей электропитания и кабелей локальной сети применяются помехоподавляющие сетевые фильтры. Уязвимые места, такие как окна, защищаются демпферными прокладками или многослойным остеклением.

Однако, как показывает исследование В. И. Кутузова [3], увеличение количества стекол не всегда приводит к усилению звукоизоляции на частотах речевого сигнала, поскольку возможны резонансные явления в воздушных промежутках между стеклами и волновое совпадение.

Активные СЗИ [2] используют устройства, создающие электромагнитное шумовое поле в диапазоне частот информативного сигнала по каналу ПЭМИН. Активный метод обеспечивает защиту не только от утечки информации по каналам побочного электромагнитного излучения компьютера, но и от иных угроз. В частности, он снижает возможность использования встроенных подслушивающих устройств, а также проведения разведывательных операций, основанных на анализе излучения других технических средств, находящихся в защищаемом помещении [4].

Активные СЗИ [2] создают электромагнитное шумовое поле, препятствующее утечке информации через каналы ПЭМИН. Они включают генераторы шума, маскирующие устройства и средства постановки помех. Преимуществами активных методов являются их эффективность в подавлении излучений и активном противодействии разведывательным операциям. Однако такие устройства могут оказывать вредное воздействие на организм и требуют периодической проверки работоспособности.

В связи с тем, что периодичность проведения специальных исследований (СИ) [5] в рамках аттестации ОИ для различных категорий может достигать год или два, за это время СЗИ выделенного помещения может выйти из строя, и это будет незаметно при визуальном осмотре.

Для практической проверки работоспособности таких СЗИ существует множество специальных технических средств для обнаружения радиоизлуче-

ний. Среди них можно выделить индикаторы электромагнитного поля, специализированные радиоприемники, а также автоматизированные комплексы. Помимо прочего, исследование, проведенное в статье В. Н. Никитиной [6] показало необходимость разработки мер по защите персонала от воздействия электромагнитных полей. Особенно актуально изучение биологических эффектов при одновременном воздействии многочастотных электромагнитных полей с различными механизмами действия.

На основе вышеперечисленных данных и некоторых данных из статьи Н. В. Киреева [4], был представлен сравнительный анализ в виде таблицы 1.

ТАБЛИЦА 1. Сравнительный анализ пассивных и активных СЗИ

Критерий	Пассивные СЗИ	Активные СЗИ
Экономическая целесообразность	Высокая стоимость экранированных помещений	Более доступные для отдельных устройств
Удобство эксплуатации	Не требуют постоянного обслуживания	Требуют периодической проверки
Область применения	Экранирование устройств, зон и помещений	Подавление излучений, защита линий коммуникации
Риск неисправности	Минимальный благодаря простой конструкции	Высокий из-за сложного оборудования
Дополнительные преимущества	Уменьшение внешних шумов	Исключение подслушивания и анализа излучений

Таким образом, комплексное применение средств защиты информации является наиболее эффективным подходом, который учитывает, как физические особенности объекта защиты, так и особенности возможных технических каналов утечки.

Список используемых источников

1. Копытов П. Д. и др. Построение формальных моделей распространения побочных электромагнитных излучений по техническим каналам утечки информации для объектов вычислительной техники от технических средств разведки // Вестник УрФУ. Безопасность в информационной сфере, 2023. Т. 1. № 47. С. 102–111.

2. Лынов Е. В., Никифоров М. С., Конкин А. А., Чумаченко Д. К. Пассивные и активные методы защиты информации от утечки по каналу ПЭМИН // Седьмая научно-практическая конференция молодых ученых и специалистов АО «ГРПЗ»: сборник научных статей, Рязань, 27 октября – 03 ноября 2020 года. Рязань: Рязанская региональная общественная организация Союз социально активной молодежи «Созвездие», 2021. С. 84-98. EDN JBKXDE.

3. Кутузов В. И. Повышение эффективности защиты информации от утечек информации через окна по акустическому и виброакустическому каналу при использовании средств активной защиты // Евразийский научный, 2020. С. 13.
4. Киреева Н. В., Семенов А. В. Утечка информации по каналам ПЭМИ и способы их защиты // Международный журнал прикладных и фундаментальных исследований, 2016. № 8–4. С. 499–504. URL: https://applied-research.ru/ru/article/view?id=10110 (дата обращения 07.12.2024).
5. Сидельников Е. В., Столяров М. А. Разработка устройства контроля средств защиты объекта информатизации от утечки информации по каналам ПЭМИН // Техника и безопасность объектов уголовно-исполнительной системы: сборник материалов Международной научно-практической конференции: в 2 т., Воронеж, 20–21 мая 2020 года. Том 1. Воронеж: Издательско-полиграфический центр «Научная книга», 2020. С. 366-369. EDN SUCGOD.
6. Никитина В. Н., Калинина Н. И., Дубровская Е. Н., Плеханов В. П. Электромагнитная обстановка на рабочих местах при использовании активных средств защиты информации. Гигиена и санитария. 2023; Т. 102 (8). С. 800–805. https://doi.org/10.47470/0016-9900-2023-102-8-800-805. EDN: nglvkl.

Babkov I., Sidelnikov A. **TECHNICAL CHANNELS OF INFORMATION LEAKAGE IN AUTOMATED SYSTEMS. PASSIVE AND ACTIVE PROTECTION MEASURE.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In automated systems, technical channels of information leakage pose a serious threat to data security. The main channels of electromagnetic radiation and interference include unintended emissions from equipment, which can be intercepted by malicious actors. To protect against such leaks, active measures are used, including the creation of interference, and passive measures, such as shielding and signal filtering. An effective combination of these methods minimizes the risk of information leakage and enhances the overall security of the system.

Key words: information security, technical protection of information, TEMPEST, automated systems, passive protection, active protection.

УДК 004.56
ГРНТИ 81.93.29

ТЕСТИРОВАНИЕ ЭФФЕКТИВНОСТИ DEVSECOPS ПРОЦЕССОВ

М. Н. Бенч, Н. А. Косов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Тестирование эффективности DevSecOps процессов – это не просто метод проверки стабильности разработки, а ключевой этап, позволяющий оценить уровень интеграции безопасности в жизненный цикл программного обеспечения. В условиях постоянного роста угроз кибербезопасности и усложнения программных систем, компании сталкиваются с необходимостью обеспечения безопасности на всех этапах, от проектирования до эксплуатации

уязвимости, инциденты безопасности, угрозы конфиденциальности, кибербезопасность

Для обеспечения безопасности на всех этапах жизненного цикла от проектирования до эксплуатации недостаточно просто внедрить инструменты автоматизации и интегрировать тесты безопасности – важно понимать, насколько эффективно работают существующие процессы, и как их можно улучшить [1].

Тест DevSecOps призван ответить на два ключевых вопроса: насколько текущие процессы устойчивы к уязвимостям и инцидентам, и каким образом можно повысить их производительность и стабильность. Эти задачи актуальны в свете того, что большинство современных организаций сталкиваются с ограничениями времени, ресурсов и инструментов, которые ограничивают их способность к полной интеграции DevSecOps. Без тестирования компании рискуют упустить важные аспекты безопасности, что может привести к серьезным последствиям, включая утечки данных, репутационные риски и финансовые потери.

Тест проводится с целью анализа эффективности DevSecOps с использованием систематических метрик и алгоритмов. Основной подход заключается в том, чтобы измерить текущие показатели, выявить проблемные области и предложить решения для их оптимизации. При этом тестирование охватывает такие аспекты, как скорость разработки, стабильность релизов и способность быстро реагировать на инциденты. Основой теста служат метрики DORA, которые предоставляют объективную картину эффективности процессов.

Эксперимент

Для определения текущей зрелости процессов DevSecOps и выявления их узких мест был проведен эксперимент в среде разработки крупной ИТ-компании. Основной задачей стало измерение ключевых показателей эффективности, анализ слабых мест в CI/CD конвейере и тестирование подходов к оптимизации процессов. Эксперимент основывался на использовании метрик DORA, алгоритмов анализа данных и инструментов автоматизации.

Исходные условия и подготовка

Эксперимент начался с подготовки инфраструктуры и сбора данных. Для анализа была развернута среда CI/CD на базе Jenkins и GitLab CI, где уже использовались автоматизированные инструменты тестирования. SonarQube проводил статический анализ кода (SAST), выявляя уязвимости и кодовые дефекты, а OWASP ZAP выполнял динамическое тестирование приложений (DAST). Splunk, в свою очередь, использовался для мониторинга и анализа логов, что позволяло фиксировать закономерности [2].

Эксперимент проводился в течение трех месяцев в производственной среде крупной ИТ-компании, использующей CI/CD конвейеры для ежедневных релизов программного обеспечения. Главной задачей стало не только измерение базовых метрик, но и их последующий анализ для выявления проблемных областей и внедрения оптимизаций. Эксперимент охватил три основных этапа: сбор данных, анализ логов и оптимизация процессов.

Этап 1. Сбор данных. Для анализа были использованы данные о 1800 релизах, собранные в течение 90 рабочих дней. Эти релизы представляли собой разнообразные изменения – от мелких багфиксов до крупных обновлений функционала. Информация включала временные метки выполнения задач в CI/CD конвейере, результаты автоматизированного тестирования безопасности и логи производственных серверов.

Использование CI/CD платформ Jenkins и GitLab CI позволило собирать данные автоматически. Каждый этап конвейера, от проверки кода до развертывания, генерировал логи, которые хранились в централизованной системе мониторинга Splunk. Кроме того, результаты тестов безопасности, проводимых с помощью SonarQube и OWASP ZAP, интегрировались в аналитическую платформу для последующего анализа [3].

Этап 2. Анализ базовых показателей. Базовые метрики эффективности были рассчитаны на основе собранных данных. Средняя частота развертываний составила 15 релизов в день, что соответствовало уровню начальной зрелости DevSecOps процессов. Однако анализ показал, что значительная часть

времени уходила на ожидание завершения автоматизированных тестов безопасности. В частности, тестирование часто задерживалось из-за ложных срабатываний, что указывало на недостатки конфигурации.

Среднее время восстановления после инцидентов (MTTR) находилось на уровне 4 часов. Это время включало в себя обнаружение сбоя, анализ логов для выявления причины и внедрение исправлений. Установлено, что значительная доля инцидентов была связана с конфигурационными проблемами на серверах. Процент неудачных релизов составлял 8 %, что указывало на высокую вероятность сбоев при развертывании, особенно для крупных изменений [4].

Этап 3. Использование алгоритмов анализа данных. Для выявления закономерностей в данных и идентификации проблемных областей использовались алгоритмы машинного обучения. В частности, Random Forest применялся для классификации логов CI/CD процессов и выявления факторов, связанных с задержками и сбоями. Gradient Boosting использовался для предсказания вероятности неудачных релизов на основе таких параметров, как размер обновления, число изменений в коде и количество тестов.

Анализ логов позволил выявить несколько ключевых проблем:

1. Конфигурационные ошибки. Сервера с определенными сетевыми параметрами регулярно вызывали сбои при развертывании. Это требовало пересмотра конфигураций и устранения конфликтов.

2. Избыточное тестирование. Некоторые этапы тестов безопасности выполнялись с избыточной частотой, что приводило к увеличению времени выполнения конвейера.

3. Ложные срабатывания. Некорректная настройка SonarQube и OWASP ZAP приводила к большому числу ложных срабатываний, что замедляло релизы.

Этап 4. Внедрение оптимизаций. На основании анализа были предложены и внедрены следующие изменения:

– оптимизация конфигурации серверов;

– автоматизация тестов безопасности;

– интеграция предиктивного анализа.

Этап 5. Измерение улучшений. После внедрения изменений показатели эффективности существенно улучшились. Средняя частота развертываний увеличилась до 22 релизов в день, что свидетельствует об ускорении CI/CD процессов. MTTR сократился с 4 часов до 2,6 часов, а процент неудачных релизов снизился до 5,8 %. Эти результаты подтверждают, что устранение конфигурационных ошибок и оптимизация тестов безопасности оказывает значительное влияние на производительность [5].

Дополнительно было установлено, что использование алгоритмов машинного обучения позволило предотвратить 5 потенциальных сбоев. Эти инциденты были выявлены на основе предиктивного анализа логов, что продемонстрировало ценность интеграции аналитических подходов в DevSecOps.

Результаты эксперимента

Эксперимент показал, что систематический подход к анализу и оптимизации DevSecOps процессов позволяет не только измерить текущую эффективность, но и значительно ее улучшить. Результаты подтверждают, что использование метрик DORA, алгоритмов анализа данных и инструментов автоматизации создает мощную основу для повышения зрелости DevSecOps. Внедрение изменений позволило повысить частоту развертываний на 47 %, сократить среднее время восстановления на 35 % и уменьшить процент неудачных релизов на 27 %. Будущие исследования могут быть направлены на дальнейшую интеграцию предиктивного анализа в CI/CD конвейеры, а также на разработку новых моделей анализа, способных учитывать более сложные сценарии и данные.

Результаты тестирования показали значительное улучшение эффективности процессов DevSecOps. Частота развертываний увеличилась до 22 релизов в день за счет сокращения времени ожидания на этапах тестирования. Среднее время восстановления после инцидентов (MTTR) уменьшилось с 4 часов до 2,6 часов, что свидетельствует о лучшей управляемости системы. Процент неудачных релизов снизился с 8 % до 5,8 %, что также связано с улучшением тестирования безопасности и устранением инфраструктурных проблем.

Дополнительно были выявлены долгосрочные преимущества использования алгоритмов анализа данных. Например, 25 ранее незамеченных аномалий, связанных с настройкой тестов и серверов, были устранены, что позволило минимизировать вероятность повторных ошибок. Использование машинного обучения для предсказания сбоев оказалось особенно полезным: оно позволило предупредить 5 потенциальных проблем в реальном времени, что ранее невозможно было сделать вручную.

Заключение

Эксперимент продемонстрировал, что интеграция алгоритмов анализа данных и автоматизированных инструментов безопасности позволяет существенно повысить эффективность DevSecOps процессов. Улучшение таких показателей, как MTTR и процент успешных релизов, подтверждает, что системный подход к анализу и оптимизации может существенно сократить затраты

времени и ресурсов. Эти результаты служат доказательством того, что использование метрик и алгоритмов не только измеряет эффективность, но и открывает новые возможности для улучшения производительности DevSecOps.

Список используемых источников

1. Маккей Д. Как с помощью DevSecOps защитить облачные сервисы / Д. Маккей // Директор информационной службы, 2016. № 3. С. 46. EDN VUBNJZ.
2. Самойленко В. В., Матросова Е. В. Применение практик DevOps при работе по AGILE методологиям // Аллея науки, 2018. Т. 4. №. 10. С. 963–969.
3. Голубь И. С., Глаголев В. А. Сравнение инструмента CI/CD двух сервисов Jenkins и GiLab // Постулат, 2021. № 2.
4. Natekin A., Knoll A. Gradient boosting machines, a tutorial // Frontiers in neurorobotics. 2013. Vol. 7. PP. 21.
5. Киреев Н. А., Кильчанова А. Д. Применение метода GRADIENT BOOSTING для классификации активности человека на основе данных акселерометра // Новые информационные технологии и системы, 2023. С. 51.

Bench M., Kosov N. **TESTING THE EFFICIENCY OF DEVSECOPS PROCESSES.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Testing the effectiveness of DevSecOps processes is not just a method for checking the stability of development, but a key stage that allows you to assess the level of security integration into the software life cycle. In the context of constant growth of cybersecurity threats and the complexity of software systems, companies are faced with the need to ensure security at all stages, from design to operation.

Key words: Vulnerabilities, security incidents, privacy threats, cybersecurity.

УДК 004.75
ГРНТИ 81.93.29

ВЛИЯНИЕ ПРИМЕНЕНИЯ ФАЙЕРВОЛА NFTABLES НА ПРОИЗВОДИТЕЛЬНОСТЬ СЕТЕВЫХ ВЗАИМОДЕЙСТВИЙ В ВИРТУАЛИЗИРОВАННОЙ СРЕДЕ

Э. В. Бирих, Д. В. Сахаров, Е. А. Травкина
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье исследуется влияние файервола nftables на производительность сетевых взаимодействий в виртуализированной среде. Основное внимание уделяется зависимости задержек передачи файлов от конфигурации правил файервола. Эксперимент проведен на виртуальных машинах с использованием инструментов для анализа трафика и измерения задержек. Результаты демонстрируют, что строгие правила nftables значительно увеличивают сетевые задержки, особенно при передаче крупных файлов, что подчеркивает необходимость баланса между требованиями безопасности и пропускной способностью сети.

информационная безопасность, файерволы, nftables, сетевые задержки, виртуальные машины, анализ трафика

Информационная безопасность давно стала неотъемлемой частью сетевой инфраструктуры. Одним из методов обеспечения сетевой безопасности является использование файерволов, позволяющих контролировать и ограничивать сетевой трафик, предоставляя защиту от нежелательных подключений и потенциальных атак. Тем не менее, применение файерволов может негативно сказываться на производительности сети, особенно при передаче больших объемов данных [1].

Файерволы, или брандмауэры, являются ключевыми элементами защиты сетей, обеспечивая барьер между внутренними и внешними ресурсами сети и предотвращая несанкционированный доступ к конфиденциальным данным. Основная их задача – фильтровать трафик в соответствии с заданными правилами, пропуская безопасные пакеты и блокируя подозрительные или явно вредоносные. Для этого файерволы работают на различных уровнях сетевой модели, на сетевом и транспортном уровене, где они анализируют и управляют потоками данных, исходя из источника и назначения пакетов, портов, протоколов и других критериев.

Среди различных решений для фильтрации сетевого трафика, выделяется nftables – современный инструмент, который заменяет устаревшие iptables и другие компоненты фильтрации, исторически используемые в Linux. Nftables представляет собой универсальную систему, которая упрощает управление

правилами фильтрации благодаря использованию единой архитектуры, основанной на таблицах, цепочках и правилах. В отличие от iptables, где правила обрабатываются последовательно, nftables позволяет создавать группы правил и фильтров, что улучшает производительность и уменьшает задержку. Архитектура nftables дает возможность создавать сложные фильтры, обеспечивая высокий уровень безопасности при минимальных затратах ресурсов процессорного времени (CPU) и оперативной памяти.

Важный аспект, который стоит учитывать при работе с файерволами, – это сетевые задержки, которые могут возникать из-за обработки трафика на каждом уровне фильтрации. Основные источники задержек связаны с проверкой пакетов и управлением соединениями. Например, stateful файерволы, такие как nftables, отслеживают состояние каждого соединения, что дает возможность пропускать только пакеты, соответствующие уже установленным сессиям. Это, однако, добавляет дополнительную нагрузку на систему, так как файервол должен постоянно обновлять таблицу активных соединений. Кроме того, количество и сложность правил также напрямую влияют на задержку: чем больше фильтров и условий используется, тем больше времени требуется на их проверку. Поэтому файерволы, в особенности в условиях интенсивного сетевого трафика, могут создавать дополнительные задержки, которые накапливаются и становятся значимыми для производительности сети.

Для проведения исследования была развернута инфраструктура на основе двух виртуальных машин, работающих под управлением операционной системы Ubuntu. Обе виртуальные машины были запущены на гипервизоре VMware ESXi. В таблице 1 представлена конфигурация виртуальных машин и используемое программное обеспечение в рамках исследования.

ТАБЛИЦА1. Программное обеспечение и инструменты

Параметр конфигурации	Описание
Гостевая ОС	Ubuntu Linux (64-bit), версия 22.04 LTS
Совместимость	VMware ESXi 6.7 и выше, VM version 14
Ресурсы виртуальных машин	
CPU	2 виртуальных процессора
Память	4 GB (активно используется 3 GB)
Жесткий диск	30 GB
Программное обеспечение и инструменты	Описание
Wireshark 3.6.2	Использовался для анализа сетевого трафика между виртуальными машинами
Nftables 0.9.8	Использовался для создания и управления правилами файервола на виртуальных машинах

Эксперимент проводился на двух виртуальных машинах, развернутых в одной локальной сети. Для проверки сетевой доступности между ними была успешно выполнена проверка доступности узлов в сети.

Передача файлов осуществлялась с помощью утилиты Netcat по протоколу TCP через ip и порт назначения. Transmission Control Protocol (TCP) – это ориентированный на соединение сквозной протокол на транспортном уровне модели OSI, разработанный для обеспечения связи между парами процессов на отдельных, но взаимосвязанных хостах в сети [2]. Описанная отправка файлов обеспечила прямую передачу данных между виртуальными машинами, что позволило детализировать измерения задержек без дополнительных усложнений, связанных с использованием других протоколов.

Для анализа трафика и измерения сетевых задержек использовалась утилита Wireshark. Трафик фильтровался по критерию: tcp port, что позволило сосредоточиться только на анализе передаваемых данных через заданный порт. С помощью Wireshark измерялись время передачи каждого файла с установлением сессии между виртуальными машинами.

Эксперимент проводился в двух различных сценариях. Первый этап: вычисление производительности передачи файлов между виртуальными машинами без каких-либо ограничений со стороны файервола. Второй этап: вычисление производительности сети с детализированной конфигурацией правил nftables, включающая строгие ограничения (ограничение размеров файлов, отслеживание соединений, логирование трафика и др.).

Таблица 2 демонстрирует результаты передачи файлов при различных настройках сети. В таблице указано среднее и суммарное время передачи файлов, что позволяет наглядно увидеть закономерность в зависимости от размера передаваемого пакета и присутствия файервола.

ТАБЛИЦА 2. Результаты анализа трафика через Wireshark

		Без nftables для 50 файлов	Без nftables для 1 файла	С nftables для 50 файлов	С nftables для 1 файла
Тип файла	Размер файла	Суммарное время передачи файлов	Среднее время передачи файла	Суммарное время передачи файлов	Среднее время передачи файла
.txt	10Kb	0,178516353	0,003570327	0,199803004	0,00399606
	100Kb	0,249622763	0,004992455	0,289273903	0,005785478
	1Mb	0,672076184	0,013441524	0,938939894	0,018778798
	10Mb	4,964029593	0,099280592	7,978279203	0,159565584
.jpg	100Kb	0,236086679	0,004721734	0,291949304	0,005838986
	1Mb	0,722575148	0,014451503	0,90398349	0,01807967
	5Mb	2,415960799	0,048319216	3,174890288	0,063497806

		Без nftables для 50 файлов	Без nftables для 1 файла	С nftables для 50 файлов	С nftables для 1 файла
	10Mb	4,737008169	0,094740163	7,83489392	0,156697878
.zip	1Mb	0,663721914	0,013274438	0,983784893	0,019675698
	10Mb	4,955887085	0,099117742	8,240239943	0,164804799
	50Mb	26,20664172	0,524132834	37,02893803	0,740578761
	100Mb	56,77623212	1,135524642	103,3949032	2,067898064
.mp3	1Mb	0,69671077	0,013934215	0,927483932	0,018549679
	5Mb	2,487209797	0,049744196	3,194800954	0,063896019
	10Mb	4,963586887	0,099271738	8,193983902	0,163879678
	50Mb	26,04782965	0,520956593	39,38499029	0,787699806
.mp4	1Mb	0,673989393	0,013479788	1,003849954	0,020076999
	10Mb	4,851452557	0,097029051	8,354939284	0,167098786
	50Mb	26,19834929	0,523966986	38,32949009	0,766589802
	100Mb	56,78902749	1,13578055	106,3489928	2,126979856

Расчет среднего времени передачи для каждого типа файла производился по формуле:

$$\bar{T} = \frac{\sum_{i=1}^{N} T_i}{N},$$

где T_i – время передачи i-го файла, сек.; N – количество передач.

Таблица 3 обобщает средние значения времени передачи одного файла каждого размера. Это сравнение демонстрирует разницу в задержке при активации и деактивации файервола.

ТАБЛИЦА 3. Соотношение размерности файлов с задержкой трафика

Размер	Без nftables для 1 в среднем	С nftables для 1 в среднем	Задержки в сек
10Kb	0,003570327	0,00399606	0,000425733
100Kb	0,004857094	0,005812232	0,000955138
1Mb	0,013716294	0,019032169	0,005315875
5Mb	0,049031706	0,063696912	0,014665206
10Mb	0,097887857	0,162409345	0,064521488
50Mb	0,523018804	0,764956123	0,241937318
100Mb	1,135652596	2,09743896	0,961786364

Анализ таблицы 3 показывает, что рост задержки сети зависит от увеличения размера файла и применения правил файервола. В среднем, задержка

увеличивается линейно с увеличением размера файла, однако с включенным файерволом задержки возрастали значительно больше по мере увеличения объема данных, чем без него.

В рамках проведенного исследования было наглядно продемонстрировано, что файервол, обеспечивая защиту сети, в то же время снижает скорость передачи данных. Задержки при передаче файлов значительно возрастают при активном файерволе, и среднее время передачи данных увеличивается из-за дополнительной обработки пакетов на транспортном и сетевом уровне модели OSI.

Результаты эксперимента подтвердили, что размер файла оказывает большее влияние на задержку, чем его тип, и увеличение времени передачи имеет почти линейную зависимость от размера файла, что указывает на ограниченность пропускной способности в условиях строгой фильтрации трафика. Строгая конфигурация nftables обеспечивает высокий уровень безопасности, но снижает пропускную способность, особенно при передаче больших объемов данных. Это подтверждает необходимость балансирования между требованиями безопасности и потребностью в минимальных задержках для поддержания высокого качества обслуживания.

Поскольку результаты исследования подтвердили, что реализация политики безопасности через файерволы, такие как nftables, может привести к незначительным задержкам трафика. Тем не менее, способность файерволов защищать сетевую инфраструктуру от несанкционированного доступа и различных угроз делает применение файерволов обоснованным и необходимым.

Список используемых источников

1. Бирих Э. В., Рябов Е. Ю., Сахаров Д. В. Методология формирования модели угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. С. 103–107.
2. Красов А. В., Гельфанд А. М., Коржик В. И., Котенко И. В., Петрив Р. Б., Сахаров Д. В., Ушаков И. А., Шариков П. И., Юркин Д. В. Построение доверенной вычислительной среды. М.: Индивидуальный предприниматель Петрив Роман Богданович, 2019. 78 с.

Birikh E., Saharov D., Travkina E. **IMPACT OF APPLYING THE NFTABLES FIREWALL ON THE PERFORMANCE OF NETWORK INTERACTIONS IN A VIRTUALIZED ENVIRONMENT.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article explores the impact of the nftables firewall on the performance of network interactions in a virtualized environment. It focuses on the relationship between file transfer delays and firewall rule configurations. The experiment was conducted on virtual machines using tools for traffic analysis and delay measurement. The results show that strict nftables rules significantly increase network delays, particularly for large file transfers, emphasizing the need to balance security requirements with network throughput.

Key words: Information security, firewalls, nftables, network delays, virtual machines, traffic analysis.

УДК 004.738
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ЗОНЫ ПОКРЫТИЯ WLAN ДЛЯ ПОВЫШЕНИЯ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ

К. М. Боднарчук, Я. А. Ильин, М. М. Ковцур
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В последние годы актуальность вопроса кибербезопасности значительно возросла, особенно в условиях постоянного роста числа подключенных устройств и использования беспроводных сетей. Уязвимости Wi-Fi-сетей могут стать причиной утечек данных, несанкционированного доступа и других инцидентов безопасности. Site Survey является необходимым процессом для улучшения покрытия и минимизации зон некачественного сигнала, что может оказать влияние на безопасность сети, так как оптимизация размещения точек доступа и мощность сигнала способствуют защите от внешних угроз. Настоящая статья посвящена исследованию того, как Site Survey помогает усилить киберзащиту сети, предотвращая потенциальные риски и поддерживая безопасную зону покрытия.

Wi-Fi Site Survey, кибербезопасность, оптимизация покрытия, безопасность сети, защита данных, корпоративные сети

Создание оптимального покрытия Wi-Fi (Site Survey) играет важную роль при защите сети от внешних угроз. Неправильное размещение точек доступа (AP) или недостаточно сильный сигнал может создать зоны, доступные для злоумышленников снаружи здания или из других помещений, не предназначенных для использования сети [1]. Эти уязвимости могут подвергнуть сеть риску несанкционированного доступа и прослушивания.

Рассмотрим два варианта покрытия Wi-Fi в здании (рис. 1, 2)

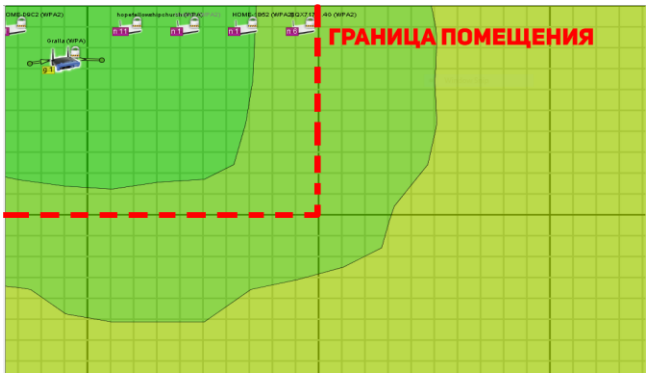


Рис. 1. Зона покрытия

В первом варианте (рис. 1) очерчена граница помещения, внутри которой необходимо спроектировать качественное и надежное покрытие Wi-Fi сети. В

большей части инструментария для проведения Wi-Fi Site Survey качество покрытия измеряется градацией от зеленого цвета до желтого/красного. Во втором случае рассматривается проникновение сигнала Wi-Fi за границы рабочего пространства. В такой ситуации злоумышленник может попытаться получить доступ к сети находясь вне помещения, но в зоне действия сигнала корпоративной сети (рис. 2):

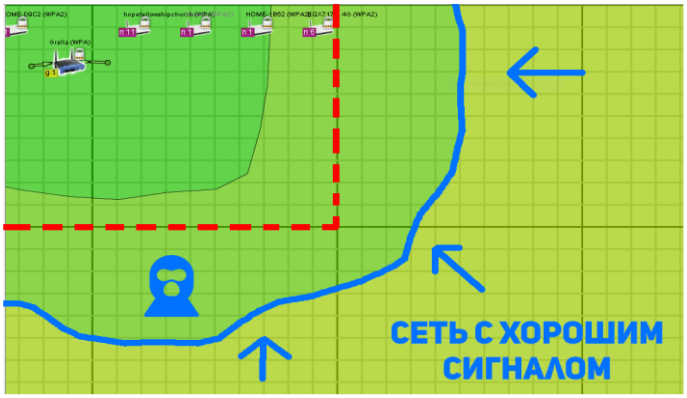


Рис. 2. Зона покрытия, выходящая за пределы территории

Такой вид покрытия может облегчить злоумышленнику возможность получения несанкционированного доступа в корпоративную сеть. Для предотвращения проникновения в сеть злоумышленника, необходимо расположить точки доступа так, чтобы зона покрытия как можно меньше выходила за необходимые границы (рис. 3):

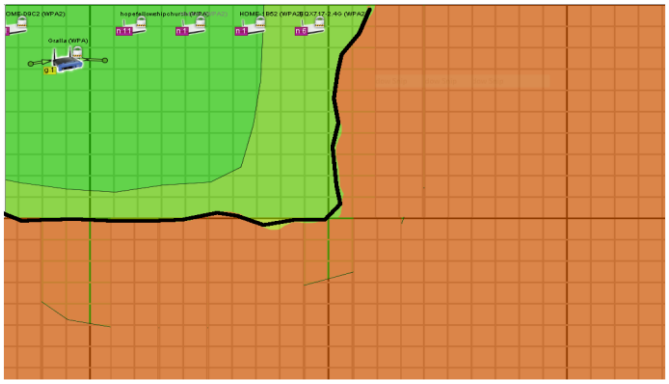


Рис. 3. Наиболее безопасная зона покрытия

Обратная ситуация возникает при недостаточном (слабом) покрытии, когда появляются зоны слабого сигнала или так называемые «мертвые зоны». Они могут привести к следующим угрозам:

– перехват данных в местах с плохим покрытием: в слабых зонах злоумышленники могут перехватить данные, так как устройства могут переходить на менее защищенные сети;

– атаки с поддельными точками доступа (rogue APs): если сигнал доступен в общественных местах, злоумышленники могут установить поддельные

точки доступа, перехватывая данные от пользователей, думающих, что они подключены к безопасной сети.

Рассмотрим детальнее, как при недостаточном покрытии возникает потенциальная угроза безопасности (рис. 4):

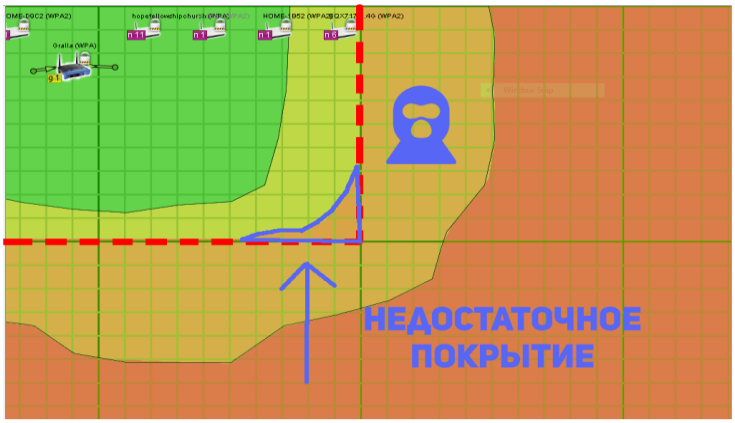


Рис. 4. Пример недостаточного покрытия

Находясь в зоне слабого сигнала, злоумышленник может создать доверенную Wi-Fi точку доступа, которая имеет такое же название, как и легитимная точка доступа в корпоративной сети. В результате этого, клиентское устройство автоматически подсоединяется к этой точке доступа и работает через нее, а злоумышленник получает возможность перехватывать трафик или атаковать устройство, находящееся в одном сегменте сети. Таким образом, задача злоумышленника состоит в том, чтобы «поднять» клон сети, к которой у потенциальной жертвы может быть сконфигурирован доступ (как с защитой, так и без). Также, при наличии рядом легитимной точки доступа, злоумышленник может попытаться ее «погасить», чтобы перенаправить клиентов на свою точку доступа.

Правильное проведение Site Survey позволяет значительно усилить киберзащиту корпоративной Wi-Fi сети, минимизируя риски несанкционированного доступа и утечек данных [2]. Основные преимущества проведения Site Survey для кибербезопасности включают следующие аспекты [3]:

1. Контроль зоны покрытия – позволяет ограничить зону распространения сигнала, предотвращая его утечку за пределы охраняемой территории и снижая риск несанкционированного подключения;

2. Оптимизация каналов и частот – уменьшает интерференцию, улучшает качество связи и снижает риски, связанные с уязвимостью перегруженных каналов;

3. Обнаружение несанкционированных точек доступа и устройств – помогает своевременно выявлять и устранять угрозы от поддельных точек доступа и неавторизованных устройств;

4. Адаптация зоны покрытия для чувствительных зон – позволяет снизить уровень сигнала в конфиденциальных зонах, минимизируя риски несанкционированного доступа;

5. Учет внешних сетей – позволяет настроить собственную сеть с учетом видимых внешних сетей, предотвращая пересечения и снижая уязвимости;

6. Постоянный мониторинг и адаптация – поддерживает актуальную конфигурацию сети, адаптируясь к изменению условий и снижая потенциальные риски безопасности.

Эти преимущества делают Site Survey важным инструментом для обеспечения киберзащиты Wi-Fi сети, позволяя заранее идентифицировать и устранять потенциальные угрозы.

Современные решения и технологии, применяемые для защиты корпоративных Wi-Fi сетей, включают разнообразные инструменты для мониторинга, предотвращения вторжений и контроля зоны покрытия сети. Вот ключевые подходы и технологии, которые помогают реализовать безопасное и эффективное управление беспроводной инфраструктурой.

1. Системы предотвращения беспроводных вторжений (Wireless Intrusion Prevention Systems, wIPS).

wIPS – это специализированные системы, предназначенные для мониторинга радиочастотного спектра и обнаружения несанкционированных устройств в пределах охраняемой территории [4]. Они работают в реальном времени и позволяют:

– обнаруживать поддельные точки доступа (rogue APs), которые злоумышленники могут установить для перехвата трафика;

– автоматически блокировать попытки подключения неавторизованных устройств;

– проводить сканирование зоны покрытия, обнаруживая утечки сигнала и слабые зоны, где возможен несанкционированный доступ.

2. Программные инструменты для радиообследования.

Эти специализированные программы, такие как Ekahau Site Survey, AirMagnet, или NetSpot, они помогают оптимизировать размещение точек доступа и корректировать уровень мощности сигнала для минимизации зон, где сигнал выходит за границы контролируемой территории. Site Survey Software предлагает:

– создание тепловых карт покрытия, чтобы наглядно оценить зоны слабого или избыточного сигнала;

– возможность настройки мощности сигнала каждой точки доступа для сокращения зон «утечки» за пределы охраняемой территории;

– учет видимых внешних сетей, что помогает своевременно обнаруживать и корректировать конфигурацию сети для защиты от потенциальных угроз.

Эти решения в совокупности позволяют значительно повысить защищенность корпоративной Wi-Fi сети, минимизируя риски, связанные с несанкционированным доступом и утечкой данных.

Оптимизация зоны покрытия сети Wi-Fi важна для обеспечения безопасности защищенных сетей такого рода. Site Survey позволяет точно оценить покрытие, чтобы исключить утечку сигнала за пределы сети и минимизировать риск несанкционированного доступа. Важно также проверять посторонние беспроводные сети в радиусе корпоративной WLAN для своевременного выявления угроз. Комплексная защита достигается с помощью систем wIPS или специализированного радиообследования, что повышает устойчивость сети к внешним угрозам и поддерживает высокий уровень безопасности.

Список используемых источников

1. Радиообследование (Site Survey) зоны покрытия сети Wi-Fi. URL: https://habr.com/ru/articles/138637/ (дата обращения 08.11.24)
2. Ковцур М. М., Винников С. А., Трезоров В. И., Киструга А. Ю. Исследование влияния атак на беспроводные сети Wi-Fi 6E // Экономика и качество систем связи, 2023. № 2 (28). С. 87–92.
3. Understand Site Survey Guidelines for WLAN Deployment. URL: https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html (дата обращения 08.11.2024).
4. Ковцур М. М., Миняев А. А., Цыганов В. А. Исследование актуального инструментария Kali Linux для проведения тестов на оценку безопасности беспроводных сетей // Экономика и качество систем связи, 2023. № 2 (28). С. 93–99

Bodnarchuk K., Ilyin Y., Kovtsur M. **INVESTIGATION OF THE WLAN COVERAGE AREA TO INCREASE THE LEVEL OF INFORMATION SECURITY OF THE CORPORATE NETWORK.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In recent years, the relevance of the issue of cybersecurity has increased significantly, especially in the context of a constant increase in the number of connected devices and the use of wireless networks. Vulnerabilities in Wi-Fi networks can cause data leaks, unauthorized access, and other security incidents. Site Survey is a necessary process to improve coverage and minimize low-quality signal areas, which can have an impact on network security, since optimizing the location of access points and signal strength contribute to protection from external threats. This article is devoted to the study of how Site Survey helps to strengthen the cyber defense of the network, preventing potential risks and maintaining a secure coverage area.

Key words: Wi-Fi Site Survey, cybersecurity, coverage optimization, network security, data protection, corporate networks.

УДК 004.056.53
ГРНТИ 49.33.29

РОЛЬ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И USB-УСТРОЙСТВ В МОДЕЛИРОВАНИИ СЕТЕВЫХ АТАК

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

В статье рассматривается проблема социальной инженерии как значимой угрозы современной информационной безопасности. Особое внимание уделяется анализу человеческого фактора в контексте успешных кибератак и методам психологической манипуляции, используемым злоумышленниками. На основе актуальных исследований и практических примеров демонстрируется эффективность социально-инженерных атак, в частности, метода «road apple». Представлен анализ технических аспектов использования USB-устройств в кибератаках и рассмотрены схемы внедрения вредоносного программного обеспечения. Предложены стратегии защиты, включающие комплексный подход к обучению персонала и разработке политик безопасности. Результаты исследования подчеркивают необходимость интеграции образовательных инициатив и технических мер защиты для создания эффективной системы противодействия социально-инженерным атакам.

социальная инженерия, информационная безопасность, кибератаки, человеческий фактор, USB-устройства, обучение персонала, политики безопасности

Введение

В условиях быстрой цифровизации, которая охватывает все аспекты человеческой деятельности, проблема информационной безопасности приобретает особую остроту. Социальная инженерия, которая включает в себя набор психологических тактик, демонстрирует, что злоумышленники используют психологические стратегии. Следовательно, крайне важно изучить методы социальной инженерии и разработать тактику для повышения осведомленности пользователей о потенциальных рисках.

Социальная инженерия в сетевых атаках

Методы социальной инженерии для манипуляции пользователями

Социальная инженерия – мощный инструмент для злоумышленников, стремящихся прорваться через технические средства защиты посредством психологических манипуляций. Значение этого метода зависит от его акцента на человеческом элементе. Несмотря на то, что «социальная инженерия в строгом смысле может быть представлена в виде специальной социальной инже-

нерии, которая, если рассматривать ее в контексте информационной безопасности, относится к психологической манипуляции людьми для сбора информации, мошенничества или получения доступа к системе» [1], злоумышленники продолжают придумывать и использовать эти хитрые уловки. Это подчеркивает значение социальной инженерии не только как метода эффективной реализации схем, но и как препятствия для современной кибербезопасности.

Практическим примером использования социальной инженерии является атака «road apple», где злоумышленники намеренно оставляют зараженные USB-устройства на видных местах в надежде, что жертвы подключат их к своим компьютерам. Эта процедура изображена на схеме, на которой показано, как злоумышленники используют USB-устройства для проникновения к компьютерным системам. Наглядно, процесс получения физического доступа к компьютерной системе с помощью USB-устройства представлен на рис. 1.

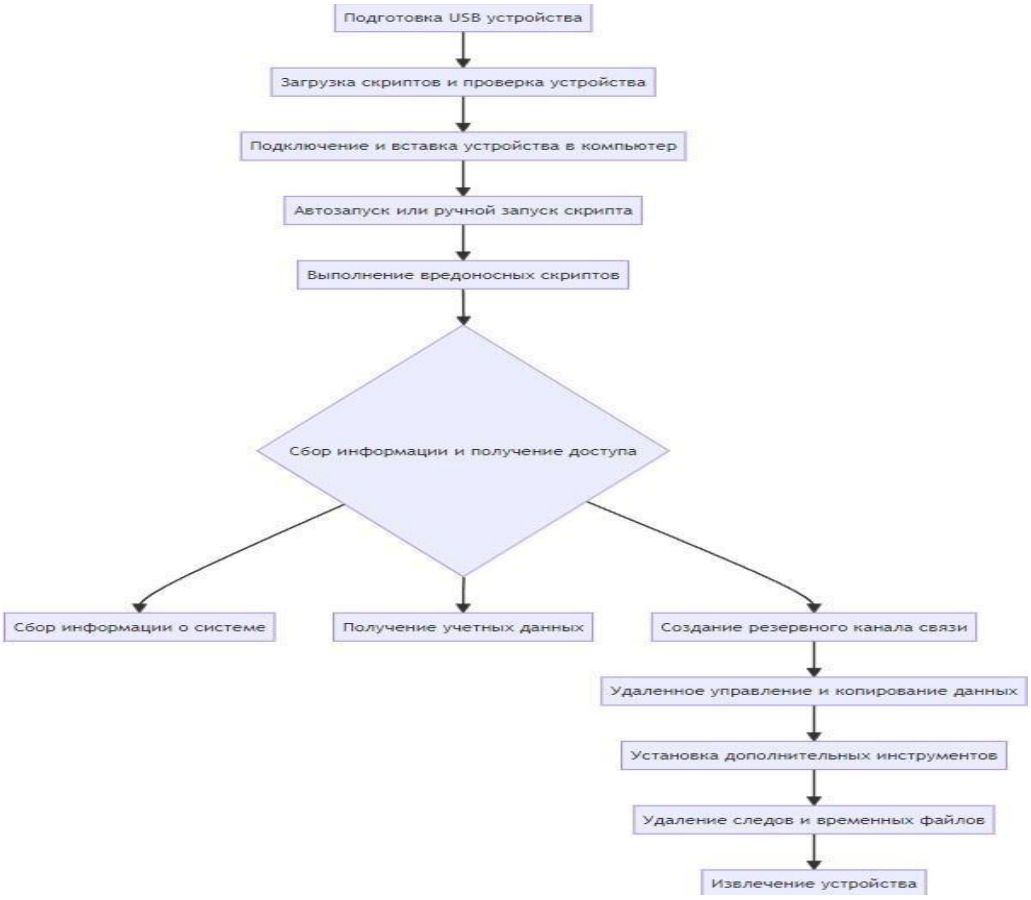


Рис. 1. Процесс получения физического доступа к компьютерной системе с помощью USB- устройства

В этих случаях злоумышленники наносят логотип компании на физический носитель, «оставляют его в местах, часто посещаемых сотрудниками, и ждут, пока жертва его найдет» [2]. Это пример того, как социальная инженерия объединяет психологические аспекты и инфраструктурную восприимчивость, чтобы убедить людей принять участие в мероприятиях, которые на пер-

вый взгляд кажутся безобидными. Подобные маневры подчеркивают необходимость четкого информирования о потенциальных опасностях и реализации обучающих инициатив внутри компаний.

Несмотря на развитие мер безопасности, человеческий фактор остается одной из главных уязвимостей современных систем. Даже если технические меры становятся все более эффективными, «хотя эффективность мер безопасности для защиты конфиденциальной информации со временем увеличивается, люди по-прежнему остаются восприимчивыми к манипуляциям, и человеческий фактор остается значительным» [3]. Это усиливает необходимость интеграции учебных инициатив и обучения сотрудников, чтобы повысить осведомленность о новых атаках и техниках социальной инженерии. Следовательно, снижение воздействия человеческого фактора становится ключевой целью для защиты данных и предотвращения различных нарушений.

Использование USB-устройств при моделировании атак

Технические аспекты физического подключения USB-устройств

Портативные запоминающие устройства, хотя и широко распространены в современную эпоху, представляют собой существенную угрозу безопасности из-за возможности незаконного распространения вредоносного программного обеспечения. Это объясняется тем, что злоумышленники могут использовать методы социальной инженерии, чтобы обманом заставить пользователей подключить взломанные устройства. Такие маневры основаны на уязвимости человеческого фактора, который остается критически важным, несмотря на совершенствование технических методов защиты. Как подчеркивают исследователи, «вирусы – это программы, способные изменить содержание файлов, привести компьютер к засорению и выполнению негативных действий. Существует множество способов распространения компьютерного вируса... или использовать зараженные съемные устройства хранения данных» [4]. Это подчеркивает необходимость технического понимания и осознания возможных опасностей, связанных с USB-устройствами.

Такое обучение должно охватывать как технические навыки, так и знания. Тщательное понимание слабых мест человека и их значения для эффективных кибервторжений помогает точно определить возможные опасности и разработать стратегии защиты. Установление и внедрение строгих протоколов безопасности и контрольных показателей во всей организации, примером которых является ISO-IEC 27001-2013, облегчит организацию структур управления данными. Это позволит минимизировать риски и повысить эффективность

защитных механизмов, обеспечивая таким образом надежную защиту от возможных атак.

Защита от социальной инженерии и атак на USB-устройства

Обучение сотрудников как профилактическая мера

Для предотвращения атак, связанных с социальной инженерией и USB-устройствами, критически важно обучение сотрудников. Сотрудники должны признать, что защита предприятия в значительной степени зависит от их способности выявлять потенциальные риски и правильно управлять конфиденциальными данными. Работники иногда допускают ошибки и упускают из виду безопасность, потому что не придают ей значения, поэтому необходимо научить их быть внимательными и осторожными с важной личной информацией [4]. Обучение должно охватывать текущие и распространенные способы атак и учить тому, как защититься от уловок, которые вынуждают людей выдать личную информацию.

Сотрудничество между техническими специалистами и персоналом из различных секторов может значительно повысить эффективность инициативы по развитию навыков. Крайне важно структурировать интерактивные занятия, которые концентрируются не только на концептуальных элементах информационной безопасности, но и на реальных примерах предотвращения социальных атак. Решение таких проблем должно быть частью деловой этики, что поможет снизить вероятность успешных атак. При разработке плана безопасности компания должна обратить внимание на выявленные в ходе проверки проблемы и угрозы. Важно, чтобы реализация плана способствовала снижению вероятности и количеству неожиданных рисков [5]. Это значит, что нужно придумать, как могут развиваться различные ситуации, которые могут пойти не так, и разработать план действий для того, чтобы все прошло безопасно.

Разработка и реализация стратегий безопасности

Важнейший аспект работы над безопасностью является упор на активном взаимодействии с угрозами. «Безопасность часто подвергается риску из-за ошибок или небрежности пользователей, поэтому крайне важно разработать и внедрить программы обучения, которые подчеркнут значимость внимательного обращения с конфиденциальной информацией» [6]. Эти программы обучают персонал правильным процедурам реагирования на угрозы посредством практического опыта и моделирования такого рода ситуаций.

Подводя итог, можно сказать, что создание хорошей системы безопасности означает размышление о рисках, которые быстро меняются в мире цифро-

вых технологий [7]. Регулярная проверка и пересмотр правил компании выявляет слабые места и улучшает план безопасности. Обучение сотрудников имеет решающее значение наряду с надлежащими мерами безопасности и полезными инструментами. Эти компоненты создают комплексную многоуровневую стратегию безопасности для смягчения любых возможных угроз. Однако злоумышленники продолжают эксплуатировать человеческие слабости, подчеркивая важность понимания и защиты от социальной инженерии.

Список используемых источников

1. Соловьев А. В. Методы и приемы манипулирования сознанием пользователя в пространстве сети // Постулат, 2022. № 12. (дата обращения 23.09.2024).
2. Стожко К. П., Стожко Д. К., Шиловцев А. В., Некрасов С. Н., Макарова Т. Н. Роль социальной инженерии в современном российском обществе // BIO Web of Conferences, 2022. Том 51. Статья 06008. (дата обращения 23.09.2024).
3. Лазарев А. С., Чернов С. Е., Струкачева Е. Е. Модель угроз и методы защиты для обеспечения безопасности созданного файлохранилища / Лазарев А. С., Чернов С. Е., Струкачева Е. Е.; под руководством Кукуева Е. А. Тюмень: Тюменский государственный университет, 2023. (дата обращения 23.09.2024).
4. Афанасьева С. В., Черепанова Е. С., Шехова Н. В. Инновационные методы предотвращения киберугроз в целях обеспечения экономической безопасности организации // Вестник Самарского университета. Экономика и управление, 2023. Т. 14, № 2. С. 7–16. (дата обращения 23.09.2024).
5. Багров А. П., Багрова В. А. Анализ международного стандарта ISO-IEC 27001-2013 // [б. и.]. – [б. г.]. – [б. и.]. (дата обращения 23.09.2024).
6. Рыжова Н. И., Громова О. Н. Киберугрозы цифрового социума и их профилактика в рамках виктимологической деятельности // Вестник РУДН. Серия: Информатизация образования, 2020. Т. 17, № 3. С. 254–268. (дата обращения 23.09.2024).
7. Петрив Р. Б. Атаки на ОС Windows с помощью внедрения кода в легитимное по и методы их обнаружения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. 2024. С. 813–819. (дата обращения 23.09.2024).

Borisenko I. **THE ROLE OF SOCIAL ENGINEERING AND USB DEVICES IN MODELING NETWORK ATTACKS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article examines the problem of social engineering as a significant threat to modern information security. Special attention is paid to analyzing the human factor in the context of successful cyberattacks and psychological manipulation methods used by attackers. Based on current research and practical examples, the effectiveness of social engineering attacks, particularly the “road apple” method, is demonstrated. The analysis of technical aspects of using USB devices in cyberattacks and schemes for implementing malicious software is presented. Protection strategies are proposed, including a comprehensive approach to personnel training and security policy development. The research results emphasize the need to integrate educational initiatives and technical protection measures to create an effective system for countering social engineering attacks.

Key words: social engineering, information security, cyberattacks, human factor, USB devices, personnel training, security policies.

УДК 004.056.53
ГРНТИ 49.33.29

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: АНАЛИЗ МЕТОДОВ И СПОСОБОВ ЗАЩИТЫ

И. И. Борисенко, И. А. Серегин
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются современные методы социальной инженерии, с особым акцентом на фишинг и его разновидности. Представлены эффективные стратегии защиты от социально-инженерных атак. Особое внимание уделяется комплексному подходу к обеспечению информационной безопасности, включающему технические меры и образовательные стратегии. Исследование основывается на анализе современных практик социальной инженерии и методов противодействия им.

социальная инженерия, фишинг, информационная безопасность, кибербезопасность, манипуляция, многофакторная аутентификация, защита данных

Введение

С ростом распространения методов социальной инженерии фишинг становится одной из наиболее актуальных угроз для информационной безопасности. Эти мошеннические методы опираются на техники, которые нацелены на манипуляцию человеческим сознанием с целью получения конфиденциальной информации. Знание механизмов таких атак является ключевым фактором для их предотвращения и защиты личных данных.

Методы социальной инженерии

Фишинг и его разновидности

Фишинг является одним из самых распространенных методов социальной инженерии, который широко используют злоумышленники для кражи конфиденциальной информации у пользователей. Этот метод использует рассылку мошеннических сообщений, которые кажутся заслуживающими доверия, и являются инструментом обслуживания злоумышленников. Различные формы фишинга включают вишинг, претекстинг и другие техники, которые активно применяются для манипуляции жертвами. Претекстинг, включает в себя выдачу за другое лицо, что влечет за собой использование заранее подготовленного повествования, позволяющего мошенникам обмануть жертву, имитируя подлинное взаимодействие. «Сущность претекстинга заключается в

использовании заранее подготовленного коммуникативного сценария, который позволяет злоумышленникам манипулировать жертвой» [1]. Это делает такие атаки особенно эффективными, поскольку жертвы часто не обращают внимания на их манипуляции.

В социальных сетях мимикрия и манипуляции представляют серьезную угрозу, поскольку именно здесь пользователи наиболее склонны взаимодействовать и раскрывать личные подробности. Приемы социальной инженерии, такие как «дорожное яблоко» и «услуга за услугу», также находят применение в этих платформах. «Приемами социальной инженерии являются: фишинг (вишинг), претекстинг, „дорожное яблоко“, „услуга за услугу“, „Троянский конь“» [1]. Эти методы позволяют злоумышленникам эффективно реализовывать свои атаки, часто без ведома жертвы.

Обучение сотрудников распознаванию признаков социальной инженерии и внедрение превентивных мер помогают минимизировать риски. Использование инструментов OSINT, которые позволяют организациям извлекать информацию из открытых источников, также способствует выявлению и нейтрализации потенциальных угроз на ранней стадии. Таким образом, комплексный подход, сочетающий в себе технические, организационные и образовательные меры, является наиболее эффективным способом противодействия атакам социальной инженерии.

Мимикрия и манипуляции в социальных сетях

Анализ методов защиты и атак

Развитие средств защиты от социальной инженерии требует применения комплексных мер, способных противостоять растущим угрозам. Вместе с техническими решениями особое внимание следует уделять образовательным программам, которые развивают у пользователей навыки распознавания угроз и приемов манипуляции.

В ответ на ряд рисков, связанных со схемами социальной инженерии, было создано множество защитных стратегий, позволяющих уменьшить их воздействие и предотвратить неблагоприятные последствия. В таблице 1 приведены основные типы атак социальной инженерии, где указаны легкость выполнения, обоснование легкости выполнения, целевая аудитория, потенциальные последствия и методы защиты.

ТАБЛИЦА 1. Основные типы атак социальной инженерии: легкость выполнения, целевая аудитория, последствия и методы защиты

Тип атаки	Легкости выполнения	Целевая аудитория воздействия	Потенциальные последствия	Методы защиты
Фишинг	Относительно простые в реализации, не требуют значительных технических навыков. Основаны на манипуляции человеческим фактором	Конечные пользователи	Утечка конфиденциальных данных, финансовые потери	Повышение осведомленности пользователей, многофакторная аутентификация
Вишинг	Более сложны, чем фишинг, так как требуют личного взаимодействия с жертвой по телефону. Необходимы навыки убеждения и социального манипулирования	Сотрудники call-центров	Компрометация корпоративных учетных записей	Обучение персонала, ограничение доступа
Претекстинг	Требуют тщательной подготовки и проработки сценария взаимодействия, но в целом относительно просты в исполнении за счет создания правдоподобного предлога	Ключевой персонал	Получение доступа к критически важным системам	Регулярное обновление ПО, строгий контроль доступа
"Дорожное яблоко"	Более технически сложные, так как требуют внедрения вредоносного ПО, но при этом используют социальную инженерию для распространения	Технические специалисты	Внедрение вредоносного ПО, нарушение работы сети	Антивирусная защита, управление доступом к сетевым ресурсам
"Услуга за услугу"	Требуют определенного мастерства в социальном манипулировании и выстраивании взаимовыгодных отношений с жертвой	Доверенные лица	Манипулирование информацией, нанесение репутационного ущерба	Политики информационной безопасности, мониторинг активности
"Троянский конь"	Относительно простые в реализации, так как достаточно замаскировать вредоносное ПО под легитимное приложение. Легкость распространения среди широкой аудитории	Широкая аудитория	Несанкционированный доступ, кража данных, удаленное управление	Регулярное резервное копирование, ограничение установки ПО

Умение пользователей идентифицировать ранние признаки манипуляции способствуют значительному снижению рисков, связанных с социальной инженерией.

Стадии атак социальной инженерии.

Тактика манипулирования важна для социальной инженерии, поскольку она позволяет злоумышленникам менять мнение жертвы через подачу информации, меняющей восприятие [2]. Этот метод напоминает программирование, где четкие инструкции и эмоциональные сигналы создают ощущение безопас-

ности, скрывая истинные намерения агрессоров. Каждый аспект восприятия, от визуального до вербального, подвержен манипулятивной тактике.

Коммуникация также оказывает большое влияние на раскачивание, укрепление доверия и сокрытие намерений злоумышленников. Тщательно продуманные каналы передачи информации вселяют в жертв повышенную осведомленность, позволяя им принимать меры без сознательного признания опасности [3].

Успех манипуляции зависит от социальных элементов, например, культурных стандартов и коллективного поведения, которые делают атаки более эффективными. Для защиты решающее значение имеют не только молчаливые, но и интеллектуальные препятствия, способные противостоять подрывной деятельности на всех уровнях.

Способы защиты от социальной инженерии

Технические меры противодействия

Регулярное обновление программного обеспечения также играет важную роль в защите от атак. Современные угрозы часто используют уязвимости в устаревших версиях программ, поэтому своевременные обновления помогают устранить потенциальные риски, интегрируя актуальные патчи безопасности. Управление доступом и резервное копирование данных также важны для обеспечения безопасности информации [4]. Поддержание программного обеспечения в актуальном состоянии существенно снижает вероятность успешных атак. Кроме технических мер, необходимо учитывать организационные аспекты.

Организационные меры, такие как обучение сотрудников правилам безопасности и распознаванию признаков социальной инженерии, в сочетании с техническими, формируют комплексный подход к защите данных и систем в современном цифровом мире.

Организационные и образовательные стратегии

Внедрение многофакторной аутентификации является одним из наиболее эффективных методов, позволяющим предотвратить несанкционированный доступ к данным. "Одним из ключевых методов защиты от атак социальной инженерии является внедрение многофакторной аутентификации, что позволяет дополнительно обеспечить безопасность доступа к системам и данным" [5]. Многофакторная аутентификация усложняет задачи злоумышленников, вынуждающих их преодолевать дополнительные барьеры, значительно снижая вероятность успешной атаки. Это особенно важно в условиях, когда фи-

шинг и другие методы социальной инженерии становятся все более изощренными и нацеленными на обход традиционных защитных механизмов.

Список используемых источников

1. Баранцев С. П., Медяник О. В., Низовских Н. А., Николаева О. А. Психологические аспекты противодействия телефонному мошенничеству в финансовой сфере: методические материалы / С. П. Баранцев, О. В. Медяник, Н. А. Низовских, О. А. Николаева. Киров: Управление Министерства внутренних дел Российской Федерации по Кировской области, 2024. (дата обращения 30.09.2024).
2. Саенко В. Н. Манипуляция сознанием в современных общественных практиках // Телескоп: журнал социологических и маркетинговых исследований, 2021. № 2. С. 124. DOI: 10.51692/1994-3776_2021_2_124. (дата обращения 30.09.2024).
3. Родивилин И. П. Социальная инженерия как угроза информационной безопасности: тенденции и защита // Иркутский национальный исследовательский технический университет, г. Иркутск, Российская Федерация. (дата обращения 30.09.2024).
4. Иванов А. В. Особенности защиты от угроз социальной инженерии // Вестник Московского университета МВД России. 2023. №7. (дата обращения 30.09.2024).
5. Таракджи Мхд Ясир, Ортис Себастьян, Паюсова Т. И. Обеспечение защиты данных от утечек через открытые источники // Тюменский государственный университет, г. Тюмень. (дата обращения 30.09.2024).

Borisenko I., Seregin I. **SOCIAL ENGINEERING AS A THREAT TO INFORMATION SECURITY: ANALYSIS OF METHODS AND METHODS OF PROTECTION.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article examines modern methods of social engineering, with a particular focus on phishing and its variations. The psychological mechanisms of manipulation used by attackers are analyzed, and effective strategies for protection against social engineering attacks are presented. Special attention is paid to a comprehensive approach to information security, including technical measures and educational strategies. The research is based on the analysis of modern social engineering practices and methods of counteracting them.

Key words: social engineering, phishing, information security, cybersecurity, manipulation, multi-factor authentication, data protection.

УДК 004.056.53
ГРНТИ 81.93.29

АНАЛИЗ ХАРАКТЕРИСТИК СОВРЕМЕННЫХ ПРОТОКОЛОВ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ И ИХ БЕЗОПАСНОСТИ

М. Э. Бударин, Т. Д. Лобащенко, А. В. Никифоров
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бриевича

Виртуальные частные сети (VPN) стали важной составляющей информационной безопасности, обеспечивая конфиденциальность и целостность данных при их передаче через общедоступные сети. В основе VPN лежат различные протоколы, которые определяют метод шифрования, туннелирования и обработки данных. На сегодняшний день наибольшее внимание привлекают три современных протокола – WireGuard, OpenVPN и IPsec. Эта статья представляет сравнительный анализ характеристик и уровня безопасности этих протоколов, выявляя их достоинства и недостатки в контексте информационной безопасности и практического применения.

VPN, WireGuard, OpenVPN, IPsec, безопасность

С развитием интернета наиболее популярными среди VPN-протоколов стали WireGuard, OpenVPN и IPsec, каждый из которых имеет свои уникальные особенности и преимущества. В статье проведен их сравнительный анализ, раскрывающий особенности и уровни безопасности для разных сфер применения.

WireGuard – относительно новый протокол, разработанный для обеспечения высокой производительности и простоты. Его минималистичная архитектура, состоящая из около 4000 строк кода, упрощает аудит и снижает риск уязвимостей [1, 2]. Протокол использует современные криптографические алгоритмы ChaCha20 и Poly1305, обеспечивая высокий уровень защиты данных [1, 3]. Однако его статическая система ключей требует ручного обновления, что ограничивает применение WireGuard в корпоративных средах [3]. Тем не менее, простота и высокая скорость делают его особенно привлекательным для мобильных устройств и сетей с ограниченными ресурсами [2, 4].

OpenVPN – это гибкий и надежный протокол с открытым исходным кодом. Он поддерживает широкий выбор криптографических алгоритмов, таких как AES-256, и работает на базе OpenSSL, обеспечивая совместимость с разными сетевыми условиями и возможность обхода брандмауэров [3, 4]. OpenVPN может работать поверх TCP и UDP, но сложная кодовая база увеличивает поверхность атаки и снижает производительность по сравнению с

WireGuard [2, 3]. Высокая поддержка платформ и гибкость делают OpenVPN надежным выбором для корпоративных VPN [5].

IPsec (Internet Protocol Security) обеспечивает безопасность данных на уровне IP и поддерживает режимы туннельного и транспортного шифрования. Этот протокол широко применяется для защиты корпоративных сетей и поддерживает алгоритмы AES и SHA [4]. Стоит учитывать, что его сложная настройка может затруднить применение в организациях без квалифицированных специалистов [5]. IPsec остается стандартом для защищенных корпоративных сетей и часто используется в государственных структурах [6].

Пояснение типов применения VPN протоколов:

1. Корпоративное использование. Применение VPN для организации защищенных каналов передачи конфиденциальных данных между офисами, удаленными сотрудниками и корпоративными серверами. Протоколы: IPsec, OpenVPN [3, 7].

2. Личное использование. Это использование VPN для обеспечения конфиденциальности интернет-активности, обхода географических ограничений и защиты данных в общедоступных сетях. Протоколы: WireGuard, OpenVPN [2, 9].

3. Мобильное использование. Применение VPN на мобильных устройствах для защиты данных при подключении к общественным сетям с минимальной нагрузкой на ресурсы устройства [3].

Каждый протокол имеет свои сильные и слабые стороны в аспекте безопасности, что делает их подходящими для различных сценариев. WireGuard, благодаря современным криптографическим алгоритмам, таким как ChaCha20 и Poly1305, предлагает надежную защиту и высокую производительность, однако его статическая система управления ключами ограничивает применение в крупных корпоративных сетях, где требуется автоматизация [7]. OpenVPN, работающий на основе библиотеки OpenSSL, обеспечивает гибкость и адаптацию к разным требованиям безопасности, что делает его универсальным выбором. Однако сложность реализации этого протокола увеличивает риск уязвимостей и снижает производительность в сравнении с более простыми решениями [8]. IPsec, в свою очередь, остается стандартом для корпоративных и государственных учреждений, предоставляя высокий уровень защиты данных на уровне IP-протокола. Его использование требует тщательной настройки и квалифицированного сопровождения, что может стать вызовом для организаций с ограниченными ресурсами [9].

Таким образом, выбор VPN-протокола должен основываться на конкретных потребностях, особенностях инфраструктуры и приоритетах в области безопасности данных.

В таблице 1 представлен сравнительный анализ характеристик рассматриваемых протоколов.

ТАБЛИЦА 1. Характеристики сравниваемых протоколов [4]

Протокол	Шифрование	Аутентификация	Производительность	Простота настройки	Применение
WireGuard	ChaCha20	Poly1305	Высокая	Простая	Личное и мобильное
OpenVPN	AES-256/OpenSSL	OpenSSL	Средняя	Средняя	Корпоративное и личное
IPsec	AES, SHA	AH, ESP	Средняя	Сложная	Корпоративное и государственное

При сравнении скорости протоколов VPN и уровня задержки WireGuard выделяется как наиболее производительный вариант. Этот протокол демонстрирует минимальные задержки и высокую пропускную способность благодаря своей легкости и оптимизированной архитектуре, что делает его эффективным для ситуаций, где важна высокая скорость передачи данных [2, 10]. OpenVPN, обладая более сложной кодовой базой, показывает средние результаты по скорости и задержке, однако его универсальность и совместимость компенсируют это в сценариях, где критичны надежность и адаптивность [7, 10]. IPsec, будучи ориентированным на корпоративные и правительственные сети, часто демонстрирует более высокие задержки по сравнению с WireGuard, особенно в условиях сложной сетевой инфраструктуры [12]. Однако он остается востребованным благодаря высокому уровню безопасности и шифрования [8].

Ниже приведены рисунки 1 и 2 сравнения скорости и задержки исследуемых протоколов.

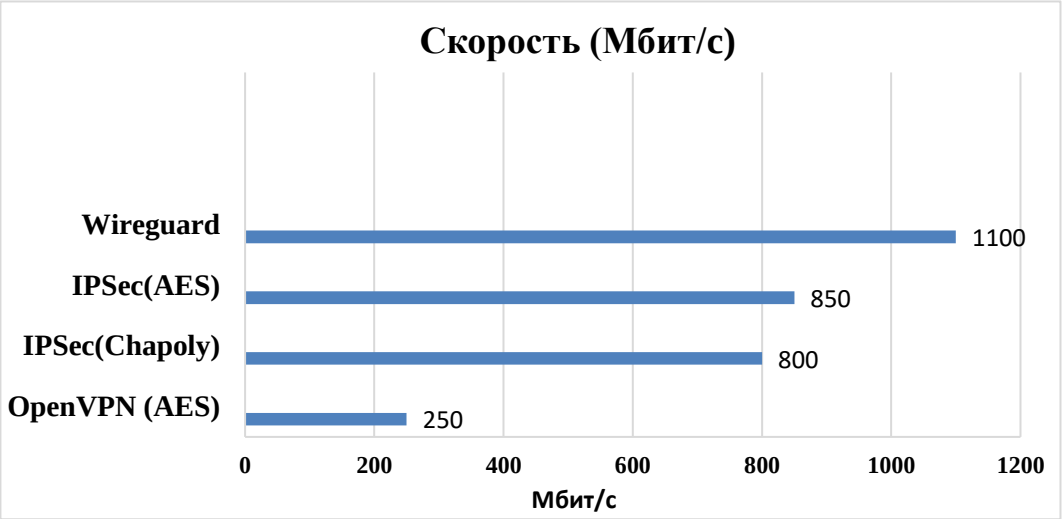


Рис. 1. Оценка скорости сравниваемых протоколов [5]

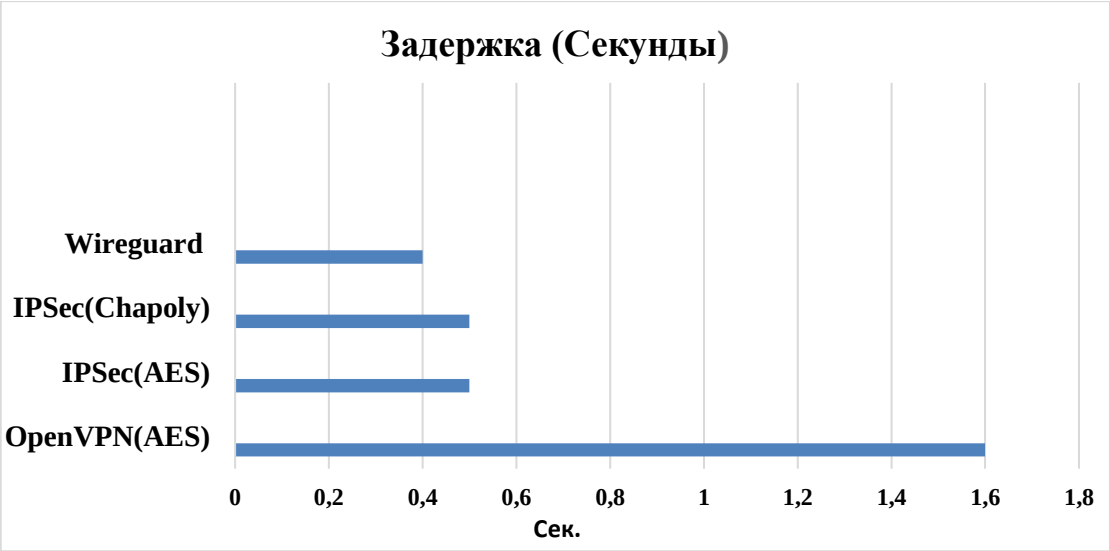


Рис. 2. Оценка задержки сравниваемых протоколов [5]

Таким образом, каждый из рассматриваемых протоколов обладает своими особенностями, однако WireGuard выделяется как наиболее предпочтительный выбор благодаря высокой скорости, простоте настройки и современному подходу к безопасности [7, 12]. Этот протокол является оптимальным для большинства пользователей, включая личное и мобильное использование, где важны минимальные задержки и высокая производительность.

Список используемых источников

1. Поликарпов С. В. Программный модуль легковесного криптоалгоритма для WireGuard VPN // Защищенные системы связи. Раздел 6. Практические аспекты криптографии, 2022. № 1. С. 45–50. Южный федеральный университет (Ростов-на-Дону). URL: https://zss.spb.ru/index.php/1-2022zss/ (дата обращения 14.11.2024).
2. WireGuard vs OpenVPN: Which VPN Protocol is Better? PureVPN. URL: https://www.purevpn.com/blog/wireguard-vs-openvpn (дата обращения 14.11.2024).
3. Гавриленко Е. В., Докшин А. Д., Ковцур М. М., Мисливский Б. С. Исследование эффективности VPN туннелей для организации удаленного доступа // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. С. 201–205
4. VPN Protocols: IPsec, WireGuard, and OpenVPN Explained. Selectel. URL: https://selectel.ru/blog/vpn-protocols/ (дата обращения 14.11.2024).
5. IPsec vs WireGuard: Security Protocols in VPN Solutions. Zenarmor. URL: https://www.zenarmor.com/docs/network-security-tutorials/ipsec-vs-wireguard (дата обращения 14.11.2024).
6. Understanding VPN Protocols: A Comparison of Security, Speed, and Compatibility. Security.org. URL: https://www.security.org/vpn/protocols/ (дата обращения 14.11.2024).
7. Ковцур М. М., Сахаров Д. В., Мисливский Б. С., Михайлова А. В. Исследования функционала pfSenygb se для сравнения VPN протоколов // Региональная информатика и инфор-

мационная безопасность. Сборник трудов XII Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 2021. С. 365–368.
8. Ковцур М. М., Сахаров Д. В., Мисливский Б. С., Михайлова А. В. Исследование методики сравнения VPN решений // Информационная безопасность регионов России (ИБРР-2021). Материалы XII Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 2021. С. 387–388.
9. OpenVPN vs WireGuard: Which VPN Protocol Should You Use?. Serverspace. URL: https://serverspace.io/about/blog/openvpn-vs-wireguard-which-vpn-is-better/ (дата обращения 14.11.2024).
10. Красов А. В., Штеренберг С. И., Москальчук А. И. Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем // Вестник Брянского государственного технического университета. 2020. № 3 (88). С. 38–46.
11. Миняев А. А., Красов А. В., Сахаров Д. В. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2020, № 1, С. 29–33. DOI: 10.46418/2079-8199_2020_1_5. EDN: ULHTJK.
12. Десницкий В. А., Сахаров Д. В., Чечулин А. А., Ушаков И. А., Захарова Т. Е. Защита информации в центрах обработки данных. СПб., 2019.

Budarin M., Lobaschenko T., Nikiforov A. **VPN PROTOCOL COMPARISON AND OPTIMAL USE CASES.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The choice of VPN protocol impacts both the performance and security of data transmission. WireGuard's high-speed, low-latency architecture makes it well-suited for mobile and personal use cases where simplicity and efficiency are prioritized. OpenVPN, with its compatibility and adaptability across various networks, remains a popular choice for corporate environments that require flexibility and network reliability. IPsec, though complex to configure, is optimal for government and enterprise sectors where strict data security policies are in place and IP-level encryption is necessary.
In terms of performance, WireGuard demonstrates lower latency and faster speeds, particularly in bandwidth-constrained environments, while OpenVPN and IPsec provide more robust solutions for environments with diverse network structures and high security needs.
Key words: VPN, WireGuard, OpenVPN, IPsec, security.

УДК 004.056.53
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ СПОСОБОВ ОБНАРУЖЕНИЯ АТАКИ EVIL TWIN В СЕТЯХ IEEE 802.11AX

С. А. Винников, А. Ю. Киструга, М. М. Ковцур
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С каждым обновлением стандарта IEEE 802.11 в технологию беспроводной передачи данных Wi-Fi привносится множество улучшений. Помимо изменения основных характеристик таких как пропускная способность, рабочая частота, радиус действия и добавления новых технологий, закрываются старые дыры в безопасности, что делает некоторые атаки неактуальными для новых поколений сетей Wi-Fi. Но несмотря на это, в сетях шестого поколения появился новый способ реализации атаки «Злой двойник» из-за добавления новой рабочей частоты. Цель работы – исследовать способы обнаружения атаки «Злой двойник».

IEEE 802.11ax, Wi-Fi, Evil Twin, 6 ГГц, сканирование, обнаружение

Одним из главных нововведений в стандарте IEEE 802.11ax было добавление новой рабочей частоты 6 ГГц [1]. Так как данная частота не использовалась в сетях прошлых поколений, ограничений связанных с поддержкой устаревших устройств не было, что позволило убрать неэффективные механизмы безопасности и добавить обязательную защиту кадров управления. Это делает сети, работающие в 6 ГГц диапазоне более защищенными. Однако отсутствие поддержки устройств, не работающих с Wi-Fi 6E привело к появлению нового способа реализации атаки Evil Twin.

Обновление сетевого оборудования в корпоративных сетях требует много времени и больших вложений. Из-за этого, большая часть корпоративных сетей базируются на сетях прошлых поколений, значит не может взаимодействовать с частотой 6 ГГц [2]. При этом на рынке представлено множество пользовательских устройств, поддерживающих новый диапазон [3], из-за чего возникает ситуация, представленная на рис.1, при которой злоумышленник может развернуть свою точку доступа [4], сотрудники компании могут к ней подключиться, но корпоративные сканеры сети не могут ее обнаружить.

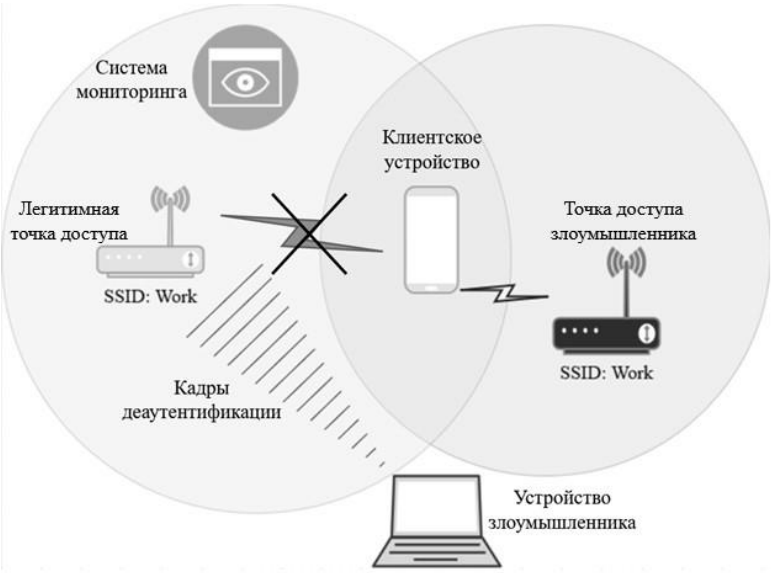


Рис. 1. Схема атаки Evil Twin

6 ГГц частота имеет 59 каналов шириной 20 МГц, поэтому обнаружение «злого двойника» внутри данной частоты также является затруднительным. Разработчики стандарта IEEE 802.11ax добавили механизмы, которые оптимизируют поиск точек доступа, однако эти механизмы можно использовать и для обнаружения атаки evil twin как внутри 6 ГГц диапазона, так и вне [5].

Первый способ обнаружения внутри 6 ГГц диапазона заключается в пассивном сканировании сети. Система мониторинга слушает сеть и обнаруживает кадры быстрой установки соединения (FILS). FILS Discovery Frames содержат информацию о точке доступа, включая SSID, каналы и другие параметры, которые помогают клиентским устройствам быстро находить доступные сети. Таким образом сокращается объем утилизации трафика, путем запрета точке доступа отвечать кадром response на probe request, в котором содержится ее имя в качестве ранее обнаруженной точки. Они периодически отправляются станциями на заранее определенных каналах, что позволяет клиентским устройствам сканировать выбранные каналы и находить AP без необходимости прослушивания всех каналов в диапазоне. Данный механизм встроен во все точки доступа, работающих на новой частоте.

Также при пассивном сканировании обращается внимание на кадры незапрашиваемого широковещательного ответа на зонд (UBPR). Unsolicited Broadcast Probe Response – это очень частые кадры probe pesponse без запроса [6]. Эти кадры содержат информацию о информацию о SSID, поддерживаемых каналах, методах аутентификации, уровнях шифрования и других параметрах сети и позволяют устройствам быстро обнаруживать доступные точки доступа в конкретном канале.

Второй способ заключается в активном сканировании. Preferred Scan Channel (PSC) – вещание маячковых кадров только в тех каналах, где осуществляется поиск сетей. Как было сказано выше каналов в 6 ГГц диапазоне

много, поэтому при активном сканировании сети прослушиваются только определенные каналы, называемые «Предпочтительные каналы сканирования»: 5, 21, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213 и 229. Это каналы в диапазоне 6 ГГц, на которых точки доступа (AP) регулярно передают маяки и другие управляющие кадры, такие как Fast Initial Link Setup Discovery Frames и Unsolicited Broadcast Probe Response. Данные каналы используются для ускорения процесса обнаружения сетей клиентскими устройствами во всем 6 ГГц диапазоне, в других диапазонах PSC не работает.

Третий способ является единственным, позволяющим обнаружить нелегитимную точку доступа вне 6 ГГц диапазона. Он заключается в обнаружении SSID точки доступа в других диапазонах с помощью сокращенных отчетов соседей (RNR). Reduced Neighbor Report – это специальный элемент в кадрах маяка и других управляющих кадрах Wi-Fi, содержащий информацию о точке доступа, как это показано на рисунке 2. Данный механизм необходим для быстрого поиска доступных сетей, но его можно использовать для обнаружения evil twin.

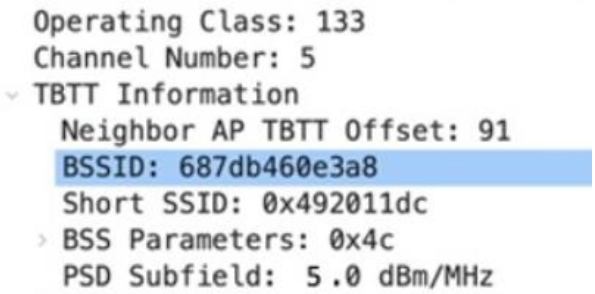


Рис. 2. RNR в Wireshark

В RNR точка доступа рассказывает о себе. Задача RNR состоит в том, чтобы в одном диапазоне рассказать о том, какие SSID у точки есть в другом диапазоне. Таким образом клиенты могут обнаруживать SSID 6 ГГц с помощью кадров маяков 2,4 ГГц или 5,0 ГГц. Важно отметить, что в неподдерживаемом диапазоне для детектирования evil twin можно опираться только на данный метод.

От использования вышеописанных механизмов, которые позволяют обнаружить «злого близнеца» злоумышленник не может отказаться, т. к. для успешной реализации атаки необходимо, чтобы точку доступа как можно быстрее обнаружили клиенты, значит нелегитимная точка доступа должна как можно интенсивнее сообщать о своей сети.

Помимо детектирования нелегитимной точки доступа, работающей в диапазоне 6 ГГц, в обнаружении атаки поможет обнаружение аномально большого количества кадров деаутентификации в сети, поскольку атака deauthentication flood дополняет evil twin, чтобы спровоцировать пользователей подключиться к точке доступа злоумышленника.

Заключение. Главная опасность атаки Evil Twin заключается в том, что многие люди могут не догадываться о данном способе реализации атаки через сеть 6 ГГц, и, соответственно, не знать о способах противодействия. В настоящее время на территории РФ данная атака мало применима, поскольку новый диапазон частот официально будет разрешен к применению только с 1 марта 2025 года [7]. Однако после 1 марта данная атака станет более вероятно к исполнению, поэтому данная работа обращает внимание на эту проблему. Описанные в статье механизмы не предназначены для обнаружения атаки, но специалисты по безопасности нашли методы их использования для защиты сетей.

Список используемых источников

1. 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 05.02.2023)
2. Ковцур М. М, Винников С. А., Трезоров 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.
3. Consumer WLAN Infrastructure // 650 group URL: https://650group.com/reports/consumer-wlan infrastructure/ (дата обращения 21.02.2023).
4. Петрова Т. В., Ковцур М. М., Карельский П. В., Поляничева А. В. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети // Современные проблемы науки и образования, 2022. С. 20–22.
5. 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 23.02.23).
6. Юркин Д. В. Никитин В. Н. Системы обнаружения вторжений в сетях широкополосного радиодоступа стандарта IEEE 802.11 // Информационно-управляющие системы, 2014. № 2 (69). С. 44–49.
7. Акт Правительства Российской Федерации «Постановление Правительства Российской Федерации "О внесении изменений в постановление Правительства Российской Федерации от 20 октября 2021 г. № 1800"» от 01.07.2024 № 897 // Официальный интернет-портал правовой информации. 2024 г. № 0001202407010020.

Vinnikov S., Kistruga A., Kovtsur M. **THE RESEARCH OF WAYS TO DETECT EVIL TWIN ATTACKIN IEEE 802.11AX NETWORKS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

With each update of the IEEE 802.11 standard, many improvements are introduced to Wi-Fi wireless transmission technology. Besides changing basic characteristics such as throughput, operating frequency, range and adding new technologies, old security holes are closed, making some attacks irrelevant for new generations of Wi-Fi networks. But despite this, there is a new way to implement Evil Twin attack in the sixth generation networks, due to the addition of new operating frequency. The aim of the paper is to investigate the ways to detect the Evil Twin attack.

Key words: IEEE 802.11ax; Wi-Fi; Evil Twin; 6 GHz; scanning; detection.

УДК 004.056
ГРНТИ 81.93.29

ОБНАРУЖЕНИЕ ИНФОРМАЦИОННЫХ ФЕЙКОВ: ИЗМЕНЕНИЯ И ВЫЗОВЫ В ПОСТ-2022 ПЕРИОД

Л. А. Виткова, С. В. Лагутина, Д. В. Сахаров
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена анализу распространения фейковой информации, включая дипфейки, поддельные документы и фейковые новости, а также методам их обнаружения. Рассмотрены каналы дезинформации, такие как социальные сети, и технологии создания дезинформации. Обсуждаются современные подходы к выявлению фейков, включая машинное обучение, и обозначены перспективные направления исследований в этой области.

фейковые новости, дезинформация, дипфейки, социальные сети, машинное обучение

В настоящее время в публичном информационном пространстве набирает обороты распространение фейковых новостей и поддельных изображений, в том числе документов с фейковыми печатями, отредактированных видео и даже псевдо-реальных новостных сюжетов, вырванных из контекста или представленных с вводящими в заблуждение заголовками или подписями.

В 2022 году Автономная некоммерческая организация (АНО) по развитию цифровых проектов в сфере общественных связей и коммуникаций «Диалог» запустила проект по проверке достоверности фактов, указанных в новостях (фактчекинг). Согласно проведенным ими исследованиям, количество фейковых новостей в Российской Федерации в 2022 году увеличилось в 4 раза по сравнению с 2021 годом, а в 2023 возросло еще на 25 % [1–2]. Более 12 миллионов копий фейковых сообщений было обнаружено экспертами в сети в 2023 году, все они собрали несколько миллиардов просмотров [3]. Среди основных драйверов активного роста фейковой информации эксперты назвали пандемию коронавируса и начало проведения специальной военной операции (СВО) в 2022 году. Беспрецедентный рост количества фейков отмечен в социальных сетях: лидирует «ВКонтакте», на эту соцсеть приходится сегодня 31 % фейковых сообщений, на втором месте – Telegram с 26 %, замыкают тройку «Одноклассники» с 20 % фейков [4].

Всероссийский центр изучения общественного мнения (ВЦИОМ) называет социальные сети ключевым каналом распространения фейковых новостей, далее с большим отставанием следуют интернет-издания, телевидение и телеграм-каналы [5]. Например, согласно социологическому опросу населения Республики Мордовия, трое из десяти опрошенных сталкивались с фейко-

выми новостями не реже нескольких раз в месяц, а двое из десяти делились ими с окружающими [5].

В попытке справиться с инфодемией, связанной с COVID-19, ВОЗ и Великобритания совместно провели исследование, которое показало, что за первые три месяца 2020 года дезинформация о коронавирусе привела к госпитализации примерно 6000 человек по всему миру [6]. А исследования Массачусетского технологического института (MIT) показало, что фейковые новости в Twitter (с 23.07.2023 – запрещенная в РФ организация) распространяются в шесть раз быстрее, чем реальные новости, и на 70 % чаще ретвитятся [6].

Распространяемые в социальных сетях новостные тексты и видео с подделкой голоса и внешности, называемые дипфейками, становятся более реалистичными за счет применения нейронных сетей для их создания, а средняя продолжительность их жизни сокращается, сейчас она составляет около 4 дней, после чего фейк исчезает или меняется, обрастая подробностями и адаптируясь под актуальную повестку. Использование бото-ферм и языковых моделей приводят к тому, что количество фейкового контента неконтролируемо увеличивается.

Вслед за ростом количества и качества фейков активно развивается и инструментарий цифровой криминалистики по их выявлению, применяется комбинированный подход с использованием разных методов машинного обучения, наблюдается тенденция и к увеличению количества научных публикаций по теме информационных фейков и их обнаружения, начиная с 2016 года [6].

В 2022-2023 годах публикации во многом касались исследований фейковых новостных текстов и видео (дипфейки), информационных атак в социальных сетях, обзоров способов и алгоритмов выявления фейков [7–10].

В 2024 году в мировом публичном пространстве стали появляться обзоры, описывающие не только ключевые модели или методы машинного/глубокого обучения для обнаружения фейкового контента, но и показатели эффективности каждой модели или метода, обзоры пробелов в существующих решениях [11–12]. Например, обзор материалов по выявлению поддельных отзывов о продуктах и услугах показал, что большинство методов обнаружения поддельных отзывов были предложены для широко распространенных в мире языков, таких как английский и китайский, современные комбинированные техники извлекают результат независимо, игнорируя корреляции между ними и прочее [12]. Это темы найдут отражение в будущих исследований в области автоматического обнаружения фейковых новостей в социальных сетях.

Заключение

Современные технологии способствуют росту объемов и качества фейкового контента, включая дипфейки, поддельные документы и фейковые ново-

сти, распространяемые в основном через социальные сети. Существующие методы обнаружения, основанные на машинном обучении, демонстрируют прогресс, но остаются ограниченными из-за адаптивности фейков. Будущие исследования будут направлены на разработку универсальных моделей для разных языков, интеграцию мультидисциплинарных подходов и прогнозирование распространения дезинформации.

Список используемых источников

1. Фейки // Лапша Медиа. URL: https://lapsha.media/feiky/
2. Тренд на ложь // Лапша Медиа. URL: https://lapsha.media/stati/half-year-fakes-2022/?ysclid=m3ihcy3xkl466612909
3. Эксперт сообщил, что в 2023 году в сети выявили 12 млн копий фейков // ТАСС. URL: https://tass.ru/obschestvo/21868693
4. Эксперты: ВКонтакте и Telegram – главные фейковые площадки Рунета // Российская газета. URL: https://rg.ru/2024/08/11/proverka-faktov.html
5. Ушкин С. Г. Не только социальные сети: каналы распространения фейковых новостей в представлениях населения // Galactica Media: Journal of Media Studies, 2024. Vol. 6, № 2. PP. 162–176. DOI 10.46539/gmd.v6i2.460. – EDN YUXQRL.
6. Dhiman P. et al. A scientometric analysis of deep learning approaches for detecting fake news // Electronics, 2023. Vol. 12. №. 4. PP. 948.
7. Калятин В. О. Дипфейк как правовая проблема: новые угрозы или новые возможности? // Закон, 2022. № 7. С. 87–103. DOI 10.37239/0869-4400-2022-19-7-87-103. – EDN FENGGS.
8. Виткова Л. А., Лешукова А. М. Детектирование объектов на изображениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 1. С. 272–275. EDN QJNFMH.
9. Виткова Л. А. Информационные атаки в социальных сетях // Региональная информатика (РИ-2022): Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции, Санкт-Петербург, 26–28 октября 2022 года. – Санкт-Петербург: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2022. С. 145–147. EDN LQTDEQ.
10. Ahmed S., Hinkelmann K., Corradini F. Combining machine learning with knowledge engineering to detect fake news in social networks-a survey //arXiv preprint arXiv:2201.08032. – 2022.
11. Phan H. T., Nguyen N. T., Hwang D. Fake news detection: A survey of graph neural network methods // Applied Soft Computing, 2023. Vol. 139. PP. 110235.
12. Singh M. K. et al. A comprehensive review on automatic detection of fake news on social media // Multimedia Tools and Applications, 2024. Vol. 83. №. 16. PP. 47319-47352.

Vitkova L., Lagutina S., Saharov D. **IDENTIFICATION OF INFORMATION FAKES: CHANGES AND CHALLENGES IN THE PERIOD AFTER 2022.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article analyze the distribution of fake information, including deepfakes, fake documents, and fake news, as well as methods of their detection. It consider disinformation channels, such as social networks, and disinformation creation techniques. The article has a discussion about modern approaches of detecting fakes, including machine learning techniques, and also outlines the promising areas of research in this area.

Key words: fake news, disinformation, deepfake, social networks, machine learning techniques.

УДК 004.056
ГРНТИ 81.93.29

ОБЗОР И ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ПРОЦЕССА DETECTION ENGINEERING В SIEM СИСТЕМАХ

Л. А. Виткова, М. В. Прохорова
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается концепция Detection Engineering. Авторы анализируют основные этапы Detection Engineering, включая оценку рисков, выбор источников данных и проверку гипотез. Выделяются ключевые задачи: выявление аномалий, обнаружение угроз, использование методов машинного обучения и разработка правил обнаружения. Особое внимание уделяется существующим ограничениям, таким как высокий уровень ложных срабатываний, нехватка квалифицированного персонала и необходимость постоянного обновления. Авторы отмечают важность интеграции мультидисциплинарных подходов и автоматизации для преодоления этих вызовов, что позволит системам эффективно адаптироваться к динамично изменяющемуся ландшафту угроз

detection engineering, SIEM системы, контент обнаружения, Detection as a Code, автоматизация обнаружения

Введение

Современные реалии информационной безопасности требуют от организаций способности быстро и эффективно выявлять киберугрозы. Увеличение объема данных, сложности атак и частоты их возникновения ставит под сомнение традиционные подходы к управлению событиями и инцидентами безопасности (SIEM). Процессы улучшения качества обнаружения сегодня часто включают в себя создание, настройку и поддержку правил и сигнатур. Сама SIEM система остается ключевым элементом системы безопасности во многих организациях. Тем не менее, этот процесс зачастую оказывается трудоемким, требующим значительных временных и человеческих ресурсов.

В ответ на эти вызовы все более актуальным становится «Detection Engineering» [1]. Такой подход позволяет автоматизировать создание и управление правилами обнаружения, обеспечивая адаптацию системы безопасности к новым угрозам. В настоящей статье рассматривается роль «Detection Engineering» в оптимизации процесса выявления угроз информационной безопасности, а также его значение для повышения эффективности работы SIEM.

Анализ

«Detection Engineering» представляет собой комплексный процесс, направленный на разработку, поддержку и тестирование правил и механизмов обнаружения угроз в условиях динамично изменяющегося ландшафта информационной безопасности. Центральным элементом этого процесса является так называемый «контент обнаружения», который включает совокупность правил, алгоритмов и иных ресурсов, предназначенных для мониторинга, анализа и идентификации подозрительных действий в информационных системах.

Ключевые задачи, решаемые в рамках «Detection Engineering» [2]:

– выявление аномалий и подозрительных действий в сетевом трафике;

– обнаружение известных угроз с применением сигнатурных методов;

– использование методов машинного обучения;

– разработка, оптимизация и внедрение правил обнаружения для систем мониторинга, таких как SIEM, а также для платформ реагирования на инциденты.

Эффективная реализация «Detection Engineering» требует интеграции мультидисциплинарных подходов, включая анализ данных, угроз информационной безопасности и разработку алгоритмов. Центральный процесс «Detection Engineering» представляет собой многоэтапный подход, направленный на создание, оптимизацию и поддержку механизмов обнаружения угроз. Он включает в себя следующие ключевые этапы [3]:

1. Определение требований и оценка рисков. На первоначальном этапе осуществляется анализ информационной инфраструктуры организации. Это включает идентификацию ключевых активов, критически важных бизнес-процессов и потенциальных уязвимостей. Для повышения точности анализа используются данные из процесса «Threat Intelligence» [4]. На их основе формируются гипотезы о возможных угрозах, которые впоследствии проверяются с использованием различных источников информации. Такими источниками могут быть журналы регистрации событий, сетевой трафик, активность пользователей и приложений, анализ файлов, электронная почта, домены и другие компоненты инфраструктуры.

2. Выбор источников данных. Список используемых источников данных определяется актуальными для организации угрозами, потенциальными нарушителями и их методами. Эти методы могут быть идентифицированы с использованием таких ресурсов, как матрица MITRE ATT&CK и База данных угроз ФСТЭК.

3. Формирование гипотез и их проверка. На основе идентифицированных угроз и анализа рисков формируются гипотезы о возможных векторах атак. Эти гипотезы тестируются путем анализа данных, поступающих из выбран-

ных источников. Такой подход позволяет не только обнаруживать угрозы в реальном времени, но и выявлять их закономерности и адаптировать систему безопасности к новым вызовам. Этот этап служит основой для построения эффективной системы обнаружения, способной учитывать уникальные особенности организации и адаптироваться к динамически меняющемуся ландшафту угроз.

На текущем этапе развития технологий автоматизация тестирования контента обнаружения остается на низком уровне зрелости. Вместо применения автоматизированных решений часто используется труд специалистов, работающих как внутри компании, так и на аутсорсинговой основе. Это замедляет процессы и увеличивает их стоимость, создавая дополнительные вызовы для реализации отечественных систем управления информационной безопасностью.

Исследование показало, что несмотря на очевидные преимущества, внедрение «Detection Engineering» в SIEM системах сопряжено с рядом ограничений:

1. Высокий уровень ложных срабатываний. SIEM системы часто генерируют значительное количество ложных срабатываний. При запуске процесса автоматизации написании правил обнаружения необходимо заранее учесть возможную потерю качества и рост ложных срабатываний и внедрять модели оценки эффективности [5].

2. Недостаток квалифицированного персонала. Для эффективной реализации «Detection Engineering» требуются высококвалифицированные специалисты, обладающие глубокими знаниями в области информационной безопасности, анализа данных и разработки алгоритмов.

3. Необходимость постоянного обновления. Постоянная эволюция угроз требует регулярного пересмотра и обновления правил обнаружения, что создает значительную нагрузку на специалистов по информационной безопасности [6].

Таким образом, хотя «Detection Engineering» является перспективным направлением для оптимизации работы SIEM систем, его успешное внедрение требует преодоления перечисленных проблем. Будущие исследования и разработки должны быть направлены на повышение уровня автоматизации и снижение зависимости от человеческих ресурсов, что позволит системам более эффективно адаптироваться к динамично изменяющемуся ландшафту угроз.

Заключение

В данной статье «Detection Engineering» рассматривается как одно из ключевых направлений развития информационной безопасности, направленное на оптимизацию работы SIEM систем в условиях усложняющегося ланд-

шафта угроз. В статье подчеркивается, что автоматизация процессов разработки и поддержки правил обнаружения способствует снижению нагрузки на аналитиков и повышению точности выявления угроз. Однако внимание также уделяется существующим вызовам, среди которых выделяются высокий уровень ложных срабатываний, дефицит квалифицированных специалистов и необходимость регулярного обновления правил обнаружения. Результаты, полученные в ходе исследования, позволяют сделать вывод, что для преодоления данных ограничений потребуется интеграция мультидисциплинарных подходов, внедрение современных технологий машинного обучения и развитие решений, ориентированных на автоматизацию.

Список используемых источников

1. Tune Your SIEM Faster by Automating Detection Engineering // Picus Security Validation Platform URL: https://www.picussecurity.com/resource/blog/optimizing-siem-via-detection-engineering-automation (дата обращения 14.11.2024).
2. Dennis Chow Automating Security Detection Engineering: A hands-on guide to implementing Detection as Code. 1st Edition изд. 2024.
3. Roddie M., Deyalsingh J., Katz G.J. Practical Threat Detection Engineering: A hands-on guide to planning, developing, and validating detection capabilities. Packt Publishing, 2023.
4. Токарев М. В., Абрамов Е. С. Разработка методики интеграции поиска и аналитики киберугроз // Современная педагогика и научные исследования в образовательной организации высшего образования, 2023. С. 275–285.
5. Валеев М. В., Царегородцев А. В. Анализ существующих систем обнаружения атак: современное состояние и перспективы развития // Международная научно-практическая конференция по компьютерной и информационной безопасности INFSEC 2023, 2023. С. 72–81.
6. Иванцов Д. С., Саенко И. Б. О разработке математической модели процесса функционирования системы управления информацией и событиями безопасности // Информационная безопасность регионов России (ИБРР-2023). 2023. С. 85.

Vitkova L., Prokhorova M. **REVIEW AND FEATURES OF THE DETECTION ENGINEERING PROCESS IN SIEM SYSTEMS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article examines the concept of Detection Engineering. The authors analyze the main stages of Detection Engineering, including risk assessment, selection of data sources, and hypothesis testing. Key tasks are highlighted: anomaly detection, threat identification, application of machine learning methods, and development of detection rules. Particular attention is paid to existing limitations, such as a high rate of false positives, a shortage of qualified personnel, and the need for constant updates. The authors emphasize the importance of integrating multidisciplinary approaches and automation to overcome these challenges, enabling systems to effectively adapt to the dynamically evolving threat landscape.

Key words: Detection engineering, SIEM systems, detection content, Detection as Code, detection automation.

УДК 004.056
ГРНТИ 81.93.29

МЕТОДЫ МИНИМИЗАЦИИ УЩЕРБА ПРИ ВОЗМОЖНЫХ ИНЦИДЕНТАХ БЕЗОПАСНОСТИ

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

В современных условиях роста кибератак организациям жизненно необходимо не только предотвращать, но и эффективно минимизировать ущерб от инцидентов безопасности. Проактивные стратегии, такие как оценка рисков и мониторинг угроз, наряду с методами быстрого реагирования и восстановления, позволяют минимизировать влияние инцидентов и защитить критически важные данные. Комплексный подход к управлению инцидентами безопасности помогает сохранить целостность ИТ-систем и оперативность работы, снижая риски для бизнеса и репутации.

кибербезопасность, инциденты безопасности, минимизация ущерба, оценка рисков, план реагирования

В условиях постоянного увеличения числа и сложности кибератак бизнесу и государственным учреждениям важно не только предотвращать потенциальные угрозы, но и разрабатывать эффективные подходы к минимизации ущерба в случае инцидентов безопасности. Инциденты могут приводить к серьезным последствиям, включая утечку данных, финансовые потери и нарушение непрерывности операций. Поэтому внедрение мер по минимизации ущерба – важная часть стратегии информационной безопасности любой организации. В данном контексте эффективными инструментами становятся оценка рисков, мониторинг, стратегии быстрого сдерживания и восстановления.

Инцидент безопасности – это событие или серия событий, угрожающих целостности, конфиденциальности или доступности информационных систем и данных организации [1]. Такие инциденты могут включать утечку данных, распространение вредоносного ПО, взлом систем или несанкционированный доступ к информации. Поскольку подобные события способны причинить значительный ущерб – от финансовых потерь до репутационных рисков и сбоев в операциях – готовность к ним и умение минимизировать их последствия становятся ключевыми элементами успешной стратегии кибербезопасности.

Проактивная оценка рисков и планирование

Проактивная оценка рисков и планирование начинается с анализа потенциальных угроз, которые могут затронуть информационные системы организации. Проведение регулярной оценки рисков и выявление уязвимостей позволяет своевременно обнаружить слабые места, требующие защиты [1]. Важным элементом данного этапа является создание плана реагирования, в котором четко обозначены последовательные шаги действий, а также распределены роли и обязанности среди сотрудников [2]. Такой подход к подготовке позволяет сократить время реакции и снизить масштаб возможного ущерба при возникновении инцидента.

Обнаружение угроз и мониторинг в реальном времени

Для своевременного обнаружения угроз используется мониторинг в реальном времени, который позволяет контролировать сетевой трафик и выявлять подозрительные активности, не нарушая при этом работу системы. Системы обнаружения и предотвращения вторжений (IDPS) автоматически анализируют данные и могут моментально блокировать потенциальные угрозы, что предотвращает дальнейшее их распространение [3]. Системы управления событиями и информацией безопасности (SIEM) собирают данные из множества источников, анализируют аномалии и отправляют оповещения, помогая операторам своевременно реагировать на инциденты. Дополнительно применяются методы анализа поведения пользователей, которые отслеживают отклонения от обычных действий и помогают выявить внутренние угрозы.

Сдерживание угроз

После обнаружения угрозы важно принять меры по ее сдерживанию:

1. Изоляция зараженных систем. Отключение скомпрометированных систем предотвращает распространение вредоносного ПО;

2. Сегментация сети. Разделение сети на независимые зоны ограничивает движение злоумышленников по системе;

3. Контроль доступа. Ограничение прав пользователей минимизирует доступ к критически важным данным.

Эффективное реагирование и коммуникация

Эффективное реагирование на инциденты невозможно без четкой структуры действий и координированной работы команды. Включение плана реагирования на инциденты позволяет не только быстро начать сдерживание угрозы, но и грамотно управлять коммуникацией с заинтересованными сторонами, включая руководство, сотрудников и внешние организации [1]. Опера-

тивное взаимодействие с правоохранительными органами может стать необходимым шагом для расследования инцидента и предотвращения последующих атак. Налаженная система коммуникации помогает обеспечить своевременное информирование всех сторон и минимизировать риск для репутации компании.

Восстановление и постинцидентный анализ

Восстановление после инцидента проводится в таком порядке:

– восстановление из резервных копий, устранение уязвимостей и повторная проверка на наличие вредоносного ПО;

– оценка инцидента позволяет выявить недостатки в реагировании и улучшить защитные меры;

– результаты анализа помогают укрепить меры защиты, пересмотреть политику безопасности и оптимизировать контроль доступа.

Краткое резюме выводов

Методы минимизации ущерба играют критически важную роль в защите данных и обеспечении бесперебойной работы организаций в случае инцидентов безопасности. Внедрение проактивных и реактивных мер позволяет быстро реагировать на угрозы и снижать их негативное воздействие на бизнес.

Направления будущих исследований

В целях дальнейшего улучшения методов минимизации ущерба при инцидентах безопасности необходимо развивать новые подходы и технологии, которые представлены в таблице 1.

ТАБЛИЦА 1. Перечень методов, которые помогут минимизировать ущерб при инцидентах безопасности

Тип метода	Описание
Интеграция с искусственным интеллектом	Использование алгоритмов машинного обучения и ИИ для автоматизации обнаружения угроз может сократить время реагирования и повысить точность идентификации инцидентов [3]
Адаптация методов к новым типам угроз	Совершенствование методов обнаружения для учета новых типов кибератак, таких как атаки на основе искусственного интеллекта и атаки с применением социальной инженерии
Разработка средств мониторинга реального времени	Создание платформ, которые способны собирать и анализировать данные об угрозах в реальном времени для обеспечения более точного и своевременного реагирования
Исследование устойчивости систем	Проведение исследований по повышению устойчивости ИТ-инфраструктуры к потенциальным инцидентам и разработка мер, направленных на сохранение работоспособности даже в условиях кибератаки

Эти направления исследований и разработок помогут организациям не только минимизировать ущерб от инцидентов, но и значительно повысить общий уровень кибербезопасности.

Список используемых источников

1. National Institute of Standards and Technology (NIST). "Computer Security Incident Handling Guide." Special Publication 800-61 Revision 2, 2012. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
2. Stallings W., Brown, L. Computer Security: Principles and Practice. Pearson Education, 2018.
3. Scarfone K., Mell, P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94, 2007. URL: https://csrc.nist.gov/publications/detail/sp/800-94/final

***Gavrilov P.* METHODS OF MINIMIZING DAMAGE IN POSSIBLE SECURITY INCIDENTS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In today's growing cyber-attack environment, it is vital for organizations to not only prevent, but also effectively minimize the damage from security incidents. Proactive strategies such as risk assessment and threat monitoring, along with rapid response and recovery methods, help minimize the impact of incidents and protect critical data. A comprehensive approach to security incident management helps maintain the integrity of IT systems and operational efficiency, reducing risks to business and reputation.

Key words: cybersecurity, security incidents, damage mitigation, risk assessment, response plan.

УДК 004.056
ГРНТИ 81.93.29

СОЦИАЛЬНЫЕ СЕТИ КАК ИНСТРУМЕНТ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

А. С. Груздев, Д. А. Комаров
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире социальные сети стали неотъемлемой частью нашей жизни. Они не только помогают нам общаться с друзьями и родственниками, но и предоставляют широкие возможности для воздействия на людей. В этой связи важно обратить внимание на такое явление, как социальная инженерия, которая активно использует социальные сети для своих целей.

социальная инженерия, манипуляция сознанием, поддельные новости, киберугроза

Понятие социальной инженерии

Социальная инженерия – это форма манипуляции, которая предполагает воздействие на мысли и поведение людей с целью достижения определенных результатов. Основная цель социальной инженерии – получить доступ к информации, ресурсам или убеждениям человека, минуя строгие технические защиты [1].

В отличие от прямых технических атак, социальная инженерия основана на психологии: манипуляторы апеллируют к доверию, страхам или любопытству, что делает ее менее очевидной для жертвы. Социальная инженерия может применяться как для безвредных целей, например, для психологических исследований [2], так и для обмана и преступной деятельности, когда манипуляция становится неэтичной [3].

Механизмы воздействия в социальных сетях

Социальные сети предоставляют широкий спектр возможностей для социальной инженерии. Пользователи часто делятся личной информацией, что упрощает задачу манипуляторам [2]. Существуют как психологические, так и технологические методы воздействия:

1. Психологические приемы. Люди доверяют профилям, которые кажутся «настоящими» и близкими. Манипуляторы могут создавать доверительные отношения, используя фотографии, комментарии, упоминания общих интересов [3]. Эмоциональное воздействие – еще один важный инструмент, с помощью

которого злоумышленники вызывают страх или сочувствие, чтобы получить нужные сведения [4].

2. Технологические инструменты. Фишинг, приманивающий контент, спам – распространенные методы манипуляции. Фишинг представляет собой поддельные ссылки и сообщения, имитирующие настоящие сервисы и побуждающие пользователей к раскрытию личных данных [3]. Кликбейт работает на основе человеческого любопытства, побуждая людей перейти по заманчивым заголовкам и делиться информацией [5].

Примеры социальной инженерии в социальных сетях

Псевдопсихологи и тренинги по личностному росту

В период пандемии COVID-19 в социальных сетях, активно начали продвигаться псевдопсихологи и тренеры по личностному росту. Они использовали методы социальной инженерии, создавая фальшивые отзывы и истории успеха [2], чтобы привлекать внимание к своим платным курсам и услугам. Люди, оказавшиеся в уязвимом состоянии из-за пандемии, часто соглашались на такие предложения, тратя деньги на сомнительные курсы [5].

Атаки на банки с использованием социальной инженерии

В последние годы российские банки столкнулись с волной атак, где злоумышленники, используя социальные сети, выдавали себя за сотрудников банков [3]. Через поддельные аккаунты в «ВКонтакте» мошенники выходили на связь с пользователями, представляясь как служба безопасности, и просили «подтвердить» данные своих банковских карт или даже перевести средства для «предотвращения подозрительной активности» [5].

Цветные революции на постсоветском пространстве

Цветные революции и протестные движения в странах бывшего СССР, таких как Украина, Грузия, Армения, Беларусь и Казахстан, демонстрируют ключевую роль социальных сетей в координации и мобилизации протестующих [3].

В Беларуси протесты 2020 года после президентских выборов широко освещались в Telegram-каналах, которые обеспечивали информационную поддержку движению и быстро сообщали о происходящих событиях, собирая большое количество участников [4].

В Казахстане в январе 2022 года протестующие использовали социальные сети для публикации и распространения сообщений, критики правительства и мобилизации граждан. Это привело к временному блокированию интернета, что также свидетельствует о влиянии социальных сетей на социальную устойчивость.

Последствия использования социальных сетей для социальной инженерии

Во-первых, это нарушение доверия между людьми. Когда люди сталкиваются с обманом и манипуляцией, они начинают сомневаться в искренности и честности окружающих, что может привести к социальной изоляции и недоверию [3].

Во-вторых, это угроза личной безопасности. Раскрытие личных данных, таких как номера кредитных карт, пароли и адреса, может привести к краже личности, финансовому мошенничеству и другим преступлениям. Люди становятся уязвимыми перед злоумышленниками, которые используют полученную информацию для своих корыстных целей [1, 4].

В-третьих, это психологическое воздействие. Манипуляции, основанные на страхе, сочувствии или любопытстве, могут вызывать у людей стресс, тревогу и депрессию. Особенно уязвимы подростки и молодые люди, которые часто становятся жертвами подобных атак [5].

Наконец, это социальные и экономические последствия. Манипуляции в социальных сетях могут влиять на общественное мнение, создавая информационные пузыри и усиливая поляризацию общества. Это затрудняет конструктивный диалог и решение важных социальных проблем. В экономическом плане мошенничество и кибератаки наносят ущерб финансовым институтам и бизнесу, снижая доверие к цифровым технологиям и сервисам [2, 3].

Противодействие социальной инженерии в социальных сетях

Для защиты от социальной инженерии в социальных сетях необходимо принимать комплексные меры. Во-первых, важно повышать цифровую грамотность и осведомленность пользователей. Для защиты от социальной инженерии важно развивать цифровую грамотность на работе, в школах, в учреждениях среднего и высшего образования адаптируя обучение к конкретной аудитории.

На работе целесообразно проводить регулярные тренинги по кибербезопасности, включая симуляции фишинговых атак, которые помогают сотрудникам распознавать угрозы и укрепляют навыки. Памятки по основам безопасности, политики корпоративной киберзащиты и постоянная поддержка от IT-отдела позволяют сотрудникам быстрее реагировать на потенциальные риски и минимизировать уязвимости [7]. В школах важно внедрять основы цифровой безопасности на уроках информатики, чтобы дети знали, как защитить личные данные. В учреждениях среднего и высшего образования можно ввести обязательные курсы и мастер-классы по кибербезопасности, где студенты

научатся распознавать угрозы и защищать личные данные. Лекции от экспертов и поддержка студенческих сообществ, занимающихся информационной безопасностью, мотивируют студентов углублять знания о киберугрозах и взаимодействовать с профессионалами [3].

Во-вторых, для эффективного противодействия социальной инженерии и защиты пользователей в сети необходимо применять комплекс технических мер, которые снижают риски атак и помогают быстро реагировать на потенциальные угрозы. Первостепенное значение имеет использование двухфакторной и многофакторной аутентификации (2FA и MFA). Важно также рассмотреть угрозу брутфорс-атак. Важно ограничить видимость личных данных, и установить параметры приватности так, чтобы только проверенные пользователи могли видеть публикации и отправлять сообщения. Если у злоумышленника есть личные сведения о человеке, такие как ФИО или дата рождения, это увеличивает вероятность успешного подбора [1]. Многие люди, к сожалению, используют простые пароли или личные данные, что облегчает брутфорс-атаку.

Двухфакторная аутентификация эффективно противостоит этой угрозе: даже если пароль будет скомпрометирован через брутфорс, злоумышленнику потребуется второй фактор (например, код, отправленный на телефон) для входа. Это создает дополнительный барьер и защищает учетные записи, даже если основной пароль становится уязвимым [6]. Сложные и регулярно обновляемые пароли также играют важную роль в безопасности. Настройка приватности в социальных сетях помогает сократить количество доступной информации, которую злоумышленники могут использовать для социальной инженерии [2].

Постоянный мониторинг активности в учетных записях позволяет обнаруживать подозрительные действия, например, попытки входа с незнакомых устройств или изменения пароля. Для безопасности переписки и передаваемых данных рекомендуется использовать end-to-end шифрование, чтобы сообщения оставались доступными только отправителю и получателю. Так, популярные мессенджеры, как WhatsApp и Telegram, применяют шифрование, предотвращающее перехват информации посторонними лицами [5].

Анализ и фильтрация трафика, проводимые через межсетевые экраны и системы обнаружения вторжений, позволяют выявлять и блокировать фишинг, вредоносные ссылки и подозрительную активность [5]. Такие системы могут оповещать о потенциальных угрозах, блокируя доступ к подозрительным сайтам. Алгоритмы машинного обучения также активно используются для выявления аномалий в поведении пользователей, автоматически анализируя и распознавая подозрительные действия.

Для защиты от социальной инженерии и других киберугроз важен комплекс технических мер, включая использование надежного антивирусного программного обеспечения. Регулярное обновление антивируса помогает защититься от новых угроз, поскольку базы данных программ пополняются свежими сведениями о вредоносных программах [8].

В-третьих, важно сотрудничать между государственными органами, бизнесом и гражданским обществом. Обмен информацией и координация усилий помогут более эффективно бороться с социальной инженерией и минимизировать ее последствия [5].

Выводы

Для противодействия социальной инженерии в социальных сетях необходимо сосредоточиться на внедрении технологий раннего выявления угроз и защиты данных. Перспективным направлением является разработка алгоритмов машинного обучения для раннего выявления и блокировки попыток социальной инженерии.

Автоматизированные системы мониторинга, основанные на анализе поведенческих паттернов, способны динамически выявлять аномалии и предвосхищать угрозы. Их интеграция в социальные сети позволит фильтровать фейковые новости, выявлять ботов и блокировать манипулятивные схемы.

Список используемых источников

1. Федеральный закон «О персональных данных» (№ 152-ФЗ от 27.07.2006 г.). – М.: Официальное издательство, 2006. 38 с.
2. 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. VI Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. С. 166–170.
3. Виткова Л. А., Чечулин А. А., Сахаров Д. В. Выбор мер противодействия вредоносной информации в социальных сетях // Вестник Воронежского института ФСИН России, 2020. № 3. С. 20–29.
4. Левкин И. М., Науменко К. А., Виткова Л. А. Особенности информационно-психологического воздействия в интернете // X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР). 2017 С. 365–367.
5. Сахаров Д. В., Шашкин В. С. Система противодействия распространению вредоносной информации в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 783–787.

6. Виткова Л. А., Сахаров Д. В., Голузина Д. Р. Модель вредоносной информации и ее распространителя в социальных сетях // Защита информации. Инсайд, 2020. № 3 (93). С. 66–72.
7. Виткова Л. А., Сахаров Д. В., Голузина Д. Р. Модель вредоносной информации и ее распространителя в социальных сетях // Защита информации. Инсайд, 2020. № 3 (93). С. 66–72.
8. Борисов С. В., Мосикян А. А., Сахаров Д. В. Боты в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 560–563.

Gruzdev A., Komarov D. **SOCIAL MEDIA AS A METHOD OF SOCIAL ENGINEERING.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the modern world, social media has become an integral part of our lives. It not only helps us communicate with friends and family but also offers extensive opportunities for influencing people. In this context, it is important to address the phenomenon of social engineering, which actively leverages social networks for its purposes.

Key words: social engineering, manipulation of consciousness, fabricated news, cyber threat.

УДК 004.056
ГРНТИ 81.93.29

ПРИМЕНЕНИЕ ПОДХОДА К ПРОЕКТИРОВАНИЮ УСТРОЙСТВ НА ОСНОВЕ МИКРОКОНТРОЛЛЕРОВ ДЛЯ ОБЪЕКТОВ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ К СЕТЕВОМУ МАРШРУТИЗАТОРУ

Л. Д. Гугунишвили, Д. С. Левшун
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья посвящена архитектуре систем проектирования устройств на основе микроконтроллеров, ориентированных на применения в сетевых маршрутизаторах, обеспечивающих функционирование объектов критически важной инфраструктуры. Особое внимание уделяется концепции проектирования защищенных устройств (Secure by Design). Рассматривается пример системы с применением такого подхода для объектов критической инфраструктуры.

система на основе микроконтроллеров, secure by design, объект критически важной инфраструктуры, информационная безопасность, сетевой маршрутизатор

Объекты критически важной инфраструктуры представляют собой сложные взаимосвязанные системы, требующие высоконадежных и защищенных решений. В связи с этим для обеспечения их надежной и эффективной работы требуется применение новых методов проектирования.

Одним из ключевых элементов таких систем являются микроконтроллеры – программируемый логический компонент, предназначенный для управления различными процессами и оборудованием.

Цель данной статьи – разработка архитектуры системы проектирования устройств на основе микроконтроллеров, а также анализ роли таких систем в обеспечении защиты объектов критически важной инфраструктуры.

На начальных этапах проектирования, устройства на основе микроконтроллеров представляет собой абстрактную модель, обобщенное описание устройства такого типа. Данное описание обычно не содержит детальной информации о конкретной реализации устройства, например, исходном коде его программного обеспечения или конструкции аппаратной схемы. При этом в нем отражены элементы устройства, их связи и свойства, а также связи данного устройства с другими устройствами [1, 2].

Помимо функциональных требований, проектируемое устройство должно обеспечивать необходимый уровень защищенности. Концепция кон-

структивно безопасных систем (англ. Secure by Design) подразумевает проактивный подход к безопасности, при котором риски безопасности учитываются и минимизируются на ранних стадиях разработки архитектуры системы [3]. Основными преимуществами такого подхода являются:

– повышение безопасности проектируемых устройств и систем с их использованием за счет минимизации рисков пропуска уязвимости и внедрения необходимых средств защиты на ранних стадиях разработки;

– ускорение разработки при меньших затратах, как результат уменьшается вероятность изменений готовой архитектуры.

Рассмотрим процесс применения данной концепции на примере устройства, представленного на рисунке 1.

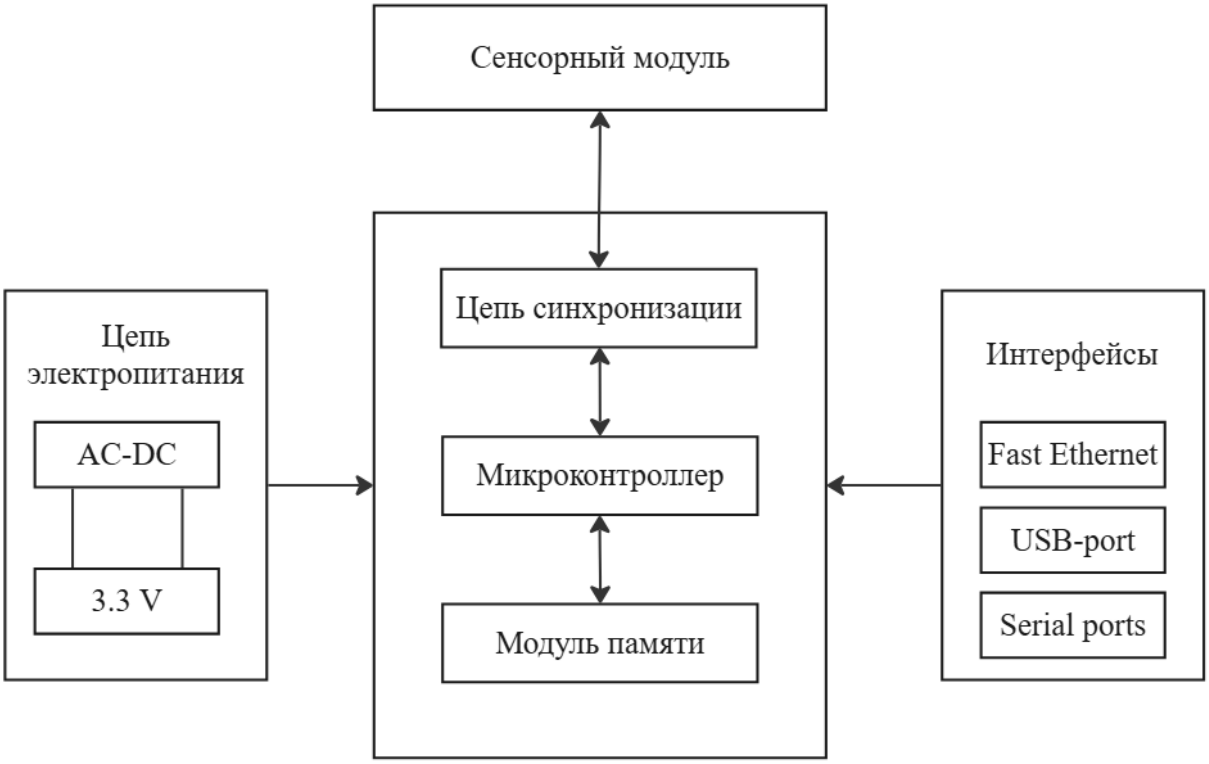


Рис. 1. Архитектура маршрутизатора

Представленное устройство состоит из 7 элементов. Ниже приведено подробное описание каждого элемента.

Элемент 1. Микроконтроллер. Функции микроконтроллера включают в себя обработку входящих пакетов данных, принятие решения о маршрутизации, обеспечение работы механизма NAT, управление другими компонентами системы [4]. На вход микроконтроллера поступают пакеты данных в формате IP, MAC-адреса, таблицы маршрутизации, конфигурационные файлы. Выходными данными являются команды для других компонентов, обновленные таблицы маршрутизации, пакеты данных с измененными заголовками.

Защита микроконтроллера включает в себя как физическую защиту устройства от внешних воздействий, так и программные методы обеспечения безопасности данных и кода. Далее представлены примеры таких мер.

Аппаратные меры:

– герметизация корпуса эпоксидными смолами;

– выбор более высокой степени защиты корпуса (например, IP68);

– наличие подтягивающих резисторов – определяют начальное состояние входов при отсутствии внешнего сигнала;

– наличие ограничивающих резисторов – защищают при перегрузке;

– учет электромагнитной совместимости.

Программные меры:

– установка диапазона допустимых значений входных данных;

– журналирование ошибок;

– шифрование данных;

– аутентификация на основе пароля, токенов или биометрических данных;

– прерывание бесконечных циклов.

Элемент 2. Модуль памяти. Хранит операционную систему маршрутизатора, конфигурационные файлы, таблицы маршрутизации, кэш, временные данные. Для обеспечения безопасности необходимо:

– своевременное обновление прошивки маршрутизатора;

– использование специальных микросхем памяти с встроенными механизмами защиты от несанкционированного доступа (например, память, содержимое которой может быть стерто только при соблюдении определенных условий (подача специального напряжения));

– обеспечение защиты памяти от повреждений, вызванных статическим электричеством.

Элемент 3. Сетевые интерфейсы. Основная функция – обеспечение физического подключения к сети. Данные представлены в виде битовых потоков. Для обеспечения защиты необходимо:

– использование корпуса с высокой степенью защиты;

– использование блокиратора портов для отключения ненужных интерфейсов;

– использование списков доступа для фильтрации трафика.

Элемент 4. Модуль сенсоров. Функции модуля сенсоров включают в себя сбор данных об окружающей среде или состоянии устройства (температура, влажность, уровень сигнала и др.). Данные представлены в виде аналоговых или цифровых сигналов, представляющие измеренные значения физических величин. В качестве мер защиты могут быть применены:

– калибровка сенсоров;

– фильтрация шумов;

– защита от электромагнитных помех.

Элемент 5. Цепь тактового генератора. Представляет собой электронную схему, генерирующую последовательность электрических импульсов с постоянной частотой. Эти импульсы, называемые тактовыми сигналами, синхронизируют работу всех его компонентов [5]. В качестве данных, как правило, использует время в цифровом формате.

К рекомендуемым мерам защиты относятся следующие:

– использование высокоточных кварцевых генераторов;

– резервное питание для поддержания времени при отключении основного питания.

Элемент 6. Модуль питания. Данный элемент преобразует переменный ток в постоянный и обеспечивает питанием все компоненты маршрутизатора. В качестве мер защиты можно использовать:

– предохранители для защиты от перегрузок;

– программный контроль напряжения и механизм отключения устройства при отклонении от заданной нормы;

– мониторинг температуры;

– программное отключение при превышении допустимого потребляемого тока.

Представленный в данной подход к проектированию устройств на основе микроконтроллеров обеспечивает должный уровень надежности и защищенности устройств. В свою очередь, это позволяет использовать его для таких устройств, расположенных на объектах критически важной инфраструктуры в рамках комплексного подхода к созданию надежных и безопасных систем. Концепция "Secure by Design" лежит в основе данного подхода, внедряя элементы защиты на самых ранних этапах жизненного цикла устройства. Подобный подход позволяет минимизировать риски, связанные с угрозами безопасности, снизить затраты, а также сократить время разработки системы.

Список используемых источников

1. Tammy Noergaard Embedded Systems Architecture. Oxford: Newnes, 2005. 657 с.

2. Левшун Д. С. Иерархическая модель для проектирования систем на основе микроконтроллеров защищенными от киберфизических атак // Труды учебных заведений связи, 2023.

3. Sawano D., Johnsson D. B., Deogun D. Secure by Design. New York: Manning, 2019. 400 p.

4. Моц М. Кибербезопасность на уровне микроконтроллеров // Control Engineering Россия, 2019. С. 70–74

5. Что такое генератор тактовых импульсов // РадиоТехИндустрия URL: https://www.r-t-i.ru/news/chto-takoe-generator-taktovyx-impulsov/ (дата обращения 14.11.2024)

Gugunishvili L., Levshun D. **APPLYING AN APPROACH TO THE DESIGN OF MICRO-CONTROLLER-BASED DEVICES FOR CRITICAL INFRASTRUCTURE FACILITIES TO A NETWORK ROUTER.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article is devoted to the architecture of systems for designing microcontroller-based devices focused on applications in network routers and intended for use in critical infrastructure facilities. Particular attention is paid to the Secure by Design concept. An example of a system using this approach for critical infrastructure facilities is considered in detail.

Key words: microcontroller-based system architecture, secure by design, critical infrastructure facilities, , information security, network router.

УДК 004.056
ГРНТИ 81.93.29

ИЗУЧЕНИЕ АСПЕКТОВ ПРИМЕНЕНИЯ МАШИННОГО ОБУЧЕНИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. С. Денисов, О. И. Пантюхин, И. Д. Родичев
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С развитием цифровых технологий обеспечение информационной безопасности становится все более актуальной задачей. Машинное обучение предлагает новые подходы к защите информационных и телекоммуникационных систем, предоставляя инструменты для анализа и противодействия современным угрозам. В данной работе исследуются возможности применения машинного обучения в области информационной безопасности, а также анализируются передовые методы. Особое внимание уделено вопросам надежности алгоритмов, защите данных и сложности использования машинного обучения в системах выявления вторжений.

информационная безопасность, машинное обучение, анализ данных, предотвращение угроз, обнаружение угроз, методы машинного обучения

В эпоху, когда данные информационных и телекоммуникационных систем становятся все более ценным ресурсом, информационная безопасность выходит на передний план как ключевая область для исследований и разработок. Благодаря способности машинного обучения выявлять значимые закономерности из больших объемов данных, открываются новые возможности для усиления защиты таких систем. В данной работе анализируются перспективы использования машинного обучения в области информационной безопасности. Рассматривается его потенциал для предупреждения, выявления и реагирования на угрозы в цифровой среде. Исследование подчеркивает ключевую роль машинного обучения в обеспечении цифровой безопасности, а также акцентирует внимание на необходимости дальнейших исследований для повышения эффективности и надежности информационных и телекоммуникационных систем. Машинное обучение представляет собой класс методов искусственного интеллекта, который позволяет автоматически создавать аналитические модели в инфотелекоммуникационных системах, принимая решения на основе анализа данных, выявления закономерностей и обучения на решениях множества задач [1].

Машинное обучение позволяет решать множество задач, среди которых особое место занимает задача классификации. Классификация сетевого тра-

фика играет ключевую роль в обеспечении широкого спектра возможностей работы в компьютерных сетях, особенно для поддержания полного контроля над информационной безопасностью. Постоянное получение данных о типе и структуре трафика, проходящего через сеть, помогает защитить компьютерные сети, проводить диагностику их состояния, выявлять сетевые проблемы и контролировать выполнение политик информационной безопасности [1, 2]. Этот подход позволяет своевременно обнаруживать и предотвращать угрозы внедрения и функционирования вредоносных программ, что способствует разработке эффективного программного обеспечения для защиты инфотелекоммуникационных систем.

В области информационной безопасности используются разнообразные методы машинного обучения, каждый из которых обладает своими особенностями и преимуществами. Наиболее распространенные из них [1, 3]:

1. Метод опорных векторов (SVM). Применяется для классификации и регрессии. В информационной безопасности SVM помогает обнаруживать вторжения и мошенничество, разделяя нормальные и аномальные данные;

2. k ближайших соседей (k-NN). Используется для классификации и регрессии. Этот алгоритм применяется для выявления аномалий и фишинговых атак;

3. Метод роя частиц (PSO). Оптимизационный алгоритм, используемый для настройки параметров в системах обнаружения вторжений;

4. Обучение с учителем. Метод, основанный на обучении модели на размеченных данных. В информационной безопасности он может использоваться для обнаружения вредоносного ПО и спама;

5. Обучение без учителя. Модель обучается на неразмеченных данных, что полезно для выявления неизвестных угроз и аномалий в поведении пользователей;

6. Обучение с частичным привлечением учителя. Гибридный подход, комбинирующий элементы обучения с учителем и без учителя, что может повысить точность обнаружения угроз.

Эти методы находят применение в различных системах, таких как системы обнаружения вторжений (IDS), системы анализа трафика (NTA), системы защиты конечных устройств (EDR), системы мониторинга событий информационной безопасности (SIEM) и системы поведенческого анализа пользователей и сущностей (UEBA) [3]. Они способствуют анализу аномального поведения, прогнозированию угроз, идентификации и аутентификации, что является ключевым для защиты цифровых активов и сетевой инфраструктуры [4].

При использовании машинного обучения для обеспечения информационной безопасности возможны следующие проблемы:

– устойчивость алгоритмов: главным препятствием для использования моделей машинного обучения в критических информационных системах является проблема, связанная с их устойчивостью к внешним воздействиям – атакам на модели машинного обучения (воздействие на нейронную сеть, вызывающее ошибки в ее результатах). Причем атака может осуществляться как с использованием уязвимостей в ПО, так и с помощью данных для обучения модели [5];

– защита данных и алгоритмов: с увеличением потребления продуктов и услуг, созданных на основе искусственного интеллекта и машинного обучения, возникает необходимость в специальных мерах для защиты не только клиентов и их данных, но и самого искусственного интеллекта и его алгоритмов от злоупотреблений, троллинга и нарушения работоспособности [6]. Это предполагает внедрение передовых методов защиты моделей машинного обучения от различных атак, направленных на манипуляцию данными или их искажение. Особое внимание должно быть уделено защите от адверсариальных атак [7], которые могут использоваться злоумышленниками для внесения искажений в процесс обработки данных и принятия решений. Помимо этого, важна регулярная проверка и обновление моделей, чтобы своевременно реагировать на появляющиеся угрозы, что будет способствовать поддержанию высокой степени надежности и безопасности информационных систем. Шифрование данных и применение современных методов безопасности также играют ключевую роль в предотвращении вмешательства в алгоритмы машинного обучения и обеспечении их надежной работы;

– применение в системах обнаружения вторжений: использование алгоритмов машинного обучения при решении задач информационной безопасности, а именно при построении систем обнаружения вторжений (IDS) нового поколения, также может вызвать определенные сложности [8]. Одной из ключевых проблем является необходимость обеспечения высокой точности обнаружения угроз при минимальном количестве ложных срабатываний. Это требует тщательной настройки и оптимизации моделей, а также регулярного обновления данных для обучения. Кроме того, требуется значительная вычислительная мощность для обработки больших объемов данных в реальном времени. Важным аспектом является также защита самих моделей машинного обучения от атак, направленных на их компрометацию или манипуляцию результатами. Необходимость интеграции IDS с другими системами безопасности и мониторинга тоже может представлять определенные трудности, требующие комплексного подхода и дополнительных ресурсов.

Это лишь некоторые из возможных проблем, и они могут варьироваться в зависимости от конкретного контекста и применения. Однако, несмотря на эти проблемы, машинное обучение продолжает играть важную роль в области информационной безопасности, помогая в обнаружении и предотвращении угроз. Более того, развитие методов машинного обучения и их интеграция с другими технологиями безопасности открывают новые перспективы для защиты информационных систем. Постоянное совершенствование алгоритмов и их адаптация к изменяющимся условиям позволяют обеспечить более высокий уровень защиты и реагировать на новые виды угроз. Таким образом, несмотря на существующие вызовы, применение машинного обучения в информационной безопасности остается важным и перспективным направлением.

В заключение, машинное обучение представляет собой мощный инструмент в области информационной безопасности, способный анализировать большие объемы данных и выявлять сложные угрозы. Разнообразие методов машинного обучения, таких как SVM, k-NN, PSO, а также подходы обучения с учителем, без учителя и с частичным привлечением учителя, позволяют гибко подходить к защите информационных систем. Эти методы применяются в различных системах, включая системы обнаружения вторжений (IDS), системы анализа трафика (NTA), системы защиты конечных устройств (EDR), системы мониторинга событий информационной безопасности (SIEM) и системы поведенческого анализа пользователей и сущностей (UEBA), для анализа аномального поведения, прогнозирования угроз и идентификации пользователей.

Тем не менее, существуют проблемы, такие как устойчивость алгоритмов, защита данных и алгоритмов, а также сложности, связанные с применением машинного обучения в системах обнаружения вторжений. Эти проблемы требуют дальнейших исследований и разработок для обеспечения надежности и безопасности применения машинного обучения в критически важных информационных системах. Несмотря на эти вызовы, машинное обучение становится ключевым элементом в стратегии защиты цифровых активов и инфраструктуры. Его роль будет только усиливаться по мере развития технологий и увеличения объемов данных. Кроме того, интеграция машинного обучения с другими передовыми технологиями безопасности обещает создать более комплексные и эффективные решения для защиты информации. Таким образом, дальнейшие исследования и инновации в этой области будут способствовать повышению устойчивости и надежности информационных систем, обеспечивая их защиту от постоянно эволюционирующих угроз.

Список используемых источников

1. Искусственный интеллект в сетях связи: Учебное пособие / А. И. Выборнова, М. А. Маколкина, Е. С. Сапунова, И. А. Пожидаева. СПб.: СПбГУТ, 2022. 48с.
2. Дмитриев Е. А., Пантюхин О. И., Рябов Г. А., Солодухин Б. В. Анализ и отбор значимых характеристик сетевого трафика для использования в машинном обучении // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 277–281.
3. Обзор алгоритмов машинного обучения в современных средствах защиты информации. URL:https://na-journal.ru/1-2024-informacionnye-tekhnologii/8801-obzor-algoritmov-mashinnogo-obucheniya-v-sovremennyh-sredstvah-zashchity-informacii (дата обращения 11.11.2024).
4. Доргушаова А. К., Довгаль В. А., Козлова Н. Ш., Козлов Р. С. Обзор использования технологий машинного обучения в обеспечении информационной безопасности данных: настоящее и будущее // Вестник Адыгейского государственного университета. Сер.: Естественно-математические и технические науки, 2024. Вып. 1 (336). С. 51–59.
5. Машинное обучение в сфере информационной безопасности – это движение в правильном направлении? URL: https://habr.com/ru/companies/infotecs_official /articles/778220 (дата обращения 11.11.2024).
6. Безопасность, искусственный интеллект, машинное обучение. URL: https://learn.microsoft.com/ru-RU/security/engineering/securing-artificial-intelligence-machine-learning (дата обращения 11.11.2024).
7. Введение в Adversarial attacks: как защититься от атак в модели глубокого обучения на транзакционных данных. URL: https://habr.com/ru/companies/vtb/articles/718024/ (дата обращения 11.11.2024).
8. Виноградов Ю. В., Назаров А. Н., Сычев А. К. Применение алгоритмов машинного обучения при решении задач информационной безопасности // Системы высокой доступности, 2018, т. 14, № 4. С. 20–22.

Denisov A., Pantyukhin O., Rodichev I. **EXPLORING ASPECTS OF MACHINE LEARNING APPLICATION IN THE FIELD OF INFORMATION SECURITY.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

With the development of digital technologies, ensuring information security is becoming an increasingly urgent task. Machine learning offers new approaches to protecting information and telecommunication systems, providing tools to analyze and counter modern threats. This paper explores the possibilities of applying machine learning in the field of information security and analyzes the best practices. Special attention is paid to the issues of algorithm robustness, data protection, and the complexity of using machine learning in intrusion detection systems.

Key words: information security, machine learning, data analysis, threat prevention, threat detection, machine learning methods.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ РЕШЕНИЙ ВТОРОГО УРОВНЯ БЛОКЧЕЙН-СЕТЕЙ

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

В статье представлен анализ актуальных угроз безопасности, с которыми сталкиваются решения для масштабируемости блокчейн-сетей, технологии второго уровня, такие как Lightning Network и zk-Rollups. К основным типам рассматриваемых угроз относятся атаки на сетевые узлы и уязвимости смарт-контрактов. В работе представлены рекомендации по повышению безопасности решений второго уровня и подчеркивается важность обеспечения безопасности на всех уровнях, включая архитектуру протокола, управление узлами и взаимодействие с пользователем. Исследование направлено на создание более безопасного и надежного будущего для технологии блокчейн и содействие ее их широкому применению в различных областях

блокчейн, технологии второго уровня, атаки на решения второго уровня, Lightning Network

Введение

В последние годы блокчейн-технологии привлекают внимание благодаря своей способности обеспечивать децентрализованные и безопасные решения в различных отраслях. Однако с ростом популярности и внедрением этих технологий возникают новые вызовы, как в области безопасности, так и выявленных актуальных недостатках блокчейн-сетей, таких как невысокая пропускная способность сети, высокие комиссионные сборы с точки зрения выполнения транзакций для мелких повседневных покупок, высокая нагрузка на основную сеть. В связи с этим начали разрабатываться, активно развиваться и внедряться решения второго уровня (L2).

Цель данного исследования заключается в выявлении актуальных угроз безопасности для технологий L2 и предложении методов их решения.

Обзор технологий масштабируемости

Технологии второго уровня (L2) представляют собой протоколы, которые работают поверх основного блокчейна. Первый уровень (L1) – это сам блокчейн с его консенсусом, безопасностью и прямыми транзакциями, в то время как второй уровень использует основные принципы первого, добавляя дополнительные функции и механизмы для увеличения возможностей основной сети. При этом особенностью подобных решений является то, что основные

процессы выполняются Off Chain, то есть, когда блокчейн не задействуется, а действия с транзакциями и обработкой данных внутри блокчейна фактически минимизированы. Тем самым эти технологии направлены на борьбу с некоторым недостатками основных развернутых блокчейн сетей. Они способствуют улучшению масштабируемости, производительности, снижению задержек и комиссий для транзакций в блокчейн-сетях.

Для анализа безопасности самого блокчейна возможно использовать представление блокчейна в виде многоуровневой структуры позволяющей выявить характерные уязвимости каждого уровня; определить и разработать подходы к защите на конкретном уровне. Распределение атак и методов защиты по уровням модели упрощает выполнение задач для обеспечения безопасности всей системы [1]. Однако такой подход не будет эффективен если рассматриваются решения второго уровня, так как L2 решения часто имеют свои уникальные модели угроз и риски, которые отличаются от рисков, характерных для основного блокчейна.

Среди основных технологий L2 можно выделить Lightning Network (LN), zk-Rollups и Optimistic Rollups, каждая из которых предлагает уникальные методы улучшения скорости и снижения затрат на транзакции. Преимущества могут включать в себя быстрые и дешевые транзакции, однако у каждой технологии есть и недостатки, такие как сложность реализации и риски безопасности. Эти решения функционируют путем взаимодействия с основными блокчейнами (L1), что создает дополнительные уровни сложности и возможные векторы атак.

Актуальные угрозы безопасности

К современным угрозам безопасности для технологий L2 относятся**:**

1. Атаки на каналы платежей (Payment Channel Attacks) – в системах наподобие Lightning Network, если злоумышленник угрожает закрытием канала в неподходящий момент, он может попытаться использовать устаревшие состояния канала для получения средств;

2. Проблемы с ликвидностью – большинство L2 решений зависит от наличия достаточного количества ликвидности. Увеличение спроса на платежи может привести к высокому уровню перегрузки, вызывая проблемы с комиссионными и задержками;

3. Централизация и доверие – некоторые L2 решения могут быть более централизованными, что увеличивает риски, связанные с надежностью и защитой конкретного узла или предоставляемого сервиса, и ставит под сомнение децентрализованный характер самой технологии;

4. Атаки на компрометацию консенсуса – в системах с механизмами консенсуса уязвимости могут возникнуть, если одна сторона компрометирует процесс подтверждения транзакций;

5. Угрозы конфиденциальности – решения второго уровня могут подвергать пользователя риску утечки информации о транзакциях, особенно если в них не предусмотрены достаточные механизмы анонимности.

Прежде всего, достаточно уязвимыми являются rollups решения второго уровня. Rollups (роллапы) – это сети, построенные на смарт-контрактах, которые масштабируют медленные блокчейны. Они выполняют транзакции и публикуют их результаты на основной блокчейн. Роллапы наследуют безопасность от основного блокчейна, но уязвимы к прямым атакам. Некоторые атаки похожи на атаки сетевого уровня (например, атаки типа "отказ в обслуживании"), в то время как другие являются результатом подключения роллапов к базовому блокчейну (например, атаки на реорганизацию) [2]. Подробные представления о возможных атаках на подобные сети приведены в таблице 1.

ТАБЛИЦА 1. Различные типы атак на роллапы и методы их осуществления

Тип атаки	Описание методики
Censorship-атаки	Атаки, которые приводят к задержкам в подтверждении состояния. Секвенсоры могут игнорировать или задерживать транзакции
DoS-атаки	Атаки, направленные на недоступность или перегрузку сети. Централизованные компоненты могут быть целью атак, вызывающих сбои в работе роллапов
Атаки на поддельные транзакции	Включение поддельной транзакции в сводный пакет. Оптимистичные сводные данные могут допускать внедрение фальшивых транзакций
Злонамеренные реорганизации	Реорганизация может быть злонамеренной и привести к повторной реорганизации.
Удержание данных	Злоумышленники могут удерживать данные, необходимые для доказательства выполнения вывода. Злоумышленники могут контролировать доступ к данным, мешая их выпуску
Атака Sybil	Попытка захвата сети через создание множества поддельных узлов. Злоумышленники могут контролировать большую часть валидаторов, чтобы манипулировать состоянием

Для более полного представления основных угроз безопасности и конфиденциальности L2 решений рассмотрим проблемы на примере Lightning Network. Исследователи выявили несколько уязвимостей в LN, в том числе атаки с раскрытием баланса каналов, атаки с изоляцией узлов и атаки с использованием «червоточин». Также есть опасения по поводу растущей централизации сети и связанных с этим уязвимостей, из-за которых она может быть подвержена атакам с разделением и целенаправленным атакам [3].

Актуальные проблемы Lightning Network:

1. Конфиденциальность баланса канала. Существует риск раскрытия баланса канала во время маршрутизации, что может привести к раскрытию конфиденциальной информации о средствах пользователей. Например, атака с раскрытием баланса может привести к раскрытию баланса канала путем вы-

полнения нескольких незавершенных платежей. Чтобы снизить этот риск, пользователям рекомендуется открывать каналы только с проверенными сторонами;

2. Безопасность платежных каналов. Платежные каналы могут быть небезопасными, особенно в сценариях, связанных с закрытием каналов или отказом участников от сотрудничества. Например, злоумышленники могут отключать каналы, многократно отправляя через них небольшие платежи и удерживая соответствующие временные блокировки, что приводит к замораживанию каналов;

3. Устойчивость к сетевым атакам. Сеть не всегда может противостоять потенциальным атакам, таким как отказ в обслуживании или атаки на вытеснение. Например, злоумышленник может изолировать узел-жертву, отключить каналы Lightning и украсть средства, не сообщая об этом жертве.

Методы анализа и защиты

Оценка безопасности решений L2 включает в себя анализ их архитектуры и реализации, а также тестирование на выявление уязвимостей. Регулярное проведение аудитов кода для выявления потенциальных уязвимостей в смарт-контрактах и других компонентах L2 решений, а также использование инструментов для статического и динамического анализа, способствуют грамотному анализу систем.

Для моделирования и оценки угроз следует применять методологии, такие как STRIDE или DREAD, и обозначать потенциальных атакующих и их мотивы, а также вероятные векторы атак.

Повышение защищенности систем второго уровня (L2) над блокчейн-сетями возможно с применением некоторых ключевых подходов:

1. Использование схем блокировки и подтверждения транзакций для предотвращения двойного расходования. Это может включать механизмы временной блокировки средств на каналах и использование escrow-счетов;

2. Внедрение децентрализованных протоколов консенсуса, которые обеспечивают согласованность данных. Для Rollups это может включать использование zk-SNARKs или других криптографических доказательств для обеспечения целостности и корректности данных;

3. Использование криптографических методов, таких как AMHL, для улучшения безопасности [4];

4. Автоматическое закрытие неактивных или ненадежных каналов для минимизации рисков в случае, если каналы являются целью атак;

5. Разработка интеграций с другими системами, которые могут обеспечить дополнительный уровень безопасности, например, путем использования мультиподписей или децентрализованных обменников для выполнения транзакций.

Заключение

В будущем можно ожидать появления новых технологий и подходов к масштабируемости, таких как интеграция искусственного интеллекта для оптимизации протоколов. Развитие угроз будет зависеть от особенностей реализации новых решений и стиля взаимодействия пользователей с блокчейном. Существующие актуальные предложения по повышению защищенности систем второго уровня потенциально могут обеспечить достаточный уровень безопасности.

Необходимо обеспечивать безопасность решений второго уровня для блокчейн-сетей, т. к. это является критически важным для стимуляции массового принятия блокчейн-технологий, что в свою очередь поможет реализовать их потенциал в различных отраслях экономики и социальных сферах.

Список используемых источников

1. Богомаз М. Э., Кушнир Д. В. Анализ возможных атак на многоуровневую модель блокчейна // Актуальные проблемы инфотелекоммуникаций в науке и образовании XII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2023. Том 1. С. 181–185.
2. Koegl A., Meghji Z., Pellegrino D., Gorzny J., Derka M. Attacks on Rollups // DICG '23: Proceedings of the 4th International Workshop on Distributed Infrastructure for the Common Good. New York, USA: ACM, 2023. PP. 25–30.
3. Dasaklis T. K., Malamas V. A Review of the Lightning Network's Evolution: Unraveling Its Present State and the Emergence of Disruptive Digital Business Models // Journal of Theoretical and Applied Electronic Commerce Research. 2023. №18 (3). PP. 1338–1364.
4. Tikhomirov S., Moreno-Sanchez P., Maffei M. A Quantitative Analysis of Security, Anonymity and Scalability for the Lightning Network // 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Genoa, Italy: 2022. PP. 387–396.

Dzigovskii V. **ANALYSIS OF CURRENT SECURITY THREATS TO SECOND-LAYER SOLUTIONS IN BLOCKCHAIN NETWORKS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The paper presents an analysis of the current security threats faced by scalability solutions for blockchain networks, specifically Layer 2 technologies (L2) such as the Lightning Network and zk-Rollups. The main types of threats discussed include attacks on network nodes and vulnerabilities in smart contracts. The study offers recommendations for enhancing the security of L2 solutions and emphasizes the importance of ensuring security at all levels, including protocol architecture, node management, and user interaction. The research aims to create a safer and more reliable future for blockchain technology and to facilitate its widespread application in various fields.

Key words: blockchain, Layer 2 technologies, attacks on Layer 2 solutions, Lightning Network.

УДК 004.56
ГРНТИ 81.93.29

РУТКИТЫ ЯДРА И АНАЛИЗ TURLA

А. С. Догадаев, Н. А. Косов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Руткиты ядра представляют собой одну из самых опасных форм вредоносного программного обеспечения. Они работают на уровне ядра операционной системы, что позволяет злоумышленникам скрывать свою активность, получать доступ к конфиденциальным данным и управлять системой без обнаружения. Эти угрозы представляют серьезную проблему, особенно для критически важных инфраструктур, таких как энергетические компании, государственные учреждения и финансовые организации.

уязвимости ядра, имунная защита, руткиты, уязвимости

Целью данной статьи является обзор механизмов работы руткитов ядра, их применение, методы маскировки и инструменты защиты, а также рекомендуемые подходы к их эффективному обнаружению и устранению. Особое внимание уделено разбору руткита Turla как одного из самых сложных и известных примеров руткитов, используемых в реальных атаках.

Иммунная защита и уязвимости ядра. Иммунная защита информационных систем предполагает комплекс мер, направленных на предотвращение и обнаружение атак. Однако руткиты ядра обладают способностью обходить эти механизмы. Работая на уровне ядра, они изменяют ключевые структуры операционной системы, что позволяет злоумышленникам маскировать свою активность и препятствовать своевременному реагированию. Ядро операционной системы отвечает за управление системными ресурсами, включая доступ к памяти, обработку системных вызовов и управление процессами. Используя уязвимости в ядре, руткиты получают контроль над этими процессами. Например, в 2022 году Лаборатория Касперского зафиксировала атаку, где руткит модифицировал вызовы sys_open и sys_read, чтобы скрывать файлы, связанные с вредоносным ПО [1].

Пример руткита Turla. Руткит Turla является одним из наиболее известных и сложных примеров вредоносного ПО. Он используется для целенаправленных атак на государственные учреждения, энергетические компании и военные организации. Впервые обнаруженный более десяти лет назад, Turla остается актуальным благодаря постоянной эволюции своих методов и модульной архитектуре, позволяющей адаптироваться к различным целям.

Turla нацелен на сбор конфиденциальной информации, ее передачу на командные серверы и длительное присутствие в системе. Он известен своим уникальным подходом к маскировке, который делает его практически невидимым для традиционных средств защиты [2].

Архитектура и механизмы работы Turla

Turla состоит из нескольких ключевых компонентов, каждый из которых играет определенную роль в атаке. Основой работы руткита является модуль ядра, который интегрируется в систему через уязвимости в драйверах или стандартных модулях ядра. После установки Turla изменяет таблицу системных вызовов (sys_call_table), перехватывая такие вызовы, как sys_open и sys_read. Это позволяет скрывать файлы, каталоги и процессы, связанные с руткитом. На уровне пользовательского пространства Turla использует инструменты для взаимодействия с командными серверами (C&C). Эти инструменты работают через зашифрованные каналы связи, встроенные в обычный интернет-трафик. В некоторых случаях руткит применяет скрытые методы связи, такие как использование спутниковых каналов, что делает его обнаружение крайне сложным [3].

Механизмы защиты Turla. Для обеспечения устойчивости к обнаружению Turla использует сложные методы защиты. Все данные, которые собирает руткит, включая содержимое файлов и сетевую активность, шифруются перед передачей. Это затрудняет анализ даже при перехвате трафика. Еще одной особенностью Turla является динамическая модификация памяти. Этот механизм позволяет руткиту изменять содержимое ключевых областей памяти, делая свой код невидимым для стандартных инструментов мониторинга. Если администратор системы пытается удалить руткит, он может автоматически восстановиться, используя резервные копии своего кода, которые хранятся в скрытых местах файловой системы [4]. Для проникновения в систему Turla часто использует уязвимости в сторонних драйверах или программах. Например, в одной из атак был применен эксплойт для уязвимости в драйверах видеокарт, что позволило внедрить модуль Turla непосредственно в ядро операционной системы.

Пример атаки Turla в российской энергетической компании. В 2021 году Turla использовался для атаки на серверы крупной российской энергетической компании. Злоумышленники применили фишинговые письма для начального проникновения в систему. После этого руткит был установлен через уязвимость в драйверах ядра. Turla активно скрывал сетевую активность и файлы, связанные с кибершпионажем, передавая данные на командные серверы, расположенные за пределами России.

Техника маскировки включала модификацию вызовов sys_call_table, что позволяло руткиту скрывать процессы, связанные с атакой. Благодаря использованию зашифрованных каналов связи руткит оставался незамеченным более трех месяцев. Атака была выявлена только с помощью инструментов поведенческого анализа, которые обнаружили аномалии в работе системного ядра.

Методы противодействия руткитам ядра. Противодействие таким сложным руткитам, как Turla, требует использования многоуровневого подхода. Эффективные меры включают:

1. Мониторинг ядра. Использование инструментов, таких как Sysmon для Windows и Auditd для Linux, позволяет выявлять изменения в таблице системных вызовов и структуре ядра;

2. Анализ сетевого трафика. Регулярный мониторинг трафика с использованием систем обнаружения вторжений (IDS) помогает выявить зашифрованне соединения, используемые руткитами;

3. Проактивная защита. Регулярное обновление операционной системы и стороннего программного обеспечения снижает риск эксплуатации уязвимостей, используемых для установки руткитов;

4. Системы поведенческого анализа. Применение алгоритмов машинного обучения для анализа логов и поиска аномалий позволяет обнаруживать скрытую активность руткитов [5].

Заключение

Руткиты ядра, такие как Turla, представляют серьезную угрозу для информационной безопасности. Их способность работать на глубоком уровне операционной системы делает их труднодоступными для традиционных методов обнаружения. Сложные механизмы защиты, включая шифрование, динамическую модификацию памяти и скрытые каналы связи, обеспечивают им высокую устойчивость.

Для противодействия таким угрозам необходимы проактивные подходы, включая мониторинг ядра, анализ сетевого трафика и использование машинного обучения. В условиях растущих угроз кибершпионажа и целенаправленных атак на критически важные системы развитие этих методов становится ключевым элементом обеспечения информационной безопасности.

Список используемых источников

1. Колисниченко Д. Н. Rootkits под Windows: теория и практика программирования «шапок-невидимок», позволяющих скрывать от системы данные, процессы, сетевые соединения // Наука и Техника, 2006. 294 с. ISBN 5-94387-266-3. EDN QMQJQP.

2. Преображенский Ю. П. Об использовании идеологии иммунного подхода при реализации систем защиты информации в компьютерных системах // Вестник Воронежского института высоких технологий. 2018. № 2. С. 51–55.
3. Ваганов М. Ю. Гибридная искусственная иммунная система защиты компьютера от процессов с аномальной активностью: дис. – диссертация кандидата технических наук: 05.13. 19. СПб., 2012. 92 с.
4. Милушков В. И. и др. Исследование угроз информационного воздействия руткит на динамические данные ядра посредством мониторинга гостевой операционной системы виртуальной машины // Глобальный научный потенциал, 2015. № 10 (55). С. 29.
5. Катасонов А. И., Цветков А. Ю. Разработка метода аппаратного обнаружения руткита в ос Linux // Рецензенты: д-р техн. наук, проф. В. Н. Ложкин. 2021. С. 132.

Dogadaev A., Kosov N. **KERNEL ROOTKITS AND TURLA ANALYSIS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Kernel rootkits are one of the most dangerous forms of malware. They operate at the kernel level of the operating system, allowing attackers to hide their activity, access sensitive data, and control the system without detection. These threats pose a serious problem, especially for critical infrastructures such as energy companies, government agencies, and financial institutions.

Key words: Kernel vulnerabilities, immune protection, rootkits, vulnerabilities.

УДК 004.56
ГРНТИ 81.93.29

РЕАЛИЗАЦИЯ УЯЗВИМОСТИ IMAGE MAGIC НА ASTRA LINUX

Р. М. Домбровский, Н. А. Косов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном цифровом мире обеспечение конфиденциальности информации становится одной из ключевых задач информационной безопасности. Растущая сложность программного обеспечения, расширение функциональности операционных систем и непрерывный рост числа кибератак делают уязвимости важной проблемой для защиты данных.

уязвимости, кибератаки, угрозы конфиденциальности, вредоносные данные

Важное значение имеют уязвимости, нарушающие конфиденциальность файлов, так как их эксплуатация может привести к утечке защищенной информации, а также нанести значительный ущерб пользователям и организациям. Примером таких уязвимостей являются проблемы в популярных приложениях и библиотеках, таких как libcurl, SoX, ImageMagick, и других. Эти уязвимости позволяют злоумышленникам обходить механизмы защиты, получать доступ к конфиденциальным данным, нарушать их целостность или вызывать отказ в обслуживании. Такие случаи требуют глубокого анализа и своевременного устранения для минимизации рисков [1].

Данная статья посвящена изучению уязвимостей операционных систем на примере Astra Linux Special Edition, выявленных в 2023 году. Рассматриваются механизмы их эксплуатации, последствия атак и методы предотвращения. Особое внимание уделяется уязвимости в пакете ImageMagick, которая остается актуальной даже после официального исправления, а также другим примерам, подтверждающим необходимость системного подхода к защите информации.

Цель исследования является выявление текущих проблем в области защиты конфиденциальности данных, анализ сценариев атак и предлагаемые меры по снижению рисков для пользователей. В рамках исследования рассмотрены как технические аспекты уязвимостей, так и организационные меры, направленные на повышение безопасности.

Уязвимости, связанные с нарушением конфиденциальности файлов, представляют собой серьезную угрозу для информационной безопасности. Эксплуатация подобных уязвимостей может позволить злоумышленникам получить доступ к защищенной информации, обходя механизмы авторизации.

Согласно данным Федеральной службы технического и экспортного контроля, в 2023 году в операционной системе Astra Linux Special Edition было выявлено 77 уязвимостей, из которых 11 можно отнести к категории уязвимо-

стей, нарушающих конфиденциальность файлов. Из этих 11 уязвимостей 5 имели открыто доступные эксплойты. Большинство из них были устранены с помощью обновлений программного обеспечения, однако случаи их эксплуатации продолжают встречаться.

Примеры уязвимостей. Одной из таких уязвимостей является проблема в библиотеке libcurl, связанная с повторным использованием FTP-соединения. Эта уязвимость, обнаруженная 7 марта 2023 года, позволяет злоумышленникам использовать неверные учетные данные при передаче файлов, что может привести к раскрытию защищаемой информации [2]. Другая уязвимость была выявлена в функции start_read() программы обработки звука SoX 2 марта того же года. Она предоставляет злоумышленникам возможность получить доступ к конфиденциальным данным, нарушить их целостность или даже вызвать отказ в обслуживании.

Особое внимание заслуживает уязвимость графического редактора ImageMagick, выявленная 6 февраля 2023 года. Эта проблема связана с ошибками при обработке входных данных и присутствует как в Astra Linux, так и в других операционных системах на базе Unix. Уязвимость позволяет атакующим использовать заранее подготовленные изображения в формате PNG с внедренными в метаданные путями к файлам, доступ к которым требуется получить. На операционных системах Astra Linux это программное обеспечение может быть предустановлено либо установлено из репозитория. Уязвимости в популярном программном обеспечении для обработки данных представляют собой значительную угрозу конфиденциальности информации. В данном исследовании был проведен эксперимент, демонстрирующий эксплуатацию уязвимости в графическом редакторе ImageMagick, обнаруженной 6 февраля 2023 года [3]. Эта уязвимость позволяет злоумышленникам извлекать конфиденциальные данные из системы, используя заранее подготовленные файлы изображений. Эксперимент проводился на операционных системах Astra Linux Смоленск и Орел.

Методика проведения эксперимента

Создание вредоносного изображения. Для демонстрации уязвимости было создано изображение в формате PNG, метаданные которого содержали пути к защищенным файлам системы, таким как /etc/passwd. Использовался специальный скрипт, позволяющий внедрить вредоносные данные в комментарии метаданных файла. Например, путь к файлу добавлялся с использованием команды:

```
exiftool -Comment="path:/etc/passwd" input.png
```

Обработка изображения в ImageMagick. Подготовленное изображение было обработано командой convert из пакета ImageMagick. В процессе обра-

ботки уязвимость позволяла извлечь содержимое указанного файла и внедрить его в выходное изображение «convert input.png output.png». При этом содержимое файла /etc/passwd было преобразовано в шестнадцатеричный формат и внедрено в новый PNG-файл [4].

Извлечение данных из обработанного изображения

Полученное изображение подвергалось анализу, и внедренная информация извлекалась с помощью инструментов для работы с шестнадцатеричным кодом, таких как xxd:

```
xxd output.png > output.hex
```

```
xxd -r -p output.hex > extracted.txt
```

В результате удалось восстановить текстовое содержимое файла, указанного в метаданных исходного изображения.

Результаты эксперимента

Эксперимент подтвердил возможность эксплуатации уязвимости, что иллюстрирует значимость обновлений и дополнительных мер безопасности. В ходе тестирования были получены следующие результаты:

1. Уязвимость успешно воспроизведена на системах Astra Linux Смоленск и Орел;
2. С помощью уязвимого ImageMagick удалось извлечь содержимое системного файла `/etc/passwd`;
2. Вредоносные PNG-файлы корректно проходили обработку, при этом интегрированные данные извлекались без каких-либо предупреждений со стороны системы.

Выводы

Проведенное исследование показало, что даже устраненные уязвимости остаются угрозой, если обновления не внедрены своевременно. Использование уязвимых версий ImageMagick в Astra Linux позволило воспроизвести атаку, которая может быть применена злоумышленниками в реальных условиях. Эксперимент также подчеркнул необходимость контроля за обработкой файлов, особенно в системах, где автоматизация процессов обработки данных является важной частью инфраструктуры [5].

Рекомендации по повышению безопасности

На основании результатов эксперимента были разработаны следующие рекомендации:

1. Обновление ПО. Регулярное применение обновлений для устранения известных уязвимостей;

2. Ограничение прав доступа. Установление строгих политик управления доступом к конфиденциальным файлам;

3. Мониторинг метаданных. Анализ и фильтрация входящих данных, включая метаданные файлов, перед обработкой;

4. Обучение сотрудников. Повышение осведомленности пользователей о возможных угрозах, связанных с обработкой файлов.

Заключение

В данной статье были рассмотрены уязвимости операционных систем на примере Astra Linux Special Edition, а также проведен обзор механизмов их эксплуатации, последствия атак и методы предотвращения.

Результаты эксперимента подчеркивают важность комплексного подхода к информационной безопасности, который включает технические и организационные меры, а также активное обучение пользователей. Уязвимости, подобные описанной, требуют систематической работы над улучшением безопасности как со стороны разработчиков, так и пользователей.

Список используемых источников

1. Кузина В. В., Глумскова И. О. Об особенностях применения операционной системы Astra Linux // Вестник ПГУАС: строительство, наука и образование, 2020. №. 2. С. 93–96.
2. Гринь Д. В. и др. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения astra linux se // Региональная информатика и информационная безопасность, 2017. С. 76–78.
3. Xia Z., Ma L., Cao S. An online image processing approach based on ImageMagick and Imagick //2014 International Conference on Information Science, Electronics and Electrical Engineering. IEEE, 2014. Т. 1. С. 176–180.
4. Уорр К. Надежность нейронных сетей: укрепляем устойчивость ИИ к обману. СПб.: Питер, 2024.
5. Посканный М. В., Косилова Е. А. Анализ защищенности операционной системы Astra Linux Смоленск // Современные информационные технологии и информационная безопасность, 2024. С. 116.

Dombrovskii R., Kosov N. **IMPLEMENTATION OF IMAGE MAGIC VULNERABILITY ON ASTRA LINUX.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In today's digital world, ensuring the privacy of information is becoming one of the key tasks of information security. The growing complexity of software, the expansion of the functionality of operating systems and the continuous growth of cyber attacks make vulnerabilities an important issue for data protection.

Key words: Vulnerabilities, cyber attacks, privacy threats, malicious data.

УДК 004.056.53
ГРНТИ 49.33.29

ОБЗОР АКТУАЛЬНЫХ HONEYPOT-РЕШЕНИЙ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ

В. Е. Дрепа, М. М. Ковцур, Д. А. Красников
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире, где с каждым разом все больше и больше ценных ресурсов и информации переходят в цифровой формат, возрастает необходимость в обеспечении надежной их защиты от несанкционированного доступа к ним с внешней стороны, их целостности и, при этом, доступности для тех, кто имеет права и привилегии на взаимодействие с теми или иными данными. В то время, как большинство компаний используют для подобных целей такие средства, как криптографические средства защиты, различные антивирусные программы и межсетевые экраны (они же брандмауэры или файрволы), среди таковых средств также числятся Honeypot-сервера.

Honeypot, хакеры, вторжение, популярность, кибербезопасность, открытый исходный код

Honeypot – это тип ресурсов информационной безопасности, которые используются в качестве наживки для злоумышленников, чтобы побудить их вторгнуться в сеть для любого незаконного использования. Такие приманки обычно настраиваются для изучения активности злоумышленника в сети, чтобы создавать более надежные средства защиты. Honeypot не несет никаких ценных данных, так как это поддельный хост, который помогает регистрировать сетевой трафик [1].

Затрагивая вопрос классификации Honeypot-систем [2], можно сказать, что на данный момент не существует абсолютно универсального решения, которое использует концепцию Honeypot. Каждое решение удовлетворяет лишь весьма ограниченному количеству задач [3]. Поэтому все существующие на данный момент Honeypot-системы можно классифицировать следующим образом [4]:

1. Комплексные системы развертывания приманок (deception-системы);
2. Веб-приманки:
   – многопротокольные веб-приманки;
   – SSH-приманки;
   – приманки, имитирующие базы данных;
   – RDP;

– электронная почта;

– иные веб-приманки.

3. Приманки для внутренних сетей;
4. Приманки-токены;
5. Другие приманки.

Далее будут представлены сравнительные таблицы обозреваемых решений. Столбец «Степень популярности» представляет собой сумму количества поисковых запросов относительно системы в поисковой системе Яндекс и балла популярности той или иной системы в поисковой системе Google, полученного с помощью сервиса Google Trends за период с 11.10.2024 по 11.11.2024.

ТАБЛИЦА 1. Сравнительный анализ современных Honeypot-решений вида «Deception-системы» с открытым исходным кодом

Honeypot-решение	Запросы в Google	Запросы в Яндекс	Степень популярности
T-Pot	1131	965	2096
OpenCanary	667	17	684
Honeypots	683	–	683
Honeytrap	172	–	172
Community Honey Network	100	–	100

В таблице 1 представлена статистика по поисковым запросам относительно различных deception-систем.

Одного-двух Honeypot-решений может быть недостаточно, особенно если речь идет о защите больших корпоративных сетей. Приманки становятся действительно эффективными, когда их много, тогда киберпреступник быстрее найдет одну из них [5]. Рекомендуется информацию с приманок собирать и анализировать в режиме реального времени. В ответ на этот запрос появились deception-системы – программы для массового развертывания и управления приманками [6].

Информации по поисковым запросам относительно нескольких deception-систем не нашлось, а именно – DejaVU, Ehoney, OWASP Honeypot, DecoyMini, HFish, Chameleon, MHN, opencanary_web и prickly-pete.

В следующих таблицах определены веб-приманки отдельных видов. Здесь перечислены более простые, отдельные Honeypot-решения, которые имитируют веб-сайты и сервисы. Они поддерживают разные протоколы, например, HTTP, HTTPS, FTP, SSH и т. д.

ТАБЛИЦА 2. Сравнительный анализ современных Honeypot-решений вида «Многопротокольные веб-приманки» с открытым исходным кодом

Honeypot-решение	Запросы в Google	Запросы в Яндекс	Степень популярности
DDoSPot	100	–	100
fapro	100	–	100
Dionaea	86	–	86

В таблице 2 представлена статистика по поисковым запросам относительно различных многопротокольных веб-приманок.

В данном списке содержатся решения, работающие с несколькими веб-протоколами одновременно. К таковым также относятся HoneyHTTPD, medusa, Glastopf, SNARE и TANNER, Masscanned, Mimicry, Heralding, Honeydb-agent и Beelzebub, однако по этим продуктам собрать статистику относительно количества поисковых запросов не удалось.

ТАБЛИЦА 3. Сравнительный анализ современных Honeypot-решений вида «SSH-приманки» с открытым исходным кодом

Honeypot-решение	Запросы в Google	Запросы в Яндекс	Степень популярности
Cowrie	586	98	684
SSH Honeypot	293	9	302
Endlessh	252	–	252
pshitt	197	–	197
docker-ssh-honey	100	–	100
ssh-auth-logger	100	–	100

В таблице 3 представлена статистика по поисковым запросам относительно различных SSH-приманок.

К указанным выше решениям также относятся sshesame, Mushorg / Glutton, FakeSSH, ssh-honeypotd и Honeyshell, однако по этим продуктам собрать статистику относительно количества поисковых запросов не удалось.

ТАБЛИЦА 4. Сравнительный анализ современных Honeypot-решений вида «Приманки, имитирующие базы данных» с открытым исходным кодом

Honeypot-решение	Запросы в Google	Запросы в Яндекс	Степень популярности
pg-server	1244	-	1244
mysql-honeypotd	100	-	100
dns.py	-	58	58

В таблице 4 представлена статистика по поисковым запросам относительно различных приманок, имитирующих базы данных.

К указанным выше решениям также относятся RedisHoneyPot и MongoDB-HoneyProxy, однако по этим продуктам собрать статистику относительно количества поисковых запросов не удалось.

Говоря о RDP-приманках, к ним также относятся, такие решения как pyrd и ad-honeypot-autodeploy. Степень популярности pyrd составила 100 баллов, по последнему же информации нет.

Относительно E-mail-приманок можно сказать, что к таковым относятся такие решения как SHIVA Spampot, Honey, imap-honey и Mailoney. Степень популярности Honey – 1216 баллов, по остальным информации нет.

К иным веб-приманкам относятся те Honeypot-решения, которые сложно было сгруппировать по какому-либо общему признаку или определить к одному из вышеупомянутых видов. Для данных решений информации по поисковым запросам нет. К таким решениям были отнесены следующие: portlurker, EoHoneypotBundle, Laravel Application Honeypot, laravel-honeypot, django-honeypot, django-admin-honeypot, Express honeypot, HellPot, honeyup.

ТАБЛИЦА 5. Сравнительный анализ современных Honeypot-решений вида «Приманки для внутренних сетей» с открытым исходным кодом

Honeypot-решение	Запросы в Google	Запросы в Яндекс	Степень популярности
hontel	921	-	921
Conpot	413	6	419
log4j-honeypot-flask	100	-	100

В таблице 5 представлена статистика по поисковым запросам относительно различных приманок для внутренних сетей.

К таковым также относятся Goblin и esp-canary, однако по этим продуктам собрать статистику относительно количества поисковых запросов не удалось.

ТАБЛИЦА 6. Сравнительный анализ современных Honeypot-решений вида «Приманки-токены» с открытым исходным кодом

Honeypot-решение	Запросы в Google	Запросы в Яндекс	Степень популярности
Canarytokens	638	187	825
Honeytoken	645	-	645

В таблице 6 представлена статистика по поисковым запросам относительно различных приманок-токенов.

К таковым также относится SpaceSiren, однако собрать статистику относительно количества поисковых запросов по этому продукту не удалось.

ТАБЛИЦА 7. Сравнительный анализ современных Honeypot-решений вида «Другие приманки» с открытым исходным кодом

Honeypot-решение	Запросы в Google	Запросы в Яндекс	Степень популярности
dshield	1124	21	1145
Fibratus	345	15	360
SentryPeer	100	-	100
miniprint	-	22	22

В таблице 7 представлена статистика по поисковым запросам относительно других приманок.

К таковым также относятся ADBHoney, vmitools, Thug, bluepot и AntiRansom, однако по этим продуктам собрать статистику относительно количества поисковых запросов не удалось.

Из собранной статистики поисковых запросов относительно приведенных в таблице Honeypot-систем можно сделать вывод, что определенные решения уже получили свое признание и обрели свою клиентскую базу, что косвенно указывает на надежность продукта и относительное удобство и комфорт в процессе эксплуатации.

Следовательно, при выборе в будущем honeypot-решения для дальнейшего его использования для определенных целей и непосредственно изучения функционала и устройства honeypot-продукта, целесообразно составить план по изучению и последующему применению отдельных продуктов, а также выразить рекомендацию к дальнейшему изучению приведенных в списке honeypot-систем.

Список используемых источников

1. Подробное руководство по Honeypot. URL: https://habr.com/ru/companies/alexhost/articles/528796/ (дата обращения 09.11.2024).
2. 70+ бесплатных приманок для ловли хакеров. URL: https://habr.com/ru/companies/ bastion/articles/731172/ (дата обращения 09.11.2024).
3. Ковцур М. М., Ахрамеева К. А., Юркин Д. В., Акилов М. В., Сравнительный анализ современных Honeypot решений для корпоративных сетей // Аллея науки, 2020. Т. 1. № 3 (42). С. 768–772.
4. Honeypot, типы и обнаружение. URL: https://habr.com/ru/articles/680056/ (дата обращения 09.11.2024).

5. Красов А. В., Петрив Р. Б., Сахаров Д. В., Сторожук Н. Л., Ушаков И. А. Масштабируемое Honeypot-решение для обеспечения безопасности в корпоративных сетях // Труды учебных заведений связи, 2019. Т. 5. № 3. С. 86–97.
6. 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.

Drepa V., Kovtsur M., Krasnikov D. **OVERVIEW OF CURRENT OPENSOURCE HONEYPOT SOLUTIONS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the modern world, where the amount of valuable resources and information are being transferred to digital format increases really fast, there is an increasing need to ensure reliable protection against unauthorized access to them from the outside, their integrity and, at the same time, accessibility for those who have the rights and privileges to interact with certain data. While most companies use tools such as cryptographic protection tools, various antivirus programs and firewalls for such purposes, Honeypot servers are also listed among such tools.

Key words: Honeypot, hackers, intrusion, popularity, cybersecurity, opensource code.

УДК 004.725.5
ГРНТИ 81.93.29

РАЗРАБОТКА МЕТОДА ФОРМИРОВАНИЯ ОБЩЕГО СЕТЕВОГО КЛЮЧА В ПРОТОКОЛЕ OWE В WI-FI СЕТЯХ

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

Одной из актуальных задач защиты данных в открытых беспроводных сетях является разработка подходов к обеспечению пользователей сетевыми ключами для шифрования и аутентификации. В статье предложен и исследован метод создания общего сетевого ключа для открытых сетей Wi-Fi, основанный на стандарте беспроводного шифрования Opportunistic Wireless Encryption.

Opportunistic Wireless Encryption – OWE, Wi-Fi сети, общий сетевой ключ, шифрование данных, широковещание

С развитием технологий беспроводной связи и увеличением числа пользователей Wi-Fi сетей, вопросы безопасности передачи данных становятся все более актуальными. Традиционные методы аутентификации, такие как WPA2-PSK и более поздние версии алгоритма, требуют от пользователей ввода паролей, что создает определенные неудобства и может подвергать сети рискам.

С целью решения вышеуказанной проблемы совместно с WPA3 Wi-Fi Alliance анонсировал новую технологию Wi-Fi Enhanced Open, основанную на стандарте оппортунистического (беспринципного) беспроводного шифрования (англ. Opportunistic Wireless Encryption, OWE). Являясь продуктом Целевой группы по разработке Интернета (Internet Engineering Task Force, IETF), OWE, указанный в стандарте RFC 8110, определяет расширение стандарта IEEE 802.11 [1].

Основной целью протокола OWE является обеспечение конфиденциальности и целостности данных, передаваемых по открытым Wi-Fi сетям. Это достигается путем выработки ключа шифрования, который используется для защиты передаваемых данных.

По сравнению с традиционными методами, требующими парольной аутентификации, OWE обеспечивает расширенную безопасность для открытых незащищенных сетей. Без предварительного согласования или обмена учетными данными OWE автоматически устанавливает шифрование без аутентификации при поддержке устройством. Таким образом пользователи

могут пользоваться преимуществами повышенной конфиденциальности без необходимости дополнительных действий [2].

Работа протокола OWE представлена на рис. 1 [3].

Рис. 1. Схема работы протокола OWE

Протокол OWE не предусматривает наличие множественного шифрования. В процессе установления соединения между точкой доступа и клиентом генерируются ключи для обеспечения безопасности информации, передаваемой по открытому каналу связи. Этот канал устанавливается только между AP (access point) и пользователем. Однако возникает необходимость в наличии общего зашифрованного канала для обмена данными между большим количеством пользователей. На данный момент протокол OWE не реализует указанную систему шифрования, тем самым ограничивая ресурсы пользователей.

Другими словами, протокол OWE позволяет получить защищенную парную связь с использованием современного оборудования, но при том ограничивает организацию множественной защищенной сети или широковещания. Потому в целях обеспечения безопасности и надежности беспроводных сетей, требуется дальнейшее совершенствование протокола OWE – разработка нового метода.

Предлагаемый метод заключается в разработке сетевого ключа для группы пользователей открытой Wi-Fi сети с целью защищенной передачи данных. Для дальнейшего описания метода было предложено соответствующее название – DKE-OWE – Decentralize Key Exchange based Opportunistic Wireless Encryption; дословно переводится как децентрализованное шифрование с обменом ключами на основе протокола OWE.

Каждый пользователь группы выполняет следующие операции:

1. Генерирует секретный (закрытый) ключ случайным образом;

2. Формирует общедоступный (открытый) ключ на основе секретного ключа;

3. Обменивается открытыми ключами с пользователями, являющимися членами группы, и составляет вспомогательные функции (все передаваемые данные шифруются пользователем и точкой доступа с помощью протокола OWE);

4. Генерирует общий сетевой ключ;

5. Осуществляет проверку корректности сформированного ключа.

Каждый этап генерации общего сетевого ключа разберем отдельно.

Генерация ключей

Перед выполнением метода пользователи согласуют открытые параметры:

– примитивный элемент поля $g \in GF(p)$;

– модуль p, по которому буду происходить вычисления, p – простое число.

Пользователь случайным образом генерирует закрытый ключ x_i, где $i = 1, 2, \ldots, n$, n – количество пользователей в группе, $x \in \{1, \ldots, p - 1\}$. Для составление открытого ключа X пользователь пользуется формулой:

$$X_i = g^{x_i} \bmod p,$$

где X_i – открытый ключевой параметр, g – примитивный элемент поля Галуа, $GF(p)$, x_i – случайно генерируемый параметр.

Значение X_i передается членам группы для дальнейших вычислений. Передача осуществляется путем отправки X_i точке доступа, которая в свою очередь отправляет данное значение другим пользователям группы. Секретный (закрытый) ключ x_i хранится у пользователя и раскрытию не подлежит.

Формирование вспомогательных функций

С помощью полученных от всех участников группы параметров i-й пользователь вычисляет вспомогательные функции y_i ($i = 1, 2, \ldots, n$) по формуле:

$$y_i = \begin{cases} 1 \big/ \prod_{j=2}^{n} X_j, \text{при } i = 1 \\ \prod_{j=1}^{i-1} X_j \Big/ \prod_{j=i+1}^{n} X_j, \text{при } 2 \le i \le n-1 \\ \prod_{j=1}^{n-1} X_j, \text{при } i = n \end{cases}$$

Получившиеся вспомогательные функции y_i пользователь хранит до момента проверки корректности созданного общего сетевого ключа.

Составление сетевого ключа

Генерирование общего сетевого ключа происходит на стороне пользователя группы по следующей формуле:

$$(\prod_{i=1}^{n} U_i)\ mod\ p = \prod_{i=1}^{n} {y_i}^{x_i} * g^{k_i}\ mod\ p.$$

Каждый пользователь вычисляет величину U_i:

$$U_i = {y_i}^{x_i} * g^{k_i}\ mod\ p,$$

и посылает получившееся значение через точку доступа другим членам группы.

Используя вышеуказанные формулы и математические свойства степеней, сократим и запишем новое выражение:

$$(\prod_{i=1}^{n} U_i)\ mod\ p = \prod_{i=1}^{n} {y_i}^{x_i} * g^{k_i}\ mod\ p = g^{\sum_{i=1}^{n} k_i}\ mod\ p.$$

Отсюда получаем, что формирование общего сетевого ключа W в открытых Wi-Fi сетях происходит по формуле:

$$W = g^{\sum_{i=1}^{n} k_i}\ mod\ p.$$

Для проверки корректности вычисленного ключа каждый пользователь группы будет использовать формулы и сравнивать получившиеся значения. При совпадении значений пользователь сможет начать шифрование и обмен информацией с помощью сгенерированного ключа. В противном случае, вычисления будут сброшены и начаты заново.

Таким образом, разработка метода формирования общего сетевого ключа в протоколе OWE представляет собой важный шаг в обеспечении безопасности открытых Wi-Fi сетей. Протокол OWE позволяет пользователям подключаться к сети без необходимости ввода паролей, при этом обеспечивая защиту передаваемых данных с помощью современных криптографических методов. Тем не менее, необходимо учитывать его ограничения, такие как отсутствие аутентификации и зависимость от надежности используемых алгоритмов.

Целесообразно продолжить исследование предлагаемого метода с целью оптимизации его параметров для обеспечения требуемого уровня безопасности в беспроводных сетях.

Список используемых источников

1. Wi-Fi CERTIFIED Enhanced Open™: Transparent Wi-Fi® protections without complexity // Wi-Fi Allience URL: https://www.wi-fi.org/beacon/dan-harkins/wi-fi-certified-enhanced-open-transparent-wi-fi-protections-without-complexity (дата обращения 10.11.24).
2. Opportunistic Wireless Encryption…Um, What's That Again? // NETWORKWORLD. URL: https://www.networkworld.com/article/966750/opportunistic-wireless-encryption-um-what-s-that-again.html (дата обращения 05.11.24).
3. IETF RFC 8110: Opportunistic Wireless Encryption (OWE), 2017. URL: https://data-tracker.ietf.org/doc/html/rfc8110 (дата обращения 09.11.2024).

Zhuravleva A. **DEVELOPMENT OF A METHOD FOR GENERATING A COMMON NETWORK KEY IN THE OWE PROTOCOL IN WI-FI NETWORKS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

One of the urgent tasks of data protection in open wireless networks is the development of approaches to provide users with network keys for encryption and authentication. The paper proposes and investigates a method of creating a common network key for open Wi-Fi networks based on the Opportunistic Wireless Encryption standard.

Key words: Opportunistic Wireless Encryption – OWE, Wi-Fi networks, shared network key, data encryption, broadcasting.

УДК 004.056.5
ГРНТИ 81.93.29

ИДЕЯ СТРАТЕГИИ ОБНАРУЖЕНИЯ УГРОЗ НА БАЗЕ КОНЦЕПЦИИ DETECTION ENGINEERING

Р. Р. Исмаилов, М. А. Спицын
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Организации сталкиваются с растущим количеством и сложностью угроз, которые требуют новых подходов и пересмотров решений по их обнаружению и предотвращению. Нужна во внедрении облачных инфраструктур также является актуальной. Анализ существующих подходов к обнаружению угроз показывает, что традиционные методы, основанные на готовых решениях вендоров, не всегда способны оперативно адаптироваться к новым угрозам и специфическим требованиям организаций. Концепция Detection Engineering представляет собой новаторский подход к разработке и управлению правилами обнаружения угроз, так как обнаружение, как явление, создается и поддерживаются как программный код с использованием современных практик разработки. Внедрение этой концепции позволяет организациям повысить эффективность обнаружения угроз, автоматизировать процессы тестирования и валидации правил, обеспечить безопасность облачной инфраструктуры. В данной статье рассматривается комплексный подход к разработке стратегии обнаружения угроз, основанный на принципах Detection Engineering, включающий методологические основы и практические рекомендации по внедрению.

обнаружение как код, инженерия обнаружения, облачная безопасность, анализ среды, обнаружение угроз, корпоративная безопасность

В условиях турбулентности в области безопасности важно сохранить концентрацию на важных задачах для сохранения хороших позиций. Во времена непростых этапов для страны, традиционные подходы к обнаружению угроз все чаще не справляются со сложными угрозами и подготовленными компьютерными атаками. Хотя традиционные системы защиты информации и управления событиями (SIEM), антивирусные решения и системы предотвращения вторжений (IPS/IDS), десятилетиями служили основой кибербезопасности, они часто опираются на жесткие, основанные на правилах методологии, которые с трудом справляются с современными направлениями атак. Эти традиционные парадигмы, которые разработаны для упрощения анализа угроз, оказываются недостаточными для обнаружения и реагирования на продвинутые постоянные угрозы (APT) или бестелесные вредоносные программы.

Также появление облачных сред, распределенной рабочей силы и сложных гибридных инфраструктур коренным образом изменило поверхность

атаки, потребовав более гибкого и программного подхода к обнаружению угроз. Для того, чтобы облачный IaaS (Infrastructure as a Service, Инфрастурктура как услуга) использовался полноценно, необходимо обратить внимание на соответствие этой инфраструктуры приказам ФСТЭК 21 и 17, 152-ФЗ. Тем не менее перечень требований регулятора в полной мере не может гарантировать беспроигрышную безопасность активов, так как традиционный метод ручного обновления сигнатур и правил, хотя и сохраняет свою ценность, не может быть масштабирован для решения задач, связанных с современными угрозами, которые часто используют законные инструменты и процессы, чтобы избежать обнаружения. Это создало острую потребность в более динамичном и управляемом кодом подходе к обнаружению угроз, который может адаптироваться так же быстро, как развиваются сами угрозы.

Авторами [1] подчеркивается важность использования процессного подхода для систем управления информационной безопасностью. Как подчеркивается в статье, информация представляет собой один из самых главных бизнес-активов любой организации, имеющим ценность для организации, находящимся в ее распоряжении и обеспечивающим добавочную стоимость и вследствие этого нуждающимся в защите. Этот тезис напрямую связан с необходимостью модернизации подходов к обнаружению угроз, ведь управление рисками строится исходя из контекста и масштаба СУИБ, а они в свою очередь базируются на инвентаризации всех активов компании, в т.ч. информации. Рассмотренные авторами выше основные вопросы управления информационной безопасностью, в настоящее время, требуют обновления применяемых методик.

В контексте Detection Engineering это означает необходимость внедрения программного подхода к обнаружению угроз как части общей системы управления информационной безопасностью. Это соответствует описанному в статье [1] процессному подходу, где к управлению ИБ применим процессный подход, который распространяется на разработку, реализацию, эксплуатацию, мониторинг, анализ, сопровождение и совершенствование СУИБ организации.

Зарубежная исследовательская компания Gartner в трендах на 2024 год [2] выделяет понятие continuous threat exposure management (CTEM, непрерывный контроль и управление угрозами) и платформы отраслевых облаков, а в 2025 [3] окружающий невидимый интеллект, в смысле использования небольших меток и сенсоров для отслеживания местоположения и состояния различных объектов т. е. активов. Затем такая информация отправляется в облако для анализа и ведения учета. Такой тренд решает вопрос asset management, но также интересен, в рамках контекста detection as code, так как метки и сенсоры – есть код.

Detection engineering – это концепция, перешедшая как термин из DevOps, которая представляет собой современный подход к обнаружению угроз, посредством интеграции механизмов обнаружения в виде кода, описывает автор [4] книги. В данном материале, в принципе, свежий взгляд на автоматизацию, и на проблемы, рассмотренные в материалах [1–3]. Автор [4] описывает жизненный цикл обнаружения как код, выделяя 5 этапов, иллюстрация которых ниже, на рисунке 1. Автор утверждает, что нехватка привязки к жизненному циклу ведет к пробелам в обнаружении. Несмотря на то что, каждая организация уникальна, их жизненный цикл обнаружения должен включать следующие шаги:

1) определение требований;
2) разработка;
3) тестирование;
4) внедерение (имплементация);
5) вывод из эксплуатации (депрекация).

Рис. 1. Жизненный цикл обнаружения

Современные методы обеспечения информационной безопасности выковываются ничем иным как нависшими угрозами. Как следствие лучшими практиками по защите информации активов компании будет следование трендам информационной безопасности [2-3].

Актуальным трендом для России, российского ИБ в целом, будет использование базы знаний, имеется в виду threat intelligence, vulnerability database, YARA, Sigma, etc. База знаний в сочетании со общепринятыми стандартами и методологией MITRE [5] позволит добиться стандартизации таксономии.

Освещение проблемы концептуализации требований обнаружения как код нашло отражение в материале [4], установив жизненный цикл для случаев использования обнаружения, следующим шагом, по мнению автора, является определение технических систем, которые необходимы для эффективного внедрения на масштабируемом уровне. Непрерывная интеграция/непрерывное развертывание (CI/CD) играет важную роль. Автором выделяется 5 компонентов:

1. Системы управления версиями (с CI-агентами). Отслеживание изменений, совместной работы и версионное управление;

2. Поддержка API. Обеспечение бесшовной интеграции с различными инструментами и платформами безопасности;

3. Синтаксис случаев использования. Стандартизированный формат для написания правил обнаружения;

4. Инструменты тестирования. Проверка эффективности правил обнаружения на отсутствие лишнего шума;

5. Управление секретами. Защита API-ключей или учетных данных.

Чтобы защитить бизнес-активы в облачных средах, организациям необходимо внедрить новые методы, возможности и инструментарий. Традиционные средства контроля безопасности, основанные на изоляции компьютера и предсказуемом состоянии системы, неэффективны. Detection Engineering способен эффективно поддерживать облачные системы, подмечает автор [6]. На практике внедрение Detection Engineering требует интегрированную инфраструктуру, представленную на рисунке 2.

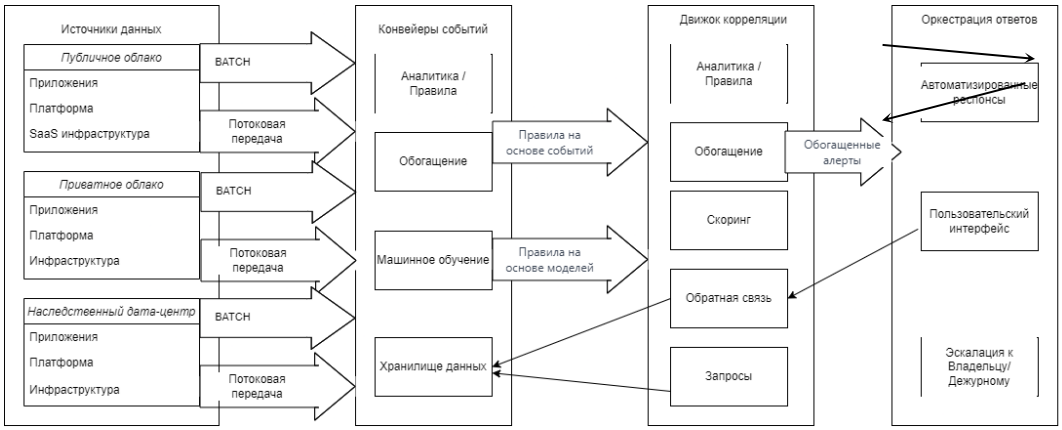


Рис. 2. Инфраструктура Detection Engineering

Использование концепции Detection Engineering позволит организациям адаптироваться к изменениям в области безопасности и масштабировать процессы обнаружения. При планировании автоматизации важно учитывать несколько ключевых аспектов: анализ инфраструктуры и источников данных для полного покрытия систем, выявление критических типов атак на основе профиля угроз организации, создание и приоритизация правил на основе оценки рисков, определение метрик эффективности обнаружения.

По мере того как организации переходят к облачным системам, безопасность должна эволюционировать, достигая большей согласованности с технологическим стеком и подходом DevOps. Это означает создание непрерывных контуров безопасности, которые сопутствуют непрерывным контурам разработки, присущим облачной экосистеме.

Инженерия обнаружения – один из способов, с помощью которых организации могут обеспечить как облачную безопасность, так и значительно повысить эффективность обнаружения угроз, автоматизировать процессы тестирования и валидации правил, а также обеспечить прозрачность, воспроизводимость результатов, даже в условиях постоянной эволюции угроз. В виду того, что он обеспечивает согласованность правил во всей инфраструктуре, а также масштабируемость решений по мере роста организации.

Список используемых источников

1. Виткова Л. А., Дудникова М. Н., Петрова А. Н. Вопросы управления информационной безопасностью // Актуальные проблемы инфотелекоммуникаций в науке и образовании VII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. С. 143–146.
2. Gartner Top 10 Strategic Technology Trends for 2024 // Gartner. URL: https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2024 (дата обращения 01.11.2024).
3. Gartner Top 10 Strategic Technology Trends for 2025 // Gartner. URL: https://www.gartner.com/en/articles/top-technology-trends-2025 (дата обращения 01.11.2024).
4. Chow D. Automating Security Detection Engineering / Chow D. – Birmingham, UK: Packt Publishing Ltd, 2024. 251 p.
5. ATT&CK Matrix for Enterprise // MITRE ATT&CK. URL: https://attack.mitre.org/ (дата обращения 01.11.2024).
6. Lewis J., Wang C. Chaos Engineering: New Approaches To Security // A Rain Capital Research Note. 2018.

Ismailov R., Spitsyn M. **THE IDEA OF A THREAT DETECTION STRATEGY BASED ON THE DETECTION ENGINEERING CONCEPT.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Organizations face an increasing number and complexity of threats that require new approaches and revisions to their detection and prevention solutions. The need for implementation in cloud infrastructures is also relevant. Analysis of existing threat detection approaches shows that traditional methods based on vendor-ready solutions are not always able to quickly adapt to new threats and specific organizational requirements. The concept of Detection Engineering represents an innovative approach to developing and managing threat detection rules, as detection, as a phenomenon, is created and maintained as program code using modern development practices. The implementation of this concept allows organizations to improve the effectiveness of threat detection, automate testing and validation processes, and ensure cloud infrastructure security. This article examines a comprehensive approach to developing a threat detection strategy based on Detection Engineering principles, including methodological foundations and practical implementation recommendations.

Key words: detection-as-code, detection engineering, cloud security, environment analysis, threat detection, enterprise security.

УДК 004.432.2
ГРНТИ 81.93.29

МЕТОДЫ ВЫЯВЛЕНИЯ ВРЕДОНОСНОГО КОДА В РЕПОЗИТОРИЯХ ПАКЕТНЫХ МЕНЕДЖЕРОВ ДЛЯ ЯЗЫКОВ ПРОГРАММИРОВАНИЯ

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

В условиях растущей зависимости разработчиков от сторонних библиотек и инструментов, использование пакетных менеджеров становится обычной практикой, однако это также создает уязвимости для внедрения вредоносного кода. В данной работе проведен сравнительный анализ ряда коммерческих и открытых инструментов, предназначенных для обнаружения потенциально опасного кода

открытые репозитории, вредоносный код, пакетный менеджер

Пакетные менеджеры и публичные репозитории играют ключевую роль в современном программировании, особенно в экосистеме разработки программного обеспечения. Они позволяют разработчикам эффективно управлять зависимостями, упрощают процесс установки, обновления и удаления библиотек и модулей, необходимые для работы проектов. Публичные репозитории предоставляют доступ к множеству готовых решений, что значительно ускоряет процесс разработки и способствует распространению открытого кода.

Возросшая популярность использования открытого кода в своих проектах привлекает злоумышленников, создавая угрозы для безопасной разработки. Доставка вредоносного кода через сторонние зависимости стала одним из опасных способов заражения.

Основные источники такого ВПО – репозитории с пакетами для разработки такие, как npm для JavaScript, PyPI, NuGet и т. д. Например, злоумышленники могут создавать пакеты, которые на первый взгляд выглядят легитимными, но на самом деле содержат уязвимости или вредоносный код. Для распространения пакетов с вредоносным кодом используют такие методы, как [0]:

1. Тайпсквоттинг (англ. typosquatting) – это практика получения известного имени с небольшой опечаткой. Злоумышленники регистрируют эти вредоносные пакеты в популярных репозиториях пакетов. Например, в репозито-

рии PyPI были обнаружены вредоносные пакеты `requesys`, `requesrs` и `requesr`, которые выдавали себя за популярный пакет `requests`;

2. Перехват программного пакета довольно непростая задача, она очень эффективна, поскольку позволяет использовать популярность доступных пакетов для высокого уровня заражения;

3. Путаница зависимостей – использует уязвимость в том, как многие менеджеры пакетов загружают зависимости во время процесса сборки. В методе путаницы зависимостей злоумышленник использует определенные имена внутренних пакетов цели и публикует вредоносный пакет во внешнем общедоступном репозитории с точным именем. Затем злоумышленник присваивает этому опубликованному пакету очень высокий номер версии. Большинство менеджеров пакетов по умолчанию предпочитают загружать внешний вредоносный пакет из-за его высокого номера версии, а не загружать младшую версию из законного внутреннего репозитория;

4. Обфускация – процесс приведения программного кода к виду, сохраняющему ее функциональность, но затрудняющему анализ и чтение. Используется совместно с предыдущими пунктами как способ скрытия вредоносного кода от явного обнаружения программистом.

Данные методы можно используются злоумышленниками для распространения вредоносного кода через популярные реестры пакетных менеджеров языков программирования: npm, PyPI, NuGet, Maven. Большинство из них не используют активные методы для предотвращения публикации пакетов с вредоносным кодом. Так у PyPI есть система выявления вредоносного кода Malware Checks, но ее правила детектирования лежат в исходном коде проекта, и обойти их достаточно просто. Сама система при этом не является блокирующей: сигналы приходят на почту администраторам, после чего они проверяют код пакета и принимают решение о блокировке. В то время как в npm присутствует проблема как “Manifest confusion” [2]. В основном пакетные менеджеры и реестры ограничиваются сканерами уязвимостей для предупреждения пользователей об их наличии в пакетах, как в Maven используется OWASP Dependency-Check.

Отсутствие способов обнаружения вирусов у разработчиков пакетных менеджеров и обнаружения новых пакетов с вредоносным кодом [3] подтолкнуло компании и различные группы программистов на реализацию своего ПО, решающий возникшую проблему. На рынке есть как платные, так и бесплатные продукты:

1. Package Analysis от Open Source Security Foundation (OpenSSF) запуск пакета в изолированной среде для изучения поведения, большой датасет пакетов npm, pypi, packagist PHP, rubygems. Из проведенного анализа можно ска-

зать, что потенциал использования данного ПО и датасета [4] помогает отслеживать обновления пакетов, следить за их поведением, например, какие консольные команды выполняются, с какими файлами взаимодействуют, а также сетевые подключения, которые можно использовать для утечки конфиденциальных данных или обеспечения удаленного доступа [5];

2. Mend SCA – совместно со статическим анализом кода использует алгоритмы машинного обучения и эвристические методы для обнаружения потенциально вредоносных конструкций в коде. Интеграция CI/CD и возможность блокировать вредоносные пакеты позволяют своевременно устранять уязвимости продукта [6];

3. PyAnalysis – данный продукт для анализа Python пакетов отечественного разработчика ПО и сервисов для кибербезопасности Positive Technologies. Реализован в виде веб-интерфейса и API запросом к системе. Отправить можно название пакета и его версию или ссылку на проект в GitHub. В ответ получаем результат анализа пакета, оценку его опасности: clean, suspicious, malicious. В качестве ответа также можно получить релизы репозитория, посмотреть исходный код и т. д. [7];

4. Xygeni – анализ зависимостей программного обеспечения для контроля компонентов с открытым исходным кодом, собственных и сторонних компонентов, используемых в цепочке поставок программного обеспечения. Сюда входит обнаружение компонентов, обнаружение распространенных атак на зависимости, таких как опечатки или путаница в зависимостях, а также расширенное управление SBOM. Как только новые пакеты публикуются, Xygeni проводит сканирование в режиме реального времени для обнаружения и блокировки вредоносного ПО на основе анализа поведения кода. Подходит для многих популярных пакетных менеджеров и их реестров пакетов [8];

5. Jfrog Xray – сканирует пакеты, рекурсивно просматривая уровни зависимостей, чтобы обнаружить проблемы и уязвимости на любой глубине. Имея постоянно обновляемую базу данных вредоносных пакетов [9] и вирусов, позволяет Xray быстро анализировать и реагировать. Интеграция SBOM позволяет инженерам DevSecOps управлять, понимать и анализировать зависимости своих компонентов [10].

Для рассмотренных решений была построена сравнительная таблица 1.

ТАБЛИЦА 1. Сравнение готовых решений

Особенности	Готовое решение				
	Package Anlysis	Mend SCA	Jforg Xray	XyGeni	PyAnalysis
Распространение	Открытое ПО	Платно	Платно	Платно	Платно
Пакетные менеджеры	npm, pypi, packagist PHP, rubygems и т. д.				PyPI
Способы анализа	SAST, анализ лицензии, анализ зависимостей	SAST, анализ лицензии, анализ зависимостей	Способы анализа	SAST, анализ лицензии, анализ зависимостей	SAST, анализ лицензии, анализ зависимостей
Наличие SBOM	-	+	Наличие SBOM	-	+

Разнообразный функционал данных готовых решений позволят команды разработчиков выбрать походящее решение для своего продукта. Package Analysis распространяется как открытое ПО, которым может пользоваться любая команда, которые является преимуществом перед остальными продуктами, которые предлагают полный функционал в виде подписки и разового платежа. Наличие SBOM является преимущество при выборе ПО, в случае, когда разрабатывается крупный проект, что позволяет упростить отслеживание и анализ установленных зависимостей [11].

Помимо уже готовых решений, разработчик может самостоятельно обеспечить безопасность своего продукта и своих данных. Следить какие пакеты устанавливаешь на официальных сайтах пакетных менеджеров, исключить ручной ввод названия пакетов, постоянное обновление пакетов, использовать спецификации SBOM на проекте [12].

В результате были изучены методы компрометации открытых репозиториев, готовые программные решения для поиска и анализа загружаемых пакетов. Дальнейшим развитием является изучение основных потребностей программистов, использующих открытые репозитории в своих проектах, и создание собственного решения для сканирования и анализа устанавливаемых пакетов, с учетом существующих технологий и методов обнаружения вредоносных пакетов [13] и особенностей, описанных раннее продуктов.

Список используемых источников

1. Jfrog: Five Examples of Infection Methods Attackers Use to Spread Malicious Packages. URL: https://jfrog.com/blog/five-examples-of-infection-methods-attackers-use-to-spread-malicious-packages/#Dependency-Confusion (дата обращения 01.11.2024).
2. Jfrog: NPM manifest Confusion: Six Month Later. URL: https://jfrog.com/blog/npm-manifest-confusion-six-months-later/ (дата обращения 10.11.2024).
3. Хакер: Из npm удалено еще 25 вредоносных пакетов. URL: https://xakep.ru/2022/02/24/more-npm-malware/ (дата обращения 10.11.2024)
4. Package Analysis: Package Analysis Dataset. URL: https://console.cloud.google.com/bigquery?d=packages&p=ossf-malware-analysis&t=analysis&page=table&project=mentorit-kogo&ws=!1m4!1m3!3m2!1sossf-malware-analysis!2spackages (дата обращения 11.11.2024).
5. Package Analysis. URL: https://github.com/ossf/package-analysis (дата обращения 01.11.2024).
6. Mend.io: Mend SCA Documentation. URL: https://docs.mend.io/platform/latest/mend-sca (дата обращения 01.11.2024)
7. Positive Technologies: PT PyAnalysis. URL: https://www.ptsecurity.com/ru-ru/services/pt-pyanalysis/?utm_source=habrpt&utm_medium=article&utm_campaign=pt-pyanalysis&utm_content=article-09 (дата обращения 01.11.2024).
8. Xygeni: Xygeni User Guides. URL: https://docs.xygeni.io (дата обращения 01.11.2024)
Jfrog: Malicious Packages. URL: https://research.jfrog.com/malicious-packages/ (дата обращения 01.11.2024).
9. Jfrog: Jfrog Help Center: Jfrog Xray Documentation. URL: https://jfrog.com/help/r/jfrog-security-documentation/jfrog-xray (дата обращения 01.11.2024).
10. Habr: (Не)безопасная разработка: как выявить вредоносный Python-пакет в открытом ПО. URL: https://www.securitylab.ru/blog/company/pt/352704.php (дата обращения 01.11.2024).
11. Scribe Security: Спецификация программного обеспечения (SBOM). URL: https://scribesecurity.com/ru/sbom/ (дата обращения 11.11.2024).
12. Овчаров В. А., Подшибякин А. С., Харжевская А. В., Шинкаренко А. Ф. Технология идентификации вредоносных пакетов в задачах аудита уязвимостей прикладных программных решений // Труды Военно-Космической Академии имени А. Ф. Можайского. 2023. № 686. С. 106–122.

Kalmykov A. **METHODS FOR DETECTING MALICIOUS CODE IN PACKAGE MANAGER REPOSITORIES FOR PROGRAMMING LANGUAGES.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

With developers increasingly dependent on third-party libraries and tools, the use of package managers is becoming common practice, but it also creates vulnerabilities for the introduction of malicious code. In this paper, a comparative analysis of a number of commercial and open source tools designed to detect potentially dangerous code is carried out.

Key words: open repositories, malicious code, package manager.

УДК 004.056
ГРНТИ 20.53.17

РАЗРАБОТКА ЗАЩИЩЕННОГО МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ ХРАНЕНИЯ ДАННЫХ ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID

М. М. Ковцур, Е. В. Коренюгин, М. В. Яссер
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья посвящена разработке мобильного приложения для операционной системы Android, предназначенное для защищенного хранения файлов пользователей. Приложение реализует методы шифрования с использованием AES, что позволяет обеспечить высокий уровень безопасности данных. Разработанное приложение включает функции шифрования, дешифрования, добавления, просмотра и удаления файлов, а также содержит удобный и интуитивно понятный интерфейс.

информационная безопасность, защищенное хранилище, криптография, шифрование, мобильные приложения

В настоящее время, с развитием отечественных технологий и увеличением объемов хранимой информации, возрастают требования к безопасности данных, особенно на мобильных устройствах. Мобильные платформы, такие как Android, широко используются для хранения личной и корпоративной информации, что делает их мишенью для атак. В связи с этим разработка приложений, обеспечивающих высокий уровень защиты данных, становится все более актуальной.

Для достижения поставленных целей была разработана система, включающая в себя несколько ключевых компонентов и реализующая весь необходимый набор функций для обеспечения безопасности пользовательских данных. Рассмотрим подробно функциональные возможности и архитектуру приложения [1].

Разработанное приложение представляет собой мобильное приложение для операционной системы Android, предназначенное для безопасного хранения файлов пользователей, используя базу данных SQLite. Одной из первых функций является просмотр файлов изображения, которую можно использовать прямо в приложении, не раскрывая их на устройстве. Это значит, что фотографии или документы не будут оставаться в открытом виде, снижая риск утечки информации. Когда файл больше не нужен, его можно удалить навсегда, без возможности восстановления. Таким образом, полное удаление, минимизирует риск попадания файлов в чужие руки.

Интуитивный интерфейс приложения адаптирован, чтобы его использование было максимально простым и удобным. Даже если пользователь впервые пользуется подобным сервисом, разобраться в нем будет легко, а риск ошибок минимален.

Архитектура приложения построена на модульном подходе, изображенная на рис. 1, что делает приложение гибким и легким в поддержке. Каждый модуль отвечает за свою часть функционала, и все они работают вместе, обеспечивая надежную защиту данных.

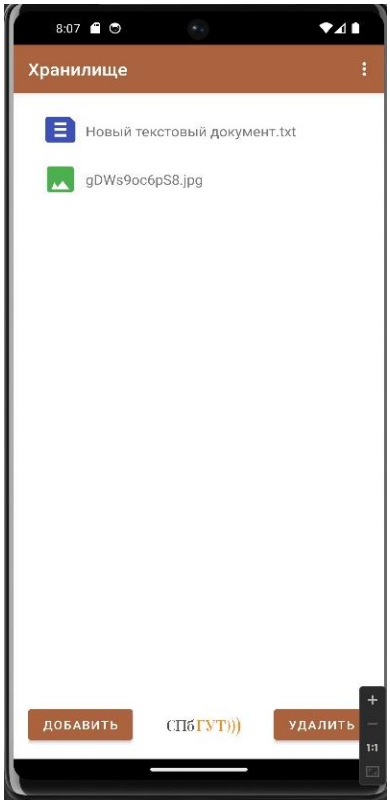


Рис. 1. Демонстрация главного экрана приложения

Главный экран – это основной экран приложения, где пользователь при добавлении файлов шифрует, и при просмотре дешифрует файлы. Модуль шифрования отвечает за защиту данных, которые хранятся в базе данных SQLite. Именно здесь происходит шифрование и дешифрование файлов с использованием алгоритма AES [2]. Адаптер файлов помогает отображать список файлов в удобном виде. Благодаря этому модулю пользователи могут легко выбирать нужные документы для дальнейших действий, будь то добавление, просмотр или удаление. Модуль аутентификации защищает доступ к приложению, предлагая пользователю пройти проверку сначала с помощью логина и пароля, а далее с помощью PIN-кода. Это дополнительный уровень безопасности, который, наряду с методами защиты от декомпиляции и анализа байт-кода [3], гарантирует, что доступ к зашифрованным файлам получат только авторизованные пользователи. Экран загрузки приветствует пользова-

теля логотипом и названием приложения при запуске, создавая приятное первое впечатление и плавный переход к экрану аутентификации.

Ключевая особенность безопасности приложения – это использование современных криптографических методов. Алгоритм прошел тщательное тестирование и доказал свою надежность даже в условиях интенсивных попыток взлома [4].

В проекте внедрены различные методы защиты данных, которые помогают сохранить конфиденциальность файлов пользователей.

Одним из таких методов является EncryptedSharedPreferences для безопасного хранения ключа шифрования, который в дальнейшем используется для защиты пользовательских данных. Это специальный класс, представленный на рис. 2, предоставляемый Android API, который автоматически шифрует данные, сохраняемые в SharedPreferences. Далее, к примеру, пароль шифруется с использованием этого ключа при помощи алгоритма AES, что гарантирует аутентифицированное шифрование и защиту данных.

```
16      // Метод для получения или генерации ключа шифрования
17      fun getEncryptionKey(context: Context): String {
18          // Создаем или получаем мастер-ключ
19          val masterKey = MasterKey.Builder(context)
20              .setKeyScheme(MasterKey.KeyScheme.AES256_GCM)
21              .build()
22
23          // Создаем EncryptedSharedPreferences для безопасного хранения ключа
24          val sharedPreferences = EncryptedSharedPreferences.create(
25              context,
26              SHARED_PREFS_FILE,
27              masterKey,
28              EncryptedSharedPreferences.PrefKeyEncryptionScheme.AES256_SIV,
29              EncryptedSharedPreferences.PrefValueEncryptionScheme.AES256_GCM
30          )
31
32          // Пытаемся получить сохраненный ключ шифрования
33          return sharedPreferences.getString(KEY_ALIAS, null) ?: generateAndStoreKey(sharedPreferences)
34      }
35
36      // Метод для генерации и сохранения нового ключа шифрования
37      private fun generateAndStoreKey(sharedPreferences: SharedPreferences): String {
38          // Генерируем случайный ключ длиной 256 бит
39          val generatedKey = ByteArray( size: 32).also { SecureRandom().nextBytes(it) }
40          val keyAsString = Base64.encodeToString(generatedKey, Base64.DEFAULT)
41
42          // Сохраняем ключ в SharedPreferences
43          sharedPreferences.edit().putString(KEY_ALIAS, keyAsString).apply()
44
45          return keyAsString
46      }
47
48  }
```

Рис. 2. Реализация шифрования паролей

Шифрование данных на устройстве – все файлы зашифровываются непосредственно на самом устройстве пользователя перед их сохранением. Это значит, что даже если кто-то попытается перехватить данные во время передачи, они все равно останутся зашифрованными и нечитабельными [5].

Что касается визуальной части, интерфейс приложения был создан с учетом современных принципов UX/UI-дизайна, чтобы сделать использование

приложения максимально удобным и приятным. Экран загрузки, изображенный на рис. 3, приветствует пользователя логотипом и названием приложения, создавая плавный и профессиональный переход к дальнейшей работе. Экран аутентификации – перед тем как получить доступ к файлам, пользователю нужно подтвердить свою личность, введя логин и пароль, далее с помощью PIN-кода. Главный экран показывает список всех файлов, находящихся в защищенном хранилище. Пользователь может быстро выбрать нужный файл и провести с ним любую операцию. Экран просмотра файлов обеспечивает возможность безопасного открытия изображений без предварительного их расшифрования на устройстве. Такой подход значительно уменьшает вероятность несанкционированного доступа к данным. Дополнительно приложение активно взаимодействует с пользователем через уведомления и диалоговые окна: они информируют о ходе выполнения задач, запрашивают подтверждение действий и сигнализируют об ошибках. Это позволяет пользователю быть в курсе всех ключевых событий и изменений в приложении, сохраняя уверенность в его работе.

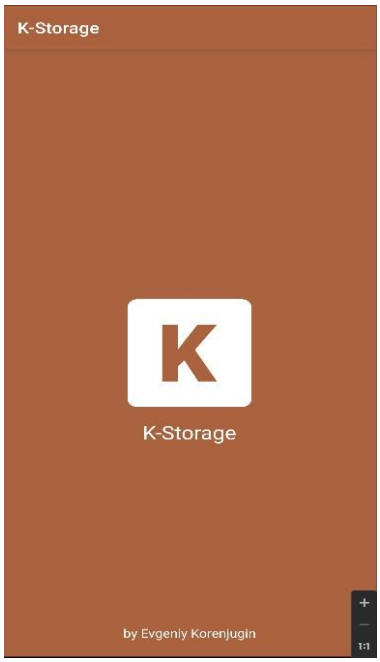


Рис. 3. Activity загрузки приложения

Для подтверждения корректности работы и надежности защиты данных в приложении были проведены разносторонние испытания.

Функциональное тестирование охватило ключевые возможности: добавление файлов, их безопасный просмотр и полное удаление. Проверка проводилась на нескольких моделях Android-устройств с различными версиями операционной системы. Результаты продемонстрировали устойчивую и безошибочную работу всех функций.

Тестирование безопасности направлено на оценку стойкости к попыткам взлома, в частности, подбору ключей шифрования. За счет использования слу-

чайно генерируемых ключей и проверенных криптографических алгоритмов приложение успешно выдержало все атаки и показало высокий уровень защиты данных [6].

Нагрузочные испытания выявляли пределы производительности при обработке крупных файлов. По результатам тестов на эмуляторе Pixel 6 Pro API 34 приложение обрабатывало файлы размером до 10 МБ за 1,41 миллисекунды, не демонстрируя задержек. Это подтверждает его способность эффективно работать с большими объемами данных без потери стабильности и производительности.

Таким образом, приложение может быть полезным как для частных пользователей, так и для корпоративных клиентов, которые хотят защитить свои конфиденциальные данные. В дальнейшем планируется расширить функциональность, добавив возможность облачного хранения с поддержкой шифрования и интеграцию новых типов файлов.

Список используемых источников

1. Коржик В. И., Яковлев В. А. Основы криптографии. Санкт-Петербург, 2016.
2. Ахрамеева К. А., Ковцур М. М., Михайлова А. В. Обеспечение информационной безопасности баз данных web-приложений // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. С. 107–110.
3. Красов А. В., Шариков П. И. Методика защиты байт-кода java-программы от декомпиляции и хищения исходного кода злоумышленником // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2017. № 1. С. 47–51.
4. Защита данных в Android-приложении // Блог Crimeadigital, 2023. URL: https://crimeadigital.ru/blog/zashhita-dannyh-v-android-prilozhenii/ (дата обращения 05.11.2024).
5. Duggu R. Encrypt Android DB using SQLCipher // Medium, 2021. URL: https://medium.com/@dugguRK/encrypt-android-db-sqlcipher-89819ff71c43 (дата обращения 09.11.2024).
6. Кириллов Д. С., Молостов Д. Д. Современные методы хранения данных в мобильных приложениях // Наука в современном мире: актуальные вопросы, достижения и инновации. Сборник статей Международной научно-практической конференции. Пенза, 2023. URL: https://elibrary.ru/item.asp?id=50080636 (дата обращения 10.11.2024).

Korenjugin E., Kovtcur M., Yasser M. **DEVELOPMENT OF A SECURE MOBILE DATA STORAGE APPLICATION FOR THE ANDROID OPERATING SYSTEM.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article is devoted to the development of a mobile application for the Android operating system designed for secure storage of user files. The application implements encryption methods using AES, which allows you to ensure a high level of data security. The developed application includes the functions of encryption, decryption, adding, viewing and deleting files, and contains a convenient and intuitive interface.

Key words: information security, secure storage, cryptography, encryption, mobile applications.

УДК 004.056.53
ГРНТИ 49.33.35

МОДЕЛИРОВАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ IoT НА УРОВНЕ УСТРОЙСТВА

Н. И. Козырева, Е. А. Савин
Поволжский государственный университет телекоммуникаций и информатики

Моделирование угроз информационной безопасности в сетях Интернета вещей (IoT) на уровне устройств, с акцентом на Botnet-атаки, рассматривает основные механизмы заражения устройств и последствия использования IoT-устройств в составе ботнетов. Описываются угрозы, связанные с атаками DDoS, кражей данных и перехватом трафика. Анализируются реальные примеры, такие как атака Mirai, и методы защиты от таких угроз: обновления программного обеспечения, использование сложных паролей, шифрование и мониторинг трафика. Подробно рассматриваются подходы к моделированию угроз и прогнозированию атак, что помогает разработать эффективные стратегии для защиты IoT-устройств и сетей.

IoT, безопасность IoT, захват устройства, информационная безопасность, Botnet-атаки, моделирование угроз, уязвимости IoT, защита IoT

С увеличением числа устройств, подключенных к интернету, и распространением Интернета вещей (IoT) возрастает и угроза информационной безопасности. В отличие от традиционных компьютерных систем, устройства IoT часто обладают ограниченными вычислительными ресурсами, слабыми механизмами безопасности и могут находиться в физически уязвимых местах, что делает их привлекательными мишенями для атак [1].

Угрозы на уровне устройства в сетях IoT имеют разнообразные формы и могут привести к серьезным последствиям, включая компрометацию конфиденциальных данных, нарушение работы сети и использование устройств для дальнейших атак. Одним из наиболее опасных типов атак является Botnet-атака, которая активно используется злоумышленниками для заражения и эксплуатации уязвимых устройств IoT.

В этой статье будет рассмотрено моделирование угроз безопасности на уровне устройства в сетях IoT, с акцентом на Botnet-атаки, их механизмы, способы защиты и методы предотвращения.

Устройства IoT, как правило, имеют слабую защиту, что делает их уязвимыми для различных типов атак. В особенности устройства, используемые в умных домах, промышленности и других сферах, могут быть подвергнуты следующим угрозам:

1. Заражение вредоносным ПО. Злоумышленники могут использовать уязвимости в программном обеспечении или неправильную конфигурацию устройства для установки вредоносного ПО;

2. Использование уязвимостей в аппаратных компонентах. Многие устройства IoT используют процессоры и чипы с известными уязвимостями, которые могут быть использованы для доступа к памяти или контролю над устройством;

3. Несанкционированный доступ. Устройства IoT часто используют слабые пароли или незащищенные протоколы связи, что облегчает получение несанкционированного доступа;

4. Атаки отказа в обслуживании (DoS/DDoS). Зараженные устройства могут быть использованы для проведения атак отказа в обслуживании (DDoS), перегружая сервера или сети трафиком;

5. Botnet-атаки. Одна из самых серьезных угроз для IoT-устройств – это создание ботнетов. Зараженные устройства могут быть использованы для атак на другие системы, что создает значительные риски для безопасности всего Интернета.

Таким образом, стоит отдельно рассмотреть Botnet-атаки и их воздействие на устройства IoT. Botnet (сеть зараженных устройств) представляет собой одну из наиболее опасных форм угроз для IoT-устройств. Злоумышленники могут создать ботнет, скомпрометировав большое количество устройств IoT, таких как камеры видеонаблюдения, умные колонки, термостаты и другие гаджеты. Зараженные устройства (боты) затем становятся частью управляющей сети и могут быть использованы для выполнения различных атак.

Botnet-атаки на устройства IoT начинаются с заражения устройств через уязвимости в программном обеспечении или через использование стандартных, легко угадываемых паролей. Процесс заражения включает следующие этапы:

1. Обнаружение уязвимых устройств. Злоумышленники используют сканеры для поиска устройств, у которых открыты порты или слабая защита (например, использование стандартных паролей);

2. Эксплуатация уязвимости. После нахождения уязвимых устройств злоумышленники используют эксплойты для получения удаленного доступа и внедрения вредоносного кода;

3. Создание ботнета. Устройства, ставшие частью ботнета, отправляют команды на другие устройства в сети или участвуют в атаке DDoS. Для управления ботнетом злоумышленники используют серверы C&C (Command and Control);

4. Использование ботнета для атак. После того, как ботнет сформирован, злоумышленники могут использовать зараженные устройства для различ-

ных целей, таких как атаки DDoS, кража данных, распространение спама или манипуляции с данными.

Одним из самых известных примеров Botnet-атаки на устройства IoT является Mirai Botnet, который в 2016 году использовал уязвимости в камерах видеонаблюдения, маршрутизаторах и других устройствах IoT для создания крупнейшего ботнета. Этот ботнет был использован для проведения атак DDoS на крупные веб-сайты и сервисы. Зараженные устройства использовали простые пароли по умолчанию, что делало их уязвимыми для атаки.

Mirai продемонстрировал, как уязвимости в IoT-устройствах могут быть использованы для создания мощных распределенных атак. В результате атаки на серверы компании Dyn, обслуживающей крупнейшие интернет-ресурсы, были затруднены доступы к таким сайтам, как Twitter, Reddit и Spotify.

Моделирование угроз – важный аспект в понимании потенциальных уязвимостей устройств и сетей. Оно позволяет предсказать возможные сценарии атак и разработать стратегии защиты [2]. Приведем алгоритм моделирования угроз Botnet-атак в IoT-сетях:

1. Анализ уязвимостей. На первом этапе моделирования необходимо анализировать уязвимости IoT-устройств, включая слабые пароли, неподдерживаемое программное обеспечение и открытые порты. Анализ позволяет определить, какие устройства могут быть скомпрометированы в первую очередь;

2. Моделирование сценариев заражения. На основе данных об уязвимостях моделируется, как атака будет распространяться по сети, если одно устройство будет заражено. Прогнозируется, как ботнет будет расширяться и какие устройства могут быть захвачены в ходе атаки;

3. Оценка воздействия. Моделирование также включает оценку воздействия на всю сеть IoT. Это может включать в себя анализ трафика, поведение устройств после заражения, а также последствия для работы сети и других устройств;

4. Прогнозирование активности злоумышленников. Модели угроз позволяют также спрогнозировать действия злоумышленников, их возможные цели и методы атак. Например, можно определить, какие устройства будут использованы для организации DDoS-атаки, и какие ресурсы будут целью этой атаки;

5. Использование машинного обучения для обнаружения угроз. Машинное обучение может помочь в обнаружении аномальных действий, связанных с ботнет-активностью. Системы на базе ИИ могут анализировать поведение устройств и сетевого трафика, чтобы выявить признаки заражения.

Для защиты от Botnet-атак при разработке и эксплуатации сетей IoT стоит применять следующие меры:

1. Регулярные обновления. Устройства должны получать своевременные обновления программного обеспечения для устранения известных уязвимостей;

2. Сложные пароли и двухфакторная аутентификация. Одной из важнейших мер защиты является установка сложных паролей для устройств и использование двухфакторной аутентификации (2FA), если это возможно;

3. Шифрование данных. Шифрование трафика между устройствами и серверами помогает защитить данные от перехвата злоумышленниками;

4. Изоляция устройств в сети. Разделение устройств на разные подсети позволяет минимизировать риск распространения ботнета в случае заражения одного из устройств;

5. Мониторинг и анализ трафика. Внедрение систем мониторинга, которые отслеживают аномалии в трафике и активности устройств, может помочь в выявлении зараженных устройств на ранних стадиях;

6. Использование межсетевых экранов (firewalls). Применение фильтрации трафика и брандмауэров позволяет блокировать подозрительные запросы и соединения, исходящие от зараженных устройств.

В заключение стоит отметить, что Botnet-атаки в сетях IoT – это серьезная угроза для информационной безопасности, которая может привести к широкомасштабным последствиям. Моделирование угроз на уровне устройств помогает выявить уязвимости, предсказать возможные сценарии атак и выработать эффективные стратегии защиты. Для предотвращения заражений устройств IoT ботнетами необходимо использовать комплексные меры защиты, включая регулярные обновления, сильные пароли, шифрование данных и системы мониторинга.

Список используемых источников

1. Интернет вещей – от исследований и инноваций до выхода на рынок / О. Вермесан, П. Фрисс (ред.). Ольборг, Дания: River Publishers, 2018 373 с. (серия River Publishers in Communications). URL: https://www.riverpublishers.com/pdf/ebook/RP_E9788793102958.pdf (дата обращения 10.11.2024).
2. Райес А., Салам С. Вещи в IoT: датчики и исполнительные механизмы // Интернет вещей: от шумихи к реальности. Cham: Springer, 2020. С. 57–77. URL: https://doi.org/10.1007/978-3-319-44860-2_3 (дата обращения 10.11.2024).

Kozyreva N., Savin E. **MODELING INFORMATION SECURITY THREATS IN IoT NETWORKS AT THE DEVICE LEVEL.**

Povolzhskiy State University of Telecommunications and Informatics

Threat modeling for information security in Internet of Things (IoT) networks at the device level, with a focus on Botnet attacks, examines the main infection mechanisms of IoT devices and the consequences of using IoT devices within botnets. The threats associated with DDoS attacks, data theft, and traffic interception are discussed. Real-world examples, such as the Mirai attack, are analyzed, along with protection methods against these threats: software updates, the use of strong passwords, encryption, and traffic monitoring. Approaches to threat modeling and attack prediction are thoroughly examined, which helps develop effective strategies for protecting IoT devices and networks.

Key words: IoT, IoT security, device hijacking, information security, Botnet attacks, threat modeling, IoT vulnerabilities, IoT protection.

УДК 004.056.53
ГРНТИ 49.33.35

МОДЕЛИРОВАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ IoT: АТАКА ЧЕРЕЗ ЗАХВАТ УСТРОЙСТВА

Н. И. Козырева, К. И. Теплов
Поволжский государственный университет телекоммуникаций и информатики

В эпоху активного развития Интернета вещей (IoT) растет количество уязвимых устройств, подключенных к сети, что влечет за собой серьезные угрозы информационной безопасности. Одной из наиболее значимых угроз является захват устройства (Device Hijacking), при котором злоумышленники получают контроль над устройством IoT, используя его для кражи данных, проведения атак или создания ботнетов. Данная статья рассматривает особенности моделирования угроз в сетях IoT позволяющие выявлять уязвимости и оценивать риски, а также разрабатывать эффективные стратегии защиты для IoT-инфраструктуры. В последующем представленная модель позволит составить граф атак для демонстрации поэтапного развития компрометации устройства и наглядного описания возможных сценариев захвата.

IoT, безопасность IoT, захват устройства, информационная безопасность, моделирование угроз, уязвимости IoT, защита IoT

С развитием технологий Интернет вещей (IoT) в повседневной жизни и бизнесе, количество подключенных устройств стремительно растет. Эти устройства, такие как умные бытовые приборы, системы безопасности, промышленные сенсоры и многие другие, делают нашу жизнь удобнее, но также создают новые угрозы для информационной безопасности. Одной из самых распространенных и серьезных угроз в сетях IoT является атака через захват устройства, известная как Device Hijacking [1]. Такая атака позволяет злоумышленникам получить полный контроль над IoT-устройством, используя его в качестве точки входа для дальнейших атак или для выполнения вредоносных действий, таких как участие в ботнетах или перехват данных.

Проблема захвата IoT-устройств усугубляется из-за частого использования простых или стандартных паролей, отсутствия регулярных обновлений и ограниченных возможностей безопасности самих устройств. Устройства IoT не всегда рассчитаны на защиту от внешних атак, и часто из-за этого являются легкой целью для злоумышленников.

Для анализа угроз захвата устройств в IoT-сетях эффективным инструментом является построение графов атак. Графы атак позволяют наглядно визуализировать возможные сценарии компрометации устройства, демонстри-

руя каждый шаг, который злоумышленник может предпринять для захвата контроля. Такие графы помогают исследовать уязвимости системы, оценивать степень риска и разрабатывать стратегии защиты, адаптированные к особенностям IoT-устройств.

Захват устройства или "Device Hijacking" представляет собой одну из самых серьезных угроз в сетях IoT, когда злоумышленник получает полный контроль над IoT-устройством. Это может быть вызвано недостаточной защитой, использованием стандартных паролей или отсутствием обновлений безопасности.

Атака через захват устройства (Device Hijacking) в сетях IoT связана с несколькими ключевыми угрозами, которые злоумышленник может использовать для компрометации устройства. Примерами таких угроз являются:

1. Слабые или стандартные пароли. Многие IoT-устройства поставляются с предустановленными заводскими паролями, которые пользователи часто забывают заменить. Стандартные пароли, такие как "admin" или "1234", делают устройства уязвимыми к несанкционированному доступу.

Злоумышленник может легко подобрать или угадать стандартный пароль и войти в систему устройства, получив полный контроль над его функциями. После захвата устройства злоумышленник может использовать его для дальнейших атак на сеть или для сбора данных;

2. Уязвимости прошивки и отсутствие обновлений безопасности. Прошивки IoT-устройств часто содержат уязвимости, которые остаются без исправлений, так как производители не всегда выпускают регулярные обновления безопасности. Многие устройства не поддерживают автоматическое обновление, что увеличивает риск использования устаревшего программного обеспечения.

Злоумышленники могут воспользоваться уязвимостями в прошивке, запустив эксплойты для захвата устройства или установки вредоносного ПО. Это позволяет злоумышленникам перехватывать команды и данные или нарушать нормальную работу устройства;

3. Открытые порты и уязвимые сетевые протоколы. Многие IoT-устройства подключаются к сети через общие порты и используют небезопасные протоколы связи, такие как HTTP без шифрования. Открытые порты делают устройство доступным для сканирования и атак извне.

Злоумышленники могут проводить сканирование сети для обнаружения открытых портов на устройствах, что позволяет атакующим выполнять атаки типа «человек посередине» (MITM) для перехвата данных или вмешательства в передаваемые команды;

4. Недостаточная аутентификация и контроль доступа. Многие IoT-устройства не имеют строгих правил аутентификации и контроля доступа. Это позволяет злоумышленникам получить доступ к устройствам с минимальными усилиями, особенно если устройство подключено к открытой или плохо защищенной сети.

Злоумышленник может подключиться к устройству, не проходя проверки аутентификации. Это открывает доступ к настройкам устройства и его данным, что позволяет злоумышленнику установить на устройстве бэкдоры или изменить его конфигурацию;

5. Недостаточное внимание к шифрованию данных. Многие IoT-устройства передают данные в незашифрованном виде, что делает их уязвимыми к перехвату информации. Эта угроза особенно актуальна для устройств, обрабатывающих конфиденциальные данные (например, медицинские устройства).

При отсутствии шифрования злоумышленник может легко перехватить данные, передаваемые между устройством и сервером или между несколькими устройствами в сети. Это позволяет злоумышленнику получить доступ к конфиденциальной информации или вмешаться в работу устройства;

6. Недостатки в аппаратной защите. Некоторые IoT-устройства не обладают достаточной защитой на аппаратном уровне, например, не имеют функции безопасной загрузки или защиты от перепрограммирования.

Злоумышленники могут физически получить доступ к устройству и изменить его конфигурацию, загрузив модифицированную прошивку. Это дает возможность установить постоянный доступ к устройству или включить его в состав ботнета.

Эти угрозы делают IoT-устройства легкими мишенями для злоумышленников. Атака через захват устройства может привести к серьезным последствиям, включая нарушение конфиденциальности данных, снижение производительности устройства и даже компрометацию всей сети, к которой подключено устройство [2].

Опишем этапы атаки Device Hijacking от выявления уязвимости до полного захвата устройства:

1. Обнаружение уязвимости. На этом этапе злоумышленник сканирует сеть для поиска уязвимых IoT-устройств. Злоумышленник ищет устройства с слабыми паролями, устаревшими прошивками, или открытыми портами, которые могут предоставить доступ к устройству;

2. Получение доступа. Найдя уязвимое устройство, злоумышленник пробует получить к нему доступ. Получив доступ, злоумышленник начинает управлять устройством;

3. Управление устройством. На этом этапе злоумышленник запускает команды, чтобы начать контроль над устройством. Это создает прямой контроль над устройством, и оно может теперь выполнять команды, заданные злоумышленником;

4. Закрепление контроля. Чтобы избежать обнаружения и сохранить доступ, злоумышленник пытается «закрепиться» на устройстве. Он может, например, установить вредоносное ПО, которое повторно подключает устройство к его системе даже после перезагрузки. Или злоумышленник создает скрытую учетную запись с правами администратора, чтобы вернуть доступ, если его закроют.

5. Нанесение ущерба. Используя свое положение, злоумышленник выполняет атакующие действия. Это могут быть:

– кража данных, например, захват видеопотоков с камер или данных с датчиков;

– атаки на другие устройства в сети – IoT-устройство может быть использовано для сканирования сети или атаки на другие узлы, что увеличивает масштабы вторжения;

– DDoS-атака – захваченное устройство может стать частью ботнета, участвующего в распределенной атаке на другие сети или сервисы.

Список используемых источников

1. Верещагина Е. А., Капецкий И. О., Ярмонов А. С. Проблемы безопасности Интернета вещей: учебное пособие. М.: Мир науки, 2021. Сетевое издание. URL: https://izd-mn.com/PDF/20MNNPU21.pdf (дата обращения 11.11.2024).

2. Таржанов Т. В., Новиков С. Н. Моделирование угрозы информационной безопасности в сети IoT и реализация защиты от этой угрозы // Интеллектуальный потенциал Сибири: материалы 29-ой Региональной научной студенческой конференции, посвященной Году науки и технологий в России, Новосибирск, 17–21 мая 2021 г. Том Часть 5. Новосибирск: Новосибирский государственный технический университет, 2021. С. 615–619. URL: https://www.elibrary.ru/item.asp?id=48099469 (дата обращения 11.11.2024).

***Kozyreva N., Teplov K.* MODELING INFORMATION SECURITY THREATS IN IoT NETWORKS: DEVICE HIJACKING ATTACK USING AN ATTACK GRAPH.**

Povolzhskiy State University of Telecommunications and Informatics

With the rapid development of the Internet of Things (IoT), the number of vulnerable devices with the active development of the Internet of Things (IoT), the number of vulnerable devices connected to the network is growing, which entails serious threats to information security. One of the most significant threats is Device Hijacking, in which attackers gain control of an IoT device by using it to steal data, conduct attacks, or create botnets. This article discusses the features of threat modeling in Yota networks that allow you to identify vulnerabilities and assess risks, as well as develop effective protection strategies for the IoT infrastructure. Subsequently, the presented model will allow you to create an attack graph to demonstrate the gradual development of device compromise and a visual description of possible capture scenarios.

Key words: IoT, IoT security, device hijacking, information security, threat modeling, IoT vulnerabilities, IoT protection.

УДК 004.56
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ VPN НА КАНАЛЬНОМ УРОВНЕ МОДЕЛИ OSI

А. Р. Конев, Н. А. Косов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире информационных технологий защита передаваемых данных является одной из ключевых задач. Рост количества удаленных рабочих мест, мобильных устройств и распределенных офисов требует надежных методов обеспечения безопасности при передаче информации по общедоступным сетям, таким как Интернет.

VPN, анализ трафика, сети, аутентификация

Виртуальные частные сети (VPN) предоставляют эффективное решение этой проблемы, позволяя создавать защищенные каналы связи поверх незащищенных сетей.

Цель данной статьи – исследовать основные технологии VPN на различных уровнях модели OSI, провести практический анализ их эффективности, включая вероятность обнаружения VPN-трафика средствами глубокого анализа пакетов (DPI), и сделать выводы о их применимости в различных условиях.

В процессе исследования были рассмотрены протоколы VPN на канальном, сетевом и сеансовом уровнях модели OSI: PPTP, L2TP/IPSec и OpenVPN (основанный на SSL/TLS). Для получения объективных данных был собран тестовый стенд, имитирующий реальные условия эксплуатации.

Методика исследования

Описание тестового стенда: был развернут лабораторный стенд, состоящий из следующих компонентов:

Серверная часть: три сервера VPN на базе ОС Ubuntu Server 20.04, настроенные для работы с PPTP, L2TP/IPSec и OpenVPN соответственно.

Клиентская часть: клиентские устройства на базе Windows 10 и Ubuntu Desktop 20.04, подключающиеся через различные сети, включая домашние сети и мобильные подключения.

Сетевая инфраструктура: использовались симулированные каналы связи с пропускной способностью 100 Мбит/с и задержками от 10 до 50 мс для имитации различных условий сети Интернет.

Инструменты измерения: для проведения тестов использовались утилиты iperf3 для измерения пропускной способности, ping и traceroute для определения задержек, Wireshark для анализа трафика, а также специализированное ПО DPI для оценки вероятности обнаружения VPN-трафика [1].

План проведения эксперимента

Настройка VPN-соединений: последовательная настройка и запуск VPN-серверов и клиентов для каждого протокола.

Измерение производительности: проведение серии тестов передачи данных для оценки пропускной способности и задержек.

Анализ безопасности: оценка сложности взлома и устойчивости протоколов к известным уязвимостям [2].

Обнаружение DPI: проверка возможности обнаружения и блокировки VPN-трафика с использованием систем DPI.

Сбор и обработка данных: сравнительный анализ полученных результатов и их визуализация в виде таблиц и графиков.

Результаты исследования

Производительность и задержки. Проведенные тесты показали следующие результаты (табл. 1).

ТАБЛИЦА 1. Средняя пропускная способность и задержки для различных протоколов VPN

Параметр	PPTP	L2TP/IPSec	OpenVPN (UDP)	OpenVPN (TCP)
Пропускная способность (Мбит/с)	92	75	80	68
Средняя задержка (мс)	12	18	15	20
Вариация задержки (джиттер, мс)	2	4	3	5

Анализ результатов

PPTP показал наибольшую пропускную способность и минимальные задержки благодаря низкой накладной нагрузке на шифрование.

L2TP/IPSec продемонстрировал снижение пропускной способности на ~18 % по сравнению с PPTP из-за более сложных криптографических операций.

OpenVPN при использовании UDP показал результаты, близкие к L2TP/IPSec, а при использовании TCP – снижение пропускной способности из-за дополнительных накладных расходов протокола TCP.

Безопасность протоколов

Безопасность протоколов представлена в таблице 2.

ТАБЛИЦА 2. Сравнение безопасности протоколов VPN

Критерий	PPTP	L2TP/IPSec	OpenVPN
Алгоритм шифрования	MPPE (128 бит)	AES (256 бит)	AES (256 бит)
Аутентификация	MS-CHAPv2	IKEv2	SSL/TLS
Уязвимости	Высокие	Низкие	Очень низкие
Поддержка двухфакторной аутентификации	Ограниченная	Да	Да

Анализ результатов

PPTP имеет известные уязвимости, связанные с протоколом аутентификации MS-CHAPv2. Современные методы взлома позволяют восстановить ключ шифрования за несколько часов [3].

L2TP/IPSec использует надежные алгоритмы шифрования и аутентификации. Однако, при неправильной настройке возможны уязвимости, связанные с протоколом IKE.

OpenVPN обеспечивает высокий уровень безопасности благодаря использованию SSL/TLS и возможности гибкой настройки параметров шифрования и аутентификации [4].

Обнаружение VPN-трафика средствами DPI

Обнаружение VPN-трафика средствами DPI приведено в таблице 3.

ТАБЛИЦА 3. Вероятность обнаружения VPN-трафика системами DPI

Протокол	Стандартные порты и протоколы	Вероятность обнаружения (%)
PPTP	TCP 1723, GRE	98
L2TP/IPSec	UDP 500, UDP 4500, ESP	95
OpenVPN (UDP)	UDP 1194	90
OpenVPN (TCP 443)	TCP 443	40

Анализ результатов

PPTP и L2TP/IPSec легко обнаруживаются средствами DPI из-за использования стандартных портов и характерных сигнатур протоколов GRE и ESP.

OpenVPN при использовании стандартного порта 1194/UDP также может быть обнаружен, однако при переключении на порт 443/TCP и использовании протокола TCP трафик маскируется под обычный HTTPS, что значительно снижает вероятность его обнаружения.

Сложность настройки и совместимость

Сложность настройки и совместимость показаны в таблице 4.

ТАБЛИЦА 4. Сравнение сложности настройки и совместимости протоколов VPN

Критерий	PPTP	L2TP/IPSec	OpenVPN
Сложность настройки	Низкая	Средняя	Высокая
Поддержка NAT-Traversal	Ограниченная	Да	Да
Требование дополнительного ПО	Нет	Нет	Да
Кроссплатформенность	Высокая	Высокая	Высокая

Анализ результатов

PPTP прост в настройке и не требует установки дополнительного ПО на клиентских устройствах, но имеет ограниченную поддержку NAT-Traversal.

L2TP/IPSec сложнее в настройке из-за необходимости конфигурации IPSec-политик, но обеспечивает лучшую совместимость с NAT.

OpenVPN требует установки клиентского ПО и более сложной настройки, однако предоставляет широкие возможности для обхода сетевых ограничений и высокую кроссплатформенность.

Проведенное исследование показало, что при выборе VPN-технологии необходимо учитывать баланс между производительностью, безопасностью и возможностью обхода сетевых ограничений.

PPTP обеспечивает высокую скорость и простоту настройки, но его использование не рекомендуется из-за низкого уровня безопасности и высокой вероятности обнаружения и блокировки трафика средствами DPI.[5]

L2TP/IPSec предлагает высокий уровень безопасности и приемлемую производительность, однако сложность настройки и проблемы с прохождением через NAT могут ограничивать его применение в некоторых сетях.

OpenVPN предоставляет оптимальный баланс между безопасностью и гибкостью настройки. Возможность маскировки трафика под HTTPS делает его предпочтительным выбором в сетях с жесткими ограничениями и DPI.

Выводы и рекомендации

Проведенное исследование и практические эксперименты позволяют сделать следующие выводы. OpenVPN обеспечивает наивысший уровень безопасности среди рассмотренных VPN-технологий благодаря использованию современных криптографических алгоритмов и протоколов. Несмотря на то, что OpenVPN может уступать PPTP в скорости передачи данных, его производительность остается на приемлемом уровне для большинства приложений, обеспечивая надежное и стабильное соединение.

Одним из ключевых преимуществ OpenVPN является возможность маскировки трафика под HTTPS, что значительно снижает вероятность его обнаружения и блокировки средствами глубокого анализа пакетов (DPI). Это особенно актуально в сетях с жесткими ограничениями и повышенным контролем трафика, где требуется обеспечить конфиденциальность и непрерывность связи.

Кроме того, OpenVPN предоставляет широкие возможности настройки, позволяя адаптироваться к различным сетевым условиям и требованиям безопасности. Гибкость конфигурации позволяет оптимизировать работу VPN в конкретных сценариях использования, обеспечивая баланс между скоростью, надежностью и уровнем защиты.

Исходя из вышеизложенного, рекомендуется корпоративным пользователям применять OpenVPN с использованием порта 443/TCP и протокола TCP, что позволяет эффективно обходить сетевые ограничения и маскировать VPN-трафик под обычный HTTPS. Для повышения уровня безопасности следует дополнительно внедрить двухфакторную аутентификацию и использовать цифровые сертификаты, что усилит защиту от несанкционированного доступа и повысит доверие к установленным соединениям.

Частным пользователям также стоит обратить внимание на OpenVPN как предпочтительный выбор, особенно если существует необходимость обхода сетевых ограничений и обеспечения конфиденциальности в открытых сетях, таких как публичные Wi-Fi точки доступа. Простота использования и высокий уровень безопасности делают OpenVPN оптимальным решением для защиты персональных данных в различных сетевых условиях.

Вместе с тем, использование PPTP не рекомендуется из-за известных уязвимостей и низкого уровня безопасности. Несмотря на простоту настройки и широкую поддержку, PPTP не отвечает современным требованиям к защите информации и может представлять серьезный риск для конфиденциальности и целостности передаваемых данных.

В заключение, выбор VPN-технологии должен основываться на тщательном анализе потребностей в безопасности, производительности и гибкости

настройки. OpenVPN, благодаря своим преимуществам, является оптимальным решением для большинства сценариев использования, обеспечивая надежную защиту и адаптивность в современных сетевых условиях.

Список используемых источников

1. Гостеева А. И., Истратова Е. Е. Сравнительный анализ технологий организации VPN-соединений //Программно-техническое обеспечение автоматизированных систем, 2021. С. 128–131.
2. Росляков А. В., Ефремов Д. А. Анализ технологии WireGuard для реализации VPN // Вестник связи, 2022. № 12. С. 8.
3. Нурмухаметов Д. Р. Анализ VPN-протоколов: OPENVPN, PPTP, L2TP/IPSEC, IKEV2/IPSEC // Научное сообщество студентов. междисциплинарные исследования, 2019. С. 46–50.
4. Муравьев К. А., Хуббатулин М. Э. Методика настройки VPN на роутерах MIKROTIK // Технологии инженерных и информационных систем, 2019. № 2. С. 22–33.
5. Кондратьев А. Н., Дубровский Н. С., Князев А. А. Анализ преимуществ и недостатков существующих сетей VPN при построении корпоративной сети // Поколение будущего: Взгляд молодых ученых-2022, 2022. С. 208–212.

***Konev A., Kosov N.* STUDY OF THE EFFECTIVENESS OF VPN AT THE CHANNEL LAYER OF THE OSI MODEL.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the modern world of information technology, the protection of transmitted data is one of the key tasks. The growth of remote workstations, mobile devices and distributed offices requires reliable methods of ensuring security when transmitting information over public networks such as the Internet.

Key words: VPN, traffic analysis, networks, authentication.

УДК 004.056
ГРНТИ 05.11.07

ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ КАК МЕТОД ЗАЩИТЫ ОТ РЕВЕРС-ИНЖИНИРИНГА В МОДУЛЯХ ЯДРА LINUX

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

В статье рассматривается использование цифровых водяных знаков как метода защиты от реверс-инжиниринга в модулях ядра Linux. Особое внимание уделяется механизмам встраивания водяных знаков в бинарные файлы и их роли в повышении безопасности программных компонентов. Обсуждаются различные подходы к созданию и применению водяных знаков, включая скрытые и явные методы, а также способы обнаружения модификаций, что позволяет эффективно отслеживать несанкционированные изменения. Рассматриваются криптографические технологии, которые могут усилить защиту водяных знаков, а также преимущества и ограничения данного подхода. Статья также затрагивает вопросы реальной практики внедрения цифровых водяных знаков в компоненты ядра Linux и их перспективы для повышения уровня безопасности в условиях современного реверс-инжиниринга.

цифровые водяные знаки, реверс-инжиниринг, защита от реверс-инжиниринга, безопасность программного обеспечения, ядро Linux, модули ядра, защита программ, бинарные файлы

Современная безопасность операционных систем, в том числе Linux, сталкивается с рядом угроз, среди которых реверс-инжиниринг является одной из самых опасных. Исследователи безопасности, злоумышленники и конкуренты могут применять методы реверс-инжиниринга для анализа и модификации программного обеспечения, в том числе модулей ядра. Это представляет собой серьезную угрозу для целостности системы, ее конфиденциальности и защиты от несанкционированного доступа.

Одним из методов защиты от подобных атак является использование цифровых водяных знаков – техник, позволяющих скрытно встраивать идентификационные или контрольные данные в программный код или его компоненты. Эти водяные знаки могут служить не только для идентификации оригинального источника кода, но и для обнаружения несанкционированных изменений, что является важным элементом защиты от реверс-инжиниринга.

Данная статья посвящена исследованию методов использования цифровых водяных знаков для защиты модулей ядра Linux от реверс-инжиниринга. Мы рассмотрим основные подходы к встраиванию водяных знаков в бинарные файлы, а также их роль в обеспечении безопасности, включая примеры криптографических методов защиты и практическую реализацию.

Применение цифровых водяных знаков в программном обеспечении

Встраивание водяных знаков в программное обеспечение может быть использовано для различных целей, таких как защита авторских прав, обнаружение изменений в коде, идентификация источников модификаций и предотвращение несанкционированного использования. Важно, чтобы водяные знаки были достаточно устойчивыми к манипуляциям, но при этом не нарушали работу программы или ее производительность.

Одним из самых распространенных методов применения водяных знаков является встраивание их в бинарные файлы программы [1]. Этот подход часто используется в случае защиты готовых исполнимых файлов и библиотек. Водяные знаки в бинарном формате могут быть внедрены в различные участки программы, не влияя на ее поведение.

Методы встраивания водяных знаков в бинарные файлы – добавление скрытых данных в неиспользуемые или резервные области памяти [1]. В бинарных файлах существуют различные области памяти, которые не задействованы в работе программы (например, пустые секции или служебные данные). В эти области можно вставить закодированные водяные знаки, которые не нарушат выполнение программы.

Встраивание водяных знаков в драйверы и модули ядра Linux: для модулей ядра Linux, в том числе драйверов и других низкоуровневых компонентов, защита от реверс-инжиниринга особенно важна. Ядро Linux предоставляет мощные средства для разработки драйверов и модулей, и встраивание водяных знаков в эти компоненты позволяет отслеживать, обнаруживать и предотвращать их несанкционированные изменения.

Методы встраивания водяных знаков в модули ядра – скрытые фрагменты данных в модулях – водяные знаки могут быть внедрены в неактивные участки памяти или данные в модуле ядра. Например, они могут быть скрыты в структурах данных или изменениях в коде, которые не влияют на основные функции драйвера.

Реверс-инжиниринг и его угроза для безопасности

Реверс-инжиниринг – это процесс анализа программного обеспечения с целью понять его структуру, алгоритмы и внутреннюю работу. В контексте компьютерной безопасности реверс-инжиниринг может быть использован как для легитимных целей (например, исследование уязвимостей и безопасность), так и для незаконных действий, таких как обход защиты, взлом программ и систем, или создание вредоносного ПО. В случае с операционными системами, такими как Linux, реверс-инжиниринг представляет собой значительную угрозу для безопасности, особенно когда речь идет о модификации или

вмешательстве в модули ядра, драйверы и другие низкоуровневые компоненты.

Цели и методы реверс-инжиниринга

Реверс-инжиниринг может преследовать различные цели в зависимости от контекста. Основными целями являются [2]:

1. Изучение функциональности программы. Злоумышленники и исследователи могут разбирать программу, чтобы понять ее алгоритмы, логику работы и взаимодействие с системой. Это может привести к выявлению уязвимостей, которые могут быть использованы для атак;

2. Обход защиты программ. Многие коммерческие программы и операционные системы имеют различные механизмы защиты, такие как лицензирование, шифрование, антивирусная защита или защиту от модификаций. Реверс-инжиниринг позволяет нарушить эти механизмы, например, удалив или обойдя лицензионные ограничения.

Для выполнения реверс-инжиниринга обычно используются следующие методы:

– анализ исходного кода (если исходный код доступен, то изучение его структуры, алгоритмов и паттернов может выявить уязвимости);

– декомпиляция и дизассемблирование (когда исходный код недоступен, используется декомпиляция бинарных файлов [2] или дизассемблирование исполнимых файлов для получения низкоуровневого представления программы. Это позволяет извлечь информацию о логике работы программы, ее структурах данных, алгоритмах и т. д.)

Угрозы реверс-инжиниринга для безопасности системы

Реверс-инжиниринг представляет собой серьезную угрозу для безопасности операционных систем, особенно для компонентов ядра Linux и драйверов. Если злоумышленники могут проанализировать и модифицировать код на уровне ядра, они могут получить полный контроль над системой. Вот основные угрозы, которые создает реверс-инжиниринг:

– взлом защиты авторских прав и интеллектуальной собственности;

– обнаружение уязвимостей и эксплойты;

– модификация поведения системы.

Реверс-инжиниринг и модули ядра Linux

Ядро Linux является важнейшим компонентом операционной системы, и его безопасность критически важна для всей системы. Реверс-инжиниринг компонентов ядра, таких как драйверы, модули или сам драйвер безопасности, может иметь тяжелые последствия:

– уязвимости в ядре;
– нарушение целостности системы.

Методы защиты от реверс-инжиниринга

Для защиты от реверс-инжиниринга существуют различные методы и техники, которые могут затруднить или полностью предотвратить возможность анализа и модификации кода:
– обфускация кода;
– шифрование и подпись кода;
– встраивание водяных знаков.

Методы защиты от реверс-инжиниринга с помощью водяных знаков

1. Методы встраивания водяных знаков в бинарные файлы: изменение структуры данных без влияния на функциональность

Встраивание водяных знаков в бинарные файлы программ является одним из наиболее эффективных методов защиты от реверс-инжиниринга, поскольку позволяет скрыть дополнительную информацию, которая будет служить индикатором подделки или модификации. Важно, чтобы этот процесс не влиял на основную функциональность программы, и чтобы водяной знак не был заметен для злоумышленников и обычных пользователей. Вот несколько подходов к встраиванию водяных знаков в бинарный код:
– использование неиспользуемых или неактивных частей памяти.

2. Обнаружение модификаций: как можно обнаружить подмену или модификацию водяного знака и, соответственно, вмешательство в код

Важной частью защиты с использованием водяных знаков является способность обнаружить изменения в коде программы, которые могут свидетельствовать о вмешательстве злоумышленников. Даже если водяной знак был внедрен в бинарный файл или исходный код, его целостность может быть нарушена, если файл был изменен или подменен. Чтобы защитить программное обеспечение и выявить такие вмешательства, применяются различные методы обнаружения модификаций:
– проверка целостности водяных знаков с помощью хеширования [3]. Один из самых простых методов защиты водяных знаков – это создание хеш-суммы всего бинарного файла или его частей, в том числе скрытых данных, содержащих водяной знак. При каждом запуске или проверке программы можно вычислять хеш и сравнивать его с заранее сохраненной версией. Если хеши не совпадают, это означает, что файл был изменен, и водяной знак был, вероятно, нарушен. Такой подход может быть полезен для проверки целостности программы или модуля ядра.

Заключение

Обнаружение модификаций водяных знаков с помощью хеширования, цифровых подписей и других методов мониторинга позволяет оперативно выявить любые изменения в программном коде и принимать меры по предотвращению угроз. В свою очередь, динамическая защита, основанная на проверке водяных знаков в процессе работы программы или при загрузке модулей ядра, усиливает систему безопасности, позволяя оперативно реагировать на потенциальные угрозы.

Таким образом, применение цифровых водяных знаков является важным элементом комплексной стратегии защиты программного обеспечения, которая позволяет значительно затруднить реверс-инжиниринг и повысить безопасность как на уровне отдельных приложений, так и на уровне всей операционной системы. В условиях постоянного развития технологий взлома и атаки на программные системы, использование таких методов защиты становится необходимым для обеспечения безопасности данных и защиты от угроз, связанных с несанкционированными модификациями кода.

Список используемых источников

1. Коржик В. И. и соавт. Исследование в области цифровой стеганографии и применение цифровых водяных знаков: методическое пособие / В. И. Коржик и соавт. 2-я редакция. СПб., 2017. 5 стр.
2. Красов А. В. Стратегия обеспечения авторского права и сохранения целостности ПО через интеграцию цифровых водяных знаков в исполняемые файлы / А. В. Красов // Перспективы науки, 2022. № 4 (151). Стр. 16–25. EDN OHFBUV.
3. Красов А. В., Верещагин А. С., Абатуров В. С. Приемы инкапсуляции данных в экзешники. // Вестник Санкт-Петербургского государственного электротехнического университета "ЛЭТИ", 2012. Выпуск 8. С. 51–55. EDN PFDDUD.

Konkov V., Krasov A. **DIGITAL WATERMARKS AS A METHOD OF PROTECTION AGAINST REVERSE ENGINEERING IN LINUX KERNEL MODULES.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article discusses the use of digital watermarks as a method of protection against reverse engineering in Linux kernel modules. Special attention is given to the mechanisms of embedding watermarks into binary files and their role in enhancing the security of software components. Various approaches to creating and applying watermarks are discussed, including both hidden and explicit methods, as well as techniques for detecting modifications, which allow for effective tracking of unauthorized changes. Cryptographic technologies that can strengthen watermark protection are also considered, along with the advantages and limitations of this approach. The article also touches upon practical aspects of implementing digital watermarks in Linux kernel components and their potential to improve security in the face of modern reverse engineering challenges.

Key words: Digital watermarks, reverse engineering, protection against reverse engineering, software security, Linux kernel, kernel modules, program protection, binary files.

УДК 004.56
ГРНТИ 81.93.29

ПРОТОКОЛ OAUTH: ГРАНТ «КОД АВТОРИЗАЦИИ» КАК СТАНДАРТ БЕЗОПАСНОЙ АВТОРИЗАЦИИ

Н. А. Косов, Э. О. Филипов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современные цифровые экосистемы требуют не только функциональности, но и высокого уровня безопасности при работе с пользовательскими данными. С развитием технологий и ростом количества онлайн-сервисов встал вопрос о создании универсального и надежного механизма, который позволял бы сторонним приложениям безопасно взаимодействовать с пользовательскими данными без необходимости передачи конфиденциальных данных, таких как логины и пароли.

безопасная авторизация, кибербезопасность, токен, OWASP

Введение

Протокол OAuth выступает в качестве современного стандарта авторизации, используемого для контроля доступа клиентских приложений к различным ресурсам. Согласно данным исследования, проведенного компанией Cybersecurity Ventures, объем данных, передаваемых через API, в 2022 году вырос примерно на 30 %. Этот факт подчеркивает ключевое значение вопросов безопасности при работе с подобными технологиями. В условиях, когда информация фактически стала «цифровым золотом», защита ее конфиденциальности превратилась в обязательный элемент любой устойчивой цифровой экосистемы.

Среди разнообразия механизмов авторизации особый интерес представляет так называемый грант «Код авторизации» (Authorization Code Grant), применяемый в рамках OAuth. Данный подход обеспечивает повышенную гибкость и надежность особенно при работе с серверными приложениями. Его широкое распространение в ведущих технологических платформах – от Google до Facebook и Microsoft – свидетельствует о признании его эффективности в индустрии.

Основные принципы гранта «Код авторизации»

Механизм гранта «Код авторизации» в OAuth базируется на четком разделении этапов, связанных с получением разрешения, и этапов, при которых

фактически происходит обмен конфиденциальными данными. Подобный подход позволяет избежать прямой передачи токенов доступа через браузер и тем самым снижает вероятность компрометации данных.

Взаимодействие между клиентским приложением, сервером авторизации и пользователем обычно описывают четырьмя ключевыми шагами.

Этап 1. Запрос авторизации.

Изначально клиентское приложение направляет запрос к конечной точке авторизации OAuth-сервиса. В этом запросе указываются такие параметры, как client_id (уникальный идентификатор клиента), redirect_uri (адрес для обратного вызова), response_type (обычно «code»), набор прав доступа (scope) и маркер состояния (state) для защиты от CSRF-атак [1].

```
GET /authorization?client_id=10111213&
redirect_uri=https://clientapplication.ru/callback&
response_type=code&
scope=openid %20profile&
state=ba13d489bd00e3c24 HTTP/1.1
Host: oauth-authorization-server.ru
```

Здесь клиент как бы «просит разрешение» на доступ к определенным аспектам учетной записи пользователя. Если требуется получить, к примеру, базовые сведения о пользователе, достаточно указать scope=openid profile, тем самым минимизируя набор данных, к которым клиент получит доступ.

Этап 2: Аутентификация и подтверждение

После получения запроса сервер авторизации перенаправляет пользователя на страницу входа. Здесь пользователь вводит свои учетные данные – логин и пароль – и затем знакомится со списком запрашиваемых разрешений. На этом шаге человек может осознанно принять или отклонить запрос на доступ к своим данным.

Подобная прозрачность и контроль особенно важны в контексте растущей обеспокоенности пользователей безопасностью персональной информации. По данным Statista, около 82 % пользователей в 2021 году выражали тревогу относительно сохранности своих данных при использовании сторонних приложений. Следовательно, этап согласия – это не просто техническая деталь, а важный фактор формирования доверия к платформе.

Этап 3: Получение кода авторизации

Когда пользователь соглашается предоставить разрешения, сервер авторизации возвращает его на страницу, указанную в redirect_uri. В этот момент в параметрах запроса клиентское приложение получает временный и одноразовый «код авторизации», а также значение state для проверки подлинности и непрерывности сессии:

```
GET /callback?code=abc123&state=ba13d489bd00e3c24 HTTP/1.1
Host: clientapplication.ru
```

Этот код не раскрывает никаких личных данных, а служит лишь промежуточным звеном для дальнейшего обмена на токен доступа.

Этап 4: Обмен кода авторизации на токен доступа

Последний шаг – клиентское приложение по защищенному каналу отправляет полученный код на сервер OAuth, подкрепляя запрос секретным ключом клиента (client_secret). В ответ выдается токен доступа, который позволит приложению выполнять запросы к API от имени пользователя [2]:

```
POST /token HTTP/1.1
Host: oauth-authorization-server.ru
Content-Type: application/x-www-form-urlencoded
grant_type=authorization_code&
code=abc123&
redirect_uri=https://clientapplication.ru/callback&
client_id=10111213&
client_secret=xyz987
```

Такой механизм широко применяют, например, в функционале «Войти через Google», дающем сторонним приложениям доступ к профилю пользователя или его календарю при сохранении высокого уровня защищенности. Преимущества гранта «Код авторизации» очевидны: удобство для разработчиков, безопасность для конечных пользователей и гибкость при настройке различных уровней доступа [3].

Уязвимости и проблемы внедрения

Несмотря на надежность самого протокола, практика показывает, что уязвимости часто возникают при неправильной реализации. Исследования OWASP свидетельствуют о том, что около 60 % известных уязвимостей OAuth

связаны с неверной валидацией redirect_uri [4]. Например, если сервер авторизации недостаточно тщательно проверяет соответствие указанных адресов зарегистрированным значениям, злоумышленник может перенаправить пользователя на поддельный ресурс и перехватить передаваемые данные.

Рекомендации по повышению уровня безопасности

Для максимальной защиты при использовании OAuth необходимо придерживаться нескольких ключевых принципов:

1. Регулярное обновление токенов. Токены доступа должны иметь ограниченный срок жизни, а в случае необходимости должны быть легко отозваны [5];
2. Строгая проверка redirect_uri. Только заранее зарегистрированные и проверенные адреса можно допускать к перенаправлению пользователя;
3. Использование параметра state: Уникальный маркер state помогает избежать CSRF-атак, гарантируя целостность процесса авторизации;
4. Обучение разработчиков. Важно повышать осведомленность о типичных уязвимостях и методах их предотвращения, регулярно обновлять знания и следить за актуальными рекомендациями.

Заключение

Грант «Код авторизации» в рамках протокола OAuth зарекомендовал себя как надежное, удобное и гибкое решение для безопасного предоставления доступов к ресурсам серверных приложений. При корректной настройке и соблюдении всех рекомендаций этот механизм эффективно минимизирует риски утечки информации и повышает общую устойчивость цифровой платформы к киберугрозам.

Современная цифровая среда, насыщенная всевозможными сервисами и API, нуждается в прозрачных и безопасных решениях. OAuth в сочетании с грантом «Код авторизации» уже стал своего рода отраслевым стандартом, помогающим создавать доверительные отношения между пользователями, приложениями и поставщиками ресурсов. Рассматриваемый подход демонстрирует свою актуальность в условиях растущей сложности экосистем и постоянных угроз кибербезопасности, формируя фундамент для долговременного и безопасного развития цифровых сервисов.

Список используемых источников

1. Ильина Л. А., Павлов Д. В. Авторизация в системе PolyAnalyst с использованием протокола OAuth 2.0 // Аллея науки, 2017. № 5. С. 481–484.

2. Leiba B. Oauth web authorization protocol // IEEE Internet Computing, 2012. Т. 16. № 1. С. 74–77.
3. Трокоз Д. А. и др. Типовое решение задачи авторизации пользователя в информационной системе // XXI век: итоги прошлого и проблемы настоящего плюс, 2019. Т. 8. № 4. С. 33–38.
4. Кортунов А. С., Заитов Э. Т. Способ и система авторизации веб-сайта в веб-браузере. 2020.
5. Трокоз Д. А. и др. Типовое решение задачи авторизации пользователя в информационной системе // XXI век: итоги прошлого и проблемы настоящего плюс, 2019. Т. 8. № 4. С. 33–38.

Kosov N., Filipov E. **OAUTH PROTOCOL: GRANT "AUTHORIZATION CODE" AS A SECURE AUTHENTICATION STANDARD.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Testing the effectiveness of DevSecOps processes is not just a method for checking the stability of development, but a key stage that allows you to assess the level of security integration into the software life cycle. In the context of constant growth of cybersecurity threats and the complexity of software systems, companies are faced with the need to ensure security at all stages, from design to operation

Key words: Secure Authentication, Cyber Security, Token, OWASP.

УДК 004.056
ГРНТИ 81.93.29

ОРГАНИЗАЦИЯ МОНИТОРИНГА, УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ И РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ С ИСПОЛЬЗОВАНИЕМ МНОГОФУНКЦИОНАЛЬНОГО ЗОНДА НА БАЗЕ ОДНОПЛАТНОЙ ВЫЧИСЛИТЕЛЬНОЙ ПЛАТФОРМЫ

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

Настоящая статья посвящена разработке и использованию многофункционального зонда для информационной безопасности, построенного на базе одноплатного компьютера Orange Pi 5 с операционной системой Armbian. Обсуждаются аспекты его применения в мониторинге сетевого трафика, управлении уязвимостями, предотвращении атак и расследовании инцидентов. Приведены основные этапы настройки и использования зонда, который может интегрироваться в сетевую инфраструктуру, повышая ее устойчивость к угрозам.

информационная безопасность, Orange Pi 5, Armbian, мониторинг, уязвимости, расследование инцидентов

В условиях растущих угроз информационной безопасности, обеспечение защиты сетевых инфраструктур требует современных и доступных решений. Одноплатный компьютер Orange Pi 5, работающий под управлением Armbian, является универсальной платформой для создания многофункционального зонда, способного выполнять мониторинг, управлять уязвимостями и проводить расследования инцидентов.

Orange Pi 5 оснащен 8-ядерным процессором Rockchip RK3588 и поддерживает до 32 ГБ оперативной памяти, что делает его подходящим для обработки сетевого трафика и выполнения сложных задач безопасности. Наличие множества интерфейсов позволяет использовать его для мониторинга и анализа трафика в реальном времени. ОС Armbian предоставляет оптимизированную для одноплатных компьютеров среду с инструментами для настройки сети и безопасностью (рис. 1).

Рис. 1. Одноплатный компьютер Orange Pi 5

Так же в Orange Pi 5 есть требуемый набор интерфейсов для подключения периферийных устройств и сетей, таких как гигабитный Ethernet, порты USB 3.0, HDMI и слот для карт памяти micro SD, при этом имеется возможность подключения и использования SSD M2 диска для размещения ОС и ПО, таким образом повышая производительность и высвобождая MicroSD разъем для доругих задач. Универсальность набора устройств позволяет интегрировать платформу в разные сетевые инфраструктуры и использовать в качестве основного элемента для мониторинга и анализа трафика.

Зонды на базе одноплатной платформы Orange Pi 5 и операционной системы Armbian могут осуществлять мониторинг сетевого трафика – основной элемент информационной безопасности. Реализация такой системы включает в себя несколько этапов, установку и настройку необходимого программного обеспечения, сбор, анализ данных и визуализацию результатов мониторинга [1].

Для мониторинга сетевого трафика на Orange Pi 5 можно использовать ряд инструментов с открытым исходным кодом, такие как Wireshark, tcpdump, Suricata. Все эти программы могут быть установлены на Orange Pi 5 через репозиторий Armbian с помощью пакетного менеджера apt. Совместно с зондом могут применяться устройства ответвления трафика Ethernet Suriken [2].

Далее после установки ПО нужно настроить и запустить мониторинг для перехвата всех отправленных и полученных пакетов. Для этого можно использовать Wireshark или tcpdump. Эти утилиты фильтруют трафик по различным критериям (IP-адрес, протокол, порт), что облегчает анализ и снижает нагрузку на систему.

Suricata можно настроить для работы в режиме анализа и предупреждения. Она поддерживает создание правил для обнаружения подозрительных

паттернов в трафике, таких как попытки сканирования портов или атаки с использованием известных уязвимостей [3].

Для анализа и визуализации данных, собранных с помощью зонда, можно использовать интеграцию с внешними системами или инструментами, такие как Grafana и Elastic Stack (ELK).

Автоматизации мониторинга и оповещения о критических событиях зонд можно настроить для отправки уведомлений при обнаружении угроз или аномалий в трафике. Тут помогут системы управления событиями, такие как Zabbix или Nagios, которые могут интегрироваться с Suricata и другими инструментами мониторинга.

Управление уязвимостями начинается с регулярного сканирования сети на наличие уязвимых точек, с использованием OpenVAS или Lynis. Обнаруженные уязвимости классифицируются по уровню критичности для дальнейшего приоритета устранения. Использование патч-менеджмента позволяет своевременно устранять выявленные уязвимости [4].

Предотвращение атак является одним из этапов защиты после выявления и устранения уязвимостей. Для этого можно использовать такие методы как системы предотвращения вторжений (IPS), межсетевые экраны (Firewall), анализ логов и реагирование.

Системы предотвращения вторжений (IPS), на базе Orange Pi 5, можно настроить с использованием Suricata, которая может работать как в режиме обнаружения атак (IDS), так и в режиме их предотвращения (IPS). Suricata анализирует сетевой трафик в реальном времени, выявляет подозрительные активности и может автоматически блокировать вредоносные пакеты.

Так же один из вариантов – это межсетевые экраны (Firewall). Межсетевые экраны (например, iptables или nftables) позволяют контролировать входящий и исходящий трафик на основе заданных правил. Это помогает ограничить доступ к критическим ресурсам сети и минимизировать риски от внешних угроз. Настройка правил firewall на Orange Pi 5 может включать блокировку несанкционированных подключений, фильтрацию трафика по IP-адресам и портам, а также контроль исходящего трафика.

Сбор и анализ логов сетевой активности и системных событий помогает обнаруживать подозрительные действия. Инструменты, такие как Fail2Ban могут автоматически блокировать IP-адреса, с которых проводятся подозрительные попытки входа, предотвращая атаки с подбором паролей. Интеграция с системой логов rsyslog и инструменты анализа, такие как Elastic Stack (ELK), позволят быстро выявлять подозрительные активности и реагировать на них.

Для успешного расследования инцидентов важно собирать как можно больше информации о событиях в системе и в сети. Многофункциональный

зонд на базе Orange Pi 5 позволяет организовать сбор данных в режиме реального времени с использованием нескольких подходов таких как логирование системных событий, анализ сетевого трафика и использование систем обнаружения вторжений (IDS).

Сбор журналов играет важную роль в расследованиях, он записывает каждое действие в системе. Такие инструменты, как rsyslog и journald, используются для сбора и хранения журналов, которые фиксируют данные о входах в систему, сетевой активности, запусках приложений и других системных событиях. Эта информация помогает определить момент возникновения атаки, отследить ее источник и понять ее природу. Журналы можно настроить для отправки на центральный сервер или интегрировать с системами управления журналами Elastic Stack (ELK).

Используются системы обнаружения вторжений (IDS) с помощью инструмента Suricata. Он находит применение для мониторинга трафика в реальном времени и автоматического обнаружения подозрительных действий. Suricata регистрирует инциденты, связанные с атаками, и сохраняет их для анализа. Эти журналы содержат сведения о сработавших правилах безопасности, помогая определить тип атаки, например сканирование портов или попытки эксплуатации уязвимостей.

Для автоматизации процесса расследования инцидентов можно использовать системы управления событиями безопасности и информацией (SIEM), такие как ELK Stack (Elasticsearch, Logstash, Kibana) или Graylog. SIEM-системы собирают логи и другие данные в одном месте, проводят корреляцию событий и предоставляют инструменты для анализа и визуализации. Это позволяет централизовать сбор данных, создавать правила для автоматического реагирования на угрозы и визуализировать инциденты для более эффективного анализа.

После выявления инцидента необходимо оперативно принять меры для его нейтрализации и минимизации последствий. Реагирование на инциденты включает несколько ключевых этапов это изоляция пострадавших систем, устранение уязвимостей, анализ и восстановление данных, улучшение защиты.

Важно как можно быстрее изолировать атакуемые или скомпрометированные системы от сети, чтобы предотвратить дальнейшее распространение атаки. Это можно сделать с помощью межсетевого экрана или вручную отключив подозрительные устройства от сети.

Если атака произошла из-за известной уязвимости, важно немедленно ее устранить. Это может включать установку обновлений безопасности, изменение конфигураций системы или отключение уязвимых сервисов. OpenVAS

или Lynis помогут обнаружить уязвимости, которые могли быть использованы для атаки [5].

После устранения угрозы нужно провести анализ последствий инцидента, чтобы оценить степень повреждения данных или системы. Важно восстановить систему до состояния, которое было до инцидента, используя резервные копии или другие меры по восстановлению.

После завершения инцидента нужно пересмотреть меры безопасности, чтобы предотвратить повторение атаки. Это включает улучшение конфигурации системы, обновление правил межсетевого экрана, установку дополнительных средств обнаружения и предотвращения угроз.

Для автоматизации оповещений можно использовать инструменты: Zabbix, Nagios, они могут отправлять уведомления при обнаружении подозрительных действий или срабатывании правил безопасности. Оповещения можно настраивать для отправки по электронной почте, в мессенджеры (например, Telegram), или в специализированные системы оповещения.

Таким образом, многофункциональный зонд на основе одноплатной платформы Orange Pi 5 с операционной системой Armbian представляет собой экономически выгодное и весьма гибкое решение для обеспечения информационной безопасности. Такой зонд дает возможность решать целый ряд задач: от мониторинга сетевого трафика и управления уязвимостями до предотвращения атак и оперативного реагирования на инциденты.

Преимущество данного решения заключается в применении широкого спектра инструментов с открытым исходным кодом: Suricata, OpenVAS, Wireshark, Lynis, и интеграция с платформами логирования и анализа данных, например ELK Stack. Это дает возможность в реальном времени отслеживать сетевую активность и предотвращать атаки. Проводить детальный анализ инцидентов, устраняя уязвимости по мере их обнаружения. Благодаря автоматизации процессов с использованием SIEM-систем, Graylog и ELK, облегчает процесс расследования инцидентов и управления безопасностью.

Список используемых источников

1. Flamy-AI. Инструкции по настройке системы безопасности на базе Orange Pi 5. URL: https://github.com/flamy-ai/orange-pi-5-security-camp (дата обращения 10.10.2024).
2. Armbian. Документация по настройке и использованию ОС Armbian для одноплатных компьютеров, таких как Orange Pi. URL: https://docs.armbian.com/ (дата обращения 10.10.2024).
3. Lynis. Инструмент для аудита безопасности и управления уязвимостями в системах на базе Linux. URL: https://cisofy.com/lynis/ (дата обращения 11.10.2024).
4. Fail2Ban. Инструмент для защиты от атак и предотвращения брутфорс-атак. URL: https://www.fail2ban.org/ (дата обращения 11.10.2024).

5. OpenVAS. Open Vulnerability Assessment System. URL: https://www.greenbone.net/en/openvas/ (дата обращения 12.10.2024).

Minochenkov N. **ORGANIZING MONITORING, VULNERABILITY MANAGEMENT AND INCIDENT INVESTIGATION USING A MULTIFUNCTIONAL PROBE BASED ON A SINGLE-BOARD COMPUTING PLATFORM.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article is devoted to the development and use of a multifunctional probe for information security, built on the basis of a single-board computer Orange Pi 5 with the Armbian operating system. Aspects of its application in monitoring network traffic, vulnerability management, preventing attacks and investigating incidents are discussed. The main stages of setting up and using the probe, which can be integrated into the network infrastructure, increasing its resilience to threats, are given.

Key words: information security, Orange Pi 5, Armbian, monitoring, vulnerabilities, incident investigation.

УДК 004.056.5
ГРНТИ 81.93.29

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОС НА БАЗЕ OPENSOURCE РЕШЕНИЙ

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

Растущая распространенность внедрения ОС на базе открытого исходного кода представляет увеличение угроз связанных с ними. По мере того как методы возникновения уязвимостей эволюционируют, они все чаще обходят традиционные методы обнаружения, используя различные компоненты и библиотеки интегрированные в системы.

ОС, уязвимости, открытый исходный код

Операционные системы на базе решений с открытым исходным кодом, такие как Linux, получают все большее распространение в корпоративной среде и государственных учреждениях. Однако активное внедрение подобных решений связано с ростом числа инцидентов, связанных с киберугрозами. По данным компании «Лаборатория Касперского», количество инцидентов с конкурентным программным обеспечением значительно увеличилось в 2023 году. Особенно остро стоит проблема уязвимостей в компонентах с открытым исходным кодом, где большое внимание уделяется использованию устаревших и необновленных библиотек.

Например, уязвимость Log4Shell в Apache Log4j, обнаруженная в 2021 году, привела к возникновению систем компрометации, многие из которых работали над ОС с открытым исходным кодом [1].

Согласно отчету OpenLogic и Open Source Initiative за 2023 год, 80 % организаций расширили использование технологий Open Source, в том числе операционных систем. Тем не менее, они сталкиваются с такими проблемами, как нехватка квалифицированных специалистов и сложности с регулярным обновлением компонентов. В ответ на эти вызовы 37 % компаний начали вкладывать средства в обучение сотрудников и юридическую поддержку для обеспечения использования открытого исходного кода [2].

На данный момент чаще всего уязвимости встречаются в следующих компонентах ОС собранных на базе открытого исходного кода, которые представлены в таблице 1.

ТАБЛИЦА 1. Частые уязвимости компонентов ОС на базе OpenSource

Компонент	Уязвимость	Проблемы вызванные уязвимстью
Ядро Linux	StackRot (CVE-2023-3269)	Уязвимость в управлении стековой памятью позволяет локальному пользователю повышать привилегии и выполнять произвольный код
Библиотеки	OpenSSL (Heartbleed)	Уязвимости в криптографических библиотеках приводят к утечке данных
Менеджеры пакетов	Npm, PyPI	Атаки на цепочку поставок из-за режима зависимости
Сетевые сервисы	OpenSSH, OpenVPN	Обход аутентификации и уничтожение данных при ошибках в обеспечении
Web-сервисы	Apache, Nginx	SQL-инъекции, XSS и RCE из-за уязвимостей при обработке запросов
Системы контейнеризации	Docker, Kubernetes	Эскалация привилегий через уязвимости в конфигурации контейнеров
Базы данных	MySQL, PostgreSQL	Атаки через незащищенные конфигурации и уязвимости в логике обработки запросов

Методы по решению проблем, связанных с уязвимостями, требуют комплексного ограничения безопасности операционных систем с открытым исходным кодом. Компании и разработчики должны уделять особое внимание анализу и выбору решений с открытым исходным кодом, чтобы минимизировать риски и обеспечить свою защиту труда.

Пути возникновения уязвимостей

Ошибки в коде: при эксплуатации ПО и ОС на базе открытого исходного кода, уязвимости возникают по причинам человеческого фактора и включением компонентов с некорректным использованием функций или модулей, что приводит к утечкам информации и небезопасному вызову системных функций.

Использование уязвимых зависимостей: программные продукты на основе открытого исходного кода часто включают в себя библиотеки и модули, которые разрабатываются независимыми командами или разработчиками. Уязвимости таких зависимостей могут проникнуть в конечное ПО, если эти библиотеки не обновляются регулярно или если разрабатываемое ПО не проходит тщательное тестирование [3].

Человеческий фактор: недостаток знаний у разработчиков или отсутствие культуры безопасности в компании может привести к внедрению уязвимых решений. Частой проблемой является отключение проверки SSL-сертификатов в коде при разработке часто забывается и остается включенным в продакшн-версиях.

Также проблемой обеспечения безопасности ОС на базе применения решений с открытым исходным кодом является существование фактических и юридических коллизий по поддержке и обеспечению безопасности выпущенных продуктов. Можно выделить три основные:

1. Фактологическая: компании должны обеспечивать и поддерживать мейнтейн, иметь при себе различные технологии и среды для тестирования продуктов. Тестирование не должно проводится с использованием одного сценария возникновения уязвимости и устранения ее. Необходимо проводить статический и динамический анализ ПО в длительных промежутках времени;

2. Юридическая: компании должны иметь ответственность за выпускаемое и разрабатываемое ПО. Если ПО распространяется на платной основе, компания должна производить функциональную готовность для внесения исправлений, стабильность. Сотрудники компании должны иметь минимальный уровень кибербезопасности при работе с пользовательскими данными во избежания утечек информации;

3. Отслеживание событий: компании обязаны иметь при себе некоторые доказательства, что используют прописанные продукты и руководствуются заданными стандартами безопасности. Какие системы журналирования используются, что входит в системы логирования. Необходима честная и прописанная в документах доказательная база.

Избежать возможных проблемы связанных с ОС разработанными на базе решений с открытым исходным кодом можно следующими методами:

– минимизировать количество библиотек и компонентов, включенных в систему. Чем меньше существует зависимостей, тем ниже риск возникновения уязвимостей;

– использовать проверенные и официальные образы контейнеров, проводить регулярное сканирование на наличие уязвимостей;

– пересобрать компоненты исходного кода, проверив ненужные модули, чтобы контролировать состав и системы безопасности;

– применять строгие системы безопасности, такие как контроль прав доступа и мониторинг событий, а также регулярно обновлять разработанные продукты.

Краткое резюме выводов

Для эффективного предотвращения проблем безопасности при использовании ОС на базе открытого исходного кода необходимо подходить к решению проблем с различной стороны: минимизация зависимостей, пересборка компонентов, использование проверенных контейнеров и систем. Соблюде-

ние методических рекомендаций и внедрение мер безопасности на всех этапах эксплуатации помогают снизить риски и повысить защищенность систем.

Направления будущих исследований

Будущие исследования в области безопасности ОС на базе решений с открытым исходным кодом будут сосредоточены на разработке более эффективных инструментов автоматического анализа уязвимостей, включая интеграцию машинного обучения. Улучшить безопасность контейнеризированных средств, разработав более сложные методы предоставления и обеспечения безопасности. Также необходимы новые стандарты тестирования безопасности, включая стимулирующий и статический анализ, чтобы повысить качество защиты. Важным направлением является исследование компаний, ответственных за внедрение ОС с открытом исходным кодом в Российской Федерации, использующих решения с открытым исходным кодом, для устранения исправлений уязвимостей и соблюдения стандартов безопасности.

Список используемых источников

1. Открытый исходный код: топ-10 рисков для бизнеса. URL: https://www.kaspersky.com/blog/open-source-top-10-risks/47875/ (дата обращения 05.11.2024).
2. Отчет 2023 State of Open Source: основные выводы и анализ. URL: https://opensource.org/blog/2023-state-of-open-source-report-key-findings-and-analysis (дата обращения 07.11.2024).
3. Компоненты ПО с открытым кодом могут содержать уязвимости. Как повысить безопасность кода? URL: https://web-control.ru/novosti/news_post/komponenty-po-s-otkrytym-kodom-mogut-soderzhat-uyazvimosti-kak-povysit-bezopasnost-koda (дата обращения 09.11.2024).

Nizhlukchenko I. **PROBLEMS OF OS SECURITY ON THE BASIS OF OPENSOURCE SOLUTIONS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The growing prevalence of OpenSource OS deployments presents an increase in the threats associated with them. As vulnerability techniques evolve, they increasingly bypass traditional detection methods by utilizing various components and libraries integrated into systems.

Key words: OS, vulnerabilities, OpenSource.

УДК 004.056
ГРНТИ 81.93.29

АВТОМАТИЗАЦИЯ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ: АНАЛИЗ ПРЕИМУЩЕСТВ И ВОЗНИКАЮЩИХ ПРОБЛЕМ

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

Автоматизация тестирования безопасности веб-приложений становится все более актуальной в связи с ростом числа кибератак и повышением требований к безопасности информационных систем. Традиционные методы ручного тестирования не всегда позволяют обеспечить необходимое качество и скорость проверки веб-приложений. Автоматизация тестирования позволяет значительно повысить эффективность и точность выявления уязвимостей, что в свою очередь снижает риски возникновения инцидентов информационной безопасности.

безопасность, веб-приложение, тестирование безопасности, автоматизация

Автоматизированные средства тестирования безопасности веб-приложений

Автоматизированное тестирование – процесс тестирования веб-приложений с использованием средств автоматизации, сканеров уязвимостей (Sqlmap, Xsstrike, Burp Scanner, OWASP ZAP, Nessus) [1].

Автоматизация тестирования безопасности веб-приложений стала неотъемлемой частью процесса разработки современного программного обеспечения. По сравнению с ручным тестированием, автоматизация предлагает ряд существенных преимуществ, которые позволяют повысить эффективность и надежность обеспечения безопасности веб-приложений.

Автоматизированное тестирование обладает множеством достоинств, связанных главным образом с высокой скоростью выполнения тестов и возможностью выполнять однотипные тесты снова и снова [2].

Качество тестирования также существенно повышается при использовании автоматизации. Автоматизированные тесты выполняются с высокой точностью и повторяемостью, что минимизирует риск возникновения человеческих ошибок. Это позволяет обнаруживать даже самые незначительные уязвимости, которые могут быть пропущены при ручном тестировании.

Автоматизация тестирования также способствует снижению затрат на исследование безопасности информационных систем. Хотя первоначальные инвестиции в приобретение и настройку инструментов автоматизации могут

быть значительными, в долгосрочной перспективе эти затраты окупаются за счет сокращения времени тестирования и повышения эффективности работы тестировщиков. Кроме того, автоматизация позволяет избежать ошибок, которые могут привести к дорогостоящим инцидентам безопасности.

Наконец, автоматизация тестирования позволяет обеспечить более высокий уровень безопасности веб-приложений. Регулярное автоматизированное тестирование позволяет выявлять уязвимости на ранних этапах разработки, что существенно снижает риски успешной эксплуатации этих уязвимостей злоумышленниками. Автоматизация также позволяет проводить более глубокий анализ безопасности, выявляя сложные и трудно обнаруживаемые уязвимости.

Несмотря на очевидные преимущества, автоматизация тестирования безопасности веб-приложений сопряжена с рядом проблем и ограничений.

Одной из наиболее значимых является ограниченная возможность тестирования некоторых типов уязвимостей. Автоматизация эффективна для обнаружения известных уязвимостей, но менее приспособлена для выявления новых, нестандартных угроз, требующих творческого подхода и глубокого понимания принципов работы приложения.

Помимо ограничений тестирования некоторых типов уязвимостей, стоит отметить, что при автоматизированном тестировании возможны ложные срабатывания, что требует значительных временных затрат на их проверку.

Из проблем автоматизированного тестирования также стоит выделить ограниченную глубину анализа, так как автоматизированные инструменты в основном ориентированы на поиск известных уязвимостей, и могут пропустить нестандартные и сложные атаки. Такие задачи, как безопасность API или нарушения, осуществляемые человеком (например, атаки методом подбора), не являются сильной стороной автоматизированного теста на проникновение [3].

Ручное тестирование безопасности веб-приложений

Помимо автоматизированных инструментов, в процессе тестирования на проникновение широко применяется ручное тестирование. Ручное тестирование – это процесс тестирования веб-приложений специалистами вручную для выявления уязвимостей и недочетов в безопасности системы [1]. Оно позволяет эксперту по безопасности глубоко погрузиться в систему, анализировать ее поведение в различных условиях и обнаруживать уязвимости, которые могут быть пропущены автоматизированными сканерами.

К преимуществам ручного тестирования можно отнести следующее:

1. Гибкость. Эксперт может адаптироваться к динамично меняющейся среде и изменять стратеги атаки в зависимости от полученных результатов;

2. Творческий подход. Человек способен мыслить нестандартно и находить уязвимости, которые не описаны в базах данных известных уязвимостей;

3. Глубокий анализ. Ручное тестирование позволяет детально изучить логику работы приложения, что помогает обнаружить уязвимости, связанные с особенностями его реализации;

4. Тестирование социальной инженерией. Многие уязвимости связаны с человеческим фактором. Ручное тестирование позволяет оценить устойчивость сотрудников к социальным атакам.

Из недостатков ручного тестирования стоит отметить следующее:

1. Высокая стоимость. Ручное тестирование требует значительных временных затрат и привлечения высококвалифицированных специалистов;

2. Субъективность. Результаты ручного тестирования могут зависеть от опыта и знаний конкретного эксперта;

3. Ограниченная масштабируемость. Ручное тестирование сложно масштабировать для больших и сложных систем.

Автоматизированное и ручное тестирование – два взаимодополняющих подхода, каждый из который имеет свои преимущества и недостатки. Для наглядного сравнения этих двух подходов ниже приведена таблица 1.

ТАБЛИЦА 1. Сравнение автоматизированного и ручного тестирования безопасности веб-приложений

Критерий	Автоматизированное тестирование	Ручное тестирование
Скорость	Высокая скорость выполнения тестов	Низкая скорость из-за ручного выполнения каждого теста
Покрытие	Широкое покрытие известных уязвимостей	Глубокий анализ, возможность обнаружить нестандартные уязвимости
Стоимость	Высокие первоначальные инвестиции в инструменты, но низкая стоимость выполнения тестов в долгосрочной перспективе	Низкие первоначальные затраты, но высокая стоимость выполнения тестов в долгосрочной перспективе
Масштабируемость	Высокая масштабируемость для больших проектов	Низкая масштабируемость для больших и сложных проектов
Обнаружение новых уязвимостей	Ограниченное обнаружение новых, нестандартных уязвимостей	Высокая вероятность обнаружения новых уязвимостей
Гибкость	Низкая гибкость из-за заранее определенных сценариев	Высокая гибкость, возможность адаптироваться к меняющимся условиям

Список используемых источников

1. Барулина В. В. Сравнительная характеристика ручного и автоматизированного тестирования программного обеспечения // Вестник магистратуры, 2020. № 4-2 (103).
2. Берегейко О. П., Дубовский А. С. Автоматизация тестирования веб-приложений // Вестник магистратуры, 2016. №12-4 (63).
3. Что такое автоматизированное тестирование на проникновение. URL: https:// continuumgrc.com/ru/what-is-automated-penetration-testing/ (дата обращения 13.11.2024).

Novikov D. **AUTOMATED TESTING FOR WEB APPLICATION SECURITY: A COMPARATIVE ANALYSIS OF BENEFITS AND DRAWBACKS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The automation of web application security testing is becoming increasingly relevant due to the growing number of cyberattacks and rising security requirements for information systems. Traditional manual testing methods do not always provide the necessary quality and speed for assessing web applications. Automating security testing significantly improves the efficiency and accuracy of vulnerability detection, thereby reducing the risk of information security incidents.

Keywords: security, web application, security testing, automation.

УДК 004.041
ГРНТИ 20.53.19

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МУЛЬТИЯЗЫЧНЫХ ПАРСЕРОВ ПРОГРАММНОГО КОДА НА ПРИМЕРЕ ЯЗЫКОВ PYTHON И JAVASCRIPT

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

В данной работе проведен сравнительный анализ мультиязычных парсеров программного кода на примере Python и JavaScript. Исследование оценивает эффективность парсеров при обработке кода на этих языках, результатом которого является выбор наилучшего решения для применения в высоконагруженных анализаторах вредоносного программного обеспечения.

ANTLR4, tree-sitter, Lark, python, javascript, сравнительный анализ

Развитие открытого исходного кода стало ключевым фактором прогресса в сфере программирования. Без открытого доступа к коду и коллективного вклада разработчиков со всего мира, многие технологические достижения были бы невозможны. В сообществе наиболее популярными языками являются JavaScript и Python [1], благодаря их гибкости и широкому спектру применения, они стали основой для множества проектов, способствуя обмену идеями и ускоряя инновации.

Распространение открытого исходного кода несет и потенциальные угрозы безопасности. Скачивая пакеты из PyPi, npm и аналогичных менеджеров, есть риск нечаянно загрузить и запустить на своем компьютере вредоносное программное обеспечение собственноручно [2]. Образы контейнеров Docker и расширения для Visual Studio Code также не являются исключением. Поэтому важно уделять внимание безопасности открытого кода, чтобы защитить сообщество от действий злоумышленников. Постоянный аудит и проверка исходного кода становятся необходимыми мерами для обеспечения надежности и безопасности проектов.

В связи с этим возникает необходимость в специализированных инструментах, способных обеспечить тщательный анализ кода на различных языках программирования. Мультиязычные парсеры программного кода становятся ключевым звеном в этом процессе, так как они позволяют автоматически обрабатывать и проверять исходные тексты на языках, для которых есть грамматика и лексика. Также эти парсеры строят абстрактное синтаксическое дерево, что необходимо для комфортной обработки кода после парсинга.

Первичным характеристиками отбора мультиязычных парсеров были выбраны: наличие библиотеки для работы с языком программирования Python, построение абстрактного синтаксического дерева и поддержка сообщества. Под поддержкой сообщества понимается количество скачиваний в менеджере пакетов PyPi [3] и количество звезд на репозитории. Более конкретный анализ представлен в таблице 1.

ТАБЛИЦА 1. Первичный отбор мультиязычных парсеров

Название	Скачиваний в месяц	Количество звезд	Построение AST
antlr4-python3-runtime	16784161	17200	Да
tree-sitter-python	537996	18600	Да
Lark	9399012	4900	Да

Таким образом, для последующего анализа были выбраны ANTLR 4 версии, tree-sitter и Lark, который прошли по первичным критериям отбора.

В репозитории парсера Lark есть сравнительный график двух алгоритмов Lark и парсера ANTLR по скорости выполнения и использованию памяти, результаты представлены на рисунке 1.

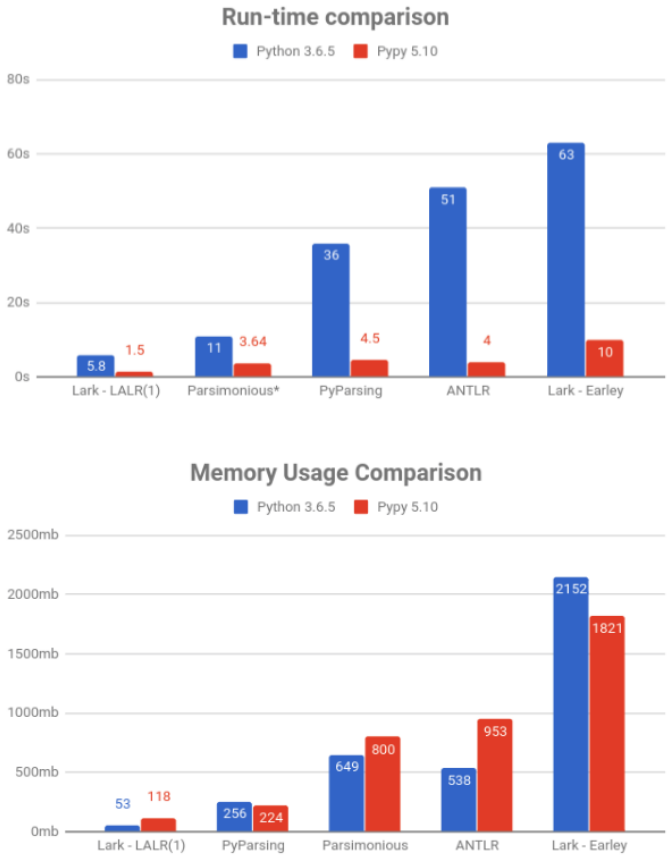


Рис. 1. Сравнительный график Lark и ANTLR

Исходя из этих данных, можно сказать, что Lark на алгоритме LALR значительно превосходит ANTLR, но на этом его преимущества закачиваются. О слабостях Lark речь пойдет далее.

Из выбранных парсеров была составлена таблица с их теоретическими характеристиками [4], они представлены в таблице 2.

ТАБЛИЦА 2. Теоретические характеристики парсеров

Характеристика	ANTLR4	Tree-sitter	Lark
Алгоритм парсинга	Адаптивный LL	LR	LALR
Токенов для просмотра	Адаптивный	1	1
Асимптотическая сложность	O(n^4)	O(n)	O(n)
Стратегия парсинга	Сверху вниз	Снизу вверх	Снизу вверх
Генерация AST	Да	Да	Да
Устойчивость к ошибкам	Да	Да	Нет

ANTLR4 использует адаптивный LL-парсинг [5]. Этот алгоритм является развитием классического LL-парсинга и способен динамически адаптироваться к особенностям грамматики во время выполнения. Он комбинирует предсказательный парсинг с возможностью использования предикатов и бэк-трекинга, что позволяет обрабатывать более широкий класс грамматик, включая некоторые неоднозначные конструкции [6].

Tree-sitter основан на алгоритме LR-парсинга. LR-парсеры читают входную последовательность слева направо и строят правый вывод снизу вверх. Алгоритм LR использует один токен для просмотра вперед, что обеспечивает детерминизм и возможность парсинга контекстно-свободных грамматик без необходимости бэк-трекинга.

Lark применяет алгоритм LALR-парсинга (Look-Ahead LR). LALR является оптимизацией LR, которая уменьшает количество состояний в таблицах парсера, сохраняя при этом способность распознавать большинство практических языков программирования. Это достигается путем объединения состояний, имеющих одинаковые элементы ядра.

У ANTLR4 асимптотическая сложность в худшем случае составляет $O(n^4)$ [7]. Такая высокая сложность связана с использованием бэк-трекинга и предикатов в адаптивном LL-парсинге. В ситуациях с сильно неоднозначными грамматиками или при обширном использовании предикатов, парсер может затрачивать значительные ресурсы для разрешения вариантов разбора.

Tree-sitter и Lark имеют линейную сложность O(n), что означает, что время парсинга пропорционально размеру входных данных. Это достигается

благодаря детерминированности алгоритмов LR и LALR, которые не требуют бэк-трекинга и могут парсить входную последовательность за один проход.

Парсинг сверху вниз, используемый в ANTLR4, начинает разбор с начального символа грамматики и пытается развернуть его в последовательность терминалов, соответствующих входным данным [8]. Этот метод интуитивно понятен и удобен для реализации семантических действий, но может столкнуться с проблемами при обработке леворекурсивных правил и требует осторожности при разработке грамматики.

Парсинг снизу вверх, применяемый в Tree-sitter и Lark, работает, начиная с входных токенов, и постепенно объединяет их в нетерминалы по правилам грамматики, движется к начальному символу. Этот подход более устойчив к леворекурсивным грамматикам и часто более эффективен для сложных языков.

Затем было проведено исследование скорости парсинга и построения абстрактного синтаксического дерева на ста наиболее популярных Python и JavaScript пакетах. В таблице 3 представлены средние время парсинга одного пакета с помощью соответствующих парсеров.

ТАБЛИЦА 3. Эмпирическое сравнение скорости парсинга

	ANTLR для js	ANTLR для python	tree-sitter для js	tree-sitter для python
Среднее время парсинга одного пакета	25,170	237,780	0,016	0,214

Стоит также отметить, что парсер Lark не смог составить конкуренцию ANTLR4 и tree-sitter, поскольку для него отсутствуют готовые грамматики для языка JavaScript, а при использовании грамматики для Python3, парсер выдает ошибку при первом дандер-методе. Это делает его менее практичным для использования в реальных проектах, где необходима поддержка распространенных языков.

Стоит отметить удобство использования tree-sitter. Для того, чтобы собрать и запустить ANTLR4, разработчику бы понадобилось намного больше действий и преодолеть намного больше проблем, чем для запуска tree-sitter.

В результате проведенного анализа можно сделать вывод, что лучшим парсером среди рассмотренных оказался tree-sitter. Он демонстрирует наилучшую производительность и обладает линейной сложностью, что делает его оптимальным выбором для высоконагруженных систем, где скорость исполнения является критически важным фактором. ANTLR4, хотя и уступает в скорости, обладает преимуществами в виде гибкости, что может быть полезно для

сложных грамматик и ситуаций, где требуется адаптивность. Однако для систем с высокой нагрузкой tree-sitter явно выигрывает, позволяя избежать необходимости держать десятки контейнеров для обработки каждого пакета.

Список используемых источников

1. The top programming languages // Octoverse Github. URL: https://octoverse.github.com/2022/top-programming-languages (дата обращения 12.11.2024).
2. Rakovsky S., Magomedov S. Ensuring the Security of Open Python Projects: The Challenge of Assessing Potentially Destructive Functionality // International Journal of Open Information Technologies, 2023. Т. 11. № 10. С. 113–118.
3. Ищите, устанавливайте, публикуйте Python-пакеты в индексе пакетов Python // pypi. URL: https://pypi.org/ (дата обращения 14.11.2024).
4. Afshan L., Farooque A., Muhammad W. A. Comparison of leading language parsers – antlr, javacc, sablecc, tree-sitter, yacc, bison // 13th International Conference on Software Technology and Engineering, Osaka, Japan, 27-29 oct 2023. PP. 7–13.
5. Ortin F., Quiroga J., Rodrigez-Prieto O. An empirical evaluation of lex/yacc and antlr parser generation tools // plos one 2022. Vol. 17. № 3.
6. Осипов О. К. Описание контекстно-свободных грамматик в формате данных json для генераторов синтаксических анализаторов // Электронные библиотеки, 2022. № 6. С. 1301-1323.
7. Зоркин А. С., Змеев Д. О. Гибридный алгоритм поиска академического плагиата исходного кода с использованием парсера antlr // Материалы XX Международной конференции имени А. Ф. Терпугова. Томск: Национальный исследовательский Томский государственный университет, 2022. С. 13–18.
8. Sosinskaya S. S., Dorofeev R. S., Dorofeev A. S. Automation of a decision tree conversion into a fuzzy inference system using antlr // 43rd international convention on information, communication and electronic technology, mipro proceedings. Opatija: Institute of Electrical and Electronics Engineers Inc., 2020. С. 1024–1027.

Pimashin E. **COMPARATIVE ANALYSIS OF MULTILINGUAL CODE PARSERS: A CASE STUDY OF PYTHON AND JAVASCRIPT.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This work presents a comparative analysis of multilingual code parsers using Python and JavaScript as examples. The study evaluates the efficiency of parsers in processing code written in these languages, resulting in the selection of the most suitable solution for use in high-load malware analysis systems.

Key words: ANTLR4, tree-sitter, Lark, python, javascript, comparative analysis.

УДК 004.056
ГРНТИ 81.93.29

АВТОМАТИЗИРОВАННЫЙ АНАЛИЗ ИЗМЕНЕНИЙ В СЕТЕВЫХ КОНФИГУРАЦИЯХ УСТРОЙСТВ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

В. Д. Проничев, И. А. Ушаков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе предлагается ознакомиться с реализацией нейронной сети для обнаружения изменений в конфигурационных файлах на базе DMVPN (Dynamic Multipoint Virtual Private Network) сети. Данная модель использует ранее сформированный эталонный конфигурационный файл и обучается на нем для выявления отклонений, которые информируют об изменениях в конфигурации. В статье представлены основные этапы по подготовке данных, построении архитектуры сети и ее дальнейшем использовании.

изменение конфигурации, нейронные сети, DMVPN, эталонная конфигурация, бинарная классификация, информационная безопасность

Введение

Нейронные сети представляют собой основу современного искусственного интеллекта [1]. Вдохновленные человеческим мозгом, они успешно решают сложные задачи, недоступные традиционным методам обработки данных [2].

В области кибербезопасности нейронные сети могут использоваться для [3]:

– обнаружение вторжений;

– создание устойчивых моделей информационных систем;

– обнаружение мошеннических действий и вредоносного программного обеспечения;

– оценка риска и анализ поведения системы.

Особенность нейронных сетей – способность обнаруживать скрытые зависимости и предотвращать комплексные угрозы безопасности.

Существуют разные архитектуры построения нейронных сетей [4]:

– однослойная;

– многослойная (MLP);

– сверточная (CNN);

– рекуррентная (RNN);

– генеративно-состязательная (GAN).

В данной работе будет использована рекуррентная нейронная сеть, а именно LSTM (Long Short-Term Memory), способная эффективно обрабатывать последовательные данные.

Основная часть

Целью данной работы является разработка нейронной сети для обнаружения изменений в конфигурации DMVPN на основе эталонного конфигурационного файла.

Для решения поставленной цели были сформированы следующие задачи:

– подготовка данных;

– преобразование данных для обучения сети;

– архитектура модели;

– обучение и тестирование модели;

– анализ результатов.

Подготовка данных

Макет сети был собран на базе отечественного оборудования Eltex ESR-200 [5]. В качестве примера сформируем эталонный конфигурационный файл на основе конфигурации одного из маршрутизаторов, как показано на рис. 1.

```
#НАСТРОЙКА ИНТЕРФЕЙСОВ#
int gi 1/0/5
    ip firewall enable
    ip address 10.10.10.1/30
int gi 1/0/7
    ip firewall enable
    ip address 10.110.10.1/24
```

```
#НАСТРОЙКА IPSEC#
security ike proposal IKE_PROP_HUB_1
    dh-group 14
    authentication algorithm sha2-512
    encryption algorithm aes256

security ike policy IKE_POL_HUB_1
    pre-shared-key ascii-text encrypted ABC0FF
    proposal IKE_PROP_HUB_1

security ike gateway IKE_GW_HUB_1
    ike-policy IKE_POL_HUB_1
    local address 10.110.10.1
    local network 10.110.10.1/32 protocol gre
    remote address 192.168.20.10/32
    remote network 192.168.30.10/32
    mode policy-based

security ipsec proposal IPSEC_PROP_HUB_1
    authentication algorithm sha2-512
    encryption algorithm aes256

security ipsec policy IPSEC_POL_HUB_1
    proposal IPSEC_PROP_HUB_1
security ipsec vpn IPSEC_HUB_1
    mode ike
    ike establish-tunnel route
    ike gateway IKE_GW_HUB_1
    ike ipsec-policy IPSEC_POL_HUB_1
```

```
#НАСТРОЙКА GRE-ТУННЕЛЯ#
configure
    tunnel gre 1
    local address 10.110.10.1
    ip address 172.16.1.1/29
    multipoint
    ip firewall enable
    ip nhrp multicast dynamic
    ip nhrp ipsec IPSEC_HUB_1 dynamic
```

```
#ACCESS LIST#
ip access list extended Service_inf
    rule 1
        match source-address any
        match destination-address any
        action permit

route-map DMVPN_BGP
    rule 1
    exit

route-map DMVPN_PBR
    rule 1
        match ip access group Service_inf

int gi 1/0/7
    ip policy route-map DMVPN_PBR
```

```
#МАРШРУТИЗАЦИЯ BGP#
router bgp 65000
    neighbor 172.16.1.2
        update-source 172.16.1.1
        bfd-enable
        remote-as 65002
        address-family ipv4 unicast
            route-map DMVPN_BGP in
            route-map DMVPN_BGP out
    neighbor 172.16.1.3
        update-source 172.16.1.1
        bfd-enable
        remote-as 65003
        address-family ipv4 unicast
            route-map DMVPN_BGP in
            route-map DMVPN_BGP out
```

Рис. 1. Эталонная конфигурация

Для обучения модели необходимо создать как эталонные (рис. 1), так и модифицированные версии конфигурационных файлов. Пример показан на рис. 2, где слева эталонная конфигурация, а справа – модифицированная.

```
#НАСТРОЙКА ИНТЕРФЕЙСОВ#
int gi 1/0/5
    ip firewall enable
    ip address 10.10.10.1/30
int gi 1/0/7
    ip firewall enable
    ip address 10.110.10.1/24

#МАРШРУТИЗАЦИЯ BGP#
router bgp 65000
    neighbor 172.16.1.2
        update-source 172.16.1.1
        bfd-enable
        remote-as 65002
        address-family ipv4 unicast
            route-map DMVPN_BGP in
            route-map DMVPN_BGP out
```

```
#НАСТРОЙКА ИНТЕРФЕЙСОВ#
int gi 1/0/5
    ip firewall disable
    ip address 10.10.10.1/30
int gi 1/0/7
    ip firewall disable
    ip address 10.110.10.4/24

#МАРШРУТИЗАЦИЯ BGP#
router bgp 65002
    neighbor 172.16.1.2
        update-source 172.16.1.5
        bfd-enable
        remote-as 65000
        address-family ipv4 unicast
            route-map DMVPN_DGP in
            route-map DMVPN_DGP out
```

Рис. 2. Выборка конфигураций

Разметка добавляется к каждому конфигурационному файлу, где метка 0 означает, что конфигурация соответствует эталону, а 1 – конфигурация с модификацией.

Преобразование данных для обучения

Для обработки текста нейронной сетью необходимо разбить конфигурационные файлы на токены [6], что позволит преобразует текст в формат, который нейронная сеть сможет анализировать и обучаться на нем.

На рис. 3 показан пример объявления двух списков, где первый представляет собой конфигурации, а второй метки, которые указывают, являются ли эти конфигурации эталонными или измененными.

```
configs = [
    "int gi 1/0/5 ip firewall enable ip address 10.10.10.1/30
int gi 1/0/7 ip firewall enable ip address 10.110.10.1/24
router bgp 65000 neighbor 172.16.1.2 update-source 172.16.1.1"
    "int gi 1/0/5 ip firewall disable ip address 10.10.10.1/30
int gi 1/0/7 ip firewall disable ip address 10.110.10.4/24
router bgp 65002 neighbor 172.16.1.2 update-source 172.16.1."
]
labels = [0,1]
```

Рис. 3. Токенизация

Теперь необходимо подготовить эти данные для подачи в нейронную сеть и ее последующего обучения, преобразуя текст в числовые последовательности (векторизация), как показано на рис. 4.

```
from tensorflow.keras.preprocessing.text import Tokenizer
from tensorflow.keras.preprocessing.sequence import pad_sequences

tokenizer = Tokenizer(num_words=1000)
tokenizer.fit_on_texts(configs)
sequences = tokenizer.texts_to_sequences(configs)
X = pad_sequences(sequences, maxlen=100)
y = labels
```

Рис. 4. Векторизация

Архитектура модели

Как отмечалось ранее, была выбрана рекуррентная нейронная сеть (RNN), а именно LSTM. На рис. 5 показан код, который создает и компилирует модель нейронной сети на основе LSTM для задачи бинарной классификации.

```
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import LSTM, Dense, Embedding

model = Sequential()
model.add(Embedding(input_dim=1000, output_dim=64, input_length=50))
model.add(LSTM(64, return_sequences=False))
model.add(Dense(1, activation='sigmoid'))

model.compile(optimizer='adam', loss='binary_crossentropy', metrics=['accuracy'])
```

Рис. 5. Построение нейронной сети

Обучение и тестирование модели

Данные разделяются на тренировочные и тестовые для оценки производительности, а также обучаем модель и оцениваем ее на тестовой выборке, как показано на рис. 6.

```
from sklearn.model_selection import train_test_split

X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)

model.fit(X_train, y_train, epochs=10, batch_size=32, validation_data=(X_test, y_test))
```

Рис. 6. Обучение и тестирование модели

Завершив обучение, модель может быть использована для анализа новых конфигураций, в случае обнаружения изменений от эталона, модель возвращает вероятность наличия таких изменений (рис. 7).

```
new_config = "int gi 1/0/6 ip firewall disable ip address 10.12.10.1/30
int gi 1/1/7 ip firewall enable ip address 10.110.10.1/24
router bgp 65000 neighbor 172.16.1.2 update-source 172.16.1.1"
new_sequence = tokenizer.texts_to_sequences([new_config])
new_sequence_padded = pad_sequences(new_sequence, maxlen=100)

prediction = model.predict(new_sequence_padded)
if prediction > 0.7:
    print("Есть изменения!")
else:
    print("Изменений нет")
```

Рис. 7. Проверка модели на новой конфигурации

Для проверки работоспособности в список конфигураций и меток было добавлено множество эталонных и модифицированных конфигураций, как показано на рис. 8.

```
configs = [
    "int gi 1/0/5 ip firewall enable ip address 10.10.10.1/30",
    "int gi 1/0/6 ip firewall enable ip address 10.10.10.2/30",  # Изменён IP
    "int gi 1/0/7 ip firewall enable ip address 10.110.10.1/24",
    "int gi 1/0/8 ip firewall enable ip address 10.120.10.1/24",  # Изменён IP
    "int gi 1/0/5 ip firewall enable ip address 10.10.10.1/30",
    "int gi 1/0/7 ip firewall disable ip address 10.120.10.1/24",  # Изменён IP и firewall
    "int gi 1/0/5 ip firewall enable ip address 10.10.10.1/30",
    "int gi 1/0/7 ip firewall enable ip address 10.130.10.1/24",  # Изменён IP
    "int gi 1/0/5 ip firewall enable ip address 10.10.10.1/30",
    "int gi 1/0/7 ip firewall enable ip address 10.120.20.1/24",  # Изменён IP
    "int gi 1/0/5 ip firewall enable ip address 10.10.10.1/30",
    "int gi 1/0/7 ip firewall enable ip address 10.110.10.1/24",
    "router bgp 65000 neighbor 172.16.1.2 update-source 172.16.1.1",
    "router bgp 65000 neighbor 172.16.1.3 update-source 172.16.1.1",  # Изменён BGP-сосед
    "router bgp 65000 neighbor 172.16.1.4 update-source 172.16.1.1",  # Изменён BGP-сосед
    "router bgp 65001 neighbor 172.16.1.4 update-source 172.16.1.1",  # Изменён BGP-сосед и AS
    "router bgp 65001 neighbor 172.16.1.2 update-source 172.16.1.2",  # Изменён BGP-сосед и source
]

labels = [0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1]  # 0 — эталон, 1 — изменён
```

Рис. 8. Обновление списков

В качестве новых данных будет использовано следующее: int gi 1/0/10 ip firewall disable ip address 190.110.20.1/24 (рис. 9).

```
Epoch 8/10
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 72ms/step - accuracy: 0.5833 - loss: 0.6693 - val_accuracy: 0.666
7 - val_loss: 0.6411
Epoch 9/10
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 70ms/step - accuracy: 0.5833 - loss: 0.6652 - val_accuracy: 0.666
7 - val_loss: 0.6319
Epoch 10/10
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 71ms/step - accuracy: 0.5833 - loss: 0.6607 - val_accuracy: 0.666
7 - val_loss: 0.6215
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 191ms/step
Изменение обнаружено
```

Рис. 9. Результат

Из рисунка видно, что точность обнаружения изменений на обучающих данных составляет 58,33 %, а на валидационных данных – 66,67 %. Но несмотря на низкую точность модель справилась со своей задачей и обнаружила изменения в конфигурации.

Выводы

В ходе выполнения работы была разработана и обучена модель нейронной сети для обнаружения изменений в конфигурационных файлах DMVPN-сети.

Модель недостаточно точна, что обусловлено небольшим набором обучающих данных. В будущем необходимо увеличить набор обучающих данных и добавить исправления в архитектуру самой модели, чтобы она могла более эффективно работать со сложными и разнообразными конфигурациями.

Список используемых источников

1. Ермаков В. Развитие нейронных сетей: современные достижения и будущее. URL: https://vc.ru/u/3352034-vlad-ermakov/1194650-razvitie-neironnyh-setei-sovremennye-dostizheniya-i-budushee (дата обращения 25.10.2024).
2. Пересечение нейробиологии и искусственного интеллекта. URL: https://falconediting.com/ru/blog/peresechenie-neirobiologii-i-iskusstvennogo-intellekta/ (дата обращения 15.11.2024).
3. Романюк П. Основы нейронных сетей: Теория и практика. URL: https://habr.com/ru/articles/587694/ (дата обращения 27.10.2024).
4. Махкамов Н. Я. Нейронные сети: насколько они полезны для человечества // CAJAR. 2024. №10–1. URL: https://cyberleninka.ru/article/n/neyronnye-seti-naskolko-oni-polezny-dlya-chelovechestva (дата обращения 08.11.2024).
5. Проничев В. Д. Исследование механизмов отказоустойчивости при построении DMVPN с использованием отечественных маршрутизаторов [Рукопись] : вып. квалиф. раб. на соискание степ. бкл. по спец. 11.03.02 / В. Д. Проничев; научный руководитель И. А. Ушаков; рец. И. А. Ушаков; Санкт-Петербургский гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича, Кафедра ЗСС. 2023. 60 с.
6. Обработка текстов в нейронных сетях. URL: https://yourtodo.ru/ru/posts/obrabotka-tekstov-v-nejronnyih-setyah/ (дата обращения 10.11.2024).

Pronichev V., Ushakov I. **AUTOMATED ANALYSIS OF CHANGES IN DEVICE NETWORK CONFIGURATIONS BASED ON NEURAL NETWORKS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This work proposes a neural network implementation for detecting changes in configuration files based on DMVPN (Dynamic Multipoint Virtual Private Network) network. This model uses a previously generated reference configuration file and is trained on it to detect outliers that inform about configuration changes. The article presents the main stages of data preparation, network architecture construction and its further use.

Key words: reconfiguration, neural networks, DMVPN, reference configuration, binary classification, information security.

УДК 004.896
ГРНТИ 28.23.27

ПРОБЛЕМЫ ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ ВНУТРЕННИХ НАРУШИТЕЛЕЙ (ИНСАЙДЕРОВ)

В. А. Страйстар, И. А. Ушаков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С увеличением объема данных и сложностью задач, связанных с информационной безопасностью, использование методов глубокого обучения для обнаружения инсайдера становится все более актуальным. Тенденции применения искусственного интеллекта растут, но применение этих методов не лишено ряда сложностей и проблем, они требуют тщательного анализа и решения. В данной статье будут рассмотрены основные проблемы, возникающие при использовании глубокого обучения для выявления внутреннего нарушителя.

инсайдер, искусственный интеллект, глубокое обучение, набор данных

Актуальность

Проблема инсайдеров продолжает оставаться одной из наиболее значительных и актуальных угроз для информационной безопасности компаний и организаций. Инсайдеры, имея авторизацию внутри учреждения, обладают уникальным доступом к ценным данным и ресурсам, что делает их действия особенно рискованными и сложными для выявления [1].

Введение

На данный момент появляется все больше исследований с применением глубокого обучения для решения вопросов информационной безопасности, методы выявление внутренних нарушителей не стали исключением. Исследователи создают и обучают различные модели нейронных сетей, но и здесь не обошлось без значительных недостатков. На рисунке 1 представлены проблемы, возникающие при обучении моделей глубоких нейронных сетей для обнаружения инсайдеров в сетевом трафике.

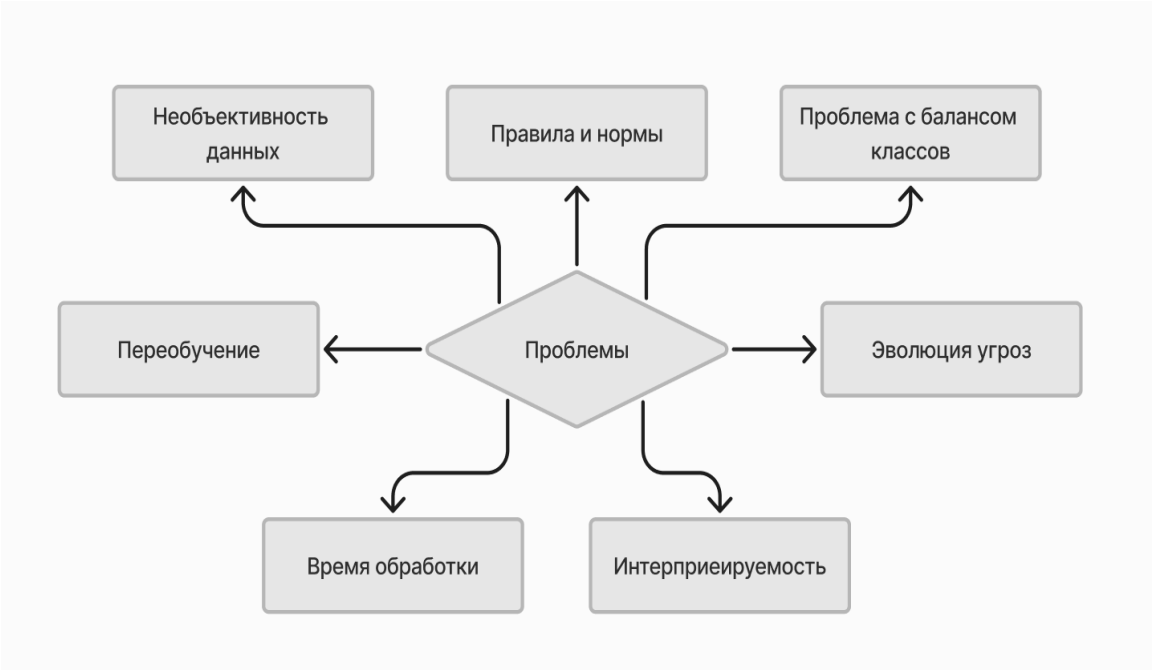


Рис. 1. Рассматриваемые проблемы.

Необъективность данных

Глубокие нейронные сети требуют больших объемов данных для обучения. Однако данные о сетевом трафике могут быть нестабильными, неполными или необъективными, что затрудняет обучение моделей. Существуют несколько наборов данных, которые могут использоваться для обнаружения инсайдерских угроз и аномального поведения внутри корпоративных сетей [2]. Далее описаны некоторые из них.

SL-KDD/KDD-99 – это датасет, полученный из оригинального датасета KDD Cup 99. Датасет содержит обычный и вредоносный трафик сети, а также описания каждого типа атаки. Датасет включает в себя 41 столбец, в которых представлены различные атрибуты сетевого трафика, включая IP-адреса, порты, протоколы, флаги TCP, количество переданных байт и др.

RUU представляет собой датасет, в который входят события на хосте от 34 обычных пользователей и 14 самозванцев. Четырнадцать волонтеров выполняют роль маскировщиков, пытаясь обнаружить данные с финансовой ценностью.

Набор данных TWOS представляет собой другой тип набора, который включает как самозванцев, так и предателей. Он включает действия 24 пользователей за 5 дней, собранные во время многопользовательской игры, где смоделированы 12 сеансов самозванцев и 5 сеансов предателей. Данные содержат журналы из различных источников, таких как журналы мыши, нажатия клавиш, сетевые операции и системные вызовы монитора хоста.

Набор данных CERT (чаще всего именно это набор используется в различных исследований для построения моделей по обнаружению инсайдеров) состоит из пяти файлов журналов, в которых фиксируются компьютерные действия всех сотрудников моделируемой организации: logon.csv, в который записываются операции входа и выхода из системы всех сотрудников, email.csv, в который записываются все операции с электронной почтой, http.csv, который записывает все операции просмотра веб-страниц, file.csv, который записывает действия с участием съемного носителя, decive.csv, который записывает использование флэш-накопителя.

Перечисленные наборы являются синтетическими, к тому же они не были созданы специально для выявления внутренних угроз. Некоторые из них не содержат вредоносных данных вообще, тогда как другие являются устаревшими.

Проблема с балансом классов

В задачах обнаружения нарушителей часто наблюдается сильный дисбаланс между нормальным и аномальным трафиком. Это может привести к тому, что модель будет плохо распознавать редкие, но важные случаи нарушений [3]. Для примера можно рассмотреть самый популярный набор данных, который используется во многих исследованиях: CERT Insider Threat Dataset. Данные входящие в набор являются несбалансированными, в нем содержится около 700 тыс. легитимных пользователей и всего 1.5 тыс. пользователей, помеченных как злоумышленники. Это значительно ухудшает процесс обучения глубокой сети, среди огромного количества легитимных пользователей, пользователи с меткой инсайдера теряются. После обучения такая модель не сможет отличать норму от аномалии.

Переобучение

Модели глубокого обучения могут легко переобучиться на тренировочных данных, особенно если они сложные и содержат много параметров, что может снизить их обобщающую способность при работе с новыми, невиданными данными [4].

Правила и норма

В сетевом трафике может быть множество легитимных, но необычных паттернов, которые могут быть ошибочно классифицированы как нарушения. Различить легитимные отклонения от настоящих угроз сложно. Злоумышленник является законным пользователем системы, именно поэтому достаточно

сложно провести границу между тем, что является нормой, и тем, что является вредоносным. Большинство существующих методов, которые используются для обнаружения инсайдеров, применяют подходы обнаружения аномалий, классифицирующие небольшие отклонения от так называемой «нормы» как аномалию. Такие методы, как правило, вызывают ложные тревоги при обработке данных случаев [5].

Время обработки

Модели глубокого обучения могут требовать значительных вычислительных ресурсов и времени для анализа трафика в реальном времени, что может быть критическим для систем обнаружения нарушителей [6]. Например, сбор журналов действий сотрудников, несомненно, полезен для поведенческого анализа работы сотрудников, однако объем этих данных достигает огромных размеров. Для обработки такого количества данных требуется достаточно много времени.

Интерпретируемость

Глубокие нейронные сети часто являются «черными ящиками», что делает трудным понимание их решений и действий. Это может быть проблемой, когда необходимо объяснить, почему было принято то или иное решение о выявлении угрозы.

Эволюция угроз

Угрозы и методы атак постоянно эволюционируют. Модели глубокого обучения, обученные на одном наборе данных, могут быстро устареть, когда атакующие начинают использовать новые техники.

Заключение

Хотя глубокое обучение имеет большой потенциал для обнаружения инсайдеров, многие проблемы и задачи усложняют картину. Изложенные проблемы подчеркивают необходимость комплексного подхода к использованию глубокого обучения в системах обнаружения злоумышленников, сочетая его с другими методами и технологиями.

Список используемых источников

1. Ушаков И. А. Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных: специальность 05.13.19 «Методы и системы защиты информации, информационная безопас-

ность»: диссертация на соискание ученой степени кандидата технических наук / Ушаков Игорь Александрович. Санкт-Петербург, 2020. 215 с. EDN ISTTII.
2. Shuhan Yuan, Xintao Wu, Deep learning for insider threat detection: Review, challenges and opportunities, Computers & Security, Volume 104, 2021, 102221, ISSN 0167-4048, DOI 10.1016/j.cose.2021.102221.
3. Аль-Ани М. М. Эффективность глубокого обучения и методы машинного обучения в кибербезопасности / М. М. Аль-Ани, А. Д. Алшаиби, Е. Ю. Костюченко // Проблемы правовой и технической защиты информации, 2021. № 9. С. 7–9. EDN UAWTDI
4. Al-Mhiqani MN, Ahmad R, Zainal Abidin Z, Yassin W, Hassan A, Abdulkareem KH, Ali NS, Yunos Z. A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations. *Applied Sciences*. 2020; 10(15):5208.
5. Шарибаев А. Н., Шарибаев Р. Н., Абдулазизов Б. Т., Тохиржонова М. Р. Проблемы в области глубокого обучения с подкреплением // Форум молодых ученых. 2023. № 6 (82). URL: https://cyberleninka.ru/article/n/problemy-v-oblasti-glubokogo-obucheniya-s-podkrepleniem (дата обращения 10.11.2024).
6. Бекматов А. К., Рустамов Т. С. Роль глубокого обучения в улучшении точности систем обнаружения вторжений // Экономика и социум, 2024. № 6–1 (121). URL: https://cyberleninka.ru/article/n/rol-glubokogo-obucheniya uluchshenii-tochnosti-sistem-obnaruzheniya-vtorzheniy (дата обращения 10.11.2024).

Straystar V., Ushakov I. **DEEP LEARNING CHALLENGES FOR INSIDER DETECTION.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

With the increasing volume of data and the complexity of information security tasks, the use of deep learning methods for insider detection is becoming increasingly relevant. The trends in the use of artificial intelligence are growing, but the use of these methods is not without a number of difficulties and problems, they require careful analysis and solution. This article will discuss the main problems that arise when using deep learning to detect an insider.

Key words: insider, artificial intelligence, deep learning, dataset.

УДК 004.056
ГРНТИ 49.33.29

АВТОМАТИЗИРОВАННАЯ ГЕНЕРАЦИЯ ТРАФИКА ЦЕНТРОВ УПРАВЛЕНИЯ ВПО НА ПРИМЕРЕ ФРЕЙМВОРКА ПОСТЭКСПЛУАТАЦИИ MERLIN

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

Генерация трафика при взаимодействии сервера управления и целевой машиной может сильно отличаться, при использовании различных параметров агента. Сбор данных для анализа трафика может занять много времени, особенно если необходимо исследовать множество агентов взаимодействия. Для решения данной проблемы можно использовать средство автоматизации ansible, которое на основе заранее заданных скриптов и команд, выполнит действия по созданию агента C2 с уникальными параметрами, его установку на целевую машину и сбор необходимых данных по взаимодействию между ними.

Command and Control, анализ трафика, вредоносное ПО, автоматизация, Ansible

Для управления компьютером пользователя злоумышленники могут использовать сервер управления и контроля: так называемый *C2* (*command and control*) сервер. Обычно это машина, на которой стоит управляющие инструменты, позволяющее контролировать зараженное устройство в сети, передавая команды и получая информацию от вредоносного программного обеспечения (ВПО), установленного на целевых машинах [1].

Способы атак различны, но обычно *C2* включает один или несколько скрытых каналов связи между устройствами. Эти каналы используются для передачи инструкций взломанным устройствам, загрузки дополнительных вредоносных данных и передачи украденных данных злоумышленнику. Основной стратегией является смешивание с легитимным трафиком, например, *HTTP*/*HTTPS*. Также вызовы из *C&C* можно маскировать, используя шифрование [2].

Для предотвращения заражения компьютера, и чтобы им не смог управлять злоумышленник через удаленный сервер, специалистам по информационной безопасности необходимо знать как с этим бороться. Развертывание для исследования *C2* серверов представляет собой важный шаг в анализе и изучении сетевого трафика, связанного с вредоносным программным обеспечением. Одной из ключевых проблем для специалистов по кибербезопасности

является нехватка примеров трафика и семплов для исследования, что увеличивает время анализа взаимодействия вредоносного ПО с сетью при использовании множества различных параметров. Основная задача заключается в сборе и анализе трафика при установлении связи *C2* сервера с целевым компьютером, а также при их взаимодействии между собой.

Для эффективного изучения рассматриваемых случаев требуется создание контролируемой среды, которая эмулирует реальные сценарии взаимодействия серверов *C&C* и целевых машин. Это позволит произвести анализ при использования различных типов соединения между машинами и выявлять закономерности в работе ВПО. Типовая модель поведения вредоносного ПО в трафике, представленная на рис. 1, включает несколько последовательных этапов, отражающих процессы взаимодействия с сетью и инфицированной машиной. К основным этапам относятся: проникновение в систему, установление связи с *C2* сервером, передача данных и выполнение команд.

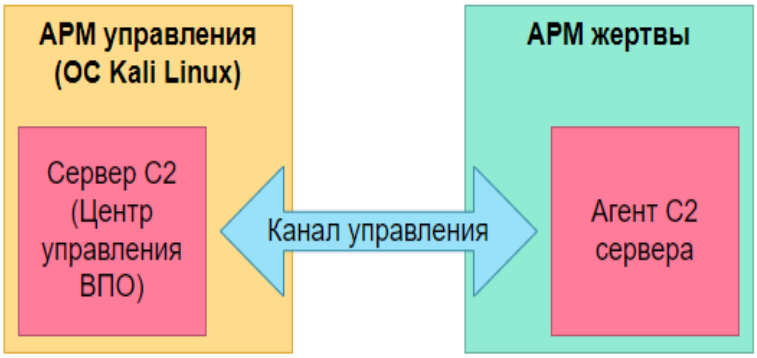


Рис. 1. Схема работы ВПО

Обязательными параметрами для выполнения команд C&C сервера являются: IP-адреса жертвы и сервера управления, протокол, отвечающий за передачу информации, порт назначения, сетевые команды, частота отправки и иные значения, зависящие от типа ВПО. Эти характеристики дают множество различных вариантов для создания и изучения трафика, создаваемого вредоносными программами.

Для демонстрации работы по автоматизированному сбору трафика был взят инструмент пост-эксплуатации для управления и контроля устройствами Merlin. Он позволяет создавать каналы связи, используя следующие протоколы: HTTP/1.1, HTTP/2, HTTP/3 и HTTPS.

Сбор трафика выполняется с помощью приложения Tshark. Используемый фильтр, позволяет захватывать пакеты, которые принадлежат непосредственно *C2* серверу и целевой машине.

В ручном режиме установка C&C сервера, его настройка, создание агента, запуск сбора трафика и выполнение команд занимает около 10 минут (основано на личных исследованиях). Учитывая различные протоколы связи и другие параметры, сбор необходимых пакетов для исследования взаимодействия сервера и целевой машины займет больше часа. К тому же воспроизвести все действия одновременно не получится, так как требуется непрерывное присутствие человека для ввода команд. Это не только способствует увеличению вероятности ошибки, но и отвлекает непосредственно от задачи по анализу трафика. Для автоматизированной настройки тестового стенда можно использовать Ansible [3]. Он упрощает процесс исследования и сбора информации за счет заранее подготовленных плейбуков, которые предназначены для управления конфигурациями. С его помощью можно автоматически выполнять необходимые задачи по настройке.

Была разработана система для автоматического развертывания сервера управления и контроля, его настройки, сбора и дальнейшего исследования трафика на основе Ansible. Она эмулирует действия, выполняемые специалистом вручную. Данная система позволяет эффективно развернуть и настроить C&C сервер, подключить к нему целевую машину на базе Linux, находящуюся в одной подсети. Алгоритм работы для развертывания сервера *C2*, машины-жертвы и сбора трафика представлен на рис. 2.

Действия, описанные после выбора параметров взаимодействия и до логирования, выполняются плейбуком. Запуск программы автоматизации выполняется под учетной записью администратора, так как установка и настройка *C2* сервера требует прав суперпользователя.

После запуска плейбука и установления связи командного сервера с агентом ВПО дамп сетевого трафика по-умолчанию сохраняется в директории */tmp/*. Название файла или же другая директория для сохранения, задаются непосредственно при заполнении шаблонизированного документа.

На рис. 3 представлен фрагмент выполнения плейбука. Шаги с установкой *C2* сервера и передача агента на целевую машину не показаны. На рисунке изображен процесс выполнения задач, по запуску и настройке агента взаимодействия с заданными параметре на *C&C* сервере, старт перехвата трафика с требуемыми фильтрами и старт агента на целевой машине.

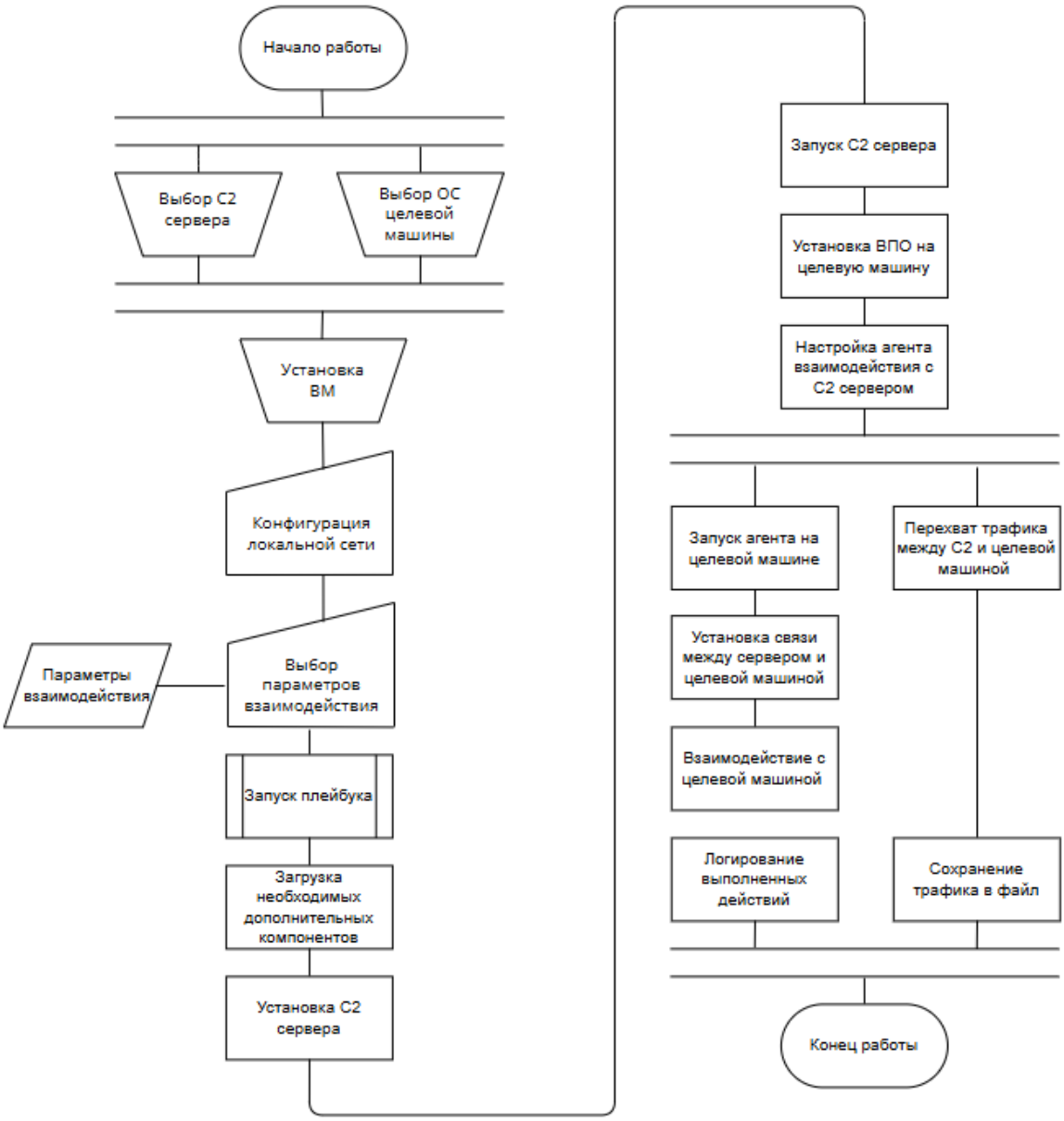


Рис. 2. Блок схема алгоритма развертывания стенда

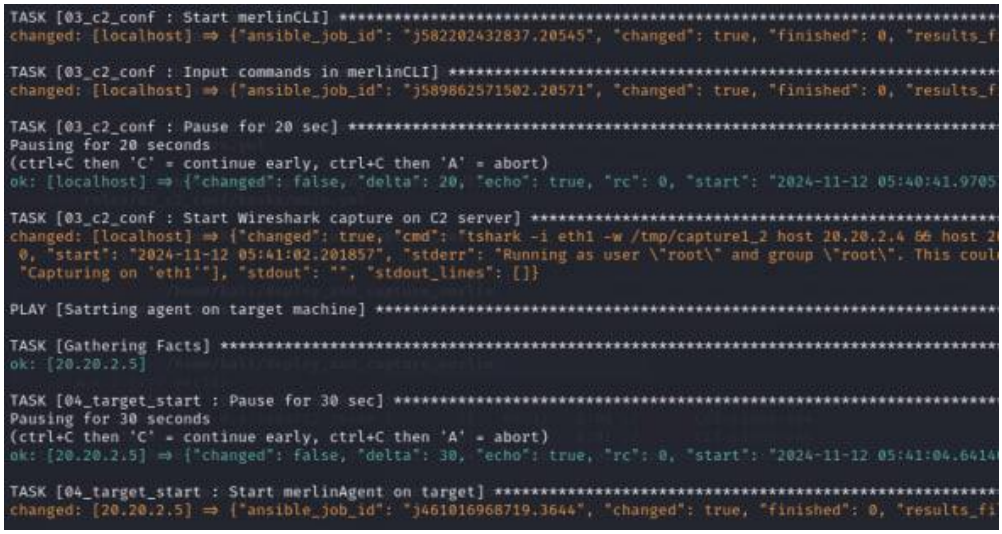


Рис. 3. Сообщения о выполнении задач

После выполнения плейбука запустим Wireshark и загрузим сгенерированный дамп трафика. На рис. 4 представлен фрагмент трафика, захваченного при взаимодействии ВПО Merlin через протокол HTTP на порту 80. На нем демонстрируется POST-запрос от целевой машины с IP-адресом 20.20.2.5 на *C2* сервер, с адресом: 20.20.2.5. Данный метод используется для отправки данных на сервер.

Рис. 4. POST-запрос и ответ от сервера перехваченных http пакетов

Отличительной особенностью данного пакета, от обычных POST-запросов при передаче данных с помощью HTTP, является то, что содержимое в теле запроса не просто текст [4], а закодированные данные в по стандарту base64. Об этом нам говорит поле application/octet-stream [5] – это вид бинарных данных, которые будут выполняться, или же данные для выполнения которых необходимо отдельное приложение. В заголовке указан параметр authorization, который включает в себя JWT (JSON Web Token), для аутентификации сессии. После получения данных сервер отвечает клиенту пакетом с кодом 200 OK, что указывает на успешное получение данных.

Следующие аномалии, которые были зафиксированы при анализе дампа, могут косвенно подтвердить, что данный трафик является вредоносным:

– использование JWT с протоколом HTTP;

– большой размер тела запроса;

– передача закодированной информации;

– разбиение передачи данных с использованием параметра chunked в заголовке Transfer-Encoding.

Разработанное решение позволяет в автоматизированном режиме генерировать вредоносный трафик между сервером *C2* и целевой машиной, который в дальнейшем можно использовать для анализа работы ВПО. Оно не только упрощает процесс сбора информации, но за счет заранее собранных шаблонов, позволяет быстро развернуть необходимую среду для тестирования.

Список используемых источников

1. C2-сервер URL: https://www.securitylab.ru/glossary/c2_server/?ysclid=m34nrqrhoa120005027
2. Что такое Command and Control? Описание инфраструктуры управления и контроля. URL: https://habr.com/ru/companies/varonis/articles/559512/
3. Merlin Command and Control framework. URL: https://merlin-c2.readthedocs.io/en/latest/
4. Что такое Ansible и как его использовать. URL: https://tproger.ru/translations/ansible-how-to-use
5. Методы GET и POST. URL: https://evmservice.ru/blog/metody-get-i-post/# %D0 %9C %D0 %B5 %D1 %82 %D0 %BE %D0 %B4_POST
6. MIME types. URL: https://developer.mozilla.org/ru/docs/Web/HTTP/MIME_types

Taratynov I. **AUTOMATED GENERATION OF TRAFFIC OF VPO CONTROL CENTERS ON THE EXAMPLE OF THE MERLIN POST-EXPLOITATION FRAMEWORK.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The generation of traffic for interaction between the command-and-control server and the target machine can vary significantly depending on the different agent parameters used. Collecting data for traffic analysis can be time-consuming, especially if it’s necessary to examine multiple interaction agents. To address this issue, an automation tool like Ansible can be used. Based on predefined scripts and commands, Ansible can create a C2 agent with unique parameters, install it on the target machine, and gather the necessary data on the interaction between them.

Key words: Command and Control, traffic analyzation, malware, automation, Ansible.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ ВРЕМЕНИ ВЫПОЛНЕНИЯ СЛУЖЕБНЫХ ЗАПРОСОВ ПЛАТФОРМ БОЛЬШИХ ДАННЫХ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ И ЗЛОУМЫШЛЕННИКОВ

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

В условиях стремительного роста объемов данных и критически важной роли платформ больших данных в различных сферах, анализ времени выполнения служебных запросов становится ключевым инструментом для обеспечения безопасности и стабильности [1]. Аномалии в продолжительности обработки запросов могут сигнализировать о возникновении проблем, таких как перегрузка системы, неэффективность запросов или даже деятельность злоумышленников. Данный анализ позволяет выявлять и предсказывать потенциальные проблемы, оптимизировать производительность и повышать уровень безопасности, что делает его важным для поддержания целостности и надежности платформ больших данных в условиях растущих рисков.

большие данные, hadoop, информационная безопасность, аномалии, злоумышленники, анализ, служебный запрос

Развитие технологий и рост объемов данных сделали платформы больших данных, такие как Hadoop, неотъемлемой частью многих сфер деятельности. Их способность эффективно обрабатывать и анализировать огромные массивы информации открывает новые горизонты для анализа, прогнозирования и принятия решений. Однако эта революция в области обработки данных несет с собой и новые угрозы, связанные с обеспечением информационной безопасности. Хранилища больших данных, содержащие конфиденциальную информацию, становятся объектом повышенного интереса для злоумышленников, стремящихся получить доступ к ценным данным, нарушить работу системы или просто причинить вред. Именно поэтому обеспечение информационной безопасности в системах больших данных приобретает критическое значение [2].

Одним из эффективных инструментов для обнаружения аномалий и потенциальных угроз является анализ времени выполнения служебных запросов. Мониторинг данных показателей, позволяет не только выявлять угрозы, но и оптимизировать работу всей системы, предотвращая сбои и повышая ее производительность [3]. Для оценки точности прогнозирования времени выполнения запросов, можно использовать среднеквадратическую ошибку (MSE).

Эта метрика вычисляет среднее квадратичное отклонение между прогнозируемыми и фактическими значениями времени выполнения запросов. MSE определяется согласно формуле 1.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(y_i - \tilde{y}_i\right)^2$$

где n – количество наблюдений, y_i – фактическое время выполнения i–го запроса, $\tilde{y}_i$– прогнозируемое время выполнения i–го запроса.

Следовательно, MSE позволяет количественно оценить, насколько близки прогнозы модели к реальным данным. Чем меньше значение MSE, тем более точными считаются прогнозы.

Анализ времени выполнения служебных запросов может быть улучшен с помощью применения MSE для оценки аномалий. Например, если прогнозируется время выполнения запросов на основе исторических данных, MSE поможет определить, насколько сильно фактическое время выполнения отклоняется от прогнозируемого. Высокое значение MSE может указывать на наличие аномалий, таких как перегрузка системы или попытки злоумышленников вмешаться в процесс обработки данных.

Таким образом, использование MSE в сочетании с анализом времени выполнения служебных запросов предоставляет мощный инструмент для повышения уровня безопасности и надежности систем больших данных.

На рисунке 1 представлена схема взаимодействия, которая отражает базовую архитектуру системы обработки больших данных.

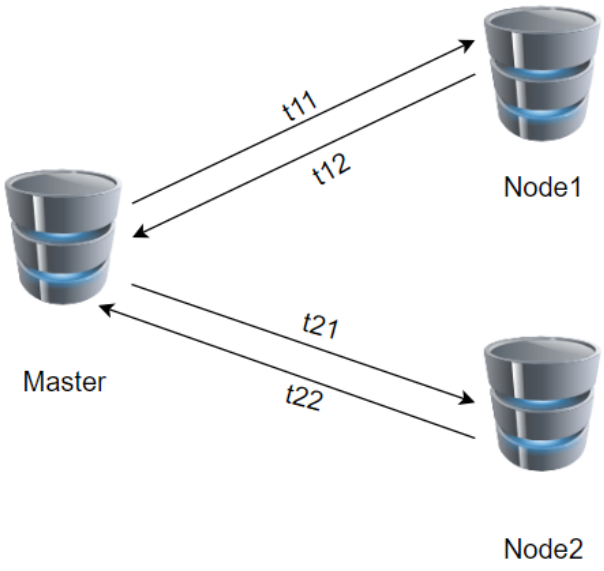


Рис. 1. Взаимодействие компонентов

Компонент «Master» выступает в роли хранилища данных, а компоненты «Node1» и «Node2» представляют собой вычислительные узлы, выполняющие различные операции над данными. Стрелки между компонентами обозначают передачу данных, и время выполнения операций, соответственно.

Процесс взаимодействия:

1. Инициализация. Узлы Node1 и Node2 подключаются к мастеру и регистрируются;

2. Распределение задач. Мастер получает задачу на обработку данных и разбивает ее на подзадачи;

2. Отправка запроса. Мастер отправляет узлам запросы на выполнение соответствующих подзадач (t11, t21);

4. Выполнение задач. Узлы выполняют свои подзадачи и отправляют мастеру запросы на подтверждение завершения (t12, t22);

5. Сбор результатов. Мастер собирает результаты от всех узлов и формирует итоговый результат.

Для проведения анализа времени выполнения служебных запросов предлагается использовать инструмент Wireshark. Он позволяет перехватывать сетевые пакеты и детально изучать их содержимое [4]. Путем анализа заголовков пакетов можно определить типы запросов, а также время их отправки и получения. Рассмотрим типы запросов, которые можно встретить при детальном рассмотрении сетевых пакетов.

В системах Hadoop существует множество различных типов служебных запросов, каждый из которых выполняет определенную функцию.

Типы служебных запросов в Hadoop:

1. Запросы к NameNode. Эти запросы направлены на взаимодействие с NameNode, отвечающим за управление файловой системой HDFS. Они включают в себя операции по созданию, удалению, переименованию файлов, а также запросы на метаданные файлов, такие как размер, модифицированные даты, права доступа;

2. Запросы к DataNode. Эти запросы связаны с DataNode, отвечающим за хранение и предоставление доступа к блокам данных. Они включают в себя операции по чтению и записи блоков, а также запросы на статус DataNode, например, доступный объем памяти;

3. Запросы к JobTracker. Эти запросы направляются на JobTracker, отвечающий за управление заданиями MapReduce [5]. Они включают в себя отправку заданий, мониторинг прогресса выполнения, запросы на статус заданий и управление ресурсами кластера;

4. Запросы к TaskTracker связаны с выполнением отдельных задач MapReduce. Эти запросы связаны с TaskTracker, отвечающим за выполнение

задач MapReduce. Они включают в себя запросы на выполнение задач, отчеты о статусе выполнения и запросы на ресурсы, необходимые для выполнения задачи.

Анализ времени выполнения различных типов запросов является ключевым для обеспечения стабильной и эффективной работы кластера Hadoop. Анализируя время выполнения, можно выявить следующие аномалии:

– нетипично длительное время выполнения запросов для системы, может свидетельствовать о перегрузке системы, проблемах с оборудованием или попытке выполнения ресурсоемких операций;

– частые ошибки выполнения запросов, могут указывать на наличие ошибок в конфигурации системы или на попытки взлома [6];

– необычные шаблоны активности, могут свидетельствовать о попытках сканирования системы или других видах атак.

Анализ времени выполнения запросов позволяет не только выявлять проблемы, но и оптимизировать работу кластера Hadoop. Например, анализ времени выполнения запросов к NameNode может помочь в оптимизации конфигурации файловой системы, а анализ времени выполнения запросов к JobTracker – в оптимизации планирования задач MapReduce.

Анализ времени выполнения служебных запросов в системах Hadoop является важным инструментом для обнаружения аномалий и потенциальных угроз информационной безопасности [7].

Ключевые преимущества анализа времени выполнения запросов:

– раннее обнаружение проблем, позволяет выявить проблемы до того, как они приведут к серьезным сбоям в работе системы;

– повышение безопасности, помогает в предотвращении несанкционированного доступа к данным и ресурсам;

– оптимизация производительности, позволяет оптимизировать работу системы Hadoop для повышения ее производительности и эффективности.

Таким образом, анализ времени выполнения запросов в платформах больших данных позволяет обнаружить аномалии и злоумышленников, а также проактивно предотвращать будущие инциденты.

Объединяя данные из разных источников и применяя мощные алгоритмы анализа временных рядов, организации могут идентифицировать аномалии, выявлять ранние признаки атак и определять оптимальные временные интервалы для профилактических мер. Благодаря этому повышается способность к быстрому реагированию на угрозы и оптимизации систем [8].

В условиях растущих объемов данных и киберугроз такой подход становится необходимым для обеспечения безопасности информации. Внедрение современных методов сбора данных и анализа временных рядов позволяет организациям перейти на новый уровень защиты информации, гарантируя безопасность и непрерывность работы в условиях постоянно растущих рисков.

Список используемых источников

1. Виткова Л. А. и др. Использование Big Data в процессах обеспечения безопасности информационной сферы // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 186–191.
2. Пестов И. Е. Метод сбора и первичной обработки метрик инстансов облачной инфраструктуры, метод передачи метрик загруженности облачной инфраструктуры и инстансов в кластер обработки средствами и методами больших данных для защиты информации и обеспечения информационной безопасности // Автоматизация и моделирование в проектировании и управлении, 2021. С. 213–217.
3. 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. № 4. С. 26–35.
4. Василишин Н. С. и др. Методы сбора и анализа сетевого трафика на основе технологий больших данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. С.127–131.
5. Пискун Г. А., Алексеев В. Ф., Воронко Т. М. Обзор программной платформы Apache Hadoop для обработки и хранения больших данных // Материалы IX Междунар. науч.-практ. конф., Минск 18 мая 2023 г. С. 465–471.
6. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Региональная информатика и информационная безопасность: межриг. сб. тр. 2018. С. 236–240.
7. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 4. С. 76–84.
8. Пестов И. Е. и др. Метод передачи метрик загруженности инстансов облачной инфраструктуры в кластер обработки средствами и методами больших данных для защиты информации и обеспечения информационной безопасности // I-methods. 2022. Т. 14. № 1.

Fedotovskaya A. **ANALYZING THE EXECUTION TIME OF SERVICE REQUESTS OF BIG DATA PLATFORMS TO IDENTIFY ANOMALIES AND INTRUDERS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the context of the rapid growth of data volumes and the critical role of big data platforms in various fields, the analysis of the execution time of service requests is becoming a key tool for ensuring security and stability. Anomalies in the processing time of requests can signal the occurrence of problems such as system overload, inefficiency of requests, or even the activity of intruders. This analysis allows you to identify and predict potential problems, optimize performance and improve security, which makes it important to maintain the integrity and reliability of big data platforms in the face of increasing risks.

Key words: big data, hadoop, information security, anomalies, intruders, analysis, service request.

УДК 004.421.5
ГРНТИ 27.43.15

АНАЛИЗ КОМБИНАЦИЙ МЕТОДОВ ПРЕОБРАЗОВАНИЯ СИГНАЛА С ФИЗИЧЕСКОГО ДАТЧИКА СЛУЧАЙНЫХ ЧИСЕЛ, ОСНОВАННОГО НА КОЛЬЦЕВЫХ ОСЦИЛЛЯТОРАХ

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

Физические датчики случайных чисел служат для выработки псевдослучайной последовательности, которая применяется в разных сферах защиты информации. В данной статье проводится исследование комбинаций методов преобразования последовательностей, полученных с физического датчика случайных чисел, основанного на 8 кольцевых осцилляторах. Были рассмотрены 3 комбинации методов преобразования. Тестирование было проведено при помощи пакета тестов NIST STS. Результаты тестов показали, что порог прохождения тестов у преобразованных последовательностей выше, чем у исходных.

физические датчики случайных чисел, псевдослучайная информация, преобразование последовательности

Генерация псевдослучайной последовательности бит очень важна в защите информации, так, например, стойкость и эффективность криптографического алгоритма напрямую зависит от сгенерированной последовательности. Псевдослучайные последовательности так же могут применяться при использовании сессионных ключей или для генерации паролей пользователей. Главное преимущество физического датчика случайных чисел заключается в отсутствии возможности повторного получения идентичных последовательностей.

Российские компании, проводящие разработки в сфере криптографической защиты информации, заинтересованы в создании ФДСЧ на основе кольцевых осцилляторов [1] по причине быстрой генерации последовательностей данным ФДСЧ и его малыми размерами с физической точки зрения. В свою очередь, генератор такого типа имеет слабое фазовое дрожание, из-за чего получаемый сигнал требует преобразования.

В ФДСЧ такого типа используются цепочки из нечетного количества инверторов, соединенных в кольца, что приводит к созданию обратной связи

(рис. 1). Количество колец определятся техническими характеристиками генератора и может достигать 100 штук и более [2]. Данный вид ФДСЧ фиксирует задержки прохождения сигнала через цепочки инверторов [3].

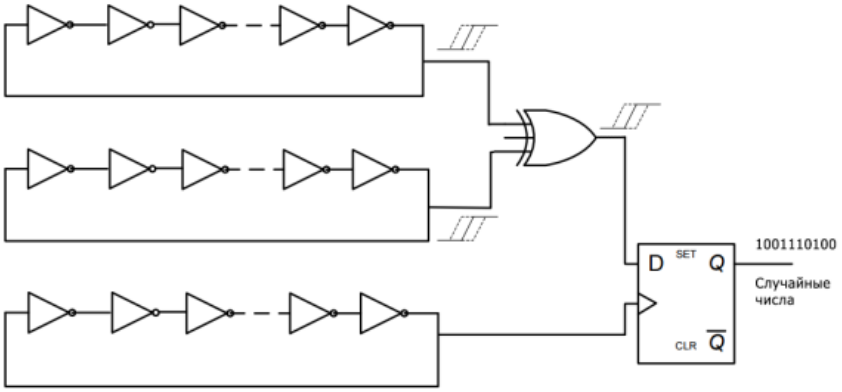


Рис. 1. Схема ФДСЧ, основанного на кольцевых осцилляторах

Исходные данные представляли собой 8 последовательностей бит, полученных с каждого кольца осциллятора. При первом изучении сигнала наблюдения показали, что исходные последовательности обладают чередующимися сериями бит 0 и сериями бит 1, большими 2 по длине. По этой причине был вычислен вариационный ряд серий 1 (таблица 1) и серий 0 (таблица 2) для каждого из 8 колец.

ТАБЛИЦА 1. Вариационный ряд для серий бит, состоящих из 1

№ к.	Длина серии бит, сост. из 1												
	1	2	3	4	5	6	7	8	9	10	11	12	13
1	5	2	1	40346	49082	0	0	0	0	0	0	0	0
2	1	1	1	19097	64437	0	1	0	0	0	0	0	0
3	0	1	1	1	22083	48288	0	2	0	0	0	0	0
4	1	3	1	1	2	33644	28514	0	0	0	0	0	1
5	2	2	2	0	0	1	21430	31495	0	0	0	0	1
6	1	0	0	0	2	1	1	42306	6862	1	1	0	1
7	0	1	2	0	1	2	0	38500	10372	1	0	0	0
8	1	0	1	0	0	2	0	1	1	29397	9621	1	0

ТАБЛИЦА 2. Вариационный ряд для серий бит, состоящих из 0

№ к.	Длина серии бит, сост. из 0												
	1	2	3	4	5	6	7	8	9	10	11	12	13
1	5	2	1	53961	35467	0	0	0	0	0	0	0	0
2	1	2	2	16630	66940	0	0	0	0	0	0	0	0
3	2	0	0	0	22423	47948	2	1	0	0	0	0	0
4	2	1	1	1	0	36651	25508	0	0	1	1	0	0
5	1	0	0	0	1	1	25473	27456	0	1	0	0	0
6	0	0	0	0	2	2	0	42846	6324	1	0	1	0
7	1	2	1	1	0	2	1	41317	7557	0	0	0	0
8	0	5	1	1	0	0	1	0	1	29081	9933	1	0

В блоке постобработки ФДСЧ для преобразования исходных последовательностей применяются следующие методы [4]:

– операции XOR к выходным последовательностям;

– хэш-функции;

– функции экстракции.

Всего было предложено 3 схемы преобразования исходных последовательностей.

Первая схема преобразования последовательностей представляет собой использование определенного алгоритма замены серий бит и операции сложения по модулю два. Алгоритм замены серий бит индивидуален для каждого сигнала, получаемого со всех рассматриваемых колец, и заключается в следующем: для каждой последовательности высчитывается вариационный ряд серий бит 1 и 0, по результатам которого выбирается две серии длины n и $n+1$, которые повторяются в последовательности наибольшее число раз, после чего серии длины n заменяются на 0, а серии длины $n+1$ – на 1. Полученные последовательности подвергаются операции XOR друг с другом.

Вторая схема преобразования последовательностей имеет сходства с первой и включает в себя улучшенный алгоритм замены серий бит и операцию *XOR*. В данной схеме отдельно рассматриваются серии бит 0 и серии бит 1 разной длины n и $n+1$. Серии бит 0 длины n заменяются на серию 00, серии бит 1 длины n – на серию 01, серии бит 0 длины $n+1$ – на серию 10, серии бит 1 длины $n+1$ – серию бит 11. Полученные последовательности подвергаются операции XOR друг с другом.

Третья схема преобразования последовательностей предполагает разбиение сигналов на блоки длиной $n = 512$. Ко всем элементам одного блока применяется операция сложения по модулю два, после чего происходит замена блока на полученный результат. Полученные последовательности подвергаются операции XOR друг с другом.

Все схемы преобразования были реализованы на языке программирования Python.

Для проведения тестирования использовался пакет NIST STS [5]. Данный пакет включает в себя 15 статистических тестов, которые разработаны для проверки гипотезы о наличии свойств псевдослучайной последовательности двоичных последовательностей произвольной длины, порождаемых ФДСЧ.

Для тестов установлен уровень значимости $\alpha = 0{,}01$. В каждом тесте рассчитывается p-уровень значимости P-value. Если P-value $< \alpha$, то нулевая гипотеза отвергается, то есть последовательность не обладает свойствами случайной. На основе p-уровня значимости делается вывод об успешном (PASSED) или безуспешном (FAILED) прохождении теста.

Исходные 8 последовательностей длиной 800 000 бит с 8 кольцевых осцилляторов были подвержены 13 тестам на свойства псевдослучайной последовательности, это связано с ограничением 2 тестов на количество входных данных в размере от 1 000 000 бит. Максимальное количество успешно пройденных тестов на свойства псевдослучайной последовательности равняется 6, минимальное – 5, из 13 возможных. Полученные данные свидетельствуют о том, что преобразование сигнала, полученного с 8 кольцевых осцилляторов, является актуальной задачей с целью получения последовательности, результативность прохождения тестов на свойства псевдослучайной последовательности которой будет выше исходной.

Заключительным этапом было выполнено тестирование на свойства псевдослучайной последовательности преобразованных последовательностей, полученных с 8 кольцевых осцилляторов. Результаты тестирования приведены в таблице 3.

ТАБЛИЦА 3. Тестирование на свойства псевдослучайной последовательности последовательностей, полученных путем применения схем преобразования сигнала, полученного с 8 к. осц.

	Сх. 1	Сх. 2	Сх. 3
Кол-во тестируемых бит, шт	160 000		
Количество успешных тестов, шт	8	8	4

Таким образом, результаты тестирования показали, что применение комбинаций методов преобразования сигнала позволяют повысить порог прохождения тестов на свойства псевдослучайной последовательности. Благодаря применению таких комбинаций ФДСЧ, основанный на кольцевых осцилляторах, способен генерировать последовательности с высоким уровнем свойств случайности.

Список используемых источников

1. Liang Dai, Harjani R. A low-phase-noise CMOS ring oscillator with differential control and quadrature outputs // Conference: ASIC/SOC Conference, 2001. Proceedings. 14th Annual IEEE International
2. Vikram Belur Suresh. On-chip true random number generation in nanometer CMOS. URL: http://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1872&context=theses (дата обращения 11.10.2024).
3. Прощеряков А. А., Иванюк А. А. Кольцевой генератор и его неповторимый температурный коэффициент линейной регрессии. URL: http://libeldoc.bsuir.by/bitstream/123456789/3312/1/Кольцевой генератор и его неповторимый температурный коэффициент линейной регрессии.PDF (дата обращения 15.10.2024).
4. Кнут Д. Э. Искусство программирования. Том 2. Получисленные алгоритмы. М.: Вильямс, 2007. 832 с.
5. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. URL: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf (дата обращения 09.10.2012).

Shilikov D. **ANALYSIS OF COMBINATIONS OF SIGNAL CONVERSION METHODS FROM A PHYSICAL RANDOM NUMBER SENSOR BASED ON RING OSCILLATORS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Physical random number sensors are used to generate a random sequence, which is used in various fields of information security. This article investigates combinations of sequence conversion methods obtained from a physical random number sensor based on 8 ring oscillators. 3 combinations of conversion methods were considered. The testing was carried out using the NIST STS test suite. The test results showed that the transformed sequences have a higher threshold for passing the test than the original ones.

Key words: physical random number generator, pseudorandom information, sequence conversion.

УДК 004.056.5
ГРНТИ 81.93.29

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ. ВЫЯВЛЕНИЕ ПРИЧИН ВОЗНИКНОВЕНИЯ СОВРЕМЕННЫХ УЯЗВИМОСТЕЙ И ЦЕЛЕЙ ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ

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

Повсеместное распространение веб-приложений, в современных реалиях, вынужденно сталкиваться с множеством противоречий. С одной стороны, удобство, пришедшее с появлением огромного числа веб-приложений, позволило оптимизировать сроки реализации множества задач общества. С другой стороны, с увеличением количества веб-приложений, также увеличилось и количество уязвимостей в этих приложениях, используемые мошенниками в целях обмана владельцев систем или целевых пользователей данных систем.

Цель данной работы - выявить причины возникновения уязвимостей веб-приложений, а также выяснить наиболее популярные уязвимости, вытекающие из установленных причин.

информационная безопасность; веб-приложения; безопасность веб-приложений; уязвимости веб-приложений

Современные веб-приложения

Массовое распространение веб-приложений привело к оптимизации многих процессов, занимавших раннее у множества людей огромное количество времени на исполнение. Такие явления, как ожидание в очереди для оплаты коммунальных платежей или перевода денежных средств, приобретение продуктов домой или же процесс обучения различным навыкам – ныне получили ускорение, реализованное путем интеграции множества из этих сервисов в веб-ресурсы. Однако, помимо улучшений – повсеместное внедрение веб-приложений привело и к увеличению количества проблем, вызванных эксплуатацией различных уязвимостей как в механизмах самих приложений, так и в уязвимостях пользовательского опыта. И в случае, если пользовательский опыт имеет ряд проблем по вине недостаточного ознакомления самих пользователей с системами или возможными вариантами различных махинаций злоумышленников, направленных на обман доверия пользователя, то уязвимости самих приложений, зачастую, возникают по вине упущений важных аспектов в процессе разработки или внедрения систем [1].

Главными причинами, по вине которых практически каждое выходящее веб-приложение подвержено тем или иным угрозам, принято считать [2]:

1. Срок релиза приложения важнее, чем безопасность приложения. Большинство выходящих веб-сервисов, призванных улучшить пользовательский опыт потенциальных клиентов или повысить конверсию, вынуждены выходить в процессе спринтов и переработок. Потому, компании-разработчики зачастую устанавливают сроки реализации главной задачей, упуская возможность выпуска приложения позже, но при этом в более защищенном варианте.

2. Уязвимости в готовом/стороннем программном обеспечении. Современная разработка всегда проходит с использованием сторонних библиотек, компонентов, плагинов, визуализаторов или CMS (систем управления содержимым). Они применяются в целях облегчить процесс разработки приложений и продуктов, однако, помимо облегчений – несет за собой и потенциальные уязвимости. Ведь, если в одном из таких используемых компонентах расположена уязвимость – то и итоговое веб-приложение подвержено тем же уязвимостям.

3. Главная задача бизнеса – получение прибыли. В случае, если компания-разработчик не обладает большим бюджетом, то она вынуждена упускать уязвимости в процессе разработки, если на закрытие данных уязвимостей необходимо затрачивать дополнительные средства. Ведь, зачастую, главным источником прибыли для компаний-разработчиков является выпускаемый продукт и то, в какие сроки данные продукты способны выйти в эксплуатацию. За счет чего, большая часть инвестиционного бюджета – уходит непосредственно на разработку приложения, и только остаток вложенных средств – отправится на внедрение процессов, обеспечивающих минимальную безопасность веб-ресурса.

В связи с выявленными причинами, возникают свойственные для каждой из причин уязвимости, получившие наибольшее распространение для эксплуатации.

Наиболее популярными уязвимостями веб-приложений в 2024 году, согласно отчету “State of Application Security in 2024” от CloudFlare, можно назвать [3]:

1. Атаки на бизнес-логику приложений, подобные перегрузу системы бронирования, форм аутентификации, резервирование записей в организации или автоматическое создание форм обратной связи. Все, что способно увеличить интенсивность вызова API веб-приложения, позволяющее вывести его из строя;

2. Применение supply chain атак, нацеленное на стороннее ПО, применяющееся в процессе разработки веб-ресурса. Ведь, если в каком-либо сторон-

нем решении существует популярная уязвимость, злоумышленники будут намеренно атаковать все веб-приложения, в процессе разработки которых использовалось данное программное обеспечение. Решением данных уязвимостей служит предварительный анализ стороннего ПО, используемого или готовящегося к использованию в среде разработки продукта, а также внедрение практик по разработке и применению Playbook-ов, в случае выявления 0-day-уязвимостей в используемых сторонних компонентах;

3. Возросшее количество трафика и комплексность DDoS-атак, главная проблема которых заключается в постоянном развитии технологий, повышающих возможности генерировать все более высокие объемы вредоносного трафика. Кроме того, сами атакующие перешли на более современный подход, в которым, вместо использования устаревших ботнет-сетей, ныне используются множества облачных серверов, позволяя не только повышать объем трафика – но и более надежно скрывать местоположение злоумышленника. Решением безопасности для предотвращения DDoS-атак является фильтрация входящего интернет-трафика, с использованием White/Black-листов адресов или выделение больших серверных ресурсов для перевода вредоносного трафика на свободные ноды.

По итогам анализа причин возникновения уязвимостей в современных веб-приложениях, удалось также определить и характерные для каждой причины уязвимости. Это позволяет нам не только усовершенствовать подход к разработке веб-приложений, но и потенциально может создать обязательные требования для эффективно разработки веб-ресурсов с заранее решенными рядами уязвимостей, защитив пользователей, пользовательский опыт работы с приложениями и персональные данные самих пользователей.

Следующая цель проведения исследования состоит в подробном изучении уязвимостей, возникающих со стороны пользовательского опыта эксплуатации веб-приложений, которые способны привести к убыткам для компаний-разработчиков, позволив выявить возможные пути закрытия данных уязвимостей.

Список используемых источников

1. Винарчук А. В. Безопасность веб-приложений: основные уязвимости и способы защиты // Научный лидер, 2024. № 3 (153). URL: https://scilead.ru/article/5637-bezopasnost-veb-prilozhenij-osnovnie-uyazvimo

2. Путято М. М., Самвелович А. М., Лещенко В. В., Немчинова В. О. Анализ типовых уязвимостей при построении веб-приложений // Вестник АГУ, 2022 г. № 3. С. 77–85.

3. Веб-ресурс CLOUDFLARE – отчет о трендах: Статистика уязвимостей веб-приложений в 2024 году / CLOUDFLARE Trends Report: State of Application Security in 2024. URL: https://www.cloudflare.com/2024-application-security-trends/

***Yakubovich S. WEB* APPLICATION SECURITY TREADS ANALYZE. IDENTIFY THE CAUSES OF MODERN VULNERABILITIES AND THE REASONS FOR VULNERABILITY EXPLOITATION.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The widespread distribution of web applications in modern realities is forced to face many contradictions. On the one hand, the convenience that came with the advent of a huge number of web applications made it possible to optimize the timing of the implementation of many social problems. On the other hand, with the increase in the number of web applications, the number of vulnerabilities in these applications, used by fraudsters to deceive system owners or target users of these systems, has also increased. The purpose of this work is to identify the causes of web application vulnerabilities, as well as to find out the most popular vulnerabilities arising from the identified causes.

Key words: Information security; web applications; web application security; web application vulnerabilities.

ГУМАНИТАРНЫЕ, ЭКОНОМИЧЕСКИЕ И ЭКОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ЦИФРОВОГО ОБЩЕСТВА

5.1. Вопросы регионоведения и межкультурных коммуникаций в цифровую эпоху

УДК 94(44).086
ГРНТИ 03.09.55

КРАТКИЙ АНАЛИЗ ДЕЯТЕЛЬНОСТИ ФРАНЦУЗСКОГО СОЮЗА И ФРАНЦУЗСКОГО СООБЩЕСТВА

М. А. Аверьянов, А. Б. Гехт
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается многогранный процесс распада французской колониальной империи, ускоренный глобальными изменениями и антиколониальными движениями после Второй мировой войны. Рассматриваются военные конфликты в Индокитае и Алжире, ставшие символами неудачи попыток сохранить контроль силовыми методами, а также мирная деколонизация Африки. Отдельное внимание уделено Французскому союзу и Французскому сообществу как попыткам модернизировать управление заморскими территориями, которые на практике стали инструментами контроля, а не предоставления автономии. Несмотря на формальное признание независимости, Франция сохранила экономическое и военное влияние, что негативно сказалось на дальнейшем характере отношений с бывшими колониями.

деколонизация, французская колониальная империя, антиколониальные движения, Французский союз, Французское сообщество, неоколониализм

Распад французской колониальной империи был сложным, многоэтапным процессом, который происходил в условиях глобальных изменений и был во многом ускорен событиями Второй мировой войны. К ее началу Франция контролировала обширные территории в Африке, Азии и Океании, а ее колониальная империя считалась одной из самых крупных в мире. Оккупация и сражения на территории метрополии и колоний в Северной Африке подорвали ее экономическое положение и политическое влияние, создавая благоприятные условия для усиления стремления колоний к независимости [1]. Кроме

того, антиколониальные настроения получили поддержку США и СССР, которые рассматривали колониализм как устаревший концепт, несовместимый с провозглашенными принципами свободы и демократии.

После окончания войны Франция попыталась вернуть себе прежнее влияние и контроль. В Индокитае уже в 1946 году вспыхнула Первая Индокитайская война, в которой Франция пыталась подавить силы Вьетминя, поддерживавшие независимость. Война оказалась затяжной и изнуряющей, а поражение французской армии в 1954 году при Дьен Бьен Фу стало символом краха французского господства в Индокитае. В результате Женевских соглашений Франция была вынуждена признать независимость Вьетнама, Лаоса и Камбоджи [1].

Одновременно с этим процессами, Франция столкнулась с сопротивлением в Северной Африке. В Алжире колониальная политика Франции вызвала многочисленные протесты и рост националистических настроений. В 1954 году началась Алжирская война, которая длилась восемь лет и сопровождалась ожесточенными боями, терактами и репрессиями. Для Франции эта война стала болезненным конфликтом, который расколол общество и окончательно продемонстрировал невозможность удержания колоний силой. В 1962 году, после долгих переговоров и давления как внутри страны, так и со стороны международного сообщества, Франция согласилась предоставить Алжиру независимость [2].

В Африке к югу от Сахары деколонизация прошла более мирным путем. В 1960 году, известном как «Год Африки», Франция предоставила независимость большинству своих колоний в этом регионе, включая Сенегал, Мали, Нигер и другие страны. Важно отметить, что этот процесс был частично продиктован желанием Франции сохранить экономическое и культурное влияние на бывшие колонии путем создания неоколониальных структур сотрудничества, таких как организация Франкофонии и многочисленные экономические договоры [2].

Несмотря на то, что Франции не удалось создать со своими колониями прочного и долговечного содружества, попытка организации Французского союза представляется важным событием, в контексте процесса деколонизации, охватившем мир в рассматриваемый период. Крайне важно изучить данный пример, чтобы иметь более полное представление о тех взаимоотношениях, которые имеет Франция со своими бывшими колониями на современном этапе.

Итак, 13 октября 1946 года, по итогам референдума, проведенного во Франции и ее заморских владениях, была принята новая конституция, провозгласившая, в числе прочего, и создание Французского союза. Согласно ее пре-

амбуле, Четвертая Республика обязывалась привести зависимые территории к самоуправлению, отвергая колониализм, основанный на неравенстве и произволе, и гарантировала доступ к руководящим должностям, а также реализацию гражданских прав и свобод. Однако этот идеал оставался скорее декларацией, поскольку, на самом деле, равенство распространялось лишь на индивидуальные права, а не на права народов и наций в целом [3]. Введение полной автономии для колоний не предусматривалось, а перспектива независимости откладывалась на неопределенный срок.

Отметим, что создание Французского союза все же было направлено на модернизацию отношений между метрополией и заморскими владениями, сохраняя их в рамках единой системы, но с обещанием большего равенства и сотрудничества. В теории, он должен был заменить жесткую колониальную структуру на более прогрессивный союз, который предоставлял больше возможностей для равноправного взаимодействия. Если бы демократические принципы, заложенные в устройство союза, были реализованы в полном объеме, то они могли бы способствовать приобретению колониями большей автономии. Однако на практике политический истеблишмент Франции стремился ограничить влияние этих положительных инициатив и превратил Французский союз в инструмент подавления, сохраняя традиционные механизмы колониального контроля [3].

Что же касается институционального устройства, то во главе союза стоял президент Французской республики (являвшийся также президентом союза), руководящими органами являлись Верховный совет и Ассамблея. Верховный совет включал представителей метрополии и заморских территорий и собирался раз в год по решению президента, но его постановления носили рекомендательный характер и не были обязательны для французского правительства. Ассамблея Французского союза созывалась на паритетной основе: половина членов избиралась от метрополии, другая половина – от заморских департаментов и территорий [3]. Однако на практике деятельность Ассамблеи подчинялась интересам Франции, и ее решения не влияли на деятельность метрополии, которая сохраняла исключительное право на управление заморскими территориями.

Французские власти допустили участие представителей колоний в центральных органах власти, включая Национальное собрание, Сенат и Экономический совет, где колониям были выделены небольшие квоты. В 1957 году представители заморских территорий составляли лишь 38 депутатов из 627 в Национальном собрании, 39 сенаторов из 320 в Совете республики и 13 членов из 148 в Экономическом совете [3]. Французские власти тем самым демонстрировали видимость демократичности, но строго контролировали ко-

личество делегатов от колоний, чтобы их влияние не угрожало интересам метрополии.

Французский союз просуществовал 12 лет и прекратил свое существование одновременно с Четвертой республикой. За это время его структура несколько менялась и модернизировалась, но основной принцип колониального контроля оставался неизменным. Рост национально-освободительных движений в колониях стал ключевым фактором, который привел к упадку объединения.

Следующий этап во взаимодействии Франции и ее заморских владений начался с создания Французского сообщества, которое также закреплялось в конституции Пятой республики, утвержденной на референдуме 28 сентября 1958 года. Государства, присоединившиеся к сообществу, формально обретали автономию и могли самоуправляться, самостоятельно решая внутренние вопросы, что было закреплено в статье 77 [4]. Однако, несмотря на эту автономию, их суверенитет оставался существенно ограниченным. Власти метрополии сохраняли за собой контроль над внешней политикой, обороной, экономикой и финансами, утверждая, что именно сообщество отвечает за внешние связи, оборону, денежную политику, использование стратегических ресурсов, а также регулирование транспорта и связи.

Франция, как и прежде, обеспечила свое присутствие на всех ключевых позициях сообщества: президент Французской республики одновременно являлся его главой, а основные министерства – иностранных дел, обороны, внутренних дел, экономики и финансов, управляли соответствующими областями деятельности на уровне всего объединения. Хотя Верховный законодательный орган сообщества – Сенат – формально включал представителей как Франции, так и африканских государств (186 сенаторов от Франции и 98 от африканских стран), реальная власть находилась у президента сообщества [4].

Тем не менее, обретение статуса государств в составе сообщества стало первым шагом к полной независимости для африканских стран. В декабре 1958 года правительства Судана, Сенегала, Верхней Вольты и Дагомеи на встрече в Бамако договорились о создании Федерации Мали и потребовали независимости. Хотя Франция смогла убедить Верхнюю Вольту и Дагомею не участвовать в Федерации, объединение Судана и Сенегала все же было сформировано, и в июне 1960 года французское правительство вынуждено было признать ее независимость. Независимость также получила Малагасийская республика. В конституцию сообщества вынужденно была добавлена поправка, допускавшая пребывание в нем стран, получивших политическую независимость. В августе 1960 года независимыми стали Чад, Центральноафриканская республика, Конго, Габон, Дагомея, Нигер, Верхняя Вольта и Берег

Слоновой Кости, а в ноябре – Мавритания [5]. В результате этих изменений французская колониальная империя в Тропической Африке фактически прекратила свое существование. Франция сохранила за собой только территории Французского Сомали, Коморские острова и остров Реюньон.

После 1960 года Французское сообщество стало функционировать по модели Британского содружества, и его центральные органы фактически утратили свое значение. Однако Франция сумела сохранить влияние в бывших колониях, заключив с ними двусторонние договоры о «дружбе и сотрудничестве». Большинство африканских стран сообщества вошли в валютно-финансовую систему «зоны франка», где французский франк свободно обращался наравне с местными валютами, а Париж сохранял контроль над их финансами и торговлей [5]. Существенное влияние Франция сохранила и в военной сфере, заключив с африканскими странами договоры о «взаимном обеспечении обороны», которые позволяли французским войскам находиться в этих странах. Эти договоренности неоднократно использовались в 60-70-х годах для сохранения французского влияния в франкоязычных странах Африки.

Неудачи Французского союза и Французского сообщества объясняются рядом причин, связанных как с внутренними противоречиями, так и с внешними факторами. В первую очередь, идея сохранить колониальные владения в статусе зависимых территорий в условиях глобального подъема антиколониального движения была обречена на провал. Несмотря на декларируемую автономию, реальная власть оставалась сосредоточенной в руках французских властей, что создавало иллюзию самоуправления, но не предоставляло полноценного суверенитета. Неспособность предоставить настоящую независимость подорвала доверие африканских государств, а зависимость от Франции, особенно в сферах экономики и обороны, еще больше усиливала напряженность.

Кроме того, колониальная система столкнулась с активным сопротивлением и ростом национально-освободительных движений, стремившихся к подлинной независимости и стремительно набиравших популярность. Даже попытки адаптировать структуру сообщества под модель британского содружества не смогли предотвратить распад, поскольку франкоцентричная политика и стремление удержать контроль над ключевыми сферами государственных интересов африканских стран породили сильные антиколониальные настроения. Наконец, влияние Франции в международных отношениях стало ослабевать из-за растущей конкуренции с другими странами, что вынудило ее пересмотреть свои методы управления бывшими колониями. Все эти факторы привели к тому, что французская колониальная система в своем традиционном

виде стала стремительно утрачивать свое значение и в конечном итоге была упразднена.

Список используемых источников

1. Филиппова Е. И., Филиппов В. Р. Распад колониальной империи в политике памяти Пятой Республики // Известия АлтГУ. 2020. №S6 (116). URL: https://cyberleninka.ru/ article/n/raspad-frantsuzskoy-kolonialnoy-imperii-v-politike-pamyati-pyatoy-respubliki (дата обращения 02.11.2024).
2. Пахоруков К.И. Франция – государства Африки: о некоторых аспектах децентрализованного сотрудничества // Вестник РУДН. Серия: Всеобщая история. 2023. №4. URL: https://cyberleninka.ru/article/n/frantsiya-gosudarstva-afriki-o-nekotoryh-aspektah-detsentralizovannogo-sotrudnichestva (дата обращения 02.11.2024).
3. Черкасов П. П. Судьба империи. Очерк колониальной экспансии Франции в XVI – XX вв // М., Наука. 1983. С. 81–85.
4. Долматова Е. А. Модернизация и инновация в колониальной политике Шарля де Голля // Ученые записки ОГУ. Серия: Гуманитарные и социальные науки. 2012. №1. URL: https://cyberleninka.ru/article/n/modernizatsiya-i-innovatsiya-v-kolonialnoy-politike-sharlya-de-gollya (дата обращения 02.11.2024).
5. Арутюнян Ж. А. Механизмы сотрудничества Франции с африканскими колониями / Ж. А. Арутюнян // Регион и мир. 2019. Т. 10. № 4. С. 35–39.

Averyanov M., Geht A. BRIEF ANALYSIS OF THE ACTIVITIES OF THE FRENCH UNION AND THE FRENCH COMMUNITY.

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article examines the multifaceted process of the disintegration of the French colonial empire, accelerated by global change and anti-colonial movements after the Second World War. The military conflicts in Indochina and Algeria, which became symbols of the failure of attempts to maintain control by force, as well as the peaceful decolonisation of Africa, are examined. Special attention is paid to the French Union and the French Community as attempts to modernise the administration of overseas territories, which in practice became instruments of control rather than autonomy. Despite the formal recognition of independence, France retained economic and military influence, which had a negative impact on the future nature of relations with the former colonies.
Key words: decolonisation, French colonial empire, anti-colonial movements, French Union, French Community, neo-colonialism.

УДК 327.7.94
ГРНТИ 11.25.47

ОТ СБСЕ К ОБСЕ: КРАТКИЙ ОБЗОР ТРАНСФОРМАЦИИ ОРГАНИЗАЦИИ

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

Совещание по безопасности и сотрудничеству в Европе (СБСЕ), основанное в 1975 году, возникло в условиях холодной войны с целью уменьшения напряженности между Востоком и Западом. Принятый тогда Хельсинкский Заключительный акт установил ключевые принципы, такие как суверенитет, нерушимость границ и права человека. Однако политические перемены конца 1980-х и 1990-х годов, включая распад Советского Союза и социалистического блока, поставили перед СБСЕ новые задачи и вызвали необходимость институциональных реформ. ОБСЕ расширила полномочия, став полноценной международной организацией с возможностью миротворческих операций и мониторинга прав человека. Тем не менее, современные вызовы, такие как обострение региональных конфликтов и необходимость адаптации к новым угрозам, требуют дальнейших реформ для повышения оперативности и эффективности ОБСЕ в XXI веке.

ОБСЕ, холодная война, безопасность в Европе, Будапештский саммит

Организация по безопасности и сотрудничеству в Европе (ОБСЕ) – созданная в 1975 году, представляет собой одну из ключевых международных межправительственных организаций, играющих важную роль в урегулировании споров и конфликтов в Европе, в обеспечении безопасности, стабильности и сотрудничества на европейском континенте. Ее создание, развитие и трансформация стали результатом многолетних усилий государств-членов, направленных на преодоление противоречий и угроз, возникающих в ходе исторических процессов и политических изменений. [1]

Предпосылки к созданию Совещания по безопасности и сотрудничеству в Европе (СБСЕ) появляются в разгар холодной войны, в 1950–1960-е годы, когда нарастающее противостояние между Восточным и Западным блоками создало необходимость поиска путей для снижения напряженности и укрепления мира в Европе, однако противоречия между странами враждующих блоков помешал реализации идеи. Прорыв произошел в конце 1960-х годов, когда страны Запада стали более заинтересованы в создании общеевропейского механизма безопасности, что совпало с политикой «разрядки» в отношениях между Востоком и Западом. В 1969 году на совещании министров иностранных дел стран-участниц НАТО в Брюсселе было принято решение поддержать

идею проведения общеевропейского совещания по вопросам безопасности. Это было воспринято Советским Союзом и его союзниками как готовность к диалогу, что дало мощный импульс процессу подготовки [1].

Переговоры о создании СБСЕ начались в 1972 году в Хельсинки, где представители 35 стран Европы, США и Канады обсуждали основные принципы, на которых будет строиться эта организация. Целью было создание площадки для постоянного диалога и взаимодействия между странами, имеющими различные политические системы и интересы, для укрепления стабильности и предотвращения конфронтаций [2].

В августе 1975 года в Хельсинки был подписан Заключительный акт СБСЕ, который стал основополагающим документом и определил принципы, лежащие в основе сотрудничества участников. Заключительный акт включал так называемые «Хельсинкские принципы», среди которых были:

– уважение суверенитета и равноправия всех государств;

– невмешательство во внутренние дела других стран;

– принцип нерушимости границ и территориальной целостности;

– мирное урегулирование споров;

– уважение прав человека и основных свобод.

Эти принципы были разделены на три основные «корзины», что символизировало комплексный подход к безопасности.

1. Первая корзина – политико-военные вопросы и меры укрепления доверия.

2. Вторая корзина – экономическое, научное и экологическое сотрудничество.

3. Третья корзина – гуманитарные вопросы, включая права человека, культурные и образовательные связи.

Заключительный акт не имел юридической силы и не налагал обязательств на страны, но его политическое значение было огромным. Подписавшие страны взяли на себя моральные обязательства следовать этим принципам, и это заложило основу для укрепления безопасности и сотрудничества в Европе [3]. Однако к концу 1980-х и началу 1990-х годов политические и социальные изменения в Европе создали новую международную среду, в которой организация в существовавшем формате не могла эффективно функционировать.

Первым толчком к преобразованию СБСЕ стал распад социалистического блока и завершение холодной войны. В 1989 году падение Берлинской стены символизировало конец многолетнего противостояния между Востоком и Западом и начало демократических реформ в странах Восточной Европы [4]. Эти государства теперь нуждались в поддержке для создания стабильных полити-

ческих структур и перехода к рыночной экономике, и для этого требовалась новая форма международного сотрудничества. Последовавший за этими событиями распад Советского Союза в 1991 году образовал 15 новых независимых государств, каждая из которых столкнулась с комплексом политических, экономических и социальных проблем [5]. Внезапное возникновение новых границ и национальных меньшинств стало причиной напряженности и нестабильности. Постсоветским странам требовалась поддержка в урегулировании внутренних и внешних конфликтов, а также в построении международно признанных и безопасных границ.

В то же время Европа столкнулась с жестокими вооруженными конфликтами в бывшей Югославии, события которых наглядно показали, что Европе необходима новая система коллективной безопасности, способная оперативно реагировать на локальные конфликты, предотвращать эскалацию насилия и проводить миротворческие операции [6]. Наряду с этим, в новых независимых государствах начали обостряться этнические и межнациональные конфликты, как, например, в Нагорном Карабахе, Приднестровье и Абхазии [7]. Эти кризисы требовали незамедлительного внимания и особого подхода со стороны международного сообщества.

Также стоит отметить, что с окончанием холодной войны возросла значимость вопросов защиты прав человека и демократических норм. Страны бывшего социалистического лагеря стремились к демократическим преобразованиям, что требовало создания механизмов для поддержки этих реформ и мониторинга их соблюдения. Эти изменения также привели к тому, что СБСЕ, ранее сфокусированное на политическом диалоге, стало стремиться к более активному участию в решении гуманитарных вопросов [8].

Все вышеперечисленные политические и социальные изменения в Европе бросали СБСЕ вызовы, в условиях которых организация не могла эффективно выполнять поставленные перед ней задачи и цели. Появилась потребность в институциональной реформе, создании структур безопасности и институтов по мониторингу прав человека. Расширение проблем, стоявших перед СБСЕ, требовало увеличения ресурсной базы организации, что включало увеличение финансирования, привлечение профессионалов в области безопасности, права и гуманитарной деятельности. Также важно было наладить тесное взаимодействие с другими структурами, такими как НАТО, Европейский Союз и ООН, для эффективного разделения обязанностей по поддержке безопасности в Европе и урегулирования конфликтов [9].

Реформы СБСЕ начались в конце 1980-х, первым шагом к которым стала Венская встреча (1986–1989 гг.), где был намечен курс на расширение сферы деятельности СБСЕ [10]. В условиях стремительных перемен в Восточной Ев-

ропе к моменту падения Берлинской стены стала очевидна потребность в новой структуре безопасности, способной объединить страны континента вокруг общих ценностей.

В 1990 году на Парижской встрече была подписана Парижская хартия для новой Европы. В условиях политических преобразований в Восточной Европе этот документ фактически провозгласил конец Холодной войны и зафиксировал курс на построение демократического общества, основанного на правах человека и верховенстве закона. Парижская хартия также заложила основы для новых механизмов СБСЕ, таких как институт наблюдения за выборами, защиты прав человека и раннего предупреждения конфликтов [9].

Следующими реформами СБСЕ стало создание новых структур, а именно: Бюро по демократическим институтам и правам человека (БДИПЧ), Центр предотвращения конфликтов и институт Верховного комиссара по делам национальных меньшинств. Эти учреждения стали инструментами для контроля за соблюдением прав человека, поддержания демократических процессов и мирного урегулирования возникающих кризисов, что стало особенно актуально с началом конфликтов в бывших югославских республиках и на территории распадающегося СССР [11].

В 1992 году на встрече в городе Хельсинки года участники СБСЕ закрепили принципы мирного урегулирования конфликтов и дали организации право на проведение миротворческих миссий, что стало важным шагом к ее дальнейшему институциональному оформлению. СБСЕ активно включилось в работу по разрешению локальных кризисов, таких как конфликты в Нагорном Карабахе, Приднестровье, Абхазии и Боснии. Из совещательной структуры организация приобретала более существенную роль в европейской политике, что позволяло ей перейти от пассивного наблюдения к активным действиям [12].

Окончательное преобразование произошло в 1994 году на Будапештском саммите, где было принято решение о создании полноценной международной организации под названием Организация по безопасности и сотрудничеству в Европе (ОБСЕ). Новое название отразило более активный и ответственный подход к вопросам безопасности и сотрудничества, подчеркивая возросшую значимость ОБСЕ в международной политике. Теперь организация получила право не только заниматься урегулированием конфликтов, но и способствовать укреплению демократических институтов и наблюдать за соблюдением прав человека по всему региону [13].

В результате преобразования ОБСЕ стала важнейшей платформой для многостороннего диалога и взаимодействия по вопросам безопасности, прав человека и демократии. Реформы, проведенные в конце 1980-х – начале

1990-х годов, преобразовали ОБСЕ из консультативной структуры в многостороннюю организацию с обширным мандатом, охватывающим вопросы безопасности, защиты прав человека и содействия демократическим преобразованиям. Создание структурных институтов в организации позволило ОБСЕ выйти на новый уровень оперативного реагирования на кризисы и поддержания стабильности в регионе. ОБСЕ внесла значительный вклад в урегулирование конфликтов в Балканах, на Кавказе и в Восточной Европе, создав важные прецеденты мирного разрешения споров и мониторинга за соблюдением прав человека [14].

Однако, несмотря на эти достижения, с момента преобразований прошло более двух десятилетий, и ситуация в Европе существенно изменилась. Современные вызовы, такие как обострение региональных конфликтов, ослабление демократических институтов и нарастающие миграционные потоки, ставят под вопрос способность ОБСЕ эффективно адаптироваться к новым реалиям. Учитывая ограниченность мандата, вновь возникшую потребность в увеличении финансирования организации, а также необходимость согласования решений между всеми 57 участниками, ОБСЕ часто оказывается не в состоянии быстро и эффективно реагировать на угрозы безопасности [15].

Таким образом, можно заключить, что реформы 1990-х годов значительно повысили эффективность деятельности организации в решении поставленных перед ней целей, однако политические и социальные условия в Европе претерпели множества изменений, к которым ОБСЕ вновь требуется адаптация. Очевидна потребность в обновлении ее механизмов, в частности усилении полномочий для реагирования на кризисы, увеличении финансирования и модернизации структур. Принципы, заложенные в Заключительном акте СБСЕ и Парижской хартии, остаются актуальными, но их реализация требует пересмотра форматов сотрудничества. ОБСЕ должна развиваться, чтобы соответствовать вызовам XXI века и оставаться ключевым институтом для обеспечения мира и стабильности на европейском континенте.

Список используемых источников

1. Организация по безопасности и сотрудничеству в Европе. URL: https://www.osce.org/ru/ (дата обращения 13.11.2024). https://www.osce.org/ru/

2. Заключительный акт Совещания по безопасности и сотрудничеству в Европе // РИА Новости. URL: https://ria.ru/20100801/ 260016995.html?ysclid=m3h060jugs215442758 (дата обращения 13.11.2024).

3. Хельсинкский Заключительный акт. URL: https://www.osce.org/ru/ministerial-councils/39505 (дата обращения 14.11.2024).

4. Берлинская стена. Досье // ТАСС. URL: https://tass.ru/info/1559157?ysclid =m3h0qcfndo742929484 (дата обращения 13.11.2024).

5. История распада СССР. Предпосылки и основные шаги // ТАСС. URL: https://tass.ru/info/13298931?ysclid=m3h0s0kiue935948534 (дата обращения 13.11.2024).
6. OSCE and Yugoslavia - Important dates, timeline // Organization for Security and Co-operation in Europe. URL: https://www.osce.org/odihr/52914 (дата обращения 13.11.2024).
7. История нагорнокарабахского конфликта // ТАСС. URL: https://tass.ru/info/8979501 (дата обращения 13.11.2024).
8. Доклад ОБСЕ: Десять лет деятельности БДИПЧ: на благо прав человека и демократии (1991–2001) // Organization for Security and Co-operation in Europe. URL: https: https://www.osce.org/files/f/documents/4/c/20458.pdf (дата обращения 13.11.2024).
9. Парижская хартия // Organization for Security and Co-operation in Europe. URL: https://www.osce.org/files/f/documents/3/4/39520.pdf (дата обращения 14.11.2024).
10. Итоговый документ третьей встречи, Вена, 4 ноября 1986 года - 19 января 1989 года // Organization for Security and Co-operation in Europe. URL: https://www.osce.org/ru/mc/40885 (дата обращения 14.11.2024).
11. Доклад ОБСЕ: Что такое БДИПЧ? // Organization for Security and Co-operation in Europe. URL: https://www.osce.org/files/f/documents/5/1/13702.pdf (дата обращения 14.11.2024).
12. СБСЕ Хельсинкский документ 1992 года. Вызов времени перемен. // Organization for Security and Co-operation in Europe. URL: https://www.osce.org/files/f/documents/8/0/39534.pdf (дата обращения 14.11.2024).
13. Будапештский документ 1994 года. На пути к подлинному партнерству в новую эпоху // Organization for Security and Co-operation in Europe. URL: https://www.osce.org/ files/f/documents/b/a/39558.pdf (дата обращения 14.11.2024).
14. Conflict Prevention in Europe: Does the OSCE Have a Future? // Wilson Center. URL: https://www.wilsoncenter.org/publication/254-conflict-prevention-europe-does-the-osce-have-future (дата обращения 14.11.2024).
15. Summary: OSCE Focus Conference 2023 // GCSP. URL: https://dam.gcsp.ch/ files/doc/summary-osce-focus-conference-2023 (дата обращения 14.11.2024).

Bondar N. FROM THE CSCE TO THE OSCE: A BRIEF OVERVIEW OF THE TRANSFORMATION OF THE ORGANIZATION.

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The Conference on Security and Cooperation in Europe (CSCE), established in 1975, emerged during the Cold War with the aim of reducing tensions between East and West. The Helsinki Final Act, adopted at that time, set forth key principles such as sovereignty, the inviolability of borders, and human rights. However, the political transformations of the late 1980s and early 1990s, including the dissolution of the Soviet Union and the socialist bloc, posed new challenges for the CSCE and highlighted the need for institutional reform. The organization subsequently expanded its mandate, evolving into the Organization for Security and Cooperation in Europe (OSCE), with the authority to conduct peacekeeping operations and monitor human rights. Nevertheless, contemporary challenges, including escalating regional conflicts and the need to adapt to emerging threats, underscore the necessity for further reforms to enhance the OSCE's responsiveness and effectiveness in the 21st century.

Key words: OSCE, Cold War, European security, Budapest Summit.

УДК 341.162
ГРНТИ 28.23.02

РАЗВИТИЕ МЕЖДУНАРОДНОГО КОНТРОЛЯ ЗА ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ПРИМЕРЕ ДЕЯТЕЛЬНОСТИ КОНСУЛЬТАТИВНОГО ОРГАНА ООН (КОИИ ООН) ПО ИСКУССТВЕННОМУ ИНТЕЛЛЕКТУ

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

С каждым годом прогресс в развитии технологий, основанных на машинном обучении, становится все быстрее. Это диктует новые вызовы не только техническим корпорациям, но и международному праву. В связи с этим международным сообществом предпринимается ряд действий, направленных на регуляцию новейших технологий. Целью данной статьи является анализ работы одной из организаций, осуществляющих работу в этом направлении – Консультативный орган по искусственному интеллекту (КОИИ), функционирующий в рамках ООН. Основное внимание уделяется анализу документа, ставшего своеобразным итогом годовой деятельности международного экспертного сообщества, «Глобальному цифровому договору», а также его оценкам.

ООН, КОИИ, искусственный интеллект, глобальный цифровой договор

На фоне стремительного роста популярности как применения различных форм программного обеспечения, основанного на технологиях машинного обучения, так и в целом популяризации понятия «искусственный интеллект» в общественно-политическом дискурсе в 2023 г. под руководством Генерального Секретаря ООН Антонио Гутерриша была создана новая структура – Консультативный орган по искусственному интеллекту (КОИИ). «ИИ может помочь преодолеть препятствия на пути к достижению ключевых целей развития, но это зависит от того, будут ли технологии ИИ использоваться ответственно и всеми, включая развивающиеся страны, которым необходимо срочно ускорить устойчивое развитие», – отметил Генеральный секретарь. […] Масштабное использование этих технологий без особого внимания к вопросам безопасности вызывает беспокойство. Под угрозой может быть защита личных данных, целостность и правдивость распространяемой информации и в более широком смысле – даже демократические ценности. […] «Именно поэтому я организовал глобальную междисциплинарную дискуссию с участием

многих заинтересованных сторон о возможностях и управлении ИИ, о связанных с ним рисках и проблемах», – пояснил Генсек ООН. [1]. В конце того же года был опубликован первый промежуточный доклад «Управление ИИ на благо человечества». В нем содержался призыв к более тесному согласованию между международными нормами и тем, как разрабатывается и внедряется ИИ [2].

Основные положения, описанные в документе, можно свести к следующим тезисам:

– несмотря на то, что развитие искусственного интеллекта трансформирует наш мир, на данный момент его преимущества сконцентрированы в руках небольшого числа частных компаний и ограниченного круга государств. При этом негативные последствия от применения ИИ также распределяются неравномерно. Для того чтобы обеспечить доступность ресурсов, создать более инклюзивные механизмы представительства и надзора, обеспечить ответственность за причиненный ущерб, а также гарантировать, что геополитическая конкуренция не будет стимулировать безответственное использование ИИ или препятствовать его ответственному управлению, необходимо внедрить глобальную систему управления с равным участием всех государств-членов;

– искусственный интеллект обладает потенциалом радикально преобразовать доступ к знаниям и повысить эффективность во всех сферах жизни во всем мире. Новое поколение новаторов расширяет границы науки и техники в области ИИ. Внедрение искусственного интеллекта повышает производительность и стимулирует инновации в секторах от здравоохранения до сельского хозяйства как в развитых, так и в развивающихся странах. Наряду с этими позитивными изменениями, возникают вопросы о том, какие условия необходимы для того, чтобы выгоды от ИИ распределялись справедливо и безопасно среди всего человечества, а также для устранения и управления негативными последствиями, включая влияние на занятость населения. Важной задачей для политиков является, с одной стороны, создание успешных экосистем развития ИИ по всему миру, а с другой - обеспечение подотчетности как новых, так и действующих субъектов, участвующих в этих процессах. Таким образом, ключевым вызовом является нахождение баланса между стимулированием инновационного потенциала ИИ и обеспечением его справедливого и безопасного применения в интересах всего общества;

– искусственный интеллект обладает потенциалом содействовать прогрессу в тех областях, где рыночных механизмов недостаточно. К таким сферам относятся: прогнозирование экстремальных погодных явлений и мониторинг биоразнообразия, расширение образовательных возможностей и доступа

к качественному здравоохранению, а также оптимизация энергетических систем. Государственные органы и общественный сектор могут использовать технологии искусственного интеллекта для повышения качества предоставляемых гражданам услуг, а также для улучшения обслуживания уязвимых слоев населения в интересах всего общества.

Спустя девять месяцев после начала работы, в преддверии проведения в сентябре 2024 г. Саммита Будущего, КОИИ подготовил новый доклад – о регулировании искусственного интеллекта [3]. Он является политически нейтральным и содержит в себе положения общие для всех стран. Так, группа экспертов подготовила семь рекомендаций по регулированию ИИ:

1) создание *независимой Международной научной группы по искусственному интеллекту*, которая сможет объединить экспертов из разных стран и дисциплин и будет работать при поддержке учреждений ООН;

2) начать в рамках ООН *межправительственный диалог по вопросам управления ИИ.* В рамках него делится опытом и разработками, которые возможно внедрить сразу в нескольких странах;

3) организация *обмена стандартами в области искусственного интеллекта,* с участием представителей национальных и международных организаций;

4) создание *сети для развития потенциала в области ИИ.* Среди прочего она должна предоставлять тренеров, вычислительные мощности и данные для обучения ИИ исследователям и предпринимателям, которые стремятся применять эту технологию в общественных интересах; запустить программу стипендий для перспективных специалистов;

5) создание *глобального фонда* для развития ИИ, который сможет управляться независимой структурой. Фонд, в том числе, должен обеспечивать предоставление вычислительных ресурсов для специалистов в странах, где их нет, и создать репозиторий для ИИ-моделей и наборов данных, которые могут использоваться для целей устойчивого развития;

6) создание глобальной *структуры по управлению данными* для искусственного интеллекта, на примере Всемирной организации интеллектуальной собственности;

7) создание *офиса ИИ,* который будет подчиняться генсекретарю ООН.

Также в докладе отмечены несколько опасностей в развитии технологий, связанных с ИИ: использование Искусственного Интеллекта может наносить вред окружающей среде, так как на его создание требуются большие энергетические ресурсы; неравномерное развитие может приводить к усилению разрыва между странами. По заявлениям экспертов риски можно минимизиро-

вать путем глобального сотрудничества и выработки международных норм по регуляции ИИ.

Выводы данного доклада легли в основу «Глобального цифрового договора» – документа, содержащего основные международные принципы по развитию инновационных технологий. В нем доступ к интернету рассматривается как естественное право человека, при этом страны, подписавшие договор обязываются противодействовать дискриминации в вопросе доступа к интернету и защищать права человека в интернет-пространстве [4].

Однако мировым сообществом данный документ был встречен неоднозначно. Так, во время XIV российского форума по управлению Интернетом, советник департамента международной информационной безопасности МИД России Б. А. Васильев заявил, что данный договор не соответствует интересам развивающихся стран. По его словам, первоначальная версия договора направлена только на интересы цифровых платформ и не предусматривает какого-либо государственного регулирования. Это может допускать «навязывание интересов» пользователям, ввиду отсутствия у них выбора. Это также отмечали другие эксперты уже после принятия окончательной версии договора.

Другим камнем преткновения стал вопрос цифрового суверенитета государства, который практически не регулируется в данном договоре. Само слово «суверенитет» встречается в тексте всего четыре раза, в то время как куда более условно относящееся к проблематике текста понятие «гендер» имеет более тридцати прямых упоминаний. Фактически, в договоре роль государств в урегулировании цифрового права приравнивается к роли цифровых платформ и частного бизнеса.

Независимые эксперты также отмечают возможную неэффективность данного договора. Константинос Комайтис (руководитель направления цифрового управления, демократии и технологий, представитель Атлантического совета) также высказал критику в отношении этого договора. Он отметил, что в нем отсутствует привязка к уже существующим процессам и органам. Создание новых структур с нуля будет провоцировать еще большие дебаты и отдалять мировое сообщество от консенсуса. «Отсутствие сотрудничества между государствами-членами привело к тому, что текст оказался слабым и неопределенным – он слаб в отношении прав человека, слаб в отношении управления Интернетом и слаб в отношении подключения», – заявил К. Комайтис [5].

В свою очередь, профессор Сколтеха И. В. Оселедец считает, что реализация норм, единых для всех государств, может быть затруднена различиями в системах права и стандартах к инновационным технологиям. По его мнению,

следует создать единый консультативный орган, который сможет давать рекомендации, исходя из особенностей стран.

Другой вопрос подняла Элисон Гиллвальд, исполнительный директор Research ICT Africa. Она считает, что составители договора не до конца понимают причины цифрового неравенства. Несмотря на то, что одной из главных целей документа является достижении равного доступа к цифровым ресурсам, в нем его отсутствие рассматривается только с точки зрения людей, у которых нет никакой возможности использовать интернет. Однако, множество людей при формальном доступе к интернету не могут себе позволить достаточное его качество, из-за тяжелой финансовой ситуации они остаются невидимыми в глобальной сети, при этом не попадая под программы по развитию. Э. Гильвальд отмечает: «Отсутствие цифрового участия у большинства людей, особенно африканцев, делает их невидимыми, недопредставленными и дискриминируемыми в гигантских массивах данных передовых технологий, основанных на информации, и это нельзя исправить с помощью рамок «ответственного и этичного» ИИ» [6].

Исходя из вышеперечисленных противоречий, Российская Федерация приняла решение дистанцироваться от консенсуса по «Глобальному цифровому договору». Однако, МИД также выступил с заявлением, что правительством признается важность международного сотрудничества в данном вопросе и осознаются все риски, которые несет применение технологий, связанных с ИИ. Тем не менее, Российская Федерация будет готова вернуться к обсуждению новых цифровых договоров, при условии учитывания ООН ее мнения.

Таким образом, проблемы развития международного права в области применения технологий, основанных на машинном обучении, с каждым годом становятся все актуальнее. Большое влияние на это оказала пандемия Covid-19, во время которой увеличилось не только количество пользователей «глобальной паутины», но и обострились назревавшие конфликты. События буквально нескольких лет усугубили разрыв в цифровом развитии стран и показали, насколько уязвимыми могут быть люди, не имеющие доступа к Интернету. Значительно выросло количество киберпреступлений, ежегодно появляются десятки новых видов интернет-мошенничества с использованием технологий, основанных на применении ИИ. Борьба с этим требует коллективных решений от всех государств. Однако, качественное противодействие вызовам невозможно без достижения всеобщего консенсуса. Международные договоры не будут эффективны, если их примет только часть государств: подобное положение вещей будет не только способствовать дальнейшему росту между-

народной напряженности, но и закреплять разобщенность человечества в подходах к применению передовых технологий.

Список используемых источников

1. Гутерриш дал старт работе глобального Консультативного органа по искусственному интеллекту // Новости ООН. URL: https://news.un.org/ru/story/2023/10/1446237 (дата обращения 12. 10. 2024).
2. 2023 Промежуточный отчет: Управление ИИ в интересах человечества/Interim Report: Governing AI for Humanity, ООН, AI Advisory Body // Национальный портал в сфере искусственного интеллекта. URL: https://ai.gov.ru/knowledgebase/mezhdunarodnye-dokumenty-po-razvitiyu-ii/2023_promeghutochnyy_otchet_upravlenie_ii_v_interesah_chelovechestva_interim_report_governing_ai_for_humanity_oon_ai_advisory_body/ (дата обращения 12. 10. 2024).
3. В ООН представили план по управлению искусственным интеллектом. // Организация Объединенных Наций. URL: https://news.un.org/ru/story/2024/09/1456466 (дата обращения 12. 10. 2024).
4. «Pact for the Future, Global Digital Compact and Declaration on Future Generations» dated sept. 22, 2024 // United Nations Publishing House. 2024.
5. Analysis: a brave new reality after the UN's Global Digital Compact // Digital Forensic Research Lab. URL: https://dfrlab.org/2024/10/01/analysis-a-brave-new-reality-after-the-uns-global-digital-compact/ (accessed: 12. 10. 2024).
6. Reactions to the Adoption of the UN Global Digital Compact // Tech Policy Press. URL: https://www.techpolicy.press/reactions-to-the-adoption-of-the-un-global-digital-compact/ (accessed: 12. 10. 2024).

***Gekht A.* DEVELOPMENT OF INTERNATIONAL CONTROL OVER ARTIFICIAL INTELLIGENCE'S USE ON THE EXAMPLE OF THE ACTIVITIES OF THE UN'S ADVISORY BODY ON ARTIFICIAL INTELLIGENCE.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Every year the progress in the development of Artificial Intelligence becomes faster and faster. It dictates new challenges not only to technical corporations, but also to international law. In this regard, a series of actions aimed at the regulation of the latest technologies are undertaken as well. The purpose of this article is to analyze the work of one of the organizations working in this direction – the Advisory Body on Artificial Intelligence (ABAI). Much attention is paid to the document that has become a kind of a result of their annual activities, the "Global Digital Compact", as well as its assessments.

Key words: the UN, Artificial Intelligence, ABAI, Global Digital Compact.

УДК 32
ГРНТИ 11

АНАЛИЗ ПРАКТИЧЕСКОГО ВОПЛОЩЕНИЯ ИДЕЙНОГО НАСЛЕДИЯ РИХАРДА КУДЕНХОВЕ-КАЛЕРГИ

А. Б. Гехт, А. И. Капуков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье проводится анализ практического воплощения идейного наследия ключевого деятеля панъевропейского движения Рихарда Куденхове-Калерги. Рассматривается влияние идеологии Калерги на современные общественно-политические процессы, а также на формирование международных отношений. Авторы исследуют различные аспекты идейного наследия Калерги, его воплощение в условиях современной единой Европы, подчеркивая его значимость в контексте идейного фундамента Европейского союза.

Рихард Куденхове-Калерги, европейская интеграция, европейская идея, Пан-Европа, Панъевропейский союз

Попытки сформировать влиятельную, экономически мощную и стабильную Единую Европу в период между двумя мировыми войнами тесно переплетены с работой выдающегося общественного деятеля графа Рихарда Куденхове-Калерги. Он стал основателем и руководителем Панъевропейского союза, который можно справедливо считать одной из основополагающих инициатив на пути к современному Европейскому союзу.

В 1923 году в столице Австрии, Вене, Куденхове-Калерги выпустил свою знаковую работу – манифест «Пан-Европа». В этой книге он изложил концепцию объединения государств Европейского континента в единый союз, противостоящий другим мощным мировым объединениям: Панамерике, Паназии, Британской империи и СССР. Этот труд быстро был переведен на множество языков и вызвал широкий общественный интерес [1].

После выхода книги Куденхове-Калерги основал Панъевропейский союз, задачей которого стало продвижение идеи единства в рамках Европы. Граф активно стремился создать национальные секции данной организации в разных странах континента, налаживая взаимодействие с европейскими политиками. Особенно важным для него было сближение Франции и Германии. Он выступал за полное примирение этих стран и пересмотр некоторых положений Версальского договора [2]; спустя почти два десятилетия после окончания Второй мировой войны, благодаря Елисейскому договору 1963 года, произошло реальное объединение французской и немецкой сторон, ставшее крае-

угольным камнем архитектуры международных отношений в Западной Европе.

Нельзя не отметить, что именно Рихард Куденхове-Калерги стал одним из первых европейцев, кто предложил концепцию создания федеративного союза из европейских стран. Он выступал за учреждение Европейского парламента, названного Федеральной ассамблеей, а также федерального суда и свободного таможенного союза. Интересно, что в послевоенные годы Куденхове-Калерги также ратовал за формирование европейских вооруженных сил для поддержания мира, и, хотя многие современные лидеры Европы (например, А. Меркель, Э. Макрон) высказывают схожие идеи, создание единой европейской армии так и не состоялось. Стоит отметить, что граф составил основополагающий текст Европейского Пакта, который, по сути, стал первым проектом общеевропейской конституции.

Куденхове-Калерги уделял исключительно важное внимание популяризации идеи Европы через школьное образование. Он сам работал над изменениями в учебных планах, которые должны были уточнить понятие Европы и четко обозначить ее границы, а также исторические и культурные регионы. Граф полагал, что сама концепция "европейской истории" станет понятной только при тщательном разграничении от "мировой истории". Важной частью распространения европейской идеи он считал работу печатных изданий. Также Калерги выступал за идеи по созданию Европейской Академии, в которой ведущие представители европейской культуры могли бы работать совместно, обходя политику, на благо общей европейской культуры. Главной задачей Академии должно было стать проведение конференций для достижения консенсуса по культурным вопросам [3].

Занимательны мысли Куденхове-Калерги о будущих этнических трансформациях единой Европы предвосхитили современные процессы массовой миграции. В своем основополагающем произведении «Практический идеализм» (1925) философ утверждал, что будущее человечество станет гибридом, а различные расы и касты уступят место новому разнообразию личностей. Он отмечал, что в семьях с родственным скрещиванием все дети будут схожи, тогда как в смешанных семьях каждый из них будет формировать уникальную вариацию [4].

Куденхове-Калерги активно способствовал созданию экономического сотрудничества в Европе, организуя экономические конференции и обсуждая ключевые вопросы. Вскоре после одного из многочисленных конгрессов был основан Панъевропейский экономический центр. На этих форумах он вместе с единомышленниками высказывал идеи о создании Европейского банка, который затем стал прообразом современного Европейского центрального

банка. К концу 1930-х годов он стремился вовлечь в экономическую интеграцию страны Дуная, такие как Австрия, Венгрия и Чехословакия, поддерживая инициативы по Римским протоколам [5]. Тем не менее, эти и многие другие начинания графа оказались нереализованными из-за мирового экономического кризиса, предшествовавшего Второй мировой войне.

Следует отметить, что Куденхове-Калерги предпочитал самостоятельно формулировать идеи и разрабатывать концепции, надеясь, что к его национальным секциям присоединятся политики и ученые, согласные с его взглядами. Это привело к тому, что Панъевропейский союз приобрел преимущественно элитарный характер и идеи его лидера часто вызывали противоречия. Так, выступая против А. Гитлера, Калерги, в то же время, проявлял сдержанные симпатии к некоторым аспектам политики Б. Муссолини [6]. Отношение графа к Советскому Союзу также менялось: в первые годы 1920-х он критиковал советский режим, но к 1935 году, подписанию Советско-Французского пакта, его взгляд изменился, когда он увидел положительные стороны большевистской и сталинистской идеологии, предполагая, что в будущем европейская элита не будет формироваться на основе социального происхождения [7].

Таким образом, идеи Рихарда Куденхове-Калерги значительно опередили свою эпоху и, к великому сожалению, многие его инициативы остались неосуществленными из-за мирового экономического кризиса 1930-х годов и итогов Второй мировой войны. Лишь после войны начался активный процесс формирования интеграционных объединений в Европе, и концепция, предложенная основателем Панъевропейского союза, стала основой для современного Европейского союза с его Шенгенским соглашением, Европарламентом, единой валютой, кульминацией европейского права и другими наднациональными институтами. Вследствие этого, Рихард Куденхове-Калерги по праву считается одним из идеологических «отцов» современной Единой Европы, которая во многом являет собой попытку воплощения его прогрессивных идей.

Список используемых источников

1. Официальные данные Еврокомиссии. Европейский союз: уроки интеграции // Экономист. 1998. № 10.
2. Версальский мирный договор 1919 г. Большая Российская Энциклопедия. URL: https://bigenc.ru/c/versal-skii-mirnyi-dogovor-1919-8c76ec. (дата обращения 11.11.2024).
3. Истоки европейской идеи. Helpiks. URL: https://helpiks.org/3-80369.html. (дата обращения 12.11.2024).
4. Практический идеализм Куденхове-Калерги. STUDYLIB. URL: https://studylib.ru/doc/6394608/prakticheskij-idealizm.-kudenhove-kalegri. (дата обращения 13.11.2024).
5. Кораблева А. Е. Панъевропейский проект Р. Куденхове-Калерги и международные отношения в Европе в 20-30 гг. XX века. Дисс. канд. ист. наук. Нижний Новгород, 2009.

6. Куденхове-Калерги Р. Н. Европейский манифест // Европейский альманах. М., 1991. С. 120–126.
7. Громова А. В. Подунайские страны в интеграционных концепциях Рихарда Куденхове-Калерги и Милана Годжи // Реформы вчера, сегодня, завтра. М.,1999. № 11-12. С. 162-178.

Gekht A., Kapukov A. **ANALYSIS OF THE PRACTICAL IMPLEMENTATION OF THE IDEAL HERITAGE OF RICHARD COUDENHOVE-KALERGI.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article analyzes the practical implementation of the ideological legacy of the key figure of the pan-European movement Richard Coudenhove-Kalerga. The influence of Kalerga's ideology on modern socio-political processes, as well as on the formation of international relations, is considered. The authors explore various aspects of Kalerga's ideological heritage, its embodiment in the conditions of a modern united Europe, emphasizing its importance in the context of the ideological foundation of the European Union.

Key words: Richard Coudenhove-Kalerga, European integration, European idea, Pan-Europe, Pan-European Union.

УДК 327
ГРНТИ 11.15.25

ОСОБЕННОСТИ PR-ПРОДВИЖЕНИЯ КОСМИЧЕСКОЙ ПОЛИТИКИ РФ НА СОВРЕМЕННОМ ЭТАПЕ

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

В данной статье рассматривается PR-сопровождение космической политики как важный инструмент формирования имиджа России на мировой арене. Анализируются теоретические основы PR-деятельности, включая стратегическое планирование коммуникаций и управление репутацией, а также их применение в контексте космической отрасли. Особое внимание уделяется значению PR-сопровождения для демонстрации технологического лидерства России, привлечения международных партнеров и инвестиций, популяризации космических исследований и противодействия негативной информации.

космическая политика, международные отношения, космические исследования, геополитика, PR-сопровождение, технологическое лидерство, «мягкая сила»

PR-сопровождение космической политики представляет собой комплекс мероприятий, направленных на формирование положительного имиджа космической отрасли страны и продвижение ее интересов в сфере освоения космоса на международной арене. В контексте российской космической программы PR-сопровождение играет ключевую роль в укреплении позиций страны как ведущей космической державы и способствует развитию международного сотрудничества.

В современном геополитическом пространстве космическая деятельность играет важную роль не только в научно-техническом развитии государств, но и в формировании их международного имиджа. Российская Федерация, как одна из ведущих космических держав, активно использует PR-сопровождение своей космической политики в качестве инструмента «мягкой силы» для укрепления своих позиций на мировой арене.

Теоретические основы концепции «мягкой силы» были заложены американским политологом Джозефом Наем. Впервые он представил этот термин в своей статье, опубликованной в 1990 году в журнале «Foreign Policy». В этой работе Най утверждал, что государства могут достигать своих целей не только с помощью принуждения или экономических стимулов, но и через привлекательность своей культуры, политических ценностей и внешней политики [1]. Он противопоставил «мягкую силу» понятию «жесткой силы», которая осно-

вывается на использовании военной и экономической мощи для достижения желаемых результатов.

Най определил «мягкую силу» как способность влиять на других, побуждая их хотеть того же, чего хочет государство, без применения насилия или подкупа. Он выделил три ключевых ресурса, способствующих формированию «мягкой силы»: культура, наука и технологии, политические ценности и легитимная внешняя политика. Эти элементы играют важную роль в международных отношениях, позволяя государствам укреплять свои позиции на мировой арене.

В последние годы научно-техническое развитие, особенно в области мирного использования космоса, становится все более значимым элементом геополитических стратегий многих стран. С ростом коммерческой космической деятельности, развитием новых технологий и увеличением интереса к космосу государства осознают необходимость укрепления своих позиций в этой сфере. Однако традиционные показатели силы, такие как военная и экономическая мощь, не являются единственными факторами, определяющими успех государства.

В рамках космической политики концепция «мягкой силы» появилась как способ укрепления позиций страны в космосе. Идея о важности «мягкой силы» в этой области является относительно новой, и до сих пор существует недостаток академических исследований на эту тему. Тем не менее, уже сейчас государства применяют различные инструменты «мягкой силы» для достижения своих целей в космической политике [2]. Страны с высоким технологическим потенциалом, эффективными дипломатическими стратегиями и успешными информационными кампаниями смогли использовать эти преимущества для достижения конкурентных позиций в новой космической гонке.

Одним из ключевых факторов формирования положительного имиджа является правильно разработанная стратегия пропаганды через средства массовой информации. Успехи в космической сфере становятся важными новостными повода и широко освещаются, влияя на общественное мнение как внутри страны, так и за ее пределами. Среди направлений популяризации космической науки можно выделить публикации в СМИ, киноиндустрию (включая художественные, научно-популярные и документальные фильмы, а также анимацию) и телепередачи, которые подчеркивают значимость изучения космоса и способствуют росту интереса к космической науке среди населения.

Стоит отметить, что в XXI веке одним из наиболее эффективных каналов коммуникации стал Интернет. Космические агентства стран прошли процесс цифровизации и активно демонстрируют свои достижения на современных платформах для взаимодействия с аудиторией [3]. В этом контексте стоит от-

метить деятельность таких крупных космических агентств, как NASA, Европейское космическое агентство (ESA) и Роскосмос, которые имеют собственные каналы и страницы в соцсетях.

Стратегии PR-сопровождения космической политики Российской Федерации представляют собой комплекс мероприятий, направленных на продвижение имиджа России как ведущей космической державы, а также на укрепление ее позиций в международной космической сфере. Эти стратегии включают несколько ключевых направлений, которые обеспечивают информационную поддержку государственных инициатив и достижений в космосе.

Одной из основных стратегий является формирование положительного имиджа России как технологического лидера в космической отрасли. Это достигается через активное освещение успехов российских космических программ, таких как запуск ракет-носителей «Союз» и «Ангара», а также участие в международных проектах, таких как Международная космическая станция (МКС). Примером может служить освещение миссии «Союз МС-19», которая привлекла внимание мировой общественности и продемонстрировала готовность России к выполнению сложных космических задач.

Важным элементом PR-сопровождения является развитие международного сотрудничества. Россия на протяжении современного этапа активно взаимодействовала с другими странами в рамках совместных проектов, таких как программа МКС или миссия «ExoMars» с Европейским космическим агентством (ESA) [4]. Эти проекты широко освещались в средствах массовой информации (СМИ) и способствовали укреплению позиций России на международной арене. Тем не менее, начиная с 2022 года потенциал сотрудничества со странами Запада начал ослабевать, и поэтому одной из приоритетных задач в сфере космической политики стало выстраивание научно-технологического партнерства с дружественными странами, – к примеру, с Китаем. В качестве примера можно отметить пример сотрудничества с Китаем по созданию лунной станции и ряд других перспективных проектов, которые в перспективе способствуют развитию сотрудничества в сфере освоения космического пространства [5].

Еще одной важной стратегией является популяризация космических исследований среди широкой общественности. Роскосмос активно использует социальные сети и цифровые платформы для распространения информации о своих достижениях. Например, трансляции запусков ракет и жизнь на МКС транслируются через «YouTube» и другие платформы («ВКонтакте», «Telegram»), что способствует повышению интереса к российской космонавтике среди молодежи и широкой аудитории.

Кроме того, PR-сопровождение играет ключевую роль в противодействии негативной информации. В условиях международной конкуренции и геополитической напряженности важно формировать объективное представление о российских космических программах. После неудачного запуска миссии «Луна-25» Роскосмос активно информировал общественность о планах продолжения лунной программы уже в рамках миссий «Луна-26» и «Луна-27», что помогло сохранить доверие к российской космонавтике [6].

Наконец, PR-сопровождение способствует продвижению российских космических технологий и услуг на международном рынке. Россия активно развивает экспорт своих космических услуг, включая запуск спутников для других стран и предоставление услуг дистанционного зондирования Земли. Примером может служить сотрудничество с Индией по запуску спутников для их национальной программы. Кроме того, важно отметить и фактор участия России в конференциях и форумах международного уровня – в ноябре 2024 года государство приняло участие в выставке «Air Show China – 2024», что имеет значительное значение для укрепления позиций страны в глобальной космической индустрии [7]. На объединенном стенде Роскосмоса, в который входят девять организаций, таких как НПО Лавочкина и РКК «Энергия», демонстрируются образцы как существующей, так и перспективной ракетно-космической техники. В частности, НПО Лавочкина представила макеты аппаратов «Беркут-ВР», «Арктика-М», а также «Луна-26». РКК «Энергия» продемонстрировала макеты Российской орбитальной станции (РОС) и нового поколения транспортного корабля. НПО «Энергомаш» представила макеты различных ракетных двигателей, включая жидкостные и плазменные.

Таким образом, в условиях нарастающей геополитической напряженности и ограниченных возможностей для научного сотрудничества со странами Запада, применение PR-стратегий в сфере космической политики Российской Федерации приобретает особую важность. Эти стратегии становятся ключевым инструментом для поддержания и укрепления позиций России как ведущей космической державы на международной арене. PR-сопровождение космической политики РФ в текущих условиях играет важную роль в формировании положительного имиджа страны и ее космической отрасли. Оно помогает демонстрировать технологические достижения и инновационный потенциал России, несмотря на санкции и политические ограничения. Это особенно важно для привлечения новых партнеров и инвесторов из стран, не участвующих в санкционной политике против России.

Список используемых источников

1. Nye J. Jr. Soft power // Foreign Policy, 1990. № 80. 209 p.
2. Сафарова Р. Р. Освоение космоса как элемент «мягкой силы» в современной мировой политике // Актуальные вопросы мировой политики. СПб: Научно-исследовательский центр «Пересвет», 2020. С. 72–79.
3. Сурма И. В. Цифровая дипломатия в мировой политике // Государственное управление. Электронный вестник, 2015. № 49. С. 220–249.
4. Бирюкова Д. Р. Космическая политика как один из механизмов обеспечения стратегических интересов России // Постсоветские исследования, 2018. № 7. С. 679–687.
5. Зайнуллина П. Р., Махнев В. А. Проблемы развития российско-китайского сотрудничества в авиакосмической отрасли // Теории и проблемы политических исследований, 2022, Том 11. № 4А. С. 222–230.
6. Зеленый Л. М. Научный руководитель Института космических исследований РАН: Луна – не место для прогулок // Интерфакс, 2024. URL: https://www.interfax.ru/interview/990557 (дата обращения 10.11.2024).
7. От «Беркута-ВР» до Российской орбитальной станции: перспективные разработки Роскосмоса в Китае // Роскосмос, 2024. URL: https://www.roscosmos.ru/41029/ (дата обращения 12.11.2024).

***Ivanova A.* FEATURES OF PR-PROMOTION OF RUSSIA'S SPACE POLICY AT THE PRESENT STAGE.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article examines the PR support of space policy as an important tool for shaping Russia's image on the global stage. The theoretical foundations of PR activities are analyzed, including strategic communication planning and reputation management, as well as their application in the context of the space industry. Special attention is paid to the significance of PR support for demonstrating Russia's technological leadership, attracting international partners and investments, popularizing space research, and countering negative information.

Key words: space policy, international relations, space research, geopolitics, PR support, technological leadership, «soft power».

УДК 329
ГРНТИ 11.15.51

ЭНВАЙРОНМЕНТАЛИЗМ В ПОЛИТИЧЕСКОЙ ЖИЗНИ СОВРЕМЕННОЙ АРГЕНТИНЫ

М. А. Килина, И. А. Цверианашвили
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена анализу положения и статуса такого социально-политического движения, как энвайронментализм. Несмотря на разнообразие политических идей и концепций, представленных в Аргентине в наши дни, энвайронментализм пользуется достаточно скромной поддержки среди населения страны. Тем не менее, многие представители молодого поколения страны разделяют многие принципы современного энвайронментализма.

Аргентина, зеленое движение, энвайронментализм, защита природы, проблемы окружающей среды

Появление экологических движений получило широкое распространение в Аргентине с начала XXI в. Существует ряд факторов, которые в совокупности способствовали развитию и распространению энвайронментализма. С одной стороны, в Аргентине происходила политизация экологической проблематики, возникшая в глобальном масштабе, в сочетании с реальностью политического, социального и экономического кризиса в стране, пик которого приходится на события декабря 2001 года [1]. К этому добавилась озабоченность определенных сообществ экологическими проблемами, которые касались их непосредственно. Деятельность, которую осуждает энвайронментализм, способна непосредственно повлиять на образ жизни населения, которое в большинстве своем не чувствовало призыва под знаменами прежнего экологизма и которое, тем не менее, собиралось продолжать борьбу.

Экологические движения в Аргентине относительно малочисленны по сравнению с другими странами мира. Как политические элиты, так и рядовые граждане страны разделяют укоренившуюся веру в развитие за счет интенсивной добычи и экспорта природных ресурсов. Аргентинские ученые и активисты называют это «экстрактивизмом», что означает реализацию проектов, наносящих социальный и экологический ущерб. Инакомыслящие часто подвергаются стигматизации или преследованиям.

В Аргентине действуют неправительственные организации и группы, в том числе Аргентинская ассоциация юристов-экологов (англ. Argentine

Association of Environmental Lawyers [2]), которая уже более двадцати лет представляет собой пространство для активизма, связанного с экологической и социальной справедливостью. Ассоциация поддерживает территориальные движения, пропагандистские акции, стратегические судебные процессы и коммуникационные стратегии, чтобы добиться социальной и экологической справедливости для всех людей и живых существ на территории Аргентины. Его основатели Энрике Виале вместе с исследователем и философом Маристеллой Свампа стали лидерами общественного мнения, создавая стратегии для национальных и региональных движений. Виале и Свампа являются авторами Южного экосоциального пакта (исп. Pacto Ecosocial del Sur [3]), проекта, аналогичного американскому «Зеленому новому курсу», который был разработан и адаптирован к условиям Латинской Америки. Еще одна организация, действующая в Аргентине – Союз гражданских собраний, которая организует фронтальное противодействие проектам по добыче полезных ископаемых. Еще одна организация – Аргентинский фонд дикой природы (исп. Fundación Vida Silvestre Argentina [4]) – с 1977 г. заключает соглашения с муниципалитетами по вопросам экологического планирования и регулирования, внедряет такие концепции, как биокоридоры, и реализует инициативы с участием различных слоев населения. Немаловажной организацией в Аргентине является американская Природоохранительная организация (англ. The Nature Conservancy [5]), которая с 2008 г. реализует инициативы, объединяющие различные природные решения для повышения эффективности производства за счет инноваций и внедрения технологий. Усилия данной организации были направлены на развитие знаний и расширение существующего опыта для содействия устойчивому развитию сельского хозяйства в Аргентине. Для достижения этой цели организация работает по трем направлениям: пресная вода, функциональные ландшафты и леса, и углерод. На данный момент организация занимается масштабным проектом по сохранению пастбищ Патагонии. С годами огромный выпас скота в регионе привел к разрушению и деградации естественной среды обитания; типичная овца может съедать до 2 килограмм растительности в день, что привело к дефициту растительности на юге Аргентины. Суровые зимы, сильные ветры, сухой климат и чрезмерный выпас скота на патагонских лугах способствовали развитию эрозии и опустынивания в Аргентине. В результате этих природных катаклизмов, а также неправильного выпаса скота многие виды фауны, зависящие от растительности и водных путей в экорегионе, оказались под угрозой исчезновения из-за загрязнения, вызванного стоком ила, и общей потери среды обитания [6].

В стране также действуют молодежные движения, такие как Молодежь за климат (исп. Jóvenes por el Clima [7]), основанное в 2019 г. В его проекты вхо-

дит создание школы педагогов-экологов и развитие подразделений организации, которые занимаются политическими исследованиями в области изменения климата и окружающей среды. За последние пять лет усилия данной организации привели к участию 100 000 человек в климатических демонстрациях по всей Аргентине и принятию ключевых законов, включая закон об изменении климата и закон об экологическом образовании. Кроме этого, в стране существуют общины коренного населения, защищающие жизнь на своих территориях, и многие другие коалиции с участием университетских работников, левых партий и профсоюзов. На данный момент представители аргентинского энвайронментализма как никогда ранее стремятся объединиться в попытках отстоять свои интересы.

Президент Аргентины Хавьер Милей, вступивший в должность в декабре 2023 г. и получивший известность благодаря своим агрессивным и экстремистским заявлениям в качестве участника телевизионных дискуссий, сумел направить в нужное русло желание перемен миллионов людей, недовольных политическим истеблишментом и значительным экономическим кризисом [8].

Во время своей предвыборной кампании нынешний президент неоднократно заявлял, что защита окружающей среды – это ненужное ограничение свободы бизнеса. Он также заявил, что не верит в то, что изменение климата вызвано деятельностью человека, и отверг эту идею как социалистическое изобретение [8]. После своего избрания Милей выдвинул «исправленный» пакет законов, которые, в частности, значительно сократят защиту ледников и лесов, а также приведут к дальнейшему дерегулированию горнодобывающей промышленности. Законопроект предусматривает, в частности, наделение правительств провинций правом разрешать вырубку лесов в районах, где она в настоящее время запрещена, при одновременном сокращении бюджета на борьбу с незаконной вырубкой лесов и лесными пожарами. Это вступает в явное противоречие с положениями закона о защите лесов, принятого в 2007 году после продолжительных обсуждений. В настоящее время, по официальным данным, общая площадь естественных лесов Аргентины составляет 53 184 501 га. По оценкам глобальной неправительственной организации Greenpeace [9], в случае принятия законопроекта в исходном виде, около 42 млн га, или 80 % естественных лесов Аргентины, находящихся сегодня под охраной, будут открыты для вырубок, что негативно повлияет на биоразнообразие, а также вызовет проблемы в социальной и культурной сферах. Предлагаемые реформы также сократят ресурсы, выделяемые Национальному фонду охраны и обогащения коренных лесов, который получает деньги от экспорта сельскохозяйственной и лесной продукции. Это лишило бы средств, зарезервированных для мониторинга лесов, что, в свою очередь, может нанести вред

экспорту, поскольку борьба с вырубкой лесов стала требованием для бизнеса на многих рынках мира.

Кроме того, указом (в настоящее время оспариваемым) был отменен закон, ограничивающий типы и объемы земель, которые могут быть приобретены иностранными компаниями. Это открывает возможности для беспорядочной покупки стратегических пограничных территорий, водных путей и других природных ресурсов.

Хавьер Милей также распустил созданное в 1991 году Министерство окружающей среды и устойчивого развития (исп. Ministerio de Ambiente y Desarrollo Sostenible), которое курировало политику правительства в области охраны окружающей среды и содействовало устойчивому развитию. В настоящее время с 10 декабря 2023 года является государственным секретариатом, зависимым от Министерства внутренних дел и отвечает за продвижение, распространение и развитие деятельности в своей области, интеграцию с различными государственными организациями, а также соблюдение права на здоровую окружающую среду, гарантированного Конституцией Аргентины.

На этой почве аргентинские активисты интенсивно принимают участие в протестах против планов президента. Например, в марте 2024 года экологи выступили против того, что новый президент пытается ослабить ограничения на добычу полезных ископаемых вблизи ледников и отменить лесозащитные меры [10].

Кроме этого, аргентинский президент не стал отмалчиваться и после происшествия, связанное с футболистом Лионелем Месси. 6 августа 2024 года активисты испанской экологической организации Будущее Растений (исп. Futuro Vegetal), которые называет себя «коллективом гражданского неповиновения и ненасильственного прямого действия» и борются с климатическим кризисом [11], облили черной и красной краской особняк аргентинского футболиста Лионеля Месси на острове Ибица из-за того, что футболист, якобы, купил этот дом нелегально. Один из активистов развернул плакат с надписью: «Спасите планету. Ешьте богатых. Упраздните полицию» [12]. Действия экоактивистов по отношению к аргентинскому футболисту осудил президент Хавьер Милей и выступил с речью, где назвал их трусами и коммунистами и попросил власти Испании обеспечить безопасность для его сограждан.

Таким образом, энвайронментализм в Аргентине не пользуется успехом и остается маргинальным на политической арене. Тем не менее, в последние годы наблюдается рост интереса к экологическим вопросам, особенно среди молодежи и в крупных городах.

Список используемых источников

1. Кортес-Конде Р. Экономический кризис в Аргентине: причины и последствия // Экономическая история. Обозрение / Под ред. Л.И.Бородкина. Вып. 10. М., 2005. С.180–182.
2. Argentine Association of Environmental Lawyers. URL: https://argentinelawyers.org/ (дата обращения 04.10.2024)
3. Pacto Ecosocial del Sur. URL: https://pactoecosocialdelsur.com/ (дата обращения 04.10.2024) Fundación Vida Silvestre Argentina. URL: https://www.vidasilvestre.org.ar/ (дата обращения 04.10.2024).
4. The Nature Conservancy. URL: https://www.nature.org/en-us/about-us/where-we-work/latin-america/argentina/ (дата обращения 04.10.2024).
5. Preserving Patagonian Grasslands and Gauchos. URL: https://www.perc.org/2010/03/01/preserving-patagonian-grasslands-and-gauchos/ (дата обращения 06.10.2024).
6. Jóvenes por el Clima. URL: https://jovenesporelclima.org.ar/ (06.10.2024).
7. How Argentina's protesters are responding to a new president who wants to end environmental protections and sell off natural resources. URL: https://theconversation.com/how-argentinas-protesters-are-responding-to-a-new-president-who-wants-to-end-environmental-protections-and-sell-off-natural-resources-222200 (дата обращения 12.10.2024).
8. Greenpeace. URL: https://www.greenpeace.org/international/ (дата обращения 04.10.2024).
9. Экологи Аргентины протестуют против роста горнодобычи в стране. URL:https://www.prometall.info/eco/mirovaya-pracktika/ekologi_argentiny_protestuyut_protiv_rosta_gornodobychi_v_strane (дата обращения 12.10.2024).
10. Futuro Vegetal. URL: https://futurovegetal.org/ (дата обращения 12.10.2024).
11. Президент Аргентины об атаке экоактивистов на виллу Месси. URL: https://www.sports.ru/football/1116294752-prezident-argentiny-milej-ob-atake-ekoaktivistov-na-villu-messi-v-ispa.html (дата обращения 12.10.2024).

Kilina M., Tsverianashvili I. **ENVIRONMENTALISM IN THE POLITICAL LIFE OF MODERN ARGENTINA.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article is devoted to the analysis of the position and status of such a socio-political movement as environmentalism. Despite the diversity of political ideas and concepts presented in Argentina today, environmentalism enjoys rather modest support among the population of the country. Nevertheless, many members of the country's younger generation share many of the principles of contemporary environmentalism.

Key words: Argentina, green movement, environmentalism, environmental protection, environmental issues.

УДК 330.354
ГРНТИ 06.52.13

МИГРАНТЫ КАК ДВИЖУЩАЯ СИЛА ТЕХНОЛОГИЧЕСКОГО ПРОГРЕССА И ЭКОНОМИЧЕСКОГО РОСТА США

Е. Н. Климентьев, Д. А. Патрушева
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Миграция играет ключевую роль в экономическом развитии и технологическом прогрессе Соединенных Штатов Америки. На протяжении всей своей истории США привлекали мигрантов, что способствовало формированию многообразного общества и динамичной экономики. В настоящее время иммигранты составляют значительную часть рабочей силы страны, занимая около 17,6 % всех рабочих мест. Они не только заполняют вакансии в низкоквалифицированных секторах, но и вносят значительный вклад в высокотехнологичные отрасли, где их доля среди работников науки и инженерии достигает около трети процента [1].

мигранты, экономический рост, технологический прогресс, Кремниевая долина

Миграция продолжает обогащать страны богатством идей и навыков, стимулируя инновации и предпринимательство. Исследования показывают, что более половины стартапов с миллиардными оборотами были основаны иммигрантами, что подчеркивает их важнейшую роль в развитии технологических и бизнес-преобразований.

Кремниевая долина, или Силиконовая долина, является примером этого явления. Будучи глобальным центром инноваций, она во многом обязана своим динамизмом иммигрантам, которые привносят в нее разнообразный опыт и творческие способности. Благодаря этому вкладу появились революционные технологии и родились ведущие компании.

В 2023 году США столкнулись с рекордными уровнями миграции, что сформировало их социальный и экономический ландшафт. Министерство внутренней безопасности сообщило, что только в декабре границу США пересекли 225 000 мигрантов, и в том году было выдано более 1,17 миллиона новых грин-карт, а это, в свою очередь, самый высокий показатель за последние семь лет [2].

Администрация президента Байдена стремилась упорядочить иммиграцию с помощью таких программ, как восстановление инициатив для граждан Кубы, Гаити, Никарагуа и Венесуэлы, что позволило до 30 000 мигрантов ежемесячно въезжать в страну на законных основаниях. Однако проблемы сохра-

няются, включая борьбу с несанкционированным пересечением границы и нехватку ресурсов у пограничных служб. Администрация подверглась критике несмотря на то, что в 2023 году экономика США выросла на 2,5 %, превысив показатель предыдущего года в 1,9 % [3].

Мигранты оказывают значительное влияние на развитие технологического прогресса и экономического потенциала США, особенно в высокотехнологичных отраслях. В 2023 году мигранты составляют около 17,6 % рабочей силы страны, и их роль в научно-исследовательской и инженерной деятельности становится все более заметной. Примерно треть процента работников в сфере НИОКР (научных исследований и опытно-конструкторских разработок) составляют иностранцы [1].

Одним из наиболее заметных аспектов влияния мигрантов является их роль в создании стартапов. Более половины стартапов с оценкой более одного миллиарда долларов имеют хотя бы одного основателя-мигранта. Примеры таких компаний включают Google, основанный Сергеем Бриным, родившимся в России, и Tesla, где одним из ключевых фигур является Илон Маск, родившийся в Южной Африке.

Высококвалифицированные иммигранты играют важнейшую роль в таких отраслях, как IT, машиностроение и STEM (наука, технологии, инженерия и математика). Бюро статистики труда отмечает, что 17 % обладателей докторских степеней в американской рабочей силе - иммигранты, которые заполняют критические пробелы и стимулируют научные исследования и разработки. Разнообразие культурных и образовательных традиций приводит к появлению уникальных идей, способствуя созданию более инновационных и конкурентоспособных команд на мировой арене. Исследования подтверждают, что разнородные команды принимают лучшие решения и быстро адаптируются к изменениям.

С точки зрения экономического влияния миграция также положительно сказывается на экономике страны. Приток мигрантов может привести к увеличению ВВП на триллионы долларов. Иммигранты создают новые компании и способствуют росту существующих бизнесов за счет увеличения потребительского спроса.

Что касается расового состава мигрантов, то на сегодняшний день выходцы из Азии составляют крупнейшую группу среди мигрантов в высокотехнологичных секторах. По данным Pew Research Center, азиаты составляют около 60 % иностранных работников в области науки и технологий. Наиболее представленные страны – это Индия и Китай, которые обеспечивают значительное количество специалистов по STEM. В то же время миграция из Ла-

тинской Америки по-прежнему значительна, хотя она постепенно снижается по сравнению с иммиграцией из Азии.

В нынешнем 2024 году Кремниевая долина все также остается ведущим центром технологических инноваций и стартапов, которому не так сильно и чувствительно мешают изменения в иммиграционной политике и фон экономических проблем. Находясь в центре глобальных потрясений и стремительной технологической эволюции регион продолжает демонстрировать необычную устойчивость и способность адаптироваться к меняющимся условиям.

В 2024 году наблюдается увеличение интереса к стартапам, основанным мигрантами, что подтверждается участием 24 стартапов из Центральной Азии на конференции TechCrunch Disrupt, что стало значимым для продвижения инновационных идей и привлечения венчурных инвестиций [4].

Много идет речей о тесном сотрудничестве между местными инкубаторами и международными стартапами в Кремниевой долине. Например, инновационный центр Silkroad Innovation Hub стал ключевым центром притяжения для основателей из Центральной Азии, привлек более 30 миллионов долларов венчурного капитала и провел более 200 мероприятий с участием более 10 000 человек, что уже таким небольшим примером нельзя не говорить о вкладывании иммигрантами не только в разнообразие экосистемы Кремниевой долины, но и в создание рабочих мест и инновационных решений [4].

Несмотря на отток населения в предыдущие годы, который был вызван пандемией и изменениями в иммиграционной политике, Кремниевая долина продолжает демонстрировать экономический рост. В 2023 году уровень безработицы в регионе оставался на рекордно низком уровне – 2,9 %, а объем венчурного финансирования достиг беспрецедентных $95 миллиардов. Такие цифры говорят сами за себя – технологический сектор остается прочным и привлекательным для инвесторов [5].

Тем не менее, Кремниевая долина сталкивается с рядом проблем. Сокращение числа новых иммигрантов из-за ужесточения миграционной политики создает определенные трудности для высокотехнологичных компаний, которые зависят от иностранных специалистов. В 2021 году количество мигрантов из-за рубежа составило всего 2,9 тысячи человек – на 64 % меньше по сравнению с предыдущим годом [6].

Технологический сектор может столкнуться с неопределенностью из-за потенциального повышения пошлин и изменений в иммиграционной политике в 2024 и последующих годах. Некоторые эксперты считают, что Трамп будет сосредоточен на внутренней политике и может ограничить приток высококвалифицированных мигрантов, что негативно скажется на инновациях и развитии технологий. Однако, инвестиции в искусственный интеллект и дру-

гие передовые технологии могут продолжать оставаться основным двигателем роста в этом секторе, независимо от политической ситуации.

Список используемых источников

1. Иммиграция в США: ее роль в экономике и иммиграционная политика американского правительства // Cyberleninka. URL: https://cyberleninka.ru/article/n/immigratsiya-v-ssha-ee-rol-v-ekonomike-i-immigratsionnaya-politika-amerikanskogo-pravitelstva (дата обращения 02.11.2024).
2. Рекордное количество мигрантов прибыли в США в 2023 году // Новые Известия. URL: https://newizv.ru/news/2023-12-31/rekordnoe-kolichestvo-migrantov-pribyli-v-ssha-v-2023-godu-425771 (дата обращения 02.11.2024).
3. Догнать Америку: почему экономическая модель ЕС проигрывает конкурентам // Forbes. URL: https://www.forbes.ru/mneniya/511972-dognat-ameriku-pocemu-ekonomiceskaa-model-es-proigryvaet-konkurentam (дата обращения 02.11.2024).
4. Silkroad Innovation Hub представил 24 стартапа из Центральной Евразии на TechCrunch Disrupt 2024 // Astana hub. URL: https://astanahub.com/ru/article/silkroad-innovation-hub-predstavil-24-startapa-iz-tsentralnoi-evrazii-na-techcrunch-disrupt-2024 (дата обращения 07.11.2024).
5. Население Кремниевой долины сократилось впервые после 17 лет роста // Интерфакс. URL: https://www.interfax.ru/world/823002 (дата обращения 07.11.2024).
6. Кремниевая долина пережила крупнейший отток населения, но стала богаче // Секрет Фирмы. URL: https://secretmag.ru/news/kremnievaya-dolina-perezhila-krupneishii-ottok-naseleniya-no-stala-bogache-19-02-2022.htm (дата обращения 07.11.2024).

Klimentiev E., Patrusheva D. **MIGRANTS AS A DRIVER OF TECHNOLOGICAL PROGRESS AND ECONOMIC GROWTH IN U. S.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Migration plays a key role in the economic development and technological progress of the United States of America. Throughout its history, the United States has attracted migrants, which has contributed to a diverse society and dynamic economy. Currently, immigrants make up a significant portion of the country's labour force, occupying about 17.6 % of all jobs. They not only fill vacancies in low-skilled sectors, but also make a significant contribution to high-tech industries, where their share among science and engineering workers reaches about one-third of % [1].

Key words: migrants, economic growth, technological progress, Silicon Valley.

УДК 327
ГРНТИ 11.25.91

ЭВОЛЮЦИЯ ВНЕШНЕЙ ПОЛИТИКИ КАНАДЫ В АРКТИЧЕСКОМ РЕГИОНЕ ПРИ ДЖАСТИНЕ ТРЮДО

А. В. Неровный, И. Р. Яцышин
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье проводится анализ эволюции внешней политики Канады в Арктике в период премьерства Джастина Трюдо с акцентом на 2016-2023 годы. Авторы выделяют усилия Канады по обозначению границ, увеличению военного присутствия, развитию научного сотрудничества и поддержке проектов в Арктическом совете. Исследование не только указывает на амбиции Канады в Арктическом регионе, но также раскрывает сложности, связанные с присутствием и влиянием России в регионе.

внешняя политика Канады, Арктика, Джастин Трюдо, сотрудничество, окружающая среда, коренные народы, Глобальная арктическая инициатива лидерства

В период с 2016 по 2017 год внимание властей Канады было направлено на решение широкого спектра задач в Арктическом регионе (как на территории страны, так и за ее пределами). В ходе процесса согласования совместных форм активности властями были инициированы переговоры на разном уровне со множеством со множеством государств. Значительные усилия были направлены на установление конструктивного диалога с Российской Федерацией. Кроме экономических и социальных инициатив в вышеупомянутом регионе Канада выделяет в качестве приоритетного направления национальную безопасность. Кроме того, важную роль играют вопросы экологической безопасности Арктики. В 2017 году именно на базе данного региона канадцам удалось пролоббировать свою инициативу по защите окружающей среды, которая стала традиционной в политике премьер-министра Джастина Трюдо. Еще одним столпом политического курса Трюдо стала всесторонняя поддержка коренного населения арктических провинций страны. По итогу данные усилия привели к подписанию документа, в котором все страны Арктического региона подтверждают важность Парижского соглашения по климату, а также соглашаются с необходимостью принятия мер по улучшении экологической обстановки в регионе. Также со странами Арктического региона и Канадой был заключен договор об сближении в рамках научного сотрудничества [1]. Помимо всего прочего значимость арктического вектора в вышеуказанный период (2016-2017 гг.) подчеркивается и другими формами активности:

обозначением (уточнением) государственных границ, согласованием договора о рыболовстве, а также попыткой увеличения собственного военного присутствие в регионе.

В период с 2018 по 2019 год Канада немного снизила темпы освоения и развития данного региона, но амбиций в вопросе лоббирования своих национальных интересов по сути никуда не делись [2]. На государственном уровне неоднократно поднимался вопрос в части обновления политики страны в северном измерении. На совещаниях по делам региона власти упорно продвигали ряд приоритетных инициатив. В этот список входили: добыча минеральных и энергетических ресурсов, атмосферные загрязнения, вопросы судоходства и забота о коренных народов в части их морально-психологического состояния [3–5].

Следует отметить, что до 2018 года Канада позиционировала себя в системе международных отношений в качестве лидера в Арктическом регионе. К подобной трактовке своего места на мировой политической арене власти снова вернутся в период 2021-2022 гг. Такое поведение было связано с внушительными инвестициями из бюджета страны и непомерными ожиданиями в научно-исследовательской области, которые возлагали находящиеся у власти политики. Тем не менее, присутствие в регионе такого соперника, как Российская Федерация, вряд ли давало (и дает) Канаде возможность считать себя лидирующим игроком. Вдвойне иронично, что «главный партнер» Канады в лице США не только поддерживает данную мысль, но и прямо признает первенство со стороны России в ряде вопросов [6].

В период с 2019 по 2020 год в арктической политике Канады наблюдался значительный эволюционный сдвиг. Канадой на официальном уровне были обозначены границы региона, рамочный документ получил название «Основы политики в отношении Арктики и Севера» (англ. The Arctic and Northern Policy Framework). Канада, уже очевидно видя конкурентов более серьезно взялась за Арктику. Документ должен был позволить решить некоторые из возникших проблем: обеспечить спокойствие и порядок в Арктическом регионе, всесторонне защищать коренные народы и т. д. В нем подчеркивалось продвинутое сотрудничество с другими государствами, которые присутствуют в северном полушарии. Кроме этого, хоть и с некоторым опозданием, до Арктики дошла еще одна визитная карточка политики прогрессивного премьер-министра – активное продвижение гендерного равенства. С учетом специфики и положения дел в регионе, инициативы и сам подход в целом можно признать как действительно эволюционные. Канада начинает активно привлекать посольства других стран, с целью интенсификации совместных действий и пропаганды собственных интересов в Арктике [7]. Также Канаде хотелось занять лидирующее

место в какой-то конкретной области деятельности. Не удивительно, что именно при Джастине Трюдо ей стала экология [8]. Существенными победами Канада отличилась в деле утверждения суверенитета в регионе, в переговорах по поводу статуса Гренландии, в деле организации значительного числа научных экспедиций и исследовательских миссий. Именно в период с 2019 по 2020 год Канада закончила десятилетние работы по оформлению претензий на континентальный шельф и подала соответствующую заявку в ООН [9–10].

В период с 2020 по 2021 год Канада сохранила темпы развития и действовала в соответствии с уже принятыми документами. Основные направления работы изменились незначительно прошлого периода. Кроме того, политические элиты страны смирились с тем, что с присутствием России в регионе придется считаться, и разработали «Инициативу глобального лидерства в Арктике» (англ. Global Arctic Leadership Initiative, GALI), что позволило соединить вместе все выдвигаемые инициативы. На осуществление задуманного было выделено дополнительное финансирование, в размере, примерно, 30 млн. долл. Эти средства будут выделяться до 2025 года. Каждый новый транш планируется делать больше предыдущего. Это говорит о том, что политика Канады в Арктическом регионе только эволюционирует и набирает обороты [11].

В период с 2021 по 2022 год Канада планировала придерживаться обозначенных ранее целей. Были осуществлены инвестиции в размере 4 млн. долл. для развития пропаганды и укрепления безопасности национальных интересов в регионе. Также был организован постоянный секретариат рабочей группы Арктического совета. Канада в очередной раз заявила о своей приверженности независимости Арктического региона. При этом никак не комментируя свое же возрастающее с каждым годом внимание к делам в регионе. Также заметно возросло внимание к претензиям на континентальный шельф. Формировался ответ на пересмотренную заявку своего главного конкурента в регионе – России по данному вопросу [12–13].

В период с 2022 по 2023 год Канада, посредством Инициативу глобального лидерства в Арктике, усилила свое влияние в регионе еще больше. Было выделено 6,4 млн. долл. на поддержку инициатив, направленных на укрепление ценностей и интересов Канады в Арктическом совете, лоббирование проектов по биоразнообразию, защите морской среды, готовности к чрезвычайным ситуациям и поддержке коренных народов. Канада также углубила сотрудничество с арктическими союзниками, особенно США [14].

Эволюция внешней политики Канады в арктическом измерении заметна гораздо лучше, чем в большинстве других направлений. Это связано с желанием государства быть страной-лидером в данном регионе и подтверждается

повышенными финансовыми вливаниями, а также активизацией научно-исследовательской работы в довольно значительных объемах. Политика Канады в Арктическом регионе эволюционировала и приобрела два новых, но неизменных для премьер-министра Трюдо направления: экология и гендерное равенство. Также интенсификацию развития и желание доминировать в регионе подкрепляет эскалация военного присутствия в нем Канады. Стоит отметить и длящиеся десятилетие работы по созданию документа поднимающего вопросы континентального шельфа и претензий на него, что является одним из самых важных текущих аспектов политики Канады в Арктическом регионе и символизирует пиковый интерес последней к нему. Внимания достойна и «Инициатива глобального лидерства в Арктике», созданная Канадой для упорядочения и комплектации инициатив, а также перспектив относительно региона, на которую также было выделено дополнительное финансирование до 2025 года, что уже открыто говорит о значимости роли Арктического региона для Канады при Джастине Трюдо.

Список используемых источников

1. Departmental Results Report 2016-17 // Government of Canada website. URL: https://www.international.gc.ca/gac-amc/publications/plans/drr-rrm/drr-rrm_1617.aspx?lang =eng#a12 (дата обращения 11.11.2024).
2. Косова А. Ю. Арктическая стратегия канадского премьер-министра Джастина Трюдо: особенности и перспективы развития // Россия в глобальном мире, 2017. № 10 (33). С. 144–151.
3. Казанин А. Г. Арктическая политика США и Канады и ее нефтегазовый аспект // Вопросы управления, 2019. № 3 (39). С. 51–54.
4. Departmental Results Report 2017–18 // Government of Canada website. URL: https://www.international.gc.ca/gac-amc/publications/plans/drr-rrm/drr-rrm_1718.aspx?lang= eng#a5_1 (дата обращения 08.11.2024).
5. Departmental Results Report 2018–19 // Government of Canada website. URL: https://www.international.gc.ca/gac-amc/publications/plans/drr-rrm/drr-rrm_1819.aspx?lang=eng#a3_1 (дата обращения 01.11.2024).
6. Rosen K. R. A Battle for the Arctic Is Underway. And the U.S. Is Already Behind. Climate change is opening the Arctic. Can the U.S. and NATO surpass Russian capabilities and ambitions in a new Cold War? // Politico. 17.12.2022. URL: https://www.politico.com/news/ magazine/2022/12/17/climate-change-arctic-00071169 (дата обращения 10.11.2024).
7. Аксютина А. В. Механизмы международного сотрудничества Канады в Арктике // Новые импульсы развития: вопросы научных исследований. Сб. статей Международной научно-практической конференции, 2020. Т. 1. С. 137–140.
8. Дзюбан В. В. Арктическая политика Канады в XXI веке // Электронный научный журнал «Архонт». 2020. № 1 (16). С. 9–12.
9. Quinn E. Canada extends continental shelf claim, increasing overlaps with Russia in Arctic // The Barents Observer. 23.12.2022. URL: https://www.thebarentsobserver.com/arctic/canada-ex-

tends-continental-shelf-claim-increasing -overlaps-with-russia-in-arctic/118511 (дата обращения 10.11.2024).
10. Departmental Results Report 2019–20 // Government of Canada website. URL: https://www.canada.ca/en/public-service-commission/services/ publications/departmental-results-report-2019-2020/full-report.html (дата обращения 01.11.2024).
11. Departmental Results Report 2020–21 // Government of Canada website. URL: https://www.international.gc.ca/transparency-transparence/ departmental-results-reports-rapport-resultats-ministeriels/2020-2021.aspx?lang=eng#a3_1 (дата обращения 11.11.2024).
12. Departmental Results Report 2021–22 // Government of Canada website. URL: https://www.international.gc.ca/transparency-transparence/ departmental-results-reports-rapport-resultats-ministeriels/2021-2022.aspx?lang=eng#a3_1 (дата обращения 11.11.2024).
13. Магомедова О. С. Сравнительный анализ арктической международно-правовой политики Канады и США // Право. Журнал Высшей школы экономики, 2023. Т. 16. № 1. С. 229–246.
14. Departmental Results Report 2022–23 // Government of Canada website. URL: https://www.canada.ca/en/shared-services/corporate/publications/2022-23/departmental-results-report-2022-23.html (дата обращения 08.11.2024).

Nerovnyi A., Yatsyshin I. **THE EVOLUTION OF CANADA'S ARCTIC FOREIGN POLICY UNDER JUSTIN TRUDEAU.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article examines the evolution of Canada's Arctic foreign policy during the premiership of Justin Trudeau, focusing on 2016-2023. The authors highlight Canada's efforts to define its borders, increase its military presence, develop scientific cooperation, and support projects in the Arctic Council. The study not only highlights Canada's ambitions in the Arctic region, but also reveals the complexities associated with Russia's presence and influence in the region.

Key words: foreign relations of Canada, the Arctic, Justin Trudeau, cooperation, environment, indigenous peoples, Global Arctic Leadership Initiative.

УДК 327
ГРНТИ 10.87.31

ЕВРОАТЛАНТИЧЕСКАЯ ИНТЕГРАЦИЯ ГРУЗИИ: СОДЕРЖАНИЕ, ДИНАМИКА И ПЕРСПЕКТИВЫ

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

В данной работе исследуется евроатлантическое направление в внешней политики Грузии во многом через диахронический анализ. С помощью данного метода, исследование опирается на временные изменения, т.е. разделение данного процесса на определенные этапы. При написании работы, были выделены сопутствующие преграды (внешние и внутренние), с которыми сталкивается Грузия на выбранном евроатлантическом курсе. В заключении были сформированы соответствующие перспективы вступления Грузии в НАТО в результате проведенного анализа и с быстро развивающиеся глобализации в мире.

Евроатлантическая интеграция, НАТО, геополитика, безопасность, внешнеполитический курс, региональная безопасность, военно-политическое сотрудничество

В 1991 году Грузия стала самостоятельным государством. Но, между тем, в достаточно затруднительном положении как в экономическом, так и территориальном плане. Во многом данные процессы послужили формированию имеющегося на сегодняшней день евроатлантического курса в стране. Главные политики страны в начале 90-годов не раз заявили о том, что интеграция в Европу должна стать приоритетом для страны на дальнейшие годы [1].

Начало отношений Грузии с НАТО отчитывается с 1992 года, в котором Грузия присоединилась к Совету североатлантического сотрудничества, позднее Совет евроатлантического партнерства – СЕАП [2]. Позже в 1994 году, Грузия присоединилась к программе «Партнерство ради мира» (ПРМ). В 1999 году Грузия присоединилась к «Процессу планирования и анализа» (ППА), который является обязательным условием для возможного предоставления плана действий по членству в НАТО (ПДЧ) в будущем. Одним из важнейших моментов в отношениях между НАТО и Грузией стал 2002 и 2003 годы, поскольку Грузия официально заявила о своих евроатлантических устремлениях на саммите в Праге в 2002 году. В 2003 году пришедшее после «революции роз» новое правительство декларировало приверженность широкомасштабным преобразованиям в ключевых сферах жизни общества.

Приверженность идее присоединения к НАТО в Грузии менялась в зависимости от внешней и внутренней политической обстановки, и первые заявления о планировании вступления в Альянс были официально озвучены в 2002 году президентом Грузии Эдуардом Шеварднадзе на саммите НАТО в Праге [3]. В декабре того же года было подписано соглашение между правительством Грузии и США о сотрудничестве в военной сфере и в марте документ был ратифицирован грузинским парламентом. В мае 2003 года Совет национальной безопасности Грузии определил приоритетные направления программы индивидуального сотрудничества с НАТО, а Эдуард Шеварднадзе подписал распоряжение о создании правительственной комиссии по интеграции Грузии в НАТО. Первый конкретный шаг в направлении присоединения к НАТО был сделан в 2004 году, когда Грузия подписала Дорожную карту НАТО-Грузия. В рамках этого документа, Грузия обязалась провести широкомасштабные реформы в сфере обороны и безопасности, которые должны были сделать ее готовой к присоединению к альянсу. Саммит НАТО в Бухаресте в 2008 году закрепил в общественно-политическом обсуждении тему вступления Грузии в альянс.

Государства Южного Кавказа были включены на повестку различных саммитов НАТО в качестве приглашенных гостей или участников партнерства. Например, на саммите НАТО в Бухаресте в 2008 году, лидеры Армении, Азербайджана и Грузии были приглашены для участия в заседании Комиссии НАТО-Грузия. На саммите в Варшаве в 2016 году, принимавшем решение о создании Бригады высокой готовности на восточном фланге НАТО, Грузия была упомянута в контексте региональной безопасности, отмечалось и то, что партнерство с государствами Южного Кавказа остается важным для обеспечения безопасности и стабильности в регионе. В коммюнике саммита НАТО в июне 2004 года в Стамбуле было заявлено об «особом внимании в взаимодействии с партнерами на Южном Кавказе» и о «поддержании решения Грузии и Азербайджана разработать индивидуальный план партнерства с НАТО, что представляет собой важный шаг по усилию этих стран более тесного партнерского отношения с альянсом». В декларации следующего саммита НАТО, который состоялся в ноябре 2006 года в Риге, Южный Кавказ, а точнее одна из государств данного региона – Грузия, упоминается в одном абзаце, где сказано о том, что с Грузией будет вестись «интенсивный диалог», следовательно, членство прямо не упоминалось, но приветствовался вклад Грузии в международные операции по поддержанию мира и безопасности [4].

Причина интереса и стремления альянса по укреплению связей и установление общих интересов безопасности и стабильности в Грузии является ее выгодное географическое расположение и, благодаря которому возможно ис-

пользование Грузии в качестве транзитной территории для транспортировки нефти и газа из Каспийского бассейна, через который проходят два основных нефтепровода: один к Черному морю, а второй через Турцию к Средиземному морю. Так, трубопровод Баку-Тбилиси-Джейхан (БТД), является одним из этапов экспортного маршрута в Европейский Союз, известного как Южный коридор [5]. Так, в совместной статье Бондаря Н. А., Гехта А. Б., Ивлева Д. С., Потапенко Т. Г. и Цыгоняева А. Ю. на тему отмечается, что «Экономическое значение региона Южного Кавказа определяется тем, что его восточная часть богата углеводородными ресурсами, к разработке которых прямой доступ имеют американские и европейские энергетические корпорации» [6].

Грузия продолжает двигаться к присоединению к Альянсу и взаимодействует с ним в рамках Плана действий по членству в НАТО (MAP), но присоединение к НАТО остается непростым вопросом, так как оно может стать поводом для конфронтации с Россией, которая является соседом Грузии и имеет территориальные претензии к ней. Грузия внесла большой вклад в международные миссии НАТО, даже больше, чем у многих существующих членов, и в то же время соответствует цели Альянса по расходам на оборону в размере 2 %. Грузия была крупнейшим донором на душу населения в рамках миссии НАТО «Решительная поддержка» в Афганистане. Благодаря обороноспособности и оперативной совместимости с армиями членов НАТО его военные стандарты соответствуют стандартам НАТО. Кроме того, присоединение к НАТО требует выполнения определенных критериев, таких как экономическая и политическая стабильность, демократические реформы и военные реформы [7]. Грузия сделала значительные успехи в этих областях, однако, все еще существуют нерешенные проблемы, такие как региональные конфликты и коррупция внутри страны. Но все же вместе с этим, НАТО активно поддерживает Грузию в ее усилиях по выполнению критериев для присоединения к альянсу, в частности, оказывая помощь Грузии в проведении реформ в военной сфере и улучшении безопасности на своей территории [8].

В 2020 году инициативы в пакете сотрудничества НАТО-Грузия охватил множество сфер – от воздушной до киберпространства, в которых включались дополнительные мероприятия по проведению регулярных совместных учений НАТО-Грузия. На саммите в 2022 году, проходившем с 29 по 30 июня в Мадриде – были одобрены ряд индивидуальных мер поддержки официального Тбилиси, что в очередной раз выделило Грузию как одного из важных партнеров, находящегося в зоне стратегического интереса НАТО [9].

Последний проводимый опрос среди населения Грузии о НАТО 2 февраля 2023 года был организован Национальным демократическим институтом (NDI), в котором было показано, что поддержка ЕС достигла цифры 81 %, а

73 % грузин продолжают поддерживать членство в НАТО, по сравнению с 69 % в предыдущем опросе 2022 года. Только 30 % респондентов считают, что правительство Грузии делает все возможное для обеспечения членства Грузии в ЕС и НАТО, 56 % считают, что правительство Грузии делает недостаточно и ничего для этого не делает, а 14 % не знают или отказываются отвечать [10]. Возможность присоединения к альянсу может стать фактором мобилизации общества и укрепления доверия к государственным институтам. Также есть и те, кто против идеи присоединения страны к НАТО, которые опасаются возможных негативных последствий, таких как усиление напряженности с Россией или потеря ресурсов на участие в международных военных операциях [11, 12]. В 2022 году, Грузия получила новый политический импульс в направлении присоединения к НАТО, когда на саммите НАТО в Мадриде было снова подтверждено, что Грузия, имеет перспективы на присоединение к альянсу.

Оценивая перспективы вступления Грузии в НАТО на сегодняшний день, можно сказать, что среднесрочной перспективе статус- кандидата и предоставление плана действий по членству в НАТО страна не получит. В первую очередь в свете внутренней расшатанности и нестабильности страны и неразрешенности территориальных вопросов.

Список используемых источников

1. Georgia and the world: a vision and strategy for the future. Foreign Policy Concept of Georgia. URL http://www.bits-berlin.de/NRANEU/Russia-Caucasus/georgiaforeignpolicy.pd
2. Министерство иностранных дел Грузии. URL: http://www.mfa.gov.ge (дата обращения 22.09.2024).
3. Statement by President of Georgia Eduard Shevardnadze at the EAPC Summit. Prague 22 Nov. 2002. URL: https://www.nato.int/docu/speech/2002/s021122h.htm (дата обращения 04.04.023).
4. Коммюнике Стамбульского саммита 2004 г. URL: https://www.nato.int/cps/en/natohq/official_texts_21023.htm?selectedLocale=ru (дата обращения 02.04.23).
5. По Баку-Тбилиси-Джейхан на мировые рынки транспортировано 4,4 миллиарда баррелей нефти. URL: https://azertag.az/ru/xeber/po_baku_tbilisi_dzheihan_na_mirovye_rynki_transportirovano_44_milliarda_barrelei_nefti-3262040 (дата обращения 12.10.2024).
6. Бондарь Н. А., Гехт А. Б., Ивлев Д. С., Потапенко Т. Г., Цыгоняева А. Ю. Политика ЕС и США в отношении Грузии: краткая характеристика // Вопросы национальных и федеративных отношений, 2023. Т. 13. № 2 (95). С. 678-690.
7. Центр НАТО в Грузии. URL: http://www.natoinfo.ge (дата обращения 07.09.2024)
8. Асимметрия мировой системы суверенитета: зоны проблемной государственности / Под ред. М. В. Ильиной, И. В. Кудряшовой. М.: МГИМО Университет, 2011. 248 с.
9. Public Attitudes in NDI Survey. URL: https://civil.ge/archives/523658 (дата обращения 03.04.23).
10. Мадридский саммит НАТО 2022 год. URL: https://www.nato.int/cps/en/natohq/news_196910.htm?selectedLocale=ru (дата обращения 07.09.2024).

11. Концепция национальной безопасности Грузии. URL: http://www.civil.ge/geo/article.php?id=24953 (дата обращения 16.09.2024).
12. Давиташвили З. Грузия: Нейтралитет или Западная ориентация? // Центральная Азия и Кавказ, 2002. №5 (23). 240 с.
13. Александринин О. Вектор европейской интеграции во внешне политике Грузии: взгляд из России // Региональный диалог. URL: http://refional-dialogue.com/ge/articles/ (дата обращения 09.10.2024).

Okudzhava A. **EURO-ATLANTIC INTEGRATION OF GEORGIA: CONTENT, DYNAMICS AND PROSPECTS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article analyzes the Euro-Atlantic direction of Georgia's foreign policy through diachronic analysis. With the help of this method, the research is based on temporal changes, i.e. the division of this process into certain stages. While writing the paper, the accompanying obstacles (external and internal) faced by Georgia in its chosen Euro-Atlantic course were highlighted. In conclusion, the relevant perspectives of Georgia's accession to NATO have been formulated as a result of the analysis and the rapidly developing globalization in the world.

Key words: Euro-Atlantic integration, NATO, geopolitics, security, foreign policy, regional security, military-political cooperation.

УДК 75.03
ГРНТИ 18.11.00

ЭКОЛОГИЧЕСКИЕ ПРОБЛЕМЫ АРКТИЧЕСКОГО РЕГИОНА В ВОСПРИЯТИИ ЖИВОПИСИ

К. В. Полякова
Российский государственный гидрометеорологический университет

Искусство является универсальным инструментом не только духовного развития, познания окружающей действительности. Искусство – важнейший инструмент государственной идеологии, формирования общественного мнения, оно выстраивает диалог между государством и обществом, между политическими системами разных стран, помогая безболезненно найти общие точки соприкосновения и разрешить возникающие противоречия для совместного движения вперед, сохранения хрупкого мира на планете.

экология, экологическое искусство, арктический регион, живопись

Искусство и экология – две темы, постоянно звучащие в общественной жизни разных стран, не оставляющие равнодушными представителей разных социальных и культурных групп, политических воззрений и вероисповеданий. Общим неизменно является то, что проблемы взаимодействия общества и природы не только не утрачивают своей актуальности, но и приобретают все большее значение по мере нарастания научно–технического прогресса, степени развития потребностей людей, что безусловно откладывает отпечаток на состояние окружающей среды.

Понятие искусства многогранно и многоаспектно, оно «пересекается с самыми различными сторонами человеческой жизни: затрагивая эмоции и разум, пробуждая память, вторгаясь в сферу как частной, так и публичной жизни, оно тем самым участвует в процессе воспитания и социализации».

Художественные произведения формируют общественное мнение, ведут диалог со зрителем, поднимают сложные социальные проблемы современности, вызывают споры и полемику, привлекают внимание к проблемам общества: глобальной безопасности, бедности и социального неравенства, климатическим изменениям, потери биоразнообразия, истощения природных ресурсов, экологическим кризисам.

Особое внимание в современном мире уделяется экологическим проблемам: урбанизации, сильнейшему загрязнению окружающей среды, уничтожению фауны и флоры, вырубке лесов, окислению вод океана и др. В XXI веке возросло хозяйственное воздействие человека на природу – «деградацию

окружающей среды стали сравнивать с «экологическим стрессом» [1]. Зачастую экономические выгоды от освоения природных богатств не учитывают хрупкости окружающей экосистемы, ее способности к самовосстановлению. Развитие науки и техники «стало выдвигать экологические проблемы на первый план, и сейчас уже всем ясно, что человечество движется к краю пропасти под влиянием конфликта природы и культуры» [2].

Понимание нависшей экологической угрозы и возможной необратимой катастрофы для человечества заставляют прогрессивных представителей правительств разных стран, ученых, международные организации объединять усилия по сохранению окружающей среды. И в этом вопросе экология и искусство неразрывно связаны. Не секрет, что многие природные ландшафты в следствии антропогенного воздействия человека утеряны безвозвратно и то, как они были прекрасны, мы можем увидеть на фотографиях, видеофильмах, картинах художников.

Исторический анализ процесса взаимодействия общества и природы показывает, что чем больше степень изменений, произведенных человеком в природе, тем сильнее влияние, оказываемое на общество со стороны последней, поскольку человек все более зависит уже не только от природы как таковой, но и от результатов своей деятельности в природе [3].

Актуальность экологической тематики нашло отражение в экологическом искусстве – совокупности разных жанров изобразительного искусства, в которых художник обращается к теме взаимоотношения человека и природы. Этот жанр направлен на сохранение, восстановление, обновление форм жизни, ресурсов и экологии. Художники, философы, активисты стараются пробудить общество к разумному иррациональному использованию природы через инсталляции, преферанс, анимации, фотографии. Однако не только современное экологическое искусство оказывает влияние на сознание человека и призывает к сохранению окружающей среды.

Арктика – экологически чувствительный регион с экстремальным климатом с низкими температурами, снегом, льдом и вечной мерзлотой. До начала XX века основными видами деятельности в Арктическом регионе были оленеводство, охота, рыбная ловля. Хозяйство коренных народов Севера не наносило большого вреда природе [4].

Белый регион привлекал внимание художников России, Китая и других стран – каждый из них через свои произведения выразил особое отношение к суровому краю. Неповторимая красота природа суровой Арктики нашла отражение в работах русских художников. Один из них Александр Алексеевич Борисов (1866–1934) – первый живописец Арктики, основоположник арктической живописи. Свои удивительные работы от написал в начале 20 века. «Это

все превосходные и верные, как зеркало, картинки, строго нарисованные и необыкновенно написанные. В них ярко выражена любовь этого русского Нансена к черной воде океана, с белыми льдинами, свежесть и глубина северных тонов, то мрачных, то озаренных резким светом низкого солнца»– так отозвался о работах молодого художника Илья Ефимович Репин (рис. 1, 2).

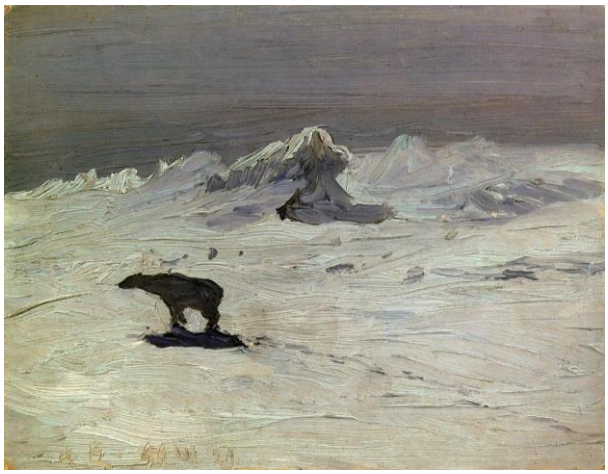


Рис. 1. Александр Борисов. Лунная ночь. Медведь на охоте. 1899 г.

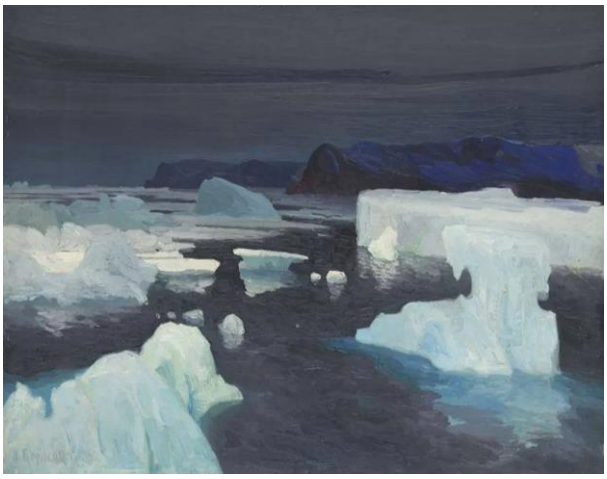


Рис. 2. Александр Борисов. В области вечного льда. Лето 1897 г.

Художник умело решил две главные задачи: подробно представил еще не тронутую, неизведанную и чистую территорию, а также создал художественный образ Арктики. Изображая пейзажи неизвестного края, Александр Алексеевич стремился создать живописно целостный образ, в котором бы соблюдалась фактологическая точность и передавались живые впечатления, эмоциональное состояние наблюдателя [5]. Необходимо подчеркнуть отличительную черту творчества художника – это уважительный интерес ко всем особенностям жизни обитателей Севера, создание образа человека и природы с которыми нужно говорить на равных несмотря на столь отдаленное расположение от «цивилизации».

В середине XX веке масштабы хозяйственного освоения российской части Арктики существенно расширились. И в местах промышленного освоения начались механическое разрушение почв, дестабилизация вечномерзлых грунтов и деградация экосистем [5]. В работах Ильи Константиновича Вылко (Тыко Вылко) отчетливо видно освоение, использование нетронутой в начале XX века Арктики (рис. 3). Глубоко художественный взгляд на окружающий мир сопровождал художника на протяжении всей его жизни.

Рис. 3. Тыко Вылка. Мыс Дровяной. 1950 г.

В 1950–х годах на Новой Земле началось возведение ядерного полигона – все ненецкое население было выселено с острова. Илья Константинович Вылко выразил свою любовь к Северу и отобразил прощание с неповторимой природой на мысе Дровяной.

Глобальный экологический кризис завершает XX век. Потребительское отношение к природе переходит на новый уровень. Наблюдается загрязнение Мирового океана, изменения ландшафтов, повышенная концентрация нефтяных углеводородов в питьевой воде, загрязнение окружающей среды и т.д. Именно в конце века подписывается более сотни природоохранных соглашений и конвенций, таких как: Киотский протокол (Киото, Япония 1997); Конвенция о биологическом разнообразии (Рио–де–Жанейро, Бразилия, 1992); Конвенция о трансграничном загрязнении воздуха на большие расстояния (Женева, Швейцария, 1979) и многие другие. Вслед за политиками и научным сообществом свою обеспокоенность катастрофическим загрязнением природы выразили художники. Так Сергей Семенович Асташев в своей картине «Прощай, Арктика»! (рис.4.) показал непродуманное вмешательство человека в живую природу и непоправимые последствия такого акта для экосистемы уникального арктического региона.

Рис.4. Асташев С.С. Прощай, Арктика! 1989.

Художники двадцать первого века не только обращают внимание на экологические проблемы, но и на своем примере показывают, как человек может их решить. Быть может, если бы не технический прогресс, заставляющий человечество все больше потреблять природные ресурсы и утилизировать промышленные отходы, то никто бы не придумал «экологическое искусство». Идеи, транслируемые в работах художников, не решают проблемы, они дают импульс, меняющий взгляды огромного количества людей в перспективе.

Художница Лиза Рэй посветила свою картину «Арктика» (рис. 5) глобальному потеплению и вымиранию символа Арктики – белому медведю из-за таяния льдов.

Рис. 5. Лиза Рэй. Арктика. 2014 г.

Таким образом экология, в простом понимании, показывает отношение человека к природе. А отношение к природе – это одна их сфер «общественной жизни человека, заключающая в себе нравственно–ценностное содержание». И это содержание менялось на протяжении истории человечества: от высшего начала и объекта поклонения (греческая цивилизация), до утилитарного – полностью лишающего природу «ценностного статуса, низводя ее до уровня средства для достижения экономической выгоды. Последствия такого подхода порождают глобальный экологический кризис, в котором оказалось современное человечество. И только признание личной ответственности человека за сохранение природной среды дает возможность сохранить для будущих поколений, найти социально–приемлемые выход из сложной экологической ситуации.

Список используемых источников

1. Вальковская В. В. Экологическое сознание как самосознание цивилизации: Автореф. дис. на соиск. учен. степ. д.филос.н.: Спец. 09.00.11 / Вальковская Виктория Викторовна; Моск. гос. ун–т им. М.В. Ломоносова. – М., 2000. 37 с.
2. Седова Н. Б. Экологические проблемы Арктики и их социально–экономические последствия / Н. Б.Седова, Е. Ю. Кочемасова // ЭКО, 2017. № 5. С. 160–171.
3. Каган М. С. Философия культуры. СПб.: ТОО ТК «Петрополис», 1996. 416 с.
4. Аксенова С. В. Искусство А. А. Борисова глазами современников и следующих поколений // Полярные чтения-2021. С. 405–419.
5. Глобальные проблемы современного общества: учебно–методическое пособие / автор–составитель С. В. Смирнов. Казань: Издательство Казанского университета, 2022. 74 с. URL: https://kpfu.ru/staff_files/F193521533/Globalnye_problemy_sovremennogo_obshhestva.pdf (дата обращения 25.10.2024).

Polyakova K. **ENVIRONMENTAL PROBLEMS OF THE ARCTIC REGION IN THE PERCEPTION OF PAINTING.**

Russian State Hydrometeorological University

Art is a universal tool not only for spiritual development, but also for cognition of the surrounding reality. Art is the most important tool of state ideology, the formation of public opinion, it builds a dialogue between the state and society, between the political systems of different countries, helping to painlessly find common ground and resolve emerging contradictions for joint movement forward, preserving fragile peace on the planet.

Key words: ecology, environmental art, Arctic region, Arctic artists.

УДК 656.025.2
ГРНТИ 39.21.02

ТРАНСПОРТНАЯ ПОДВИЖНОСТЬ НАСЕЛЕНИЯ РЕГИОНОВ РОССИИ НА ПРИМЕРЕ ДАЛЬНЕГО ЖЕЛЕЗНОДОРОЖНОГО СООБЩЕНИЯ

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

В современной России дальнее железнодорожное сообщение играет важнейшую роль в обеспечении пространственной связности территорий на разных иерархических уровнях. Геополитическая обстановка, сложившаяся в современном мире, привела к перераспределению потоков пассажиров в региональном разрезе и трансформации подвижности населения на железнодорожном транспорте. В статье сравниваются значения рассматриваемого показателя в разрезе 2016 и 2023 гг., а также выделяются ключевые причины его динамики.

железнодорожный транспорт, поезда дальнего следования, мобильность населения

Интенсификация жизни населения в современном мире требует постоянного роста пространственной мобильности, в том числе и транспортной. В классической форме транспортная подвижность населения оценивается на основе числа перемещений пассажиров из точки А в точку В, что требует достаточной точности при получении данных при анализе видов транспорта [1]. Такой подход является скорее прикладным и не позволяет оценить транспортное поведение населения, но дает возможность оценить изменчивость подвижности населения [2]. Конечно, важно отдавать себе отчет в том, что в реальности классический показатель (число поездок на 1 жителя в год) подвижности не отображает картину мобильности населения в региональном разрезе, поскольку не позволяет учесть поездки исключительно местных жителей [3], однако он способствует изучению пространственной мозаичности интенсивности использования видов транспорта [4, 5]. Анализ различий между территориями в значениях выбранного нами показателя в современной географической науке происходил в межстрановом [6], внутристрановом [5] и внутрирегиональном [4] разрезе. На текущий момент исследования железнодорожного транспорта дальнего следования в разрезе подвижности населения носят несистемный характер. В исследованиях специалистов в сфере экономики железнодорожного транспорта практически не представлен географический аспект [7, 8], а исследования географов достаточно редки [2, 9, 10].

В исследовании мы сравниваем значения показателя подвижности населения [9] в 2016 и 2023 гг. (рис. 1, 2). С нашей точки зрения этот параметр является индикатором значимости дальнего железнодорожного сообщения обеспечении пространственной связности региона: чем выше показатель подвижности населения, тем большую роль в системе региональных потоков играют поезда дальнего следования. В современной России наибольшее значение дальнее железнодорожное сообщение играет в регионах с маргинальной транспортной освоенностью сухопутными видами транспорта [9] (Архангельская область, Республика Коми, Ямало-Ненецкий автономный округ, Амурская область, Хабаровский край), а также в привлекательных для внутреннего туризма регионах (Краснодарский край, Республика Карелия). Наименьшая подвижность присуща республикам Северного Кавказа, регионам Южного Урала и Юга Сибири, что обусловлено, в первую очередь, их невыгодным транспортно-географическим положением.

Среднее значение показателя подвижности в России – 0,6 поездок на 1 человека в 2016 г. и 0,71 в 2023 г. В целом, несмотря на общий рост потоков за рассматриваемый период в 25 регионах было зафиксировано сокращение подвижности населения. К ним относятся следующие группы регионов:

– регионы Юга России с низкой общей подвижностью населения и растущими потоками на авиатранспорте: республики Чечня, Дагестан, Ингушетия, Калмыкия;

– приграничные регионы, потерявшие в период пандемии COVID-19 значимые для них межгосударственные потоки: Калининградская область, Оренбургская область, Саратовская область, Астраханская область, Омская область, Челябинская область;

– депопулирующие регионы Севера Европейской части России, Сибири и Дальнего Востока: Архангельская область, Кировская область, Республика Коми, Курганская область, Республика Хакасия, Сахалинская область.

регионы со снизившимися вахтовыми потоками в связи с перераспределением занятости населения по территориям России – Ханты-Мансийский и Ямало-Ненецкий автономные округа.

Отдельно стоит выделить Калужскую область (падение подвижности на 63 %), потерявшую транзитное транспортно-географическое положение в связи с прекращением связей с Украиной, что привело к резкому сокращению числа поездов дальнего следования. Также примечательно сжатие подвижности населения в республике Коми с 2,13 в 2016 г. (наиболее «подвижный» регион в 2016 г.) до 1,59 поездок на 1 человека в 2023 г (5 место в 2023 г.), что вызвано сокращением числа поездов дальнего следования, депопуляцией населения и падением объемов вахтовых потоков.

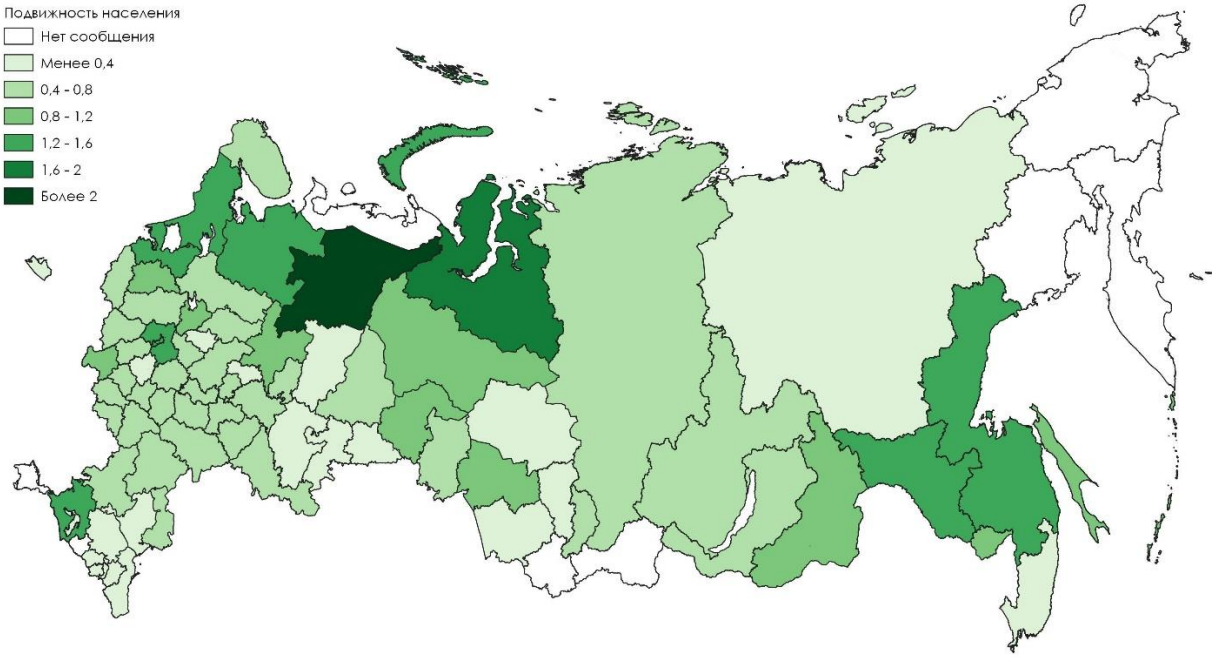


Рис. 1. Подвижность населения регионов России в дальнем железнодорожном сообщении в 2016 г., поездок на 1 жителя в год

Рис. 2. Подвижность населения регионов России в дальнем железнодорожном сообщении в 2023 г., поездок на 1 жителя в год

В 49 регионах России, напротив, выросла транспортная подвижность населения на дальнем железнодорожном транспорте. По особенностям причин роста стоит выделить следующие группы регионов:

– регионы, утратившие прямое авиационное сообщение с иными территориями страны, – Краснодарский край, Ростовская область, Воронежская область, Липецкая область, Курская область, Белгородская область, Ставропольский край;

– регионы, в которых за период с 2016 по 2023 гг. был открыт ряд новых железнодорожных маршрутов (в том числе скоростных), улучшивших их транспортную связность, – Ивановская область (рост подвижности на 130 %), Псковская область, Республика Карелия, Костромская область, Ярославская область, Смоленская область, Алтайский край, Республика Саха-Якутия;

– регионы, характеризующиеся растущими вахтовыми потоками, направленными на развитие железнодорожного каркаса России (БАМ 2.0) – Амурская область, Хабаровский край, Еврейская автономная область.

Подводя итоги, стоит отметить, что в целом в России за период с 2016 по 2023 гг. значительно выросла роль дальнего железнодорожного сообщения, особенно для тех территорий, которые в связи с закрытием аэропортов Центра и Юга России, лишились иных возможностей относительно комфортно и быстро добраться до точки назначения. Другим фактором, позитивно отразившимся на росте значения дальнего железнодорожного сообщения в регионах и подвижности населения на нем, стоит отметить постепенную «ласточкизацию» наиболее пассажиронапряженных связей между крупными городами и окружающими их локальными центрами, что наиболее типично для регионов Центра и Северо-Запада России, а также для территорий Западной Сибири (в особенности, для Алтайского края). Напротив, негативное влияние оказывает современная геополитическая ситуация, особенно в приграничных регионах или регионах, находящих на прямых транспортных путях в зарубежные страны. Наиболее тяжелая ситуация с точки зрения динамики подвижности характерна для Калужской области и Калининградской области, для которой негативные явления усугубляются политикой Литовской Республики. Также негативная динамика характерна для наиболее депрессивных территорий Севера, Сибири и Дальнего Востока, где потоки до сих пор не восстановились до уровня 2019 г.

Список используемых источников

1. Мулеев Е. Ю. «Транспортное поведение», «подвижность» и «мобильность»: к вопросу о концептуализации терминов // Социологический журнал, 2015. № 3. С. 8–28.

2. Семина И. А. Подвижность населения как транспортно-географическая проблема // Успехи современного естествознания, 2019. № 8. С. 73–78.

3. Кибальчич О. А. Вопросы географического изучения пассажирских перевозок // Проблемы экономических связей и транспорта (в связи с экономическим районированием). М.: Географическое общество Союза СССР. Московский филиал., 1962. С. 27–57.

4. Саввинова А. Н., Захаров М. И. Картографирование транспортной подвижности населения республики Саха (Якутия) // Интеркарто. Интергис. 2022. Т. 28. № 2. С. 229–243.
5. Тархов С. А. Авиаподвижность населения Индии: региональные различия // Известия Российской академии наук. Серия географическая. 2023. Т. 87. № 5. С. 677–689.
6. Тархов С. А. Влияние COVID-19 на авиаподвижность населения в странах Европы в 2020 году // Изв. РАН. Сер. геогр. 2021. Т. 85. № 6. С. 804–818.
7. Макарова Е. А. Суржин К. В., Пиунов А. Г., Соколовский А. В. Классификация пассажиропотоков на базе АСУ «Экспресс» для определения транспортной подвижности между регионами Российской Федерации // Вестник Научно-исследовательского института железнодорожного транспорта (ВЕСТНИК ВНИИЖТ), 2015. № 3. С. 42–47.
8. Остапчук В. Н. Транспортная подвижность населения и ее влияние на неравномерность пассажирских перевозок на железнодорожном транспорте // История и перспективы развития транспорта на севере России, 2013. № 1. С. 100–105.
9. Самбуров К. В. Пространственная иерархия пассажирских железнодорожных узлов и пунктов России: дис. ... канд. геогр. наук : 1.6.13 / Самбуров Кирилл Владимирович. Москва, 2023. 360 с.
10. Самбуров К. В. Транспортно-географическое районирование Еврейской автономной области на основе пассажирского железнодорожного сообщения дальнего следования // Сибирь и Дальний Восток России в формирующемся пространстве Большой Евразии, 2021. С. 142–145.

Samburov K. **TRANSPORT MOBILITY OF THE POPULATION OF RUSSIAN REGIONS USING THE EXAMPLE OF LONG-RANGE RAILWAY COMMUNICATION.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In modern Russia, long-distance rail service plays a vital role in ensuring spatial connectivity of territories at different hierarchical levels. The geopolitical situation that has developed in the modern world has led to a redistribution of passenger flows in the regional context and a transformation of population mobility in rail transport. The article compares the values of the indicator in question for 2016 and 2023, and highlights the key reasons for its dynamics.

Key words: railway transport, long-distance trains, population mobility.

5.2. Реклама и связи с общественностью в цифровом обществе

УДК 316.454.52
ГРНТИ 14.35.07

СТРАТЕГИИ ОБУЧЕНИЯ ИНОЯЗЫЧНОМУ АКАДЕМИЧЕСКОМУ ЧТЕНИЮ ДЛЯ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ

Е. П. Желтова, Н. В. Маршева
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются практические и академические аспекты курса по иностранному языку, а также методы и подходы к обучению, акцентирующие внимание на стратегическом планировании эффективного обучения, направленном на развитие аналитического и критического мышления. Особое внимание уделяется роли академического чтения в подготовке магистрантов технических специальностей, где критически важным является умение работать с разнообразными источниками информации и анализировать иноязычные научные тексты. Описываются план, содержание и этапы практического занятия с использованием электронного курса в СДО СПбГУТ и электронных интерактивных технологий.

техника чтения, критическое мышление, аналитические навыки, академическая коммуникация, методика обучения ИЯ

Научные исследования и академическое чтение тесно взаимосвязаны, поскольку и то, и другое включает процесс получения, анализа и синтеза информации для получения знаний и понимания определенного предмета или темы. Научные исследования часто включают в себя значительный объем академического чтения, поскольку исследователи должны изучить и проанализировать существующую как отечественную, так и зарубежную литературу по интересующей их теме, чтобы разработать вопросы, гипотезы и методы исследования. Они также должны быть в курсе последних исследований в своей области, чтобы убедиться, что их работа актуальна и вносит вклад в существующий массив знаний.

В данном контексте курс «Иностранный язык для научно-исследовательской работы» (ИЯ для НИР), включенный как обязательная дисциплина в про-

граммы Института Магистратуры (ИМ) СПбГУТ с 2019 года, ориентирован на магистрантов технического вуза, занимающихся исследовательской и проектной работой, и направлен на развитие компетенций в области академической коммуникации на иностранном языке.

В содержании курса аспект академическое чтение / Academic Reading – это активный процесс обучения, требующий от студентов активной работы с материалом, использования навыков критического мышления и развития исследовательских навыков.

Развитие навыков академического чтения на ИЯ необходимо студентам ИТ-специальностей для создания прочного фундамента знаний и понимания своей предметной области. Кроме того, академическое чтение необходимо студентам для проведения исследований и создания оригинальных работ. Они должны уметь находить, оценивать и использовать соответствующие источники информации для поддержки своих аргументов и идей. Стремление к получению новых знаний, культуре познавательной деятельности и саморазвитию является приоритетным направлением в образовательной деятельности современных студентов вузов и их ориентации на деятельное участие в научно-исследовательской работе, самостоятельном научном поиске, что делает этот процесс более успешным благодаря навыкам академического чтения и академического письма на ИЯ.

В основе методики обучения при реализации курса «ИЯ для НИР» лежат модульное обучение и современные педагогические технологии, а также методические приемы для развития у студентов-исследователей критического и креативного мышления, аналитических навыков и навыков коммуникации на ИЯ. Для эффективности и повышения качества обучения, помимо традиционных методов, используются современные образовательные технологии, а размещение материалов курса в СДО вуза (lms.spbgut.ru) позволяет использовать их как в традиционном формате обучения, так и в формате гибридного обучения [1, 2, 3]. При небольшом количестве практических занятий по предмету (по 28 часов в двух семестрах) предполагается самостоятельное изучение студентами части материала, что позволяет во время занятия уделить активной пошаговой проработке материала, а также практическим и проектным заданиям.

Ниже приводится план и содержание практического занятия (2 ак. часа) по дисциплине «ИЯ для НИР» с применением элементов интерактивного обучения для студентов-магистрантов 1 курса ИМ в СДО СПбГУТ по Модулю 3 Academic Reading and Academic Writing / Академическое чтение и академическое письмо.

Тема практического занятия: Основы академического чтения. Цель: Развитие навыков и техник чтения у студентов магистратуры. Задачи: ознакомить студентов с профессионально-ориентированными видами чтения, включая синтетическое и аналитическое [4], ознакомительное, изучающее, просмотровое, поисковое [5]; изучить техники академического чтения и критического чтения; улучшить понимание и запоминание прочитанного с помощью целевых стратегий чтения. Материалы: учебное пособие [1, стр. 34-49], академические тексты, относящиеся к изучаемой студентами области; электронные и раздаточные материалы с примерами отрывков для практики чтения; компьютеры или мобильные устройства (телефоны, планшеты) с доступом к электронному курсу в СДО; чек-листы для оценки навыков чтения (см. Табл. 1), которые могут быть созданы преподавателем.

Этапы занятия

Подготовительный этап */ разминка* (5 минут). В начале занятия студенты выполняют диагностический тест в СДО на знание основ академического чтения [3]. Результаты диагностического теста позволяют определить общий уровень знаний студентов по изучаемой теме и внести необходимые коррективы в содержание материала, при необходимости.

Warm up: активизация темы с использованием метода мозгового штурма.

Проблема: студентам задаются вопросы на ИЯ*: Как часто и много ли вы читаете текстов в рамках своего научного изыскания? Какие при этом используете техники чтения? Объясните, как меняется ваш собственный процесс чтения, когда вы сталкиваетесь с разными жанрами текста: как читать учебник и первоисточник; как читать научную статью и стихотворение и т. д.*

Lead-in: подготовка к иноязычному общению с помощью приложения для создания интерактивных опросов (например: Strawpoll). Цель: понимание значимости академического чтения для учебной и научной деятельности. Примеры вопросов на ИЯ: *What are some benefits of reading for master's degree students? a) Developing critical thinking skills b) Broadening knowledge base c) Increasing understanding of the subject matter studied d) All of the above; What can academic reading help master's degree students do? a) Explore different perspectives on topics through primary sources b) Critically analyze information c) Draw conclusions from evidence presented d) All of the above; What can master's degree students synthesize into their own work through reading? a) New ideas b) Primary sources c) Journal articles d) None of the above.*

I этап (15 минут): активизация лексики по изучаемой теме с применением игрового метода интерактивного обучения – приложения Quizlet (Рис. 1).

Рис. 1. Активизация лексических единиц с программой Quizlet

Данный тренажер позволяет использовать разные режимы работы с лексикой - заучивание в виде карточек, отработка произношения, письмо, правописание. Режим игры Quizlet Live так же используется для создания эмоционального заряда и мотивации к лидерству. Используется режим командной или индивидуальной игры, что развивает ответственность за принятое решение перед коллективом, повышает саморефлексию.

II этап (25 минут): мини-лекция по теме “Academic reading techniques: skimming, scanning and critical reading” и закрепление материала о техниках и стратегиях академического чтения.

После изучения теоретического материала идет активное обсуждение и закрепление в формате групповой, парной и индивидуальной работы по изучению и объяснению трех основных техник чтения с приведением примеров того, когда каждая техника может быть использована эффективно. К примеру:

– техника *skimming* заключается в быстром ознакомлении с текстом. Продемонстрировать данную технику можно, выбрав образец академического текста и смоделировав, как определить ключевую информацию, основные

идеи и заголовки. Отработать на практике данную технику чтения, раздав раздаточные материалы;

– техника *scanning* – быстрый поиск конкретной информации в тексте. Отработать на практике данную технику чтения, предоставив студентам образцы текстов и упражнений на определение ключевых слов и вопросов на быстрый поиск конкретной информации;

– техника *critical reading* – целью критического чтения является анализ и оценка содержания текста. Изучить стратегии критического чтения, такие как аннотирование, резюмирование и задавание критических вопросов. Отработать на практике, обсудив важность активного чтения, постановки под сомнение предположений и представленного материал, источника и автора текста, затем раздав образцы академических текстов студентам.

III этап (30 минут): практика применения техник чтения в виде выполнения заданий: прочитать академический текст / медиатекст, связанный с областью исследований за отведенное время; сделать заметки в процессе чтения для понимания и анализа текста; аннотировать и кратко изложить ключевые моменты текста и др. При анализе конкретных составляющих академического чтения выделяется: умение понять специфику логического построения текста для того, чтобы сделать правильный вывод; умение извлечь из текста информацию более общего или более частного характера; умение догадаться о значении незнакомых слов по контексту [6, 7].

Тексты для реферирования и аннотирования на ИЯ, а также виды заданий (составление словаря-тезауруса, выделение ключевых слов, задания на перифраз) опираются на базовые принципы интерпретации текста и призваны способствовать эффективному и равномерному развитию навыков использования лексико-грамматических замен, синонимов и антонимов, компрессии и развертывания и выступают в качестве подготовительного этапа к непосредственной переводческой деятельности специализированных текстов.

IV этап (15 минут): оценка и самоанализ / Self assessment & Self-reflection.

Групповое обсуждение и осмысление проблем и выводов, полученных в результате применения техник чтения, обсудив размышлениям о преимуществах каждой техники чтения и о том, как их можно применить в будущей академической деятельности. При работе студентов в СДО вуза с интерактивными заданиями преподаватель имеет возможность оперативно предоставить обратную связь студенту и выявить пробелы в усвоении темы. Также для оценивания навыков академического чтения студентов можно использовать чеклист “Peer assessment checklist for academic reading” (таблица 1).

ТАБЛИЦА 1. Экспертная оценка и критерии навыков академического чтения

Assessment Criteria: 1,2,3,4,5 Points	Name	Name	Name
1. Understanding of the main ideas and arguments presented in the text			
2. Ability to identify and analyze key concepts and themes			
3. Accuracy of interpretation and evaluation of evidence presented in the text			
4. Ability to critically evaluate the author's arguments and evidence			
5. Knowledge of relevant background information and context			
6. Ability to make connections between the text and other related works			
7. Clarity and coherence of the written response to the reading			
8. Use of appropriate academic language and tone			
9. Correct grammar, punctuation, and spelling			
10. Overall quality and effectiveness of the written response in the form of an abstract / annotation			
Total:			

V Заключительный этап: самостоятельная работа студентов по выполнению задания на поиск, анализ и оценку литературных источников с указанием факторов, которые делают источник надежным и заслуживающим доверия.

Обучение магистрантов иноязычной коммуникации по предложенной методике способствует формированию коммуникативных и исследовательских компетенций за счет повышения уровня академической грамотности, что в целом ведет к плавному переходу от общения на учебном (академическом) языке к научному стилю коммуникации для дальнейшего применения полученных навыков в НИР. Данное обобщение подтверждается увеличением показателей [8], которые были получены в виде опроса студентов с помощью диагностического теста в начале изучения модуля и в конце. Выполненные задания и результаты тестирования студентов, прошедших обучение данного модуля, показали, что они не только получили академические знания, знания языковых форм, средств современных коммуникативных технологий, стратегий и тактик академического чтения, но и повысили навыки презентации собственных идей, критические и аналитические навыки, навыки работы в команде.

Список используемых источников

1. Желтова Е. П., Маршева Н. В. Иностранный язык для научно-исследовательской работы. Английский для магистрантов: учебное пособие / Е. П. Желтова, Н. В. Маршева. СПб.: СПбГУТ, 2022. 96 с.
2. Левченко В. В., Агрикова Е. В., Воронина М. А. Формирование навыков академической коммуникации: организация работы // Высшее образование в России, 2017. № 4 (211). С. 58–62.
3. Система дистанционного обучения СПбГУТ по курсу «Иностранный язык для научно-исследовательской работы». URL: https://lms.spbgut.ru/course/view.php?id=935 (дата обращения 11.10.2024).
4. Клычникова З. И. Психологические особенности обучения чтению на иностранном языке: пособие для учителя / З. И. Клычникова. 2-е изд., испр. М.: Просвещение, 1983. 207 с.
5. Фоломкина С. К. Обучение чтению на иностранном языке в неязыковом вузе: учеб.-метод. пособие / С. К. Фоломкина; науч. ред.: Н. И. Гез. 2-е изд., испр. М.: Высш. шк., 2005. 253 с.
6. Pearson Ch. Advanced academic skills in the low-level ESL class // TesOl Quarterly, 1981. Vol. 15. № 4. PP. 413–423.
7. Землякова К. В. Формирование компетенций работы с медиатекстом на иностранном языке у студентов коммуникативных направлений / К. В. Землякова, А. В. Кульназарова // Вестник Гуманитарного факультета Санкт-Петербургского государственного университета телекоммуникаций им. профессора М. А. Бонч-Бруевича. 2020. № 12. С. 36–44. URL: https://bafo-forum.ru/media/pages/docs/ba87289ea8-1632744672/gf.pdf
8. Маршева Н. В. Анкета “What type of reader are you: a “surface” or superficial reader and a “deep” or critical reader?” URL: https://forms.gle/DZAn7RzynWwXZ7Bo7 (дата обращения 11.10.2024).

Zheltova E., Marsheva N. **STRATEGIC APPROACHES TO ACADEMIC READING FOR RESEARCH.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article explores the practical and academic aspects of the course “Foreign Language for Research”, emphasizing the strategic planning essential for effective research-oriented language learning. It highlights the development of master’s degree students’ skills in academic reading, analytical thinking, and critical thinking while presenting the plan, content, and stages of practical training sessions that incorporate interactive technologies and the e-course within SPbSUT’s distance learning systems.

Key words: reading technique, critical thinking, analytical skills, academic communication, language teaching methodology.

УДК 339.138
ГРНТИ 45.01.14

ПРОДВИЖЕНИЕ ФОТОУСЛУГ В ЦИФРОВОЙ СФЕРЕ

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

В условиях высокой конкуренции на рынке фотоуслуг особенно важным является эффективное продвижение, направленное на привлечение целевой аудитории и формирование позитивного имиджа фотографа. В статье рассматриваются основные стратегии и инструменты, которые помогают фотографам продвигать свои услуги, привлекать новых клиентов и выстраивать лояльные отношения с существующими. Исследуются принципы интернет-маркетинга, особенности контентной стратегии и роль социальных медиа в продвижении фотоуслуг. Также выделены современные тенденции, влияющие на поведение клиентов и их предпочтения в выборе фотографа.

продвижение, целевая аудитория, УТП, социальные сети, стратегия продвижения, интернет-маркетинг

За последние несколько лет все более стремительно развивается рынок фотоуслуг, добавляя в сферу больше конкурентов. В современном обществе каждый человек, имеющий камеру на смартфоне, способен самостоятельно делать фотографии в хорошем качестве, тем самым уменьшая потребность в профессиональных фотографах для повседневных задач.

Однако, это не значит, что услуги фотографа не актуальны и никому не нужны, наоборот, их работа остается востребованной в особых случаях, таких как свадьбы, портретные съемки, фотосъемки для рекламных кампаний и других событий. Именно поэтому, для фотографа особо важно уметь выделять свои работы и услуги среди множества конкурентных предложений. Для этого необходимо обладать каким-то уровнем знаний по продвижению и учитывать особенности своей целевой аудитории.

Продвижение услуг фотографа с помощью интернет-маркетинга требует не только высокого уровня профессионализма, но и составления маркетинговой стратегии. Рынок фотоуслуг разнообразен, и для каждого сегмента требуются свои подходы и инструменты продвижения.

Эффективное продвижение невозможно без понимания целевой аудитории, ее интересов и потребностей.

Целевая аудитория – группа людей, которая выявлена по каким-то признакам и на которую нацелены те или иные месседжи и технологии [1]. Фото-

граф должен определить, какие клиенты больше всего заинтересованы в его услугах: это семьи, молодожены, бизнесмены, модели и агентства. Определив целевую аудиторию, фотограф может направить свои усилия на людей, которые действительно заинтересованы в его работе и с большей вероятностью будут получать заказы.

Одним из наиболее важных факторов успешного продвижения является разработка уникального торгового предложения (УТП), которое выделит фотографа среди конкурентов. УТП – это концепция создания рекламной кампании, основанной на выдающихся характеристик продукта или бренда [2].

Уникальное торговое предложение может основываться на стилистике работы (портретная фотосъемка, семейная, свадебная, коммерческая фотография), на особых условиях сотрудничества, которые смогут сразу привлечь целевую аудиторию и повысить узнаваемость или на уникальной технике съемки, которая станет изюминкой фотографа и выделит его среди конкурентов.

Зачастую, перед покупкой товара потребители заходят в Интернет и социальные сети, чтобы почитать отзывы о товарах или услугах, которые они хотят приобрести [3]. В современном мире интернет-сайты являются важнейшим инструментом продвижения услуг фотографов, а также основной платформой для демонстрации работ, получения экспертной информации и возможности взаимодействия с клиентами, пример. Создание качественного и функционального веб-сайта не только улучшает имидж фотографов, но и помогает привлечь новых клиентов и увеличивает шансы на успешное продвижение бизнеса.

Первым, главным элементом веб-сайта фотографа, является портфолио. Это виртуальная витрина, на которой представлены лучшие готовые изделия. Портфолио должно быть тщательно отобрано и демонстрировать различные стили, техники и приемы фотографов, чтобы потенциальные клиенты могли оценить, подходит ли стиль работы профессионалов для их нужд.

Сегодня ВКонтакте является основной платформой для продвижения. Социальные сети помогают многим фотографам продемонстрировать свои работы, закулисье и рассказать о процессе съемки. Благодаря инструментам платформы можно создавать короткие видеоролики, которые могут попадать в рекомендации и привлекать больше подписчиков и потенциальных клиентов.

ВКонтакте – одна из крупнейших социальных сетей в России и странах СНГ, которая помогает бизнесу в продвижении. Социальная сеть предоставляет личный кабинет продвижения. Этот инструмент дает возможность компаниям и профессионалам, включая фотографов, находить целевую аудито-

рию, взаимодействовать с пользователями и увеличивать охваты. В личном кабинете можно запускать рекламные кампании, которые можно настроить на разные цели и форматы.

Личный кабинет позволяет использовать таргетированную рекламу, благодаря которой можно показывать объявления целевой аудитории по возрасту, полу, интересам, географии и другим параметрам. Промо-статьи – это рекламные записи, которые появляются в ленте пользователей. Промо акции и специальные предложения способны увеличить покупательскую лояльность к продукту, сделать цену в торговой точке более конкурентной по отношению к другим продуктам, а также стимулировать дополнительный импульс к покупке и привлечь новых покупателей [4]. Внешне такие записи похожи на простые посты, но которые могут содержать полезную или выгодную для аудитории информацию. Такой формат особо выгоден фотографам, так как дает возможность показать свои работы, что сразу привлечет внимание потенциальных клиентов.

Также, личный кабинет включает в себя возможность размещать рекламные кампании в виде баннеров, слайдеров и других визуальных форматов, которые будут ярко выделяться на фоне повседневной, иногда серой и неинтересной информации. Благодаря статистики пользователь может узнать, как работает выставленная рекламная кампания, сколько человек ее увидело и какой бюджет за определенное время был потрачен. Аналитика предоставит информацию об эффективности кампании и даст советы о правильности написания ключевых слов, возраста аудитории и других параметров. Это позволят оперативно корректировать стратегии и оптимизировать рекламные бюджеты.

На сегодняшний день статистика показывает, что клиентам важны не просто фотоуслуги, они ищут уникальность. В 2024 году трендом в этой сфере является оказание комплексных услуг, другими словами, люди хотят полную организацию съемок. Такой кейс уникальной услуги, поможет выделить фотографа среди конкурентов, так как на рынке очень тяжело найти услуги фотографа под ключ. Клиенты хотят получать результат, соответствующий стилю фотографа и предпочтениям, а не шаблонные фотографии.

В современном мире информация лучше воспринимается посредством образов, поэтому создание коротких видео, будет хорошим вариантом продвижения. Такие видео могут содержать в себе полезную информацию для клиентов или юмор, использование которого поможет повысить лояльность клиентов. Также, такие ролики могут показывать ваши сильные стороны. Например, кадры с фотосессии с объяснениями, в таком ролике фотограф может упоминать время работы, показывать, как он снимает или обрабатывает. Такая от-

крытость и транслирование своих навыков поможет расположить потенциальных клиентов и подтолкнет их к покупке услуги фотографа.

Продвижение фотоуслуг требует комплексного подхода, включающего работу над уникальным предложением, использованием современных инструментов маркетинга и взаимодействием с клиентами на различных платформах. Успешный фотограф должен не только иметь высокие профессиональные навыки, но и уметь привлекать и удерживать клиентов, выстраивая с ними доверительные отношения. Необходимо следить за тенденциями на рынке, чтобы соответствовать ожиданиям клиентов и предлагать им инновационные и качественные решения. Важно учитывать, что тренды меняются, методы продвижения тоже, следовательно необходимо постоянно обучаться, искать новые решения, которые продвинут услуги и принесут больше клиентов и записей на фотосъемки.

Список используемых источников

1. Гуляев А. А., Гершун Г. С., Лахтин А. Ю. Целевые аудитории как предмет педагогических технологий // Вестник РМАТ, 2019. №3. URL: https://cyberleninka.ru/article/n/tselevye-auditorii-kak-predmet-pedagogicheskih-tehnologiy (дата обращения 14.11.2024).
2. Уникальное торговое предложение // Образовательный портал «Справочник». Дата написания статьи 08.12.2017. URL https://spravochnick.ru/reklama_i_pr/unikalnoe_torgovoe_predlozhenie/ (дата обращения 14.11.2024).
3. Меньшенина А. А. Технологии продвижения в социальных сетях // Вестник науки, 2023. №2 (59). URL: https://cyberleninka.ru/article/n/tehnologii-prodvizheniya-v-sotsialnyh-setyah (дата обращения 14.11.2024).
4. Михайлова А. Д., Кован С. Е. Промо-акция как стратегический инструмент управления категорией // Стратегии бизнеса. 2015. №12 (20). URL: https://cyberleninka.ru/ article/n/promo-aktsiya-kak-strategicheskiy-instrument-upravleniya-kategoriey (дата обращения 14.11.2024).

Krivonos A., Kulnasarova A. **PROMOTION OF PHOTOGRAPHIC SERVICES IN THE DIGITAL AREA.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In conditions of high competition in the market of photo services, effective promotion aimed at attracting the target audience and creating a positive image of the photographer is especially important. The article discusses the main strategies and tools that help photographers promote their services, attract new customers and build loyal relationships with existing ones. The principles of marketing, the features of content strategy and the role of social media in the promotion of photo services are investigated. Modern trends affecting the behavior of clients and their preferences in choosing a photographer are also highlighted.

Key words: promotion, target audience, USP, social networks, promotion strategy, internet marketing.

УДК 659.442
ГРНТИ 19.01.29

ОСОБЕННОСТИ ВЗАИМОДЕЙСТВИЯ ИНКЛЮЗИВНЫХ БРЕНДОВ СО СВОЕЙ АУДИТОРИЕЙ

А. А. Русова, С. Ю. Щур
Санкт-Петербургский политехнический университет Петра Великого

Для построения коммуникаций с аудиторией инклюзивные бренды сталкиваются с проблемами в выборе визуального стиля, связанными с этическими ограничениями и предубеждениями. В связи с этим в статье проведен анализ существующих брендов и способов их взаимодействия с аудиторией, на основе этого выявлены наиболее эффективные элементы коммуникаций.

брендинг, визуальные коммуникации, айдентика, цветовая палитра

Брендингу отводится ключевая роль в создании эмоциональной визуальной связи с аудиторией. Для привлечения внимания, выражения своей идентичности бренды пользуются такими приемами как, например, цветовые палитры, основанные на психологии потребностей целевой аудитории; ключевые визуальные элементы для подчеркивания уникальности; графические символы и метафоры для передачи сложных идей; а также использование анимации, дополненной реальности, аудио сопровождения.

Современным брендам, при коммуникации с аудиторией, важно передать настроение и атмосферу, то есть быть комфортными для них и жить на одной волне. Выбор цветовой гаммы для построения визуальных коммуникаций с целевой аудиторией будет оказывать влияние на их эмоциональную реакцию, а затем и формировать ощущения [1]. Помимо цветовой палитры не менее важно «цеплять» внимание аудитории какими-либо графическими элементами и метафорами, которые помогают брендам передать смыслы без слов, а также демонстрировать свою особенность и уникальность. Брендам, связанным с разного рода инклюзиями, очень важно создать со своей целевой аудиторией особую связь с ощущением комфорта, безопасности, места, где каждый будет замечен и услышан. Для выявления особенностей визуальных коммуникаций инклюзивных брендов, были проанализированы фирменные стили таких брендов как: «Антон тут рядом», «Йом Йом», «Простые вещи» и «Мир хоккея для особенных детей».

Цель данного исследования – определить и проанализировать способы визуальных коммуникаций у инклюзивных брендов для выявления их влияния на формирование эмоциональной связи со своей целевой аудиторией.

Задачи исследования:

1. Проанализировать айдентику инклюзивных брендов;

2. Исследовать цветовые решения;

3. Рассмотреть роль графических метафор в визуальных коммуникациях инклюзивных брендов;

4. Определить, как визуальные коммуникации способствуют формированию идентичности брендов;

5. Выявить ключевые аспекты, способствующие успешной визуальной коммуникации.

Объект исследования – инклюзивные бренды.

Предмет исследования – особенности визуальных коммуникаций, используемых брендами.

«Антон тут рядом» – фонд системной поддержки людей с аутизмом, основанный в 2013 году в Санкт-Петербурге [2]. Его целевая аудитория обширна – это взрослые люди с особенностями развития, а также все неравнодушные и желающие поддержать фонд люди и бизнесы.

Для коммуникации с аудиторией бренд использует минимальный набор цветов: черный, белый – основные; красный – акцентный. У бренда нет цели сыграть на цветовом разнообразии. Здесь цвет используется для базового разделения информации – белый и черный, и для выделения главных смысловых элементов – красный.

Привлечение внимания происходит за счет авторского шрифта и иллюстраций, которые были созданы вместе с подопечными, их визуальные метафоры и тонкий юмор дают стилю фонда отойти от излишне нейтральных или, наоборот, трендовых направлений [3]. И это главный прием бренда, позволяющий отделиться от других. Шрифт, основанный на леттеринге Антона Харитонова (первого студента фонда, с него, в 2013 году, началась его история) и Сергея Тиснека (студент и художник фонда), передает идею бренда, так как это шрифт нейроотличного человека, а также дал начало визуальному стилю фонда [4]. Отзеркаленные буквы в текстах, и даже в самом логотипе, позволяют заострить на себе внимание пользователя, дольше задержать его и изучить подробнее элементы. Иллюстрации, лишенные идеальности: пропорций, ровных линий и т. д., однако, находящиеся на ровно сверстанном сайте, или на сувенирной продукции, где также уравновешиваются какими-либо ровными формами, смотрятся очень органично и запоминающееся.

Таким образом, бренд «Антон тут рядом» выбирает в своей визуальной коммуникации акцент на шрифтах и иллюстрациях нейроотличных людей, которые привлекают внимание своей необычностью. Дизайнер бренда объясняет использование авторской графики и леттеринга трансляцией главной

мысли – «мы такие, мы имеем право быть похожими на себя» [5], а визуальные метафоры подопечных фонда позволяют бренду остаться в стороне от нейтральных или трендовых направлений [6].

«Йом-Йом» – инклюзивный центр из Санкт-Петербурга. Его целевая аудитория – это родители обычных детей и детей с особенностями, а также образовательные учреждения и организации [7].

Можно сказать, что цвета здесь символизируют окружение заботой, вниманием, показывают уважение, безопасность и бережное отношение. Цветовая палитра играет значимую роль, она передают настроение и эмоции аудитории, ощущение комфорта и понятности. Цвета – часть визуальной айдентики.

Идея бренда передается аудитории не только цветовой палитрой, но и благодаря визуальной метафоре – гирлянде, раскрывающей идею инклюзии. Дети с особенностями развития – это лампочки в гирлянде, которые никто не видит, но они – часть нашей общей жизни. Бренд «включает лампочки» и делает детей видимыми для общества, чтобы «гирлянда светила ярче, ведь какой может быть праздник, если не все лампочки включены». Образ интерпретации гирлянды передается простыми графическими элементами – круги в фирменных цветах с разной степенью размытия – так видят гирлянду те, кто щурится от смеха и радости [8]. Такой образ передает свет, тепло и детское ощущение чуда. Такая айдентика выражает ощущение свечения и глубины.

Таким образом «Йом Йом» создает образ инклюзии, правильный и понятный для коммуникации с широкой аудиторией. С помощью цветовых сочетаний и несложных графических элементов бренд рассказывает об инклюзии с помощью яркой метафоры.

«Простые вещи» – это мастерские в Петербурге, где работают взрослые люди с ментальными особенностями. Их целевая аудитория – взрослые люди с особенностями, волонтеры и бизнесы [9].

Бренд объединил в себе идею передачи эмоций и с помощью цвета, и с помощью авторских иллюстраций и леттерингов, созданных подопечными мастерской. Такой дизайн подчеркивает дружественную атмосферу и вдохновляет [10].

Стоит отметить, что, в отличие от бренда «Антон тут рядом», «Простые вещи» используют для визуальных коммуникаций разнообразную цветовую палитру. Можно предположить, что такие цветовые сочетания дополнительно передают настроение и атмосферу бренда, их позиционирование.

Айдентика бренда – иллюстрации и леттеринги подопечных мастерских демонстрируют уникальность вещей, создающихся в их стенах. Тем самым бизнесу показывается уникальных подход в реализации их заказов.

«Мир хоккея для особенных детей»: основная их деятельность направлена на создание условий для развития адаптивных видов хоккея в России и повышения их роли в социальной реабилитации детей и молодежи с инвалидностью [11]. Целевая аудитория бренда – дети с особенностями и их родители, профессиональное тренерское сообщество и организации, поддерживающие их развитие.

У бренда нет визуальных метафор или сложных элементов в качестве айдентики. Бренд, отчасти через цвета, передает ощущение большой спортивной семьи, которая принимает человека не за победы и спортивную эффективность, а за его горящие глаза и желание быть частью этой команды.

Визуальные коммуникации инклюзивных брендов играют критическую роль в формировании эмоциональной связи с целевой аудиторией. Каждый из рассмотренных брендов использует уникальные подходы, чтобы подчеркнуть свои ценности и задачи в области инклюзии. Проанализировав вышеупомянутые бренды, можно выделить следующие особенности их коммуникаций.

1. Бренд «Антон тут рядом» фокусируется на индивидуальности через авторские шрифты и иллюстрации, созданные студентами фонда. Такие графические элементы создают ощущение уникальности и принадлежности, позволяя пользователям увидеть особенность и право быть собой.

2. Инклюзивный центр «Йом-Йом» использует цветовую палитру и метафору гирлянды, чтобы донести идею инклюзии, создавая образ единства и связи. Такой подход помогает визуально включать детей с особенностями в общество, акцентируя внимание на том, что каждый «светит» по-своему, но важно, чтобы «светили» все.

3. Мастерская «Простые вещи» объединяет разнообразие цветов и уникальные иллюстрации, передавая атмосферу творчества и особой ценности каждого человека. Это находит отклик как у подопечных, так и у бизнесов-заказчиков продукции, демонстрируя уникальность и креативность выпускаемой продукции.

4. «Мир хоккея для особенных детей» строит свою коммуникацию на простоте и ощущении большой сплоченной спортивной семьи, где важны не только достижения, но и стремление к общему делу. Этот подход актуален для создания дружелюбной и поддерживающей атмосферы внутри федерации.

Таким образом, успех брендов, связанных с инклюзией, во многом зависит от их способности строить идентичность, вызывающую эмоции и создающую ощущение надежности и принадлежности у их целевой аудитории. Каждый из них подчеркивает важность связи и принятия, что является ключом к успешной коммуникации с аудиторией.

Список используемых источников

1. Nayanika Singh, S. K. Srivastav. Impact of Colors on The Psychology of Marketing – A Comprehensive Over View // Management and Labour Studies Vol 36, № 2. May 2011. С. 199–209.
2. Антон тут рядом. URL: https://antontut.ru (дата обращения 23.10.2024).
3. Как фонд «Антон тут рядом» стал главным городским ньюсмейкером в области культуры. URL: https://www.sobaka.ru/city/society/183615 (дата обращения 23.10.2024).
4. Кто это придумал и как это работает: команда фонда «Антон тут рядом». URL: https://obdn.ru/articles/kto-eto-pridumal-i-kak-eto-rabotaet-komanda-fonda-anton-tut-ryadom (дата обращения 23.10.2024).
5. Кто это придумал и как это работает: команда фонда «Антон тут рядом». URL: https://obdn.ru/articles/kto-eto-pridumal-i-kak-eto-rabotaet-komanda-fonda-anton-tut-ryadom (дата обращения 23.10.2024).
6. Как фонд «Антон тут рядом» стал главным городским ньюсмейкером в области культуры. URL: https://www.sobaka.ru/city/society/183615 (дата обращения 23.10.2024).
7. Йом-Йом – детский центр в Санкт-Петербурге. URL: https://yom-yom.ru/mission (дата обращения 24.10.2024).
8. Здесь мой йом. Брендинг инклюзивного проекта «Йом-Йом». URL: https://dezzza.ru/portfolio/zdes-moj-jom-brending-inklyuzivnogo-proekta-jom-jom/ (дата обращения 24.10.2024).
9. Простые вещи. URL: https://prostieveschi.ru/about-us/ (дата обращения 25.10.2024).
10. Грибанова М. О. Особенности дизайна и продвижения в сфере инклюзивных сообществ / М. О. Грибанова. // Культурологические чтения–2022. Культурное наследие и актуальные культурные практики: репрезентации, трансформации, перспективы: материалы Всероссийской (с международным участием) научно-практической конференции. Екатеринбург: Издательство Уральского университета, 2022. С 281.
11. Нас объединил хоккей. URL: https://paraicehockey.ru/federatsiya-adaptivnogo-hokkeya/ (дата обращения 25.10.2024).

Rusova A., Shchur S. **FEATURES OF INTERACTION OF INCLUSIVE BRANDS WITH THEIR AUDIENCE.**

Peter the Great St. Petersburg Polytechnic University

To build communications with audiences, inclusive brands face challenges in choosing a visual style associated with ethical restrictions and biases. In this regard, the article analyzes existing brands and ways of their interaction with the audience, based on this, the most effective elements of communication are identified.

Key words: branding, visual communications, identity, color palette.

5.3. Цифровая трансформация, инновации, бизнес

УДК 658.5
ГРНТИ 28.17.31

ИНТЕГРАЦИЯ ИНСТРУМЕНТОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УПРАВЛЕНИИ БИЗНЕС-ПРОЦЕССАМИ КОМПАНИИ

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

В данной работе рассматривается применение инструментов искусственного интеллекта в управлении бизнес-процессами компании. Особое внимание уделяется определению нейронных сетей и больших языковых моделей (LLM), их способам применения в бизнес-процессах. Также исследуются функциональные возможности платформы Bitrix24 с модулем Copilot для оптимизации внутренних коммуникаций и маркетинга, а также результаты использования сервисов Yandex Cloud AI (SpeechKit, YandexArt, YandexGPT-4) в создании маркетинговых материалов.

искусственный интеллект, Bitrix24-Copilot, Yandex Cloud AI, нейронные сети, большие языковые модели (LLM), внутренние коммуникации, маркетинг, цифровая экономика

24 декабря 2018 года правительством Российской Федерации была утверждена программа «Цифровая экономика Российской Федерации», где отдельно был выделен раздел «Нейротехнологии и искусственный интеллект». Данная программа указывает на то, что необходимо способствовать развитию российских IT-компаний, а также создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств [1].

Нейронные сети – это математические модели, основанные на принципах биологических нейронных сетей и представляющие систему соединенных и взаимодействующих искусственных нейронов; согласно мнению Джоэла Граса [2], каждый нейрон взвешивает входящие сигналы и реагирует, если результат превышает определенный порог. Искусственный интеллект (ИИ) – это область информатики, занимающаяся созданием систем, способных выполнять задачи, требующие человеческого интеллекта, такие как обучение, рассуждение и распознавание.

Большие языковые модели (Large Language Models, LLM) – это разновидность нейронных сетей, специализированных на обработке и генерации естественного языка. Обученные на обширных корпусах текстовых данных, LLM способны понимать контекст, генерировать связные тексты, отвечать на вопросы и выполнять различные задачи обработки естественного языка (NLP). Примеры LLM включают модели серии GPT, такие как GPT-3 и GPT-4, а также их российский аналог YandexGPT-4.

Влияние генеративного ИИ на производительность труда может стать таким же преобразующим, как революции печатного станка, интернета и конвейерной линии, и аналитическая компания Oliver Wyman [3] в 2024 году оценила, что он может ежегодно экономить 300 миллиардов рабочих часов. Хотя генеративный ИИ существует более 50 лет, активное его использование сотрудниками различных отраслей началось только с запуском ChatGPT и других нейросетей на больших языковых моделях.

Автоматизация рутинных задач с помощью генеративного ИИ позволяет работникам сосредоточиться на более творческих и значимых аспектах работы, открывая возможности для сотрудничества между людьми и ИИ и расширяя границы того, что мы определяем как продуктивность.

Генеративный ИИ создает все более сложные риски для организаций, включая как известные проблемы, такие как "галлюцинации" ИИ и трудности с интерпретацией алгоритмов, так и неизвестные риски, связанные с влиянием ИИ на людей, что может привести к непредвиденным последствиям; поэтому компании и общества должны принять будущее, где риск и награда сосуществуют, основываясь на динамической модели тестирования, измерения и обучения.

В условиях быстрого технологического развития и усиления конкуренции предприятия совершенствуют бизнес-процессы путем интеграции искусственного интеллекта в управление маркетингом и внутренними коммуникациями, исследуя применение ИИ на примере хлебной компании с использованием платформы Bitrix24 с Copilot и сервисов Yandex Cloud AI (SpeechKit, YandexArt, YandexGPT-4), что позволяет автоматизировать рутинные операции и повысить эффективность взаимодействия.

Хлебная компания столкнулась с рядом существенных проблем, требующих интеграции инструментов поддержки искусственного интеллекта в бизнес-процессы, особенно во внутренние коммуникации и маркетинг:

1) фрагментация внутренних коммуникационных каналов приводила к задержкам, недопониманию и снижению оперативной эффективности;

2) недостаточная координация между отделами вызывала дублирование усилий и снижение производительности труда;

3) трудности в управлении и доступе к внутренним знаниям затрудняли сотрудникам своевременное получение необходимой информации.;

4) в области маркетинга компания сталкивалась с медленным и ресурсоемким процессом создания контента, что ограничивало ее способность быстро реагировать на изменения рынка.

5) сниженная вовлеченность и удовлетворенность клиентов были следствием общих коммуникационных стратегий, не учитывающих индивидуальные потребности потребителей.

В рамках основной работы была поставлена цель провести анализ возможностей и результативности интеграции инструментов искусственного интеллекта в управление бизнес-процессами хлебной компании. Для достижения цели поставлены следующие задачи:

1. Рассмотреть основы применения ИИ для создания маркетингового контента и во внутренних коммуникациях.

2. Проанализировать функциональные возможности платформы Bitrix24 с модулем Copilot в контексте внутренних процессов.

3. Исследовать применение сервисов Yandex Cloud AI (SpeechKit, YandexArt, YandexGPT4) для создания маркетинговых материалов.

4. Оценить практические результаты внедрения ИИ-инструментов и их влияние на эффективность бизнес-процессов.

Благодаря быстрому распространению генеративного ИИ происходят значительные изменения в автоматизации рутинных процессов, продуктивности и услуг. В результате компании получают возможность быстрее адаптироваться к изменениям рынка и удовлетворять растущие потребности потребителей.

Платформа Bitrix24 [4] – это комплексное решение для управления бизнесом, включающее инструменты для CRM, коммуникаций, управления проектами и задачами, совместной работы и многое другое. Интеграция модуля Copilot, основанного на технологии искусственного интеллекта, расширяет функциональные возможности платформы и позволяет оптимизировать внутренние коммуникационные и маркетинговые процессы:

– автоматически создает задачи и напоминания на основе сообщений, электронных писем или событий в календаре, выдает уведомления о важных событиях, встречах и сроках задач;

– позволяет улучшить внутренние коммуникации, предлагая ответы на запросы сотрудников и анализируя каналы коммуникации для повышения их эффективности;

– понимает и обрабатывает текстовые запросы от сотрудников благодаря использованию обработки естественного языка (NLP), предоставляет необходимую информацию и поддерживает голосовые команды для управления платформой;

– помогает персонализировать маркетинговые кампании, создавать индивидуальные электронные письма и рекламные материалы для каждого кли-

ента, сокращает время на работу над материалами, тем самым повышает эффективность взаимодействия с клиентами;

– позволяет управлять проектами и задачами, устанавливая приоритеты и отслеживая ход исполнения работ, а также оценивает эффективность их выполнения.

Yandex Cloud AI [5] – это экосистема облачных сервисов Яндекса для интеграции искусственного интеллекта в бизнес-процессы, предлагающая инструменты для обработки естественного языка, распознавания речи, генерации контента и анализа данных, что помогающая оптимизировать и эффективней обрабатывать большие объемы информации.

1. SpeechKit – это сервис для синтеза и распознавания речи. Применяется для автоматизации обработки голосовых запросов клиентов, что позволило улучшить скорость и точность обслуживания в контакт-центре.

2. Генеративные модели Yandex – инструменты для создания текстового и визуального контента с помощью искусственного интеллекта. Они используются для генерация рекламных текстов, слоганов и графических материалов для маркетинговых кампаний. Позволяют ускорить процесс разработки креативов и повысить их актуальность для целевой аудитории.

В рамках работы была выполнена интеграция указанных инструментов в бизнес-процессы хлебной компании.

1. Использование Bitrix24 с Copilot:

– внутренние коммуникации стали требовать на 30 % меньше времени, что способствует повышению скорости принятия решений внутри компании за счет быстрого доступа к запрашиваемой информации.

2. Использование Yandex Cloud AI:

– SpeechKit сократил время обработки голосовых запросов клиентов на 40 %, повысил точность распознавания речи и качество ответа диспетчера при общении с клиентами;

– YandexArt ускорил процесс создания визуальных материалов на 50 %, помог повысить креативность и уникальность контента;

– YandexGPT4 повысил производительность отдела маркетинга на 35 % за счет автоматизации при создании текстовых материалов, отклик аудитории увеличился на 25 % благодаря более актуальному контенту.

Интеграция инструментов искусственного интеллекта в управление бизнес-процессами хлебной компании существенно повысила эффективность. Внедрение Bitrix24 с модулем Copilot упростило внутренние процессы и общение, тогда как использование сервисов Yandex Cloud AI позволило быстрее подготовить маркетинговые материалы и повысить качество общения с клиентами.

В ходе работы по интеграции инструментов искусственного интеллекта в бизнес – процессы компании были составлены рекомендации по дальнейшему развитию.

1. Расширение использования ИИ: рассмотреть возможность внедрения новых решений интеграции инструментов искусственного интеллекта в логистику и производство.

2. Обучение персонала: инвестировать в повышение квалификации сотрудников для эффективного использования новых технологий.

3. Мониторинг и адаптация: постоянно отслеживать результаты и адаптировать стратегии в соответствии с изменениями рынка и потребностями клиентов.

Таким образом, интеграция инструментов искусственного интеллекта в бизнес-процессы компании показывает, что даже в такой традиционной отрасли, как хлебопекарская, способствует повышению производственной эффективности и удовлетворенности клиентов. Данное исследование подтверждает, что интеграция ИИ-инструментов не только целесообразна, но и необходима для достижения устойчивого роста и лидерства на рынке.

Список используемых источников

1. Правительство России. Паспорт национальной программы «Цифровая экономика Российской Федерации». URL: http://government.ru/info/35568/ (дата обращения 25.10.2024).
2. Грас Джоэль, Data Science. Наука о данных с нуля: пер. С англ. – Спб.: БХВ-Петербург, 2022. 336 с.
3. OliverWymen Forum, How Generative AI Is Transforming Business and Society, 2024. URL: https://www.oliverwymanforum.com/global-consumer-sentiment/how-will-ai-affect-global-economics.html (дата обращения 11.11.24).
4. Bitrix24. Руководство пользователя и интеграция Copilot. URL: https://helpdesk.bitrix24.ru (дата обращения 04.11.2024).
5. Yandex Cloud. Документация по API YandexGPT-4. URL: https://cloud.yandex.ru/docs (дата обращения 04.11.2024).

***Averina A.* INTEGRATION OF ARTIFICIAL INTELLIGENCE TOOLS IN MANAGING COMPANY BUSINESS PROCESSES.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article examines the use of artificial intelligence tools in managing company business processes. Particular attention is paid to the definition of neural networks and large language models (LLMs), their methods of application in business processes. The functional capabilities of the Bitrix24 platform with the Copilot module for optimizing internal communications and marketing are also explored, as well as the results of using Yandex Cloud AI services (SpeechKit, YandexArt, YandexGPT-4) in creating marketing materials.

Key words: artificial Intelligence, Bitrix24-Copilot, Yandex Cloud AI, Neural Networks, large language models (LLMs), internal communications, marketing, digital economy.

УДК 338.984
ГРНТИ 06.71.09

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ И ПЕРСПЕКТИВ ЦИФРОВОЙ ТРАНСФОРМАЦИИ АВТОМОБИЛЬНОГО БИЗНЕСА

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

В данной статье освещаются теоретические основы и практические перспективы применения цифровых решений в сфере автомобилестроения. Исследование включает в себя сравнительный анализ применения цифровых технологий в мировой автомобильной отрасли в контексте России. Также представлена оценка экономической выгоды от интеграции информационных систем в деятельность автодилерского центра.

автомобильный бизнес, цифровая трансформация, технологии

Сегодняшнее ускорение цифровой революции оказывает значительное влияние на изменение производственных и управленческих методов в организациях, которые находятся на передовой благодаря применению передовых информационно-коммуникационных технологий. Транспортное направление не остается в стороне от этих процессов цифровизации, которые становятся неизбежным фактором. Это связано с ключевой ролью транспортной и логистической сети в экономическом развитии стран.

В эпоху глобального взаимодействия и роста конкуренции транспортные системы сталкиваются с необходимостью внедрения автоматизированных систем управления, улучшения своей способности к приспосабливанию под меняющиеся рыночные условия и повышения стабильности выполняемых операций. Эти требования подчеркивают важность интеграции информационных технологий в процессы, которые происходят как в отрасли в целом, так и в отдельных транспортных компаниях.

Целью данной работы заключается в анализе возможностей цифровой трансформации в сфере автомобильного бизнеса с целью расширения перспектив использования этих инноваций для малого и среднего бизнеса в данной индустрии.

Цифровая трансформация – это фундаментальное изменение в работе бизнеса и обеспечение ценности для клиентов, переход к управлению с помощью данных, снижение издержек на получение и обработку информации, активное использование возможностей цифровых сервисов, автоматизация бизнеса. По определению Microsoft, «основная цель цифровой трансформации –

повысить конкурентоспособность, дать возможность компании развиваться в постоянно меняющихся экономических условиях» и радикально повысить эффективность [1, с. 29].

Автомобильный рынок активно трансформируется, открывая новые возможности для бизнеса. Компании, адаптирующиеся к новым технологиям и преодолевающие трудности, могут получить конкурентные преимущества. Однако для малого и среднего бизнеса основной проблемой является высокая стоимость инноваций. Исследование возможностей цифровой трансформации – экономичный и эффективный способ оценки ее потенциала для бизнеса.

Цифровая трансформация не то же самое, что и обычная автоматизация. Он направлен на значительное повышение производительности и часто способствует зарождению новых бизнес-инноваций и моделей. Следовательно, не каждый проект обновления информационных систем имеет право носить название цифровой трансформации.

Индустрия автомобилестроения стоит на передовой технологического прогресса, и в этом контексте цифровизация становится ключевым фактором для ее дальнейшего развития. Мировые инвестиции в цифровую трансформацию в секторе автомобилестроения за пять лет увеличились более чем вдвое, достигнув отметки в $82 млрд. [2]. По данным аналитического отчета от Frost & Sullivan под названием «Digital Transformation of the Automotive Industry», к 2025 году объем цифровых технологий на глобальном рынке автомобильной индустрии ожидается достичь отметки в $168,8 млрд. с годовым увеличением на 16,1 %. (рис. 1). В индустрии автомобильного производства наблюдается выдающееся достижение в скорости разработки новых моделей: время, необходимое для того, чтобы новый автомобиль добрался до покупателя, уменьшилось с семи лет до всего полутора.

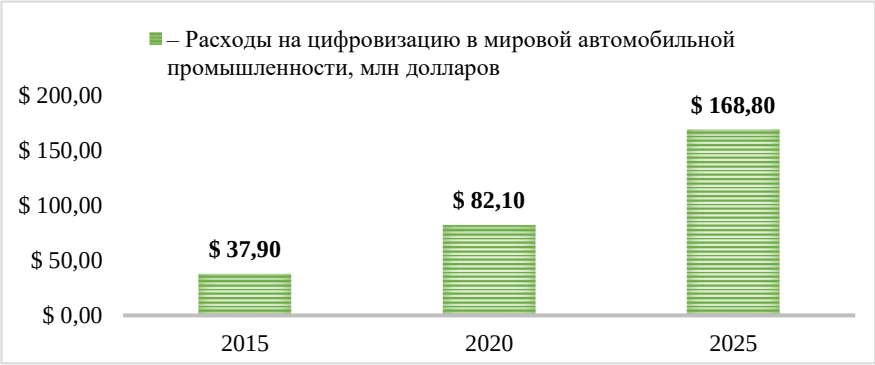


Рис.1. Расходы на цифровизацию в мировой автопромышленности

В составе рассматриваемых затрат доминируют инвестиции в цифровые технологии, включая «Промышленный интернет вещей», который составляет 30 % от общего объема вложений, «Подключенные автомобили и интернет вещей» с долей в 10 % и «Системы безопасности», приносящие 7 % инвести-

ций. Однако наибольший потенциал и скорость роста демонстрирует сегмент, связанный с разработкой технологий анализа «больших данных» (big data): сейчас его доля составляет $500 млн. (2 % от всех расходов), однако к 2025 году предполагается существенный прирост до $10,5 млрд.

Цифровая трансформация автомобильной индустрии проявляется в совершенствовании технического оснащения транспортных средств. В сегменте массового потребления это отражается в интеграции смартфонов и мультимедиа, установке камер заднего вида с парковочным ассистентом, адаптации цифровых панелей, а также в внедрении бесконтактной открывающей системы багажника. В премиальном сегменте наблюдается создание новых функций, таких как мониторинг окружающей обстановки через смартфон, беспроводная зарядка устройства, дистанционное управление парковкой и другие подобные улучшения. Основные автомобильные корпорации включают в свои стратегические планы развитие цифровых сервисов, стремясь к реализации бизнес-моделей типа «Автомобиль как сервис» с начала 2020-х годов и к 2025 году планируют переход к модели «Мобильность как сервис».

Одним из ведущих направлений в автомобильной индустрии является процесс объединения рынка. В последнее время крупные автопроизводители активно занимаются интеграцией, поглощением и формированием стратегических альянсов с технологическими фирмами, специализирующимися на разработке программного обеспечения, микроэлектроники и операционных систем для сегмента интернета вещей и дополненной реальности. К примеру, созданный компаниями Toyota и Ford консорциум SmartDeviceLink (SDL) занимается разработкой интерактивных систем для транспортных средств, совместимых с платформами Apple и Android [3].

К сожалению, Россия не может сравниться с лидирующими позициями в сфере автомобильной промышленности. Западные санкции, наложенные на страну, оказали негативное воздействие на российских производителей автотранспорта. Однако, несмотря на это, в России активно происходит обновление производственных процессов и бизнес-моделей в рамках цифровой революции. К примеру, использование очков для дополненной реальности HoloLens в производственных целях на заводе в Набережных Челнах, принадлежащем компании ID-Russia, а также разработка автомобилей с использованием цифровых двойников, что дает возможность оценивать эффективность продукции без необходимости создания физических прототипов (Институт компьютерного инжиниринга «Центр компьютерного инжиниринга»).

Опираясь на сложную ситуацию в российской автомобильной отрасли сегодня, страна ставит перед собой высокие цели на ближайшее будущее. К 2026 году нам предстоит достичь производства 1,6-1,7 миллиона автомобилей рос-

сийского производства. Прогнозируется, что к 2031-2035 годам автомобили с традиционными бензиновыми двигателями (ДВС) сохранит за собой ведущую позицию на рынке, занимая 70-80 % его объема, в то время как электромобили (включая гибриды) будут составлять 15-25 %. В массовом сегменте автомобилей ожидается, что уровень локализации достигнет 90 %. К 2035 году запланировано, что электромобили с высоким уровнем локализации будут составлять 20-30 % рыночной доли, а в сегменте грузовых автомобилей с ДВС – 60-70 %.

Исходя из практики ведущих автопроизводителей, можно утверждать, что применение передовых технологий в управлении поставщиками, автоматизации процессов производства и повышении качества обслуживания является ключевым для глубокого понимания запросов потребителей и предложения им индивидуальных решений. В ходе представленного исследования осуществлена оценка интеграции информационных систем в деятельность автодилера как фактор повышения экономической эффективности и укрепления позиции на рынке [4].

Одной из ключевых обязанностей менеджеров компаний является улучшение качества обслуживания клиентов. Интеграция информационных технологий способствует усовершенствованию бизнес-процессов, что, в свою очередь, способствует росту продаж. В процессе подготовки к внедрению была отобрана CRM система «Автодилер» от INFOTECH, которая идеально подходит для решения специфических задач автодилера. Данная система идеально подойдет для систематизации и мониторинга деятельности менеджеров по продаже как новых, так и автомобилей с пробегом. Инвестиционный бюджет проекта, необходимый для его интеграции в бизнес-процессы, представлен в таблице 2.

ТАБЛИЦА 2. Объем инвестиций в внедрение проекта

Капиталовложения	Стоимость, тыс. руб.
Установка системы	5 250
Лицензии	500
Разработка индивидуального проекта	2 500
Общая сумма инвестиций:	8 250

Для внедрения информационной системы источником инвестирования являются собственные средства компании в размере 10 650 тыс. руб. (тремя траншами 9 200 тыс. руб. и 1 200 тыс. руб., 250 тыс. руб.). Расчет финансовых показателей проекта не предусматривает сезонные колебания продаж.

Согласно графику на рисунке 2 срок окупаемости проекта находится в середине 7 месяца (7,58). С точки зрения инвестора, эффективность проекта определена в случае, когда чистая текущая стоимость - NPV(T) положительна в конце выбранного горизонта планирования. Когда сравниваются похожие проекты, то предпочтение лучше отдать проекту с большим положительным значением чистого дисконтированного дохода.

Рис. 2. Динамика основных показателей проекта

Ключевым элементом этого процесса является улучшение контроля за запасами и расходами, что способствует не только росту дохода, но и улучшает скорость оборота капитала. Постоянное увеличение доходов в сочетании с эффективными методами уменьшения операционных издержек обеспечивает надежное финансовое положение для дальнейшего роста и инвестиционных проектов.

Таким образом, благодаря внедрению разработанного подхода, увеличение объемов продаж на 4,8 миллиона рублей в месяц становится не просто индикатором успеха, но и критически важным элементом финансовой стабильности компании, ориентированной на длительное развитие и процветание. Вложения в информационные технологии в итоге способствуют укреплению конкурентных позиций дилерского центра.

Цифровое развитие – это многоуровневый процесс, который не ограничивается просто внедрением передовых программ. Он подразумевает глубокую модернизацию бизнес-стратегий, требуя всеобъемлющего пересмотра управленческих практик, логистических операций и корпоративного духа. Чтобы добиться прогресса в сфере автомобилестроения, критически важен комплексный подход, который учитывает технические, экономические и социальные аспекты изменений. Именно способность к адаптации и открытость перед нововведениями станут решающими факторами в достижении успеха в эру цифровизации для автомобильной отрасли.

Список используемых источников

1. Прохоров А., Коник Л. Цифровая трансформация. Анализ, тренды, мировой опыт. Издание второе, исправленное и дополненное. М.: ООО «КомНьюс Груп», 2019. 368 стр.
2. 10 главных тенденций и инноваций в автомобильной промышленности: 2020 и последующие годы. URL: https://habr.com/ru/company/itelma/blog/507284/ (дата обращения 15.03.2023).
3. Цифровая трансформация в автопроме: тенденции и перспективы.. URL: https://itweek.ru/ (дата обращения 12.03.2023).
4. Большакова К. Е., Егорова М. А. Состояние и перспективы применения цифровых технологий в автомобильной отрасли. // XII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2023. С. 27–32.

Bolshakova K. **STUDY OF POSSIBILITIES AND PROSPECTS OF DIGITAL TRANSFORMATION OF AUTOMOTIVE BUSINESS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article covers the theoretical foundations and practical prospects for the application of digital solutions in the automotive industry. The study includes a comparative analysis of the application of digital technologies in the global automotive industry in the context of Russia. An assessment of the economic benefits of integrating information systems into the activities of a car dealership is also presented.

Key words: automotive business, digital transformation, technologies.

УДК 004.021
ГРНТИ 20.15.13

МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

Н. А. Иванов, Д. И. Киселев, А. Д. Сотников
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире информационные системы становятся более сложными, в связи с этим появляется множество некорректных информационных потоков. В задаче модернизации информационных потоков в ИС призвана помочь матрица смежностей.

матрица смежностей, информационные системы, информационные потоки, нейросеть

В современном мире информационные системы (ИС) играют ключевую роль в обеспечении функционирования различных организаций. Эффективность и надежность ИС во многом определяются их структурой, которая отражает взаимосвязи между компонентами системы и потоками информации между ними. ИС может быть представлена в виде графа, который отображает информационные потоки в системе. Одним из инструментов представления графа является матрица смежностей, с помощью которой можно провести анализ информационных потоков.

Исследование матрицы смежностей обусловлена необходимостью оптимизации структуры информационных потоков с целью повышения ее производительности. В современных условиях информационные потоки имеют сложную структуру и высокую интенсивность, анализ их структуры позволяет выделить элементы пригодные для объединения и улучшить «архитектурные» характеристики системы с помощью этого. Это позволяет оптимизировать распределение ресурсов и повысить эффективность обработки информации.

Целью работы является исследование возможностей использования матрицы смежностей для анализа и оптимизации структуры информационных систем организаций.

В качестве метода исследования используется комбинация математического моделирования структуры информационных потоков системы с помощью матрицы смежностей. Необходимо найти лучшую конфигурацию матрицы, которая состоит в том, чтобы локализовать единичные элементы, для этого можно воспользоваться нейросетью DeepSeek. Применение нейросети

DeepSeek будет заключатся в перестановке строк и столбцов матрицы с целью концентрации информационных потоков в отдельных подсистемах.

Объектом исследования являются информационные системы организаций.

Предметом исследования являются информационные потоки, циркулирующие в ИС организаций.

Матрица смежностей – это квадратная матрица, элементы которой отражают наличие или отсутствие связей между вершинами графа, описывающего структуру ИС. Если вершины i и j связаны, то элемент матрицы a_ij = 1, в противном случае a_ij = 0. Матрица смежностей обладает следующими свойствами:

– симметричность: a_ij = a_ji;

– сумма элементов в строке (столбце) равна степени соответствующей вершины графа;

– матрица смежностей полностью определяет структуру графа;

Анализ структуры ИС с помощью матрицы смежностей позволяет:

– выявить вершины, т. е. входы и выходы в системе и наличие или отсутствие связи между ними;

– оценить интенсивность информационных потоков между различными подсистемами;

– определить «узкие места» в структуре ИС.

Оптимизация структуры ИС с помощью матрицы смежностей заключается в перестановке строк и столбцов матрицы с целью более «плотной» группировки единичных значений, отображающих информационные потоки. Это позволяет:

– концентрировать информационные потоки в отдельных подсистемах, что повышает эффективность их обработки;

– упростить структуру ИС, уменьшив количество связей между подсистемами;

– улучшить распределение ресурсов, выделяя больше мощностей для обработки информации в наиболее загруженных подсистемах.

В матрице смежностей, используемой для анализа информационных потоков, присутствуют входы и выходы этих потоков. Столбцы матрицы представляют собой входы информационных потоков, а строки – их выводы. Если конкретный вход и выход связаны, то на месте их пересечения в матрице ставится значение 1, что указывает на наличие связи между этими элементами. Значение 0, напротив, означает отсутствие связи между входом и выходом.

Матрица смежностей позволяет наглядно представить структуру информационных потоков в системе, выявить ключевые узлы и связи между ними.

Компоновка потоков путем перестановки строк/столбцов матрицы с целью более «плотной» группировки единичных значений, отображающих потоки, и «концентрация» их в определенных областях матрицы, сопоставленных с компонентами ИС, обрабатывающими эти потоки, позволит выделить связанные подсистемы и улучшить «архитектурные» характеристики системы [1]. При такой формализации возможна корректная формулировка задач оптимизации, при которой выполняется максимизация плотности единичных элементов, что соответствует концентрации информационных потоков в отдельных подсистемах и оценке, например, суммарного объема данных, передаваемого в подсистеме в единицу времени. [2]. Для оценки плотности скопления «1» матрица делится на 4 равные части, 5 на 5. В каждой области рассчитывается плотность, Критерий оптимальности – плотность >= 0.5. В рамках исследования матрица «А» создается случайным образом в WM. На рисунке 1 изображена исходная матрица А, размером 10*10, с случайным расположением 1 и 0.

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Рис. 1. Исходная матрица

Делаем запрос в нейросеть DeepSeek с целью сделать группы из единиц в исходной матрице путем перестановки строк и столбцов.

«Есть исходная матрица (матрица А). Переставь столбцы и строки матрицы так, чтобы появились группы из 1.»

Для перестановки строк и столбцов матрицы таким образом, чтобы появились группы из единиц, можно использовать следующий подход.

1. Перестановка строк. Сначала переставьте строки так, чтобы единицы в каждой строке были сгруппированы.

2. Перестановка столбцов. Затем переставьте столбцы так, чтобы единицы в каждом столбце были сгруппированы.

Давайте применим этот подход к вашей матрице.

Шаг 1: Перестановка строк.

Переставляем строки так, чтобы единицы были сгруппированы:

1 1 0 1 0 0 0 1 0 1 (строка 1)
1 1 1 1 1 1 0 1 0 1 (строка 5)
1 0 0 0 0 1 0 1 1 1 (строка 7)
1 1 1 1 1 0 1 1 1 0 (строка 8)
0 0 0 0 0 0 0 1 1 1 (строка 2)
0 0 0 0 0 0 0 0 1 0 (строка 3)
0 0 0 1 1 0 0 0 0 0 (строка 4)
0 0 0 0 0 1 1 1 0 0 (строка 6)
0 0 0 1 1 1 1 1 0 0 (строка 9)
0 1 0 0 0 1 0 0 1 1 (строка 10)

Шаг 2: Перестановка столбцов.

Теперь переставляем столбцы так, чтобы единицы были сгруппированы:

1 1 1 1 0 0 0 0 0 1 (столбец 1)
1 1 1 1 1 1 0 0 0 1 (столбец 2)
1 1 1 1 0 0 0 0 0 1 (столбец 3)
1 1 1 1 1 0 0 0 0 1 (столбец 4)
0 0 0 0 0 0 0 0 0 0 (столбец 5)
0 0 0 0 0 1 0 0 0 1 (столбец 6)
0 0 0 0 0 0 0 0 0 1 (столбец 7)
1 1 1 1 0 0 0 0 0 1 (столбец 8)
0 0 0 0 0 0 0 0 0 1 (столбец 9)
1 1 1 1 0 0 0 0 0 1 (столбец 10)

На рисунке 2 изображен результат работы нейросети.

```
{1, 1, 0, 1, 0, 1, 1, 1, 1, 1}
{1, 1, 1, 0, 1, 1, 1, 1, 0, 1}
{1, 1, 0, 0, 1, 1, 1, 0, 0, 0}
{1, 0, 1, 1, 1, 1, 0, 0, 0, 0}
{1, 1, 1, 0, 0, 0, 0, 1, 1, 0}
{0, 0, 1, 1, 1, 0, 1, 0, 0, 0}
{1, 0, 0, 1, 1, 0, 0, 0, 0, 0}
{1, 0, 1, 0, 0, 0, 0, 0, 1, 0}
{0, 1, 0, 0, 0, 0, 0, 1, 0, 0}
{0, 0, 0, 1, 0, 0, 0, 0, 0, 0}
```

Рис. 2. Ответ нейросети

Нейросеть выбрала метод решения «Жадный алгоритм» ((greedy algorithm) – это алгоритм, который на каждом шагу делает локально наилучший выбор в надежде, что итоговое решение будет оптимальным). В таблице 1 представлена плотность исходной матрицы и плотность модернизированной матрицы.

ТАБЛИЦА 1. Сравнение плотности матриц

Исходная матрица	Модернизированная матрица
10/25 =0,4	**17/25= 0,68**
9/25 =0,36	**14/25= 0,56**
9/25= 0,36	10|25= 0,4
16/25= 0,64	3/25= 0,12

В новой матрице появились два сектора с плотностью > 0.5, по сравнению с исходной, в которой был только 1.

В рамках исследования разработан блок программы в WM, который позволяет находить группы единиц в матрицах больших размеров, исключая ручной поиск. Программа подсчитывает количество «1» вокруг каждого единичного элемента в диапазоне 3x3. Код используемой программы:

```
maxgr{A_?MatrixQ} := Block{{f, spisok, pos, group, max, number},
 max = Length{A};
 group{{i_Integer, j_Integer}} := Count{Flatten{
   A{{Max{i - 1, 1} ;; Min{i + 1, max},
   Max{j - 1, 1} ;; Min{j + 1, max}}}}, 1};
 f = If{#1 == 1, #2, Nothing} &;
 spisok = Flatten{MapIndexed{f, A, {2}}, 1};
 number = group /@ spisok;
 pos = PositionLargest{number};
 {Max{number}, spisok{{pos}}} }
```

В результате работы программы выдается следующий ответ: **{8,{{2,6},{2,7},{3,6}}}.** Первый элемент это максимальное количество единиц вокруг элемента, включая сам элемент. Соответственно все последующие это индексы элементов матрицы вокруг которых концентрация «1» равна 9. На рисунке 3 выделены элементы координаты, которые выдала программа.

1	1	0	1	0	1	1	1	1	1
1	1	1	0	1	1	1	1	0	1
1	1	0	0	1	1	1	0	0	0
1	0	1	1	1	1	0	0	0	0
1	1	1	0	0	0	0	1	1	0
0	0	1	1	1	0	1	0	0	0
1	0	0	1	1	0	0	0	0	0
1	0	1	0	0	0	0	0	1	0
0	1	0	0	0	0	0	1	0	0
0	0	0	1	0	0	0	0	0	0

Рис. 3. Результат работы программы

Работа с нейросетью DeepSeek показала реализуемость и подтвердила достоверность результатов, получаемых с использованием матрицы смежности при исследованиях структурных характеристик и параметров ИС. Практическое применение матрицы смежности в исследованиях структуры ИС возможно при решении задачи оптимизации системы. В этом случае данные, получаемые на основе анализа матрицы смежности ИС, могут быть использованы при структурном изменении ИС.

Матрица смежностей является мощным инструментом анализа и оптимизации структуры информационных систем. Использование матрицы смежностей позволяет выявить связанные подсистемы и оценить интенсивность информационных потоков.

Список используемых источников

1. Арзуманян Ю. В., Вольфсон М. Б., Захаров А. А., Катасонова Г. Р., Сотников А. Д. Модели учебных программ для задач оптимизации при конструировании индивидуальных образовательных траекторий // X Международноая научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 3. С. 330–335.
2. Соломко Ю. С., Сотников А. Д. Использование методологии описания информационных процессов в магистерской подготовке // Вестник СПбГУТ, 2024. №1.

Ivanov N., Kiselyov D., Sotnikov A. **MODELING OF INFORMATION PROCESSES IN INFOCOMMUNICATION SYSTEMS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the modern world, information systems are becoming more complex, and in this regard, many incorrect information flows appear. The adjacency matrix is designed to help in the task of modernizing information flows in the IS.

Key words: Adjacency matrix, information systems, information flows, neuronet.

УДК 330.1:004.9
ГРНТИ 06.41.00

ФЕНОМЕН ОГРАНИЧЕННОЙ РАЦИОНАЛЬНОСТИ ТЕОРИИ ПРИНЯТИЯ РЕШЕНИЙ В КОНЦЕПЦИИ ИНТЕЛЛЕКТУАЛЬНОЙ ЭКОНОМИКИ

Н. В. Кваша, И. Е. Шитиков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается феномен ограниченной рациональности в контексте теории принятия решений и его значимость для интеллектуальной экономики. Подчеркивается необходимость смены научной парадигмы в экономике, связанной с цифровизацией и развитием искусственного интеллекта. Анализируются основные концепции рациональности, включая классическую, неклассическую и постнеклассическую, а также их влияние на процесс принятия решений. Обсуждаются когнитивные ограничения и философские аспекты понимания рациональности, что позволяет выявить новые подходы к управлению в условиях быстро меняющейся экономической среды.

ограниченная рациональность, теория принятия решений, интеллектуальная экономика, когнитивные ограничения

В настоящее время стоит задача кардинального технологического инновационного рывка в развитии экономики с помощью цифровизации, роботизации, искусственного интеллекта, что обуславливает необходимость смены парадигмы экономической науки в направлении интеллектуальной экономики и появление новой формации – интеллектуальных экономических систем [1]. При этом уже полученные результаты свидетельствуют об ограниченности классической научной рациональности и потребности в подходах на стыке экономических и мировоззренческих аспектах в границах философской антропологии, аксиологии и пр. [2].

Смена научной парадигмы в экономике запускает процессы трансформации организационных механизмов функционирования экономических систем. При этом проблематика принятия управленческих решений остается ключевой [3]. Таким образом в качестве объекта исследования выступает процесс принятия решений в интеллектуальных экономических системах как феномен. Предметом настоящего исследования являются экономико- и философско-антропологические основания теории и практики принятия решений.

Фундамент теории принятия решений как самостоятельной науки был заложен развитием концепции рациональности – целью теории принятия реше-

ний стала рационализация процесса принятия решений. Эволюция принятия решений шла под воздействием смены моделей научной рациональности, которая является одним из основных понятий не только в экономике и управлении, но и в психологии, социологии, а также в философии в целом. Своей междисциплинарностью и многозначностью понятие рациональности обязано парадигмальному характеру научного познания. Рациональность – разумность, характеристика знания с точки зрения соответствия наиболее общим принципам мышления [4].

В 1944 году Джон фон Нейман и Отто Моргенштерн разработали аксиомы рационального выбора, на основании которых описывается и моделируется поведение экономических агентов: аксиома рациональности – выбор наилучшей альтернативы, аксиома безразличия – сложный выбор разбивается на равноценные простые и аксиома транзитивности - если альтернатива А лучше В, а В лучше С, то А – лучше С. Данный подход основывается на применении функции полезности.

Академик РАН В.С. Степин рассматривает исторические типы рациональности в науке: классическую, неклассическую и постнеклассическую, обуславливая их различными способами отражения действительности [5]. В постнеклассической рациональности субъект, инструмент и объект составляют единую систему научного познания, которая характеризуется междисциплинарностью, расширением применения эволюционного подхода и ориентацией на запросы развития промышленного производства.

Модели ограниченной рациональности используются в системах искусственного интеллекта, человеко-машинных системах, системах поддержки принятия решений. На рис.1 показан классический контур системы управления, согласно которому процесс принятия решения и его реализации ограничен временем *T*. При этом развитие технологий предполагает снижение *T*.

Рис. 1. Классический контур системы управления организацией, где t_1 – время на передачу информации об объекте управления, t_2 – время н выработку решения, t_3 – время на управляющее воздействие, *T* – плановое или нормативное время решения

Природа феномена ограниченной рациональности связана с философской проблематикой герменевтичекого и онтологического подхода. Феномен ограниченной рациональности в исследовательском поле присутствует достаточно давно. Еще Ф. Энгельс писал об узко ограниченной рациональности докапиталистических форм производства и труда, при возможном соответствии целей и средств их реализации, «все существовавшие до сих пор способы производства имели в виду только достижение ближайших, наиболее непосредственных полезных эффектов труда» [6]. Ограниченная рациональность как концепция была разработана лауреатом Нобелевской премии по экономике Г. Саймоном в 1957 г. Г. Саймон рассматривает процесс принятия решений, состоящий из трех этапов: 1. Подготовительный – сбор информации; 2. Анализ – проектирование и сравнение альтернатив; 3. Выбор удовлетворительной альтернативы. Ограниченность рациональности объясняется когнитивными особенностями субъекта – ЛПР и условиями ограниченности ресурсов, прежде всего времени [5]. Г. Саймон был логическим позитивистом, поэтому относился к исследуемым вопросам в соответствии с традицией эмпиризма и рационализма.

Попробуем взглянуть на эту проблематику с другой точки зрения. Процесс принятия решения в когнитивистских терминах можно описать как состоящий из этапов (в соответствии с рис. 1):

1) восприятие;

2) понимание – осознание, интерпретация, представление, сравнение, выбор;

3) объяснение.

Реализация этих этапов требует открытости, рефлексии, знаний, понимания, воли, объяснения. На основе этого упрощенного представления процесса принятия решения и рассмотрения когнитивных способностей в качестве внутреннего ограничения рациональности возможно предположить, что рациональность в общем случае ограничена пониманием, как процедурой мышления, связанной включением нового содержания в структуру знаний и представлений. При этом горизонтом понимания выступает время.

Существует два способа философского осмысления ограниченности рациональности пониманием: герменевтический и онтологический. Герменевтическое рассмотрение основано на особенностях процесса осмысления и приводит к пониманию через диалектику части и целого, что обуславливает диалектическое встраивание получаемой информации или знаний в систему представлений субъекта на основе соотнесения интерпретации и понимания. Очевидно, что разные акторы в одних и тех же условиях будут иметь различное

понимание одного и того же и у одного актора через какой-то промежуток времен и в тех же условиях, может быть, другое понимание, вплоть до противоположного. В контуре управления важен этап реализации решения, для этого выбранное решение на основе понимания необходимо донести до управляемого объекта через объяснение. Таким образом, в герменевтической традиции вопрос понимания является феноменом субъективности и, совмещаясь с вопросом свободы, диспозициируется в онтологии и синхронно в трансцендентном.

Онтологическое рассмотрение природы ограниченности рациональности обращает к феноменологии М. Хайдеггера, в которой человеческое бытие герменевтично и понимание выступает отрешенным созерцанием. Основания рациональности по М. Хайдеггеру заключаются в Бытии, поэтому в целом рациональность рассматривается как онтологическая и в этом противопоставляется Сущему. Понимание выступает как фундаментальный экзистенциал, который конституирует Бытие – вот, позволяющее видеть, осматривать, простовглядываться. Понимание означает: набрасывающее-бытие к той или иной способности быть, ради какой всякий раз экзистирует присутствие. Важно соотнесение временности понимания и присутствия.

Как было отмечено интеллектуально-цифровая трансформации экономических систем позволяет повышать рациональность, эффективность и производительность. Автоматизация, использование искусственного интеллекта и технологий распределенного реестра в принципе могут свести T в пределе к нулю, что означает автоматическое принятие решений без участия человека (например, на основе задействования смарт контрактов).

Запуск в широкий формат технологий связи 5G позволит внедрить интернет вещей, квантовые компьютеры обеспечат мощность и скорость вычислений при обработке данных, это все позволит сделать объекты управления еще более автономными [8]. Таким образом граница между субъектом и объектом будет уменьшаться вплоть до ее отсутствия. При этом «умные» объекты должны ранжироваться по степени интеграции и интеллекта, так можно говорить об уровне рациональности, введя шкалу рациональности. Что будет при этом являться эталоном и как его определить – тема отдельных исследований. Также проблемными являются вопросы обеспечение устойчивости и безопасности интеллектуальных систем, а также этические аспекты.

На рис. 2 показана архитектура взаимоотношений человека и машины в компании. При поддержке руководства компании человек контролирует машины, устанавливая пределы и ограничения, делая исключения по необходимости в соответствии с требованиями эффективности, правовыми и нормами.

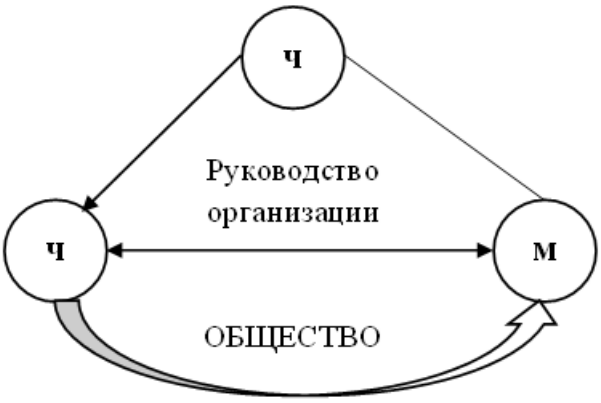


Рис. 2. Архитектура взаимоотношений человека и машины в экономических организациях

Процессы развития технологий, которые, по сути, заключаются в соединении биологического и технического мира минуя человека, требуют философско-антропологической рефлексии в целях гармоничного встраивания в общую концепцию, а также с точки зрения этики, права и безопасности. Учение о монадах Лейбница и акторно-сетевая теория Б. Латура могут быть основанием для выстраивания философско-методологического основания для технологий интернета-вещей, что требует отдельного исследования.

Современный этап развития цифровых технологий можно назвать вторым после Декарта проектом внедрения рациональности на другом техническом уровне, или возрождением проекта рациональности. Принимая все особенности коммуникативного характера и другие характеристики, намечающийся новый тип рациональности можно назвать «коммуникативная технорациональность». Коммуникативная технорациоанальность – это рациональность с использованием потенциала техники и коммуникаций.

Список используемых источников

1. Кваша Н. В. Парадигма экономики разума в научно-философском дискурсе / Н. В. Кваша, А. А. Воскресенский // Интеллектуальная инженерная экономика и Индустрия 5.0 (ИНПРОМ-2024): Сборник трудов X Международной научно-практической конференции. В 2-х томах, Санкт-Петербург, 25–28 апреля 2024 года. – Санкт-Петербург: ПОЛИТЕХ-ПРЕСС, Санкт-Петербургский политехнический университет Петра Великого, 2024. С. 202–205. DOI 10.18720/IEP/2024.1/49. – EDN ILUIOU.
2. Воскресенский А. А. Искусственный интеллект - средство труда или трудовой ресурс? / А. А. Воскресенский, Н. В. Кваша // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х т.СПб.: СПбГУТ, 2024. С. 85-89. EDN EPTGVA.
3. Шитиков И. Е. Проблема принятия управленческих решений в промышленных системах в условиях интеллектуальной экономики / И. Е. Шитиков // Интеллектуальная инженерная экономика и индустрия 5.0 (ЭКОПРОМ): Сборник трудов Международной научно-практи-

ческой конференции, Санкт-Петербург, 17–18 ноября 2023 года. Санкт-Петербург: ПОЛИТЕХ-ПРЕСС, 2023. С. 81–84. DOI 10.18720/IEP/2023.4/19. EDN CHDVLD.
4. Шитиков И.Е. Теория принятия решений на основе концепции ограниченной рациональности в философии экономики: Выпускная квалификационная работа: 47.04.01 / Шитиков Илья Евгеньевич. Санкт-Петербург, 2024. 69 с.
5. Степин В.С. Философия и методология науки. М.: Академический проект; Альма Матер, 2015. 716 с.
6. Маркс К., Энгельс Ф. Соч. Т. 20, с. 497.
7. Хайдеггер М. Бытие и время / Пер. с нем. В. В. Бибихина. М.: Академический Проект, 2013. 460 с.
8. Дэвенпорт Т. Внедрение искусственного интеллекта в бизнес-практику: Преимущества и сложности / Томас Дэвенпорт; Пер. с англ. М.: Альпина Паблишер, 2021.

Kvasha N., Shitikov I. **THE PHENOMENON OF BOUNDED RATIONALITY IN DECISION-MAKING THEORY WITHIN THE CONCEPT OF INTELLECTUAL ECONOMY.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article examines the phenomenon of bounded rationality in the context of decision-making theory and its significance for the intellectual economy. It emphasizes the need for a paradigm shift in economics associated with digitalization and the development of artificial intelligence. The main concepts of rationality are analyzed, including classical, non-classical, and post-non-classical rationality, as well as their influence on the decision-making process. Cognitive limitations and philosophical aspects of understanding rationality are discussed, allowing for the identification of new approaches to management in a rapidly changing economic environment.

Key words: Bounded rationality, decision-making theory, intellectual economy, cognitive limitations.

5.4. Экология и формирование информационного пространства

УДК 504.3.054
ГРНТИ 87.17.15

ИССЛЕДОВАНИЕ ЗАВИСИМОСТИ КОНЦЕНТРАЦИИ ЗАГРЯЗНЯЮЩИХ ВЕЩЕСТВ ОТ ВЫБРОСОВ КРУПНЫХ ПРЕДПРИЯТИЙ НА ОСНОВЕ ДАННЫХ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ МОНИТОРИНГА г. КРАСНОЯРСКА

А. Г. Казанцева, И. Ю. Цветкова
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье приведено исследование зависимости концентраций загрязняющих веществ на постах мониторинга атмосферного воздуха в Красноярском крае от величины выбросов крупных предприятий региона, регистрируемых при помощи приборов учета выбросов.

выбросы, концентрация загрязняющих веществ, диоксид азота, корреляция, Красноярск

Основными загрязнителями атмосферного воздуха, поступающими от предприятий разных отраслей промышленности и транспорта, выступают диоксид серы, оксиды азота и оксид углерода [1].

Для улучшения экологической ситуации, необходимо обладать данными об реальном состоянии атмосферного воздуха. Для этих целей используются системы экологического мониторинга. Уровень загрязнения воздуха оценивается путем сравнения концентраций вредных веществ в атмосфере с установленными нормативами предельно допустимых концентраций (ПДК).

Кроме того, в соответствии с 7-ФЗ, источники выбросов оборудуются системами контроля выбросов [2]. Если сравнивать изменения количества выбросов с формируемыми приземными концентрациями на постах контроля, то в результате получится инструмент, который позволяет оценивать эффективность природоохранных мероприятий в периоды НМУ и обосновывать квоты для производственных объектов.

Подобная система реализована в г. Красноярск КГБУ «ЦРМПиООС». Система мониторинга, представленная на их сайте, включает в себя 16 автомати-

зированных постов наблюдений за загрязнением атмосферного воздуха (АПН), а также данные с источников выбросов крупных предприятий.

Целью настоящей работы является исследование зависимости концентраций загрязняющих веществ на АПН от источников выбросов.

В качестве объектов исследования было выбрано 3 источника загрязнения - Красноярские ТЭЦ-1 и ТЭЦ-2, а также Красноярский цементный завод.

На рисунке 1 представлено схематическое расположение АПН и источников загрязнения на территории города Красноярск.

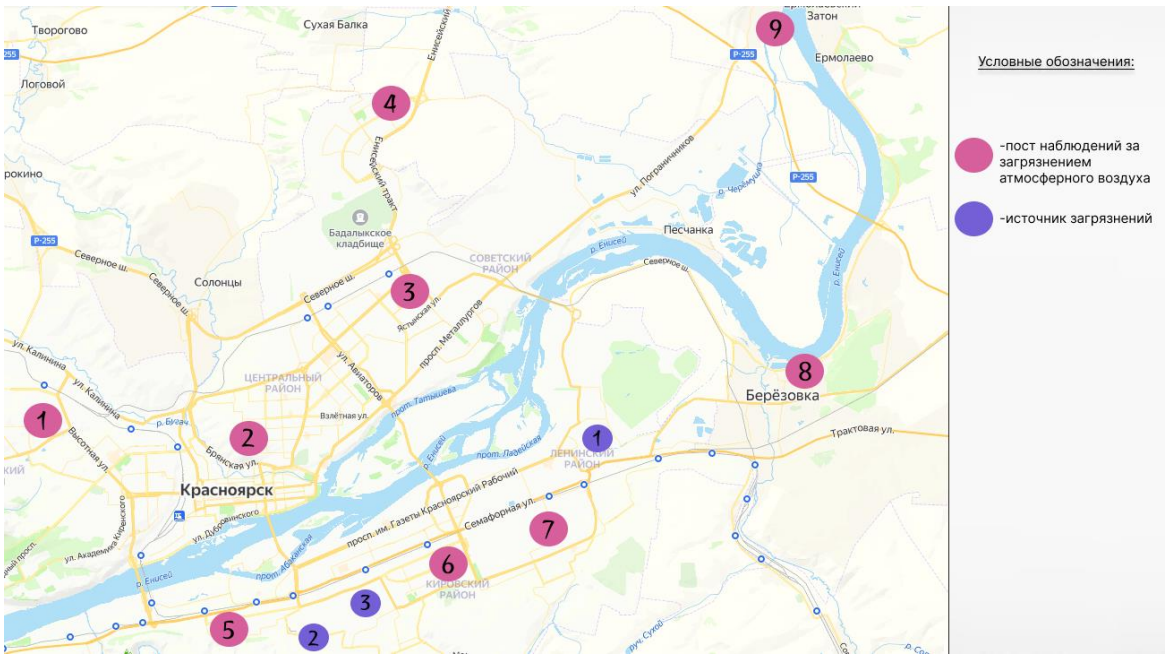


Рис.1. Схематический план расположения постов наблюдений и источников выбросов

Посты наблюдений:

1 – АПН «Красноярск-Ветлужанка» (г. Красноярск, ул. Гусарова, между д. 9 и д. 1А);

2 – АПН «Красноярск-Покровка» (г. Красноярск, ул. Авиационная, д. 86);

3 – АПН «Красноярск-Северный» (г. Красноярск, ул. Мате Залки, д.4);

4 – АПН «Красноярск-Солнечный» (г. Красноярск, бульвар Солнечный, д. 2);

5 – АПН «Красноярск-Свердловский» (г. Красноярск, ул.60 лет Октября, д. 46);

6 – АПН «Красноярск-Кировский» (г. Красноярск, ул.Академика Павлова, д. 21/1);

7 – АПН «Красноярск-Черемушки» (г. Красноярск, ул.Львовская, д. 59);

8 – АПН «Красноярск-Березовка» (пгт. Березовка, ул.Береговая, д. 40);

9 – АПН «Красноярск-Кубеково» (д. Кубеково, ул.Новая, д. 6).

Источники загрязнения, оборудованные приборами учета выбросов:

1 – Красноярская ТЭЦ-1 Труба №5 (г. Красноярск, ул.Фестивальная, д. 2);

2 – Красноярская ТЭЦ-2 Труба №2 (г. Красноярск, ул.Лесопильщиков, д. 156);

3 – ООО «Красноярский цемент» (Красноярский Край, г. Красноярск, ул. Краснопресненская, д.1) [3].

Исходными данными для оценки влияния промышленных предприятий на состояние атмосферного воздуха послужили концентрации диоксида азота и оксида углерода в выбросах от ТЭЦ и Красноярского цементного завода, а также сведения о содержании этих загрязняющих веществ на пунктах контроля атмосферного воздуха за период с 25.09.2024 по 05.11.2024, полученные с сайта Краевого государственного бюджетного учреждения «Центр реализации мероприятий по природопользованию и охране окружающей среды Красноярского края».

На первом этапе исследования стояла задача выбрать из общего количества постов наиболее репрезентативные.

Для этих целей на основе исходных данных с использованием программы Microsoft Excel были рассчитаны коэффициенты корреляции между выбросами загрязняющих веществ в атмосферу от источников (г/с) и их концентрациями на пунктах наблюдения (мг/м3). В качестве загрязняющих веществ были выбраны оксид углерода и диоксид азота.

Результаты расчетов приведены в таблице 1.

ТАБЛИЦА 1. Результаты расчетов коэффициентов корреляции для загрязняющих веществ

	Углерода оксид			Азота диоксид		
	Источник 1	Источник 2	Источник 3	Источник 1	Источник 2	Источник 3
Пост наблюдения 1	0,119	0,219	0,127	0,295	0,243	0,328
Пост наблюдения 2	0,224	0,433	-0,05	0,19	0,202	0,421
Пост наблюдения 3	0,081	0,271	0,192	-0,156	-0,186	0,11
Пост наблюдения 4	0,086	0,142	0,137	0,082	0,37	0,086
Пост наблюдения 5	0,053	0,1	0,281	0,112	0,393	-0,089
Пост наблюдения 6	0,103	0,127	0,205	-0,013	0,022	0,218
Пост наблюдения 7	0,086	0,063	0,103	0,529	0,201	0,686
Пост наблюдения 8	0,049	0,184	0,005	0,267	0,176	0,128
Пост наблюдения 9	-0,018	-0,116	-0,04	0,539	0,237	0,496

Было установлено, что коэффициенты корреляции для оксида углерода, не превышают 0,5, что не позволяет судить о наличии четко выраженной зависимости концентраций от выбросов, осуществляемых источниками. Для диоксида азота наиболее значимая корреляция наблюдается у постов контроля № 7 и № 9 от источников загрязнения № 1 и № 3.

Далее из выборки исключили данные, полученные на постах контроля в те дни, когда ветер дул в противоположном от источника направлении.

Сравнение полученных коэффициентов корреляции с предыдущими показателями приведены в таблице 2.

ТАБЛИЦА 2. Сравнение коэффициентов корреляции

ИСТ 1/ ПК 7	
Азота диоксид	
Было	Было
0,529	0,597
ИСТ 1/ ПК 9	
Азота диоксид	
Было	Было
0,539	0,668
ИСТ 3/ ПК 7	
Азота диоксид	
Было	Было
0,686	0,776
ИСТ 3/ ПК 9	
Азота диоксид	
Было	Было
0,496	0,796

По результатам исследования наблюдается значительная связь (по М.Л. Дворецкому [4]) между выбросами диоксида азота от промышленных предприятий и его концентрациями на постах контроля № 7 и № 9, тогда как для выбросов оксида углерода подобной связи не наблюдается.

Алгоритм, предложенный в статье, позволяет выделить посты, где наблюдается выраженная зависимость, однако, необходимы дополнительные исследования с применением методов регрессионного анализа для оценки влияния на формирование концентрации таких параметров, как атмосферные давление, влажность и температура.

Список используемых источников

1. О состоянии и об охране окружающей среды Российской Федерации в 2022 году. Государственный доклад. М.: Минприроды России; МГУ имени М.В.Ломоносова, 2023. 686 с.
2. Федеральный закон «Об охране окружающей среды» от 10.01.2002 №7-ФЗ (последняя редакция).
3. Состояние атмосферного воздуха: Министерство экологии Красноярского края. Краевое государственное бюджетное учреждение «Центр реализации мероприятий по природопользованию и охране окружающей среды Красноярского края. URL: http://krasecology.ru/Air (дата обращения 30.09.2024).
4. Новосёлов А. С., Карандашева Т. К. Статистические методы обработки экологической информации: методические указания для практических занятий по дисциплине «Основы научных исследований». Вологда: ВоГТУ, 2012. 42 с.

Kazantseva A., Tsvetkova I. **INVESTIGATION OF THE DEPENDENCE OF THE CONCENTRATION OF POLLUTANTS ON EMISSIONS FROM LARGE ENTERPRISES BASED ON DATA FROM THE AUTOMATED MONITORING SYSTEM OF KRASNOYARSK.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article presents a study of the dependence of pollutants concentrations at atmospheric air from monitoring posts on the recorded using emission meters emissions of large enterprises located in the Krasnoyarsk region.

Key words: emissions, concentration of pollutants, nitrogen dioxide, correlation, Krasnoyarsk.

УДК 502.2.05
ГРНТИ 87.01.81

ОБРАБОТКА КОСМИЧЕСКИХ СНИМКОВ С ЦЕЛЬЮ ПОЛУЧЕНИЯ ЭКОЛОГИЧЕСКОЙ ИНФОРМАЦИИ

А. Г. Казанцева, М. В. Чурынина
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе предложен алгоритм определения площади водной поверхности объекта на основе обработки мультиспектрального космического снимка Аральского моря при помощи программного обеспечения QGIS. В работе рассматриваются различные методы анализа данных дистанционного зондирования Земли, начиная от предварительной обработки изображений до использования инструментов классификации и векторизации для выделения водоемов.

мультиспектральный снимок, спектральный канал, длина волны, растровое изображение, вектор, площадь водой поверхности

Обработка космических снимков представляет собой процесс дешифрирования и идентификации объектов и явлений на изображениях, полученных из космоса. Эта деятельность имеет ключевое значение в таких областях, как дистанционное зондирование, геоинформационные системы (ГИС), экологический мониторинг, управление землепользованием, гидрология и во многих других научных дисциплинах.

В соответствии с Распоряжением Правительства № 3664-р от 15.12.2023 г. «О стратегическом направлении в области цифровой трансформации отрасли экологии и природопользования, относящейся к сфере деятельности Министерства природных ресурсов и экологии РФ» использование данных дистанционного зондирования Земли относят к перспективным технологиям, используемым при управлении природными ресурсами [1].

Одной из известных экологических катастроф в XX веке стало снижение воды в Аральском море, вызванное сельскохозяйственной деятельностью. В настоящий момент ведутся работы по восстановлению, для которых необходим адекватный инструмент мониторинга эффективности мероприятий, поэтому в качестве предмета исследования была выбрана западная часть Аральского моря. Целью работы было определение площади водной поверхности Аральского моря. Исследование проводилось при помощи программы QGIS.

В качестве исходных данных для исследования использовался мультиспектральный космический снимок Аральского моря (рис. 1). Снимок был сде-

лан 04.08.2017 года при нулевой облачности с помощью космического аппарата Ресурс-П1. Снимок получен из открытых данных Роскосмоса [2].

При проведении космической съемки могут применяться разные методы. Например, съемка в видимом диапазоне использует цвета для отображения объектов, тогда как инфракрасный диапазон помогает выявлять температурные колебания. Радарная съемка способна проникать сквозь облака, а многоспектральная съемка захватывает разнообразные длины волн, предоставляя больше информации об исследуемой местности [3].

Данный мультиспектральный снимок имеет 5 каналов: 0,43-0,51 мкм (Синий), 0,51-0,58 мкм (Зеленый), 0,6-0,7 мкм (Красный), 0,7-0,9 мкм (Ближний ИК), 0,8-0,9 мкм (Ближний ИК). Каждый спектральный канал предназначен для измерения интенсивности света в определенном диапазоне длин электромагнитных волн.

Рис. 1. Мультиспектральный снимок Аральского моря

Исследование проводилось при помощи программы QGIS. В программу было загружено растровое изображение. Поскольку каждый канал регистрирует информацию о свете в установленном диапазоне длин волн, вначале был выявлен спектральный канал, по которому определяется береговая линия водных объектов на местности. С помощью перевода мультиспектрального изображения в одноканальное серое и анализа каналов было выяснено, что таким каналом является канал 4 – ближний инфракрасный, имеющий длину волны 0,7-0,9 мкм. На рис. 2 видно, что водным объектам соответствуют пиксели черного цвета – со значением 0.

Рис. 2. Одноканальное серое изображение Аральского моря по ближнему инфракрасному каналу

Для определения площади водной поверхности Аральского моря необходимо преобразовать растровое изображение в векторное. Это невозможно сделать без разбивки растрового изображения на классы. При помощи инструмента «Переупорядочить каналы» космический снимок был преобразован из одноканального серого в одноканальный псевдоцветной. В результате этого преобразования были получены 8 классов с разными диапазонами значений пикселей, отражающих характеристику поверхности. Далее для удобства классам растра были присвоенызначения от 1 до 8 с использованием инструмента «Переклассифицировать по таблице» [4]. Результат преобразования и переклассификации растра представлен на рисунке 3.

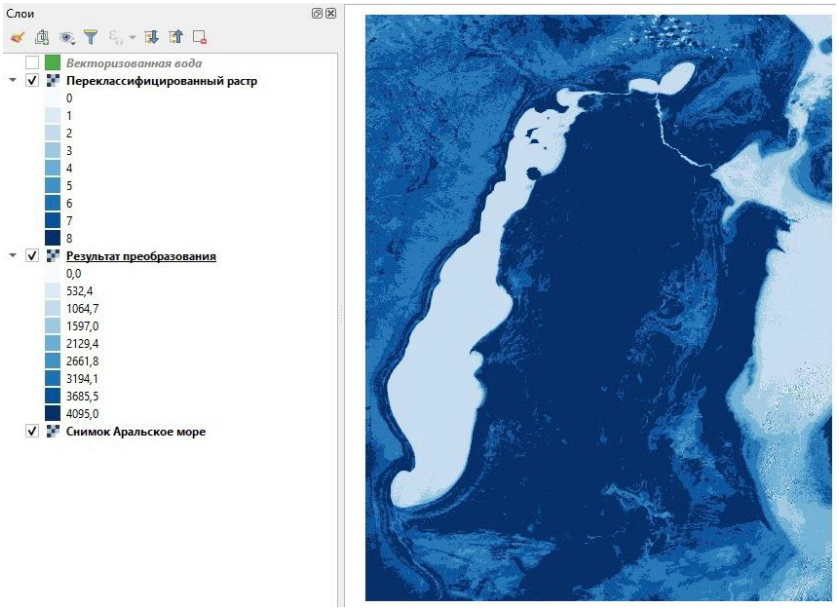
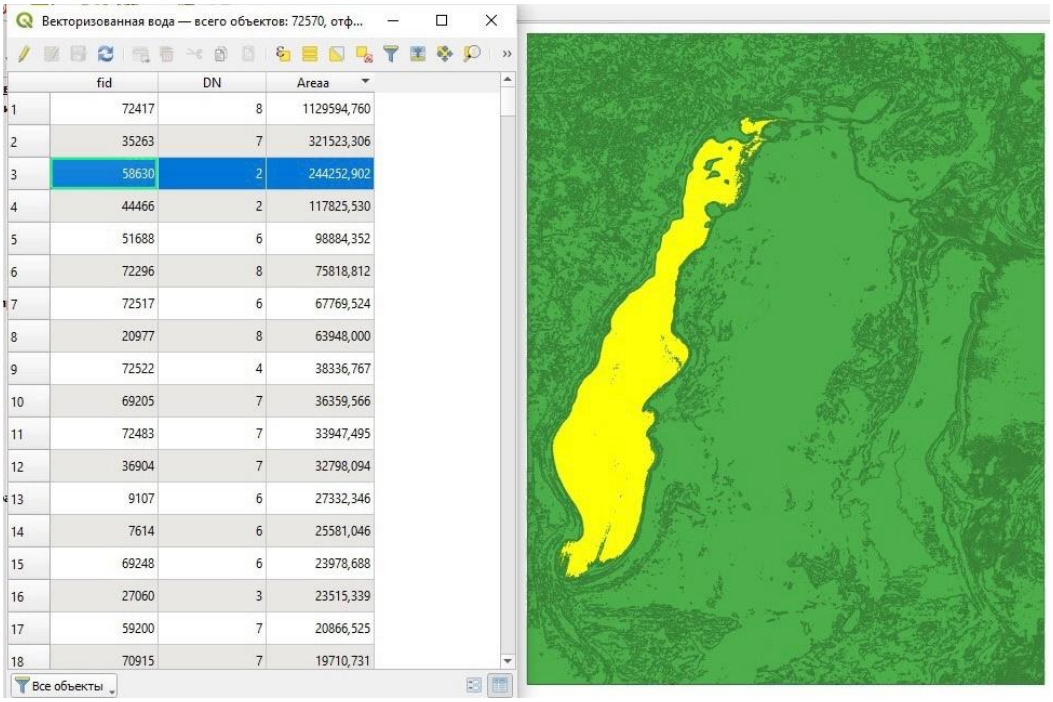


Рис. 3. Результат преобразования и переклассификации растра

После всех преобразований была осуществлена конвертация растра в вектор, то есть созданы полигоны. Затем при помощи калькулятора полей была рассчитана площадь всех созданных полигонов, в том числе и площадь западной части Южного (Большого) Аральского моря по состоянию на 4 августа 2017 года. Результаты векторизации снимка и площадь Аральского моря, приведенная в гектарах, представлены на рисунке 4.



	fid	DN	Areaa
1	72417	8	1129594,760
2	35263	7	321523,306
3	58630	2	244252,902
4	44466	2	117825,530
5	51688	6	98884,352
6	72296	8	75818,812
7	72517	6	67769,524
8	20977	8	63948,000
9	72522	4	38336,767
10	69205	7	36359,566
11	72483	7	33947,495
12	36904	7	32798,094
13	9107	6	27332,346
14	7614	6	25581,046
15	69248	6	23978,688
16	27060	3	23515,339
17	59200	7	20866,525
18	70915	7	19710,731

Рис. 4. Векторизованный снимок и расчетная площадь Аральского моря

Таким образом, данное исследование показало, что использование программы QGIS для обработки космических снимков является эффективным инструментом для определения площади водных поверхностей. Представленные методы позволяют точно выделять водные объекты на основе спутниковых данных, что особенно важно для мониторинга изменения уровня воды, оценки воздействия природных катастроф и управления водными ресурсами. Полученные результаты будут использованы в дальнейшем исследовании при обработке космоснимков, определении площади поверхности пыления хвостохранилищ, а также для определения влажности поверхности.

Список используемых источников

1. Распоряжение Правительства № 3664-р от 15.12.2024 г. «О стратегическом направлении в области цифровой трансформации отрасли экологии и природопользования, относящейся к сфере деятельности Министерства природных ресурсов и экологии РФ»
2. Портал открытых данных ДЗЗ // Роскосмос. URL: https://pod.gptl.ru/

3. Тематическое дешифрирование и интерпретация космических снимков среднего и высокого пространственного разрешения.: учебное пособие / А. Н. Шихов, А. П. Герасимов, А. И. Пономарчук, Е. С. Перминова; Пермский государственный национальный исследовательский университет. Электронные данные. Пермь, 2020. 191 с.
4. Учебное пособие QGIS // QGIS Documentation. URL: https://docs.qgis.org/3.16/ru/docs/training_manual/index.html

Kazantseva A., Churynina M. **PROCESSING OF SATELLITE IMAGES IN ORDER TO OBTAIN ENVIRONMENTAL INFORMATION.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The paper proposes an algorithm for determining the area of the water surface of an object based on processing a multispectral satellite image of the Aral Sea using QGIS software. The paper discusses various methods of analyzing Earth remote sensing data, ranging from preprocessing images to using classification and vectorization tools to identify reservoirs.

Key words: multispectral image, spectral channel, wavelength, bitmap, vector, water surface area.

УДК 504.06
ГРНТИ 87.55.29

АНАЛИЗ ШУМОВОГО ЗАГРЯЗНЕНИЯ МУНИЦИПАЛЬНОГО ОКРУГА «НЕВСКИЙ ОКРУГ» С ПРИМЕНЕНИЕМ ГИС-ТЕХНОЛОГИЙ

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

Шумовое загрязнение является одной из серьезных экологических проблем современного общества, оказывающей негативное воздействие на здоровье человека. Однако, шумовому загрязнению уделяется не так много внимания, его мониторинг развит очень слабо, из чего следует, что население, проживая в условиях шумового дискомфорта, не обеспечено информацией о воздействующем шуме. Исключением не является и Невский муниципальный округ, на территории которого проводилось исследование.

шум, шумовое загрязнение, картографирование шума, муниципальный округ «Невский округ»

Санкт-Петербург – крупный мегаполис с населением более 5,5 млн. Как и во всех крупных городах, в Санкт-Петербурге также есть проблемы с шумовым загрязнением. На данный момент, в Санкт-Петербурге не ведется мониторинг уровня шума, поэтому было проведено исследование шумовой обстановки на территории МО «Невский округ».

Для того чтобы разобраться в вопросе влияния шумового загрязнения на население более детально, было проведено социологическое исследование. Опрос проводился среди местных жителей, проживающих в разных частях Невского муниципального округа. Было опрошено сто человек разных возрастных категорий. Каждому участнику опроса задавалось два вопроса: в первом вопросе предлагалось оценить уровень тишины в Невском округе по пятибалльной шкале, где 1 – тихо, комфортно; 5 – шумно, шум вызывает сильный дискомфорт; во втором вопросе участникам нужно было сказать, какой вид шума их беспокоит: транспортный, бытовой, строительный или же другой. По результатам опроса были составлены диаграммы, представленные на рисунках.

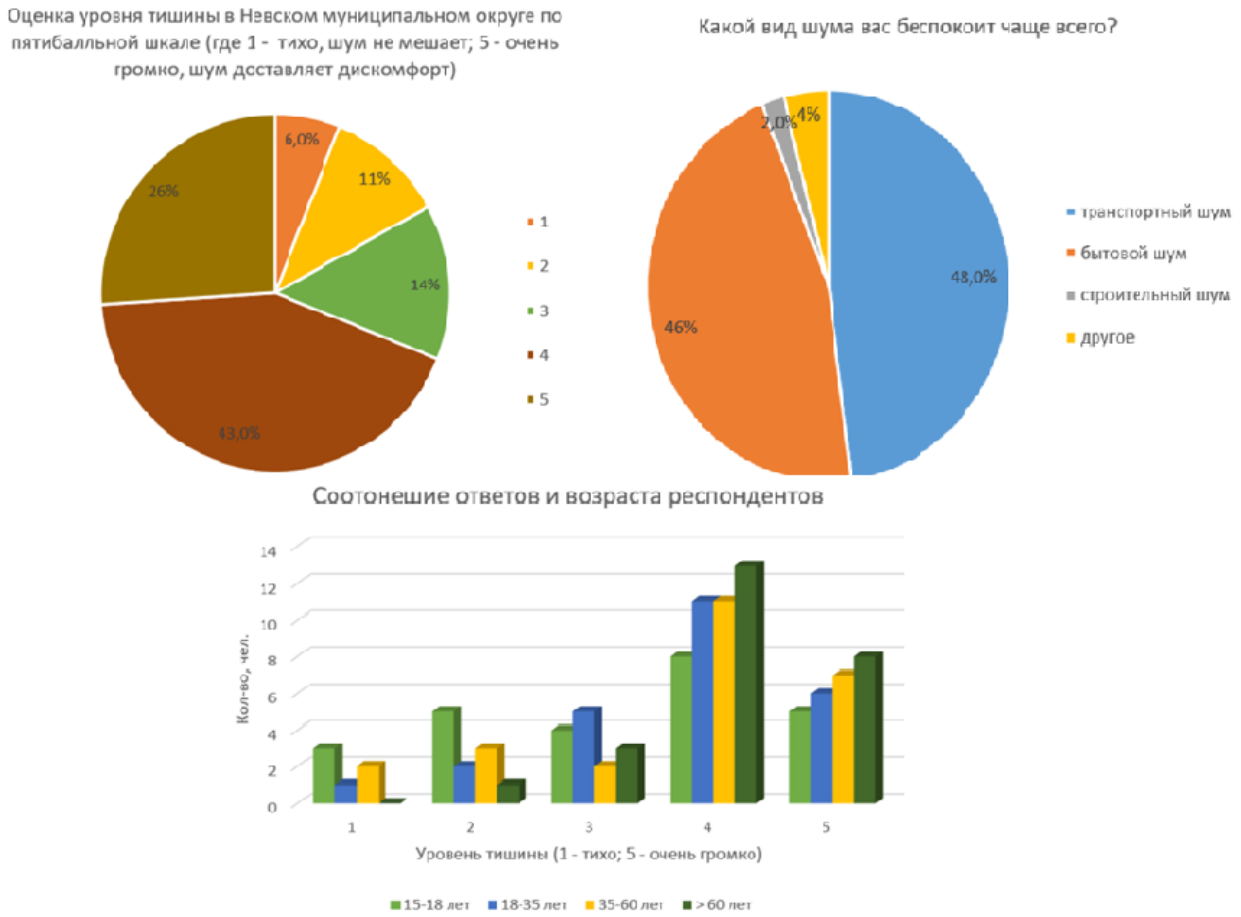


Рис. 1. Результаты социологического исследования

По результатам опроса были сделаны выводы, что большинство людей не удовлетворено уровнем тишины в округе, причем с возрастом люди начинают обращать несколько больше внимания на шумовой дискомфорт.

Следует отметить, что в округе начаты строительные работы по возведению Большого Смоленского моста. Мост призван обеспечить более удобное транспортное сообщение между Большим Смоленским проспектом на левом берегу и улицей Коллонтай на правом берегу реки. Несмотря на то, что необходимость переправы в Невском районе очевидна, проект внесет свой вклад в шумовое загрязнение: изначально источником шума будут строительные работы, а после открытия движения по мосту увеличится транспортная нагрузка на улицы округа. Стройка и сам мост проходят вплотную к жилым домам на Октябрьской набережной, что доставит дискомфорт их жителям. [1, 2]

Всего было взято 343 точки на территории Невского округа, где проводились замеры. 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).

На рисунке 2 представлена карта расположения точек измерения с фактическим значением.

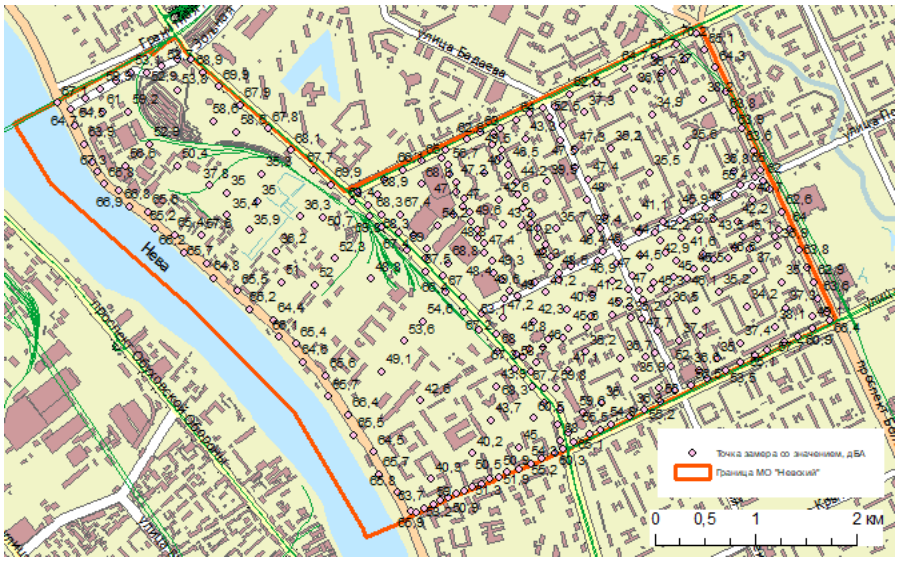


Рис. 2. Карта точек замеров уровня шума, дБА

Для визуализации шумового загрязнения была создана карта с интерполяцией растра методом ОВР (обратно взвешенные расстояния) (рисунок 3).

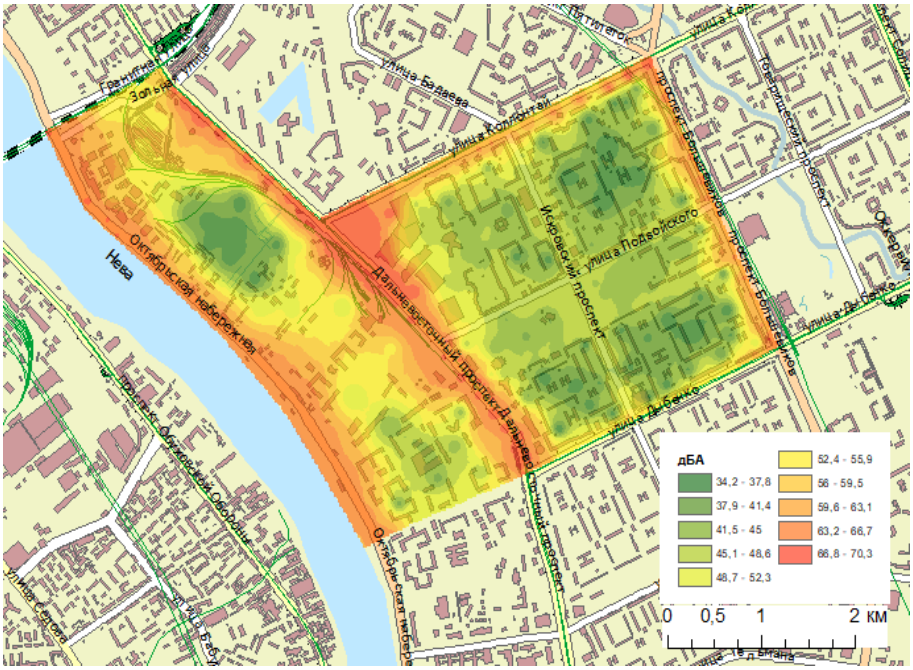


Рис. 3. Карта шумового загрязнения Невского муниципального округа

Согласно СанПиН 1.2.3685-21 допустимый уровень шума в дневное время (7:00-23:00) составляет 55 дБА. Проанализировав карту, становится очевидно, что на части территории Невского муниципального округа значения превышают допустимые. [3, 4] Точки с наибольшими значениями находятся вдоль Дальневосточного проспекта (максимальный уровень звука 70,3 дБА) и улицы Коллонтай (70,2 дБА). Несколько менее шумные, но также намного превышающие нормы значения были получены вдоль Октябрьской набереж-

ной и проспекта Большевиков; на улице Дыбенко уровень шума находится в основном в пределах нормы, в единичных точках значения превышают допустимые, чаще всего данные точки расположены на перекрестках. Это объясняется большим количеством транспорта, в том числе на Дальневосточном проспекте, улице Коллонтай и улице Дыбенко проходят трамвайные пути. Хотя следует заметить, что большинство трамваев – новые, не создающие практически никакого шума, поэтому в шумовое загрязнение вносят вклад только иногда встречающиеся старые трамваи. [5]

Наименьшие показатели уровня шума зафиксированы во всех дворах, в парке Строителей и на Киновеевском кладбище, из чего можно сделать вывод, что основным источником шума в Невском округе является транспорт.

Для точек, расположенных по адресу ул. Коллонтай, 21к1 и Дальневосточный пр., 25к1 были проведены расчеты шумозащитных экранов, так как показатели уровня шума на данных участках превышают максимальный уровень шума для территорий непосредственно прилегающие к жилым домам, который согласно СанПиН 1.2.3685-21 равен 70 дБА. [3, 4]

По результатам расчетов на улице Коллонтай шумозащитный экран не рекомендуется устанавливать, так как экран лишь частично эффективен, а его возведение экономически не выгодно.

На Дальневосточном проспекте, согласно расчетам, установка шумозащитного экрана является целесообразной. Для более наглядного представления была построена диаграмма спектров шума, представленная на рисунке 4.

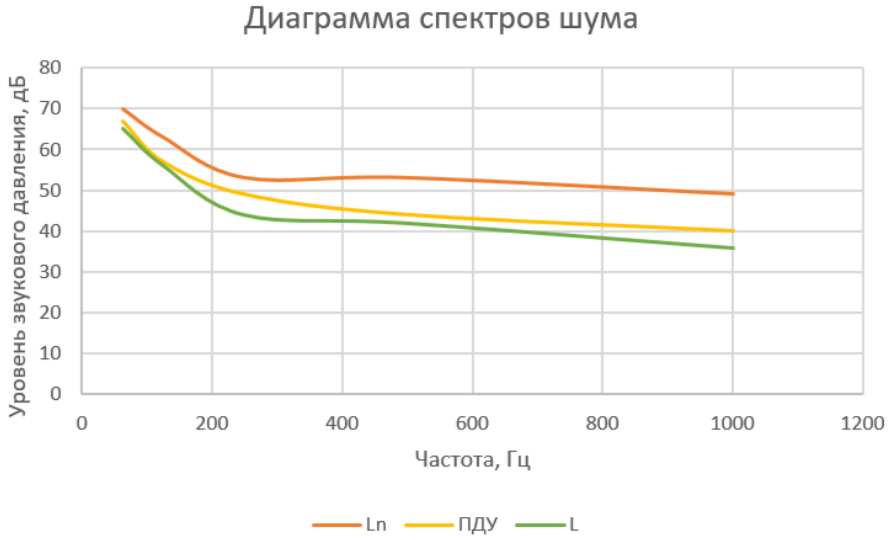


Рис. 4. Диаграмма спектра шума. Верхний спектр показывает уровень шума в расчетной точке от источника шума (Ln); средний – допустимый уровень шума для селитебной территории (ПДУ); нижний – уровень шума в расчетной точке с учетом шумозащитного экрана (L)

В Невском муниципальном округе уровень шумового загрязнения, в целом, является приемлемым, однако в результате замеров были выявлены точки с превышением допустимого уровня шума, а в результате социологического опроса сделаны выводы, что население не удовлетворено уровнем тишины в своем округе, поэтому есть смысл провести некоторые шумозащитные мероприятия: например, на участках, где шумозащитный экран является нецелесообразным, можно провести озеленение, ввести ограничение скорости движения.

Список используемых источников

1. Каким будет Большой Смоленский мост и почему? // Фонтанка.ру, 2024. URL: https://www.fontanka.ru /2024/02/27/73274192/ (дата обращения 10.11.2024).
2. Строить Большой Смоленский мост через Неву начнут 24 декабря в Петербурге. // Вечерний Санкт-Петербург, 2023. URL: https://vecherka-spb.ru/2023/12/23/stroit-bolshoi-smolenskii-most-cherez-nevu-nachnut-24-dekabrya-v-peterburge (дата обращения 10.11.2024).
3. Федеральный закон от 30.03.1999 № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения». Справочно-правовая система «Консультант Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_22481/ (дата обращения 10.11.2024).
4. СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания». Информационно-правовой портал «ГАРАНТ». URL: https://base.garant.ru/400274954/#block_1000 (дата обращения 10.11.2024).
5. СП 51.13330.2011. Защита от шума. Актуализированная редакция. СНиП 23-03-2003. Информационно-правовой портал «ГАРАНТ». URL: https://base.garant.ru/6180771/ (дата обращения 10.11.2024).

Loseva A. **ANALYSIS OF NOISE POLLUTION OF THE NEVSKY DISTRICT MUNICIPAL DISTRICT USING GIS TECHNOLOGIES.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Noise pollution is one of the serious environmental problems of modern society, which has a negative impact on human health. However, not much attention is paid to noise pollution, its monitoring is very poorly developed, which means that the population is living in conditions of noise discomfort, but it is not provided with information about the impacting noise. The Nevsky Municipal District, on the territory of which the research was conducted, is no exception.

Key words: noise, noise pollution, noise mapping, municipal district "Nevsky district".

УДК 551.501.7
ГРНТИ 37.31.02

ВЛИЯНИЕ ДНЕВНОГО СВЕТА НА ОПРЕДЕЛЕНИЕ КОЭФФИЦИЕНТА ОСЛАБЛЕНИЯ ДЛЯ СЛАБО ЗАМУТНЕННОЙ АТМОСФЕРЫ ЛИДАРНЫМИ СИСТЕМАМИ

Е. Ю. Михтеева, И. А. Потапова, А. Л. Скобликова, Т. Ю. Яковлева
Российский государственный гидрометеорологический университет

В этой работе акцентируется внимание на лидарном зондировании атмосферы, которое представляет собой один из самых современных и перспективных методов для изучения физических свойств атмосферы. Однако воздействие дневного света существенно влияет на точность этого подхода, особенно при оценке прозрачности воздуха. Игнорирование этой технической особенности может привести к неверным результатам измерений. В статье обсуждаются возможные пути решения данной проблемы, включая методы коррекции данных. Также проводится анализ массивов данных, полученных с помощью системы LIDAR, с акцентом на типичную зависимость мощности излучения от расстояния, характерную для слабо замутненной атмосферы.

лидар, аэрозоль, загрязнение, фоновое освещение, метод исследования, лидарное зондирование атмосферы

Для жителей города вид смога и дымовых потоков в воздухе стал настолько обыденным, что не вызывает у них беспокойства за здоровье и безопасность. Тем не менее, без регулярного мониторинга невозможно обеспечить благоприятные условия не только для людей, но и для всех живых существ. Существует множество методов и инструментов для наблюдения за окружающей средой, и для лучшего понимания каждого из них необходима их систематизация. В зависимости от используемых подходов мониторинг можно разделить на дистанционный, автоматизированный, химический, биологический и геофизический. Кроме того, существуют более детализированные классификации по другим критериям. В данной работе будет уделено внимание одному из самых современных методов дистанционного мониторинга – лидарному зондированию атмосферы, который является дистанционным и одним из наиболее прогрессивных способов изучения физических свойств атмосферы [1–3]. Однако дневной свет значительно влияет на точность этого метода, особенно при оценке прозрачности атмосферы. Игнорирование этой технической особенности может привести к неверным результатам измерений [4,

5]. В статье рассматриваются возможные решения данной проблемы, а также анализируются данные, полученные с помощью системы LIDAR.

На рисунке 1 представлен типичный график зависимости мощности излучения от расстояния, характерный для слабо замутненной атмосферы [6–8].

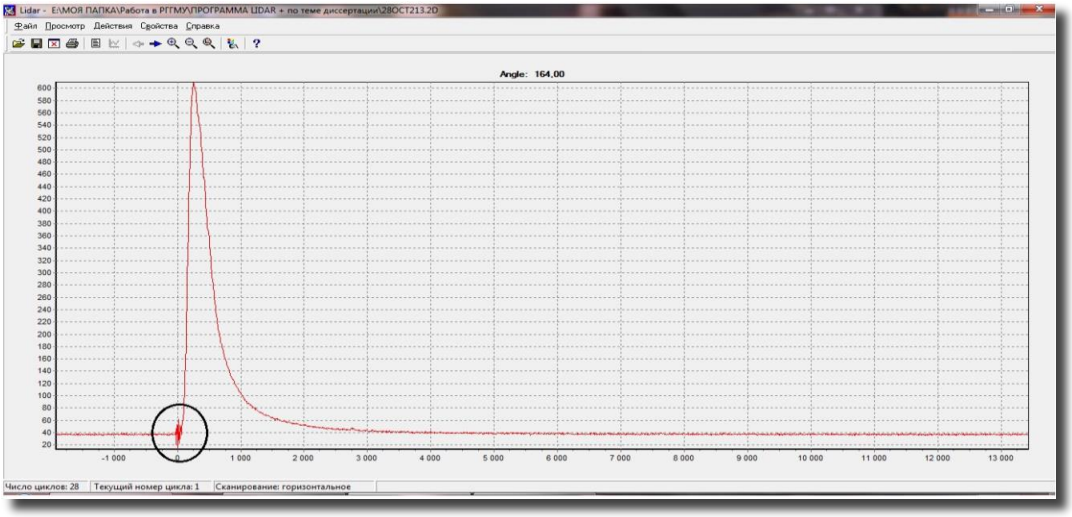


Рис. 1. Зависимость мощности эхосигнала от расстояния

Перед излучением рабочего сигнала системой LIDAR, приемник фиксирует мощность дневного излучения на длине волны зондирования, который, теоретически, должен совпадать с мощностью принимаемого сигнала, полученного на больших расстояниях. Однако, вначале передачи сигнала возникает техническая проблема, которая приводит к сбоям в настройках приемного устройства и, как результат, к значительным погрешностям в измерениях. При изучении загрязнения в слабо замутненной атмосфере крайне важно выявить ошибки, которые могут возникнуть в процессе эксперимента.

Для анализа информации, полученной с помощью LIDAR, применяется лидарное уравнение [1–3, 9–12], которое устанавливает связь между мощностью сигнала обратного рассеяния и коэффициентами обратного рассеяния и ослабления, т. о. одно уравнение содержит два неизвестных. Для решения этой проблемы обычно один из неизвестных задается или измеряется другим способом. Но первый вариант может сопровождаться большими ошибками при поиске другого коэффициента, а применение второго варианта приведет к усложнению системы, используемой для измерений. Для того, чтобы избавиться от перечисленных сложностей и разрабатываются новые методы решения лидарного уравнения

$$P_i = P_* + \frac{B}{R_i^2} exp(-2\sigma R_i),$$

где $B = A\beta$,

A – постоянная лидара,

β – коэффициент обратного рассеяния,

σ – коэффициент ослабления,

P – мощность сигнала обратного рассеяния,

P_* – мощность солнечного излучения, рассеянного атмосферой в направлении на приемное устройство ЛИДАРа,

R – расстояние между лидаром и $i-$м рассеивающим элементом.

Обычно, для оценки случайной погрешности мощности дневного света на принимаемой длине волны, рассматривается метод, который основывается на усреднении значения мощности, полученного приемником вдоль зондируемой трассы при анализе значительного количества импульсов. В этом процессе случайная ошибка P_*, оказывающая влияние на эффективность метода, вычисляется с помощью следующего выражения:

$$\delta = \left\{\frac{\sum_{ijk=1}^{n}\left(P_{ijk=1}-P_*\right)^2 \Delta_{ijk}^2}{\sum_{ijk=1}^{n}\Delta_{ijk}^2}\right\}^{\frac{1}{2}}, \quad (1)$$

где

$$\Delta_{i,j,k}^0 = \begin{vmatrix} P_{i,} & 1/R_i^2 & 1/R_i \\ P_j & 1/R_j^2 & 1/R_j \\ P_k & 1/R_k^2 & 1/R_k \end{vmatrix},$$

$$\Delta_{i,j,k} = \begin{vmatrix} 1 & 1/R_i^2 & 1/R_i \\ 1 & 1/R_j^2 & 1/R_j \\ 1 & 1/R_k^2 & 1/R_k \end{vmatrix},$$

$$P_{ijk} = \Delta_{ijk}^0 / \Delta_{ijk}.$$

Выражение (1) можно переписать в следующем виде:

$$\delta = \sqrt{\left\{\frac{D_1}{D_0} - P_*^2\right\}}$$

В этой работе, для оценки случайной погрешности мощности дневного света на принимаемой длине волны, рассматривается метод, который также основывается на усреднении значения мощности, полученного приемником вдоль зондируемой трассы при анализе значительного количества импульсов. Однако, случайную ошибку среднего значения фонового освещения P_* можно рассчитать, используя линейное приближение:

$$\delta = C_*\left\{\sum_1^n \left(\frac{\partial P_*}{\partial P_1}\right)^2 P_i\right\}^{\frac{1}{2}}. \quad (2)$$

Причем

$$\delta P_i = C_* \sqrt[n]{P_i}.$$

Из выражения (2), следует, что для различных рассматриваемых точек трассы зондирования, выражение для случайной ошибки будет иметь следующий вид:

$$\delta = \frac{C_*}{D_0}\left\{\sum_1^n \left(\Delta_1 - \frac{\Delta_2}{R_i^2} + \frac{\Delta_3}{R_i}\right)^2 P_i\right\}^{\frac{1}{2}},$$

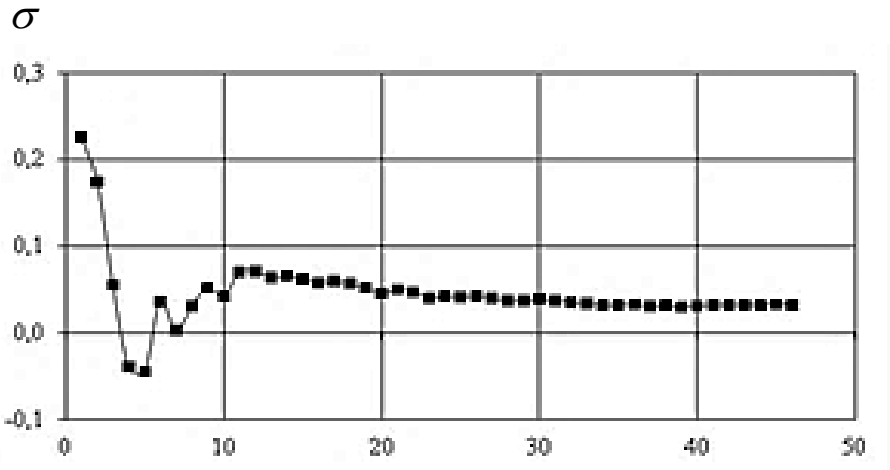
где

$$\Delta_1 = \sum_1^n \frac{1}{R_i^2} \sum_1^n \frac{1}{R_i^4} - \left(\sum_1^n \frac{1}{R_i^3}\right)^2,$$

$$\Delta_2 = \left(\sum_1^n \frac{1}{R_i^2}\right)^2 - \sum_1^n \frac{1}{R_i} \sum_1^n \frac{1}{R_i^3},$$

$$\Delta_3 = \sum_1^n \frac{1}{R_i^2} \sum_1^n \frac{1}{R_i^3} - \sum_1^n \frac{1}{R_i} \sum_1^n \frac{1}{R_i^4}.$$

Использование данного метода позволяет существенно уменьшить случайную погрешность при уменьшении шага зондирования. Это особенно актуально для средней величины мощности дневного света на принимаемой длине волны. На рисунке 2 представлен график, иллюстрирующий зависимость коэффициента ослабления от количества шагов при усреднении по 51 импульсной посылке. Из анализа графика видно, что чем больше усредняется шагов, тем меньше разброс значения коэффициента ослабления, что в свою очередь показывает уменьшение погрешности определения искомого параметра. А это увеличивает точность получения окончательного результата.



Номер шага, шаг 225 м.

Рис. 2. Результаты определения коэффициента ослабления по 51 посылке импульсов

Тем не менее, необходимо учитывать, что в представленных данных присутствует приборная погрешность, которая существенно искажает определение концентраций частиц, загрязняющих атмосферу.

Задача становится более сложной, когда требуется анализировать сигнал, полученный при посылке одного импульса. В таких случаях используется метод наименьших квадратов, который основан на анализе квадрата разности между левой и правой частями лидарного уравнения [13], записанного для каждой характерной точки сигнала [14].

$$P_i - P_* - \frac{B}{R_i^2} exp(-2\sigma R_i) = 0,$$

$$\delta^2 = \sum_1^n \left(P_i - P_* - \frac{B}{R_i^2} exp(-2\sigma R_i) \right)^2. \quad (3)$$

Результаты вычисления коэффициента ослабления, полученные по формуле (3) в случае единичного импульса представлены на рисунке 3.

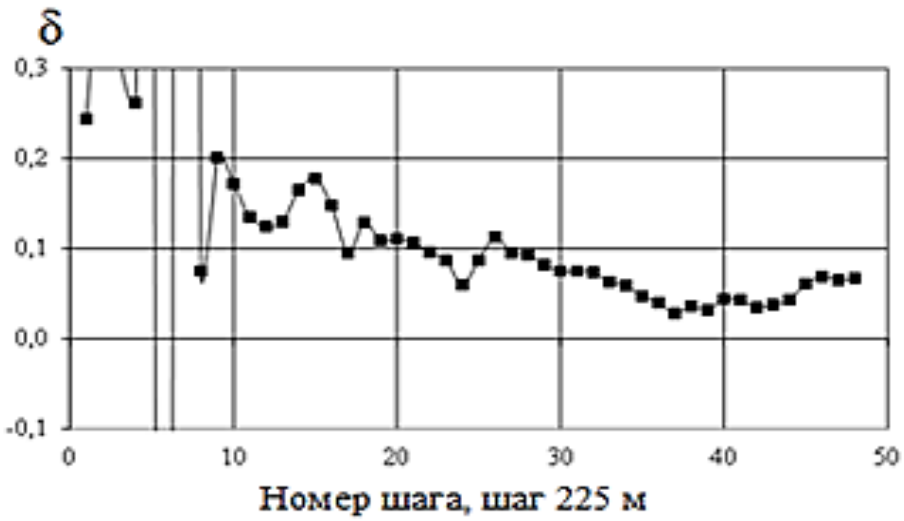


Рис. 3. Погрешность определения коэффициента ослабления при посылке одного импульса, R (*i*=1) = 2500 м

Анализ этого графика показывает, что когда используется предложенный метод, несмотря на колебания в величине ошибки, точность измерений остается достаточно высокой при большом количестве шагов. Этот подход также может быть применен в случаях, когда измерение прозрачности атмосферы проводится единичными импульсами.

В заключение следует отметить, что, в данной работе рассматривается важная проблема определения характеристик атмосферного аэрозоля, что имеет большое значение для понимания процессов, происходящих в атмосфере и их влияния на климат и экологию. Это особенно актуально, поскольку точность таких методов критически важна для корректной интерпретации экс-

периментальных данных. В работе представлен метод интерпретации аэрозольной информации, основанный на решении лидарного уравнения.

Результаты исследования подтверждают высокую точность данного метода, а также подчеркивают важность точного определения фоновой засветки. Примененный алгоритм подходит для невоспроизводимых измерений в условиях слабо замутненной атмосферы.

Тем не менее, необходимо дальнейшее усовершенствование и разработка новых подходов для обеспечения быстрой обработки данных не только для аэрозольной фракции, но и для концентрации газовых компонентов при лидарном зондировании. Это открывает новые горизонты для более точного и надежного изучения атмосферного аэрозоля и газовых составляющих, что, в свою очередь, может способствовать более глубокому пониманию их роли в климатических процессах и экосистемах.

Список используемых источников

1. Егоров А. Д., Потапова И. А., Ржонсницкая Ю. Б., Драбенко В. А. Лидарное зондирование атмосферного аэрозоля // Метеорологический вестник, 2013. Т. 5. № 2. С. 42–51.
2. Егоров А. Д., Потапова И. А. Лидарные исследования прозрачности атмосферы // Труды Главной геофизической обсерватории им. А. И. Воейкова, 2004. № 553. С. 131–142.
3. Егоров А. Д., Потапова И. А., Ржонсницкая Ю. Б., Ошуркова А. А. Методы лидарного зондирования аэрозольных загрязнений атмосферы импульсами конечной длительности // Ученые записки Российского государственного гидрометеорологического университета. 2011. № 18. С. 48–56.
4. Бобровский А. П., Дьяченко Н. В., Михтеева Е. Ю., Потапова И. А., Скобликова А. Л., Хлябич П. П., Яковлева Т. Ю. Определение фоновой засветки слабо замутненной атмосферы и ее влияние на точность определения прозрачности // Материалы V Всероссийской научно-практической конференции «Современные тенденции и перспективы развития гидрометеорологии в России». 2022. С. 372–376.
5. Бобровский А. П., Дьяченко Н. В., Егоров А. Д., Косцов В. В., Калиничев Д. В., Куклин О. А., Михтеева Е. Ю., Потапова И. А., Скобликова А. Л., Хлябич П. П., Яковлева Т. Ю. Алгоритм лидарного определения фоновой засветки и коэффициента ослабления слабо замутненной атмосферы без итерационного процесса // В книге: Современные проблемы гидрометеорологии и устойчивого развития Российской Федерации Сборник тезисов Всероссийской научно-практической конференции. 2019. С. 58-60.
6. Бобровский А. П., Дьяченко Н. В., Егоров А. Д., Косцов В. В., Калиничев Д. В., Михтеева Е. Ю., Потапова И. А., Скобликова А. Л., Хлябич П. П., Яковлева Т. Ю. Влияние фоновой засветки на точность определения прозрачности слабо замутненной атмосферы // В сборнике: ИНФОГЕО-2019. Стратегическое управление развитием территорий. Сборник трудов VI международной научно-практической конференции. 2019. С. 134–136.
7. Дьяченко Н. В., Егоров А. Д., Потапова И. А., Скобликова А. Л., Саноцкая Н. А., Яковлева Т. Ю. Итерпретация слабого радиационного излучения при лидарном зондировании атмосферы // Сборник тезисов международного симпозиума «Атмосферная радиация и динамика» (МСАРД-2019). СПб., 2019. С. 189–190.

8. Yegorov A. D., Potapova I. A., Rzhonsnitskaya Yu. B., Sanotskaya N. A., Shchadin A. V. Atmospheric aerosol measurements and reliability problem: new results // International Journal of Remote Sensing, 2014. V. 35. PP. 5750–5765.
9. Бобровский А. П., Дьяченко Н. В., Косцов В. В., Михтеева Е. Ю., Потапова И. А., Скобликова А. Л., Хлябич П. П., Яковлева Т. Ю. Лидарная прозрачнометрия слабо замутненной атмосферы // В сборнике: Современные тенденции и перспективы развития гидрометеорологии в России. Материалы IV Всероссийской научно-практической конференции, приуроченной к Году науки и технологий. Иркутск, 2021. С. 495–500.
10. Драбенко В. А., Егоров А. Д., Галкин И. А., Потапова И. А., Драбенко Д. В., Игнатенко В. М., Потапова В. Р. Способ аспирационной оптической спектрометрии аэрозольных частиц // Патент на изобретение RU 2681256 C2, 05.03.2019. Заявка № 2016120373 от 25.05.2016.
11. Потапова И. А., Егоров А. Д., Дьяченко Н. В., Саноцкая Н. А., Скобликова А. Л., Яковлева Т. Ю. Интерпретация слабого радиационного излучения при лидарном зондировании атмосферы // В книге: Атмосферная радиация и динамика (МСАРД – 2019). Международный симпозиум. Тезисы. 2019. С. 189–190.
12. Дьяченко Н. В., Потапова И. А., Саватнеев А. Н., Хлябич П. П., Яковлева Т. Ю. Интерпретация лидарной информации при зондировании грубодисперсной аэрозольной фракции // В сборнике: Инновационные методы математики и физики в экологических и гидрометеорологических исследованиях. Сборник трудов Всероссийской научно-практической конференции. Под редакцией И. В. Зайцевой. СПб., 2023. С. 105–110.
13. Egorov A. D., Potapova I. A., Shchukin G. G. Lidar methods for probing an atmospheric aerosol // Journal of Optical Technology. 2001. Т. 68. № 11. С. 801–804.
14. Егоров А. Д., Потапова И. А., Ржонсницкая Ю. Б. Обращение лидарных сигналов малой мощности // Оптический журнал, 2007. Т. 74. № 10. С. 25–28.

Mikhteeva E., Potapova I., Skoblikova A., Yakovleva T. **THE EFFECT OF DAYLIGHT ON THE DETERMINATION OF THE ATTENUATION COEFFICIENT FOR A SLIGHTLY CLOUDY ATMOSPHERE BY LIDAR SYSTEMS.**

Russian State Hydrometeorological University

In this work, special attention is paid to lidar sensing of the atmosphere, which is one of the most modern and promising ways to study the physical characteristics of the atmosphere. However, changing the background illumination has a significant impact on the accuracy of this method, especially when assessing the transparency of the air environment. Neglecting this technical feature can lead to erroneous measurement results. The article discusses possible solutions to this problem, including data correction methods. In addition, the analysis of data arrays obtained using the LIDAR system is carried out, with an emphasis on the typical signal of the dependence of radiation power on distance, characteristic of a slightly cloudy atmosphere.

Key words: Lidar information, aerosol, pollution, background illumination, method, lidar sensing of the atmosphere, slightly cloudy atmosphere.

УДК 504.064.37
ГРНТИ 34.35.51

ИССЛЕДОВАНИЕ ДИНАМИКИ РАЗВИТИЯ ГОРОДСКОЙ ЗАСТРОЙКИ г. СЫКТЫВКАР

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

В работе представлены результаты исследования динамики развития территорий, занимаемых застройкой в г. Сыктывкар. Изучены показатели изменения озелененности территорий города. Сбор материалов космической съемки осуществлялся в периоды разных лет с учетом возможностей спутников Landsat-5, Landsat-7, Landsat-8. Основой исследования является регулярная сетка, которая включает в себя 10 жилых кварталов г. Сыктывкар. В результате исследования космических снимков и заполнения регулярной сетки было установлено, что площадь зеленых территории города уменьшается. Процесс увеличения городской застройки приводит к потере качества биологического разнообразия. Городское биоразнообразие и городская природа влияют на благосостояние городских жителей и пригодность городов для жизни.

г. Сыктывкар, урбанизация, застройка, городская природа, зеленые территории, космическая съемка

Наступил век урбанизации, в настоящее время более половины человечества живет в городах, и ожидается, что этот процент будет только увеличиваться. По разным оценкам, около 60 % городских районов? которые будут существовать в 2050 году еще не построены. Таким образом, дизайн городов будущего – и эволюция сегодняшних – будут определять здоровье и благополучие миллиардов людей [1]. Сегодня города являются центрами социального обмена, жизнеспособности экономики и инноваций. Однако темпы и масштабы глобальных преобразований в месте, где живут люди, создают угрозы биоразнообразию и природе, которые требуют серьезного внимания. На данный момент развитие городской застройки осуществляется без особого внимания к сохранению зеленых пространств. Таким образом, природоохранное планирование часто игнорирует города как места, где биоразнообразие практически отсутствует [2]. Признание многочисленных социальных преимуществ природы в городах, так и способов, которыми города и городская культура могут поддерживать биоразнообразие, имеет множество преимуществ. Поэтому крайне важно, чтобы развитие городской застройки учитывало качество предоставление экосистемных услуг [3].

Тема данной работы имеет высокую степень актуальности. Прежде всего по причине неминуемого увеличения урбанизированных территорий и необходимости сохранения природного ландшафта. При плановом развитии городской застройки данный показатель, наравне с показателем биологического разнообразия, должен учитываться в первую очередь, именно эти значения будут указывать на экологическое качество территории [4, 5]. Период исследования по данной теме составил 38 лет, были собраны данные о городской застройке с 1986 года по 2023 год, космоснимки отбирались с шагом в 4 года. Таким образом, можно проследить динамику изменения озелененности территорий города Сыктывкара, что позволяет оценить качество окружающей природной среды на примере развития урбанизированного ландшафта города Сыктывкара.

Целью представленного исследования является оценка количественного показателя озелененных территорий в условиях развивающейся городской застройки.

Для достижения цели были поставлены следующие задачи:

1. Определить роль озелененных территорий в условиях развития урбанизированного ландшафта на основе анализа теоретических и прикладных работ ученых.

2. Определить область проведения исследования.

3. Апробировать применение методики использования регулярной сетки в анализе количества озелененных территорий на основе космоснимков разных лет.

Данные космической съемки, которые относятся к отдельным географическим районам или городам, часто легче воспринимаются, если они представлены визуально. Визуализация при помощи регулярных сеток также полезна для выявления некоторых закономерностей или тенденций, которые приведут к соответствующим выводам. Регулярная сетка, наложенная на космический снимок? может быть разной, например, она может состоять из точек, шестиугольников или прямоугольников. Использование регулярных сеток с прямоугольной или квадратной структурой на практике обусловлено относительной простотой математического аппарата для оперирования данными [6].

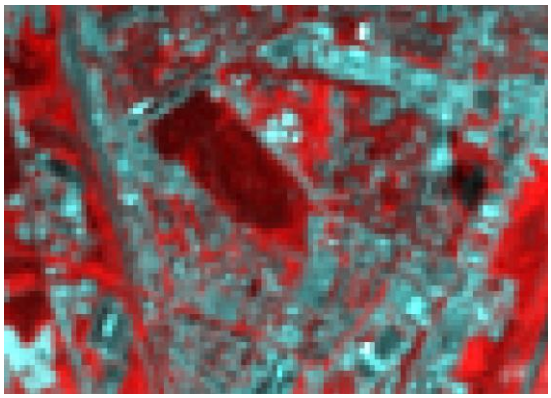
При заполнении регулярной сетки важно решить какие территории будут отмечены в ней. Самый простой и действенный способ – поделить территории на застройку и зеленые участки. Зеленые участки определяются как все области, которые являются естественными, не сильно нарушенными или полностью искусственно созданными ландшафтами. Парки, набережные, придорожные насаждения не считаются естественными. Однако природные экосистемы в пределах парков, где доминируют местные виды, могут быть вклю-

чены в расчет. Сингапурский индекс также учитывает «восстановленные экосистемы» и «озелененные территории». Основой регулярной сетки послужила территория г. Сыктывкара, которая включает в себя 10 жилых кварталов (рис 1.).

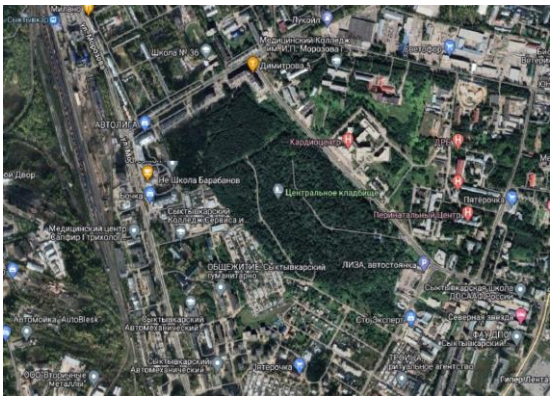
Рис. 1. Область исследования динамики развития городской застройки г. Сыктывкар

Для исследования динамики развития территории городской застройки использовались космические снимки спутников Landsat-5, Landsat-7, Landsat-8, которые имеют разрешение 30*30 м/пиксель, и содержат набор мультиспектральных каналов, которые являются хорошим средством для проведения анализа [7]. Разрешение снимков создает обоснование для выбора размера одной клетки регулярной сетки 30*30 метров.

Для более детального результата подходящими являются 3 канал (Green), 4 канал (Red) и 5 канал (Near Infrared). Каналы 3 и 4 представляют собой видимые зелёный и красный диапазоны. Канал 5 измеряет ближний инфракрасный спектр. Он особенно важен для экологических исследований, поскольку листья растений имеют высокий коэффициент отражения в этой части спектра. Исследование проводилось в комбинации каналов 5-4-3, это стандартная комбинация каналов, которая носит название «искусственные цвета». Растительность отображается в оттенках красного, городская застройка – зелено-голубых, а цвет почвы варьируется от темно до светло коричневого (рис. 2). Хвойные леса будут выглядеть более темно-красными или даже коричневыми по сравнению с лиственными. Этот набор каналов очень популярен и используется, главным образом, для изучения состояния растительного покрова, с недавнего времени данную комбинацию стали использовать при анализе динамики урбанизированных территорий [7].



а



б

Рис. 2. Беличий парк и Центральное городское кладбище г. Сыктывкар: а – снимок спутника Landsat-5 (комбинация каналов 5-4-3); б – снимок Google Satellite Hybryd.

После отбора космических снимков и заполнения регулярной сетки стало возможным посчитать общую площадь занятую застройкой и площадь зеленых территорий (таблица 1). При заполнении сетки учитывались лишь те участки, которым можно было придать безошибочное значение, например, в ячейке находится только участок застройки или же в ячейке находится только участок растительности. Почвенным участкам, на которых отсутствует растительность или же присутствует в малом количестве придавалось отдельное значение, но из-за невозможности разделения они были посчитаны вместе с зелеными территориями города.

ТАБЛИЦА 1. Данные распределения площадей г. Сыктывкар

Год	Озелененная территория, га.	Застройка, га.
1986	596,6	858,52
1990	498,7	956,42
1994	485	970,12
1998	413,1	1042,02
2002	410,9	1044,22
2006	408,6	1046,52
2010	385,5	1069,62
2014	381,9	1073,22
2018	371	1084,12
2023	344,2	1110,92

По данным анализа озелененная территория с каждым годом теряет свою площадь, что напрямую связано с увеличением городской застройки. Самые сильные изменения произошли в период с 1986 по 1990 год, когда площадь городской застройки увеличилась на 97,9 гектаров. Значительные изменения также произошли в период с 2006 по 2010 год и с 2018 по 2023 год, в эти периоды городская застройка увеличилась на 23,1 гектар и на 26,8 гектаров, соответсвенно. Полученные данные можно представить выделением отдельного слоя объединенных ячеек сетки, зеленым цветом отмечены территории присутствия растительности, светло-коричневым отмечены почвенные участки в непосредственной близости к озелененным территориям (рис. 3).

а б в г

Рис. 3. Результат заполнения регулярной сетки:
а – 1986 год; б – 1998 год; в – 2010 год; г – 2023 год.

Таким образом, использование космических снимков разных лет с наложением слоя регулярной помогает проследить изменения в динамике развития городской застройки. Регулярная сетка также обладает преимуществом простоты анализа и визуализации данных. Увеличение площади урбанизированных территорий г. Сыктывкар сопряжено с уменьшением площади растительного покрова и озелененных территорий. Несмотря на общую тенденцию к увеличению площади и доли застройки, в некоторых участках города отмечено увеличение доли озелененных территорий. Это прежде всего, участки застройки 1960-1980 годов, на которых за анализируемый промежуток времени разрослись древесные насаждения, созданные непосредственно после застройки. Стоит отметить, что темпы преобразования территории г. Сыктывкар создают угрозы биологическому разнообразию и природе, которые требуют особого внимания и применения инструментов планирования.

Список используемых источников

1. Liu, X., Huang Y., Xu X., Li X., Li X., Ciais P., Lin P., et al. High-Spatiotemporal-Resolution Mapping of Global Urban Change from 1985 to 2015. 2020. Nature Sustainability 3. 564–70.
2. James W. Quinn. Combinations of Landsat TM / ETM+ Bands. 2001. URL: http://web.pdx.edu/~emch/ipl/bandcombinations.html (дата обращения 01.09.2024).
3. World Bank Group. Unlocking Nature-Smart Development: An Approach Paper on Biodiversity and Ecosystem Services. Washington, 2021. DC: World Bank. URL: https://openknowledge.worldbank.org/handle/10986/36047 (дата обращения 29.10.2024).
4. Elmqvist, Thomas, Michail Fragkias, Julie Goodness, Burak Güneralp, Peter J. Marcotullio, Robert I. McDonald, Susan Parnell, et al. Urbanization, Biodiversity and Ecosystem Services: Challenges and Opportunities: A Global Assessment. Dordrecht, Netherlands: Springer. 2013. URL: https://link.springer.com/content/pdf/10.1007 %2F978-94-007-7088-1.pdf. (дата обращения 29.09.2024).
5. Rodricks S. Singapore City Biodiversity Index. 2010. URL: https://www.teebweb.org/wp-content/uploads/CaseStudies/Singapore %20City %20Biodiversity %20Index.pdf (дата обращения 29.09.2024).
6. Подольская Е. С., Ершов Д. В., Ковганко К. А. Метод определения размера ячейки регулярной сети для инфраструктурного зонирования территории с целью охраны лесов от пожаров. М.: Центр по проблемам экологии и продуктивности лесов РАН, 2023. № Т. 6. № 2. С. 149–162.
7. Keeler B. L., Hamel P., McPhearson T., Hamann M. H., Donahue M. L., Meza Prado K. A., Arkema K. K., et al. Social-Ecological and Technological Factors Moderate the Value of Urban Nature // Nature Sustainability, 2019. Vol. 2 (1). PP. 29–38. URL: https://doi.org/10.1038/s41893-018-0202-1 (дата обращения 29.09.2024).
8. Барталев С. А., Егоров В. А., Жарко В. О., ЛулянН Е. А., Плотников Д. Е., Хвостиков С. А., Шабанов Н. В. Спутниковое картографирование растительного покрова России. М.: ИКИ РАН, 2016. 208 с.
9. Chan L., Hillel O., Elmqvist T., Werner P., Holman N., Mader A., Calaterra E. User's Manual on the Singapore Index on Cities' Biodiversity (also known as the City Biodiversity Index). Singapore, 2014. URL: https://www.cbd.int/authorities/doc/Singapore-Index-User-Manual-20140730-en.pdf (дата обращения 29.09.2024).
10. Puppim de Oliveira J. A., Doll C. N., Moreno-Peñaranda R., Balaban O. Urban Biodiversity and Climate Change // Global Environmental Change, 2014. № 1. PP. 461–68.

***Ozhegov V.* A STUDY OF THE DYNAMICS OF URBAN DEVELOPMENT IN SYKTYVKAR.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The paper presents the results of a study of the dynamics of the development of territories occupied by buildings in Syktyvkar. Indicators of changes in the greening of the city's territories have been studied. The collection of satellite imagery materials was carried out during different periods of the year, taking into account the capabilities of the Landsat-5, Landsat-7, and Landsat-8 satellites. The basis of the study is a regular grid, which includes 10 residential quarters of Syktyvkar. As a result of studying satellite images and filling in a regular grid, it was found that the green area of the city is decreasing. The process of increasing urban development leads to a loss of the quality of biological diversity. Urban biodiversity and urban nature affect the well-being of urban residents and the liveability of cities.

Key words: Syktyvkar, urbanization, building, urban nature, green areas, satellite imagery.

УДК 504.06
ГРНТИ 87.55.33

КАРТОГРАФИРОВАНИЕ ЭЛЕКТРОМАГНИТНЫХ ПОЛЕЙ ПРОМЫШЛЕННОЙ ЧАСТОТЫ В КРАСНОГВАРДЕЙСКОМ РАЙОНЕ САНКТ-ПЕТЕРБУРГА

В. В. Пентегова, В. И. Стурман
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе выполнены измерения напряженности электрического поля и магнитной индукции, на основе которых созданы картографические материалы электромагнитной обстановки в Красногвардейском районе Санкт-Петербурга. Превышений предельно допустимых уровней не отмечено, но широко распространены значения магнитной индукции, превышающие ориентировочные безопасные уровни согласно результатам зарубежных исследований. Выявлены аномалии, характеризующиеся повышенными значениями магнитной индукции.

электромагнитные поля, электромагнитное загрязнение, картографирование электромагнитный полей

Электромагнитное загрязнение относится к физическому загрязнению, приводящему к изменению физических параметров воздуха на конкретной территории. Целенаправленное использование электромагнитной энергии в самых разнообразных областях человеческой деятельности привело к тому, что к существующему магнитному и электрическому полям Земли, добавилось электромагнитное поле искусственного происхождения, создаваемое самыми разнообразными излучающими устройствами. Эффекты воздействия электромагнитных полей на человека связаны с индуцированием ими внутри тела электрических токов различной частоты и интенсивности, что может приводить к неблагоприятным последствиям для здоровья [1].

В Санкт-Петербурге электромагнитному облучению подвержены около 30 % населения, которые связаны с воздействием электромагнитных полей посредством профессиональной деятельности; приблизительно 60 % от общего числа населения Санкт-Петербурга, находящегося под действием электромагнитных полей вне производственной сферы: проживающие рядом с воздушными линиями электропередачи, в домах с большим количеством бытовых электрических приборов, а также пользователи персональных электронно-вычислительных машин, сотовых телефонов, радиотелефонов и др. [2]. В целях более глубокого изучения свойств электромагнитных полей урбанизирован-

ной среды было выполнено их исследование в Красногвардейском районе Санкт-Петербурга.

Для проведения исследования был выбран инструментальный метод разовых измерений электромагнитных полей. Для замеров напряженности электрического поля и магнитной индукции использовался прибор – Индикатор электромагнитных полей промышленной частоты «ВЕ-50И». Измерения электромагнитных полей проводились согласно МР 4.3.0177-20 «Методика измерения электромагнитных полей промышленной частоты 50 Гц на селитебной территории» на высоте 1,8 м от поверхности земли [3]. Кроме того, с целью выявления электросетевых кабелей подземной прокладки были также произведены замеры на расстоянии 0,5 м от поверхности земли. Картографические изображения были выполнены в программе ArcGIS ArcMap 10.8. Для более наглядного представления результатов напряженности электрического поля и магнитной индукции были созданы карты с интерполяцией методом ОВР (обратно взвешенных расстояний) (рисунок 1, 2).

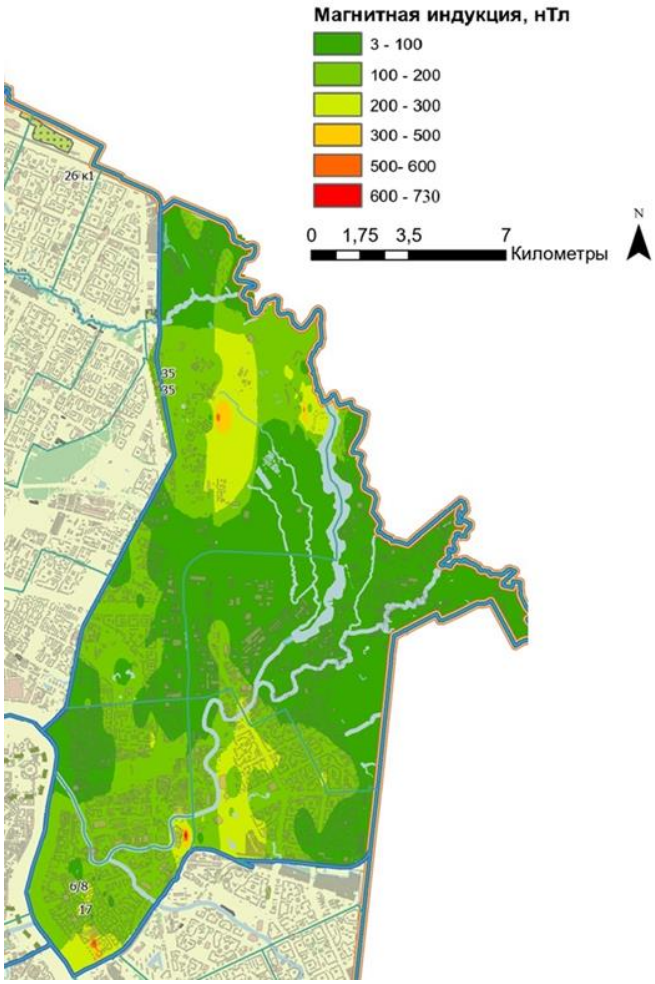


Рис. 1. Картографическое изображение магнитной индукции (нТл) в Красногвардейском районе Санкт-Петербурга

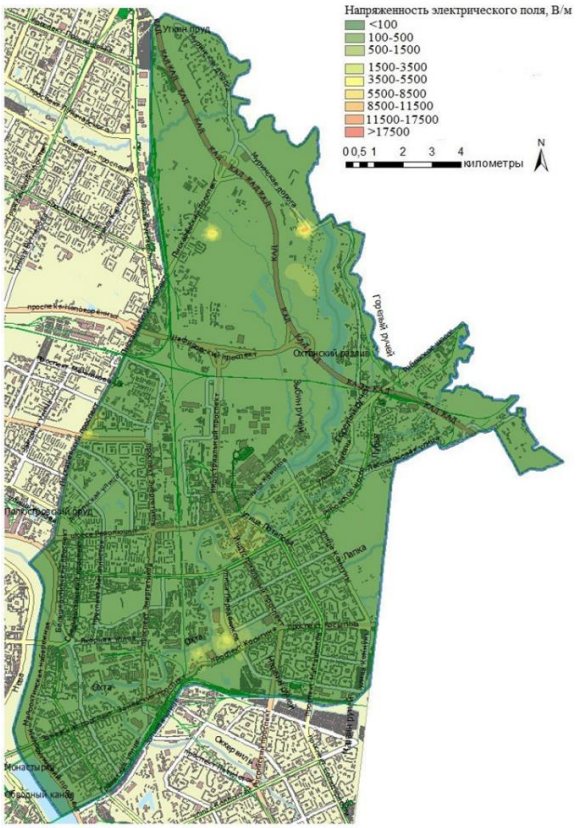


Рис. 2. Картографическое изображение напряженности электрического поля (В/м) в Красногвардейском районе Санкт-Петербурга

Основными источниками магнитной индукции в Красногвардейском районе Санкт-Петербурга являются распределительные щитки, электропроводка, проведенная на фасадах зданий, системы вентиляции и кондиционирования, вывески магазинов, кафе, ресторанов; напряженности электрического поля – высоковольтные линии (ВЛ).

В соответствии с результатами картографического изображения (рисунок 1, 2) низкие значения напряженности электрического поля (от 3,05 В/м до 4,5 В/м) и магнитной индукции (от 11 нТл до 13,5 нТл) характерны для парковых/лесопарковых зон, а также незастроенных территорий. Повышенные значения напряженности электрического поля наблюдались вблизи ВЛ-110 кВ у остановки общественного транспорта (464 В/м) на Индустриальном проспекте, а также рядом с системой вентиляции (121 В/м), расположенной на здании по адресу: Муринская дор., д. 10, корп. 1.

Высокие значения магнитной индукции в районе зафиксированы рядом с электрической подстанцией (730 нТл), менее высокие в сравнении с ней, но не менее существенные значения – (667 нТл, 302 нТл) вблизи трансформаторной подстанции и медицинского учреждения. Существенно более высокие значения магнитной индукции были отмечены в пределах аномалий, которые обусловлены наличием недостаточного экранирования кабелей подземной прокладки (таблица 1, рисунок 3).

ТАБЛИЦА 1. Сведения о выявленных аномальных значениях магнитной индукции, нТл

Место измерений	Измеренные значения, нТл
Ул. Таллинская, 27, двор	683
Заневский пр., 34к1	611
Новочеркасский пр.,14	586
Ул. Миронова, 8, двор	615
Большая Прохоровская ул., 45	701
м. Новочеркасская, вход №1	814
Ул. Стасовой, 4к1, двор	712

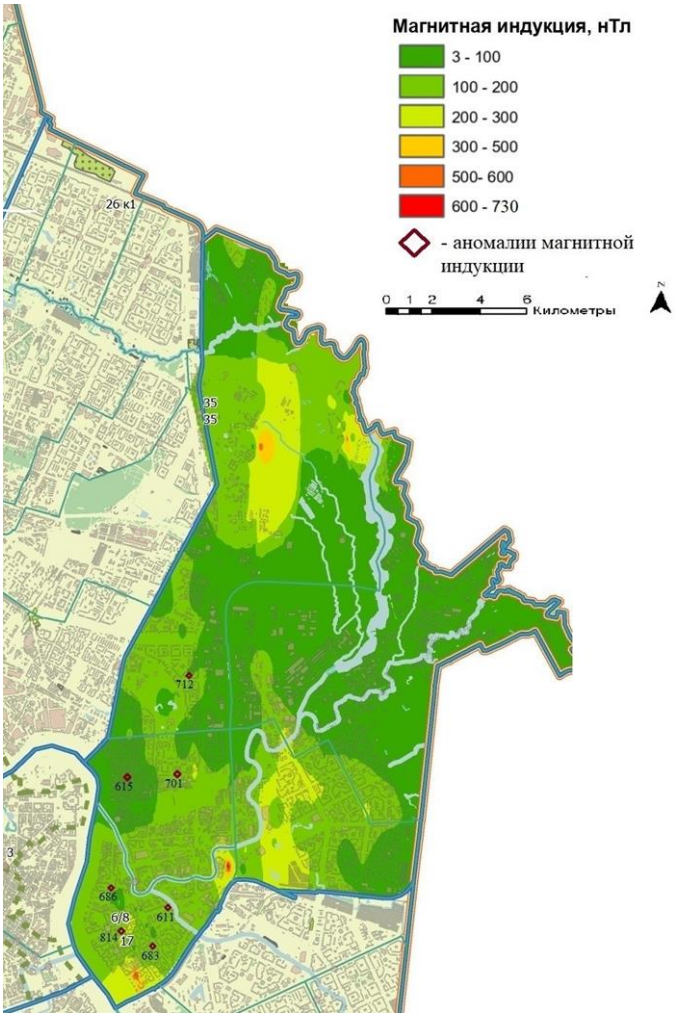


Рис. 3. Картографическое изображение выявленных аномалий магнитной индукции (нТл) в Красногвардейском районе Санкт-Петербурга

Таким образом, в рамках исследования электрических и магнитных полей в Красногвардейском районе Санкт-Петербурга можно сделать вывод: превышений предельно допустимых уровней ни для магнитной индукции (10 мкТл), ни для напряженности электрического поля (1 кВ/м) согласно СанПиН 1.2.3685-21 [4]. зафиксировано не было, однако ориентировочно безопасные уровни магнитной индукции 200-400 нТл [5], определенные по оценкам ряда зарубежных организаций, превышены примерно до 1,8 раза. Значения аномалий магнитной индукции ниже в 14-17 раз, чем действующий в России норматив для территорий жилой застройки в соответствии с СанПиН 1.2.3685-21, но ориентировочно безопасные уровни (200-400 нТл) в аномалиях превышаются до 1,5-1,8 раза.

Список используемых источников

1. Пресман А. С. Электромагнитные поля и живая природа. М.: Наука, 1968. 288 с.
2. Минин Б. А. СВЧ и безопасность человека. М.: Советское радио, 1974. 348 с.
3. «МР 4.3.0177-20. 4.3. Методы контроля. Физические факторы. Методика измерения электромагнитных полей промышленной частоты 50 Гц на селитебной территории. Методические рекомендации» (утв. Главным государственным санитарным врачом РФ 04.12.2020). URL: https://www.consultant.ru/document/cons_doc_LAW_380783/. (дата обращения 28.05.2024).
4. Постановление Главного государственного санитарного врача РФ от 28.01.2021 № 2 «Об утверждении санитарных правил и норм СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания». URL: https://www.consultant.ru/document/cons_doc_LAW_375839/. (дата обращения 28.05.2024).
5. Muller B. Electrosmog. Hausgemachtes Problem// BildWiss. 1996. № 4. P. 12–14.

Pentegova V., Sturman V. **MAPPING ELECTROMAGNETIC FIELDS OF INDUSTRIAL FREQUENCY IN THE KRASNOGVARDEYSKY DISTRICT OF ST. PETERSBURG.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The work involved measurements of the electric field strength and magnetic induction, on the basis of which cartographic materials of the electromagnetic environment in the Krasnogvardeisky district of St. Petersburg were created. No exceedances of maximum permissible levels were noted, but magnetic induction values exceeding the estimated safe levels according to the results of foreign studies were widespread. Anomalies characterized by increased values of magnetic induction were identified.

Key words: electromagnetic fields, electromagnetic pollution, mapping of electromagnetic fields.

УДК 504.055 (470.23)
ГРНТИ 87.55.33

УЧЕТ НАЛОЖЕНИЯ СЕКТОРОВ БАЗОВЫХ СТАНЦИЙ ПРИ ЭКОЛОГИЧЕСКОМ МОНИТОРИНГЕ ЭЛЕКТРОМАГНИТНЫХ ПОЛЕЙ

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

В статье представлены результаты исследования влияния наложения секторов базовых станций сотовой связи на пространственное распределение электромагнитных полей радиочастотного диапазона в городе Мурино. С помощью ГИС-технологий были обработаны полученные данные и составлена карта наложений секторов базовых станций на интерполированные значения плотности потока энергии. Результаты показали, что на исследуемой территории в зонах наложения 5 и более секторов базовых станций, использующих центральную частоту 900 МГц, формируются области максимальных значений плотности потока энергии. Кроме этого, данные области формируются при наложении 3 и более секторов, если хотя бы один использует стандарт LTE.

электромагнитные поля, плотность потока энергии, базовые станции сотовой связи, ГИС-технологии

В современной высокоурбанизированной среде мы окружены всевозможными источниками электромагнитного излучения радиочастотного диапазона, без которых невозможны такие технологии как телевидение, сотовая связь, радиосвязь, Wi-Fi, GPS-навигация, сигнализация и пр. Но, к сожалению, в большинстве случаев отмечено негативное воздействие электромагнитных полей радиочастотного диапазона (ЭМП РЧ) на окружающую среду и здоровье человека [1, 2]. Огромное количество технических средств и повышение их нагрузки способствуют формированию электромагнитного загрязнения. Особенно это актуально для пригородов мегаполисов, потому что, как правило, для них характерна плотная высотная застройка с интенсивным покрытием сотовой сети связи, снабжением территории большим количеством передающих радиотехнических устройств, а также преобладание относительно молодого населения, активно пользующегося средствами связи. К мероприятиям по защите от воздействия ЭМП РЧ относится изменение характеристик и режимов работы источников излучения. Но, как показывают проведенные раннее исследования электромагнитного фона [3,4], распределение ЭМП РЧ в пространстве обычно неоднородное, из-за чего возникают сложности в определении источников, формирующих области повышенных значений.

На территории Российской Федерации для обеспечения экологической безопасности населения от негативного воздействия передающих радиотехнических объектов в соответствии с нормативными документами [5,6] установлены предельно допустимые уровни (ПДУ) ЭМП. Для диапазона частот 0,3-330 ГГц нормирование осуществляется по показателю плотности потока энергии (ППЭ), ПДУ составляет 10 мкВт/см^2 для помещений жилых и общественных зданий и для селитебных территорий.

Оценка электромагнитного фона проводилась в микрорайоне Западный г. Мурино, расположенного на северо-западе Всеволожского района Ленинградской области. Для исследования ЭМП РЧ была выбрана селитебная территория с плотной высокоэтажной жилой застройкой. Для определения параметров секторов базовых станций сотовой связи использовался открытый сервис картирования вышек сотовой связи и покрытия CellMapper, который показывает детальную информацию о сетях EDGE, GSM, CDMA, UMTS, LTE, LTE-A [7]. Для исследования была выбрана центральная частота 900 МГц со стандартами EDGE, GSM и LTE. На данной частоте было обнаружено 109 секторов от 60 базовых станций сотовой связи (БССС), из них 59 зон провайдера Мегафон и 50 секторов провайдера МТС.

Для измерения ЭМП РЧ использовался измеритель уровня электромагнитного излучения МЕГЕОН 07300 (ООО «МЕГЕОН», Россия), предназначенный для измерений в диапазоне от 50 МГц до 3,5 ГГц. Замеры проводились согласно методике [8] 16.09.2024 г.- 28.10.2024 г. на частоте 900 МГц в 636 точках с интервалом 30-50 м.

Обработка данных проводилась в программе QGIS 3.16.11. Была выбрана географическая система координат WGS 84, в качестве базовой карты использовалась Open StreetMap (OSM) к которой в дальнейшем привязывался фрагмент карты из портала Яндекс.Карты. С помощью внутренних инструментов программы осуществлялся перенос геометрии и параметров секторов БССС из сервиса CellMapper, затем данные были визуализированы с учетом параметров стандартов связи и провайдеров (рис.1). Затем, была произведена обработка полученной геометрии для выявления зон наложения секторов БССС (рис. 2). Также, в программе производилась статистическая обработка, интерполяция и визуализация полученных значений ППЭ. В результате была построена карта наложений секторов БССС на интерполированные значения ППЭ (рис. 3).

На исследуемой территории электромагнитный фон повышен, превышения предельно допустимого уровня ЭМП РЧ обнаружены в 31,6 % точках, в том числе превышения ПДУ в 3-5 раз отмечены в 4,4 % случаев. Максимальное зафиксированное значение составило 52,29 мкВт/см^2. Области максималь-

ных значений в большинстве случаев формируются на юге территории и приурочены к бульвару Менделеева с пересекающими его улице Шувалова и Воронцовским бульваром. Среднее значение ППЭ в данной области составляет 17,20 мкВт/см^2. Кроме этого, участки повышенных значений формируются на смежной территории во дворах на юго-западе и юго-востоке исследуемого участка. Отдельные районы максимальных значений отмечены на Петровском бульваре и Екатерининской улице, со средним значением 9,86 мкВт/см^2.

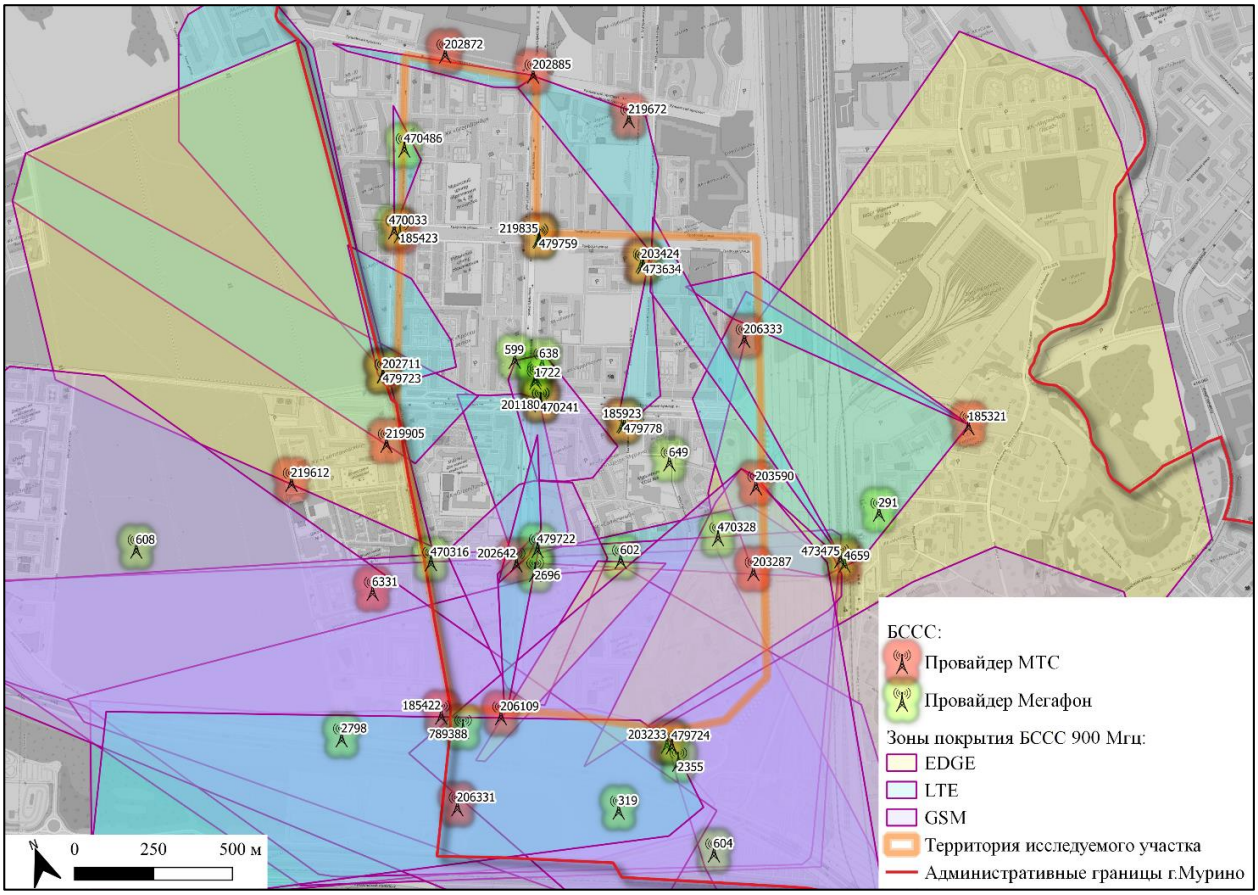


Рис. 1 Зоны секторов БССС на частоте 900 МГц

От 12 базовых станций сотовой связи наложение в 3 и более слоя происходит у 17 секторов, из которых 8 относятся к компании МТС, остальные к Мегафон. Наложение 3 зон секторов БССС, использующих стандарт GSM, отмечено в южной части исследуемой территории, стандарты EDGE и LTE - в западной, центральной и восточной районах. Наложение 4 зон секторов формирует на юге 3 области, две из которых образуются стандартами EDGE и GSM, и одна технологиями LTE и GSM. Наложение 5 и более секторов происходит стандартами EDGE, GSM и LTE центральном участке Бульвара Менделеева, и стандартами GSM, LTE на перекрестке Бульвара Менделеева и улицы Шувалова. В итоге, наибольшая площадь наложения секторов формируется в южной части исследуемого участка, а наибольшее количество пересечений

приурочено к центральной части бульвара Менделеева и перекрестку с улицей Шувалова.

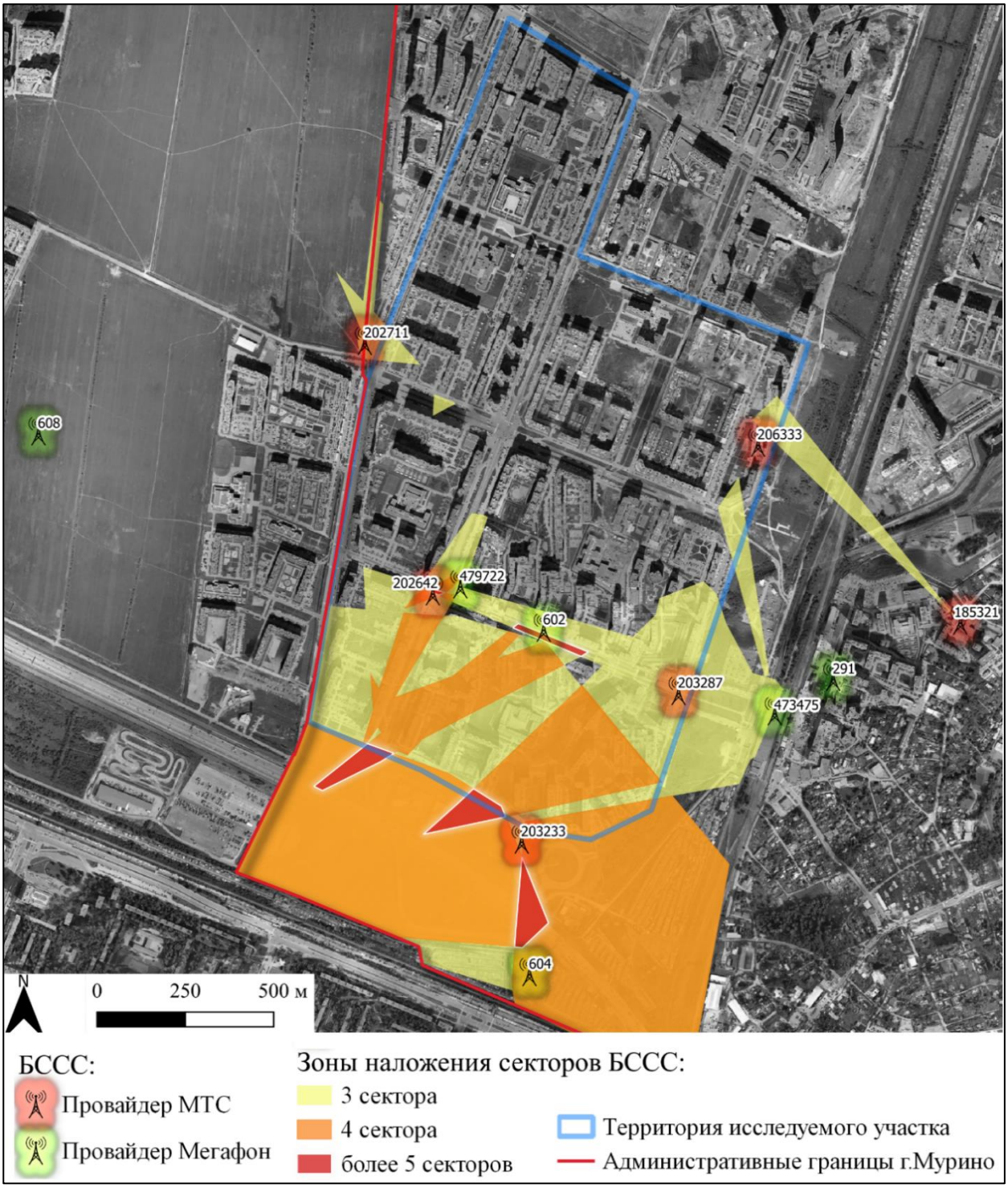


Рис. 2 Зоны наложения секторов БССС на частоте 900 МГц

В результате сравнения данных интерполированных значений ППЭ и участков наложения секторов БССС приблизительно 63 % площади участков наибольших значений ППЭ входят в зоны наложения секторов. Но, практически 40 % территории в зоне наложения секторов не относится к областям повышенных значений ППЭ. В зоне наложения 3 секторов 62 % площади не от-

носится к областям повышенных значений, в зоне наложения 4 секторов к таким областям не относится 42 % площади, а в зоне наложения 5 и более секторов БССС менее 1 % территории не относится к областям повышенных значений ППЭ. При этом, в зонах наложения секторов со стандартом LTE области повышенных значений ЭМП занимают 96 % площади. Источниками являются БССС 185321, 202711, 202642 провайдера МТС и БССС 473475, 479722 провайдера Мегафон.

Таким образом, на исследуемой территории в зонах наложения 5 и более секторов БССС, использующих центральную частоту 900 МГц, формируются области максимальных значений плотности потока энергии электромагнитных полей радиочастотного диапазона. Кроме этого, данные области формируются при наложении 3 и более секторов, если хотя бы один использует стандарт LTE. Источниками максимальных значений плотности потока энергии с учетом наложения секторов являются БССС 185321, 202711, 202642 провайдера МТС и БССС 473475, 479722 провайдера Мегафон. Стоит отметить, что для данной работы использовался открытый сервис картирования вышек сотовой связи и покрытия, для более корректной оценки необходимо проведение исследования покрытия сети сотовой связи в г. Мурино.

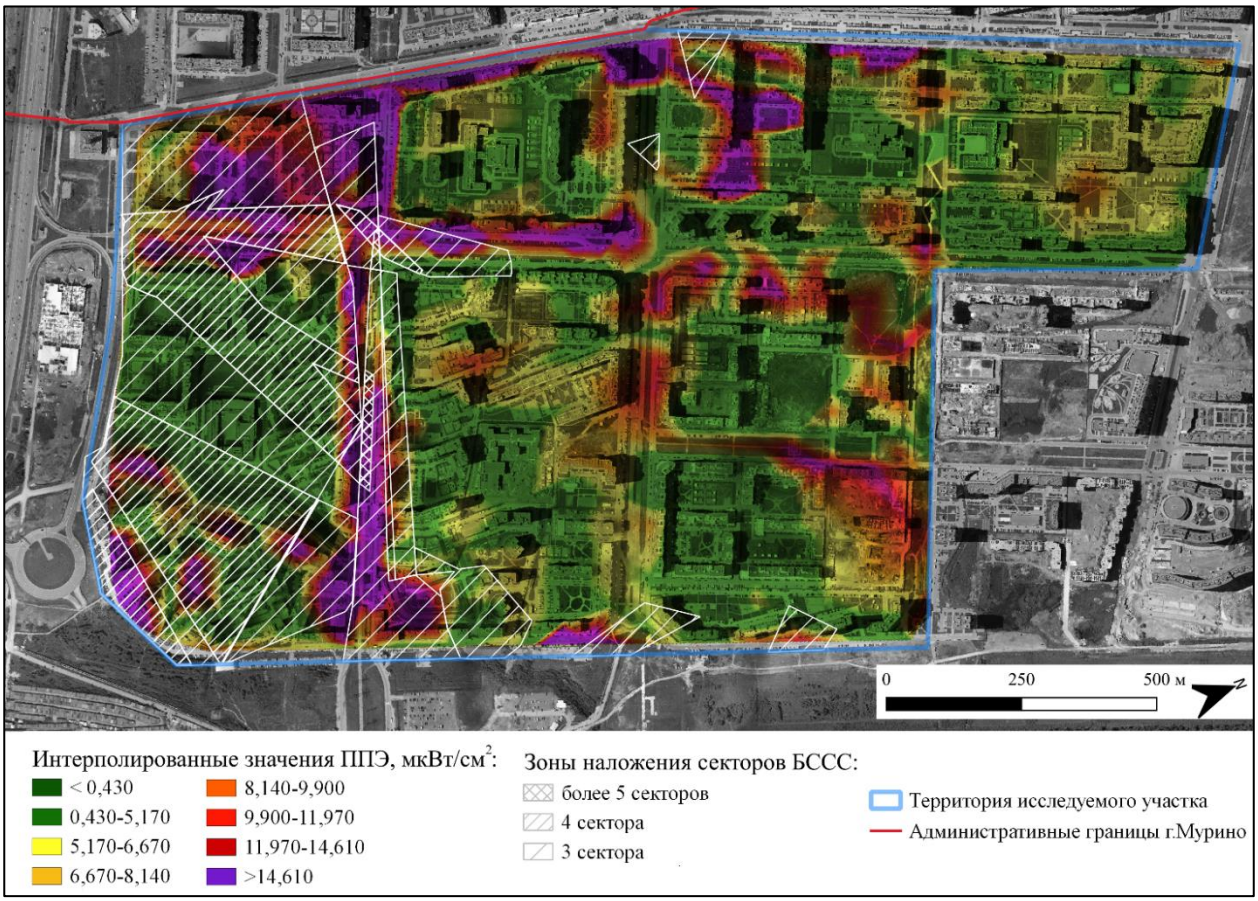


Рис.3 Карта наложений секторов БССС на интерполированные значения ППЭ

Список используемых источников

1. Panagopoulos D. J., Chavdoula E. D., Margaritis L. H. Bioeffects of mobile telephony radiation in relation to its intensity or distance from the antenna. Int J Radiat Biol. 2010; 86:345–357.
2. NationalToxicologyProgram. Toxicology and carcinogenesis studies in Sprague Dawley (Hsd:Sprague Dawley SD) rats exposed to whole-body radio frequency radiation at a frequency (900 MHz) and modulations (GSM and CDMA) used by cell phones. Natl Toxicol Program Tech Rep Ser: NTP-TR-595. 2018.
3. Pichugina A., Sturman V., Yatsenko M. Application of GIS technology for electromagnetic field assessment // Вестник факультета цифровых технологий, сборник научно-теоретических статей. СПб.: СПбГУТ, 2023. Стр.438–442.
4. Пищугина А. Д. Картографирование электромагнитных полей радиочастотного диапазона в урбанизированной среде (на примере г. Мурино) // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2023). Региональная научно-методическая конференция магистрантов и их руководителей. Сборник лучших докладов конференции. СПб.: СПбГУТ, 2023. Том 1. Стр. 133–137.
5. СанПиН 2.1.8/2.2.4.2302-07 Гигиенические требования к размещению и эксплуатации передающих радиотехнических объектов. Постановление Главного государственного санитарного врача РФ от 19 декабря 2007 г. № 91. URL: https://docs.cntd.ru/document/902081974 (дата обращения 29.10.2024).
6. СанПиН 1.2.3685-21 Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания. Постановление Главного государственного санитарного врача РФ от 28 января 2021 г. № 2. URL: https://docs.cntd.ru/document/573500115 (дата обращения 29.10.2024).
7. Сервис картирования вышек сотовой связи и покрытия CellMapper. URL: https://www.cellmapper.net/ (дата обращения 29.10.2024).
8. МУК 4.3.1167-02 Определение плотности потока энергии электромагнитного поля в местах размещения радиосредств, работающих в диапазоне частот 300 МГц-300 ГГц. URL: https://docs.cntd.ru/document/1200030406 (дата обращения 29.10.2024).

Pischugina A. **ACCOUNTING FOR OVERLAPPING SECTORS OF BASE STATIONS IN ECOLOGICAL MONITORING ELECTROMAGNETIC FIELDS.**

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article presents the findings of a study into the impact of overlapping areas of cellular base stations on the spatial distribution of radio frequency electromagnetic fields in the city of Murino. Using GIS technology, the data were processed and a map was created showing the overlaps of base station areas on interpolated energy flux density values. The results revealed that in the study area, regions with maximum energy flux densities form in overlapping zones with five or more base station sectors using a central frequency of 900 MHz. Additionally, these areas also form when three or more sectors overlap and at least one of them uses the LTE standard.

Key words: electromagnetic fields, energy flux density, cellular base stations, GIS technologies.

АВТОРЫ СТАТЕЙ

АВДЕЕВА Таисия Михайловна	студент группы ИСТ-212 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
АВЕРИНА Алина Алексеевна	магистрант группы БИМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
АВЕРЬЯНОВ Максим Алексеевич	магистрант группы ЗР-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
АЛЕХИН Роман Вячеславович	магистрант группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
АЛЬКАТТАН Самех	магистрант группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
АМАЛИЕВ Хашим Сурхоевич	магистрант группы ИКТБ-38м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
АНДРИАНОВ Дмитрий Максимович	магистрант группы ИСТ-331м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

БАБКОВ Иван Николаевич	кандидат технических наук, доцент кафедры информационной безопасности компьютерных сетей, преподаватель базовой кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
БЕЛЯЕВ Богдан Романович	магистрант группы ИСТ-431м, художник-дизайнер управления маркетинга и рекламы Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
БЕНЧ Максим Николаевич	магистрант группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А.Бонч-Бруевича
БЕРЕЗКИН Александр Александрович	кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
БИРИХ Эрнест Владимирович	старшийпреподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
БОДНАРЧУК Кирилл Михайлович	студент группы ИБС-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
БОЛЬШАКОВА Кристина Евгеньевна	магистрант группы БИМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
БОНДАРЕНКО Игорь Борисович	кандидат технических наук, доцент, доцент кафедры информационно управляющих систем, заместитель декана по научной работе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

БОНДАРЬ Николай Алексеевич	магистрант группы ЗР-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
БОРИСЕНКО Иван Иванович	магистрант группы ИКТЗ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
БОТАЛОВ Андрей Алексеевич	аспирант кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
БУДАРИН Макар Эдуардович	магистрант группы ИКТЗ-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
БУДАРНЫЙ Глеб Сергеевич	магистрант группы ИКТБ-38м, ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
БУСЫГИН Константин Николаевич	магистрант Санкт-Петербургского государственного университета промышленных технологий и дизайна
ВАСИЛЬЕВ Иван Денисович	студент группы 2-МГ-56 Санкт-Петербургского государственного университета промышленных технологий и дизайна
ВИННИКОВ Семён Андреевич	магистрант группы ИКТЗ-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ВИТКОВА Лидия Андреевна	кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича .ru

ВОЛОШИНОВ Денис Вячеславович	доктор технических наук, профессор, заведующий кафедрой информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ГАВРИЛОВ Павел Русланович	магистрант группы ИКТБ-48м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ГЕХТ Антон Борисович	кандидат исторических наук, доцент, заведующий кафедрой истории и регионоведения, заместитель декана факультета социальных технологий и экономики данных по научной работе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ГОЛЬДИН Илья Игоревич	магистрант группы ИСТ-431м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ГРОМОВ Андрей Владимировчи	студент группы ИСТ-431м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ГРУЗДЕВ Александр Сергеевич	магистрант группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ГУГУНИШВИЛИ Лали Джумберовна	магистрант группы ИКТЗ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ДЕНИСОВ Александр Сергеевич	магистрант группы ИКМ-31з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ДЗИГОВСКИЙ Владислав Андреевич	магистрант группы ИКТЗ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

ДИБРОВА Олеся Павловна	магистрант группы ИСТ-431м, инженер технической поддержки кафедры системы обработки данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ДО Фук Хао	аспирант кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ДОГАДАЕВ Андрей Сергеевич	магистрант группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ДОЛУДЕНКО Богдан Владимирович	магистрант Санкт-Петербургского государственного университета промышленных технологий и дизайна
ДОМБРОВСКИЙ Роман Михайлович	магистрант группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ДОРОХОВА Екатерина Юрьевна	магистрант группы ИСТ-431м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ДРЕПА Владислав Евгеньевич	аспирант кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ДЮСМЕТОВА Азалия Айдаровна	магистрант группы ИКТБ-47м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЕГОРОВ Иван Михайлович	магистрант Санкт-Петербургского государственного университета промышленных технологий и дизайна
ЖЕЛТОВА Елена Петровна	доцент, кандидат педагогических наук, доцент кафедры иностранных языков Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

ЖУРАВЛЕВА Анастасия Сергеевна	магистрант группы ИКТЗ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЗАБОРОВСКАЯ Наталья Валентиновна	магистрант группы ИСМ-31з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЗУРАХОВ Владимир Сергеевич	магистрант Санкт-Петербургского государственного университета промышленных технологий и дизайна
ИВАНЕНКО Елена Александровна	магистрант группы ИСТ-331м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ИВАНОВ Никита Андреевич	магистрант группы БИ-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ИВАНОВ Роман Алексеевич	магистрант группы ИКТЗ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ИВАНОВА Анна Михайловна	ассистент кафедры истории и регионоведения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ИЛЬИН Ярослав Александрович	магистрант группы ИКТБ-38м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ИСМАИЛОВ Руслан Рявкатьевич	студент группы ИКТБ-41 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КАЗАНЦЕВА Анна Геннадьевна	кандидат технических наук, доцент кафедры экологической безопасности телекоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

КАЛМЫКОВ Азамат Асланбиевич	магистрант группы ИКТБ-48м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КАМАЛОВА Анастасия Олеговна	магистрант группы ИКТБ-47м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КАПУКОВ Алексей Иванович	магистрант группы ЗР-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КАРЛИНА Карина Сергеевна	студент группы 2-МГ-56 Санкт-Петербургского государственного университета промышленных технологий и дизайна
КВАША Надежда Владимировна	кандидат экономических наук, доцент, доцент кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КИЛИНА Мария Алексеевна	студент группы ЗР-12 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КИРИЛОВА Диана Сергеевна	магистрант группы ИКТЗ-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КИРИЧЕК Руслан Валентинович	доктор технических наук, профессор, ректор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, заслуженный деятель науки Санкт-Петербурга
КИСЕЛЁВ Данил Ильич	магистрант группы БИ-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

КИСТРУГА Антон Юрьевич	аспирант кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КЛИМЕНТЬЕВ Егор Николаевич	магистрант группы ЗР-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КНЯЗЕВА Елена Валерьевна	доцент Высшей школы дизайна и архитектуры, руководитель образовательной программы «Дизайн в цифровом маркетинге» Санкт-Петербургского политехнического университета Петра Великого
КОВЦУР Максим Михайлович	кандидат технических наук, доцент, доцент кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КОЗЛОВА Анна Николаевна	магистрант группы 3145401/40101 Санкт-Петербургского государственного политехнического университета Петра Великого
КОЗЫРЕВА Надежда Ивановна	кандидат технических наук, доцент кафедры информационной безопасности Поволжского государственного университета телекоммуникаций и информатики
КОЛМАКОВ Антон Евгеньевич	магистрант группы ИСТ-311м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КОМАРОВ Даниил Алексеевич	студент группы ИБС-01 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

КОНЕВ Алексей Романович	магистрант группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КОНЬКОВ Владимир Владимирович	магистрант группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КОПЫТОВА Елена Вячеславовна	магистрант группы ИСМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КОРЕНЮГИН Евгений Валерьевич	студент группы ИБС-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КОРНЮШКИН Дмитрий Александрович	аспирант группы кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КОРОВКИНА Екатерина Викторовна	магистрант группы ИСТ-311м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КОСОВ Никита Алексеевич	старший преподаватель кафедры информационной безопасности компьютерных сетей государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КРАСНИКОВ Даниил Андреевич	магистрант группы ИКТЗ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КРАСОВ Андрей Владимрович	кандидат технических наук, заведующий кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

КРИВОНОС Анастасия Олеговна	магистрант группы РСО-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КРЫЛОВ Андрей Альбертович	кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
КРЮКОВ Александр Николаевич	кандидат технических наук, доцент, доцент кафедры радиотехнических устройств Рязанского государственного радиотехнического университета имени В. Ф. Уткина
КУЛИНЫЧ Наталья Дмитриевна	магистрант Санкт-Петербургского государственного университета промышленных технологий и дизайна
КУЛЬНАЗАРОВА Анастасия Витальевна	доцент, кандидат политических наук, заместитель декана факультета социальных технологий и экономики данных по воспитательной работе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЛАГУТИНА Светлана Викторовна	магистрант группы ИКТБ-48м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЛЕВШУН Дмитрий Сергеевич	кандидат технических наук, доцент кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЛИТВИНОВ Владислав Леонидович	кандидат технических наук, доцент, и. о. декана факультета информационных технологий и программной инженерии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

ЛОСЕВА Алёна Сергеевна	магистрант группы ЭП-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЛЮБАЩЕНКО Тимофей Дмитриевич	магистрант группы ИКТЗ-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
МАВРИЧЕВ Вячеслав Константинович	магистрантгруппы ИСМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
МАМАЕВ Евгений Александрович	магистрант группы ИКТС-43м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
МАНЖУЛА Константин Алексеевич	магистрант группы ИКТБ-47м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, старший инженер сетевой инфраструктуры ПАО Сбербанк
МАНО Гифт	магистрант группы ИКТБ-47м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
МАРКОВ Александр Сергеевич	магистрант группы ИКТЗ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
МАРУШИНА Милена Евгеньевна	магистрант группы ИСТ-431м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
МАРШЕВА Наталия Владимировна	старший преподаватель кафедры иностранных языков Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
МИНОЧЕНКОВ Никита Сергеевич	магистрант группы ИБС-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

МИХАЙЛОВ Артем Александрович	магистрант группы ИКТЗ-41М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
МИХТЕЕВА Елена Юрьевна	кандидат химических неук, доцент, доцент кафедры высшей математики и физики Российского государственного гидрометеорологического университета
МУСАЕВА Татьяна Вагифовна	кандидат технических наук, доцент, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
НЕРОВНЫЙ Артём Викторович	старший преподаватель кафедры истории и регионоведения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
НИЖЛУКЧЕНКО Илья Дмитриевич	магистрант группы ИКТБ-48м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
НИКИФОРОВ Александр Вячеславович	магистрант группы ИКТБ-47м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
НИКИФОРОВ Павел Алексеевич	магистрант группы ИСТ-331м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
НОВИКОВ Дмитрий Сергеевич	магистрант группы ИКТБ-38м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ОЖЕГОВ Владислав Андреевич	магистрант группы ЭП-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ОКУДЖАВА Анна Элгуджаевна	специалист отдела менеджмента качества Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

ПАНТЮХИН Олег Игоревич	кандидат технических наук, доцент, доцент и преподаватель кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ПАТРУШЕВА Дарья Андреевна	старший преподаватель кафедры истории и регионоведения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ПЕНТЕГОВА Вероника Владимировна	магистрант группы ЭП-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ПЕСТОВ Игорь Евгеньевич	кандидат технических наук, доцент кафедры защищенных систем связи, преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ПЕТРОВ Дмитрий Валерьевич	магистрант группы ИСМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ПЕШКИНА Валерия Валерьяновна	магистрант группы ИКТЗ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ПИМАШИН Егор Николаевич	магистрант группы ИКТБ-48м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ПИЩУГИНА Александра Дмитриевна	студент группы ЭП-31м 2 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ПОЛЯКОВА Ксения Вячеславовна	магистрант Российского государственного гидрометеорологического университета

ПОЛЯНИЧЕВА Анна Валерьевна	старший преподаватель кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ПОТАПОВА Ирина Александровна	доктор физико-математических наук, доцент, профессор кафедры высшей математики и физики Российского государственного гидрометеорологического университета
ПРОНИЧЕВ Владислав Дмитриевич	магистрант группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ПРОХОРОВА Мария Викторовна	магистрант группы ИКТБ-48м Санкт-Петербургского государственного телекоммуникаций им. проф. Бонч-Бруевича
РАЙЛЯН Даниил Павлович	магистрант Санкт-Петербургского государственного университета промышленных технологий и дизайна
РАМЗАЕВ Кирилл Константинович	магистрант группы ИСТ-331м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
РОДИЧЕВ Иван Дмитриевич	магистрант группы ИКМ-31з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
РУБАЦКИЙ Роман Андреевич	магистрант Санкт-Петербургского государственного университета промышленных технологий и ди-зайна
РУДЕНКО Сергей Андреевич	магистрант группы ИКТБ-38м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
РУСОВА Альбина Александровна	студент группы № 3145401/40601 Санкт-Петербургского политехнического университета Петра Великого

САВИН Егор Алексеевич	магистрант группы ИКТм-41 Поволжского государственного университета телекоммуникаций и информатики
САМБУРОВ Кирилл Владимирович	кандидат географических наук, старший преподаватель кафедры истории и регионоведения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
САХАРОВ Дмитрий Владимирович	кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
СЕРЕГИН Илья Александрович	магистрант группы Р-42м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
СИДЕЛЬНИКОВ Антон Сергеевич	магистрант группы ИКТБ-48м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
СКОБЛИКОВА Анна Львовна	кандидат физико-математических наук, доцент, доцент кафедры высшей математики и физики Российского государственного гидрометеорологического университета
СМИРНОВ Даниил Николевич	ассистент кафедры информационной безопасность компьютерных сетей, ассистент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
СОТНИКОВ Александр Дмитриевич	профессор, доктор технических наук, доцент кафедры бизнес-информатики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
СПИЦЫН Михаил Александрович	магистрант группы ИКТЗ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

СТАРОВЕРОВ Андрей Игоревич	магистрант группы ИКТЗ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
СТАРОДУБЦЕВ Валентин Игоревич	студент группы 2-МГ-56 Санкт-Петербургского государственного университета промышленных технологий и дизайна
СТРАЙСТАР Валерия Александровна	магистрант группы ИКТБ-48м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
СТУРМАН Владимир Ицхакович	доктор географических наук, профессор, профессор кафедры экологической безопасности телекоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ТАЛАКИН Евгений Николаевич	магистрант группы ИКТЗ-31М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ТАМБОВСКИЙ Александрович Николаевич	магистрант группы ИКТБ-37м, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ТАРАТЫНОВ Иван Дмитриевич	магистрант группы ИКТб-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ТЕПЛОВ Кирилл Игоревич	магистрант группы ИКТм-41 Поволжского государственного университета телекоммуникаций и информатики
ТЕРЯЕВ Михаил Алексеевич	студент группы ИКТБ-48 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ТРАВКИНА Елизавета Алексеевна	студент группы ИКБ-14 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

ТРОФИМОВ Евгений Александрович	магистрант группы ИКТБ-48м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ТУРУСИДА Дональд	магистрант группы ИКТБ-47м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
УШАКОВ Игорь Александрович	кандидат технических наук, доцент, и. о. заведующего кафедрой информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ФЕДОТОВСКАЯ Анастасия Дмитриевна	магистрант группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А.Бонч-Бруевича
ФИЛИПОВ Эдуард Олегович	магистрант группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А.Бонч-Бруевича
ФИЛИППОВ Феликс Васильевич	кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ФИРСОВ Виталий Николаевич	магистрант группы ИСМ-31з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ХАДДАД Мухаммед Нур	студент группы Иктб-47м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЦВЕРИАНАШВИЛИ Иван Алексеевич	старший преподаватель кафедры истории и регионоведения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

ЦВЕТКОВА Ирина Юрьевна	магистрант группы ЭП-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЧАЛОВА Екатерина Игорьевна	магистрант Санкт-Петербургского государственного университета промышленных технологий и дизайна
ЧЕНСКИЙ Александр Александрович	магистрант группы ИКПИ-392м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЧЕРНОБРОВКИН Сергей Владимирович	адъюнкт кафедры автоматизированных систем специального назначения Военной академии связи имени Маршала Советского Союза С. М. Буденного
ЧИЗИБА Эндрю	магистрант группы ИКТБ-37м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЧИСТЯКОВ Александр Сергеевич	магистрант Санкт-Петербургского государственного университета промышленных технологий и дизайна
ЧУРЫНИНА Марина Владимировна	магистрант группы ЭП-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ШИЛИКОВ Дмитрий Александрович	магистрант группы ИКТБ-47м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ШИРОКОВ Андрей Алексеевич	магистрант группы ИСТ-431м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ШИТИКОВ Илья Евгеньевич	студент группы ИКМ-43з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

ШИЯН Андрей Анатольевич	кандидат педагогических наук, доцент, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ШТЕРЕНБЕРГ Станислав Игоревич	кандидат технических наук, доцент кафедры защищенных систем связи, заместитель декана факультета кибербезопасности по научной работе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ШУЛЫНДИНА Мария Сергеевна	магистрант группы ИКТЗ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЩЁГОЛЕВ Ефим Константинович	магистрант группы ИКТЗ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЯКОБСОН Дмитрий Алексеевич	магистрант группы ИКТЗ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЯКОВЛЕВА Татьяна Юрьевна	кандидат физико-математических наук, доцент, доцент кафедры высшей математики и физики Российского государственного гидрометеорологического университета
ЯКУБОВА Наиля Равильевна	старший преподаватель кафндры информационных управляющих системСанкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЯКУБОВИЧ Сергей Александрович	магистрант группы ИКТБ-38м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича
ЯССЕР Марк Владимирович	магистрант группы ИКТЗ-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

ЯЦЫШИН Илья Русланович — магистрант группы ЗР-31м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

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

ПОДГОТОВКА ПРОФЕССИОНАЛЬНЫХ КАДРОВ В МАГИСТРАТУРЕ В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ (ПКМ-2024)

Сборник лучших докладов
Том 2

Научное издание

Вёрстка
М. О. Мотыгина, М. С. Шулындина
Корректура
Д. Н. Яшугин
Дизайн логотипа Г. И. Юрьев
Подписано в печать 31.01.2025
Объём 39,31 усл.-печ. л.

Объединенная редакция рецензируемых научных изданий СПбГУТ
193232 СПб., пр. Большевиков, 22, корп. 1