



БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Сборник материалов
62-й научной конференции
аспирантов, магистрантов и студентов
13–17 апреля 2026 года



Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет информационной безопасности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

62-я научной конференции аспирантов,
магистрантов и студентов БГУИР

Сборник материалов

13–17 апреля 2026 года
Минск, БГУИР

Редакционная коллегия:

Главный редактор:

Дробот С.В. – декан ФИБ, канд. техн. наук, доцент, председатель.

Заместитель главного редактора:

Белоусова Е.С. – зам. декана по научной работе ФИБ, ответственный за подготовку, выпуск программы и электронного сборника материалов конференции по направлению «Информационная безопасность».

Члены редколлегии:

Давыдова Н.С. – канд. техн. наук, доцент каф. ИКТ;

Чепикова В.В. – ст. преподаватель каф. ИКТ;

Бойправ О.В. – канд. техн. наук, доцент, зав. каф. ЗИ;

Мокеров В.С. – ассистент каф. ЗИ;

Белошицкий А.П. – канд. техн. наук, доцент, доцент каф. ИИС;

Брилевский В.И. – ассистент каф. ИИС.

62-я научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 13-17 апреля 2026 г., БГУИР, Минск, Беларусь: сборник материалов. – Мн. – 2026. – 254 с.; ил.

Опубликованы материалы докладов, представленных на 62-й научной конференции аспирантов, магистрантов и студентов БГУИР по направлению «Информационная безопасность».

Материалы одобрены оргкомитетом и публикуются с учетом того, что авторская позиция и стилистические особенности публикаций полностью сохранены при соблюдении требований к оформлению.

Сборник предназначен для широкого круга специалистов в области систем инфокоммуникаций, защиты информации, информационно-измерительных систем, а также будет полезен научным и инженерно-техническим работникам, преподавателям, аспирантам, магистрантам и студентам технических вузов.

СОДЕРЖАНИЕ

СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ»

Программный комплекс статического анализа уязвимостей исходного кода на JavaScript и TypeScript Батура А.И.	8
Обнаружение речевой активности в условиях реального шума До А.Т.	13
Сравнительный анализ сканеров уязвимостей Ляшко М.И.	19
Виртуальная инфраструктура для проведения кибертренировок Несмашный Е.А., Румас С.С., Потапович И.А., Ананченко Р.А., Дубовский В.В.	24
Анализ методов защиты веб-приложений от атак типа SQL-инъекция Сальникова В.А.	28
Методика интегрированного анализа событий в информационных системах Сташкевич С.О.	33
A Machine Learning Framework for Multiclass Detection of DDoS Network Attacks Pan Huiqin	38
Efficient Web-Vulnerability Detection Technique Using Hybrid SAST-DAST Analysis and Machine Learning Kondo K.N.	40
Интеллектуальные методы выявления киберугроз на основе Big Data Ходжамаммедов М.М.	43
Test Results for the Method of Information Security Event Management in Linux-Kernel-Based Operating Systems Nguyen H.H.	44
Research and Development of Plagiarism Detection Methods Based on Deep Neural Networks Nguyen L.T.	46
Электромагнитная совместимость блоков беспилотных летательных аппаратов Асиненко А.М.	49
Программная платформа для фишинговых симуляций Биюмен Е.А.	52
Метод обнаружения синтезированных видео без специального оборудования Богусевич О.А.	55
Интеграция облачного сервиса Cloudflare как элемента защиты информационной системы от DDoS-атак Бодров Д.А.	57
Исследование амплитудно-импульсной и широтно-импульсной модуляции в контексте скрытой передачи информации Боровиков К.А.	60
Сценарий тестирования на проникновение в сервис онлайн-разархиватора Максимович Р.А., Боровиков К.А.	63
Алгоритмическое обеспечение локально-адаптивного агента киберразведки Войткус И.А.	66
Локально-адаптивный Telegram-агент для OSINT-разведки Войткус И.А.	68
Методика защиты RFID-меток от атак копирования и ретрансляции Ворожцов А.О.	71
Исследование эффективности различных видов дискретной модуляции для систем защищенной передачи данных Дейкало И.С.	72
Архитектура нейросетевой системы семантической инверсии для генерации псевдоречи Денскевич А.Д.	75
Анализ уязвимостей протокола маршрутизации OSPF и методы их уменьшения в корпоративных сетях Долгая А.С.	78

Обзор современных методов глубокого обучения в области обнаружения аномалий в информационных сетях	
Драгунов А.Д.	81
Квадратурная амплитудная модуляция (QAM) как основа современных высокоскоростных систем связи: анализ уязвимости к ошибкам синхронизации	
Егоров В.А.	83
Сравнительный анализ технологий генерации одноразовых паролей	
Каршакевич В.М.	86
Разработка обучающей игры для формирования навыков по защите от угроз информационной безопасности	
Клиндухов Я.А., Мажаева С.Д.	89
Синергетический эффект при комбинировании разнородных кибератак	
Ковалевич М.А.	93
Сравнительный анализ алгоритмов хеширования	
Ковалевич М.А., Филипченко К.В.	96
Амплитудно-фазовая модуляция как средство повышения скрытности передачи данных	
Колесник Н.В.	99
Сравнение рекуррентных нейронных сетей для обработки речевых сигналов	
Коржова И.А.	102
Обеспечение безопасности серверной инфраструктуры на базе фреймворка Ktor для анализа оперативной обстановки	
Кочеров Р.С.	105
Актуальные вопросы изменения законодательства Республики Беларусь в сфере кибербезопасности	
Лукашевич З.Ю.	108
Образовательный хаб для подготовки специалистов в области защиты информации	
Маршалова К.Ц., Бююмен Е.А.	110
Методика тестирования на проникновение для подразделений кибербезопасности	
Михайловский С.Г.	112
Амплитудно-импульсная и широтно-импульсная модуляции в системах управления и защиты информации	
Осадчий И.В.	115
Методы активной и пассивной защиты от атак типа BadUSB на основе эмуляции HID-устройств	
Погирейчик В.В.	118
Оценка защищенности и практические методы эксплуатации уязвимостей корпоративных межсетевых экранов на примере Check Point T-110	
Седляр А.С., Боздаг Бора	120
Особенности реализации нейросетей на платформах STM32/CORTEX-M для задач обнаружения закладных устройств импульсно-рефлекторным методом	
Сурвило И.С.	122
Исследование скрытности сигналов с различными видами манипуляциями на основе анализа их спектральных характеристик	
Фам Тхи Хонг Ньунг, Михайловский Д.А.	125
Программный модуль защиты H17-сообщений: аналитический обзор литературных источников	
Фомин Д.А.	127
Государственное регулирование деятельности в сфере защиты информации: сравнительный анализ подходов Беларуси и стран Европейского союза	
Шерышев Р.В.	129
Методика обнаружения IoT-атак при помощи SIEM-системы Wazuh	
Шумченя М.А., Лукашик Л.А.	131
Интеграция модели машинного обучения в межсетевой экран CHUWALL	
Яниславский К.О., Мартинкевич Д.М.	134

СЕКЦИЯ «СИСТЕМЫ И СЕТИ ИНФОКОММУНИКАЦИЙ»

Оценка эффективности современных детекторов объектов в задачах одновременной локализации, картографирования и трекинга (SLAMOT) Левоненко И.И., Робачевский А.Д.	137
Модуль умножителя частоты в диапазоне 18-40 ГГц Кийко В.В.	145
Игровая индустрия как сфера ИТ и ИКТ. Состояние и перспективы развития в Республике Беларусь Мацкевич В. В.	148
Сравнительный анализ производительности сетевых топологий с использованием методов теории массового обслуживания Бондарь А.В., Вабищевич А.С., Михайлов К.В., Позняк В.М.	155
OSINT-технологии в задачах выявления поверхности атак корпоративных инфокоммуникационных систем Лапина С.С.	159
Гибридная архитектура: интеграция блокчейна и edge computing в управлении беспилотным транспортом Алмаждуб М.А.	161
Интеллектуальная система адаптивного мониторинга качества восприятия инфокоммуникационных услуг Элтарabili М.С.	164
Повышение отказоустойчивости в компьютерных сетях Скиб А.И.	168
Сравнительный анализ протоколов VPN (IPsec vs OpenVPN vs WireGuard) для безопасной передачи данных Пурус А.О., Голубев А.А.	171
Сравнительный анализ проводных, беспроводных и ячеистых сетей Бродович Б.Е.	175
Современные многоканальные приемники СВЧ-диапазона: классификация и области применения Шапошникова Н.П.	176
Методы оптимизации агрегации событий в системах Real-Time Bidding при высоких нагрузках Анциферова Е.И.	177
Сравнительный анализ затухания сигнала в гетерогенных сетях сотовой связи на основе измерений RSSI в городских условиях Минска Родионов М.А.	181
Роль маппинга в проектировании и эксплуатации современных инфокоммуникационных сетей Романюк Я.С.	185
Повышение эффективности беспилотных систем через совместное управление энергопотреблением и подсистемами видеонаблюдения Воронович Д.Ю., Максак М.Ю.	188
Кросс-модальный перенос знаний как фактор развития логического рассуждения в языковых моделях Оруджев М.М.	191
Многофакторная аутентификация (MFA) как базовый метод защиты корпоративной сети Жуков Н.А.	192
Dynamic Channel Modeling and Performance Analysis for UAV Communications Chi Zhang	195
Deep Learning-Based Skeleton Extraction Jiarou Wang	197
Vehicle-mounted vision-lidar intermediate fusion perception algorithm based on dynamic dbscan and adaptive weights Xinyu Zhang	199
Semantic Communication System for Vehicle Detection Based on CNN Encoder and Supernet Architecture Qikai Wang	202
Comparison of DSO and ORBSLAM3 in Indoor Environments Using Monocular Visual SLAM Qiyao Yang	204

UAV-to-Satellite Image Geo-Localization via Dual-Branch Deep Learning: A Comparative Study of ResNet-18 and MLP-Mixer	
Qinghan Yu	206
A Comparative Study of Error-Correcting Codes for Multi-Cell Upsets in Memories: CLC and OPCoSA	
Lin Wei	208
A Review of Collaborative Optimization of Task Allocation and Path Planning in Multi-Robot Systems	
Xinyue Shao	210
Performance Analysis of LS and LMMSE Channel Estimation for 5G NR OFDM Systems over Time-Varying Fading Channels	
Shuo Wang	214
Multi-Sensor Fusion for Mobile Robot Perception	
Bin Zhang	216
Методика повышения помехоустойчивости видеоинформационного обмена в сетях БПЛА на основе регрессионного восстановления фоновых областей	
Купрейчик А.С.	219
Методы обработки PDF-файлов в финансовых системах	
Матлаш Т.С.	225
Архитектура подсистемы блокчейн для медицинских данных	
Кацко М.О.	226
Hybrid Transformer-Graph Neural Network Feature Matching based Methodology for Robust Template Object Localization	
Bach N.V.	230
Time Delay-Phase Harmonic Model of Transmitted Laser Signal for Gas Concentration Estimation	
Bach N.V.	234

СЕКЦИЯ «ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ СИСТЕМЫ»

Методика определения метрологических характеристик устройств сличения национального эталона мощности электромагнитных колебаний	
Доронина А.В.	237
Аппаратно-программная архитектура информационно-измерительной системы с сетевыми возможностями	
Зокиров Д.Т.	241
Спутниковый терминал связи VSAT	
Коледа В.В.	243
Методы обеспечения целостности и достоверности данных в информационно-измерительных приборах критической инфраструктуры	
Маевский П.К.	246
Применение нейросетей для линеаризации термоЭДС термопар как альтернатива полиномиальной модели	
Мороз А.С.	249
Анализ методов и средств контроля метрологических характеристик многоканальных приемных устройств	
Шапошникова Н.П.	251

СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ»

УДК 004.4:004.056.5

ПРОГРАММНЫЙ КОМПЛЕКС СТАТИЧЕСКОГО АНАЛИЗА УЯЗВИМОСТЕЙ ИСХОДНОГО КОДА НА JAVASCRIPT И TYPESCRIPT

Батуро А.И., студент гр.461401

Белорусский государственный университет информатики и радиоэлектроники¹
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук, доцент

Аннотация. Рассмотрена разработка сервиса статического анализа безопасности для JavaScript и TypeScript на основе парсера tree-sitter, правил по абстрактному синтаксическому дереву и внутрифайлового анализа загрязнения данных с ограниченной межпроцедурностью и пакетной передачей файлов через REST API. Результаты сопоставляются с таксономией CWE; поддерживаются форматы JSON, SARIF 2.1.0 и асинхронный режим выполнения. Описаны архитектура комплекса, состав правил, особенности анализа потоков данных и программный интерфейс. Приведены количественные результаты сопоставления с инструментом Semgrep на внутреннем каталоге синтетических примеров и на внешнем корпусе semgrep-rules/javascript, пояснена методика трёх контуров оценки, сформулированы ограничения и направления развития.

Ключевые слова. статический анализ, JavaScript, TypeScript, абстрактное синтаксическое дерево, анализ загрязнения данных, CWE, SARIF, Semgrep, REST API, оценка качества, безопасность приложений.

Введение. Серверная и клиентская логика современных информационных систем всё чаще реализуется на языках JavaScript и TypeScript: это касается как веб-приложений, так и микросервисов на платформе Node.js. Такой стек ускоряет разработку, но сохраняет фундаментальные риски, связанные с обработкой данных, поступающих из сети: инъекции в языки запросов к базам данных и в командную оболочку, межсайтовый скриптинг, обход ограничений при доступе к файлам, небезопасная десериализация, использование слабых криптографических примитивов и ряд других классов ошибок, систематизированных в перечнях OWASP и таксономии CWE [1, 2].

Обнаружение подобных дефектов на этапе разработки возможно средствами статического анализа, не требующего исполнения программы на реальных входных данных. На практике применяются как обобщённые графовые представления кода с последующим поиском опасных путей [3], так и более лёгкие по вычислительной стоимости схемы, основанные на сопоставлении шаблонов с абстрактным синтаксическим деревом и на ограниченном анализе потоков данных. Важно согласовать точность и полноту анализа с требованиями к времени отклика при интеграции в конвейер непрерывной интеграции и с необходимостью обмена результатами с системами управления дефектами; для последнего широко используется стандарт SARIF [6].

Цель работы – разработать и описать программный комплекс, который для кода на JavaScript и TypeScript выполняет сочетание правил на абстрактном синтаксическом дереве и анализа загрязнения данных с явно заданными границами межпроцедурного охвата, предоставляет доступ по протоколу HTTP в форматах JSON и SARIF и сопоставим по результатам с распространённым открытым анализатором Semgrep [7] в рамках воспроизводимой методики.

Задачи исследования:

1. Обосновать выбор архитектуры на основе инкрементально поддерживаемого парсера и модульных правил.
2. Описать модель источников и стоков для анализа загрязнения и правила сопоставления с типовыми фреймворками.
3. Привести состав программного интерфейса и сценариев развёртывания.
4. Сформулировать методику оценки на внутреннем каталоге и внешнем корпусе;
5. Интерпретировать полученные численные результаты и ограничения комплекса.

Практическая значимость заключается в возможности встраивания сервиса в учебные лаборатории по безопасности программного обеспечения, в опытные конвейеры проверки исходного кода и в сравнительные исследования средств анализа без изменения исходного кода целевого проекта – достаточно HTTP-запроса с текстом файла или пакета файлов.

Архитектура и состав модулей. Программный комплекс реализован как сетевой сервис. Подсистема программного интерфейса построена на фреймворке FastAPI и обеспечивает валидацию входных данных, маршрутизацию запросов и согласование типов ответа. Ядро оркестрации принимает решение о языке входного фрагмента, последовательно или параллельно по политике конфигурации запускает разбор, набор правил и при включённой опции – анализ загрязнения данных, агрегирует находки, вычисляет статистику и при необходимости формирует журнал SARIF. Парсеры JavaScript и TypeScript опираются на библиотеку tree-sitter [5], что даёт устойчивость к синтаксису

современных конструкций языка и возможность точного привязки диагностик к позициям в исходном тексте.

Реестр правил организован по идентификаторам вида JS-*-NNN и покрывает, в частности, инъекции SQL и NoSQL, межсайтовый скриптинг (включая React dangerouslySetInnerHTML), инъекции команд, обход пути, загрязнение прототипа, жёстко зашитые секреты, небезопасную десериализацию, слабую криптографию, открытые перенаправления, обращения к внешним URL по данным пользователя (SSRF), уязвимости к регулярным выражениям с катастрофическим откатом (ReDoS). Каждая находка при наличии локальной базы может быть обогащена ссылкой на идентификатор CWE.

Модуль анализа загрязнения данных реализует сопоставление объявленных источников с объявленными стоками на графе, выводимом из абстрактного синтаксического дерева, с учётом вызовов функций в пределах одного файла и при пакетном запросе – с объединением индекса функций по всем переданным путям. Для асинхронной обработки длительных запросов предусмотрена постановка задачи в очередь и опрос состояния по идентификатору сканирования с использованием брокера сообщений и исполнителей фоновых задач; синхронный режим ограничен по размеру входных данных для предсказуемого времени отклика.

Конвейер обработки фрагмента исходного кода представлен на рисунке 1, связь модулей каталога исходного кода комплекса – на рисунке 2.

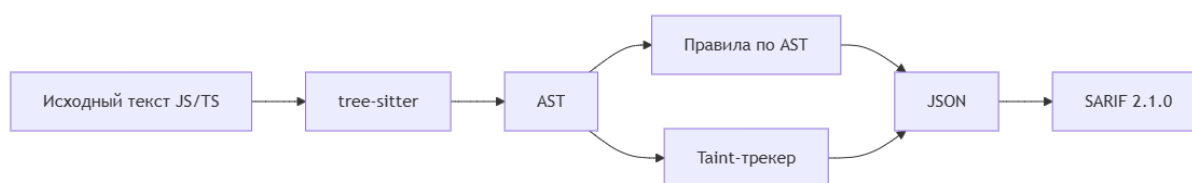


Рисунок 1 – Конвейер обработки исходного кода

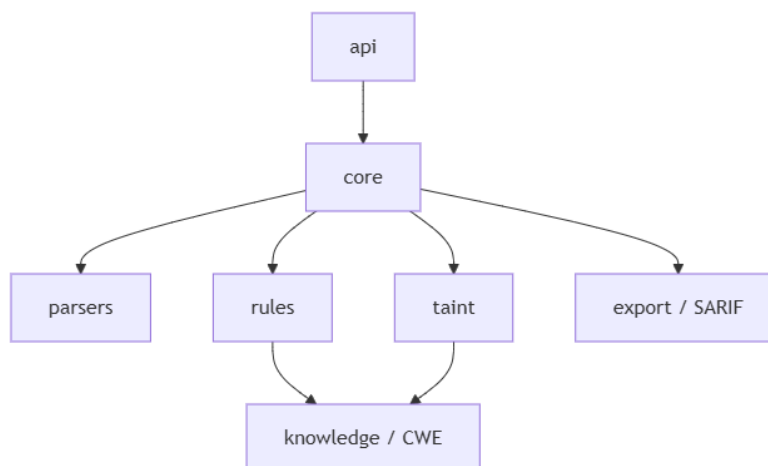


Рисунок 2 – Структура модулей программного комплекса (src/analyzer/)

Программный интерфейс и сценарии использования. Основные конечные точки HTTP следующие: синхронный анализ одного фрагмента исходного кода с телом запроса в формате JSON и опциональным выбором ответа в виде журнала SARIF 2.1.0; синхронный анализ пакета файлов с передачей отображения «путь – текст» для построения сквозного индекса вызываемых функций при анализе загрязнения; асинхронный анализ с возвратом идентификатора и последующим опросом ресурса результатов; перечисление доступных правил; проверка работоспособности сервиса. В ответе синхронного режима помимо списка находок и статистики передаётся перечень идентификаторов правил, при выполнении которых возникло исключение, чтобы оставшиеся правила всё же, отработали.

Типовой сценарий для разработчика – отправка содержимого файла с указанием псевдопути и флага включения анализа загрязнения. Для приложений, разбитых на несколько модулей, предпочтителен пакетный запрос: в него включают как точку входа (например, маршруты), так и файлы с определениями вспомогательных функций, иначе вызовы, разрешённые только по графу импорта, не будут связаны с телами функций в другом файле. Развёртывание возможно, как локально (веб-сервер приложения), так и в контейнерах с выносом брокера и хранилища состояния асинхронных задач.

Методы статического анализа. Разбор исходного текста в абстрактное синтаксическое дерево выполняется парсером *tree-sitter*; далее правила обходят узлы дерева и срабатывают при выполнении логических условий, характерных для класса уязвимости. Например, для инъекции SQL учитывается конкатенация или шаблонная подстановка пользовательских данных в строку запроса. Такой подход даёт понятные сообщения с привязкой к строке исходного кода и умеренную вычислительную сложность на файл.

Анализ загрязнения данных дополняет правила: он отслеживает распространение «загрязнения» от источников к стокам. В качестве источников используются соглашения об именовании и структуре объектов запроса, характерные для распространённых веб-фреймворков (в стиле Express, Koa, Fastify), а также ряд глобальных объектов среды исполнения. Стоки включают вызовы методов выполнения запросов к базам данных (в том числе сырого SQL в ORM), функции порождения процессов и выполнения строк кода, операции файловой подсистемы, перенаправления ответа и другие конфигурируемые шаблоны. Цепочка необязательного доступа при сопоставлении с шаблонами нормализуется к виду с обычной точкой, чтобы не пропускать эквивалентные вхождения.

Для вызовов вида выполнения запроса с отдельной строкой шаблона и массивом параметров загрязнение, попавшее только в массив параметров, трактуется как привязка к placeholder-ам, а не как встраивание в текст SQL, что снижает число ложных срабатываний на параметризованных API. Подстановки в шаблонных литералах анализируются по узлам подстановки; распространение через вспомогательные функции в одном файле и через возвращаемое значение функции учитывается в пределах ограниченной глубины вложенности вызовов. При передаче нескольких файлов индекс имён функций объединяется, что позволяет связать вызов в одном файле с определением в другом, если оба файла явно включены в запрос.

Результаты сопоставления с инструментом Semgrep и методика оценки. В качестве воспроизводимого эталона сравнения выбран инструмент Semgrep, получивший широкое распространение как в промышленной практике, так и в исследовательской среде благодаря обширным открытым наборам правил [7]. Поскольку однозначная атрибуция корректности срабатывания на уровне отдельной строки кода невозможна без независимой экспертной разметки уязвимостей, в настоящей работе применяется методика, основанная на трёх взаимодополняющих контурах оценки:

1 Внутренний каталог небольших синтетических фрагментов с метками «уязвимый / безопасный» и ожидаемым идентификатором правила; по нему вычисляются истинно положительные, истинно отрицательные, ложноотрицательные и ложноположительные исходы относительно меток каталога (сценарий `eval.cli run`). Каталог предназначен для регрессионного контроля при изменении кода анализатора, а не как репрезентативная выборка промышленных проектов.

2 Внутренний каталог небольших синтетических фрагментов с параллельным запуском Semgrep и сопоставлением строк находок с учётом файла отображения идентификаторов правил Semgrep на идентификаторы анализатора (`eval.cli compare`). Совпадения по строкам отражают согласованность при выбранной политике эквивалентности, а не эталонную истину.

3 Обход дерева файлов внешнего корпуса (в примере ниже – каталог javascript из репозитория `semgrep-rules`), единичный прогон Semgrep по конфигурации из того же дерева и построчное сопоставление с находками анализатора при политике B, когда учитываются все срабатывания обоих инструментов на общем множестве файлов (`corpus_parser_eval`).

Схема трёх контуров представлена на рисунке 3.

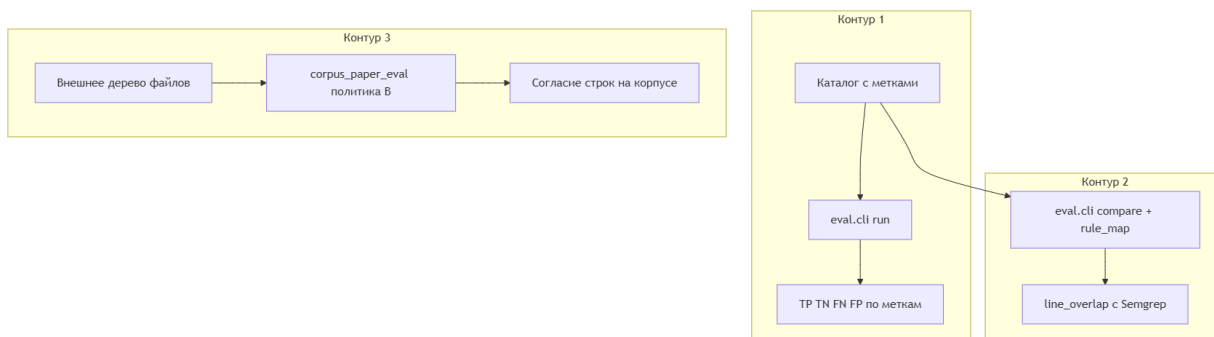


Рисунок 3 – Три контура оценки относительно каталога и корпуса

Опорные значения показателей, зафиксированные в документации репозитория для конфигурации Semgrep 1.156.0 с набором правил `semgrep-rules` (коммит 28db38e) и коммитом анализатора b59ef6c, приведены ниже. Воспроизведение результатов в последующих работах

требует явного указания версий используемых инструментов, идентификаторов коммитов наборов правил и полной командной строки запуска. Результаты для внутреннего каталога (87 тестовых случаев без метки SKIP, сценарий eval.cli compare) представлены в таблице 1.

Таблица 1 – Результаты по внутреннему каталогу

Показатель	Значение
Исходы по меткам каталога: TP / TN / FN / FP	45 / 33 / 2 / 7
Суммарное число находок: анализатор / Semgrep	76 / 27
Число совпавших пар строк (line_overlap)	16
Суммарно только анализатор / только Semgrep	31 / 7
Кейсы с хотя бы одной строкой Semgrep в карте правил	22
Кейсы с не менее чем одной совпавшей парой строк	15

Метрики TP, TN, FN и FP вычислены относительно меток внутреннего синтетического каталога, а не относительно независимой экспертной разметки. Превышение суммарного числа диагностических сообщений анализатора над числом сообщений Semgrep обусловлено двумя факторами: во-первых, одна строка исходного кода может одновременно активировать правило на дереве разбора и порождать путь загрязнения, что фиксируется как два отдельных срабатывания; во-вторых, наборы правил двух инструментов различаются по охвату классов уязвимостей. Величина пересечения по строкам определяется файлом отображения rule_map.yaml (equivalence_rules) и лишена интерпретационного смысла без предварительного согласования идентификаторов правил Semgrep с соответствующими правилами анализатора. Два зафиксированных ложноотрицательных исхода (FN) – для случаев NOSQL-HARD-VULN-01 и SSRF-HARD-VULN-01 – определяют приоритетные направления доработки: расширение соответствующих правил и уточнение модели стоков.

Результаты для внешнего корпуса (каталог semgrep-rules/javascript, 174 файла, политика B, сценарий corpus_parser_eval) представлены в таблице 2.

Таблица 2 – Результаты по внешнему корпусу

Показатель	Значение
Всего находок Semgrep / анализатора	868 / 219
Совпавшие пары строк	116
Только анализатор / только Semgrep	76 / 613

На корпусе Semgrep даёт существенно большее число срабатываний, поскольку конфигурация включает широкий набор примеров и тестов правил; анализатор нацелен на ограниченный перечень классов CWE-ориентированных правил с иной семантикой. При этом 116 совпадений по строкам показывают пересечение поведения на конкретных местах кода; 76 строк с сообщениями только анализатора и 613 – только Semgrep подчёркивают необходимость отдельной интерпретации и, при желании, комбинирования инструментов в конвейере, а не замены одного другим.

Ограничения. Поддерживаются только языки JavaScript и TypeScript. Анализ статический: не моделируется полное поведение программы при исполнении, не учитываются динамически вычисляемые имена свойств и сложные сценарии рефлексии без явных шаблонов в коде.

Граф зависимостей по import и require не строится автоматически: для разрешения вызова функции, определённой в другом модуле, соответствующий файл должен быть включён в пакетный запрос. Глубина межпроцедурного разбора в анализе загрязнения ограничена константой MAX_INTERPROC_DEPTH = 5. При переносе загрязнения через возвращаемое значение используется первое встреченное в теле функции выражение return. Краткая форма метода в объектном литерале не используется как единственное тело вызываемой функции без отдельного объявления в индексе функций.

Действуют ограничения на размер тела синхронного запроса, на число файлов и на суммарный объём текста в пакете; при задании бюджета времени анализ может быть прерван, а этап анализа загрязнения – пропущен, что должно учитываться при сравнении результатов.

Отдельные правила могут завершиться исключением во время выполнения; они перечисляются в поле failed_rules, остальные правила продолжают работу. Внутренний каталог не заменяет независимый набор промышленных уязвимостей с экспертной разметкой.

Заключение. В работе описан программный комплекс статического анализа уязвимостей для JavaScript и TypeScript, сочетающий правила на абстрактном синтаксическом дереве и анализ загрязнения данных с явно оговорёнными границами, стандартизированные интерфейсы JSON и SARIF и воспроизводимую методику сопоставления с Semgrep на каталоге и на внешнем дереве файлов. По внутреннему каталогу достигнут высокий уровень истинно отрицательных исходов на безопасных фрагментах при умеренном числе ложных срабатываний и двух оставшихся ложно

отрицательных исходах на сложных сценариях NoSQL и SSRF. На корпусе semgrep-rules/javascript инструменты демонстрируют различную плотность сообщений и частичное пересечение по строкам, что ожидаемо при разной полноте набора правил.

Направления дальнейшей работы включают построение или использование графа модулей для автоматического включения зависимостей, расширение правил и стоков для NoSQL и SSRF, уточнение моделей санитизации данных и накопление размеченного корпуса промышленного кода для оценки полноты, и точности независимо от эталона Semgrep.

Список использованных источников:

1. OWASP Top Ten [Электронный ресурс]. – Режим доступа: <https://owasp.org/www-project-top-ten/> (дата обращения: 29.03.2026).
2. Common Weakness Enumeration (CWE) [Электронный ресурс]. – Режим доступа: <https://cwe.mitre.org/> (дата обращения: 29.03.2026).
3. Yamaguchi F. et al. Modeling and Discovering Vulnerabilities with Code Property Graphs / F. Yamaguchi et al. // Proc. IEEE Symposium on Security and Privacy. – 2014.
4. Livshits B. et al. In Defense of Soundness: A Manifesto / B. Livshits et al. // Commun. ACM. – 2015. – Т. 58. – № 2.
5. Tree-sitter [Электронный ресурс]. – Режим доступа: <https://tree-sitter.github.io/tree-sitter/> (дата обращения: 29.03.2026).
6. SARIF Version 2.1.0 [Электронный ресурс]. – Режим доступа: <https://docs.oasis-open.org/sarif/sarif/v2.1.0/> (дата обращения: 29.03.2026).
7. Semgrep: оверлейные правила для статического анализа [Электронный ресурс]. – Режим доступа: <https://semgrep.dev/> (дата обращения: 29.03.2026).
8. FastAPI [Электронный ресурс]. – Режим доступа: <https://fastapi.tiangolo.com/> (дата обращения: 29.03.2026).

UDC 004.4:004.056.5

SOFTWARE COMPLEX FOR STATIC VULNERABILITY ANALYSIS OF JAVASCRIPT AND TYPESCRIPT SOURCE CODE

Baturo A.I., student gr.461401

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Belousova E.S. – PhD in Technical Sciences, Associate Professor

Annotation. A static security analysis service for JavaScript and TypeScript is presented, based on the tree-sitter parser, abstract syntax tree rules, and intra-file taint analysis with limited interprocedural scope. Files are transferred in batches via REST API. Findings are mapped to the CWE taxonomy; JSON, SARIF 2.1.0 formats, and asynchronous execution are supported. The system architecture, rule set, data flow analysis features, and API are described. Quantitative comparison with Semgrep is provided on an internal synthetic catalog and the external semgrep-rules/javascript corpus.

Keywords. static analysis, JavaScript, TypeScript, abstract syntax tree, taint analysis, CWE, SARIF, Semgrep, REST API, quality assessment, application security.

УДК 004.934

ОБНАРУЖЕНИЕ РЕЧЕВОЙ АКТИВНОСТИ В УСЛОВИЯХ РЕАЛЬНОГО ШУМА

До А.Т., магистрант гр.467311

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Зельманский О.Б. – канд. тех. наук, доцент

Аннотация. Обнаружение речевой активности (Voice Activity Detection, VAD) в зашумленных средах, особенно при низком отношении сигнал-шум (Signal-to-Noise Ratio, SNR), остается сложной задачей для реальных приложений, таких как слуховые аппараты, умные колонки и системы телеконференций. Традиционные методы VAD часто не способны обобщаться на различные типы шума и уровни SNR. В данной статье мы предлагаем новую структуру VAD на основе глубокого обучения, которая эффективно решает эту проблему. Наш подход использует модуль многомасштабного извлечения признаков для захвата как кратковременных деталей, так и долгосрочной контекстной информации из речевого сигнала. Кроме того, мы внедряем механизм самовнимания для динамического фокусирования на наиболее информативных временных кадрах и частотных полосах, что повышает устойчивость модели к нестационарным шумам. Мы оцениваем наш метод на нескольких эталонных наборах данных, включая DNS Challenge и корпус CHiME-3, при различных условиях SNR в диапазоне от -5 дБ до 15 дБ. Экспериментальные результаты показывают, что предлагаемая модель значительно превосходит современные базовые методы, достигая более высокой точности и меньшего уровня ложных тревог, особенно в условиях экстремально низкого SNR.

Ключевые слова. обнаружение речевой активности, глубокое обучение, низкое отношение сигнал-шум, зашумленные среды, многомасштабное слияние признаков, механизм самовнимания, двунаправленная GRU, DNS Challenge.

Актуальность и мотивация: VAD является критически важным этапом предварительной обработки во многих системах обработки речи: автоматическое распознавание речи (ASR), речевое кодирование, улучшение речи и т.д. В реальных условиях принимаемый сигнал часто подвержен воздействию различных типов шума: фоновый шум, импульсный шум, структурированный шум (стук клавиатуры, шаги) и особенно в области низкого SNR (ниже 0 дБ).

Одной из главных проблем при разработке надежных систем обнаружения речевой активности является многообразие типов шума, с которыми система может столкнуться в реальных условиях эксплуатации. Это могут быть как стационарные шумы, например белый или розовый шум, так и более сложные акустические помехи, включая шум толпы (речь нескольких говорящих одновременно), машинный шум, звуки транспорта и другие. Существенное усугубляющее влияние оказывает низкое отношение сигнал-шум (SNR). Когда значение SNR опускается ниже 0 дБ, энергия шума начинает превышать энергию речевого сигнала, что делает задачу различения речевых и неречевых фрагментов чрезвычайно сложной даже для современных методов глубокого обучения. Дополнительную трудность представляет нестационарный характер многих видов шума: в отличие от стационарных помех, такие шумы, как проезжающие автомобили, хлопки дверей или внезапные громкие звуки, постоянно меняют свои спектральные и энергетические характеристики во времени, что требует от VAD-алгоритмов способности быстро адаптироваться к изменяющимся акустическим условиям. Наконец, критически важным ограничением для большинства практических приложений, включая слуховые аппараты, системы голосового управления и устройства умного дома, является требование низкой задержки (low-latency): алгоритм VAD должен работать в реальном времени, принимая решение о наличии речи с минимальной задержкой, что накладывает жесткие ограничения на вычислительную сложность модели и не позволяет использовать чрезмерно глубокие или ресурсоемкие архитектуры.

В области обнаружения речевой активности (VAD) за последние десятилетия было предложено множество подходов, которые можно условно разделить на традиционные методы и методы на основе глубокого обучения. Традиционные методы, такие как алгоритмы, основанные на анализе энергии сигнала, частоте пересечения нуля (zero-crossing rate), спектральной энтропии, а также статистические подходы с использованием гауссовых смесей (GMM), демонстрируют приемлемую эффективность в условиях высокого отношения сигнал-шум и стационарных помех. Однако их главным ограничением является значительное снижение точности при низком SNR и в присутствии сложных, особенно нестационарных, шумов, что делает их непригодными для многих современных приложений. Современные методы на основе глубокого обучения позволили существенно продвинуться в решении этих проблем. В частности, широкое распространение получили архитектуры на основе глубоких нейронных сетей (DNN), сверточных нейронных сетей (CNN) и рекуррентных сетей (LSTM), которые способны автоматически извлекать релевантные признаки из речевых сигналов [1]. Дальнейшее развитие связано с комбинированием сверточных и рекуррентных слоев в рамках архитектуры CRNN (сверточная рекуррентная нейронная сеть), что позволяет эффективно моделировать как локальные спектрально-временные паттерны, так и долгосрочные

зависимости в сигнале [2]. В последние годы активно исследуется применение механизмов внимания (attention mechanisms), которые позволяют модели динамически фокусироваться на наиболее информативных частях входного сигнала, что особенно важно в условиях нестационарных помех [3]. Несмотря на достигнутый прогресс, в существующих исследованиях сохраняется значительный пробел: большинство предложенных методов все еще не способны одновременно эффективно работать в широком диапазоне типов шума и при экстремально низких значениях SNR (ниже 0 дБ). Кроме того, отсутствуют адаптивные механизмы, способные гибко подстраиваться под различные акустические условия без существенного увеличения вычислительной сложности, что открывает перспективы для дальнейших исследований в данной области.

В данной работе предлагается новый подход к обнаружению речевой активности, ориентированный на работу в условиях сложного шума и низкого SNR. Основные вклады исследования включают: (1) архитектуру многомасштабного слияния признаков для захвата характеристик на различных временных разрешениях; (2) интеграцию пространственно-временного механизма самовнимания для динамической фокусировки на информативных частотно-временных областях; (3) создание тестового набора данных с несколькими типами шума в диапазоне SNR от -5 дБ до 15 дБ; (4) экспериментальное подтверждение значительного улучшения производительности по сравнению с базовыми методами, особенно в области низкого SNR.

На рисунке 1 представлена общая архитектура предлагаемой структуры VAD на основе глубокого обучения. Модель состоит из пяти основных модулей: извлечение признаков, многомасштабное слияние признаков, пространственно-временное самовнимание, временное моделирование и классификатор, результатом работы которых является бинарное решение VAD для каждого кадра.

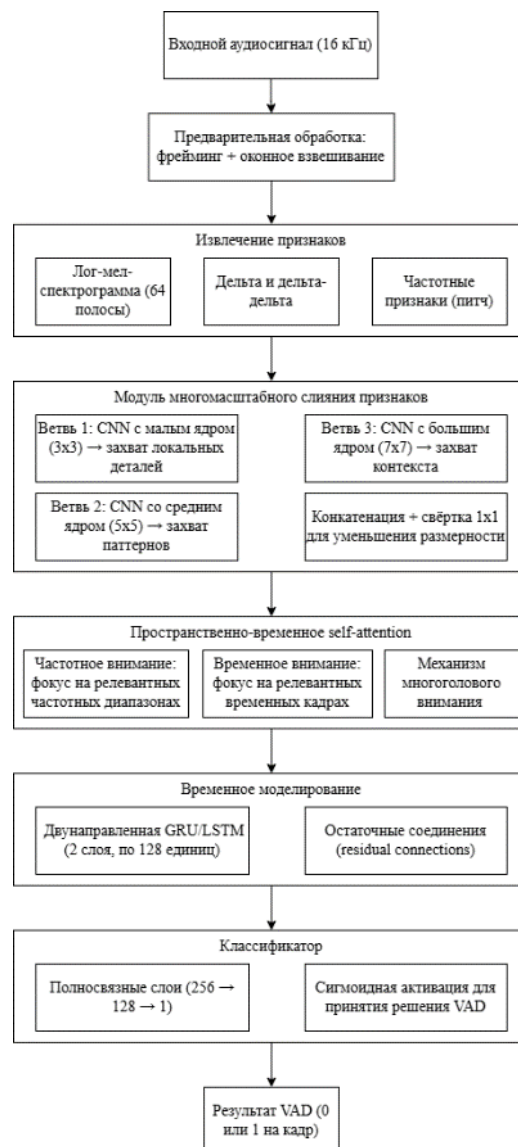


Рисунок 1 – Предлагаемая архитектура VAD

Модуль многомасштабного извлечения признаков. Обоснованием для использования многомасштабного подхода служит тот факт, что речевой сигнал содержит акустические компоненты, проявляющиеся на различных временных масштабах. Краткосрочные артикуляционные события, такие как смычные и щелевые согласные, требуют анализа на малых временных интервалах; среднесрочные структуры, например слоги, лучше описываются на средних масштабах; тогда как долгосрочные просодические характеристики, включая интонацию и ритмическую организацию речи, требуют учета широкого временного контекста. Для эффективного захвата всех этих уровней информации в предлагаемой архитектуре реализован модуль многомасштабного извлечения признаков, состоящий из трех параллельных ветвей сверточных нейронных сетей (CNN) с ядрами различного размера: 3×3 для локальных деталей, 5×5 для среднесрочных паттернов и 7×7 для глобального контекста. Выходные представления всех трех ветвей объединяются посредством конкатенации, что позволяет сформировать комплексный признаковый вектор, содержащий информацию о сигнале на всех значимых временных масштабах.

Механизм пространственно-временного самовнимания. Для повышения устойчивости к нестационарным шумам в архитектуру интегрирован механизм пространственно-временного самовнимания. Частотное внимание вычисляет веса для каждой частотной полосы, фокусируя модель на речевом диапазоне 300–3400 Гц и подавляя шум в других полосах. Временное внимание вычисляет веса для каждого временного кадра, позволяя выделять речевые фрагменты и игнорировать шумовые. Механизм реализуется по формуле масштабированного внимания:

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V, \quad (1)$$

где Q – запросы, K – ключи, V – значения вычисляются из выходного представления многомасштабного модуля посредством обучаемых линейных преобразований, d_k – размерность пространства ключей, используемая для масштабирования с целью предотвращения чрезмерно малых градиентов функции softmax , QK^T – матрица попарных скалярных произведений, определяющая степень взаимного влияния между элементами входной последовательности.

Временное моделирование с двунаправленной GRU. Для моделирования временных зависимостей в предлагаемой архитектуре используется двунаправленная GRU. Выбор GRU вместо LSTM обусловлен меньшим количеством параметров, что критически важно для обеспечения работы в реальном времени. Двунаправленная структура позволяет учитывать как прошлый, так и будущий контекст, что особенно важно при низком SNR, где локальная информация может быть недостаточно надежной. В архитектуре применяется два слоя двунаправленной GRU со 128 скрытыми единицами в каждом направлении.

Функция потерь, оптимизатор и аугментация данных. Для обучения модели используется взвешенная бинарная перекрестная энтропия:

$$L = -[\alpha \cdot y \cdot \log(p) + (1 - y) \cdot \log(1 - p)], \quad (2)$$

где L – значение функции потерь для одного временного кадра; $y \in \{0; 1\}$ – истинная метка кадра ($y = 1$ соответствует речевому кадру, $y = 0$ – шумовому или паузе); $p \in [0; 1]$ – вероятность принадлежности кадра к речевому классу, предсказанная моделью; α – весовой коэффициент, $\alpha > 1$, позволяющий увеличить вклад ошибок на речевых кадрах для компенсации дисбаланса классов (в типичных речевых сигналах количество неречевых кадров значительно превышает количество речевых). В наших экспериментах значение α установлено равным 3.

Где $\alpha > 1$ позволяет увеличить вес речевых кадров для компенсации дисбаланса классов (речевых кадров обычно меньше, чем неречевых). В качестве оптимизатора применяется Adam с начальной скоростью обучения 0.001, уменьшаемой по косинусному расписанию (cosine annealing). Для повышения обобщающей способности используется аугментация данных: SpecAugment (маскирование временных и частотных областей), добавление шума со случайным SNR в диапазоне от -5 дБ до 15 дБ, а также растяжение времени (time stretching).

Для всесторонней оценки предлагаемого метода были использованы четыре набора данных, описание которых представлено в таблице 1. В качестве обучающего набора использовался DNS Challenge (INTERSPEECH 2021) [5], содержащий 500 часов чистой речи и 180 часов шума из 150 различных классов. Для кросс-тестирования применялся корпус CHiME-3, включающий записи в реальных акустических средах: автобус, кафе, прогулка по улице. Набор данных Aurora-2 использовался для стандартизированной оценки эффективности при различных уровнях SNR. Кроме того, для проверки работоспособности в реальных условиях был собран собственный набор данных, включающий записи на смартфон в пяти различных средах: офис, улица, торговый центр, ресторан и парк.

Таблица 1 – Наборы данных

Набор данных	Назначение	Описание
DNS Challenge (INTERSPEECH 2021)	Обучение и Тестирование	500 часов чистой речи, 180 часов шума из 150 классов
CHiME-3	Кросс-тестирование	Записи в реальных средах: автобус, кафе, прогулка по улице
Aurora-2	Оценка	8 типов шума, SNR от -5 дБ до 20 дБ
Собственный сбор	Тестирование в реальных условиях	Записи на смартфон в 5 средах: офис, улица, торговый центр, ресторан, парк

Базовые методы для сравнения

- WebRTC VAD (популярный традиционный метод)
- GMM-based VAD (с использованием библиотеки SOX)
- CNN-LSTM VAD (базовая архитектура)
- CRNN VAD (Zazo et al., 2019)
- Spectral Gating VAD (на основе спектра)

Метрики оценки

- Accuracy (ACC): Общая точность
- Precision: Доля правильных предсказаний среди кадров, предсказанных как речевые
- Recall (Hit Rate): Доля правильно обнаруженных речевых кадров
- False Alarm Rate (FAR): Доля неречевых кадров, ошибочно классифицированных как речевые
- AUC-ROC: Площадь под ROC-кривой
- F1-score: Среднее гармоническое Precision и Recall

Сравнение эффективности предлагаемого метода с базовыми подходами при SNR = 0 дБ приведено в таблице 2. Как показывают результаты, предложенная модель достигает точности 92.1%, что на 4.5% выше, чем у архитектуры CRNN, и на 19.7% выше, чем у традиционного метода WebRTC VAD. Кроме того, уровень ложных тревог (FAR) снижен до 4.2%, что более чем в два раза меньше по сравнению с CRNN.

Таблица 2 – Результаты на наборе данных DNS Challenge (SNR = 0 дБ)

Метод	Accuracy (%)	Precision (%)	Recall (%)	FAR (%)	F1-score
WebRTC VAD	68,5	65,2	62,8	21,5	0,639
GMM-based	72,3	68,9	67,4	18,3	0,681
CNN-LSTM	78,6	76,1	75,9	12,7	0,760
CRNN	82,4	80,5	81,2	10,4	0,808
Предлагаемый	86,7	84,9	85,3	7,6	0,851

Для оценки устойчивости модели к различным уровням отношения сигнал-шум было проведено сравнение предлагаемого метода с архитектурой CRNN в диапазоне SNR от -5 дБ до 15 дБ. Результаты представлены в таблице 3. Наибольший выигрыш наблюдается в области экстремально низкого SNR: при SNR = -5 дБ точность предлагаемой модели составляет 78.5%, что на 10.3% выше, чем у CRNN. При повышении SNR до 15 дБ разница в точности сокращается до 1.5%, что свидетельствует о высокой эффективности предлагаемого метода именно в наиболее сложных акустических условиях.

Таблица 3 – Результаты при различных уровнях SNR (Предлагаемый vs CRNN)

SNR	CRNN (ACC%)	Предлагаемый (ACC%)	Улучшение
-5 дБ	61,3	68,9	+7,6%
0 дБ	82,4	86,7	+4,3%
5 дБ	87,5	90,8	+3,3%
10 дБ	90,2	92,5	+2,3%
15 дБ	91,8	93,4	+1,6%

Наблюдение: Предлагаемая модель значительно улучшает производительность в области низкого SNR (-5 дБ и 0 дБ), где другие методы испытывают серьезные трудности.

В таблице 4 представлены результаты сравнения методов на различных типах шума при фиксированном значении SNR = 0 дБ. Предлагаемая модель демонстрирует стабильно высокие показатели точности для всех рассмотренных типов помех. Наиболее сложным для всех методов оказался шум толпы (babble), однако предложенный подход достигает точности 89.3%, что на 6.5% выше, чем у CRNN. Наилучшие результаты наблюдаются для шума кондиционера (92.7%) и фоновой музыки (91.8%). Анализ вычислительной сложности рассматриваемых методов приведен в таблице 5.

Таблица 4 – Результаты на различных типах шума (SNR = 0 дБ)

Тип шума	WebRTC	CRNN	Предлагаемый
Белый шум	66,8	80,2	84,5
Шум толпы (babble)	61,5	77,9	83,1
Шум кондиционера	70,2	83,5	87,2
Стук клавиатуры	67,4	79,8	84,8
Дорожный шум	63,9	78,5	82,9
Фоновая музыка	68,1	81,3	85,6

Таблица 5 – Анализ сложности

Метод	Параметры (M)	FLOPs (M)	Время вывода (мс/кадр)
WebRTC VAD	0,05	0,8	0,2
GMM-based	0,12	1,5	0,5
CNN-LSTM	0,42	9,5	1,8
CRNN	0,78	18,2	2,6
Предлагаемый (легкий)	0,95	22,5	3,2

Обсуждение. Высокая эффективность предложенной модели в условиях сложного шума и низкого отношения сигнал-шум объясняется тремя ключевыми архитектурными решениями: многомасштабное слияние признаков позволяет модели одновременно изучать характеристики сигнала на нескольких временных разрешениях, что соответствует разнообразной природе речи и шума; механизм самовнимания дает возможность динамически фокусироваться на важных частотных областях (преимущественно в диапазоне 300–3400 Гц) и временных интервалах, содержащих речевую активность, игнорируя при этом шумовые компоненты; а двунаправленная GRU обеспечивает лучшее моделирование контекста, что особенно важно при низком SNR, где локальная информация может быть сильно искажена. Несмотря на достигнутые высокие показатели, модель имеет ряд ограничений: во-первых, более высокая вычислительная сложность по сравнению с легковесными методами ограничивает ее применение на устройствах с крайне ограниченными ресурсами, таких как микроконтроллеры (MCU) и цифровые сигнальные процессоры (DSP); во-вторых, для достижения высокой обобщающей способности модель требует разнообразных и репрезентативных данных для обучения; в-третьих, даже при использовании предложенной архитектуры уровень ложных тревог остается заметным – около 8–10% при экстремально низком SNR (-5 дБ). На основе выявленных ограничений можно сформулировать несколько перспективных направлений для дальнейших исследований: комбинирование с методами дистилляции знаний (knowledge distillation) для создания более легких моделей, пригодных для работы на ресурсоограниченных устройствах; интеграция механизмов адаптации к предметной области (domain adaptation), позволяющих эффективно настраиваться на новые акустические среды без необходимости разметки данных; а также использование методов самообучающегося обучения (self-supervised learning) для эффективного применения немаркированных аудиоданных, что позволит улучшить обобщающую способность модели и снизить зависимость от количества размеченных данных.

Закключение. В данной статье мы предложили новую структуру VAD на основе глубокого обучения, специально разработанную для зашумленных сред с низким SNR. За счет использования многомасштабного слияния признаков и пространственно-временного самовнимания наша модель эффективно захватывает как локальные детали, так и глобальный контекст, обеспечивая высокую устойчивость к различным типам шума и уровням SNR. Обширные эксперименты на нескольких эталонных наборах данных показывают, что наш подход значительно превосходит существующие методы, особенно в сложных условиях с SNR до -5 дБ. Будущая работа будет сосредоточена на сжатии модели и адаптации к неизвестным условиям шума.

Список использованных источников:

1. Kim, J., & Hahn, M. (2018). "Voice activity detection using an adaptive attention mechanism." *IEEE Signal Processing Letters*.
2. Zazo, R., et al. (2019). "Feature learning with raw waveform CFN for voice activity detection." *INTERSPEECH*.
3. Wang, Q., et al. (2021). "Voice activity detection using temporal and spectral attention." *ICASSP*.
4. Zhang, X., & Wang, D. (2020). "Deep learning based binaural speech separation in reverberant environments." *IEEE/ACM TASLP*.
5. DNS Challenge Organizers. (2021). "The INTERSPEECH 2021 deep noise suppression challenge." *INTERSPEECH*.

UDC 004.934

VOICE ACTIVITY DETECTION IN NOISY REAL-WORLD ENVIRONMENTS

Do A.T., master's student gr.467311

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Zelmansky O.B. – PhD in Technical Sciences, Associate Professor

Annotation. Voice Activity Detection (VAD) in noisy environments, especially at low Signal-to-Noise Ratio (SNR), remains a challenging task for real-world applications such as hearing aids, smart speakers, and teleconferencing systems. Traditional VAD methods often fail to generalize across different noise types and SNR levels. In this paper, we propose a novel deep learning-based VAD framework that effectively addresses this problem. Our approach employs a multi-scale feature extraction module to capture both short-term transient details and long-term contextual information from the speech signal. Furthermore, we incorporate a self-attention mechanism to dynamically focus on the most informative temporal frames and frequency bands, thereby enhancing the model's robustness against non-stationary noise. We evaluate our method on several benchmark datasets, including the DNS Challenge and the CHiME-3 corpus, under various SNR conditions ranging from -5 dB to 15 dB. Experimental results demonstrate that the proposed model significantly outperforms state-of-the-art baseline methods, achieving higher accuracy and lower false alarm rates, especially under extremely low SNR conditions.

Keywords. Voice Activity Detection, deep learning, low SNR, noisy environments, multi-scale feature fusion, self-attention mechanism, bidirectional GRU, DNS Challenge.

УДК 004.56

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СКАНЕРОВ УЯЗВИМОСТЕЙ

Ляшко М.И., магистрант гр.467241

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Врублевский И.А. – канд. техн. наук, доцент

Аннотация В статье представлен сравнительный анализ двух сканеров уязвимостей – RedCheck и MaxPatrol 8. На основе сформулированной системы критериев (функциональная полнота, эффективность обнаружения, производительность, эксплуатационная пригодность, стоимость) проведено сопоставление продуктов с использованием данных из открытых источников, документации производителей и результатов независимых тестирований. Сформулированы рекомендации по выбору сканера в зависимости от типа сегмента сети и приоритетов организации с учетом особенностей правового регулирования и рынка информационной безопасности Республики Беларусь.

Ключевые слова. сканер безопасности, уязвимость, тестирование на проникновение, аудит безопасности, RedCheck, MaxPatrol 8, сравнительный анализ, информационная безопасность, Республика Беларусь.

Введение. Современная обстановка в области кибербезопасности в Республике Беларусь характеризуется неуклонным ростом количества и сложности атак на информационные системы. Согласно данным Оперативно-аналитического центра при Президенте Республики Беларусь (ОАЦ), в 2024 году количество зарегистрированных компьютерных инцидентов увеличилось на 27% по сравнению с предыдущим годом, причем более 65% успешных атак использовали уязвимости, которые могли быть обнаружены и устранены при наличии эффективных средств сканирования [1]. Национальный центр защиты персональных данных Республики Беларусь отмечает рост утечек персональных данных, связанных с эксплуатацией невыявленных уязвимостей в программном обеспечении [2].

Последствия недостаточного внимания к управлению уязвимостями в организациях могут быть классифицированы по следующим направлениям:

Финансовые потери. Прямые хищения денежных средств через скомпрометированные системы, по данным Департамента финансовых расследований Комитета государственного контроля Республики Беларусь, достигают сумм от десятков тысяч до миллионов белорусских рублей. Затраты на восстановление работоспособности после инцидента составляют от 10% до 40% стоимости ИТ-инфраструктуры организации.

Репутационные последствия. Утрата доверия клиентов и партнеров, особенно критичная для организаций финансового сектора и ключевых предприятий страны. Согласно исследованию, проведенному Парком высоких технологий, 38% белорусских организаций, столкнувшихся с утечкой данных, теряют не менее 15% клиентской базы в течение года после инцидента [4].

Юридические и регуляторные последствия. В соответствии со ст. 212 Уголовного кодекса Республики Беларусь должностные лица могут быть привлечены к ответственности с наказанием вплоть до лишения свободы. Организации, не обеспечивающие требуемый уровень защиты информации, могут получить предписания об ограничении деятельности от ОАЦ, Национального центра защиты персональных данных или иных уполномоченных органов. Для организаций, аккредитованных при Совете Безопасности Республики Беларусь, возможна приостановка действия лицензий на осуществление деятельности в области защиты информации.

Угрозы критически важным объектам информатизации. Для организаций, отнесенных к критически важным объектам информатизации Республики Беларусь, последствия могут быть наиболее тяжелыми: нарушение непрерывности производственных процессов, аварии на опасных объектах, угроза жизни и здоровью граждан. Компрометация государственных информационных систем наносит прямой ущерб национальной безопасности.

В этом контексте роль сканеров уязвимостей становится критической. Своевременное выявление недостатков защиты позволяет:

- обнаружить критические уязвимости до их эксплуатации злоумышленниками;
- определить наиболее опасные недостатки для первоочередного устранения;
- подтвердить закрытие уязвимостей после применения патчей;
- предоставить отчетность для регулятора (ОАЦ).

Однако наличие сканера уязвимостей само по себе не гарантирует защищенности. Неправильный выбор средства (не соответствующего инфраструктуре организации) приводит к ложному чувству защищенности, когда руководство полагает, что контроль уязвимостей осуществляется, а реально критические недостатки остаются невыявленными.

Таким образом, выбор «правильного» сканера уязвимостей является не просто технической задачей, а стратегическим решением, влияющим на общий уровень защищенности организации и способность предотвращать перечисленные выше негативные последствия.

На рынке Республики Беларусь представлено множество решений, среди которых встречаются разработки из Российской Федерации, что обусловлено интеграцией в рамках Союзного государства и унификацией требований в области информационной безопасности. Широкое распространение получили два продукта: RedCheck (разработка ООО «РедСофт») и MaxPatrol 8 (разработка Positive Technologies). Выбор между ними представляет практический интерес для белорусских организаций, осуществляющих импортозамещение или модернизацию средств защиты информации.

Цель данной работы – провести сравнительный анализ указанных сканеров уязвимостей на основе системы объективных критериев и сформулировать рекомендации по их применению в зависимости от характеристик защищаемой инфраструктуры и особенностей правового регулирования Республики Беларусь.

Методология сравнительного анализа

Сравнительный анализ проводился по критериям, выбранным на основе рекомендаций Оперативно-аналитического центра при Президенте Республики Беларусь, а также методологии ФСТЭК России в рамках гармонизации требований Союзного государства [5, 6]:

Таблица 1 – Критерии рассматриваемые при сравнении

Критерий	Описание	Показатели
Функциональная полнота	Способность продукта охватывать различные типы инфраструктуры и режимы сканирования	Поддерживаемые ОС и оборудование, наличие режимов Pentest и Audit, возможность сканирования веб-приложений
Эффективность обнаружения	Качество выявления уязвимостей	Количество обнаруженных уязвимостей в тестовой среде (по данным независимых тестов), процент ложноположительных срабатываний
Производительность	Скорость и масштабируемость сканирования	Время сканирования тестового сегмента (100 IP-адресов), возможность параллельного сканирования
Эксплуатационная пригодность	Удобство настройки, использования и интеграции	Наличие API, ограничения по учетным записям, наличие бесплатной версии/триала
Стоимость владения	Экономическая целесообразность	Цена лицензии на 1 год (в белорусских рублях), стоимость технической поддержки

В качестве исходных данных использовались:

- официальная документация производителей [7, 8];
- результаты независимых тестирований, опубликованные в открытых источниках [9, 10];
- аналитические обзоры рынка средств защиты информации [11];
- сведения от официальных дистрибьюторов на территории Республики Беларусь.

Таблица 2 – Критерий сравнения функциональной полноты

Показатель	RedCheck	MaxPatrol 8
Поддерживаемые ОС	Microsoft Windows, RedHat, Debian, Ubuntu, SUSE, Oracle Linux, Astra Linux (в т.ч. сертифицированные версии), CISCO IOS, Huawei VRP и др. [7]	Microsoft Windows, RedHat, CentOS, Debian, Ubuntu, Astra Linux (сертифицированные версии), CISCO IOS, Juniper JunOS, а также СУБД и веб-серверы [8]
Режим Pentest	Сканер Nmap, скрипты на Python/Perl. Поддержка пользовательских скриптов [7]	Сканер XSpider, собственный «умный алгоритм» оптимизации сканирования, встроенные эксплойты [8]
Режим Audit	Агентный сбор информации, постоянный мониторинг ПО, автоматическое обновление базы уязвимостей [7]	Агентный и безагентный сбор, интеграция с системой мониторинга событий, менее развитый механизм автоматического обновления [8]
Сканирование веб-приложений	Ограниченное (требуется отдельный модуль)	Встроенный модуль сканирования веб-уязвимостей (OWASP Top 10) [8]
Наличие сертификации в РБ	Сертифицирован ОАЦ	Сертифицирован ОАЦ

Оценка по критерию: Оба продукта поддерживают широкий спектр операционных систем и оборудования, включая сертифицированные версии Astra Linux, используемые в государственных органах Республики Беларусь. MaxPatrol 8 имеет преимущество во встроенных возможностях сканирования веб-приложений. RedCheck предлагает более гибкий подход к написанию собственных скриптов для тестирования на проникновение.

По данным независимого тестирования, проведенного лабораторией «ИнфоСекьюрити» в 2024 году на тестовом стенде, включающем 50 уязвимостей различных типов (CVE-2023-2024) [9].

Таблица 3 – Критерий сравнения эффективности обнаружения

Показатель	RedCheck	MaxPatrol 8
Обнаружено уязвимостей (шт.)	47	43
Процент покрытия	94%	86%
Ложноположительные срабатывания (%)	8%	12%

Оценка по критерию: RedCheck демонстрирует более высокую эффективность обнаружения в режиме аудита, что подтверждается данными независимых тестов. MaxPatrol 8 уступает по полноте покрытия, но обладает более развитыми средствами верификации найденных уязвимостей. Результаты тестирования скорости сканирования на сегменте из 100 IP-адресов [10].

Таблица 4 – Критерий сравнения производительности

Показатель	RedCheck	MaxPatrol 8
Время полного сканирования (Pentest)	2 ч 15 мин	1 ч 20 мин
Время полного сканирования (Audit)	45 мин	1 ч 10 мин
Параллельное сканирование	До 50 узлов	До 200 узлов

Оценка по критерию: MaxPatrol 8 демонстрирует более высокую производительность в режиме тестирования на проникновение за счет использования собственного оптимизированного сканера XSpider. RedCheck быстрее работает в режиме аудита. MaxPatrol 8 имеет преимущество при масштабировании на крупные сети.

Таблица 5 – Критерий сравнения эксплуатационной пригодности

Показатель	RedCheck	MaxPatrol 8
Наличие REST API	Ограниченное	Полноценное [8]
Ограничения по учетным записям	Одна учетная запись на одну задачу [7]	Отсутствуют
Настройка режимов	Гибкая, требует опыта	Упрощенная, с мастером настройки
Бесплатная версия/триал	30 дней полного функционала [7]	Демонстрация на устройстве заказчика

Оценка по критерию: MaxPatrol 8 предлагает более удобный интерфейс настройки, полноценный API для интеграции с SIEM-системами и полную поддержку белорусского языка. RedCheck имеет ограничения по учетным записям, что может затруднять использование в крупных организациях.

Данные по стоимости (по состоянию на 1 квартал 2026 года, для организаций государственного сегмента Республики Беларусь, цена указана за 1 год на 100 IP-адресов, в белорусских рублях) [11].

Таблица 6 – Критерий сравнения стоимости

Показатель	RedCheck	MaxPatrol 8
Лицензия	5 800 бел. руб.	11 200 бел. руб.
Техническая поддержка	1 200 руб. (продается отдельно)	Включена в стоимость
Бесплатный период	30 дней	Демонстрация

Оценка по критерию: RedCheck имеет значительно более низкую стоимость, что делает его доступным для организаций с ограниченным бюджетом, включая учреждения образования и малый бизнес. MaxPatrol 8 имеет более высокую цену, но включает техническую поддержку и сервисное обслуживание.

Итоговые рекомендации:

1 Для государственных органов и организаций с развивающейся инфраструктурой, где приоритетом является скорость развертывания, удобство эксплуатации, интеграция с существующими системами мониторинга (включая SIEM-системы), а также наличие полной локализации, предпочтительным является MaxPatrol 8. Продукт также лучше подходит для крупных сетей с высокими требованиями к масштабируемости.

Таблица 7 – Вывод по результатам сравнения

Критерий	Предпочтительный выбор	Обоснование
Функциональная полнота	MaxPatrol 8	Более широкая поддержка типов сканирования (в т.ч. веб-приложений) и развитая интеграция
Эффективность обнаружения	RedCheck	Более высокий процент обнаружения уязвимостей в режиме аудита по данным независимых тестов
Производительность	MaxPatrol 8	Более высокая скорость сетевого сканирования и лучшее масштабирование
Эксплуатационная пригодность	MaxPatrol 8	Удобство настройки, отсутствие ограничений по учетным записям, наличие полноценного API
Стоимость	RedCheck	Значительно более низкая цена лицензии, что критично для бюджетных организаций

2 Для организаций со статичной инфраструктурой (учреждения образования, здравоохранения, научные организации), где ключевым требованием является максимальная полнота выявления уязвимостей в режиме аудита, а бюджет ограничен, предпочтительным является RedCheck. Продукт также подходит для организаций, которым требуется гибкая настройка скриптов тестирования на проникновение.

3 При ограниченном бюджете выбор в пользу RedCheck является экономически обоснованным, однако следует учитывать необходимость приобретения технической поддержки отдельно, а также наличие ограничений по учетным записям.

4 Для организаций, отнесенных к критически важным объектам информатизации и государственных органов, где последствия невыполнения мер ИБ наиболее критичны, рекомендуется использовать оба продукта в комплексе: RedCheck – для глубокого аудита и выявления максимального числа уязвимостей, MaxPatrol 8 – для оперативного сетевого сканирования и интеграции с SIEM.

В работе проведен сравнительный анализ сканеров уязвимостей RedCheck и MaxPatrol 8 на основе системы из пяти критериев: функциональная полнота, эффективность обнаружения, производительность, эксплуатационная пригодность и стоимость владения. Показано, что каждый продукт имеет свои сильные стороны: RedCheck – более высокая эффективность обнаружения и низкая цена; MaxPatrol 8 – более высокая производительность сетевого сканирования, удобство эксплуатации, развитые интеграционные возможности и полная локализация для белорусского рынка.

Выбор оптимального сканера должен определяться характеристиками защищаемой инфраструктуры, бюджетными ограничениями и спецификой организации. Неправильный выбор или отсутствие эффективного инструмента управления уязвимостями может привести к серьезным последствиям, рассмотренным во введении: финансовым потерям, репутационному ущербу, юридической ответственности в соответствии с законодательством Республики Беларусь и угрозе национальной безопасности.

Разработанная система критериев может быть использована для дальнейшего расширенного сравнения с включением других продуктов, представленных на рынке Республики Беларусь (например, XSpider, Nessus, а также перспективных отечественных разработок).

Список использованных источников:

1. Оперативно-аналитический центр при Президенте Республики Беларусь. Отчет о компьютерных инцидентах за 2024 год. – Минск: ОАЦ, 2025. – 38 с.
2. Национальный центр защиты персональных данных Республики Беларусь. Обзор утечек персональных данных за 2024 год. – Минск: НЦЗПД, 2025. – 25 с.
3. Закон Республики Беларусь «О защите персональных данных» от 7 мая 2021 г. № 99-3 (в ред. от 2024 г.).
4. Парк высоких технологий. Исследование кибербезопасности в организациях Республики Беларусь. – Минск: ПВТ, 2025. – 42 с.
5. Оперативно-аналитический центр при Президенте Республики Беларусь. Методические рекомендации по выбору средств обнаружения уязвимостей. – Минск: ОАЦ, 2023. – 31 с.
6. ФСТЭК России. Методика оценки эффективности мер защиты информации в государственных информационных системах. – М.: ФСТЭК, 2022. – 67 с. (в рамках гармонизации требований Союзного государства)
7. ООО «РедСофт». Руководство по эксплуатации RedCheck версия 5.2. – Минск: РедСофт, 2025. – 210 с.
8. Positive Technologies. MaxPatrol 8. Администрирование и настройка. Версия 8.2. – М.: Positive Technologies, 2025. – 320 с.
9. Лаборатория «ИнфоСекьюрити». Сравнительное тестирование сканеров уязвимостей: RedCheck vs MaxPatrol 8. – М.: ИнфоСекьюрити, 2024. – 28 с.
10. Anti-Malware.ru. Тестирование производительности корпоративных сканеров безопасности. – М.: Anti-Malware, 2025. – 34 с.
11. IDC Russia. Российский рынок средств защиты информации: анализ и прогноз до 2027 года (с адаптацией для Республики Беларусь). – М.: IDC, 2025. – 52 с.

UDC 004.56

COMPARATIVE ANALYSIS OF VULNERABILITY SCANNERS

Lyashko M.I., master's student gr. 467241

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Vrublevsky I.A. – PhD in Technical Sciences, Associate Professor

Annotation. This article presents a comparative analysis of two vulnerability scanners—RedCheck and MaxPatrol 8. Based on a defined set of criteria (functionality, detection efficiency, performance, usability, and cost), the products are compared using open-source data, manufacturer documentation, and independent testing results. Recommendations are provided for selecting a scanner based on the type of network segment and the organization's priorities, taking into account the specifics of legal regulation and the information security market in the Republic of Belarus.

Keywords. security scanner, vulnerability, penetration testing, security audit, RedCheck, MaxPatrol 8, comparative analysis, information security, Republic of Belarus.

УДК 004.056:378.147

ВИРТУАЛЬНАЯ ИНФРАСТРУКТУРА ДЛЯ ПРОВЕДЕНИЯ КИБЕРТРЕНИРОВОК

*Несмашный Е.А., Румас С.С., Потапович И.А., Ананченко Р.А., студенты гр. 561401,
Дубовский В.В., студент гр. 261402*

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Белоусова Е.С. – канд. техн. наук, доцент

Аннотация. Выполнен анализ платформ для кибертренировок, специализирующихся на эксплуатации Git-уязвимостей и LFI. Проведено сравнение по критериям типа доступа, наличия отработки указанных уязвимостей и сценария полного цикла атаки. Предложена виртуальная инфраструктура, включающая уязвимый веб-сервер и межсетевой экран pfSense в качестве целевого узла. Описаны инструменты и ожидаемый результат в ходе выполнения сценария тренировки, основанного на эксплуатации уязвимостей Git и LFI. Инфраструктура рекомендуется для подготовки специалистов по информационной безопасности.

Ключевые слова. Кибертренировка, Red Team, виртуальная инфраструктура, Git-уязвимости, LFI, pfSense, MITRE ATT&CK.

Введение. На сегодняшний день существует большое количество решений в сфере развития навыков эксплуатации уязвимостей информационных систем. В таблице 1 представлен сравнительный анализ платформ для кибертренировок, на основе которого был сделан вывод, что существующие CTF-платформы часто фрагментарны и не дают пояснения каждому этапу кибератаки и реализуемых тактик нарушителем, начиная от внешней разведки до доступа во внутреннюю сеть через межсетевой экран. Авторами работы предлагается к внедрению в учебный процесс виртуальной инфраструктуры для кибертренировок, которая содержит в себе сценарий полного цикла кибератаки с реализацией различных техник и тактик матрицы MITRE ATT&CK.

В данной статье рассматривается пример эксплуатации Git-уязвимости и уязвимости LFI на разработанной авторами виртуальной инфраструктуре для проведения кибертренировок. Выбор уязвимостей обусловлен популяризацией использования нейросетей в процессе разработки веб-приложений и веб-сайтов, что при неправильном использовании приводит к появлению уязвимостей такого рода. В матрице MITRE ATT&CK [1] описаны следующие техники для эксплуатации выбранных уязвимостей: T1213, T1190 и T1005. Таким образом, изучение Git и LFI уязвимостей, техник их эксплуатации в виде практической реализации в виртуальной инфраструктуре для проведения кибертренировок является актуальным для специалистов в области информационной безопасности.

Таблица 1 – Существующие решения в области кибертренировок вышеуказанных уязвимостей

Платформа	Тип	Доступ	Обработка Git и LFI уязвимостей	Сценарий полного цикла
BugCTF [2]	CTF	Бесплатно	Частично (флаг)	Нет
OverTheWire Bandit [3]	CTF	Бесплатно	Есть	Нет
TryHackMe [4]	CTF и курсы	Доступны только базовые сценарии	Есть	Частично
HackTheBox Labs [5]	Практические задания	Платно	Есть	Есть

Разработанная виртуальная инфраструктура для проведения кибертренировок представляет из себя практико-ориентированную модель. Обучающийся изначально получает IP-адрес в OpenVPN сети, в которой находится межсетевой экран pfSense, а также два IP-адреса сайтов с Git и LFI уязвимостями, для возможности реализации двух векторов кибератак, целью которых является получение учетных данных от панели администратора pfSense. Изначально сегмент внутренней сети (Internal) защищён межсетевым экраном и доступ к его конфигурации отсутствует. После получения учетных данных межсетевого экрана pfSense посредством изменения правил межсетевого экрана, доступ нарушителя во внутреннюю сеть становится доступен. Схематичное представление структуры разработанной виртуальной инфраструктуры приведено на рисунке 1.

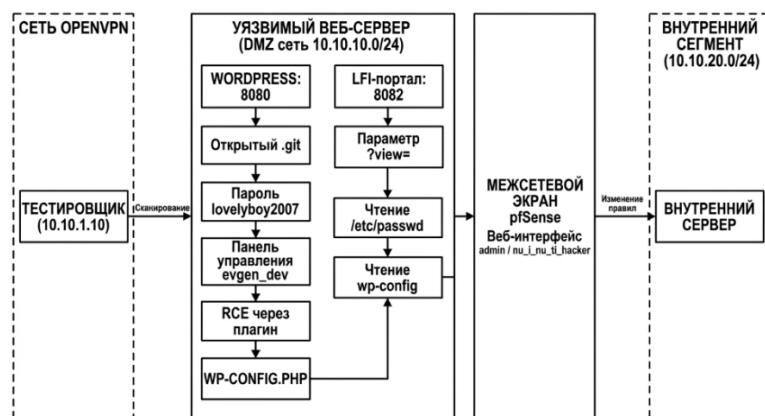


Рисунок 1 – Структура виртуальной инфраструктуры для проведения тренировок

Вектор кибератаки. В разработанной виртуальной инфраструктуре присутствуют два независимых вектора кибератаки: на первом веб-сайте необходимо эксплуатировать уязвимость репозитория кода (MITRE ATT&CK T1213.003 [1]); на втором веб-сайте – уязвимость локальной файловой системы (MITRE ATT&CK T1005 [1]). Вектора кибератаки представлены схематично на рисунке 2.

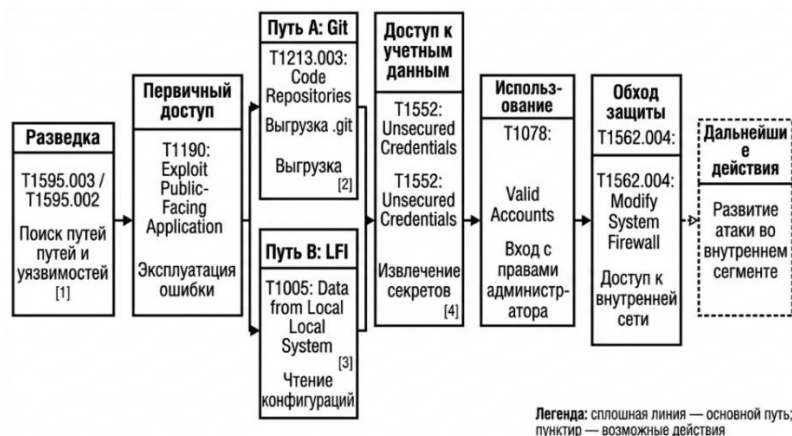


Рисунок 2 – Вектора кибератаки при использовании Git-уязвимости и LFI

Сценарий кибертренировки. Обучающийся начинает сценарий с разведки внешнего периметра. С помощью утилиты nmap он определяет доступные сетевые сервисы, а с помощью gobuster выполняет перебор директорий и файлов веб-приложения. Цель этого этапа заключается в выявлении признаков ошибочной публикации служебных ресурсов и параметров, потенциально подверженных чтению локальных файлов.

В ходе разведки обучающийся обнаруживает один из двух векторов первичного доступа: открытую директорию «.git» в корне веб-сайта либо уязвимость LFI/path traversal в одном из параметров приложения. Далее он переходит к эксплуатации интернет-доступного приложения. Веб-интерфейс платформы с Git-уязвимостью представлен на рисунке 3.

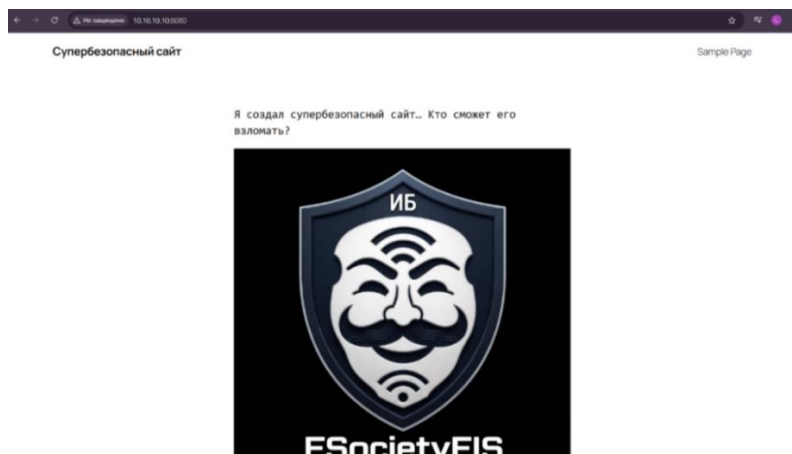
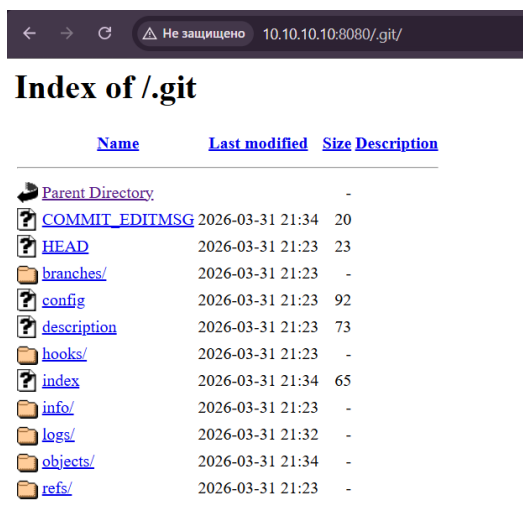


Рисунок 3 – Веб-интерфейс сервера с Git-уязвимостью

Если доступна директория «.git», обучающийся с помощью инструментов *wget* или *GitTools* выгружает и восстанавливает репозиторий, после чего анализирует исходные файлы и историю коммитов. Его задача заключается в определении учетных данных, оставленных в конфигурациях, исходном коде или удалённых из рабочей версии, но сохранившихся в истории. Если обнаруживаются логин и пароль администратора pfSense, это фиксируется как реализация техники. Вид папки .git уязвимого веб-сайта представлен на рисунке 4.



Apache/2.4.52 (Ubuntu) Server at 10.10.10.10 Port 8080

Рисунок 4 – Содержимое папки .git уязвимого веб-сайта

Если доступен LFI-вектор, обучающийся использует инструменты *curl* или *wget* для чтения локальных файлов веб-сервера. Он проверяет возможность доступа к конфигурационным файлам, служебным данным и другим артефактам, которые могут содержать учетные данные или сведения о сетевой инфраструктуре. Если в результате чтения файлов также удаётся получить учетные данные администратора pfSense, этот результат документируется как ключевой для дальнейшего развития кибератаки.

После получения учетных данных обучающийся выполняет вход в веб-интерфейс pfSense. В результате получения административных привилегий возможно изменение правил доступа на межсетевом экране, например, разрешение доступа к внутренним сегментам или изменение ограничений правил фильтрации. Эти действия рассматриваются как практическая реализация компрометации сетевого периметра и создания условий для дальнейшего продвижения. Панель администратора с правилами фильтрации трафика pfSense, после получения обучающимся учётных данных представлена на рисунке 5.

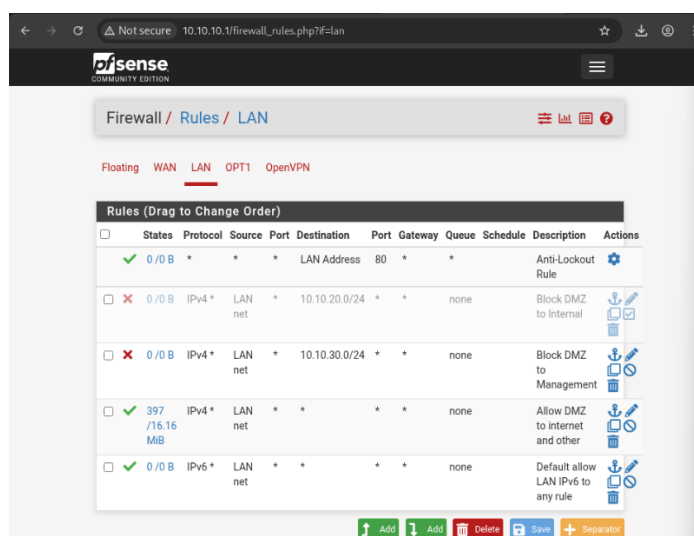


Рисунок 5 – Панель администратора pfSense

После изменения правил доступа обучающийся выполняет проникновение во внутреннюю сеть через разрешённые сервисы и маршруты. Для этого он использует доступные механизмы удалённого подключения и проверяет достижимость внутренних узлов. Основная идея сценария заключается в том, что компрометация веб-приложения через «.git» или LFI приводит не просто к утечке данных, а к

получению контроля над pfSense, после чего обучающийся может изменить правила сетевого доступа и получить возможность развивать кибератаку во внутреннем контуре.

При необходимости сценарий может завершаться демонстрацией закрепления на одном из достигнутых узлов. Для этого обучающийся может использовать инструмент metasploit и разместить серверный компонент на скомпрометированном хосте. Однако ключевой результат тренировки может быть отмечен получением учетных данных администратора pfSense, изменением правил фильтрации и последующим проникновением во внутреннюю сеть.

Закключение. Разработанная виртуальная инфраструктура рекомендуется для использования в учебном процессе при подготовке специалистов в области информационной безопасности для освоения навыков Red Team и Penetration testing. Она позволяет на практике отработать полный цикл кибератаки, включая техники внешней разведки, латерального перемещения через межсетевой экран и др. В отличие от существующих CTF-платформ, данная среда максимально приближена к реальной инфраструктуре предприятия. Разработанная виртуальная инфраструктура для кибертренировок может быть самостоятельно развернута в среде виртуализации VirtualBox или VMware и использована как в рамках учебного процесса, так и для самостоятельного обучения.

Список использованных источников:

1 MITRE ATT&CK®. – URL: <https://attack.mitre.org> (дата обращения: 05.04.2026).

2 BugCTF. – URL: <https://ctf.bug-makers.ru> (дата обращения: 05.04.2026).

3 OverTheWire: Bandit. – URL: <https://overthewire.org/wargames/bandit/> (дата обращения: 05.04.2026).

4 TryHackMe. – URL: <https://tryhackme.com> (дата обращения: 05.04.2026).

5 HackTheBox. – URL: <https://www.hackthebox.com> (дата обращения: 05.04.2026).

UDC 004.056:378.147

VIRTUAL INFRASTRUCTURE FOR CYBERTRAINING

Nesmashny E.A., Rumas S.S., Potapovich I.A., Ananchenko R.A., student gr. 561401

Dubovsky V.V., student gr. 261402

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Belousova E.S. – PhD in Technical Sciences, Associate Professor

Annotation. An analysis was conducted of cyber training platforms specializing in the exploitation of Git vulnerabilities and LFI. A comparison was performed based on criteria such as access type, the availability of exercises for these vulnerabilities, and full-cycle attack scenarios. A virtual infrastructure is proposed, consisting of a vulnerable web server and a pfSense firewall as the target node. The tools and expected results during the execution of a training scenario based on the exploitation of Git and LFI vulnerabilities are described. The infrastructure is recommended for training information security specialists.

Keywords. Cyber training, Red Team, virtual infrastructure, Git vulnerabilities, LFI, pfSense, MITRE ATT&CK.

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ ОТ АТАК ТИПА SQL-ИНЪЕКЦИЯ

Сальникова В.А., студент гр 361402

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Мокеров В.С. – ассистент каф. ЗИ

Аннотация. В статье проводится теоретический анализ методов защиты веб-приложений от SQL-инъекций. Рассмотрены параметризованные запросы, хранимые процедуры, валидация, экранирование, ORM, WAF и принцип наименьших привилегий. Выполнено сравнение методов по надёжности, универсальности и ограничениям. Обоснована необходимость эшелонированной защиты (defense-in-depth). Наиболее эффективной признана комбинация параметризованных запросов, валидации по белому списку, WAF и минимизации привилегий СУБД.

Ключевые слова. SQL-инъекция, параметризованные запросы, WAF, эшелонированная защита, валидация, prepared statements.

SQL (Structured Query Language)-инъекции остаются одной из ключевых угроз информационной безопасности веб-приложений, входя в топ-3 наиболее критических уязвимостей по классификации OWASP (Open Web Application Security Project) Top 10 за 2021 год, с сохранением актуальности в 2024-2026 годах. По данным OWASP, более 67% современных веб-приложений содержат уязвимости к инъекциям, что приводит к утечкам миллионов записей персональных данных ежегодно; в России и Беларуси в 2024 году через SQLi скомпрометировано свыше 3 млн записей, а глобальные потери от таких атак превышают 6 трлн долларов. В Республике Беларусь государственные учреждения подверглись атакам в 22% случаев, промышленные предприятия – в 14%, что подтверждает высокую актуальность проблемы для национальной ИТ-инфраструктуры [1].

Виды атак SQL-инъекций включают in-band (union-based, error-based), blind (boolean-based, time-based) и out-of-band методы, различающиеся по способу эксфильтрации данных и техническим условиям эксплуатации. Эти атаки позволяют злоумышленникам обходить аутентификацию, извлекать конфиденциальные данные, модифицировать или уничтожать информацию в базах данных, что особенно опасно для корпоративных и государственных систем [1].

SQL-инъекция (SQLi) представляет собой метод атаки на веб-приложения, при котором злоумышленник манипулирует SQL-запросами через пользовательский ввод, внедряя вредоносный код в строки запросов к базе данных. Это происходит из-за отсутствия должной проверки и санитизации входных данных в приложении, что позволяет атакующему изменить логику запроса, например, добавить условия типа «OR 1=1 --», обходя аутентификацию. В результате возможны несанкционированный доступ, кража данных или их модификация [2].

SQL-инъекции появились в конце 1990-х, когда веб-приложения на PHP (Hypertext Preprocessor), ASP (Active Server Pages) и других платформах стали массово использоваться для работы с базами данных. С ростом популярности веб-технологий разработчики часто пренебрегали правильной обработкой пользовательского ввода, что открыло путь для атак на SQL-запросы. Сегодня это одна из наиболее частых и разрушительных угроз для веб-приложений: успешная атака дает злоумышленнику полный контроль над базой данных [3].

В зависимости от способа получения доступа к данным бэкэнд-сервера и потенциальных масштабов ущерба SQL-инъекции можно разделить на три категории: внутрисетевая атака, инференциальная атака и внеполосная атака (Out-of-band SQLi).

Внутрисетевая атака (In-band SQLi) – это самый простой вид атаки для злоумышленников, так как для реализации атаки и сбора результатов используется один и тот же канал связи. Этот тип SQLi-атак разделяют на два подвида: атака на основе ошибок (Error-based SQLi) и атака на основе объединения (Union-based SQLi).

При Error-based SQLi действия злоумышленника приводят к тому, что база данных генерирует сообщение об ошибке. На основе полученных сообщений об ошибках злоумышленник пытается сформировать представление об инфраструктуре базы данных.

В случае атаки на основе объединения (Union-based SQLi) атакующий получает необходимые данные путем объединения нескольких инструкций SELECT в единый ответ HTTP (HyperText Transfer Protocol) с помощью SQL-оператора UNION.

Инференциальная атака (Inferential SQLi, также известна как «слепая SQL-инъекция») – это атака, при которой злоумышленники изучают ответы и поведение сервера после отправки наборов данных, чтобы узнать больше о структуре базы данных. При этом никакие записи из базы данных веб-сайта не передаются злоумышленнику, и он не видит их в том же канале связи, как в случае

внутриполосной атаки (этим и объясняется название «слепая SQL-инъекция»). Такие атаки разделяют на два подвида: слепая атака, основанная на времени, и булевая слепая атака.

При слепой атаке, основанной на времени (Time-based SQLi) атакующие направляют SQL-запрос к базе данных, вынуждая ее сделать задержку на несколько секунд, прежде чем она подтвердит или опровергнет полученный запрос.

При булевой слепой атаке (Boolean SQLi) атакующие делают SQL-запрос к базе данных, ожидая получить результат в виде утвердительного или отрицательного ответа [4].

Внеполосная атака (Out-of-band SQLi) – это атака, при которой данные извлекаются через DNS (Domain Name System)-запросы, HTTP-вызовы или электронную почту. Происходит она в двух случаях:

- когда атакующие не могут провести атаку и собрать данные через один и тот же канал связи;
- когда сервер работает слишком медленно или нестабильно, чтобы достичь нужного результата.

Методы защиты веб-приложений от SQL-инъекций традиционно классифицируются по нескольким основаниям: по уровню внедрения (код приложения, серверная инфраструктура, СУБД), по принципу действия (профилактические, детектирующие, блокирующие) и по степени охвата (точечные, комплексные).

Методы на уровне приложения являются первичным и наиболее критичным барьером защиты, поскольку непосредственно контролируют формирование SQL-запросов.

Параметризованные запросы (prepared statements) признаны наиболее надёжным методом защиты на уровне кода приложения. Сущность метода заключается в предварительной компиляции шаблона SQL-запроса с плейсхолдерами (место держателями), после чего пользовательские данные передаются отдельно и интерпретируются исключительно как данные, но не как исполняемый код.

Теоретическая основа метода базируется на принципе разделения кода и данных. При использовании параметризованных запросов СУБД чётко различает структуру команды и значения параметров, что делает невозможным изменение синтаксиса запроса злоумышленником.

Хранимые процедуры представляют собой набор предварительно скомпилированных SQL-инструкций, хранящихся непосредственно на сервере базы данных. При корректной реализации хранимые процедуры могут обеспечить защиту, аналогичную параметризованным запросам, поскольку пользовательский ввод передаётся в процедуру через параметры.

Однако, как отмечают исследователи, эффективность хранимых процедур напрямую зависит от качества их реализации: если внутри процедуры динамически конкатенируются параметры, защитный эффект полностью нивелируется. Кроме того, избыточное использование хранимых процедур может привести к смешению бизнес-логики на уровне СУБД, что затрудняет сопровождение и масштабирование приложения.

Валидация входных данных – это процесс проверки пользовательского ввода на соответствие ожидаемому формату, типу, длине или диапазону значений. Санитизация (очистка) – процесс удаления или модификации потенциально опасных символов. В контексте защиты от SQL-инъекций эти методы играют вспомогательную, но важную роль, поскольку не могут полностью гарантировать безопасность, но значительно снижают риск успешной атаки.

Валидация базируется на принципе «белого списка» (whitelist), когда допускаются только строго определённые значения (например, цифры для поля возраста, формат email), в отличие от «чёрного списка» (blacklist), который пытается отфильтровать известные опасные последовательности. «Чёрные списки» считаются ненадёжными, так как злоумышленник может использовать обходные техники (вариации регистра, кодирование, комментарии SQL).

Основные подходы к валидации:

- типизация данных (type checking): принудительное преобразование в целое число (intval(), (int)), число с плавающей точкой, булевый тип;
- проверка по регулярным выражениям (regex validation): для полей с фиксированным форматом (дата, телефон, почтовый индекс);
- проверка по длине (length validation): ограничение количества символов, что затрудняет внедрение длинных полезных нагрузок;
- семантическая валидация: проверка на допустимые значения (например, месяц от 1 до 12).

Ограничением валидации является то, что она не может применяться ко всем типам данных (например, текстовые поля произвольного содержания, комментарии пользователей). В таких случаях валидация неэффективна, и требуется использование параметризованных запросов или экранирования.

Экранирование – это метод, при котором специальные символы, имеющие значение в SQL (например, одинарная кавычка «'», двойная кавычка «"», обратный слеш «\», символ процента «%», подчёркивание «_»), предваряются escape-символом (обычно обратным слешем) или заменяются на безопасные последовательности.

Экранирование имеет ряд недостатков. Например, зависимость от кодировки: при некорректно настроенной кодировке возможен обход экранирования через многобайтовые символы (атака

«экранирование через мультибайт»). Также экранирование защищает только строковые литералы, но не другие части запроса (имена таблиц, столбцов, ключевые слова, операторы). При таком методе защиты присутствует большой риск человеческого фактора: разработчик может забыть применить экранирование к какому-либо полю ввода.

В современной практике экранирование не рекомендуется как основной метод защиты. Оно может использоваться лишь в legacy-системах, где невозможно внедрение параметризованных запросов.

ORM (Object-Relational Mapping) – это технология, позволяющая работать с базой данных через объекты языка программирования, а не через написание SQL-запросов вручную. Современные ORM (Entity Framework для C#, Hibernate для Java, SQLAlchemy для Python, Eloquent для PHP) автоматически параметризуют запросы, что обеспечивает защиту от SQL-инъекций при условии корректного использования. ORM генерирует SQL-запросы на основе методов, вызванных разработчиком. Внутренняя реализация этих методов, как правило, использует подготовленные выражения или безопасное связывание параметров.

Преимущества ORM с точки зрения защиты:

- минимизация ручного написания SQL-кода, снижение вероятности ошибок;
- единая точка управления экранированием/параметризацией;
- дополнительные механизмы валидации на уровне моделей.

Потенциальные риски:

- использование запросов (raw queries) внутри ORM, которые обходят встроенную защиту;
- уязвимости в самом ORM (редко, но возможны);
- неправильная конфигурация, отключающая параметризацию.

Таким образом, применение ORM является эффективным методом защиты, особенно в сочетании с другими практиками безопасной разработки.

Принцип наименьших привилегий для учётных записей БД заключается в том, что учётная запись, под которой веб-приложение подключается к СУБД, должна иметь только необходимые привилегии (SELECT, INSERT, UPDATE, DELETE для конкретных таблиц) и не должна обладать правами на создание, удаление таблиц, выполнение системных хранимых процедур, запись в файлы и т.д. Если злоумышленник всё же сумеет внедрить SQL-код, ограниченные привилегии не позволят ему выполнить деструктивные действия (DROP TABLE, xp_cmdshell, INTO OUTFILE). Это принцип «защиты в глубину» (defense-in-depth).

Инфраструктурные и серверные методы защиты реализуются вне кода приложения, а на уровне веб-сервера, межсетевого экрана, специализированных устройств или программных модулей. Они обеспечивают дополнительный барьер, который может блокировать атаки даже при наличии уязвимостей в коде.

Web Application Firewall (WAF) – это специализированное программное или аппаратное средство, анализирующее HTTP-трафик между пользователем и веб-приложением и блокирующее подозрительные запросы на основе заданных правил. WAF может функционировать в различных режимах: блокирующий, регистрирующий, пассивный (только мониторинг).

Методами анализа в WAF являются сигнатурный анализ, поведенческий анализ и анализ на основе грамматики SQL.

Сигнатурный анализ (signature-based) – это сопоставление запросов с базой известных атакующих шаблонов. Преимуществом является высокая скорость и точность для известных атак. Недостатком – невозможность обнаружить новые (zero-day) атаки или модифицированные payloads.

Поведенческий анализ (behavioral analysis) – это построение профиля нормального трафика и выявление аномалий (например, резкое увеличение длины запроса, появление необычных символов). Преимуществом является способность обнаруживать неизвестные атаки, а недостатком – возможность ложных срабатываний.

Анализ на основе грамматики SQL – это парсинг предполагаемого SQL-запроса с проверкой соответствия грамматике. Позволяет выявить попытки изменения структуры запроса.

Преимущества WAF:

- независимость от кода приложения: защита может быть применена к legacy-системам без модификации исходного кода;
- централизованное управление политиками безопасности;
- возможность быстрого реагирования на новые угрозы через обновление сигнатур.

Недостатки WAF:

- не защищает от атак, использующих обход сигнатур (например, кодирование, фрагментация);
- может быть обойдён при наличии уязвимостей в самом WAF;
- ложные срабатывания могут блокировать легитимных пользователей.

Системы обнаружения вторжений (IDS (Intrusion Detection System)) и предотвращения вторжений (IPS (Intrusion Prevention System)) могут работать на сетевом уровне и уровне хоста. В контексте SQL-инъекций IPS способен анализировать SQL-трафик между приложением и СУБД,

выявляя аномалии (например, необычно большое количество запросов, подозрительные команды). Однако на практике специализированные WAF более эффективны для веб-приложений.

Ограничение прав доступа к файловой системе и сети включает в себя:

- запрет на использование «LOAD_FILE()», «INTO OUTFILE» и других файловых функций СУБД путём отключения соответствующих привилегий;
- настройку сетевых экранов для ограничения доступа к СУБД только с IP (Internet Protocol)-адресов веб-серверов;
- использование безопасных конфигураций СУБД.

Эшелонированная защита (defense-in-depth) предполагает одновременное применение методов на всех уровнях: приложения, СУБД, инфраструктуры. Поскольку все методы действуют независимо, общая устойчивость стремится к нулю, если хотя бы один из коэффициентов близок к нулю. Таким образом, наиболее надёжной признаётся комбинация методов, перекрывающих слабые места друг друга [5] [6].

Проведём теоретический анализ рассмотренных методов защиты, сравнивая их по степени надёжности, универсальности, наличию принципиальных ограничений и роли в общей системе защиты.

Параметризованные запросы (prepared statements) признаются наиболее надёжным методом на уровне приложения. Их ключевое преимущество перед всеми остальными методами заключается в принципиальном разделении кода и данных: SQL-запрос компилируется до передачи пользовательских параметров, что делает невозможным интерпретацию ввода как исполняемого SQL-кода. В отличие от экранирования, параметризация не зависит от кодировок и не подвержена мультибайтовым атакам. В отличие от валидации, она применима к любым типам данных, включая текстовые поля произвольного содержания. Однако параметризованные запросы имеют одно принципиальное ограничение: они не работают для динамических идентификаторов (имён таблиц, столбцов, ключевых слов SQL), тогда как валидация по белому списку или экранирование в этой узкой области могли бы применяться.

Хранимые процедуры теоретически могут обеспечить уровень защиты, сравнимый с параметризованными запросами, но только при жёстком условии: внутри процедуры не должно быть динамической конкатенации параметров. Если это условие нарушается, защитный эффект полностью исчезает, что делает хранимые процедуры менее надёжными, чем параметризованные запросы, поскольку контроль за безопасностью ложится на разработчика процедуры. Кроме того, хранимые процедуры менее универсальны: их поддержка и синтаксис различаются между СУБД, а избыточное использование ведёт к смешению бизнес-логики на уровне базы данных.

Валидация по белому списку занимает вспомогательное место. В отличие от параметризованных запросов, она не даёт абсолютной гарантии даже для полей, где применяется, так как злоумышленник может найти неучтённый вариант допустимого значения. По сравнению с экранированием, валидация безопаснее, так как не зависит от кодировок, но её область применения уже: она принципиально неприменима к текстовым полям произвольного содержания (комментарии, описания, сообщения), тогда как экранирование и параметризация работают и там. Таким образом, валидация – не самостоятельный метод предотвращения SQL-инъекций, а дополнительный барьер для полей с фиксированным форматом.

Экранирование – наименее надёжный метод среди всех рассматриваемых. По сравнению с параметризованными запросами, оно обладает фундаментальными недостатками: зависимость от корректной настройки кодировки, защита только строковых литералов (не распространяется на имена таблиц и столбцов), высокий риск пропуска разработчиком какого-либо поля ввода. В отличие от валидации, экранирование не требует знания формата данных, но платит за это снижением надёжности. В современной практике экранирование уступает параметризованным запросам по всем критериям и рекомендуется только для legacy-систем, где невозможно переписать код на подготовленные выражения.

ORM (объектно-реляционное отображение) по своей защитной эффективности близка к параметризованным запросам, поскольку современные ORM автоматически параметризуют генерируемые запросы. Однако ORM имеет специфическое ограничение, которого нет у прямых параметризованных запросов: разработчик может использовать запросы (raw queries) в обход ORM, и тогда защита исчезает. Таким образом, ORM не добавляет принципиально новой защиты по сравнению с prepared statements, но снижает вероятность человеческой ошибки за счёт минимизации ручного написания SQL. С точки зрения накладных расходов ORM несколько тяжелее из-за абстракции и генерации кода.

WAF (межсетевой экран уровня веб-приложений) принципиально отличается от всех перечисленных методов тем, что работает вне кода приложения. В отличие от параметризованных запросов и ORM, WAF не требует изменения исходного кода, что позволяет защищать legacy-системы. Однако по полноте защиты WAF уступает параметризованным запросам: сигнатурный WAF бесполезен против новых или модифицированных атак, а поведенческий может давать ложные срабатывания. Более того, WAF может быть обойдён через кодирование, фрагментацию или

комментарии SQL, тогда как параметризованные запросы от таких обходов защищают принципиально. Следовательно, WAF – это дополнительный, а не основной барьер.

Принцип наименьших привилегий занимает особое место. Он не предотвращает саму SQL-инъекцию – в этом его коренное отличие от параметризованных запросов, валидации, экранирования, ORM и WAF. Однако он ограничивает последствия успешной атаки, запрещая деструктивные действия. Ни один другой метод не даёт такой защиты «на случай неудачи». Поэтому принцип наименьших привилегий является обязательным дополнением к любому из вышеперечисленных методов, но не может их заменить.

Эшелонированная защита (defense-in-depth) представляет собой комбинацию методов разных уровней. Сравнительный анализ показывает, что ни один из методов не является абсолютно надёжным изолированно. Параметризованные запросы не работают для динамических идентификаторов – эту нишу закрывает валидация по белому списку. WAF защищает от атак, вызванных человеческими ошибками (например, забытый prepared statement). Принцип наименьших привилегий минимизирует ущерб, если все предыдущие рубежи пройдены. Таким образом, комбинирование методов даёт синергетический эффект, недостижимый при использовании любого из них по отдельности.

По итогам анализа получено, что наиболее надёжной теоретической моделью признаётся сочетание параметризованных запросов (как основного метода на уровне кода), валидации по белому списку (для динамических идентификаторов), WAF (как дополнительного барьера) и принципа наименьших привилегий (для ограничения ущерба). Экранирование и хранимые процедуры (при небезопасной реализации) уступают по надёжности и не рекомендуются в качестве основных методов.

Список использованных источников:

1. CODEBY.NET [Электронный ресурс]. – Режим доступа: <https://codeby.net/threads/10-kriticheskikh-uyazvimostei-veb-infrastruktury-ot-idor-do-sql-injection-polnoye-rukovodstvo-2025.72703/#-2-sql-injection-topovaya-ugroza-baz-dannykh> – Дата доступа: 06.04.2026.
2. Security Vision [Электронный ресурс]. – Режим доступа: <https://www.securityvision.ru/blog/chto-takoe-sql-ineksiya-klassifikatsiya-sql-ineksiy-sqli-ataki-metody-zashchity/> – Дата доступа: 06.04.2026.
3. FoxmindEd [Электронный ресурс]. – Режим доступа: <https://foxminded.ua/ru/sql-inekcii/> – Дата доступа: 06.04.2026.
4. Kaspersky [Электронный ресурс]. – Режим доступа: <https://www.kaspersky.ru/resource-center/definitions/sql-injection> – Дата доступа: 06.04.2026.
5. OWASP [Электронный ресурс]. – Режим доступа: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html – Дата доступа: 06.04.2026.
6. IDS00-J. Prevent SQL injection [Электронный ресурс]. – Режим доступа: <https://cmu-sei.github.io/secure-coding-standards/sei-cert-oracle-coding-standard-for-java/rules/input-validation-and-data-sanitization-ids/ids00-j/> – Дата доступа: 06.04.2026.
8. System Binary Proxy [Электронный ресурс]. – Режим доступа: <https://attack.mitre.org/techniques/T1218/005/> – Дата доступа: 03.04.2026.
9. Rules Syntax [Электронный ресурс]. – Режим доступа: <https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/rules.html> – Дата доступа: 03.04.2026.
10. Regular Expression Syntax [Электронный ресурс]. – Режим доступа: <https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/regex.html> – Дата доступа: 03.04.2026.
11. Sysmon версии 15.2 [Электронный ресурс]. – Режим доступа: <https://learn.microsoft.com/ru-ru/sysinternals/downloads/sysmon> – Дата доступа: 03.04.2026.

UDC 004.056:004.774

ANALYSIS OF WEB APPLICATION PROTECTION METHODS AGAINST SQL INJECTION ATTACKS

Salnikova V.A., student gr 361402

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Mokerov V.S. – Assistant Professor, Department of Information Security

Annotation. The article provides a theoretical analysis of methods for protecting web applications against SQL injection attacks. The following methods are considered: parameterized queries (prepared statements), stored procedures, input validation, escaping, ORM, WAF, and the principle of least privilege. A comparison of the methods is made in terms of reliability, universality, and limitations. The necessity of defense-in-depth is substantiated. The combination of parameterized queries, whitelist validation, WAF, and database privilege minimization is recognized as the most effective approach.

Keywords. SQL injection, parameterized queries, WAF, defense-in-depth, validation, prepared statements.

УДК 004.056

МЕТОДИКА ИНТЕГРИРОВАННОГО АНАЛИЗА СОБЫТИЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Сташкевич С.О., магистрант гр. 567241

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

*Бойправ О.В. – канд. тех. наук, доцент,
заведующий кафедрой защиты информации*

Аннотация. В статье представлен обзор подходов к разработке методики интегрированного анализа событий информационной безопасности. На основе анализа нормативных правовых актов Республики Беларусь выполнена классификация событий информационной безопасности, определены характеристики источников таких событий и проведена оценка современных средств их анализа. Предложена трехуровневая гибридная модель классификации, включающая технический, тактический и стратегический уровни. Полученные результаты являются основой для дальнейшей разработки методики.

Ключевые слова. события информационной безопасности, SIEM-системы, корреляция событий, управление инцидентами, классификация событий, MITRE ATT&CK.

В условиях цифровой трансформации проблема обеспечения информационной безопасности (ИБ) приобретает критическое значение. В соответствии с Концепцией информационной безопасности Республики Беларусь, утвержденной Постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, формирование информационного общества рассматривается как национальный приоритет и общегосударственная задача [1].

Многочисленные средства защиты информации (СЗИ), используемые в организациях, порождают огромное количество событий безопасности, разбор которых вручную становится невозможным, а игнорирование недопустимо [2]. По данным аналитических отчетов, крупные компании используют в среднем 43 различных СЗИ, а некоторые – более 100 [3]. В таких условиях особую актуальность приобретает задача интегрированного анализа событий ИБ.

Целью настоящей работы является обзор существующих подходов к классификации событий ИБ, анализу характеристик источников событий и оценке средств их анализа как основы для последующей разработки усовершенствованной методики интегрированного анализа.

В соответствии со СТБ ISO/IEC 27000–2024 событие информационной безопасности определяется как установленное возникновение состояния системы, службы или сети, указывающее на возможное нарушение информационной безопасности [4].

Исчерпывающий перечень типов и записей событий информационной безопасности, подлежащих регистрации, установлен приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130 [5]. Указанный перечень подразделяет события на пять категорий: операционные системы, системы управления базами данных, телекоммуникационное оборудование, прикладное программное обеспечение, средства защиты информации.

Многоуровневая гибридная модель классификации. В рамках разработки методики интегрированного анализа предложена трехуровневая гибридная модель классификации событий информационной безопасности.

Первый, базовый уровень, осуществляет техническую категоризацию сырых событий (например, «сетевая атака», «нарушение политики», «ошибка аутентификации»). Данный уровень обеспечивает первичную группировку событий.

Второй, тактический уровень, вводит интеллектуальную приоритизацию через динамический расчёт показателя риска (Severity Score), учитывающего тип события, критичность актива, надежность источника данных и контекст возникновения. Динамический расчет позволяет автоматически отфильтровывать шум и выделять значимые инциденты.

Третий, стратегический уровень использует таксономию MITRE ATT&CK для описания события в терминах поведения злоумышленника (тактики и техники). Согласно современным исследованиям, привязка правил корреляции к матрице MITRE ATT&CK обеспечивает прозрачное понимание полноты мониторинга и помогает расставлять приоритеты при развитии системы обнаружения атак [6].

Под источником событий ИБ понимается любое программное или программно-аппаратное решение, обеспечивающее ведение журнала регистрации событий [7]. В рамках исследования проанализированы следующие типы источников в соответствии с категориями, установленными приказом № 130 [5].

1. Источники событий операционных систем – регистрируют запуск/остановку системы и процессов, аутентификацию пользователей, изменение конфигурации. В операционных системах семейства Windows настройка аудита осуществляется с помощью групповых политик, что позволяет

детально определять перечень регистрируемых событий в журналах безопасности, приложений и системы [8]. В операционных системах семейства Linux центральным механизмом аудита является подсистема auditd, обеспечивающая регистрацию системных вызовов, доступа к файлам, изменений конфигурации и действий пользователей [9]. Правила аудита задаются в конфигурационных файлах /etc/audit/audit.rules и могут быть настроены для отслеживания таких событий, как запуск процессов (execve), доступ к защищаемым файлам, неудачные попытки аутентификации и модификация системных настроек.

2. Источники событий систем управления базами данных – обеспечивают регистрацию действий администраторов, команд манипуляции данными, событий авторизации. Большинство современных СУБД (как коммерческих, так и с открытым исходным кодом) предоставляют встроенные механизмы аудита. Регистрация событий может включать успешные и неуспешные попытки входа, выполнение операторов DDL (CREATE, ALTER, DROP), DML (INSERT, UPDATE, DELETE), а также изменения прав доступа (GRANT, REVOKE). Журналы аудита обычно хранятся в собственных форматах или могут направляться в системный журнал (syslog). Для централизованного сбора требуется настройка расширенного аудита, включая включение соответствующих политик и использование коннекторов для нормализации данных.

3. Источники событий телекоммуникационного оборудования – фиксируют изменения топологии, ошибки передачи данных, сетевые соединения. К ним относятся маршрутизаторы, коммутаторы, межсетевые экраны. Основным протоколом для передачи событий является Syslog, поддерживаемый подавляющим большинством устройств. Регистрируемые события включают изменение конфигурации, включение/отключение интерфейсов, ошибки протоколов маршрутизации, а также (для межсетевых экранов) разрешенные и заблокированные соединения с указанием IP-адресов, портов и протоколов. Для сбора информации о потоках трафика также используются протоколы NetFlow, sFlow и IPFIX. Особенностью является высокая интенсивность потока событий и необходимость фильтрации для снижения нагрузки на систему сбора.

4. Источники событий прикладного программного обеспечения – включают серверные и клиентские приложения, генерирующие события аутентификации, доступа к данным, изменения конфигурации. Типичными представителями являются веб-серверы (регистрируют HTTP-запросы, ошибки, попытки несанкционированного доступа), почтовые серверы (фиксируют отправку, получение, аутентификацию), системы электронного документооборота. Форматы логирования значительно варьируются – от стандартизированных (например, Combined Log Format для веб-серверов) до проприетарных. Это требует нормализации данных при централизованном сборе для приведения к единому формату, что является одной из ключевых задач SIEM-систем [3].

5. Источники событий средств защиты информации – антивирусные комплексы, системы обнаружения и предотвращения вторжений (IDS/IPS), средства защиты от несанкционированного доступа. Эти системы генерируют события, связанные с обнаружением вредоносного ПО, срабатыванием сигнатур атак, изменениями в политиках безопасности. Форматы журналов также разнообразны (многие используют Syslog или собственные форматы). Важной особенностью является необходимость корреляции событий от СЗИ с событиями от других источников для выявления сложных многоэтапных атак. Использование модели MITRE ATT&CK позволяет систематизировать события от различных СЗИ в соответствии с этапами атаки [6].

Важной характеристикой источников является максимальный набор событий, которые могут быть зарегистрированы. В работе [7] предложен подход к определению подмножества регистрируемых событий на основе анализа правил корреляции, что позволяет минимизировать ресурсные затраты при сохранении необходимого уровня обнаружения инцидентов.

Классификация средств анализа событий ИБ. Средства анализа событий ИБ можно разделить на следующие классы.

1. SIEM-системы (Security Information and Event Management) – централизованные платформы для сбора, нормализации, корреляции и хранения событий, а также управления инцидентами. Как отмечается в исследованиях, SIEM обеспечивает интеграцию управления информацией о безопасности (SIM) и управления событиями безопасности (SEM), предоставляя организациям целостное представление о состоянии защищенности [10].

2. Системы управления логами (Log Management) – обеспечивают сбор, хранение и поиск по журналам событий, но не содержат развитых механизмов корреляции (например, Elastic Stack, Graylog).

3. Системы анализа сетевого трафика (NTA/NDR) – анализируют сетевые потоки и полные захваты пакетов для выявления аномалий и атак (Zeek, RITA).

4. Платформы поведенческого анализа (UEBA) – используют методы машинного обучения для выявления аномального поведения пользователей и сущностей.

5. SOAR-платформы – обеспечивают автоматизированное реагирование на инциденты, включая анализ событий и выполнение сценариев.

Методы корреляции событий ИБ. Корреляция событий является ключевым механизмом интегрированного анализа. Согласно исследованиям, методы корреляции классифицируются на следующие типы [11].

1. Правила на основе порогов и временных окон – срабатывают при достижении заданного количества событий определенного типа в установленном временном интервале.

2. Последовательная корреляция – выявляет заданную последовательность событий (например, «неудачный вход» → «успешный вход»).

3. Корреляция на основе топологии – учитывает зависимости между компонентами инфраструктуры.

4. Корреляция на основе машинного обучения – использует алгоритмы для автоматического выявления сложных паттернов [12].

Современные подходы к корреляции событий все чаще используют методы машинного обучения. В работе [13] предложена архитектура на основе ансамбля глубоких нейронных сетей (LSTM, CNN, BRNN) с механизмами внимания для выявления временных и контекстных паттернов в данных безопасности, а также нечеткая логика для приоритизации оповещений.

Критерии выбора средств анализа с учетом их взаимодействия. Выбор средств анализа событий не сводится к оценке каждого класса изолированно. В современных системах обеспечения информационной безопасности различные средства функционируют как взаимосвязанный комплекс, где SIEM выступает центральным узлом сбора и корреляции, NTA/NDR предоставляет данные о сетевой активности, UEBA обогащает контекст поведенческими аномалиями, а SOAR автоматизирует реагирование. Поэтому критерии выбора должны учитывать не только индивидуальные характеристики, но и способность к интеграции.

Общие критерии выбора следующие.

1. Соответствие функциональным требованиям – необходимость централизованного сбора, нормализации, корреляции, хранения, визуализации и автоматизированного реагирования.

2. Производительность и масштабируемость – способность обрабатывать ожидаемый объем событий в секунду (EPS) и масштабироваться при росте инфраструктуры.

3. Поддержка источников – наличие коннекторов для существующих типов СЗИ, сетевого оборудования, операционных систем и прикладного ПО.

4. Соответствие регуляторным требованиям – возможность регистрации событий в соответствии с обязательными перечнями и форматами (например, приказ № 130) [5].

5. Гибкость настройки – возможность создания пользовательских правил корреляции, настройки дашбордов.

6. Безопасность – наличие ролевой модели доступа, шифрования данных, возможность работы в изолированных средах.

7. Стоимость владения – включая лицензирование, внедрение, поддержку и требуемые вычислительные ресурсы.

Критерии, обеспечивающие взаимодействие средств следующие.

1. Единый формат обмена данными – поддержка стандартизированных форматов (Syslog, CEF, LEEF, STIX/TAXII) позволяет безболезненно интегрировать разнородные системы. Наличие встроенных коннекторов или возможности кастомизации приема событий снижает затраты на интеграцию.

2. Наличие программных интерфейсов (API) – открытость REST API, GraphQL или других интерфейсов необходима для двустороннего обмена данными, автоматизации настройки и извлечения информации. SIEM должен предоставлять API для выгрузки оповещений в SOAR, а SOAR – API для запроса статуса задач.

3. Совместимость с моделью данных – способность средств анализировать и обогащать события в рамках единой контекстной модели (например, привязка к единому каталогу активов, пользователей, идентификаторов). Особенно важно для совместной работы UEBA и SIEM.

4. Возможность централизованного управления и оркестрации – наличие единой панели управления или возможность передачи управляющих команд между системами (например, SIEM → SOAR → межсетевой экран). SOAR должен уметь автоматически блокировать угрозы на основе оповещений SIEM.

5. Единая политика хранения и жизненного цикла данных – согласование сроков хранения событий, ротации и архивации между системами для обеспечения целостности расследований.

6. Встроенные или сертифицированные интеграции – наличие предварительно настроенных связей между конкретными продуктами разных классов снижает риски и ускоряет внедрение.

Специфические критерии для отдельных классов с учетом взаимодействия:

7. SIEM: кроме собственных возможностей корреляции, важна возможность передачи обогащенных событий в SOAR (через API или webhooks), а также приема результатов поведенческого анализа от UEBA.

8. SOAR: ключевыми являются наличие готовых плейбуков для реагирования на типовые оповещения SIEM, поддержка двусторонней синхронизации инцидентов с SIEM и возможность управления сетевым оборудованием/СЗИ.

9. NTA/NDR: должна поддерживать экспорт детектируемых событий в SIEM в стандартном формате (Syslog, CEF) и предоставлять API для запроса детальной информации о соединениях.

10. EBA: должна уметь передавать аномалии и скоринговые оценки в SIEM, обогащая контекст инцидента.

11. Log Management: должна обеспечивать быстрый доступ к сырым логам для углубленного расследования по запросу из SIEM или SOAR.

Таким образом, выбор средств анализа событий должен осуществляться как выбор экосистемы, в которой каждый компонент выполняет свою функцию, а интеграционные механизмы обеспечивают бесшовную передачу данных и автоматизацию процессов обнаружения и реагирования.

В результате проведенного обзора определены основные направления разработки усовершенствованной методики интегрированного анализа событий информационной безопасности. Выполнены три поставленные задачи исследования.

1. Классификация событий ИБ. На основе анализа нормативных правовых актов Республики Беларусь выделены пять категорий событий. Предложена трехуровневая гибридная модель классификации, включающая технический, тактический и стратегический уровни.

2. Анализ характеристик источников событий ИБ. Проведен анализ пяти типов источников событий с учетом требований приказа № 130, определены особенности регистрации событий для каждого типа: для операционных систем (Windows – групповые политики, Linux – auditd), для СУБД – встроенные механизмы аудита, для телекоммуникационного оборудования – Syslog, NetFlow, для прикладного ПО – разнообразие форматов, для СЗИ – сигнатурные и поведенческие события.

3. Оценка характеристик средств анализа событий ИБ. Проанализированы функциональные возможности основных классов средств анализа (SIEM, Log Management, NTA/NDR, UEBA, SOAR), рассмотрены методы корреляции (правила, временные окна, топология, машинное обучение), сформулированы общие и специфические критерии выбора платформ с акцентом на их взаимодействие.

Полученные результаты являются основой для выполнения следующих этапов работы: обоснование средств для реализации методики, разработка порядка конфигурирования средств, апробация методики в тестовой среде.

Список использованных источников:

1. О Концепции информационной безопасности Республики Беларусь : постановление Совета Безопасности Респ. Беларусь от 18 марта 2019 г., № 1 // ЭТАПОН : информ.-поисковая система (дата обращения 23.03.2026).
2. Модель взаимодействия компьютерных инцидентов, событий и инцидентов информационной безопасности // Научно-аналитический журнал Санкт-Петербургского университета ГПС МЧС России. – 2025. – № 2. – С. 91–101.
3. Как управление событиями (SIEM) структурирует хаос и упрощает работу ИБ-специалиста [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/How-SIEM-Makes-Work-Easier (дата обращения: 12.03.2026).
4. СТБ ISO/IEC 27000–2024. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь. – Введ. 01.10.2024. – Минск : Госстандарт : Бел. гос. ин-т стандартизации и сертификации, 2024. – 56 с.
5. О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40 : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь от 25 июля 2023 г. № 130 // Оперативно-аналитический центр при Президенте Республики Беларусь. – URL: <https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf> (дата обращения 23.03.2026).
6. Козлов, А.А. Методология применения матрицы MITRE ATT&CK для оценки эффективности систем мониторинга событий / А.А. Козлов, В.А. Смирнов // Вопросы кибербезопасности. – 2024. – № 5. – С. 28–36.
7. Кузнецов, А.В. Способ определения регистрируемых событий / А.В. Кузнецов, С.М. Ненашев // Вопросы кибербезопасности. – 2024. – № 3. – С. 45–52.
8. Смотров, Г.С. Настройка аудита безопасности в операционных системах семейства Windows / Г.С. Смотров // Информационная безопасность : сборник материалов 60-й научной конференции аспирантов, магистрантов и студентов БГУИР. – Минск : БГУИР, 2024. – С. 92–96.
9. Audit – ROSA Wiki [Электронный ресурс]. – Режим доступа: <https://wiki.rosa.ru/index.php/Audit> (дата обращения: 23.03.2026).
10. Федорченко, А.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2 / А.В. Федорченко, Д.С. Левшун, А.А. Чечулин, И.В. Котенко // Труды СПИИРАН. – 2016. – № 6(49). – С. 208–225.
11. Wang, Y. Advanced Techniques for Alert Management in Security Information and Event Management Systems With Ensembled Deep Learning, Hybrid Optimization, and Multi-Feature Extraction / Y. Wang, L. Zhang, H. Li [Электронный ресурс] // IEEE Xplore. – 2025. – Режим доступа: <https://ieeexplore.ieee.org/document/11142305> (дата обращения: 23.03.2026).
12. Cloud Security Alliance. AI Log Analysis for Event Correlation in Zero Trust [Электронный ресурс]. – Режим доступа: <https://cloudsecurityalliance.org/blog/2025/09/26/ai-log-analysis-for-event-correlation-in-zero-trust> (дата обращения: 23.03.2026).

UDC 004.056

INTEGRATED ANALYSIS METHODOLOGY FOR INFORMATION SECURITY EVENTS IN INFORMATION SYSTEMS

Stashkevich S.O., master's student gr. 567241

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

*Bojprav O.V. – PhD in Technical Sciences, Associate Professor,
Head of the Information Security Department*

Annotation. The article presents a review of approaches to the development of an integrated methodology for the analysis of information security events. Based on the analysis of regulatory legal acts of the Republic of Belarus, the classification of information security events is carried out, the characteristics of event sources are determined, and modern event analysis tools are evaluated. A three-level hybrid classification model is proposed, including technical, tactical and strategic levels. The obtained results form the basis for further development of the methodology.

Keywords. information security events, SIEM systems, event correlation, incident management, event classification, MITRE ATT&CK

A MACHINE LEARNING FRAMEWORK FOR MULTICLASS DETECTION OF DDOS NETWORK ATTACKS

Pan Huiqin, master's degree student, 467311

*Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus*

Nasonova N.V. – PhD in Technical Sciences, Associate Professor

Annotation. This paper studies machine-learning-based multiclass detection of DDoS traffic using the CIC-DDoS2019 dataset. After preprocessing, four models are compared: SVM, Random Forest, XGBoost, and MLP. The results show that Random Forest achieves the best overall performance, with near-perfect accuracy and macro-F1. A practical deployment scheme at network boundaries is also outlined for near real-time detection.

Keywords. DDoS-attacks, machine learning, supervised learning.

DDoS attacks pose a serious threat to the availability and reliability of network services by sending a large amount of traffic to the target. As attackers continuously advance their techniques and botnet sizes expand, distinguishing malicious traffic from normal network behavior becomes increasingly challenging. Machine learning is well-suited for this task because it can automatically learn discriminative patterns from traffic data. By modeling complex, high-dimensional network behaviors, supervised learning methods can improve detection accuracy and generalize to unseen or evolving types of DDoS attacks.

Support Vector Machine (SVM) is a supervised learning algorithm based on statistical learning theory, introduced by Vapnik and others in the 1990s. Its main idea is to find an optimal separating hyperplane that maximizes the margin between classes, improving classification performance. Key mechanisms include: 1) the kernel trick, which maps nonlinearly separable data into a higher-dimensional space using kernels such as linear, polynomial, and RBF; 2) support vectors, which are the critical samples defining the decision boundary; and 3) the soft margin, which introduces slack variables to handle noise and outliers.

Random Forest is an ensemble classification algorithm that improves accuracy and robustness by combining multiple decision trees. Its main mechanism relies on two sources of randomness: first, each tree is trained on a Bootstrap sample drawn with replacement from the training set; second, at each split, only a random subset of features is considered. This increases diversity among trees and allows the model to learn different views of the data. For prediction, each tree makes an independent decision, and the final class is determined by majority voting.

XGBoost (Extreme Gradient Boosting) is an ensemble learning algorithm based on Gradient Boosting Decision Trees (GBDT). It builds trees sequentially, where each new tree learns the residual errors of the previous ones, gradually improving the overall prediction. XGBoost optimizes the objective function using a second-order Taylor expansion and includes regularization terms to reduce overfitting. It also supports parallel computation, handles missing values automatically, and offers high flexibility and scalability, which often leads to very strong performance in classification and regression tasks.

The training is based on the CIC-DDoS2019 dataset, which contains approximately 485,000 samples with 87-dimensional flow features, covering 1 type of normal traffic and 10 types of DDoS attacks. After filling in missing values, handling outliers, encoding categorical labels, and Z-score standardization, the data is split into training and test sets in an approximately 80:20 stratified manner. All preprocessing parameters are fitted only on the training set and then applied to the test set to avoid data leakage.

In terms of training strategy, traditional machine learning optimizes hyperparameters using grid search and cross-validation, while the deep model MLP uses the Adam optimizer and categorical cross-entropy loss, combined with early stopping, learning rate decay, as well as batch normalization and Dropout to control overfitting. Finally, each model is evaluated on the test set using metrics such as accuracy, precision, recall, and macro-average F1, and the training process and results can be visualized using learning curves, confusion matrices, and feature importance plots.

The performance of the random forest model on the test set is shown in Table 1. As seen from the results in the table, the four evaluation metrics are all very close to 1 overall, indicating that the model has good overall discriminative ability in the multi-classification task across 11 categories (normal traffic + 10 types of DDoS attacks). Specifically, a high precision indicates that when the model identifies an attack, the vast majority of samples indeed belong to the corresponding attack type, thereby reducing the risk of false alarms; at the same time, a high recall suggests that the model can cover most of the actual attack samples, with relatively few missed detections, allowing potential threats to be discovered more promptly. The balanced performance of precision and recall (macro-average F1-score close to 1) further demonstrates that the model's ability to recognize different attack categories is relatively even, rather than performing well only on a few categories.

Compared with SVM, XGBoost, and deep learning models (such as MLP), random forest achieves the most balanced overall performance. Therefore, it can not only achieve stable classification results on known

data distributions, but is also more suitable as the preferred model for scenarios with unknown traffic. In real network environments, attack behavior may have variations or distribution shifts, and models that can maintain both high precision and recall are often more reliable.

Table 1 – Random Forest Algorithm Parameters

Metric	Accuracy	Precision (Macro Avg)	Recall (Macro Avg)	F1-Score (Macro Avg)
Random Forest	0,998960	0,997982	0,996922	0,997455

Deploy the trained random forest detection module at network boundaries or traffic aggregation points, such as the firewall, the interior of a gateway, or in conjunction with existing NetFlow, sFlow, or mirrored traffic exports. At the collection points, extract flow-level features from the traffic (using the same 87 dimensions or selected features as in the training phase), then perform the same standardization and encoding on the features as used during training, and feed them into the random forest model to obtain the class (normal or specific attack type) and confidence level.

The detection module only performs classification and alerting, and can be decoupled from blocking and rate limiting: it sends the 'predicted category + confidence level + flow identifier' to downstream systems via message queue or interface, and the blocking module generates firewall rules, ACLs, or rate-limiting policies based on the strategies and deploys them to boundary devices. High-confidence attacks can automatically trigger blocking, medium-confidence ones can be rate-limited or have enhanced monitoring, and low-confidence ones can be recorded only for analysis.

Random forests have low inference latency, making them suitable for near real-time detection; during deployment, fix the optimal hyperparameters and preprocessing steps obtained during the training phase, and periodically retrain or validate with newly labeled traffic to cope with concept drift and new attack types, ensuring continuous effectiveness in the IDS.

List of references

1. Khemapatapan C .2- STAGE SOFT DEFENDING SCHEME AGAINST DDOS ATTACK OVER SDN BASED ON NB AND SVM[J]. 2018.
- 2.Malliga S , Kogilavani S V , Sowmya R .Deep discover: Deep learning models for detecting distributed denial of service (DDoS) attacks[J].AIP Conference Proceedings, 2022, 2393(1):7.DOI:10.1063/5.0074445.
- 3.Berqia A , Bouijij H .Predicting DoS/DDoS Attacks Using Deep Learning Models[J].2024 6th International Symposium on Advanced Electrical and Communication Technologies (ISAECT), 2024:1-7.DOI:10.1109/isaect64333.2024.10799580.
- 4.Narender M , Y. N .Deep Regularization Mechanism for Combating Class Imbalance Problem in Intrusion Detection System for Defending DDoS Attack in SDN[J].Journal of Computer Science, 2023.DOI:10.3844/jcssp.2023.334.344.
5. Draper-Gil, G., Lashkari, A. H., Mamun, M., & Ghorbani, A. A. (2016). Characterization of Encrypted and VPN Traffic Using Time-Related Features. In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP)*, 407-414. Rome, Italy.
- 6.Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2019). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, 108-116.

EFFICIENT WEB-VULNERABILITY DETECTION TECHNIQUE USING HYBRID SAST-DAST ANALYSIS AND MACHINE LEARNING

Kondo K.N., master's degree student, 467311

*Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus*

Nasonova N. – PhD in Technical Sciences, Associate Professor

Abstract: This study presents a lightweight, interpretable machine learning framework that correlates the outputs of static (SAST) and dynamic (DAST) security testing tools to reduce false positives and prioritize true vulnerabilities. Trained on the OWASP Benchmark (2,740 test cases), the Random Forest model achieves F1=0.837, recall=0.943, and reduces false positives by 66.8% compared to standalone DAST. Validation on realistic vulnerable applications (crAPI, WebGoat) showed precision@10=0.70 and 80% alert reduction on crAPI, and precision@20=0.80 with 84% alert reduction on WebGoat. SHAP analysis provides transparency, enabling analysts to understand each prediction.

Keywords. SAST, WebGoat, DAST, OWASP.

Modern web applications face increasing security threats; however, existing SAST and DAST tools suffer from high false-positive rates and fragmented results, leading to alert fatigue. Although hybrid approaches exist, they often introduce performance overhead or lack interpretability [1, 2]. This study investigates the following research question: Can an interpretable machine learning framework effectively combine SAST and DAST outputs to significantly reduce false positives and prioritize vulnerabilities compared to standalone tools while maintaining high recall? To address this question, the study introduces an innovative framework that integrates SAST (Semgrep, SpotBugs, SonarQube) and DAST (OWASP ZAP) outputs via an interpretable machine learning model to intelligently correlate evidence and prioritize vulnerabilities.

This framework is a lightweight post-processing engine that operates outside of the production network. It ingests normalized outputs from SAST tools (that are run during development) and DAST tools run against a staging environment and provides a prioritized vulnerability report. As this is a decoupled architecture, it has zero runtime overhead on production services. Integration into a DevSecOps pipeline is simple: the framework can be called as a CI/CD piece after security scans, enabling an actionable risk-ranked list to surface without requiring any modifications to existing tooling or network architecture.

The OWASP Benchmark v1.2 (2,740 test cases, 1,415 vulnerable) was used as the training dataset. For each endpoint, a feature vector is constructed. The target label is 1 if the test case/endpoint is truly vulnerable, and 0 otherwise. Raw tool outputs are normalized into a feature matrix containing binary flags for each SAST tool (semgrep, spotbugs, sonarqube) and ZAP, plus ZAP severity counts. Engineered features include: `num_tools` (total tools flagging), `agreement_semgrep_zap` (a binary indicator of corroboration between Semgrep and ZAP), `weighted_severity` = $3 \cdot \text{zap_high} + 2 \cdot \text{zap_medium} + 1 \cdot \text{zap_low}$, and `zap_relevant` (1 if any ZAP alert's CWE belongs to the 11 CWE classes present in the Benchmark, e.g., SQL injection, XSS, path traversal). A URL-to-source mapper aligns each ZAP alert with its corresponding source file using OpenAPI paths or routing definitions; SAST findings are linked similarly, enabling per-endpoint correlation. Multiple alerts or findings on the same endpoint are aggregated: ZAP severity counts are summed, and SAST flags are set to 1 if at least one finding exists in the mapped source file.

A Random Forest classifier was trained on an 80% stratified split, with hyperparameters tuned using 5-fold cross-validation. Probabilities were calibrated using Platt scaling (CalibratedClassifierCV with sigmoid) to ensure well-calibrated scores:

$$P(y = 1|f) = \frac{1}{1 + \exp(A \cdot f + B)}, \quad (1)$$

where y is the binary vulnerability label (1 = vulnerable, 0 = safe), f is the raw score from the Random Forest, $\exp$ denotes the exponential function, and A , B are parameters learned via 5-fold cross-validation.

A threshold of 0.30 was selected to maintain a recall of $\geq 90\%$. Model interpretability was provided using SHAP. Missing tool outputs (e.g., SpotBugs on non-Java services) default to 0; the model learns to handle such cases. Inference time was measured to quantify the lightweight nature of the framework. The overall architecture is shown in Figure 1.

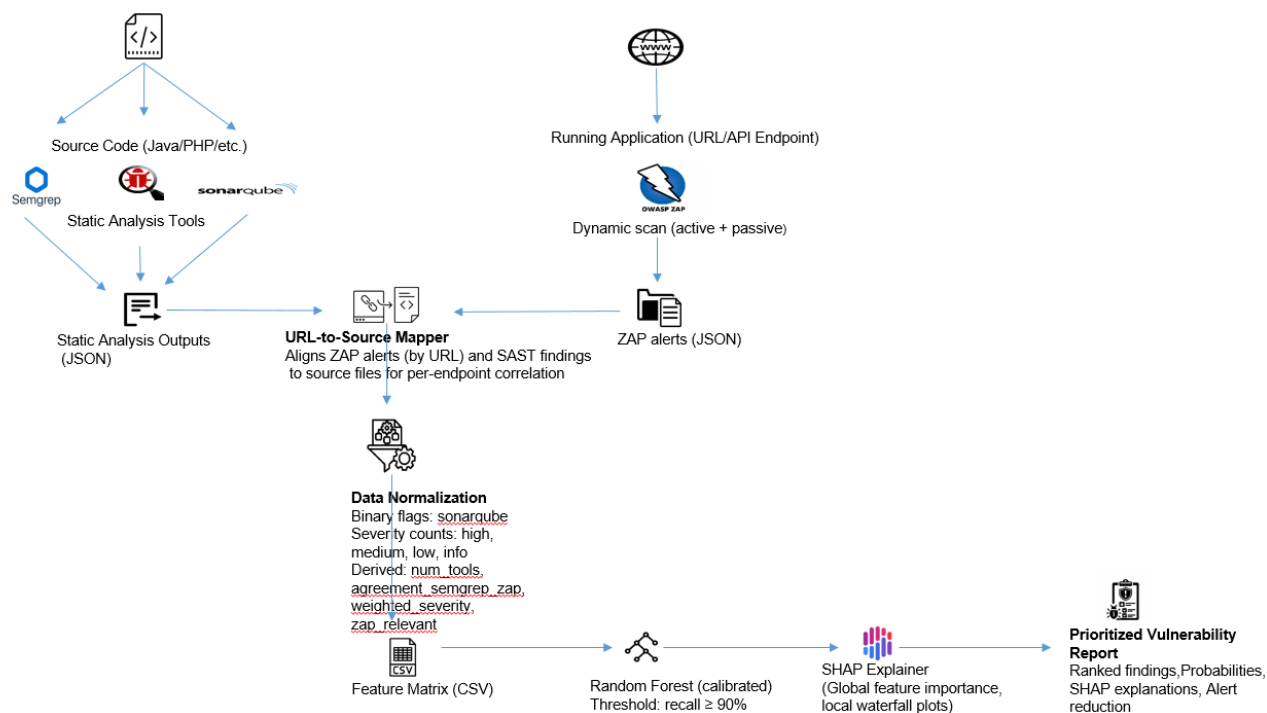


Figure 1 – Architecture of the hybrid vulnerability detection framework

On the held-out test set, which accounted for 20% of the OWASP Benchmark, the calibrated Random Forest did the following: Precision: 0.752, Recall: 0.943, F1-score: 0.837, False Positive Rate: 0.332.

Compared to the best standalone tool (Semgrep, F1=0.785), the hybrid model (F1=0.837) improves F1 by 5.2 pp and reduces false positives by 66.8% relative to ZAP's raw output. Ablation studies confirmed that ZAP features were the most important, while engineered features added measurable value. SHAP analysis (Figure 2) revealed that zap_medium and agreement_semgrep_zap as the most influential features.

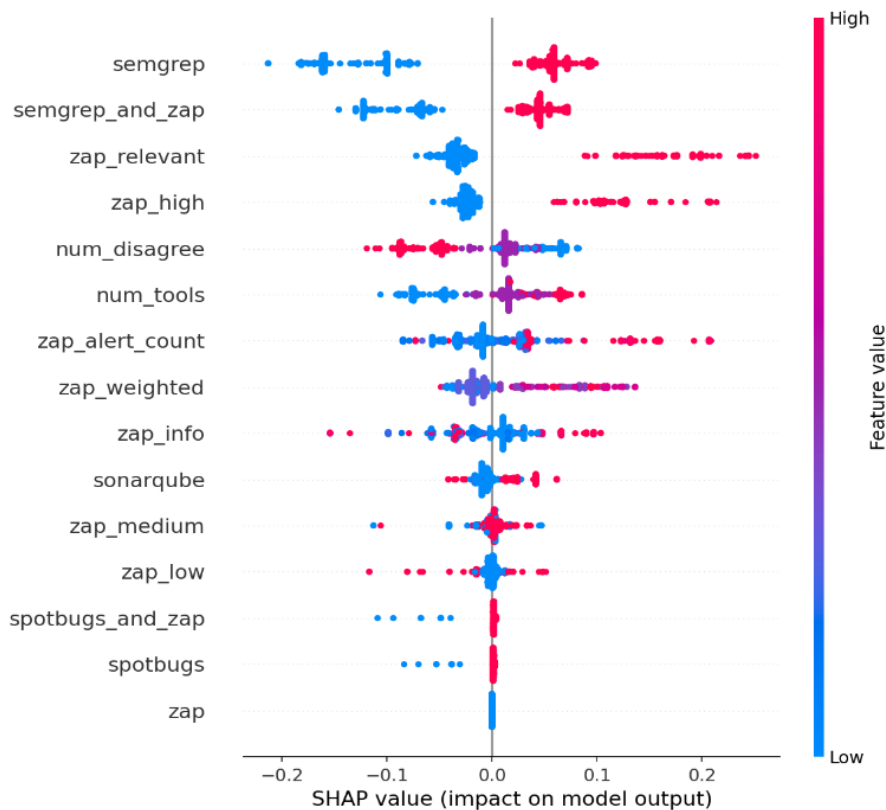


Figure 2 – SHAP summary plot showing feature importance

To assess generalizability, the framework was validated on realistic, vulnerable applications:

OWASP crAPI (modern API-first application): On a representative sample of 18 endpoints manually mapped to source code and labelled via challenge documentation (manual mapping was used only for ground-truth accuracy; in practice, mapping can be automated using route parsers), an authenticated ZAP scan produced 80 raw alerts. At a threshold of 0.30, the model flagged 16 endpoints as high-confidence, reducing the alert volume by 80%. Among the top-10 predictions, seven were true vulnerabilities (precision@10 = 0.70), and the model detected 13 of 14 known vulnerabilities (recall = 0.93). Inference time was <0.1 s, confirming lightweight operation.

OWASP WebGoat: For 126 endpoints, the model achieved precision@20 = 0.80 and reduced raw ZAP alerts by 84% (from 125 to 20), confirming consistent performance.

DVWA (PHP/MySQL): For the 10 core vulnerable endpoints, Semgrep produced 38 findings, and ZAP generated 109 alerts. The model assigned equally low probability (0.055) to all endpoints because the tool outputs were highly noisy; nevertheless, all 10 endpoints are truly vulnerable, and the top-10 predictions (all endpoints) gave precision@10 = 1.0. This result illustrates that the model remains conservative when evidence is weak, yet still ranks true vulnerabilities appropriately.

The hybrid framework successfully combines SAST and DAST evidence using an interpretable ML model, resulting in high recall while significantly reducing false positives. The explicit research question is answered positively: the model significantly reduces false positives (by 66.8–84%) while keeping the recall above 90% on both real-world and benchmark applications. Validation of realistic applications confirmed its practical value.

References

1. F. M. Tolosa et al., "On Combining Static, Dynamic and Interactive Analysis Security Testing Tools to Improve OWASP Top Ten Security Vulnerability Detection in Web Applications," *Appl. Sci.*, vol. 10, no. 24, Art. no. 9119, Dec. 2020.
2. M. Keltek, R. Hu, M. Fani Sani, and Z. Li, "LSAST: Enhancing static vulnerability detection by integrating large language models with SAST scanners," *arXiv*, 2024. [Online]. Available: <https://arxiv.org/pdf/2409.15735v2>
3. S. Qadir, E. Waheed, A. Khanum, and S. Jehan, "Comparative evaluation of approaches & tools for effective security testing of Web applications," *PeerJ Comput. Sci.*, vol. 11, p. e2821, 2025, doi: 10.7717/peerj-cs.2821.
4. G. Ibba, G. Orrù, G. Barabino, and D. R. Recupero, "A machine learning approach to vulnerability detection combining software metrics and topic modelling," *Machine Learning with Applications*, vol. 19, p. 100759, 2025.
5. M. J. S. Wicaksana and M. N. Fauzan, "Impact of Security Testing on Software Quality: A Systematic Literature Review," *Sishifo*, vol. 7, no. 2, pp. 186–200, 2025.

ИНТЕЛЛЕКТУАЛЬНЫЕ МЕТОДЫ ВЫЯВЛЕНИЯ КИБЕРУГРОЗ НА ОСНОВЕ BIG DATA

Ходжамаммедов М.М.

Государственный энергетический институт Туркменистана,
г. Мары, Туркменистан

Аннотация. В работе исследуются интеллектуальные методы выявления киберугроз в условиях обработки больших данных. Рассмотрены современные подходы, основанные на машинном и глубоком обучении, позволяющие выявлять аномалии в сетевом трафике и поведении пользователей. Особое внимание уделено интеграции аналитических моделей с распределенными вычислительными платформами и системами потоковой обработки данных. Обоснована эффективность применения интеллектуальных методов для повышения уровня информационной безопасности и своевременного обнаружения кибератак.

Ключевые слова. Big Data, киберугрозы, машинное обучение.

Современные информационно-коммуникационные системы функционируют в условиях интенсивной цифровизации и экспоненциального роста объемов данных, что существенно усложняет задачи обеспечения информационной безопасности. Увеличение количества распределенных сервисов, облачных платформ и сетевых взаимодействий приводит к расширению поверхности атак и появлению новых типов киберугроз, обладающих высокой степенью скрытности и адаптивности. В данных условиях традиционные методы защиты информации, основанные на сигнатурном анализе, демонстрируют ограниченную эффективность, поскольку не способны выявлять ранее неизвестные и модифицированные атаки.

В связи с этим ключевое значение приобретают интеллектуальные методы анализа данных, ориентированные на выявление аномалий в больших и разнородных массивах информации. Обнаружение аномалий представляет собой процесс идентификации отклонений от нормального функционирования системы, что позволяет интерпретировать такие отклонения как потенциальные признаки киберугроз. Однако в условиях Big Data данная задача характеризуется высокой вычислительной сложностью, обусловленной многомерностью признакового пространства, гетерогенностью данных и необходимостью их обработки в реальном времени [1].

Современные методы машинного обучения играют фундаментальную роль в решении задач выявления киберугроз. Особую значимость приобретают алгоритмы обучения без учителя, что обусловлено дефицитом размеченных данных в области кибербезопасности. Методы кластеризации и плотностного анализа позволяют выявлять скрытую структуру данных и идентифицировать нетипичные поведенческие паттерны. В свою очередь, алгоритм Isolation Forest реализует принцип изоляции аномальных наблюдений и демонстрирует высокую эффективность при обработке больших массивов данных благодаря линейной вычислительной сложности и масштабируемости [2].

Значительное развитие получили методы глубокого обучения, обеспечивающие возможность моделирования сложных нелинейных зависимостей в данных. Автоэнкодеры используются для построения компактных представлений данных и выявления аномалий на основе ошибки реконструкции, тогда как рекуррентные нейронные сети, включая архитектуры LSTM, позволяют учитывать временную динамику и последовательность событий. Это особенно важно при анализе сетевого трафика и пользовательского поведения, где аномалии могут проявляться в виде отклонений во временных зависимостях.

Интеграция интеллектуальных методов с технологиями Big Data является необходимым условием их практической реализации. Использование распределенных вычислительных платформ, таких как Apache Hadoop и Apache Spark, обеспечивает масштабируемость обработки данных и позволяет эффективно анализировать большие объемы информации. Дополнительно применение технологий потоковой обработки, включая Apache Kafka и Spark Streaming, обеспечивает возможность выявления киберугроз в режиме реального времени, что существенно повышает оперативность реагирования на инциденты информационной безопасности [3].

Практическое применение интеллектуальных методов демонстрирует их высокую эффективность в задачах обнаружения вторжений, анализа сетевого трафика и выявления аномального поведения пользователей. Использование гибридных моделей, объединяющих различные алгоритмические подходы, позволяет повысить точность классификации угроз и снизить уровень ложноположительных срабатываний, что является критически важным для функционирования современных систем защиты информации.

Таким образом, интеллектуальные методы выявления киберугроз на основе технологий Big Data представляют собой перспективное направление развития систем информационной безопасности. Их дальнейшее совершенствование связано с разработкой интерпретируемых моделей, способных объяснять принятые решения, повышением адаптивности к новым видам атак и интеграцией с автоматизированными системами реагирования на инциденты.

Список использованных источников

1. Chen M., Mao S., Liu Y. *Big Data: A Survey // Mobile Networks and Applications.* – 2014.
2. Liu F.T., Ting K.M., Zhou Z.-H. *Isolation Forest // ICDM.* – 2008.
3. Kleppmann M. *Designing Data-Intensive Applications.* – O'Reilly, 2017.

TEST RESULTS FOR THE METHOD OF INFORMATION SECURITY EVENT MANAGEMENT IN LINUX-KERNEL-BASED OPERATING SYSTEMS

Nguyen H.H., student of group 567311

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

*Boiprav O.V. – PhD in Technical Sciences, Associate Professor,
Head of the Information Security Department*

Annotation. This paper presents the experimental results of an implemented method designed to manage information security events on Linux-kernel-based operating systems. These information security events encompass user logins and logouts, account management, access control management, and security management. These constitute critical security events, and their effective logging has demonstrated the feasibility of the proposed method.

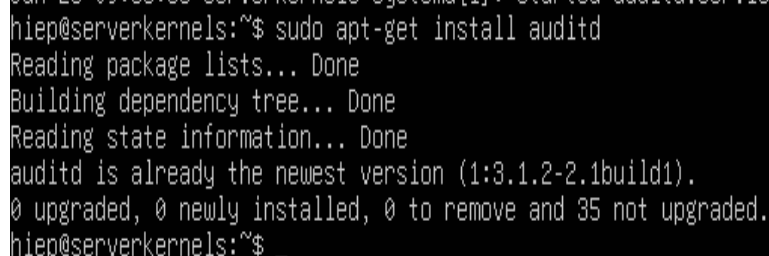
Keywords. Information security, event rules, auditd tool.

To facilitate the logging of information regarding information security events within a Linux-kernel-based operating system, the Auditd tool [1] will be installed.

Auditd tool is a system event logging tool built into most Linux distributions. It allows you to configure event logging rules and save logged events to log files.

During the configuration process, the following steps were taken.

1 Performing the command `sudo apt-get install auditd` (Figure 1).



```
hiep@serverkernels:~$ sudo apt-get install auditd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
auditd is already the newest version (1:3.1.2-2.1build1).
0 upgraded, 0 newly installed, 0 to remove and 35 not upgraded.
hiep@serverkernels:~$
```

Figure 1 – Install auditd on the operating system

2 Configure Auditd by using the following command to access the configuration file: `sudo nano /etc/audit/auditd.conf`.

3 Creating Event Rules [2].

3.1 Login event rules: recording information about users logging into the system, including login name, IP address, login time, and login type. This constitutes a critical event for detecting intruders and preventing unauthorized access.

To configure login event rules on a Linux system, the rsyslog configuration file (`/etc/rsyslog.conf`) was used: `sudo nano /etc/rsyslog.conf`.

The following two rules were added (the two rules added to the `/etc/rsyslog.conf` file serve to record all logs related to authentication and security on the Linux system into two separate files): `authpriv.* /var/log/auth.log`, `authpriv.* /var/log/secure`.

3.2 Logout event rules: logging information about users logging out of the system, including the username, IP address, and logout time. The following rule was added: `auth.* /var/log/auth.log`.

3.3 Password change event rule: logging information indicating that a user is changing their password, including the login name, IP address, and time of the change. The following rule was added: `password.* /var/log/auth.log`.

Restart the rsyslog service to activate the added services using the following command: `sudo systemctl restart rsyslog`.

3.4 Access modification event rule [3]: logging information regarding how users change access permissions for system resources, including the username, IP address, time of modification, and access type.

To configure access modification event rules on a Linux system, the auditd configuration file (`/etc/audit/rules.d/audit.rules`) was used: `sudo nano /etc/audit/rules.d/audit.rules`.

The following rule was added: `-w /etc/passwd/ -p wa -k passwd_changes`, where `-w /etc/sysconfig/` – is the path to the directory you wish to monitor; `-p wa` – specifies the type of event you wish to monitor. `w` represents a write event, and `a` represents an access modification event; `-k sysconfig_changes` – is a tag used to label these events.

3.5 System configuration change event rules: recording information about the user modifying the system configuration including their login name, IP address, time of modification, and the type of configuration changed. The following rule was added: `-w /etc/sysconfig/ -p wa -k sysconfig_changes`.

3.6 Attack event rules: recording information regarding attacks on the system including the attacker's IP address, the time of the attack, and the type of attack. The following rules were added: `-a always,exit -F arch=b64 -S execve -k detect_attack`; `-a always,exit -F arch=b32 -S execve -k detect_attack`, where `-a always,exit` – specifies the rule types; `-F arch=b64` and `-F arch=b32` – are conditions limiting the rule to 64-bit and 32-bit architectures, respectively; `-S execve` – is the specific event you wish to monitor.

3.7 Security event rules: recording information regarding security operations performed on the system including the username, IP address, time of execution, and the type of security operation performed. The following rules were added: `-w /etc/passwd -p wa -k password_file`; `-w /etc/shadow -p wa -k password_file`; `-w /etc/sudoers -p wa -k sudoers_file`.

Restart the auditd service to activate the added services using the following command: `sudo systemctl restart auditd`.

Records of information security activities: including logins, logouts, data security operations, password changes, and system configurations, are meticulously documented in log files configured with the assistance of auditd (Figures 2, 3, 4, 5). This demonstrates the effectiveness of the auditd tool in enabling users and administrators to maintain robust control over their devices in the face of security events, thereby facilitating the implementation of measures to prevent and mitigate potential threats arising from such incidents.

```
2026-03-19T03:00:46.273658+03:00 nguyen sudo: nguyen : TTY=ttty1 ; PWD=/home/nguyen
2026-03-19T03:00:46.276449+03:00 nguyen sudo: pam_unix(sudo:session): session opened
2026-03-19T03:00:46.292696+03:00 nguyen su[976]: (to root) root on pts/0
2026-03-19T03:00:46.293938+03:00 nguyen su[976]: pam_unix(su:session): session opened
```

Figure 2 – Log login activity to the file `/var/log/auth.log`.

```
root@nguyen:~# tail -5 /var/log/secure
2026-03-19T03:11:07.176288+03:00 nguyen sudo: root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/
2026-03-19T03:11:07.209467+03:00 nguyen sudo: pam_unix(sudo:session): session opened for user root(uid=0) by
2026-03-19T03:11:07.358519+03:00 nguyen sudo: pam_unix(sudo:session): session closed for user root
2026-03-19T03:11:42.673892+03:00 nguyen sudo: root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/bas
2026-03-19T03:11:42.678068+03:00 nguyen sudo: pam_unix(sudo-i:session): session opened for user root(uid=0) b
root@nguyen:~#
```

Figure 3 – Log security activity to the `/var/log/secure` file.

```
root@nguyen:~# ausearch -k passwd_changes
<no matches>
root@nguyen:~# ausearch -k passwd_changes -i
<no matches>
root@nguyen:~# ausearch -k sysconfig_changes
<no matches>
```

Figure 4 – Record password change activity

```
nguyen@nguyen:~$ sudo ausearch -k passwd_changes -i
[sudo] password for nguyen:
-----
type=PROCTITLE msg=audit(03/19/2026 03:31:06.792:450) : proctitle=/sbin/auditctl -R /etc/audit/audit.rules
type=PATH msg=audit(03/19/2026 03:31:06.792:450) : item=0 name=/etc/ inode=393217 dev=fc:00 mode=dir,755 ouid=root ogid=root rdev=00:00
one cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(03/19/2026 03:31:06.792:450) : cwd=/
type=SOCKADDR msg=audit(03/19/2026 03:31:06.792:450) : saddr={ saddr_fam=netlink nlnk_fam=16 nlnk_pid=0 }
type=SYSCALL msg=audit(03/19/2026 03:31:06.792:450) : arch=x86_64 syscall=sendto success=yes exit=1004 a0=0x3 a1=0x7fff2fd760 a2=0x4
1 pid=1124 auid=unset uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=(none) ses=unset comm=auditc
subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(03/19/2026 03:31:06.792:450) : auid=unset ses=unset subj=unconfined op=add_rule key=passwd_changes list=
-----
type=PROCTITLE msg=audit(03/19/2026 04:08:01.355:48) : proctitle=/sbin/auditctl -R /etc/audit/audit.rules
type=PATH msg=audit(03/19/2026 04:08:01.355:48) : item=0 name=/etc/ inode=393217 dev=fc:00 mode=dir,755 ouid=root ogid=root rdev=00:00
ne cap_fi=none cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(03/19/2026 04:08:01.355:48) : cwd=/
type=SOCKADDR msg=audit(03/19/2026 04:08:01.355:48) : saddr={ saddr_fam=netlink nlnk_fam=16 nlnk_pid=0 }
type=SYSCALL msg=audit(03/19/2026 04:08:01.355:48) : arch=x86_64 syscall=sendto success=yes exit=1004 a0=0x3 a1=0x7fff372938c0 a2=0x43
pid=590 auid=unset uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=(none) ses=unset comm=auditctl
i=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(03/19/2026 04:08:01.355:48) : auid=unset ses=unset subj=unconfined op=add_rule key=passwd_changes list=ex
```

Figure 5 – The password change operation has been recorded.

List of Sources:

1. *Configuring the Auditd Tool [Electronic Resource]*. – Access Mode: <https://habr.com/ru/articles/553036/>.
2. *Creating Event Rules [Electronic Resource]*. – Access Mode: <https://habr.com/ru/articles/553036/>.
3. *Creating Event Rules [Electronic Resource]*. – Access Mode: <https://www.redhat.com/en/blog/configure-linux-auditing-auditd>.

RESEARCH AND DEVELOPMENT OF PLAGIARISM DETECTION METHODS BASED ON DEEP NEURAL NETWORKS

Nguyen L.T., master's student gr. 567311

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

German Yu.O. – PhD in Technical Sciences

Annotation. This paper presents a comprehensive review of plagiarism forms in academia, including copy-paste, paraphrasing, mosaic, and idea plagiarism. It analyzes challenges posed by automatic paraphrasing tools, cross-language plagiarism, and multi-source plagiarism. The limitations of traditional detection methods such as string matching, n-gram, and TF-IDF are evaluated. Modern approaches based on deep learning (RNN, LSTM, BERT) and stylometry are discussed, leading to the formulation of a plagiarism detection problem that integrates semantic understanding and stylistic analysis.

Keywords. Plagiarism, TF-IDF, BERT, PhoBERT, RNN, LSTM, RCES, 1D-CNN, PCA, LLM.

In the context of the information explosion and the rapid development of writing tools, plagiarism in academia and content creation is becoming increasingly complex and sophisticated. Plagiarism is not simply the act of copying verbatim, but encompasses many other variations, from interpreting ideas and combining content from multiple sources to using automated tools to alter the surface appearance of the text. Each form of plagiarism poses unique challenges to detection systems, requiring approaches that go beyond traditional lexical matching techniques.

The most common and easily recognizable form of plagiarism is copy-paste plagiarism, in which a writer copies verbatim a passage of text from another source such as books, newspapers, scientific articles, or websites without citing the source. According to Helgesson and Eriksson (2015), plagiarism is defined as the act of taking another person's text and presenting it as one's own, or appropriating another person's ideas and language [1]. In the RCES classification, this is the case where the writer blatantly uses another person's entire work or copies the layout and structure of the text from a single source without alteration [2]. The basic identifying characteristic is the exact match of words, sentence structure, word order, and punctuation. Copied passages often create stylistic inconsistencies, becoming an important indicator when analyzing. Early detection methods such as exact string matching with Knuth-Morris-Pratt, Rabin-Karp, or Boyer-Moore algorithms, text fingerprinting, and n-gram methods have been widely used. Recently, deep learning with one-dimensional convolutional neural networks (1D-CNN) and feedback neural networks (RNN) has shown effectiveness in detecting short copied phrases of 5 to 7 words thanks to its ability to automatically learn local and sequential features [3].

At a more sophisticated level, paraphrasing plagiarism is a form of writing where the writer rephrases another person's ideas using different words and sentence structures but retains the core content without citing the source [1]. According to RCES, this is a case of trying to "disguise" by copying from multiple sources, cross-editing sentences or changing keywords and sentence structures [2]. Online tools like QuillBot help perform paraphrasing quickly and smoothly, posing a major challenge to detection systems that rely solely on vocabulary. The TF-IDF method with its bag-of-words model is completely ineffective because it treats synonyms as independent, causing the vector representations of two sentences with the same meaning but different phrasing to be far apart in space. Detecting this form requires a deep understanding of semantics. Modern deep learning models, especially the Transformer architecture with its self-attention mechanism, have shown superior capabilities. Models like BERT (Bidirectional Encoder Representations from Transformers) and its Vietnamese variant PhoBERT can create sentence representation vectors such that two sentences with the same meaning are close together in vector space, regardless of lexical differences.

An equally complex form of plagiarism is mosaic plagiarism or patchwriting, where the writer combines phrases and sentences from various sources to create a new passage. Each small part may be copied verbatim or slightly modified, creating a textual mosaic. There is no single source to compare it to, and the synthesized passage can flow smoothly if skillfully connected. According to Smodin, this is a form of plagiarism where the writer combines multiple works into one before inserting it into their essay [4]. The most important indicator of plagiarism is the stylistic inconsistency between parts of the same text. Each author has their own stylistic imprint in terms of word usage, sentence structure, sentence openings, and the frequency of prepositions, conjunctions, and pronouns. Stylometry, which studies and explains types of texts in terms of linguistic style and intonation [5], extracts quantitative characteristics such as average sentence length, average word length, type-token ratio, punctuation frequency, and frequency of different word types to create feature vectors for each passage. Euclidean distance, Manhattan distance, and cosine similarity measurements are used for comparison. Principal Component Analysis (PCA) techniques help reduce data dimensionality and visualize paragraphs, highlighting sections with distinct styles that stand out from the main group.

The most sophisticated level is idea plagiarism, where a writer copies the ideas, arguments, and thought structures of others but expresses them entirely in new words, even changing the presentation style. According to the Merriam-Webster definition cited by Smolin, plagiarism is the act of stealing and presenting another person's ideas or words as one's own, or using another person's work without attribution [4]. This is the most difficult form to detect with automated tools because there is no text duplication, and the line between legitimate idea influence and plagiarism is often very thin. Detecting idea plagiarism requires deep semantic understanding and highly abstract idea modeling. While large language models (LLMs) are opening up new approaches, a complete solution is still lacking, often requiring a combination of automated tools and expert evaluation.

The development of automated interpretation tools like QuillBot and Spinbot has created a significant challenge. QuillBot, for example, is considered a pioneering AI application with intelligent processing capabilities, helping millions of people save more than half their writing time by subtly improving wording while retaining the full meaning [6]. These tools can transform source text into new text with different wording and sentence structures while retaining the original meaning, with quality that is increasingly difficult to distinguish from natural writing style. Users simply copy the text into the tool, and within seconds they receive a smooth, interpreted version. This renders lexical matching-based systems obsolete, forcing methods to shift to semantic-based ones.

Furthermore, cross-language plagiarism is becoming increasingly common, especially in international academic environments where writers translate documents from English to Vietnamese and use them without citation. Modern tools such as Smolin Plagiarism Checker support more than 100 languages, allowing plagiarism checking across many different languages [4]. The resulting text may not contain any vocabulary overlap with the original. Detecting this type of plagiarism requires multilingual semantic matching capabilities, far exceeding traditional methods, and necessitates multilingual deep learning models such as mBERT and XLM-Roberta to represent text in the same vector space regardless of language.

Multi-source plagiarism also presents computational and detection challenges. Instead of copying from a single source, the writer takes sections from multiple different sources and combines them. No single pair of texts has a high enough degree of similarity to trigger an alert. Tools like Smolin can scan millions of documents and web pages in seconds to detect duplicate passages [4]. A holistic approach is needed, examining the entire questionable text, searching large databases for similar passages to each section, and using stylistic analysis to detect anomalies caused by the mixing of multiple authorial styles.

Faced with these challenges, traditional plagiarism detection methods reveal inherent limitations. Exact string matching, while fast and accurate against verbatim copy, cannot withstand minor alterations. n-gram methods allow for partial duplication detection but fail to capture semantic relationships, and are unsuitable for interpretations using synonyms or structural changes. The TF-IDF method, which incorporates cosine, is fast and can detect thematic similarity, but it assumes the word bag ignores word order, leading to serious errors (for example, the two sentences "Dog bites person" and "Person bites dog" have the same vector), and it cannot handle synonymy. In general, traditional methods share common limitations: "semantic blindness" (not understanding the true meaning), inability to detect interpretation, dependence on human-defined features, disregard for context, and susceptibility to being deceived by those familiar with their workings.

In this context, modern methods based on deep learning have brought breakthroughs. Reactive neural networks (RNNs) and their variants LSTM and GRU are designed to process sequential data, with a memory mechanism that retains previous information, helping to capture context and dependencies between words in sentences and paragraphs. LSTMs particularly overcome the gradient suppression problem, suitable for classification and prediction problems on time series of indeterminate length [3]. One-dimensional convolutional neural networks (1D-CNNs) are powerful in detecting characteristic local patterns such as copied phrases. Transformer architectures with self-attention mechanisms allow the model to consider the relationship between all words regardless of position, creating a leap forward in semantic understanding. Pre-trained models such as BERT and PhoBERT can generate semantically rich representation vectors, helping to detect interpretive sentences and even paragraphs composed from multiple sources.

Alongside deep learning, stylometry-based approaches remain crucial, particularly in mosaic plagiarism detection. The core principle is that each author possesses a unique stylistic signature, and when a text contains plagiarized passages, those passages bear the imprint of another author, creating statistically detectable anomalies. Feature systems include lexical features (sentence length, word length, part-of-speech ratio), syntactic features (punctuation frequency, word type), content features, and structural features. After extraction, each passage is represented as a feature vector, distance measurements are used for comparison, and PCA helps visualize the anomalies.

The trend of combining methods is gaining attention because no single method effectively handles all forms of plagiarism. The most promising combination is integrating deep learning with semantic understanding and stylometry with anomaly detection capabilities. In a hybrid model, deep learning handles semantic plagiarism detection (interpretation, ideas), while stylistic measurement focuses on mosaic plagiarism detection through stylistic differences between paragraphs. Another approach is a multi-tiered

model, where the first tier uses rapid methods like n-gram or TF-IDF for preliminary screening, and the second tier uses deep learning for in-depth analysis of suspected cases.

Based on the overall analysis of the current situation and challenges, the research problem of this thesis is stated as follows: Given a questionable text D, which is a sequence of sentences, and a large set of reference sources C, the task is to identify the parts of D that are highly likely to be plagiarized from one or more sources in C, and to classify the corresponding form of plagiarism as exact copying, interpretation, or mosaic plagiarism. Specific requirements include: accurate copy detection with high precision; interpretation detection even when wording changes completely but the meaning remains the same; and mosaic plagiarism detection through stylistic anomalies. The system needs to minimize false positives and omissions, and be able to explain the basis of detection to increase persuasiveness in an academic environment. Regarding constraints, the system must be able to handle English with its unique grammatical and lexical characteristics, have an acceptable processing time for medium-length texts, and not require excessively high hardware specifications.

The research hypothesis is that deep learning neural networks, especially LSTM architecture with long-term information retention and sequential data processing [5], combined with other deep learning components, can overcome the limitations of traditional methods thanks to three main capabilities: automatic feature learning from data without manual definition, semantic understanding in specific contexts, and capturing stylistic patterns to detect anomalies. The results of the deep learning neural network testing method are shown in Figure 1.

```

EXTRACTING ADVANCED STATISTICS...

BASIC TEXT STATISTICS:
• Original: 61 words, 442 chars, 3 sentences
• Suspicious: 58 words, 368 chars, 3 sentences
• Size Ratio (Suspicious/Original): 95.1%

ANALYSIS SCORES:
• Content Similarity: 0.0%
• Neural Network Confidence: 79.6%

NEURAL NETWORK PREDICTION:
• NOT plagiarized

FINAL VERDICT:
• NOT plagiarized
• Risk Level: LOW RISK
• Reason: Content similarity very low (0.0%)

MEANINGFUL COMMON WORDS (2):
as, of
    
```

Figure 1 – The results of the deep learning neural network testing method

This paper systematically and comprehensively presents the problem of plagiarism detection in the context of modern academia. The four main forms of plagiarism – verbatim copying, interpretation, mosaicism, and idea plagiarism – are clearly analyzed, along with their identifying characteristics, levels of sophistication, and corresponding detection challenges. The development of automated interpretation tools, cross-language plagiarism, and multi-source plagiarism has shown that traditional methods based on lexical matching (exact strings, n-grams, TF-IDF) are increasingly inadequate due to limitations in “semantic blindness” and the inability to detect linguistic variations. Conversely, modern approaches such as deep learning with RNN, LSTM, and BERT architectures, and style measurement methods, offer promising prospects for more effective solutions thanks to their ability to automatically learn features, understand contextual semantics, and detect stylistic anomalies. Based on that analysis, the paper poses a specific research problem: developing a semantically and stylistically integrated plagiarism detection model capable of processing English texts with high accuracy and classifying different types of plagiarism.

List of Sources:

1. Helgesson, G. and Eriksson, S. *Plagiarism in research* / G. Helgesson, S. Eriksson // *Medicine, Health Care and Philosophy*, 2015. – Vol. 18, no. 1. – P. 91-101.
2. RCES. *Plagiarism Classification* / Research Center for Educational Statistics, 2020.
3. Goodfellow, I., Bengio, Y. and Courville, A. *Deep Learning* / I. Goodfellow, Y. Bengio, A. Courville. – Cambridge : MIT Press, 2016. – P. 367-370.
4. Smodin. *Smodin Plagiarism Checker* / Smodin LLC, 2023.
5. Trudgill, P. *Sociolinguistics: An Introduction to Language and Society* / P. Trudgill. – London : Penguin Books, 2000. – P. 1-3.
6. QuillBot. *QuillBot Paraphrasing Tool* / QuillBot, 2023.

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ БЛОКОВ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Асиненко А.М., аспирант

Белорусский государственный университет информатики и радиоэлектроники¹
г. Минск, Республика Беларусь

Грабчиков С.С. – д-р тех. наук

Аннотация. В работе рассматриваются вопросы электромагнитной совместимости (ЭМС) блоков беспилотных летательных аппаратов. Исследуются физические основы ЭМС, источники электромагнитных помех и чувствительные компоненты систем БПЛА. Представлены методы обеспечения электромагнитной совместимости, включая конструктивные решения, фильтрацию сигналов и организацию кабельных систем. Освещены современные технологии защиты и стандарты в области ЭМС. Показана важность комплексного подхода к решению проблем электромагнитной совместимости при проектировании и эксплуатации БПЛА.

Ключевые слова. Электромагнитная совместимость, ЭМС, беспилотные летательные аппараты, БПЛА, электронные компоненты, электромагнитные помехи, экранирование, фильтрация сигналов, силовые системы, навигационные модули, системы управления, стандарты ЭМС, электромагнитные наводки, паразитные ёмкости, конструктивные решения, цифровая обработка сигналов.

Электромагнитная совместимость (ЭМС) представляет собой комплексное свойство электронных систем БПЛА, обеспечивающее их корректную работу при совместном функционировании. В современных беспилотных системах, где плотность размещения электронных компонентов постоянно растёт, вопросы ЭМС приобретают особую актуальность и требуют системного подхода к решению.

Физические основы электромагнитной совместимости. Электромагнитные процессы в БПЛА характеризуются сложными взаимодействиями между различными компонентами. Основными факторами, влияющими на ЭМС, являются:

- электромагнитное излучение от электронных компонентов;
- наводки в проводящих элементах конструкции;
- паразитные ёмкости и индуктивности;
- эффект близости проводников.

Эти факторы могут вызывать нежелательные взаимодействия между различными системами БПЛА, что приводит к сбоям в работе или снижению точности и надёжности функционирования аппарата. Для минимизации негативных последствий необходимо учитывать особенности электромагнитного взаимодействия на всех этапах проектирования и эксплуатации БПЛА [1].

Основными генераторами помех выступают силовые элементы системы. Электронные регуляторы скорости (ESC) при коммутации высоких токов создают импульсные помехи, которые распространяются по цепям питания и через электромагнитное излучение. Бесколлекторные двигатели порождают значительные электромагнитные наводки в ходе коммутационных процессов. Силовые преобразователи и драйверы генерируют высокочастотные помехи, а системы зарядки аккумуляторов – низкочастотные.

Помимо внутренних источников, помехи могут возникать извне: от других электронных устройств, линий электропередач, радиопередатчиков, промышленных установок и даже природных явлений (например, грозových разрядов). При проектировании БПЛА важно учитывать, как внутренние, так и внешние источники помех, чтобы минимизировать риски сбоев.

Ряд устройств в БПЛА особенно уязвимы к электромагнитным наводкам. Навигационные модули GPS/ГЛОНАСС под воздействием сильных помех искажают определение координат и скорости, что критично для автономных режимов полёта. Системы передачи видео (FPV) страдают от электромагнитных наводок, что приводит к «шуму» на экране или полной потере сигнала.

Радиоканалы управления подвержены нарушениям из-за помех – это может нарушить связь с наземной станцией и создать риск неконтролируемого полёта или аварии. Датчики инерциальной навигационной системы (ИНС) под влиянием электромагнитных полей снижают точность измерения ускорения, угловой скорости и ориентации аппарата, искажая данные о его положении.

Для защиты таких компонентов применяют экранирование, фильтрацию сигналов и продуманную компоновку системы.

Комплексный подход к ЭМС объединяет несколько направлений. В первую очередь используются конструктивные решения: металлические корпуса экранируют ключевые компоненты, правильная компоновка минимизирует взаимное влияние силовых и чувствительных элементов, экранированные кабели снижают излучение и наводки, а эффективная система заземления отводит помехи.

Важную роль играет фильтрация сигналов. Конденсаторы подавляют высокочастотные помехи, LC-фильтры (комбинации индуктивностей и ёмкостей) устраняют импульсные наводки, ферритовые

бусины нейтрализуют помехи на проводах питания, а фильтры ЭМС защищают чувствительные компоненты на входных цепях.

Организация кабельных систем также требует внимания: разделение силовых и сигнальных цепей минимизирует наводки, витые пары снижают электромагнитное излучение, группировка кабелей по функциональному назначению упрощает экранирование, а минимизация длины проводников сокращает паразитные параметры.

Специальные меры защиты включают использование дифференциальных сигналов (для повышения помехоустойчивости), гальваническую изоляцию (оптроны, трансформаторы) для разрыва электрических связей между цепями, а также проектирование с учётом требований ЭМС на этапе разработки.

Особое внимание при проектировании БПЛА уделяется взаимодействию силовых и сигнальных цепей, поскольку даже незначительные наводки могут дестабилизировать работу критически важных систем. Например, импульсные токи от бесколлекторных двигателей способны создавать электромагнитные «всплески», которые проникают в цепи управления, вызывая ложные команды или сбои в алгоритмах стабилизации полёта. Чтобы минимизировать такие эффекты, инженеры тщательно моделируют электромагнитное поле внутри корпуса аппарата – зачастую с помощью специализированного ПО, позволяющего визуализировать зоны повышенного риска и корректировать компоновку ещё на этапе проектирования.

Ключевую роль играет грамотная трассировка кабелей. Витые пары, например, не просто снижают излучение – их конструкция компенсирует магнитные поля, создаваемые током, благодаря противоположному направлению скрученных проводников. Группировка кабелей по функциональности (силовые, управляющие, аналоговые) позволяет создать «чистые» зоны, где чувствительные сигналы не пересекаются с мощными токами. При этом даже небольшие изгибы или перегибы кабелей могут резко увеличить паразитные ёмкости, поэтому инженеры стремятся прокладывать провода максимально прямыми маршрутами, избегая резких поворотов [2].

Фильтрация сигналов требует тонкого баланса между подавлением помех и сохранением целостности полезного сигнала. LC-фильтры, например, настраиваются под конкретные частоты, характерные для используемых компонентов: слишком жёсткая фильтрация может исказить форму питающего напряжения, что критично для драйверов моторов. Конденсаторы, размещаемые близко к потребителям, действуют как «локальные накопители», сглаживая скачки тока и предотвращая провалы напряжения, которые могут нарушить работу микроконтроллеров.

Экранирование – не просто установка металлических корпусов, а сложный инженерный расчёт. Например, для GPS-модулей часто применяют многослойные экраны из меди и ферритовых материалов, которые блокируют низкочастотные помехи, не ухудшая приём спутниковых сигналов. При этом важно обеспечить непрерывность экрана: даже небольшие разрывы или неплотное прилегание к корпусу превращают его в «окно» для наводок. Нередко используются гибкие экранирующие ленты для защиты разъёмов и соединений, которые подвержены механическим нагрузкам.

Гальваническая изоляция через оптроны или трансформаторы особенно важна для интерфейсов, связывающих БПЛА с наземными станциями. Такие устройства разрывают прямой электрический путь, по которому помехи могли бы проникнуть в управляющую электронику. Например, в системах передачи телеметрии оптроны предотвращают «замыкание» между бортовым питанием и наземным оборудованием, что критично при работе в условиях высокого фона (например, вблизи ЛЭП).

На этапе монтажа критически важны несколько аспектов. Экраны кабелей должны надёжно соединяться с системой заземления – иначе они сами станут антеннами, усиливающими помехи. Минимизация площади токовых контуров снижает излучаемые помехи, а оптимизация путей заземления обеспечивает эффективный отвод помех через проводники с минимальным сопротивлением.

Короткие соединения уменьшают паразитные параметры (ёмкости, индуктивности), провоцирующие наводки. Не менее важно учитывать взаимное расположение компонентов: силовые элементы (двигатели, ESC) размещают вдали от приёмных антенн и чувствительных модулей, кабели питания и управления прокладывают так, чтобы они не пересекались с сигнальными линиями, а экранированные секции (например, для GPS-модулей) изолируют от источников помех.

Нормативная база ЭМС включает международные стандарты IEC (Международной электротехнической комиссии), европейские нормы EN, российские ГОСТы, а также специфические авиационные требования. Эти документы устанавливают критерии совместимости для оборудования, используемого в БПЛА, и учитывают особенности эксплуатации летательных аппаратов.

Соблюдение стандартов – обязательное условие для сертификации и легальной эксплуатации БПЛА в большинстве стран. Несоблюдение может привести к штрафам, запрету на полёты или проблемам с получением разрешений.

Инженеры разрабатывают инновационные решения для повышения ЭМС. Метаматериалы с особыми электромагнитными свойствами позволяют создавать лёгкие, но эффективные экраны.

Интеллектуальные системы фильтрации анализируют помехи в реальном времени и автоматически настраивают параметры подавления.

Алгоритмы цифровой обработки сигналов выделяют полезный сигнал даже из сильно зашумлённого канала, улучшая работу навигационных и видеосистем. Системы активного подавления генерируют компенсирующие сигналы, «гася» внешние помехи – например, для защиты радиоканалов управления.

Кроме того, программное обеспечение для моделирования (САПР) позволяет прогнозировать электромагнитное взаимодействие компонентов до сборки, сокращая количество итераций при проектировании.

Исследования в области ЭМС продолжаются: совершенствование материалов, алгоритмов и методов моделирования напрямую влияет на надёжность, дальность связи и точность работы БПЛА [3].

В итоге можно сказать, что обеспечение электромагнитной совместимости является критически важным аспектом проектирования и эксплуатации беспилотных летательных аппаратов. Комплексный подход к решению проблем ЭМС, включающий конструктивные, технологические и схемотехнические решения, позволяет создать надёжную и эффективную систему, способную работать в различных условиях эксплуатации.

Постоянное совершенствование методов обеспечения ЭМС остаётся одним из приоритетных направлений развития беспилотной авиации, что обусловлено растущей сложностью электронных систем и повышением требований к надёжности их функционирования. В современных условиях это особенно актуально в связи с расширением сфер применения БПЛА и увеличением плотности их размещения в воздушном пространстве.

Развитие технологий ЭМС не только способствует повышению эффективности и безопасности работы БПЛА, но и открывает новые возможности для их применения в различных отраслях – от сельского хозяйства и строительства до спасательных операций и мониторинга окружающей среды.

Список использованных источников:

1. Qiu f. Et al. Thermal behavior of the yag precursor prepared by sol–gel combustion process // *ceramics international*. 2005. P. 663-665.
2. Третьяков ю.д., путляев в.и. *введение в химию твердофазных материалов: учеб. Пособие*. М.: изд-во моск. Ун-та: наука, 2006. 400 с.
3. Чевела в.в. и др. *Цитраты алюминия (III) // ученые записки казанского университета: естественные науки*. 2011. С.61-69.

ПРОГРАММНАЯ ПЛАТФОРМА ДЛЯ ФИШИНГОВЫХ СИМУЛЯЦИЙ

Биюмен Е.А., студент гр.361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. тех. наук, доцент

Аннотация. В статье анализируется статистика угроз методами социальной инженерии в корпоративном секторе за 2025–2026 годы. Рассматриваются когнитивные факторы, влияющие на успешность целевых атак, и приводится количественное обоснование неэффективности классических методов обучения. Предложена архитектура программной платформы для фишинговых симуляций, автоматизирующая процессы аудита информационной безопасности посредством модулей копирования веб-ресурсов и отслеживаемых электронных документов.

Ключевые слова. информационная безопасность; социальная инженерия; когнитивная уязвимость; фишинговые симуляции; непрерывное обучение; автоматизация аудита.

Социальная инженерия в 2025–2026 годах является доминирующим вектором первоначального проникновения в корпоративные информационные системы. По данным аналитических центров, количество писем с признаками манипуляции в корпоративных почтовых системах выросло в три раза по сравнению с показателями предыдущего года [1].

Традиционные средства контентной фильтрации демонстрируют резкое снижение эффективности. Например, в строительной отрасли доля вредоносных писем, отклоненных на этапе базовой технической проверки, снизилась с 38% до 4,5% [1]. Данный факт обусловлен массовым использованием нарушителями скомпрометированных легитимных учетных записей партнеров. В условиях, когда программно-аппаратные барьеры пропускают подавляющее большинство целевых атак, критичным элементом системы защиты становится способность самого сотрудника выявлять аномалии.

Успешность социальной инженерии базируется на эксплуатации нейробиологических особенностей распределения внимания. Нарушители конструируют сообщения таким образом, чтобы адресат обрабатывал информацию рефлексивно, исключая аналитический подход. Детальный анализ позволяет выделить ключевые параметры писем, преодолевающие когнитивные барьеры:

1 Использование реальных персональных данных и точное копирование корпоративных интерфейсов активируют эффект внутригруппового искажения. Мозг воспринимает визуально знакомую среду как безопасную, блокируя механизмы скептицизма [1].

2 Письма, доставляемые в периоды пиковых нагрузок, эксплуатируют усталость от принятия решений: способность к критическому анализу снижается, и действия выполняются автоматически [1]. Согласно аналитике, фишинговые атаки имеют недельную сезонность: пик активности нарушителей приходится на среду (22,1%) и вторник (20,9%), когда загрузка сотрудников максимальна. К концу недели наблюдается спад с минимумом в воскресенье (1,2%) [2]. Описанная сезонность активности нарушителей проиллюстрирована на рисунке 1.

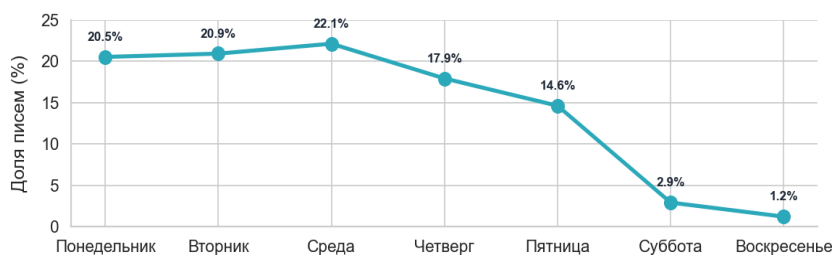


Рисунок 1 – График доли фишинговых писем в зависимости от дня недели в 2024 году

3 Использование QR-кодов в теле письма вынуждает пользователя перейти с рабочего компьютера на личный смартфон. Это выводит сотрудника из защищенной корпоративной среды и притупляет привычную настороженность [3].

4 Чаще всего ошибки возникают при маскировке фишинга под рутинные бизнес-процессы (акты сверок, уведомления систем документооборота). Из-за привыкания сотрудники обрабатывают такие письма рефлексивно. Число подобных атаккратно возросло в отраслях с интенсивным внешним документооборотом: в сфере профессиональных услуг – более чем в 8 раз, в логистике – в 3 раза, в здравоохранении – в 2 раза [1].

5 Применение факторов авторитетности (сообщения от имени руководства) и срочности провоцирует стресс. Это переключает мозг в режим быстрого реагирования, заставляя сотрудника фокусироваться исключительно на немедленном выполнении требований [4].

Традиционный подход к повышению осведомленности персонала, опирающийся на теоретические инструктажи и нормативный контроль, демонстрирует низкую продуктивность. Масштабные контролируемые исследования подтверждают полное отсутствие статистически значимой корреляции между тем, насколько недавно сотрудник прошел лекционное обучение, и его способностью противостоять реальным целевым атакам [5]. Пользователи, недавно завершившие теоретический курс, поддаются на социальную инженерию с той же вероятностью, что и лица, не проходившие его более года [5]. Теоретические знания не конвертируются в защитные рефлексy без регулярного практического закрепления.

В противовес лекционному подходу, методология регулярных фишинговых симуляций доказывает высокую результативность. Практическое погружение сотрудника в контролируемую среду учебной симуляции позволяет объективно выявить реальные поведенческие уязвимости [5]. В перспективе эффективность таких тренировок планируется усилить концепцией «моментальной обратной связи» (когда разбор ошибки предоставляется сразу после ее совершения) [6].

Важным фактором эффективности симуляций является их релевантность, использующая эффект семантического предшествования. Учебный сценарий должен строго соответствовать должностным обязанностям (например, имитация финансовых документов для бухгалтерии). Системный переход от разовых инструктажей к непрерывным релевантным симуляциям позволяет снизить базовый процент уязвимости персонала с 33,1% до 4,7% в течение одного года работы [6].

Для практической реализации описанной методологии разработана программная платформа для фишинговых симуляций. Подробная микросервисная архитектура комплекса, включающая изолированное ядро рассылок, модуль автоматизированной разведки и модуль фильтрации машинного трафика, была детально представлена в ранее опубликованной работе [7].

Процесс проведения учебной симуляции на базе разработанной платформы состоит из последовательных этапов, объединяющих работу графического интерфейса пользователя и скрытых технических механизмов. На этапе конфигурации администратор задает базовые параметры через форму сборки (рисунок 2, а). Процесс начинается с подготовки материалов: система позволяет создавать пользовательские шаблоны электронных писем и осуществлять точное копирование (клонирование) целевых веб-ресурсов для повышения реалистичности сценария. Формирование целевых групп тестируемых сотрудников реализуется двумя способами: путем прямого импорта списков или с использованием встроенного модуля автоматизированной разведки по открытым источникам. Данный модуль применяет средства морфологического анализа для извлечения персональных данных из текстовых массивов. По завершении настройки новая кампания сохраняется в статус «Черновика», а после подтверждения (нажатия кнопки запуска кампании) переходит в активный статус и отображается в общей панели управления (рисунок 2, б).

Сборка новой кампании

Название кампании: Тестовая кампания

Список целей: Группа сотрудников кампании (9 чел.)

SMTP Сервер: SMTP-сервер кампании (secadmin@lab.local)

Шаблон письма: Письмо для смены пароля

Целевая веб-страница: Веб-страница для смены пароля

Вложение: Подробная информация о смене пароля

Отмена Сохранить черновик

а

Управление Кампаниями

Организация фишинговых симуляций

Создать кампанию

Имя кампании	Статус	Действия
Тестовая кампания	В процессе	📄 🔄 🗑️

б

Рисунок 2 – Запуск и управление фишинговыми симуляциями (кампаниями)

После запуска инициируется процесс генерации писем и подстановки данных. Ключевую технологическую роль на данном этапе выполняет модуль промежуточного проксирования почтового трафика, который перехватывает исходящие сообщения до их выхода во внешнюю сеть. Промежуточный узел решает две задачи. Во-первых, осуществляется подмена технических заголовков письма для имитации легитимных корпоративных почтовых программ, что позволяет обходить базовые средства фильтрации. Во-вторых, в сообщение динамически внедряется отслеживаемое электронное вложение. Техническая реализация такого вложения базируется на внедрении связи с внешним ресурсом во внутреннюю разметку документа (стандарта Office Open

XML). Только после завершения сборки промежуточный узел маршрутизирует полностью готовое письмо на реальный почтовый шлюз для доставки адресатам.

В ходе активной фазы кампании подсистема журналирования и аналитики непрерывно фиксирует этапы взаимодействия пользователя с полученным сообщением, сохраняя каждое событие в централизованном журнале аудита. Регистрация факта открытия письма происходит при загрузке почтовым клиентом скрытого графического маркера, интегрированного в тело сообщения. Факт взаимодействия с вложением фиксируется в момент, когда текстовый редактор пользователя инициирует обращение к серверу платформы для загрузки внешнего элемента, программно внедренного в документ. При переходе по ссылке в письме система регистрирует обращение к поддельному веб-ресурсу. Для защиты от систем автоматического анализа применяются технологии генерации запутанных сетевых адресов. В случае ввода учетных данных на поддельной странице информация безопасно перехватывается с помощью обратного прокси-сервера, алгоритмы которого настроены на асинхронную потоковую передачу для предотвращения перегрузки вычислительных мощностей.

Вся собираемая статистика и записи системного журнала обрабатываются в режиме реального времени и агрегируются в виде графиков и сводных таблиц на рабочем столе администратора платформы (рисунок 3). Полученные метрики объективно отражают последовательность действий каждого тестируемого субъекта на всех этапах инцидента, предоставляя профильным подразделениям обоснованную базу для принятия решений о необходимости корректирующего обучения.

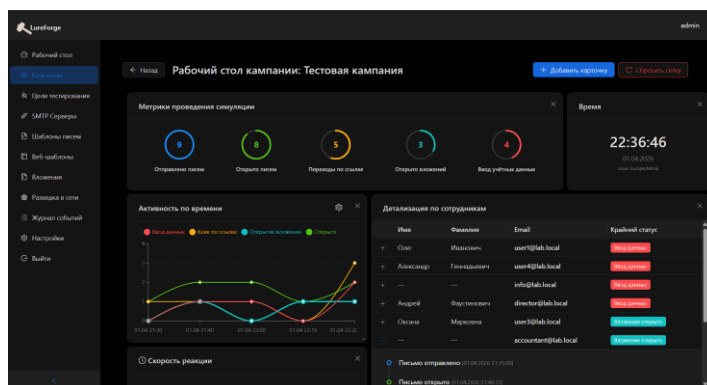


Рисунок 3 – Внешний вид рабочего стола в процессе симуляции

Проведенный анализ доказывает неэффективность теоретического обучения на фоне усложнения атак методами социальной инженерии. Предложенная платформа решает эту проблему, переводя подготовку персонала в практическую плоскость и автоматизируя аудит безопасности. Дальнейшее развитие комплекса направлено на интеграцию генеративного искусственного интеллекта с целью автоматического конструирования писем и веб-ресурсов. Дополнительно будет внедрена система «моментальной обратной связи» для проведения персонального инструктажа непосредственно в момент совершения ошибки, а также расширен спектр отслеживаемых вложений (PDF-документы, электронные таблицы, архивы) для тестирования устойчивости сотрудников к комплексным векторам компрометации.

Список использованных источников:

1. Фишинг в 2025 году стал основной угрозой для корпоративной почты [Электронный ресурс] // SecPost : аналитический портал. – Режим доступа: <https://secpost.ru/fishing-v-2025-godu-stal-osnovnoj-ugrozoy-dlya-korporativnoj-pochty>. – Дата доступа: 29.03.2026.
2. Фишинг в России [Электронный ресурс] // TAdviser : портал выбора технологий и поставщиков. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Фишинг_в_России. – Дата доступа: 01.04.2026.
3. Phishing Activity Trends Reports (Q4 2025) [Electronic resource] // Anti-Phishing Working Group (APWG). – Режим доступа: https://docs.apwg.org/reports/apwg_trends_report_q4_2025.pdf. – Дата доступа: 29.03.2026.
4. Kaspersky spam and phishing report for 2025 [Electronic resource] // Securelist by Kaspersky. – Режим доступа: <https://securelist.com/spam-and-phishing-report-2025/118785/>. – Дата доступа: 29.03.2026.
5. IEEE Symposium on Security and Privacy 2025: Controlled study at UC San Diego Health [Electronic resource] // Scribd. – Режим доступа: <https://www.scribd.com/document/908754843/ieee-25>. – Дата доступа: 29.03.2026.
6. Phishing By Industry Benchmarking Report 2025 [Electronic resource] // KnowBe4. – Режим доступа: <https://www.knowbe4.com/resources/reports/phishing-by-industry-benchmarking-report>. – Дата доступа: 29.03.2026.
7. Архитектура платформы автоматизации аудита информационной безопасности / Е.А. Биюмен, К.Ц. Маршалова // Технические средства защиты информации: матер. XXIV Междунар. науч.-техн. конф., 2026. – С. 199–202.

МЕТОД ОБНАРУЖЕНИЯ СИНТЕЗИРОВАННЫХ ВИДЕО БЕЗ СПЕЦИАЛЬНОГО ОБОРУДОВАНИЯ

Богушевич О.А., студент гр.361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Саванович С.Э. – старший преподаватель каф. ЗИ

Аннотация. В работе представлена двухуровневая методика верификации аудиовизуального контента, не требующая дорогостоящего оборудования. Первый уровень включает визуальный анализ (моргание, блики в глазах, границы лица и тени). Второй уровень – проверка аудиовизуальной синхронизации в замедленном режиме. Приведены критерии выявления синтезированных видео, порядок документирования результатов и варианты решений. Методика применима при внутренних расследованиях и проверке видеозвонков с финансовыми распоряжениями. Подчеркивается, что дистанционная проверка не заменяет личного контакта для критически важных решений.

Ключевые слова. видеозапись, синтезированное видео, верификация контента, визуальный анализ, аудиовизуальная синхронизация, моргание, блики в глазах, границы лица, тени, замедленный режим, подделка, защита информации, мошеннические атаки, расследования, двухуровневая методика.

В последние годы технологии синтеза мультимедиа стали настолько качественными, что подделку трудно отличить от оригинала. Это создаёт серьёзные риски для защиты информации. Если раньше данные чаще всего похищали с помощью вирусов или взлома, то теперь злоумышленник может создать синтезированную видеозапись или аудиозапись и тем самым нарушить доверие к доказательствам или обмануть сотрудников компании.

В данной статье предлагается двухуровневая методика верификации аудиовизуального контента на основе двух уровней анализа: визуального и аудиовизуальной синхронизации. Эти методы доступны без дорогостоящего оборудования и могут быть интегрированы в типовые процедуры защиты информации в организациях и при расследованиях.

На сегодняшний день зафиксированы случаи, когда мошенники использовали синтезированное видео для имитации руководителя компании в видеозвонке, что приводило к несанкционированным финансовым переводам. Кроме того, поддельные аудио- и видеозаписи начинают появляться в судебной практике, создавая проблему «ложного алиби»: злоумышленник может объявить подлинную улику сфабрикованной, вызвав сомнение в достоверности доказательств. Традиционные средства защиты информации – антивирусы, контроль доступа, шифрование – бессильны против такого рода угроз, поскольку они работают с формой файла, а не с его содержанием. Поэтому актуальной становится задача разработки доступных методов верификации видеоконтента, не требующих дорогостоящего оборудования.

Перед началом проверки необходимо открыть видео в плеере и подготовить лист для фиксации временных меток. Сначала выполняется беглый просмотр всего видео в обычном темпе, в ходе которого отмечаются любые фрагменты, вызывающие ощущение неестественности: странные движения губ, подозрительные блики или рывки изображения.

Затем проводится детальная проверка трёх визуальных признаков. Первый – моргание. Нормой считается 10–30 морганий в минуту. Если моргание отсутствует дольше десяти секунд подряд или движения век выглядят слишком быстрыми, это подозрительный признак. Второй признак – блики в глазах. В подлинной записи блики симметричны и синхронно смещаются при повороте головы [1]. Если блики одинаковы в обоих глазах, не меняются или появляются асимметрично, это указывает на синтез. Третий признак – границы лица и тени. Размытие, ореолы на стыке лица и фона, неестественно гладкая «пластиковая» кожа или отсутствие теней также являются подозрительными. При выявлении хотя бы одного явного артефакта проверка прекращается, и проверяющий приступает к документированию нарушений.

Выбор именно этих признаков не случаен. Моргание – сложный для синтеза биомеханический процесс; современные нейросети часто либо «забывают» его вовсе, либо генерируют с неестественной частотой. Блики в глазах зависят от физики отражения света и геометрии сцены – их правдоподобная имитация требует точного моделирования источников освещения, что на практике встречается редко. Артефакты на границах лица возникают из-за несовершенства алгоритмов сведения синтезированного лица с исходным фоном.

Следует учитывать, что эффективность визуального уровня анализа зависит от качества видеозаписи. При низком разрешении, сильной зернистости или высоком сжатии такие признаки, как блики в глазах и границы лица, могут быть плохо различимы. В этих условиях основная диагностическая нагрузка перекладывается на уровень аудиовизуальной синхронизации, который сохраняет работоспособность даже на посредственных записях. Если же качество видео не позволяет надёжно различить даже движение губ, запись признаётся неverified без применения инструментальных методов.

Если визуальный анализ не выявил нарушений, выполняется проверка аудиовизуальной синхронизации. Выбирается фрагмент речи длительностью 5–10 секунд, видео переводится в замедленный режим (0,5x). Проверяющий оценивает совпадение открытия рта с началом звука на гласных, наличие микродвижений губ перед согласными «б», «п», «м» (в естественной речи они есть, в синтезированной – часто отсутствуют), а также естественность звучания. Любое несоответствие фиксируется как признак подделки.

Затем результаты документируются: в протоколе указываются дата, название файла, временные метки артефактов, скриншоты и итоговое заключение. На основании этого принимается одно из трёх решений: видео признаётся достоверным; подозрительным (исключается из использования); либо при неоднозначных признаках направляется на дополнительную экспертизу.

Для наглядности рассмотрим типовой сценарий. Сотрудник компании получает видеосообщение от лица, которое представляется руководителем, с указанием срочно перевести деньги на указанный счёт. Прежде чем выполнять распоряжение, сотрудник открывает видео в плеере и последовательно применяет описанный алгоритм. Он замечает, что руководитель ни разу не моргнул за 15 секунд разговора, а блики в глазах остаются неподвижными при повороте головы. Этого достаточно, чтобы признать видео подозрительным и не выполнять финансовую операцию до дополнительной проверки по другому каналу связи (например, личному звонку). Таким образом, алгоритм выступает в роли оперативного фильтра, предотвращающего мошеннические действия.

Другой типичный сценарий связан с внутренним расследованием. В компанию поступает видеозапись, предположительно фиксирующая нарушение сотрудником правил безопасности. Запись вызывает сомнения у службы безопасности, так как сотрудник отрицает свою причастность и заявляет, что видео является подделкой. Специалист запускает алгоритм проверки: при замедленном воспроизведении он обнаруживает, что движение губ на ключевых фразах не совпадает со звуковой дорожкой, а на границах лица заметно мерцание пикселей. Видео признаётся синтезированным и исключается из числа доказательств.

Предложенный ручной алгоритм не конкурирует с автоматизированными системами, а дополняет их. Программные решения на основе нейросетей способны анализировать видео быстрее и глубже, но требуют установки специализированного ПО, вычислительных ресурсов и квалификации для интерпретации результатов. Ручной метод, напротив, доступен любому сотруднику с минимальной подготовкой, не требует затрат и даёт результат здесь и сейчас. Оптимальной стратегией представляется комбинированный подход: ручная проверка используется для оперативного отсева очевидных подделок, а подозрительные или особо важные видео направляются на автоматизированный анализ.

Также, предложенный алгоритм решает три практические задачи в области защиты информации. Он позволяет выявлять синтезированные видео при проведении внутренних расследований. Также, данный алгоритм может быть использован для проверки видеозвонков, содержащих финансовые распоряжения, что напрямую противостоит мошенническим атакам. Кроме того, документальная фиксация результатов проверки лишает злоумышленника возможности поставить под сомнение подлинность записи – процедура проведена по формализованному алгоритму, и её результаты можно перепроверить.

Важно подчеркнуть, что ни один алгоритм дистанционной проверки не даёт абсолютной гарантии. В ситуациях, связанных с принятием критически важных решений (финансовые переводы, передача конфиденциальных данных, изменение доступа), единственным надёжным способом подтверждения личности остаётся личная встреча или многофакторная аутентификация по независимому каналу связи.

При этом важно понимать границы применимости предложенного метода. Алгоритм не даёт стопроцентной гарантии: высококачественные синтезированные видео, созданные с использованием современных нейросетей и достаточных вычислительных ресурсов, могут не содержать видимых артефактов. Кроме того, как уже отмечалось, метод чувствителен к качеству исходной записи. Поэтому его основное назначение – оперативная фильтрация заведомо поддельных материалов и выявление грубых синтезов, тогда как для окончательного заключения в спорных случаях требуется экспертиза с привлечением специализированного программного обеспечения.

Перспективным направлением дальнейших исследований является частичная автоматизация описанного алгоритма. Это позволит снизить субъективность проверки и ускорить обработку большого объёма видеоматериалов, сохранив при этом доступность метода для организаций с ограниченным бюджетом.

Список использованных источников:

1. Айтрекинг против дипфейков [Электронный ресурс] – 2026. Режим доступа: <https://www.itsec.ru/articles/ajtreking-protiv-dipfejkov>

ИНТЕГРАЦИЯ ОБЛАЧНОГО СЕРВИСА CLOUDFLARE КАК ЭЛЕМЕНТА ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТ DDoS-АТАК

Бодров Д.А., магистрант гр. 567001

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

*Бойправ О.В. – канд. тех. наук, доцент,
заведующий кафедрой защиты информации*

Аннотация. В статье рассматриваются организационно-технические аспекты интеграции облачного сервиса Cloudflare в систему защиты информационной системы от DDoS-атак. На основе анализа учебной и научной литературы раскрыта сущность распределенных атак отказа в обслуживании, охарактеризованы их разновидности и последствия для доступности цифровых ресурсов. Обоснована необходимость многоуровневой защиты, сочетающей локальные и облачные средства фильтрации трафика. Показаны основные направления интеграции Cloudflare, включая изменение DNS-маршрутизации, использование HTTPS, применение защитных правил и режимов усиленной проверки трафика. Сделан вывод о целесообразности использования Cloudflare как внешнего уровня защиты информационной системы, дополняющего традиционные средства обеспечения информационной безопасности.

Ключевые слова. Информационная система, DDoS-атака, Cloudflare, информационная безопасность, облачная защита, фильтрация трафика, HTTPS, DNS.

В современных условиях развития цифровой среды устойчивое функционирование информационных систем становится одной из предпосылок надежной работы организаций, предприятий, учреждений и различных сетевых сервисов. Информационные системы представляют собой совокупность средств, методов и персонала, обеспечивающих хранение, обработку, передачу и предоставление данных, поддерживают взаимодействие пользователей, функционирование веб-приложений, доступ к корпоративным ресурсам и выполнение повседневных управленческих, производственных и сервисных процессов [1]. По мере роста числа цифровых услуг и усиления зависимости организаций от сетевой инфраструктуры проблема обеспечения доступности ресурсов приобретает особую значимость. Нарушение стабильности работы информационной системы даже на короткий промежуток времени способно вызвать организационные сбои, финансовые потери, снижение качества обслуживания и ухудшение репутации владельца ресурса [2, с. 215].

Одной из наиболее опасных угроз доступности информационных систем остаются DDoS-атаки. Согласно определению А.А. Головина, DDoS-атака (распределенная атака отказа в обслуживании) представляет собой целенаправленное воздействие на информационную систему, осуществляемое с большого количества распределенных источников, с целью исчерпания ее вычислительных или сетевых ресурсов и, как следствие, нарушения доступности предоставляемых сервисов для легитимных пользователей [3, с. 128]. В отличие от обычной атаки отказа в обслуживании, распределенный характер DDoS-воздействия усложняет его отражение, вредоносный поток поступает сразу из множества источников и может имитировать обычную пользовательскую активность [3, 4].

Сложность защиты от DDoS-атак связана также с тем, что они могут реализовываться на различных уровнях эталонной модели взаимодействия открытых систем (OSI). На сетевом и транспортном уровнях широко распространены flood-атаки, основанные на генерации большого количества ICMP-, UDP- или SYN-запросов. Их цель состоит в перегрузке пропускной способности канала связи, сетевых буферов, таблиц соединений либо других инфраструктурных механизмов обработки трафика. На прикладном уровне атака может принимать форму многократных HTTP- или HTTPS-запросов, внешне похожих на обращения обычных пользователей. Как подчеркнул С.И. Макаренко, такие атаки являются особенно опасными, поскольку они затрудняют четкое разграничение между вредоносной и легитимной активностью и могут оставаться незамеченными на протяжении длительного времени [4, с. 87]. Дополнительные сложности возникают при использовании шифрованного трафика, так как он увеличивает нагрузку на серверные ресурсы и одновременно усложняет глубинный анализ содержимого запросов.

Последствия DDoS-атак для информационной системы имеют многоплановый характер. А.Б. Грушо и Е.А. Линева выделяют три основных уровня проявления последствий: технический, организационный и экономический [5, с. 156]. На техническом уровне они проявляются в снижении производительности серверов, отказе веб-приложений, перегрузке сетевого оборудования и нарушении доступа к цифровым сервисам. На организационном уровне атака может привести к дестабилизации внутренних процессов, невозможности выполнения пользователями своих функций, нарушению обмена данными между подразделениями и временной остановке критически значимых сервисов. На экономическом уровне последствия выражаются в прямых потерях, связанных с простоем, необходимостью восстановления работоспособности, привлечением дополнительных ресурсов и усилением защитной инфраструктуры.

Кроме того, для систем, ориентированных на обслуживание клиентов, важную роль играют репутационные риски.

Традиционная система защиты информационной инфраструктуры, подробно описанная в учебных изданиях, предполагает использование набора локальных средств безопасности, размещенных внутри собственного контура организации [5, 6]. К ним относятся межсетевые экраны, средства контроля доступа, системы обнаружения и предотвращения вторжений (IDS/IPS), балансировщики нагрузки, механизмы сегментации сети и организационные меры реагирования на инциденты. Межсетевые экраны позволяют контролировать входящий и исходящий трафик и применять к нему правила фильтрации, основанные на адресах, портах, типах соединений и других параметрах. IDS и IPS предназначены для выявления аномального поведения, фиксации признаков известных атак и автоматического блокирования подозрительного трафика [6, с. 302]. Дополнительно могут применяться ограничения частоты запросов, резервирование серверных ресурсов, распределение нагрузки и аудит защищенности. Однако возможностей локальной инфраструктуры оказывается недостаточно при отражении массированных распределенных атак. Причина состоит в том, что вредоносный трафик уже достигает защищаемой системы и начинает потреблять ее собственные сетевые и вычислительные ресурсы [4, с. 112]. Даже если часть запросов впоследствии будет отфильтрована, сама необходимость их приема, анализа и обработки может привести к дополнительной нагрузке на серверы и оборудование.

В современных концепциях информационной безопасности все большее значение приобретает использование внешних распределенных платформ фильтрации трафика, которые способны анализировать и отсекают значительную долю вредоносного потока до его поступления к целевой информационной системе. Одним из наиболее известных решений такого типа, является облачный сервис Cloudflare. Его применение позволяет организовать внешний уровень защиты, расположенный между пользователем и исходным сервером. В общем виде принцип работы заключается в том, что запросы к защищаемому ресурсу перенаправляются через распределенную сеть узлов Cloudflare, где осуществляется их маршрутизация, анализ, проверка и фильтрация. После этого только очищенный или допустимый трафик передается на исходный сервер [7]. За счет подобной архитектуры уменьшается нагрузка на локальную инфраструктуру, снижается вероятность ее перегрузки и повышается доступность ресурса для легитимных пользователей.

Интеграция Cloudflare в информационную систему может рассматриваться как одно из направлений реализации принципа многоуровневой (эшелонированной) защиты, который является основополагающим в современной теории информационной безопасности. Данный принцип предполагает создание нескольких последовательных рубежей обороны, что позволяет затруднить преодоление защиты злоумышленником и повысить общую устойчивость системы [3, с. 95]. Такой подход не отменяет использование локальных средств безопасности, а дополняет их внешним облачным уровнем фильтрации и востребован прежде всего в ситуациях, когда информационная система предполагает публичную доступность веб-ресурсов, взаимодействие с удаленными пользователями либо подвержена существенным и трудно-прогнозируемым колебаниям сетевой нагрузки.

Интеграция Cloudflare начинается с изменения логики сетевого взаимодействия. Основное действие состоит в перенастройке DNS-записей домена таким образом, чтобы запросы направлялись не на исходный сервер организации, а в инфраструктуру Cloudflare. Тем самым формируется промежуточный узел обработки трафика, который принимает на себя значительную часть защитных функций. Фильтрация начинает выполняться до того, как пакеты достигают локальной сети. Без этого этапа применение большинства анти-DDoS-механизмов Cloudflare становится невозможным, а последующая настройка защиты теряет смысл. Следующий этап заключается в построении защищенного канала связи. Для современных информационных систем использование HTTPS и корректная настройка SSL/TLS являются базовым требованием. Криптографическая защита каналов связи остается одним из основных средств обеспечения конфиденциальности и целостности данных при передаче по открытым сетям [5, с. 210]. При интеграции Cloudflare задача организации защищенного соединения усложняется, поскольку шифрование должно быть корректно настроено одновременно на двух участках сетевого взаимодействия, между пользователем и облачным сервисом, а также между Cloudflare и исходным сервером. Данная схема может обеспечить безопасную передачу данных, сохранив при этом возможности фильтрации трафика, кэширования и контроля сетевой активности.

Cloudflare позволяет ограничивать частоту запросов, применять сетевую и поведенческую фильтрацию, различать типы трафика и выявлять признаки аномальной активности. Эти механизмы особенно значимы в тех случаях, когда вредоносные обращения внешне не отличаются от обычных пользовательских запросов. На прикладном уровне атаки нередко направляются на наиболее уязвимые и ресурсоемкие элементы веб-приложения, формы аутентификации, API-интерфейсы, динамически формируемые страницы, поисковые модули. В подобных условиях стандартной фильтрации по IP-адресам и портам недостаточно, поскольку для эффективного противодействия требуется учитывать характер и модель поведения входящих запросов.

Особое место занимает режим усиленной проверки трафика Under Attack mode. Его применение позволяет ввести дополнительный этап проверки обращений к ресурсу и тем самым затруднить доступ автоматизированных скриптов и иных источников подозрительной активности. Для пользователей доступ

к ресурсу сохраняется, однако осуществляется через промежуточную процедуру подтверждения. Наиболее оправдано использование данного режима в ситуациях, когда обычных правил фильтрации уже недостаточно для поддержания стабильной работы веб-приложения, прежде всего при атаках прикладного уровня, ориентированных на перегрузку сервера потоком формально корректных запросов.

Сервис Cloudflare используется также для защиты DNS-инфраструктуры, ускорения доставки контента, перераспределения нагрузки в периоды ее резкого роста, функционирования межсетевого экрана веб-приложений и общей оптимизации сетевого взаимодействия. Благодаря этому Cloudflare целесообразно рассматривать не как отдельный инструмент защиты, а как один из элементов архитектуры, обеспечивающей доступность, устойчивость и отказоустойчивость информационной системы. Для организаций это означает, что выбор решения должен учитывать не только угрозу атак, но и повседневные требования к стабильности цифровых сервисов.

Внутренние межсетевые экраны, IDS и IPS, безопасная конфигурация серверов, актуализация программного обеспечения, контроль уязвимостей, резервирование ресурсов и разработка регламентов реагирования сохраняют свое фундаментальное значение [3, 5]. Облачная фильтрация трафика в таком случае выступает как внешний рубеж защиты, который уменьшает объем вредоносного потока и повышает устойчивость системы, но не отменяет необходимости поддержания внутренней безопасности на должном уровне.

Особое значение многоуровневого подхода проявляется в том, что разные механизмы защиты решают различные задачи. Локальные средства позволяют контролировать внутреннюю инфраструктуру, разграничивать доступ, фиксировать инциденты и реагировать на угрозы в пределах собственного контура. Облачный сервис, напротив, наиболее эффективен на этапе предварительной фильтрации и распределения нагрузки. Сочетание данных уровней позволяет добиться заметного эффекта при отражении сложных распределенных атак [6, с. 345]. Cloudflare не подменяет традиционные средства защиты, а дополняет их, усиливая внешний уровень противодействия сетевым угрозам. Его применение оправдано в тех случаях, когда собственных ресурсов информационной системы недостаточно для устойчивого отражения интенсивного потока вредоносного трафика.

Интеграция Cloudflare в защитный контур информационной системы позволяет повысить ее устойчивость за счет переноса части защитных функций во внешнюю распределенную инфраструктуру. При такой организации снижается зависимость доступности ресурса от состояния одного канала связи или производительности отдельного сервера. Даже при значительной нагрузке часть вредоносного трафика задерживается еще до поступления на защищаемый ресурс, что создает более благоприятные условия для сохранения его работоспособности. Для систем, функционирующих в открытой сети, обслуживающих большое количество пользователей и ориентированных на постоянную доступность, это имеет важное значение.

Таким образом, высокая опасность DDoS-атак определяется тем, что их объектом выступает именно доступность информационного ресурса. Вследствие этого последствия подобных воздействий выходят за пределы технических нарушений и затрагивают организационную деятельность, стабильность предоставления сервисов и экономические показатели. Базовые локальные средства защиты формируют необходимую основу безопасности, однако при массированных распределенных атаках их возможности оказываются ограниченными. Это связано с тем, что вредоносный трафик уже достигает инфраструктуры организации, а его обработка и последующая фильтрация сами по себе создают дополнительную нагрузку на оборудование и каналы связи.

Использование Cloudflare позволяет вынести первичную фильтрацию на внешний уровень. За счет этого значительная часть подозрительного и вредоносного трафика анализируется и блокируется до его поступления к серверной инфраструктуре. В результате уменьшается нагрузка на вычислительные ресурсы и сетевые каналы, а сама информационная система получает более высокий запас устойчивости в условиях атаки. Наиболее эффективным такой подход является в составе многоуровневой защиты, где облачная фильтрация сочетается с внутренними средствами сетевой и прикладной безопасности, корректной настройкой инфраструктуры и заранее определенными процедурами реагирования на инциденты. Именно такое сочетание мер в наибольшей степени соответствует современным требованиям к защите информационных систем от DDoS-атак.

Список использованных источников:

1. Информационные системы и технологии : учебник / под ред. В.В. Трофимова. – М. : Юрайт, 2021. – 549 с.
2. Баранова, Е.К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова. – М. : РИОР, 2020. – 256 с.
3. Головин, А.А. Информационная безопасность : учебное пособие / А.А. Головин. – М. : Форум, 2020. – 352 с.
4. Макаренко, С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями : монография / С.И. Макаренко. – СПб. : Наукоемкие технологии, 2018. – 122 с.
5. Грушо, А.Б. Защита информации в компьютерных системах и сетях / А.Б. Грушо, Е.А. Линева. – М. : Горячая линия – Телеком, 2018. – 342 с.
6. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М. : ДМК Пресс, 2019. – 592 с.

ИССЛЕДОВАНИЕ АМПЛИТУДНО-ИМПУЛЬСНОЙ И ШИРОТНО-ИМПУЛЬСНОЙ МОДУЛЯЦИИ В КОНТЕКСТЕ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

Боровиков К.А., студент гр. 461401

Белорусский государственный университет информатики и радиоэлектроники г. Минск,
Республика Беларусь

Фильченкова Т.М. – старший преподаватель каф. ЗИ

Аннотация. В работе рассматривается потенциал использования амплитудно-импульсной и широтно-импульсной модуляции в качестве методов для передачи данных. Особое внимание уделяется процессу компьютерного моделирования сигналов, модифицированных для включения скрытых сообщений. Проводится анализ устойчивости полученных сигналов к несанкционированному перехвату и оценка эффективности защиты передаваемой информации.

Ключевые слова. Стеганография; сигнал; Python; модуляция; демодуляция; амплитудно-импульсная модуляция; широтно-импульсная модуляция; псевдослучайная перестановка; импульс; скрытый канал связи.

С развитием инфокоммуникационных технологий задача защиты передаваемых данных становится всё более актуальной. Наряду с традиционной криптографией, методы стеганографии позволяют скрыть сам факт передачи информации. В качестве контейнеров для скрытого канала связи были выбраны амплитудно-импульсная (АИМ) и широтно-импульсная модуляции (ШИМ).

Импульсные виды модуляции основаны на дискретизации непрерывного сигнала во времени. В качестве переносчика используется периодическая последовательность прямоугольных импульсов.

При АИМ амплитуда каждого импульса несущей последовательности изменяется пропорционально мгновенному значению модулирующего (информационного) сигнала. Известны два вида амплитудно-импульсной модуляции: АИМ-1 и АИМ-2. В первом случае вершина импульса следует за изменениями модулирующего напряжения, а во втором - вершина импульса сохраняется плоской [1].

Для описания дискретизации во времени используем так называемую импульсную функцию дискретизации a_d , которая представляет собой периодическую последовательность δ -функций, следующих друг за другом через интервалы времени Δt . Математическую модель дискретизации сигнала $S(t)$ во временной области можно представить как результат умножения этого сигнала на функцию a_d .

В реальных условиях реализовать импульсную функцию дискретизации на основе δ -импульсов невозможно, поэтому при взятии отсчетов обычно используется периодическая последовательность коротких прямоугольных импульсов с длительностью τ , которые удовлетворяют условию $\tau/\Delta t \ll 1$. В результате получим амплитудно-модулированную последовательность импульсов, т.е. АИМ-сигнал. Для иллюстрации сигналов был использован язык программирования Python с использованием библиотек `numpy` и `matplotlib` [2, 3]. Пример графиков АИМ-1 и АИМ-2 сигналов представлен на рисунке 1.

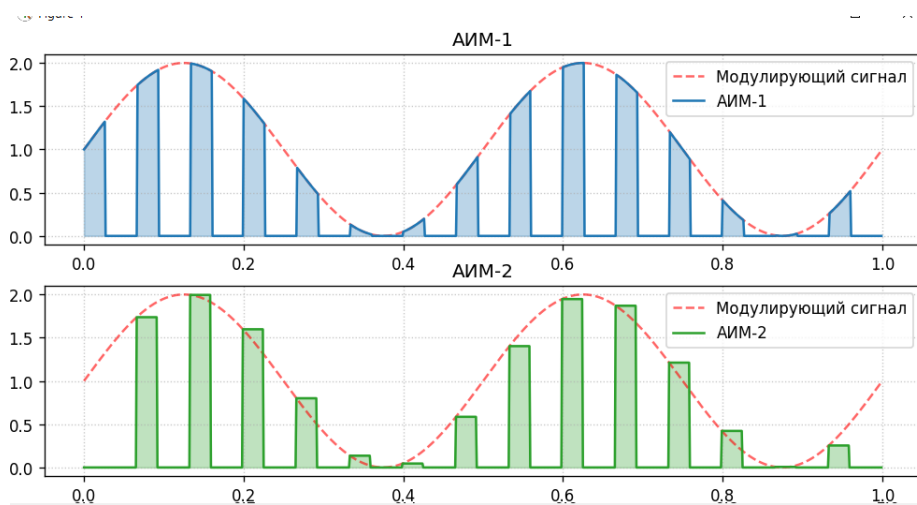


Рисунок 1 – Графики АИМ-1 и АИМ-2 сигналов

ШИМ называется такой вид модуляции, при котором информационным параметром является длительность импульсов. Различают одностороннюю ШИМ, при которой изменение длительности посылки происходит за счет перемещения одного из фронтов импульсов, и двухстороннюю ШИМ, при

которой длительность посылки изменяется в результате одновременного перемещения обоих фронтов импульсов. Для практической реализации более удобной является односторонняя широтно-импульсная модуляция [1].

По аналогии с видами амплитудно-импульсной модуляции существует два вида широтно-импульсной модуляции: ШИМ-1 и ШИМ-2. Примеры ШИМ-1 и ШИМ-2 сигналов представлены на рисунке 2, из которого видно, что для получения импульсной последовательности, модулированной по длительности, необходимо сравнить непрерывный сигнал с периодической последовательностью пилообразных импульсов. При этом начало «зубца пилы» соответствует переднему фронту импульса ШИМ, а задний фронт импульса формируется по точкам пересечения А и В, которые соответствуют равенству мгновенных значений сигналов.

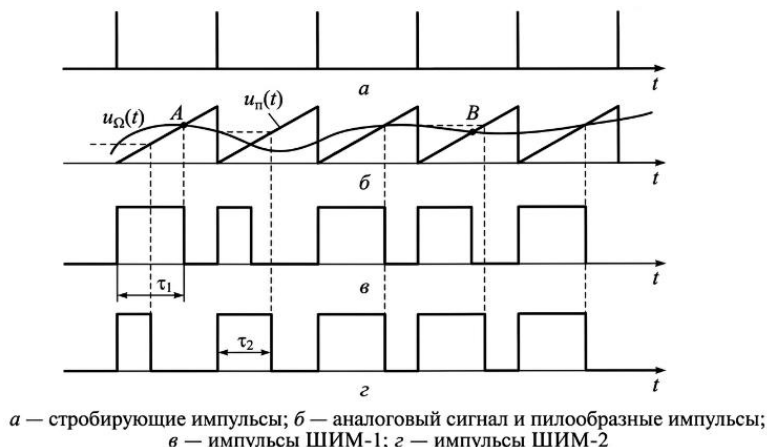


Рисунок 2 – Представление ШИМ-1 и ШИМ-2 сигналов

Для сокрытия информации в АИМ-сигналах можно, например, использовать комбинацию из генератора псевдослучайных перестановок (ГПП) и изменения длительности импульса. Для этого обе стороны должны заранее договориться об общем seed-ключе и генераторе псевдослучайных чисел. Далее, согласно алгоритму тасования Фишера-Йетса, можно получить список псевдослучайных перестановок a , где значение элемента $a[i]$ будет соответствовать номеру передаваемого импульса, который содержит i -й информационный бит. Для кодирования единицы будем отправлять соответствующий импульс с небольшим запозданием, для нуля – не будем вносить никаких изменений. Необходимо также выполнить синхронизацию по тактовой частоте, чтобы приемник мог однозначно идентифицировать внесенную задержку на фоне стандартного интервала следования импульсов. Обеспечить тактовую синхронизацию можно, например, при помощи отправки преамбулы с известной последовательностью импульсов, которая не несет информации, но позволит приемнику согласовать процесс регистрации импульсов. Для генерации псевдослучайных чисел была использована библиотека random языка Python [4]. Пример реализации подобного метода сокрытия данных представлен на рисунке 3.

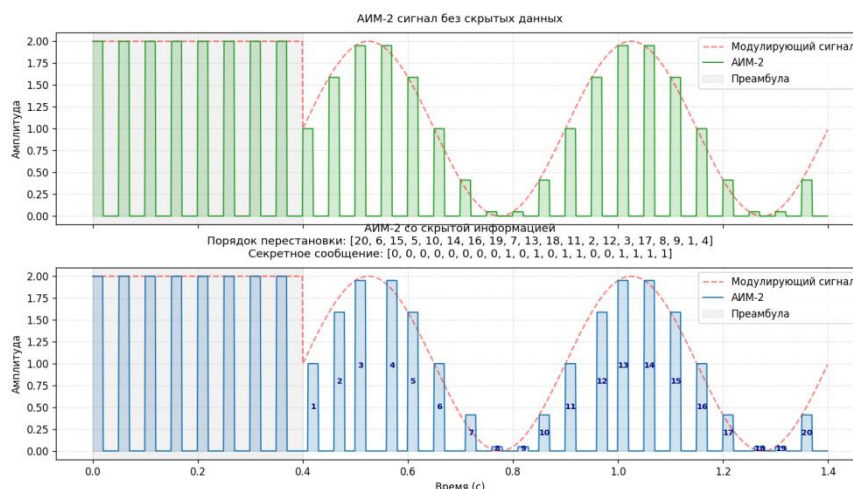


Рисунок 3 – Результат сокрытия данных в АИМ-2 сигнале

Аналогично предыдущему методу, но для ШИМ-1, можно использовать комбинацию из ГПП и изменений амплитуды передаваемых импульсов, т.к. при обычной передаче их уровень должен оставаться постоянным. Для сокрытия единицы будем незначительно увеличивать амплитуду

соответствующего импульса, для нуля – не будем вносить никаких изменений. Пример реализации подобного метода приведен на рисунке 4.

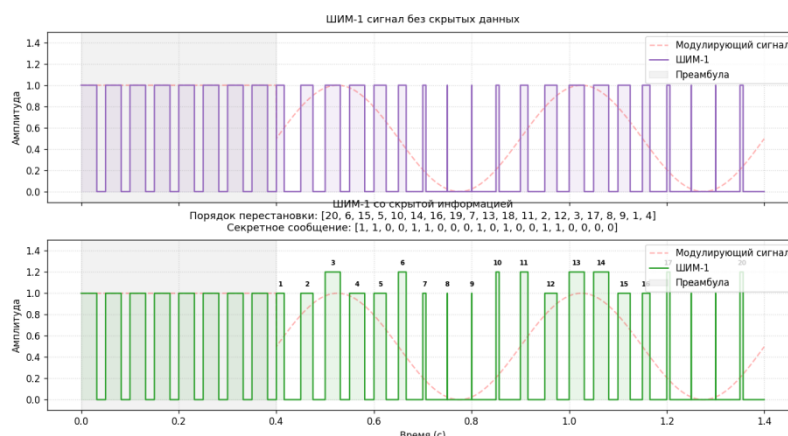


Рисунок 4 – Результат скрытия данных в ШИМ-1 сигнале

Предложенный метод скрытой передачи данных уязвим к перехвату из-за фиксированной преамбулы, позволяющей легко определить частоту сигнала. Он также чувствителен к соотношению сигнал/шум: малые колебания амплитуды могут быть неотличимы от шума, а сильные всплески – легко обнаружены. Ещё один недостаток – необходимость предварительного согласования общего ключа.

Однако у метода есть важные преимущества. Тасование Фишера-Йетса распределяет биты псевдослучайно, делая сообщение недоступным без ключа [5]. Для повышения помехоустойчивости можно внедрить избыточное кодирование, а для маскировки самого факта передачи – распределить скрытые биты по значительно большему числу импульсов (например, 10 бит на 100 импульсов).

Достаточно популярным методом сокрытия информации является метод расширения спектра, который основан на распределении энергии секретного сообщения по широкой полосе частот сигнала-контейнера [6, 7]. В процессе внедрения каждый бит сообщения преобразуется в биполярную форму и умножается на псевдослучайную последовательность, генерируемую на основе секретного ключа. Полученный широкополосный сигнал умножается на малый коэффициент и добавляется к сигналу-контейнеру. Таким образом, энергия одного бита распределяется по множеству отсчётов или частотных компонент. Такой способ имеет высокую устойчивость к шуму и низкую вероятность обнаружения, однако усложняет реализацию и ограничивает пропускную способность скрытого канала связи.

Таким образом, использование АИМ и ШИМ позволяет реализовать внедрение скрытого сообщения в передаваемые сигналы без существенного нарушения их основных параметров. В настоящее время существует множество методов стеганографии для сигналов, выбор которых определяется условиями передачи, требованиями к скрытности, устойчивости к помехам и допустимой пропускной способностью скрытого канала. При выборе оптимального метода сокрытия информации необходимо учитывать характеристики сигнала-контейнера, свойства канала передачи, допустимый уровень искажений, а также требования к надёжности извлечения сообщения.

Список использованных источников:

1. Биккенин, Р. Р. Теория электрической связи : учеб. пособие для студ. учреждений высш. образования / Р. Р. Биккенин, М. Н. Чесноков. – М. : Издат. центр «Академия», 2010. – 336 с.
2. NumPy documentation [Электронный ресурс]. – Режим доступа: <https://numpy.org/doc/>. – Дата доступа: 01.03.2026.
3. Matplotlib [Электронный ресурс]. – Режим доступа: <https://matplotlib.org/stable/users/index>. – Дата доступа: 01.03.2026.
4. Random – generate pseudo-random numbers [Электронный ресурс]. – Режим доступа: <https://docs.python.org/3/library/random.html/>. – Дата доступа: 01.03.2026.
5. Метод генерации случайной перестановки, алгоритм Фишера-Йетса [Электронный ресурс]. – Режим доступа: https://neerc.ifmo.ru/wiki/index.php?title=Метод_генерации_случайной_перестановки_алгоритм_Фишера-Йетса. – Дата доступа: 01.03.2026.
6. Серкевич, Д. С. Анализ стеганографических методов / Д. С. Серкевич, Ю. О. Герман // Информационные технологии и системы 2025 (ИТС 2025) : материалы международной научной конференции, Минск, 19 ноября 2025 / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Л. Ю. Шилин [и др.]. – Минск, 2025. – С. 233–234.
7. Смирнов, А. А. Стеганографическое встраивание данных в неподвижные изображения методом прямого расширения спектра / А. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Харків : ХУПС, 2011. – № 2. – С. 126-129

СЦЕНАРИЙ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ В СЕРВИС ОНЛАЙН-РАЗАРХИВАТОРА

Максимович Р.А., Боровиков К.А., студенты гр. 461401

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Белоусова Е.С. – канд. тех. наук, доцент

Аннотация. В статье рассматривается пример реализации сценария киберинцидента, демонстрирующий процесс тестирования на проникновение в сервис онлайн-разархиватора. Процесс создания сценария киберинцидента основывался на составленном векторе кибератаки. Для прохождения сценария описаны рекомендации и подобран инструментарий, который позволит обучающимся сформировать навыки для реализации тестирования на проникновения. Таким образом, реализованный сценарий рекомендуется к изучению для обучения молодых специалистов в областях SOC-аналитики, расследования киберинцидентов и т.п.

Ключевые слова. Информационная безопасность, форензика, киберинциденты, практическая подготовка, реагирование на инциденты, тестирование на проникновение, база знаний MITRE ATT&CK, сервис онлайн-разархиватора.

Современная цифровая среда характеризуется стремительным ростом числа и сложности кибератак. В этих условиях подготовка специалистов в области информационной безопасности требует не только теоретических знаний, но и развитых практических навыков. Одним из наиболее эффективных подходов является использование сценариев киберинцидентов – моделируемых ситуаций, имитирующих реальные киберинциденты и предоставляющие возможность их расследования. Практико-ориентированное обучение позволяет студентам погружаться в реальные условия работы специалистов по безопасности, формируя у них навыки анализа, принятия решений и работы с инструментами. Наибольший интерес сегодня вызывают задачи из компьютерной криминалистики (форензики), реверс-инжиниринга и тестирования инфраструктуры на проникновение (пентест). Именно эти навыки являются ключевыми для наиболее востребованных позиций в информационной безопасности [1].

Сценарий киберинцидента представляет собой структурированную учебную задачу, в которой обучающийся выступает в роли специалиста по информационной безопасности. Сценарии должны включать: описание инцидента, набор артефактов или целевую систему, цели, критерии оценки. Использование данных составляющих сценария позволяет максимально приблизить создаваемую ситуацию к реальной жизни.

Форензика – это процесс извлечения, анализа и предоставления электронных доказательств для раскрытия киберпреступлений [2]. Специалисты по компьютерной криминалистике занимаются сбором и анализом данных с устройств и систем, которые могут быть связаны с преступными действиями. После извлечения данных проводится анализ для выявления цифровых следов и понимания, какие действия были совершены и кем.

Обратное проектирование программного обеспечения – это процесс восстановления дизайна, спецификаций требований и функций продукта на основе анализа его кода. В ходе этого процесса создается база данных программ и генерируется информация на её основе [3]. Главной целью данного процесса, который также называется реверс-инжинирингом, является исследование некоторого уже собранного продукта с целью понять его принцип работы.

Пентест (Pentest или тестирование на проникновение) – процесс тестирования системы путем попыток ее взлома для выявления уязвимостей. Специалист по безопасности после согласования сторон пытается взломать или обойти защитные меры информационной системы, чтобы найти слабые места. Существует несколько видов тестирования на проникновение: пентест внешнего и внутреннего периметра, веб-приложений, мобильных устройств и физический пентест. В ходе тестирования на проникновение специалисты используют методы, которые могут применять нарушители, чтобы проникнуть в систему. Например, анализ сетевых уязвимостей, брутфорс-атаки, эксплуатация устаревших программных компонентов и другие тактики [4]. Главной задачей пентеста является выявление уязвимостей и оценка эффективности защиты инфраструктуры.

В ходе выполнения работы была поставлена цель: разработать комплексный сценарий киберинцидента, включающий преодоление внешнего периметра и последующую внутреннюю компрометацию инфраструктуры. Объектом кибератаки выступает веб-приложение, представляющее собой сервис онлайн-разархиватора (рисунок 1).

Система была разработана на PHP и Apache с использованием Docker для контейнеризации приложений, что позволило гарантировать изоляцию сервисов от основной системы и гибкость управления окружением. Для дополнительного уровня безопасности задействована виртуальная машина с операционной системой Linux.

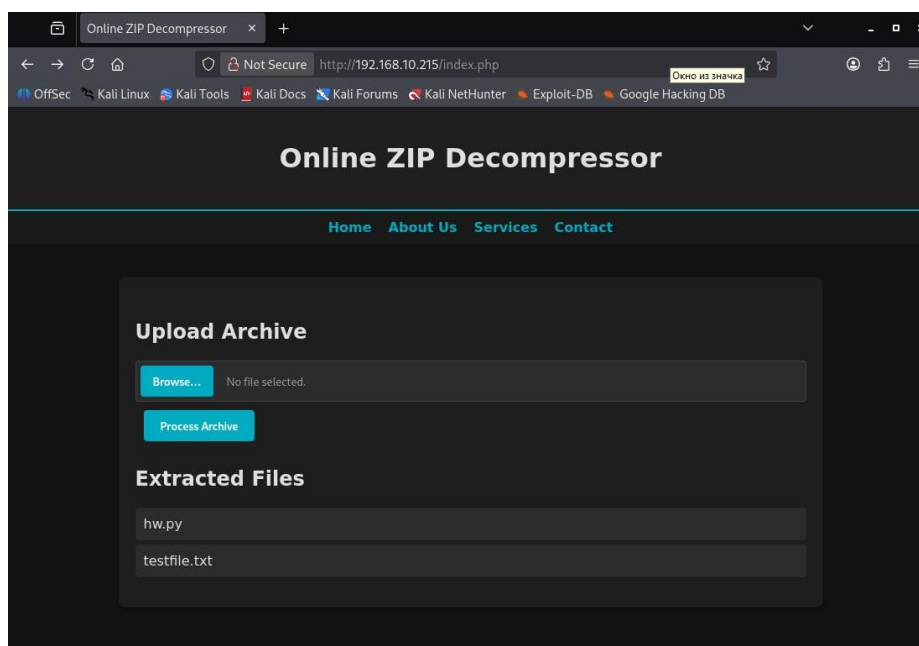


Рисунок 1 – Главная страница онлайн-разархиватора

В соответствии с общедоступной базой знаний MITRE ATT&CK был составлен вектор атаки, имитирующий последовательность действий нарушителя по компрометации целевой системы (рисунок 2) [5].

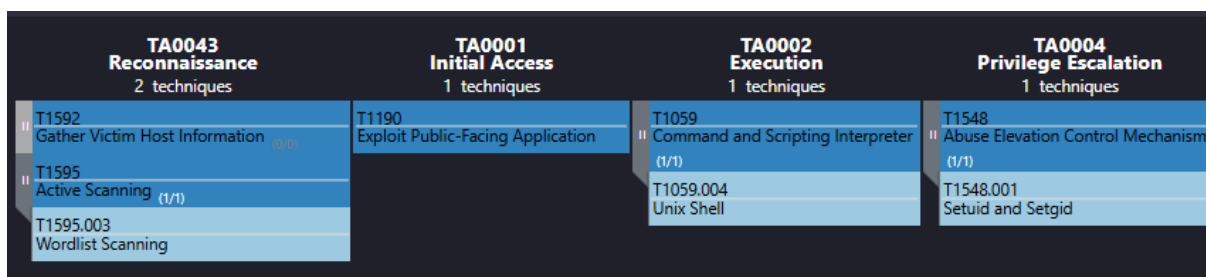


Рисунок 2 – Вектор атаки

На этапе разведки (Reconnaissance TA0043) применяется активное сканирование, в частности сканирование по словарю (Wordlist Scanning T1595.003), для обнаружения эндпоинтов веб-приложения и поиск открытых портов и информации об атакуемом узле (Active Scanning T1595, Gather Victim Host Information T1592). Первоначальный доступ (Initial Access TA0001) реализуется через эксплуатацию уязвимости целевого сервиса (Exploit Public-Facing Application T1190), который подвержен атаке типа Zip Slip (CVE-23: Relative Path Traversal). Данная уязвимость позволяет нарушителю осуществить запись файлов вне выделенной директории путем манипуляции именами файлов, содержащихся в архиве. Это приводит к этапу выполнения (Execution TA0002) путем загрузки вредоносного скрипта и использования командного интерпретатора (Unix Shell T1059.004) для получения удаленного доступа. Финальным этапом компрометации выступает повышение привилегий (Privilege Escalation TA0004) за счет злоупотребления механизмами контроля доступа, а именно – эксплуатации некорректно настроенных бинарных файлов с установленными флагами Setuid и Setgid (T1548.001).

Для успешной реализации данного сценария начинающему специалисту потребуется ряд специализированных инструментов. Для определения списка открытых портов, версий запущенных сервисов и другую информацию о хосте рекомендуется использовать инструмент nmap. Для выполнения техники Wordlist Scanning целесообразно использовать утилиты для перебора директорий, такие как ffuf или gobuster, которые позволяют быстро составить карту веб-приложения. Для генерации вредоносного архива, эксплуатирующего уязвимость Zip Slip, может применяться пользовательский скрипт на языке программирования Python. Для создания кода reverse shell удобно воспользоваться популярным инструментом для тестирования на проникновение Metasploit или онлайн-ресурсом revshells.com, на котором собрано множество вариантов для получения обратной оболочки, в зависимости от целевой системы [6]. Для отправки веб-запросов может использоваться инструмент curl, а взаимодействие с полученным веб-шеллом можно осуществить с помощью утилиты Netcat, обеспечивающей прием сетевого соединения. Для поиска векторов повышения

привилегий внутри инфраструктуры могут применяться скрипты перечисления, например, LinPEAS, а также онлайн-ресурс GTFOBins.org для поиска легитимных функций бинарных файлов в ОС Linux [7].

Успешное завершение сценария подтверждается получением прав суперпользователя и чтением специального текстового файла (рисунок 3).

```
bash-5.1$ find / -name "root.txt" 2>/dev/null
find / -name "root.txt" 2>/dev/null
/root/root.txt
bash-5.1$ cat /root/root.txt
cat /root/root.txt
cat: /root/root.txt: Permission denied
bash-5.1$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash-5.1$ find . -exec /bin/sh -p \; -quit
find . -exec /bin/sh -p \; -quit

id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
cat /root/root.txt
CTF{root_flag_system_compromised}
```

Рисунок 3 – Финальный этап задания

В результате проделанной работы был успешно спроектирован и реализован комплексный практико-ориентированный сценарий киберинцидента, направленный на формирование и закрепление прикладных навыков молодых специалистов в области информационной безопасности, в частности, в сфере тестирования на проникновения. Подобный подход позволяет обучающимся на практике освоить востребованный специализированный инструментарий и погрузиться в условия, максимально приближенные к реальным кибератакам. Навыки, полученные в ходе выполнения заданий по тестированию на проникновение, также могут быть полезны для таких позиций в информационной безопасности, как SOC-аналитик, аналитик по киберугрозам (Threat Intelligence), инженер по реагированию на инциденты (Incident Responder) и специалист по защите ПО (AppSec). Глубокое понимание техник и тактик нарушителей, сформированное в ходе пентестов, позволяет специалистам по защите качественнее настраивать системы мониторинга и выявлять аномальную активность на ранних стадиях, а тестировщикам на проникновение оттачивать приобретенные навыки.

Список использованных источников:

1. Топ-3 профессий в кибербезопасности: карьерный план на 2026 год [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/Топ-3-Cybersecurity-Jobs-AMLive-2025. – Дата доступа: 21.03.2026.
2. Форензика: искусство расследования инцидентов ИБ [Электронный ресурс]. – Режим доступа: <https://securitymedia.org/info/forenzika-iskusstvo-rassledovaniya-intsidentov-ib.html>. – Дата доступа: 21.03.2026.
3. Reverse Engineering - Software Engineering [Электронный ресурс]. – Режим доступа: <https://www.geeksforgeeks.org/software-engineering/software-engineering-reverse-engineering>. – Дата доступа: 21.03.2026.
4. Пентест: что такое тестирование на проникновение [Электронный ресурс]. – Режим доступа: <https://ddos-guard.ru/blog/chto-takoe-pentest>. – Дата доступа: 21.03.2026.
5. MITRE ATT&CK [Электронный ресурс]. – Режим доступа: <https://attack.mitre.org/>. – Дата доступа: 21.03.2026.
6. Reverse Shell Generator [Электронный ресурс]. – Режим доступа: <https://www.revshells.com/>. – Дата доступа: 21.03.2026.
7. GTFOBins [Электронный ресурс]. – Режим доступа: <https://gtfobins.org/>. – Дата доступа: 21.03.2026.

АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЛОКАЛЬНО-АДАПТИВНОГО АГЕНТА КИБЕРРАЗВЕДКИ

Войткус И.А., студент гр. 361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук, доцент

Аннотация. В работе представлено описание алгоритмического обеспечения локально-адаптивного Telegram-агента для автоматизации OSINT-разведки. Рассмотрен комплекс из трех алгоритмов: эвристическая генерация псевдонимов с учетом национальных стандартов транслитерации, динамический синтез синтаксических Dork-запросов и трехэтапный алгоритм биометрической верификации на базе нейросетевой модели Facenet. Описанные подходы позволяют автоматизировать сбор цифрового следа в локальном сегменте, обеспечивая высокую точность распознавания и соблюдение требований законодательства Республики Беларусь в области защиты персональных данных.

Ключевые слова. OSINT-разведка, алгоритмы, киберразведка, биометрические данные, защита персональных данных.

В современном мире аудит информационной безопасности организации невозможен без применения инструментов OSINT [1]. Хотя часто существующие платформы киберразведки демонстрируют низкую эффективность в локальных задачах поиска в странах СНГ из-за лингвистических барьеров и специфики формирования цифрового следа. Разработанный локально-адаптивный агент решает данные проблемы посредством внедрения специализированного алгоритмического обеспечения.

Первым алгоритмов агента является формирование массива потенциальных сетевых идентификаторов субъекта. Разработанный алгоритм эвристической генерации псевдонимов выполняет нормализацию входных данных (ФИО на кириллице) и их транслитерацию в соответствии с национальными правилами транслитерации Республики Беларусь. Далее генерируются сочетания инициалов, фамилии и разделительных знаков (например, f_familia, familia.i). Данный метод помогает подобрать нужный возможный псевдоним для дальнейшего поиска. В результате чего формируется массив возможных никнеймов для автоматической проверки через API социальных платформ и сервисов разработки.

Далее перед агентом стоит задача выявления скрытых метаданных и утечек в открытом документообороте, для чего применяется алгоритм динамического формирования Dork-запросов. Логика алгоритма заключается в синтезе необходимых URL-строк, содержащих специализированные операторы (например, ext:pdf, site:, allintext:). Алгоритм автоматически адаптирует поисковой запрос под целевой домен организации, что позволяет обнаруживать методические материалы, приказы и отчеты, содержащие конфиденциальные сведения об инфраструктуре.

Критически важным компонентом системы является функция распознавание биометрических данных и сравнение их с эталонными значениями. Для этого данный инструмент используется следующий алгоритм: выполняется инициализация лица и происходит выравнивание по линии глаз, что обеспечивает различные варианты распознавания при различных ракурсах съемки, далее подготовленное изображение подается в нейросеть Facenet [2], которая преобразует визуальные признаки в уникальный 512-мерный вектор. Модель обучена с использованием функции потерь Triplet Loss, что дает минимальное расстояние в векторном пространстве для лиц одного человека. На финальном этапе выполняется расчет косинусного сходства между вектором входного изображения и эталонными векторами из данных фотографии предоставленной для поиска (эталонной), данный расчет вычисляется по формуле:

$$S_c(A, B) = \frac{\sum_{i=1}^n A_i B_i}{\sqrt{\sum_{i=1}^n A_i^2} \sqrt{\sum_{i=1}^n B_i^2}}, \quad (1)$$

где n – размер вектора; A_i и B_i – компоненты сравниваемых векторов.

При превышении установленного порога (Threshold) система подтверждает личность субъекта. Данный подход позволяет минимизировать ложные срабатывания и проводить верификацию в реальном времени. Схема конвейера алгоритмической обработки данных приведено на рисунке 1.

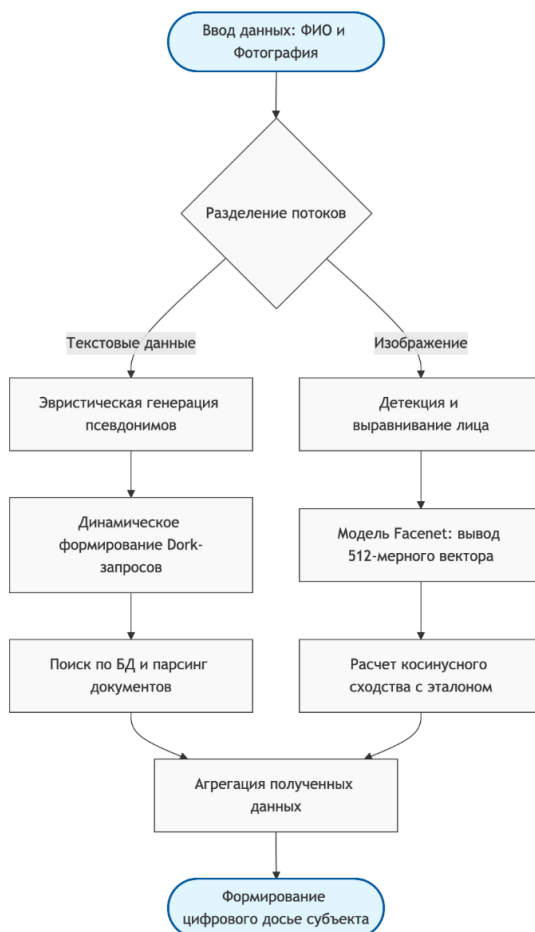


Рисунок 1 – Блок-схема конвейера алгоритмической обработки данных агентом

Перенос процессов OSINT-профилирования из глобальных облачных платформ в локально-изолированные контуры – это не только техническая оптимизация, но и необходимый шаг к достижению подлинной информационной независимости от западных принципов и инструментов. В настоящее время, когда границы между частным и публичным цифровым присутствием окончательно размыты, способность организации проводить внутренний аудит, не раскрывая сам факт этого аудита внешним игрокам, становится базовым условием выживания инфраструктуры. Данное исследование закладывает фундамент для создания нового поколения локальных систем безопасности, принося в конкретном регионе аудита, максимальную эффективность

Список использованных источников:

1. Войткус И.А. Инструмент для OSINT-разведки и реализации техники MITRIE ATTA&CK T1593 / И.А. Войткус, Е.С. Белоусова // Технические средства защиты информации: матер. XXIV Междунар. науч.-техн. конф., 2026. – С. 342–345.
2. Николенько, С. И. Глубокое обучение. Погружение в мир нейронных сетей / С.И. Николенько, А.А. Кадури, Е.О. Архангельская. – СПб.: Питер, 2018. – 480 с.

ЛОКАЛЬНО-АДАПТИВНЫЙ TELEGRAM-АГЕНТ ДЛЯ OSINT-РАЗВЕДКИ

Войткус И.А., студент гр.361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук, доцент

Аннотация. В статье рассматривается разработка локально-адаптивного Telegram-агента для автоматизации разведки по открытым источникам. Ввиду неэффективности западных платформ в локальном сегменте и ограничений решений, предложена архитектура на базе FastAPI и Telegram API. Инструмент использует локальную базу данных и включает модули лингвистической адаптации, генерации Dork-запросов и биометрической идентификации лиц DeepFace. Разработанная система обеспечивает информационный суверенитет, соответствует законодательству Республики Беларусь о защите персональных данных и позволяет безопасно, быстро формировать цифровое досье субъекта без передачи данных в зарубежные облачные сервисы.

Ключевые слова. киберразведка, OSINT, Telegram-бот, биометрическая идентификация, FastAPI, защита персональных данных.

Разработка и применение систем автоматизированного сбора данных в Республике Беларусь строго регламентируются национальным законодательством. Согласно Закону РБ от 07.05.2021 № 99-З «О защите персональных данных», обработка общедоступной информации без согласия лица допускается (ст. 6), однако автоматизированная агрегация таких данных в единый цифровой профиль требует соблюдения принципа соразмерности и целесообразности.

Особое внимание при проектировании подобных систем уделяется работе биометрического модуля: согласно ст. 8 Закона № 99-З, обработка биометрических персональных данных (распознавание лиц посредством нейросетей) требует обязательного письменного согласия субъекта. Бесконтрольное использование разработанного агента для скрытой деанонимизации третьих лиц является неправомерным и может быть квалифицировано по ст. 203-1 УК РБ «Незаконные действия в отношении информации о частной жизни и персональных данных».

В условиях постоянного роста объемов информации в открытых источниках, важным является аудит информационной безопасности организации. Согласно методологии MITRIE ATT&CK, этап сбора информации по открытым источникам включает в себя тактику T1593 [1]. В предыдущем исследовании была продемонстрирована успешная апробация способа автоматического сбора данных с использованием платформы n8n [2]. Но в ходе анализа были выявлены ограничения: недостаточная гибкость логики обработки битых данных, зависимость от внешних триггеров запуска, а также проблем управления таймаутами. Было принято решение использовать Telegram бот для передачи входных данных. Основные причины данного выбора являются:

1. В отличие от обычного веб-сайта, где сервер имеет публичный IP-адрес, бот общается с серверами Telegram, что делает соединение невидимым для прямых атак.
2. Весь трафик между оператором и ботом защищен протоколами шифрования.
3. Бот обеспечивает мобильность не только пользователей персональных компьютеров, но и предоставляет возможность разведки со смартфона.

Встраивать такой бот в ноду созданной цепочки n8n было нецелесообразно, что объясняется тем, что при гибкой настройке n8n часто обрывает соединение, если процесс длится долго. В то время как в коде данную настройку можно гибко изменять.

Центральным элементом системы является хранилище данных `university_db.json`, использование формата JSON позволило обеспечить мгновенный парсинг данных средствами стандартных библиотек Python. Как и в предыдущем исследовании роль эталонного набора данных для тестирования локальной разведки, сыграли открытые данные о преподавателях с сайта `iis.bsuir.by`. Каждая запись включает в себя: идентификационные данные, метаданные, верификационные атрибуты. Такой подход обеспечил то, что данные не покидают периметр операционной системы, на которой все установлено. Блок-схема процесса взаимодействия с агентом представлена на рисунке 1.

Практическое применение популярных коммерческих и открытых платформ киберразведки (такие как Maltego, SpiderFoot) приносит мало полезной информации на выходе в контексте локального сегмента сети в странах СНГ и Республике Беларусь. Данные таких систем в основном ориентированы на зарубежные публичные реестры и западные социальные сети. Другим фактором является лингвистический барьер, так как западные анализаторы некорректно обрабатывают кириллические метаданные, что приводит к обрыву цепочки поиска.



Рисунок 1 – Процесс взаимодействия с агентом

В связи с перечисленными факторами было принято решение об отказе использования готовых OSINT-платформ в пользу разработки собственного локально-адаптивного агента. Для этого были разработаны следующие модули:

1. Вычислительное ядро, в качестве основы которого выбран асинхронный веб-фреймворк FastAPI, его применение позволило реализовать нужную архитектуру и обеспечить параллельную обработку длительных сетевых таймаутов, возникающие при работе тяжеловесных модулей.

2. Клиентский интерфейс, представленный в виде Telegram бота, связь с которым представлена через Telegram API.

3. Модули лингвистической адаптации, использующие стандартные библиотеки Python (requests для HTTP-запросов и urllib для кодирования URL). А для предсказания возможных никнеймов был написан собственный модуль, генерирующий массивы никнеймов, которые могут подойти для дальнейшего поиска [3].

4. Модуль биометрической идентификации, реализованный с применением глубокого обучения DeepFace. В качестве вычислительной модели выбрана нейросеть Facenet для обеспечения вычисления векторных представлений лиц при работе с базой данных, созданной в начале.

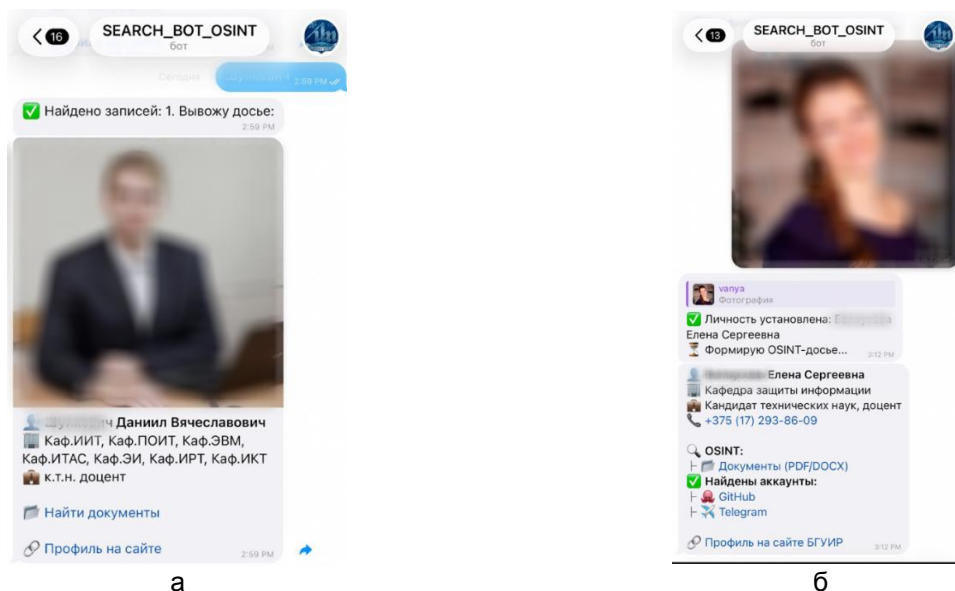


Рисунок 2 – Результат работы агента (а) и модуля идентификации по лицу (б)

Тестирование разработанного локально-адаптивного агента показало достаточно эффективные результаты. При вводе фамилии, имени и отчества или просто фамилии с, бот выдавал карточку преподавателя с информацией о должности, кафедре, номере телефона. Сгенерированные возможные никнеймы проверялись на наличие существующих аккаунтов в GitHub и Telegram, а также проводились специализированные Dork-запросы. Процесс занимает в среднем 1,5-2 секунды. Результаты проверки вышеописанных модулей, представленные ниже на рисунке 2, а.

Работа модуля биометрической идентификации реализована в соответствии со следующим алгоритмом:

1. Детектирование лица на загруженной фотографии с отсечением фона и программным выравниванием его по линии глаз для стандартизации ракурса.

2. Передача подготовленного изображения в нейросеть Facenet, которая преобразует уникальные черты лица в математический вектор, состоящий из 512 чисел.

3. Вычисление математического расстояния между полученным вектором и эталонными векторами, полученных из фотографий сотрудников БГУИР из локальной базы данных.

4. Анализ значения математического расстояния, если оно оказывается меньше заданного порога совпадения, алгоритм подтверждает личность и бот мгновенно формирует карточку досье.

Результат проверки такого компонента представлен на рисунке 3.

Таким образом, разработанный локально-адаптивный агент представляет собой не только эффективный инструмент OSINT-профилирования, но и стратегически важное решение для обеспечения информационного суверенитета, так как он учитывает специфику регионального цифрового следа (кириллица, локальные мессенджеры) и исключает риски трансграничной передачи данных в зарубежные облачные сервисы.

Список использованных источников:

1. Блэр, Р. *Согласование операций безопасности с фреймворком MITRE ATT&CK* / Р. Блэр. – Бирмингем: Packt Publishing, 2022. – 268 с. – ISBN 978-1804616697.

2. Войткус И.А. *Инструмент для OSINT-разведки и реализации техники MITRIE ATTA&CK T1593* / И.А. Войткус, Е.С. Белоусова К.Ц. // *Технические средства защиты информации : матер. XXIV Междунар. науч.-техн. конф. (Республика Беларусь, Минск, 08 апреля 2026 года)* / редкол. : О. В. Бойправ [и др.]. – Минск : БГУИР, 2026. – С. 342–345.

МЕТОДИКА ЗАЩИТЫ RFID-МЕТОК ОТ АТАК КОПИРОВАНИЯ И РЕТРАНСЛЯЦИИ

Ворожцов А.О., студент гр.461402

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пухир Г.А. – старший преподаватель каф. ЗИ

Аннотация. Метки типа RFID, в силу передачи данных по радиоканалу, уязвимы к атакам вида relay и replay. Для предотвращения использования нарушителем перехваченных данных предлагается дополнительный метод определения подлинности карты. Антенна карты меняется на печатную щелевую, со случайным расположением щелей, формирующим уникальный паттерн плотности магнитного поля.

Ключевые слова: RFID, HF, UHF, антенна, диаграмма направленности, плотность магнитного поля, Matlab, Relay-атака, Replay-атака, щелевая антенна.

Введение. В настоящее время довольно активно используются бесконтактные идентификаторы типа RFID. Данные идентификаторы диапазонов HF (13,56МГц) и UHF (865–868МГц в Европе и 902–928МГц в США) применяются в большом количестве областей, как то СКУД, маркировка товаров, общественный транспорт, логистика и многое другое. Для защиты чаще всего применяется симметричное шифрование, передача ранее записанных случайных чисел и измерение времени приёма-передачи. Данные средства защиты частично обходятся методами атак по побочным каналам или уязвимостями, заложенными производителями, что создаёт угрозу информационной безопасности [1].

UHF метки взяты в силу большего возможного разброса коэффициента отражения и меньшей длины волны по сравнению с метками HF диапазона. Так как при вышеупомянутых атаках устройство злоумышленника, будь оно специализированным или универсальным для работы с радиоэфиром, выдаёт себя за терминал, то в основном применяются методы защиты, использующие информацию, которую злоумышленник не может знать.

Предлагается добавление дополнительного физического идентификатора подлинности: антенна метки меняется на печатную щелевую антенну со случайным расположением щелей, таким образом получая уникальную диаграмму напряжённости магнитного поля. Изменением размеров и положения щелей на покрытии возможно получить значительное количество различных паттернов, с разной энтропией, градиентом и коэффициентом отражения. Так как работа ведётся в ближней зоне, то диаграмма направленности не имеет большого значения, и основные вариации будет иметь именно магнитное поле. Терминал оснащается антенной решёткой, позволяющей измерить плотность магнитного поля в разных точках пространства и вспомогательным контроллером, рассчитывающим градиент и коэффициент отражения для несущей частоты [2]. Данные значения передаются основному контроллеру, для ускорения процесса возможно привязать данные значения к ключу шифрования некоторой функцией, уникальной для каждой метки.

Расчёты проводились в САПР Matlab, на базе которого возможно создать приложение, рассчитывающее некоторое количество чертежей антенн с достаточной уникальностью для однозначной идентификации метки. Алгоритм создаёт по заданной чувствительности приёмной антенны и количеству чертежей или характеристикам щелей списки щелей с их расположением и характеристиками, при которых данные комбинации возможно различить на заданном терминале.

Для обхода данной методики защиты помимо длительного контакта с меткой, потребуется наличие оборудования, способного измерить характеристики антенны, ПО для расчёта антенны по данным характеристикам и оборудования для создания идентичной антенны. В силу этого, для проведения атаки нарушитель должен иметь значительный уровень подготовки и материально-технического обеспечения.

Полученный метод позволяет более определять подлинность RFID меток на физическом уровне, без изменения протокола, контроллеров метки и терминала, требуя лишь изменения антенны метки, антенны терминала и установки вспомогательного контроллера. Данный метод применим к любым картам диапазонов HF и UHF, обеспечивая бюджетную и эффективную защиту.

Список использованных источников:

1. Таненбаум А. Эволюция безопасности RFID//IEEE Security & privacy. – 2006. – Т.4, № 2. – С. 62–69.
- 2 В.В. Муравьев, А. А. Тамело, Д. Ф. Молодкин, Д. Б. Владимиров (2010) Расчёт и проектирование антенн и устройств СВЧ. – Минск, БГУИР.

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ РАЗЛИЧНЫХ ВИДОВ ДИСКРЕТНОЙ МОДУЛЯЦИИ ДЛЯ СИСТЕМ ЗАЩИЩЕННОЙ ПЕРЕДАЧИ ДАННЫХ

Дейкало И.С., студент гр.461402

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Фильченкова Т.М. – старший преподаватель каф. ЗИ

Аннотация. В работе проведено исследование эффективности различных видов дискретной модуляции для применения в системах защищенной передачи данных. Рассмотрены двоичная фазовая, квадратурная фазовая и частотная манипуляции. С использованием языка Python выполнено моделирование прохождения сигналов через канал с аддитивным гауссовским шумом, рассчитаны вероятности битовой ошибки и спектральная эффективность. На основе полученных данных предложены рекомендации по выбору метода дискретной модуляции для систем защищенной передачи данных.

Ключевые слова. Дискретная модуляция, манипуляция, канал связи, помехоустойчивость, спектральная эффективность, двоичная фазовая манипуляция, квадратурная фазовая манипуляция, частотная манипуляция.

Надежность канала связи в защищённых системах передачи данных в значительной степени зависит от параметров физического уровня передачи даже с учетом развитых средств защиты информации. Качество передачи определяется тем, как сигнал сохраняет свою целостность и разборчивость в условиях шума и воздействия помех. Поэтому при проектировании защищённых систем передачи данных следует уделять внимание параметрам физического уровня передачи.

Определяющим элементом физического уровня является метод дискретной модуляции. Причем выбор способа представления цифровой информации в виде параметров несущего сигнала определяет спектральную эффективность системы, а также ее помехоустойчивость.

Для исследования эффективности дискретной модуляции в системах защищённой передачи данных были выбраны следующие методы: двоичная фазовая, квадратурная фазовая и частотная манипуляции. Данные виды обеспечивают высокую помехоустойчивость и стабильность передачи информации. ФМн-2 и ФМн-4 позволяют наглядно изучить влияние числа фазовых состояний на надёжность сигнала, а ЧМн исследовать устойчивость к амплитудным помехам.

Для проверки их работы и дальнейшего анализа сигналы с ФМн-2, ФМн-4 и ЧМн были смоделированы с использованием языка Python и библиотек NumPy и Matplotlib. Далее был создан канал связи с аддитивной гауссовской помехой, описываемый формулой [1]:

$$r(t) = s(t) + n(t), \quad (1)$$

где $r(t)$ – сигнал на выходе канала, $s(t)$ – передаваемый сигнал, $n(t)$ – гауссовский шум.

После прохождения сигнала через канал связи была выполнена его демодуляция. Демодулятор для каждого битового интервала вычислял среднее значение и принимал решение о переданном бите. Затем восстановленная последовательность сравнивалась с исходной, и по числу несовпадений определялась вероятность битовой ошибки.

Для верификации результатов моделирования были рассчитаны теоретические кривые помехоустойчивости, которые описывают зависимость вероятности битовой ошибки от отношения E_b/N_0 . Для систем с двоичной и квадратурной фазовой манипуляцией теоретическая вероятность битовой ошибки определяется выражением [2]:

$$P = Q\left(\sqrt{\frac{2E}{N}}\right). \quad (2)$$

Для системы с двоичной частотной манипуляцией вероятность битовой ошибки рассчитывается по формуле:

$$P = Q\left(\sqrt{\frac{E}{N}}\right). \quad (3)$$

Результаты моделирования и теоретических расчетов представлены на рисунке 1.

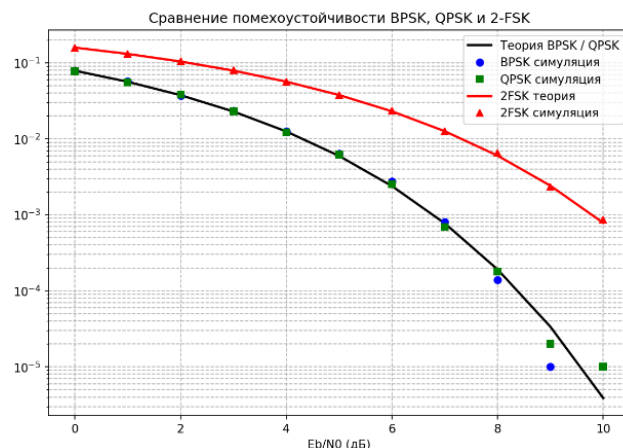


Рисунок 1 – Зависимость вероятности битовой ошибки от отношения \$E_b/N_0\$

Основываясь на полученных данных, более помехоустойчивы сигналы с ФМн-2 и ФМн-4, чем сигналы с ЧМн. В среднем проигрыш частотной манипуляции составляет 3 дБ. Это означает, что для обеспечения того же качества связи при использовании частотной манипуляции потребуется передатчик в два раза мощнее, чем при использовании ФМн-2 или ФМн-4.

Однако при выборе метода манипуляции важным параметром является не только помехоустойчивость, но и эффективность использования частотного ресурса канала связи. В современных системах передачи данных спектр является ограниченным ресурсом, поэтому необходимо стремиться к максимально эффективному использованию занимаемой полосы частот. Для оценки данного свойства используется показатель спектральной эффективности, характеризующий количество передаваемой информации на единицу полосы частот.

Чтобы определить спектральную эффективность исследуемых сигналов, строится график спектральной плотности мощности для каждого вида модуляции (рисунок 2).

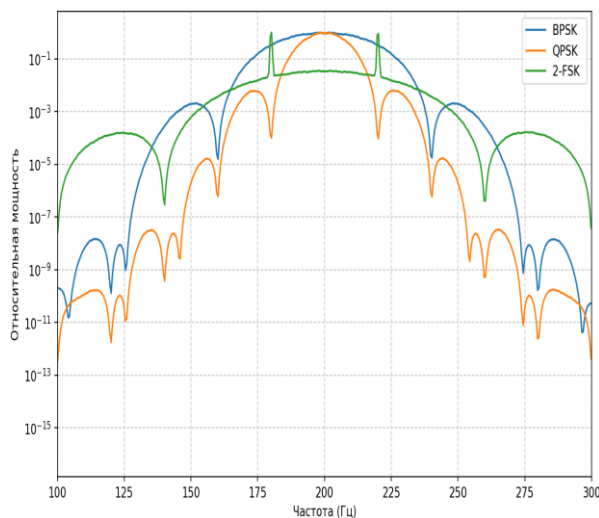


Рисунок 2 – Спектральная плотность мощности исследуемых сигналов

И для каждой схемы вычисляется спектральная эффективность по формуле [3]

$$\eta = \frac{R}{B}, \quad (4)$$

где \$R\$ – битовая скорость, \$B\$ – занимаемая полоса частот.

При этом полоса частот для каждого сигнала определялась на основе анализа спектральной плотности мощности. Данный анализ позволяет определить распределение энергии сигнала по частотам и установить диапазон частот, используемый при передаче информации. Для оценки использовалась ширина спектра, в которой сосредоточена основная часть энергии сигнала. За пределами этого диапазона амплитуды спектральных составляющих значительно уменьшаются, поэтому их влияние на передачу информации является незначительным.

Результаты моделирования показывают, что различные виды манипуляции характеризуются различной спектральной эффективностью. Сравнение проводилось при одинаковой битовой скорости передачи данных 40 бит/с, что позволяет корректно оценить занимаемую полосу частот для каждого метода. В рассматриваемых условиях для сигнала с двоичной фазовой манипуляцией занимаемая полоса частот составила 60,06 Гц, что соответствует спектральной эффективности 0,666 бит/с/Гц. Для частотной манипуляции занимаемая полоса частот равна 84,96 Гц, а спектральная эффективность составляет 0,471 бит/с/Гц.

Наиболее высокий результат был получен для квадратурной фазовой манипуляции. В ходе моделирования установлено, что занимаемая полоса частот для данного сигнала составляет 32,71 Гц, а спектральная эффективность достигает 1,223 бит/с/Гц. Такая эффективность объясняется тем, что один символ в ФМн-4 передает два бита информации, что позволяет передавать больший объем данных при меньшей занимаемой полосе частот. Таким образом, среди рассмотренных методов манипуляции наилучшее использование спектрального ресурса обеспечивает ФМн-4.

На основании полученных результатов рекомендуется использовать квадратурную фазовую манипуляцию в системах защищенной передачи данных. В первую очередь это обусловлено её высокой помехоустойчивостью. По результатам моделирования установлено, что сигналы с фазовой манипуляцией более устойчивы к шумовым воздействиям по сравнению с сигналами с частотной манипуляцией. При этом ФМн-4 сохраняет практически такой же уровень помехоустойчивости, как и двоичная фазовая манипуляция.

Также ФМн-4 характеризуется более высокой спектральной эффективностью по сравнению с ФМн-2 и ЧМн. При одинаковой битовой скорости передачи данных ФМн-4 занимает меньшую полосу частот, что обеспечивает более эффективное использование спектра канала связи. Таким образом, применение квадратурной фазовой манипуляции является наиболее целесообразным среди рассмотренных методов.

Список использованных источников:

1. Биккенин, Р. Р. Теория электрической связи : учеб. пособие для студ. высш. учебных заведений / Р. Р. Биккенин, М. Н. Чесноков. – М. : Издательский центр «Академия», 2010. – 336 с.
2. Ку, Х.Н. Анализ вероятности ошибки сигналов QPSK и BPSK / Х.Н. Ку // 56-я Научная Конференция Аспирантов, Магистрантов и Студентов БГУИР. – Минск, 2020.
3. Скороходов, Р.В. Анализ эффективности инфокоммуникационных систем / Р.В. Скороходов // 58-я научная конференция аспирантов, магистрантов и студентов БГУИР. – Минск, 2022.

АРХИТЕКТУРА НЕЙРОСЕТЕВОЙ СИСТЕМЫ СЕМАНТИЧЕСКОЙ ИНВЕРСИИ ДЛЯ ГЕНЕРАЦИИ ПСЕВДОРЕЧИ

Денскевич А.Д., аспирант

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Зельманский О.Б. – канд. техн. наук, доцент

Аннотация. Рассмотрена концепция семантической инверсии речи как альтернативы подавлению сигнала. Предложена архитектура нейросетевой системы, включающая модули распознавания, трансформации текста и синтеза речи с сохранением аллофонного профиля диктора. Обоснован выбор моделей для каждого этапа архитектуры (GigaAM, LLM, Fish Speech, IndexTTS-2) с приведением их количественных характеристик (WER, MOS, ELO, задержка). Показано, что реализация такой системы позволяет заменить смысл высказывания при сохранении индивидуальных голосовых признаков, что представляет собой новое направление в защите речевой информации.

Ключевые слова. Защита информации, семантическая инверсия, псевдоречь, нейросетевая архитектура, аллофонный профиль, защита речевой информации, синтез речи, сегментация речи, GigaAM, Fish Speech, IndexTTS-2, LLM.

Актуальные методы защиты речевой информации от утечки по техническим каналам основываются на подавлении сигнала – генерации акустических, виброакустических или электромагнитных помех, что маскирует речевой сигнал посредством повышения общего уровня сигнала [1, 2]. Существует некоторая нормативная база, которая регламентирует порядок защиты, к примеру: ГОСТ Р 50840-95 и СТБ ГОСТ Р 50840-2000. Однако ввиду стремительного развития цифровых технологий данная база может быть недостаточно актуальной. Актуальные методы всё ещё встречаются в защите переговорных комнат и помещений, содержащих конфиденциальную речь, но их использование со временем становится всё менее и менее надёжным из-за ряда ограничений: сами сигналы создают дискомфорт для слуха, либо могут на его влиять незаметно, но сохраняя влияние; сам сигнал помех требуется на достаточно высоком уровне, который превышает защищаемый сигнал на 6-10 дБ – такие методы могут быть в настоящее время не в достаточной степени эффективными, чтобы обеспечить надёжную защиту переговоров, так как существуют такие алгоритмы дешифровки, как шумоподавление и нейросетевое восстановление речи [3]. Нейросетевые приёмы способны адаптивно отделять полезный сигнал от лишнего сигнала, а шумоподавление является более консервативным и ручным способом, но не менее надёжным комплексом методов обработки сигналов, который может включать спектральное вычитание, непосредственное использование нейросетей, как, например, инструмент «нейросетевое подавление шума» и адаптивную фильтрацию. Такие методы позволяют выделять полезный речевой сигнал из общего сигнала, в котором могут быть помехи, что возможно даже при отрицательном отношении сигнала и шума.

Альтернативным подходом, обеспечивающим защиту речевого сигнала и конфиденциальность переговоров, может служить семантическая инверсия. В данном подходе сами слова и речь преобразуются в контексте смысла, выдавая по итогу нейтральную по смыслу – незаметную посторонним людям – речь, либо вовсе ложный по своему смыслу речевой сигнал. При таком подходе естественно задуматься о сохранении голосовых и эмоциональных характеристик диктора для отсутствия подозрений и внешней высокой степени естественности речи. Такой преобразованный речевой сигнал можно назвать псевдоречью, который при сохранении голосовых характеристик голоса человека, которого необходимо защитить, звучит естественно при этом сохраняя конфиденциальность информации. Такой подход не требует подавления сигнала, а обеспечивает семантическое преобразование речевого сигнала в необходимый для защиты информации, хотя в то же время, имея цель запутать злоумышленника сильнее, может работать и со старыми методами. В таком случае исходная информация остаётся защищенной, а перехват сигнала и обход акустического барьера становятся бессмысленными.

Рассмотрим архитектуру нейросетевой системы семантической инверсии посредством этапов различной обработки речевого сигнала, учитывая существующие модели далее.

Выделим три последовательных функциональных блока:

1. Блок распознавания и сегментации речи, обеспечивающий обработку речевого сигнала, выделяя из текста ряды транскрипций и общего аллофонного профиля диктора;
2. Блок трансформации содержания речи, который завязан на генерации семантически инвертированного текста, который будет сохранять при этом просодические средства языка, включающие эмоции, связи между словами, произношение и прочее;
3. Блок синтеза речи с управлением по аллофонному профилю, который даёт возможность создать необходимый акустический сигнал, используя имеющиеся голосовые признаки диктора.

Реализация данных блоков требует отдельные нейросетевые архитектуры, связываемые в алгоритм, где каждый этап, а точнее выбор способа прохождения этапа, нуждается в достаточной точности и работе в реальном времени, что будет определяться посредством выбора той или иной архитектуры.

Различные архитектуры и модели обрабатываются с разными языками в той или иной степени эффективности. Модель автоматического распознавания речи (ASR) наиболее эффективная для русского языка – GigaAM, разработанная SberDevices. Данная модель прошла независимые тесты, по результатам которых показатель WER (Word Error Rate – частота ошибок в словах) на центральном процессоре достигает 3,3% на русском языке. Данный показатель сравнивался с моделью Whisper large-v3-turbo, где модель от SberDevices GigaAM показала WER в 2,4 выше на графическом процессоре. Модель GigaAM обучена на 700 000 часах русскоязычной речи, которая использовала RNNT-декодер (Recurrent Neural Network Transducer – архитектура, объединяющая кодировщик, предсказатель и сеть совместной обработки для потокового распознавания) и показала пиковую задержку в 660 мс. Такая задержка достаточно близкая к отклику в реальном времени [4].

Распознавание текста с сегментацией на аллофоны происходит параллельно с описанным выше. Аллофонами являются некоторые реализации фонем в речи диктора, которые включаются в себя как позиции в слове, так и фонетическое окружение (слова до и после рассматриваемого слова). Аллофоны в различных языках отличаются своим количественным составом. Так в русском языке выделяются 22 гласных и 276 согласных вариаций аллофонов [5]. CTC-модель (Connectionist Temporal Classification – метод обучения нейросетей без пошаговой разметки, позволяющий находить границы фонем) может позволить обеспечить автоматическую сегментацию речи. Также в возможную помощь к данной модели может быть представлена мультимодальная модель SAM Audio от Meta, представленная в 2025 году. Данная модель выполняет сегментацию по текстовому запросу. Данная функция позволит выделять аллофоны строго обозначенного типа [6]. По итогу работы в данном блоке можно получить текст, состоящий из транскрипций, аллофонную последовательность вариаций сигналов по временной шкале и акустические параметры рассматриваемого текста – форманты (области спектральной концентрации акустической энергии, определяющие опознавание гласных и согласных). Кроме этого, выделяют длительность самих звуков и частоту голоса диктора. Всё это – аллофонный профиль диктора базового уровня.

Далее производим обработку речевого сигнала, представляющего себя стэк из транскрипций посредством большой языковой модели (LLM). Данная модель способна сгенерировать семантически инвертированные высказывания по заданным параметрам. Цель LLM в данном контексте – генерация текста схожей или той же тематики, изменив его смысл, скрыв конфиденциальную информацию, сохранив форму речи, описываемую просодическими характеристиками: ударения, длительности звуков, интонационный контур и другое. Таким образом, рассматриваются просодические характеристики (ударение, интонация, длительности). Русскоязычные большие языковые модели более эффективно работают тогда, когда разработчик ориентирован на данную аудиторию среди пользователей данной модели – работа с языком более проработана и точна. Можно выделить некоторые открытые модели: Qwen3-32B, широко поддерживающий различные языки и DeepSeek-V3.1, который показывает хорошие результаты на русскоязычных данных. При использовании моделей естественно на вход подаётся широкий профиль текста, включающий стилистические особенности текста, выделение ключевых слов и других особенностей.

Третьим блоком является синтез речи по инвертированному тексту при сохранении аллофонических характеристик диктора. Такой синтез должен поддерживать управление по извлечённым акустическим признакам (conditioning). Для решения данной задачи подойдёт ряд архитектур. Fish Speech V1.5 (от fishaudio) - архитектура, которая использует DualAR технологию – авторегрессионный трансформер, показывающий акустические токены и управляющие параметры речи. Данная архитектура оценивалась рейтингом TTS Arena, набрав 1339 балла ELO, WER 3,5% для английского языка и CER 1,3% для китайского языка [7]. Данная архитектура включает в себя многозначность и может быть адаптирована для управления по внешним векторам, в том числе для описания голоса. Другая архитектура IndexTTS-2 превосходит современные zero-shot TTS модели по показателю WER, а также по сходству с диктором и эмоциональной точности [8]. Данная архитектура позволяет независимо задавать параметры голоса, но также и эмоций - учитывается весь акустический профиль диктора, что важно при изменении текста. Конкретно русский язык имеет широкое распространение в архитектуре Tacotron 2 (она адаптирована под русский язык в исследованиях СПбГУ на основе корпуса CORPRES – аннотированного корпуса русской речи, содержащего фонетическую и просодическую разметку), который имеет результат показателя MOS (Mean Opinion Score – средняя экспертная оценка) в 4,53, что достаточно близко к человеческой речи (4,58) [9]. В качестве вокодера может использоваться WaveRNN – вокодер, использование которого способно обеспечить качество сигнала на достаточно хорошем уровне, при этом не требуя больших вычислительных мощностей, в отличие от WaveNet. Таким образом, в предложенной архитектуре управляющие параметры генерируются в первом блоке в виде вектора, кодирующего аллофонный профиль диктора (формантные частоты, длительности, основная частота и другое). Этот вектор

подаётся в синтезатор как дополнительный вход, что позволяет генерировать речь, фонетически схожую с исходной речью диктора.

Реализация данной архитектуры или алгоритма архитектур требует учёта ряда сложностей. Задержка складывается из ASR (примерно 660 мс для GigaAM), генерации большой языковой модели и синтеза речи (CosyVoice2 имеет значение примерно 150 мс [10]), таким образом выходит 1-2 с, что является удовлетворительным результатом, однако с возможностью для оптимизации, посредством квантования и малых моделей. Эмоции содержатся в аллофонном профиле диктора в виде конкретной информации, которая включает просодию. IndexTTS-2 переносит эмоциональный тон исправно [8]. Большинство моделей (Fish Speech, CosyVoice2) обучены на английском и китайском; для русского языка требуется адаптация на данных типа CORPRES, что представляется возможным ввиду схожести архитектур.

Отличие маскирования речевого сигнала посредством шума и глушения сигнала отличается от семантической инверсии концептуально – в одном случае слышен шум и против его используют различные приёмы, а в ином случае можно слышать осмысленную речь, которая на самом деле не имеет конфиденциальной информации.

Таким образом была предложена трёхблочная архитектура, включающая такие технические решения, как: GigaAM, LLM-трансформация, синтез речи на Fish Speech V1.5 или IndexTTS-2 с управлением по аллофонному профилю диктора. В речи изменяется смысл при сохранении голоса – таким образом обеспечивается высокий уровень защиты информации. Однако здесь важно учитывать индивидуальные различия дикторов и возможно помещений, адаптацию моделей под русский язык и другие параметры, к которым нейросетевые технологии адаптируются в процессе обучения. Перспективными исследованиями по данной тематике представляются: прототип такой архитектуры, её оценка по различным метрикам, а также в целом лингвистическая адекватность без цифровых галлюцинаций.

Список использованных источников:

1. Зольников, В. К. [и др.]. Исследование способов защиты информации от утечки по акустическому и виброакустическому каналам / В. К. Зольников, С. А. Сазонова, А. И. Заревич, С. С. Башун // *Моделирование систем и процессов*. – 2025. – № 2. – С. 27–40.
2. Хорев, А. А. *Техническая защита информации: учебное пособие для вузов*. В 3 т. Т. 1. Технические каналы утечки информации / А. А. Хорев. – М.: Минобороны России, 2018. – 436 с.
3. Волчихина, М. В. Алгоритм формирования адаптивной речеподобной помехи для защиты конфиденциальной речевой информации в офисных помещениях / М. В. Волчихина // *Труды учебных заведений связи*. – 2025. – Т. 11, № 5. – С. 21–27.
4. Снижение WER с 33% до 3.3% для русской речи на CPU [Электронный ресурс]. – Режим доступа: <https://www.pvsm.ru/python/445372/> – Дата доступа: 27.03.2026.
5. Бондарко, Л. В. *Фонетика современного русского языка: Учебное пособие* / Л. В. Бондарко. – СПб.: Издательство СПбГУ, 1998. – 276 с.
6. Bowen Shi [et al.]. SAM Audio: Segment Anything in Audio / B. Shi, A. Tjandra, J. Hoffman [et al.] // *arXiv preprint arXiv:2512.18099v1*. – 2025.
7. Fish-Speech-1.5 – Model Info [Электронный ресурс] // SiliconFlow. – Режим доступа: <https://www.siliconflow.com/models/fishaudio-fish-speech-1-5> – Дата доступа: 27.03.2026.
8. Zhou, S. [et al.]. IndexTTS2: A Breakthrough in Emotionally Expressive and Duration-Controlled Auto-Regressive Zero-Shot Text-to-Speech / S. Zhou, Y. Zhou, Y. He [et al.] // *arXiv preprint arXiv:2506.21619*. – 2025.
9. Google создала систему синтеза речи, почти неотличимую от человека [Электронный ресурс] // N+1. – 2017. – Режим доступа: <https://nplus1.ru/material-print/14117/> – Дата доступа: 27.03.2026.
10. FunAudioLLM/CosyVoice2-0.5B – Model Info [Электронный ресурс] // SiliconFlow. – Режим доступа: <https://www.siliconflow.com/models/funaudiollm-cosyvoice2-0-5b> – Дата доступа: 27.03.2026.

АНАЛИЗ УЯЗВИМОСТЕЙ ПРОТОКОЛА МАРШРУТИЗАЦИИ OSPF И МЕТОДЫ ИХ УМЕНЬШЕНИЯ В КОРПОРАТИВНЫХ СЕТЯХ

Долгая А.С., студент гр 361402

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Мокеров В.С. – ассистент каф. ЗИ

Аннотация. В материалах статьи рассматриваются уязвимости протокола динамической маршрутизации OSPF, его основные типы атак и методы защиты. Защита OSPF в приоритете ставит внедрение криптографической аутентификации и фильтрацию маршрутной информации с целью исключения возможности несанкционированного изменения маршрутов.

Ключевые слова. OSPF, динамическая маршрутизация, уязвимости протоколов, LSA, аутентификация, корпоративная сеть, безопасность маршрутизации

Протокол OSPF (Open Shortest Path First) является одним из наиболее распространённых протоколов динамической маршрутизации в корпоративных сетях среднего и крупного размера. Благодаря быстрой сходимости, масштабируемости и поддержке бесклассовой адресации (CIDR) он широко используется как в государственных организациях, так и в коммерческих структурах. Однако вопросы безопасности OSPF часто остаются вне фокуса внимания сетевых администраторов, поскольку приоритетом при настройке обычно является доступность и производительность, а не защита от целенаправленных атак.

Данный протокол относится к классу протоколов состояния каналов. Его работа основана на обмене между соседними маршрутизаторами сообщениями о состоянии каналов – LSA (Link State Advertisement), которые хранятся в единой базе данных LSDB. Именно эта архитектура, обеспечивающая быструю сходимость и масштабируемость, создаёт ряд фундаментальных уязвимостей.

В протоколе отсутствует обязательная аутентификация. Базовая спецификация OSPFv2 (RFC 2328) определяет аутентификацию как опциональный механизм [1]. Администратор может полностью отключить проверку подлинности OSPF-пакетов, и любой маршрутизатор, подключившийся к сегменту сети, способен установить соседство и начать рассылку LSA. Передача данных происходит в открытом виде. Даже при включении аутентификации сам OSPF-трафик не шифруется. Пароль передаётся открыто (при plain text) либо содержимое LSA остаётся доступным для перехвата (при MD5/SHA). Злоумышленник получает детальную карту сети. Архитектура OSPF построена на допущении, что все участники домена являются доверенными. После установления соседства маршрутизаторы принимают LSA без дополнительной верификации источника. Как отмечается в документации Cisco, данная уязвимость позволяет злоумышленнику полностью контролировать таблицу маршрутизации OSPF-домена [2]. Процедура выбора DR/BDR крайне уязвима. Злоумышленник может объявить максимальный приоритет и захватить роль Designated Router, что даёт ему влияние на синхронизацию LSDB в сегменте. В протоколе отсутствует защита IP-заголовка. Механизмы аутентификации OSPF (RFC 2328, RFC 5709) не защищают IP-заголовок пакета, что позволяет подменять IP-адрес источника для сброса соседств. Механизмы безопасности OSPF рассмотрены в таблице 1.

Таблица 1 – Стандартные механизмы безопасности OSPF и их ограничения

Механизм безопасности	Что обеспечивает	Основные ограничения
Plain text authentication	Базовую проверку пароля	Пароль передаётся открыто, легко перехватывается анализатором трафика; не рекомендуется к использованию в корпоративных сетях
MD5 authentication	Хэширование пароля (128 бит)	MD5 считается устаревшим алгоритмом, подвержен коллизиям; не защищает IP-заголовки
SHA authentication (RFC 7474)	Криптостойкое хэширование (160-512 бит)	Требует более высокой вычислительной мощности; поддерживается не на всех устройствах
Passive-interface	Отключает рассылку Hello на указанных интерфейсах	Не защищает от атак внутри сегмента, где OSPF должен работать; не предотвращает сниффинг трафика
Отсутствие шифрования в OSPFv2	–	Вся маршрутная информация передаётся открыто; топология сети доступна для пассивного перехвата

Атаки на OSPF можно разделить на три основные категории в зависимости от цели злоумышленника: нарушение доступности (DoS), перенаправление трафика (MITM) и сбор информации о топологии сети. Для удобства рассмотрения категории были разделены на 6 типов основных атак (таблица 2). Наиболее опасными с точки зрения последствий для корпоративной сети являются атаки первых двух типов.

Таблица 2 – Основные типы атак на OSPF

Тип атаки	Краткое описание	Уровень опасности
Внедрение ложного LSA	Злоумышленник рассылает фальшивые LSA с изменёнными параметрами маршрутов	Высокий
MaxAge LSA	Отправка LSA с возрастом 3600 секунд для удаления маршрута из LSDB	Высокий
MaxSequenceNumber	Отправка LSA с максимальным значением sequence number для «перетирания» легитимных записей	Высокий
Подмена DR/BDR	Захват роли Designated Router через объявление максимального приоритета	Средний
Сниффинг	Пассивный перехват OSPF-пакетов для получения карты сети	Средний
Атака на соседство	Установление поддельного соседства для внедрения ложной маршрутной информации	Высокий

Атака MaxAge LSA заключается в отправке специально сформированного LSA-пакета с возрастом 3600 секунд (максимальное значение). В уязвимых реализациях OSPF это приводит к удалению легитимного маршрута из таблицы маршрутизации, что создаёт «чёрную дыру» (отказ в обслуживании). Данная уязвимость подтверждена CVE-2017-8147 и затрагивает даже оборудование Huawei [3]. Внедрение ложного LSA Type 5 позволяет злоумышленнику объявить внешний маршрут с низкой метрикой, что приводит к перенаправлению трафика через атакующий узел. Такая атака даёт возможность перехватывать и анализировать трафик (MITM) (рисунок 1). Атака MaxSequenceNumber (CVE-2017-3224) использует недостатки RFC 2328 при определении «свежести» LSA. Злоумышленник может «перетереть» легитимные записи в LSDB, что приводит к нарушению маршрутизации в домене [4].

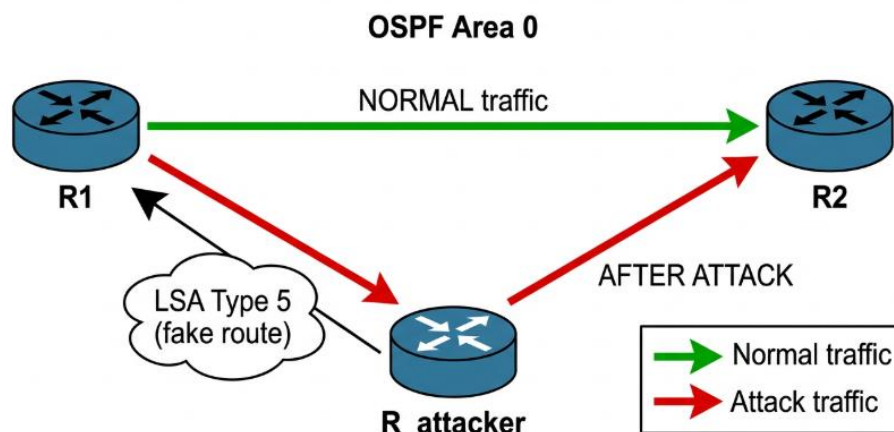


Рисунок 1 – Схема атаки MITM с внедрением ложного маршрута

Для защиты OSPF-домена от рассмотренных выше атак необходим комплексный подход, сочетающий криптографические, фильтрующие и мониторинговые меры. Ни одна из рассмотренных далее мер не является абсолютной, однако их совместное применение значительно снижает риски.

Основной мерой защиты является обязательное включение криптографической аутентификации. Рекомендуется использовать SHA-аутентификацию (RFC 7474) вместо устаревших MD5 и тем более plain text. Для OSPFv3 оптимальным решением является использование IPsec, обеспечивающего не только аутентификацию, но и шифрование всего трафика. Ключи аутентификации необходимо регулярно обновлять с помощью механизма key chain [5]. На интерфейсах, где нет соседей OSPF, следует включать режим passive-interface, который отключает рассылку Hello-пакетов и предотвращает установление поддельных соседств. Дополнительно рекомендуется использовать фильтрацию LSA с помощью distribute-list (inbound) и ограничивать максимальное количество соседей на интерфейс. Для предотвращения resource exhaustion-атак (флуд LSA) на маршрутизаторах следует настраивать CoPP (Control Plane Policing), ограничивающее скорость обработки OSPF-пакетов. На уровне коммутаторов необходимо применять port security и

DHCP snooping, чтобы затруднить физическое подключение злоумышленника в сегмент сети. Для своевременного выявления атак рекомендуется вести логирование изменений соседства (команда log-adjacency-changes), периодически анализировать LSDB на предмет аномальных записей, а также использовать системы IDS/IPS с правилами для обнаружения подозрительных OSPF-пакетов. Перечисленные далее меры защиты в совокупности позволяют существенно снизить вероятность успешной реализации атак на OSPF-домен и минимизировать их последствия для корпоративной сети.

Таблица 3 – Соответствие мер защиты типам атак

Мера защиты	Какие атаки блокирует или обнаруживает
SHA-аутентификация (RFC 7474)	Внедрение ложного LSA, MaxAge, MaxSequenceNumber, подмена DR/BDR
IPsec для OSPFv3	Внедрение ложного LSA, sniffing, подмена DR/BDR
Passive-interface	Установление поддельного соседства, внедрение ложного LSA
Фильтрация LSA (distribute-list)	Внедрение ложного LSA, MaxAge, MaxSequenceNumber
CoPP (Control Plane Policing)	Resource exhaustion (LSA flood)
Логирование и мониторинг LSDB	Обнаружение всех типов атак (постфактум)
Port security на коммутаторах	Физическое подключение злоумышленника, установление соседства

Как мы видим, в современных корпоративных сетях созданы технические возможности для защиты протокола OSPF. Технологии аутентификации и фильтрации совершенствуются, как и методы обнаружения атак. Однако главной проблемой остаётся человеческий фактор – невнимание администраторов к настройке безопасности OSPF. Нарушители активно используют эти упущения, поэтому необходимо регулярно повышать уровень компетенции специалистов в области безопасной настройки протоколов маршрутизации.

Список использованных источников:

1. RFC 2328 – OSPF Version 2 [Электронный ресурс]. – Режим доступа : <https://www.ietf.org/rfc/rfc2328.txt> – Дата доступа : 06.04.2026.
2. Cisco Systems. OSPF Security Recommendations [Электронный ресурс]. – Режим доступа : <https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13689-18.html>. Дата доступа: 06.04.2026.
3. Huawei Security Advisory – MaxAge LSA Vulnerability (CVE-2017-8147) [Электронный ресурс]. – Режим доступа: <https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170720-01-ospf-en> Дата доступа : 06.04.2026.
4. CVE-2017-3224 – OSPF MaxSequenceNumber Vulnerability [Электронный ресурс]. – Режим доступа: <https://cve.ics-sirt.io/cve/CVE-2017-3224> Дата доступа : 08.04.2026.
5. RFC 7474 – OSPF HMAC-SHA Cryptographic Authentication [Электронный ресурс]. – Режим доступа: <https://www.rfc-editor.org/rfc/rfc7474.html> Дата доступа : 08.04.2026.

ОБЗОР СОВРЕМЕННЫХ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ В ОБЛАСТИ ОБНАРУЖЕНИЯ АНОМАЛИЙ В ИНФОРМАЦИОННЫХ СЕТЯХ

Драгунов А.Д., магистрант гр.467421

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Борботько Т.В. – д-р техн. наук, профессор

Аннотация. Рассмотрены современные методы глубокого обучения в области обнаружения аномалий. Описаны возможности, особенности и принцип работы методов, их слабые места и способы их преодоления, достигнутые на рынке.

Ключевые слова: методы глубокого обучения, нейронные сети, обнаружение аномалий.

Введение. С развитием сетевых технологий и появлением Интернета вещей (IoT), структуры информационных сетей становятся более масштабными и комплексными, из-за чего повышается их уязвимость. Атаки нулевого дня, распределенный отказ в обслуживании (DDoS), программы вымогатели и другие угрозы, с которыми вынуждены сталкиваться современные специалисты информационной безопасности, требуют использовать средства защиты сильно превышающие эффективность классических решений в области обнаружения аномалий. Такими решениями стали методы глубокого обучения, которые позволяют обучать различные модели нейронных сетей для обнаружения отклонений от стандартного потока в трафике.

Основная часть. Глубокое обучение это методология в области искусственного интеллекта, основанная на многослойных нейронных сетях, с помощью которой компьютеры учат обрабатывать данные таким же способом, как и человеческий мозг. Каждый слой сети обрабатывает информацию, придавая ей вес при помощи параметров (весов и смещений), оставляя признаки или отбрасывая их посредством функции активации. Функция активации – нелинейное преобразование, определяющее выходной сигнал нейрона на основе суммы его входов перед передачей его дальше. Методы глубокого обучения разработаны для обработки многомерных данных высокой размерности, что позволяет смягчить сложности моделирования отдельных переменных.

Аномалии могут обладать множеством разнообразных характеристик в низкоразмерных данных и могут оставаться незамеченными в многомерном пространстве, что делает идентификацию нелинейных аномалий высокого порядка сложной задачей. В рамках глубокого обучения существует многоуровневый подход к обучению, который позволяет вести обучение на различных уровнях абстракции, нелинейных преобразованиях и признаках, и дающий модели возможность опознавать такие нелинейные аномалии.

Для обнаружения отклонений, методы глубокого обучения используют архитектуру нейронных сетей, за счет чего они могут извлекать признаки (Feature Extraction). Извлечение признаков – это процесс преобразования необработанных высокоразмерных данных в набор информативных числовых характеристик, что снижает размерность данных, устраняет шум и облегчает работу моделей машинного обучения. Признак можно определить как количественно измеримое свойство в наборе данных, которое влияет на стратегию реализации модели. Определяя признаки, можно определить ключевые закономерности или отклонения. Рассмотренные в рамках работы модели глубокого обучения представлены ниже.

Сверточные нейронные сети (CNN) используют слои свертки для определения признаков и хорошо подходят для анализа пространственных данных, так как изначально создавались для задач по распознаванию изображений. CNN зарекомендовали себя как точный инструмент в области обнаружения аномалий, так как в обучении они способны улавливать локальные закономерности и иерархии в больших массивах данных.

Сеть глубоких убеждений (DBN) – многослойная архитектура, разработанная для опознавания абстрактных понятий на более высоких уровнях, в то время как нижние слои позволяют распознавать закономерности. Ключевым компонентом DBN являются ограниченные машины Больцмана (RBM), которые помогают в изучении распределения вероятностей входных данных. Такой подход является стохастическим и использует обратное распространение ошибки для повышения производительности.

Ограниченная машина Больцмана (RBM), являющаяся двухуровневой архитектурой, функционирует путем анализа вероятностного распределения входных данных. Она состоит из видимого и скрытого слоев, при этом разные нейроны в одном и том же слое не могут взаимодействовать, что делает эту модель эффективной в снижении размерности. Наиболее известными вариантами являются бинарные и гауссовские RBM.

Рекуррентные нейронные сети (RNN) разработаны для извлечения признаков из временных рядов и последовательных данных, улавливая временные зависимости и представляя закономерности во времени. Интегрируя RNN с автокодировщиками и долгой краткосрочной памятью (LSTM), увеличивает точность обнаружения аберраций. За счет добавленной памяти RNN способны учитывать прошлые данные, благодаря чему они реагируют на новопоступающие данные, а также данные, обработанные моделью ранее. Этот метод глубокого обучения используется для выявления сложных постоянных угроз (APT), DDoS-атак в сетях Интернета вещей (IoT). Основным отличием RNN от остальных нейронных сетей является наличие узла обратной связи, однако традиционным RNN тяжело с долгосрочными зависимостями из-за исчезновения и взрыва градиента, что может привести к недостаточному обучению моделей и неправильной настройке весов. Для борьбы с этой проблемой были разработаны такие передовые архитектуры, как LSTM и управляемые рекуррентные блоки (GRU), которые интегрируют механизмы управления, которые модулируют поток информации, тем самым повышая эффективность улавливания долгосрочных зависимостей, к примеру, за счет того, что позволяет сети сохранять или отбрасывать информацию по мере необходимости, тем самым смягчая трудности, связанные с проблемой исчезающего градиента.

Автокодировщики это нелинейное обобщение метода главных компонент (PCA), представляющие собой нейронные сети прямого распространения без учителя. Модель обучается для восстановления входных данных и аномалий из сжатой формы, уделяя особое внимание снижению размерности. Нормальный трафик обычно восстанавливается с низкой погрешностью, в то время как аномалии восстанавливаются с большими ошибками, тем самым выделяя себя среди остального набора данных.

Генеративно-сопоставительные сети (GANs) состоят из двух основных компонентов: Генератора (G) и Дискриминатора (D). Функция генератора заключается в создании синтетических данных, тогда как роль дискриминатора – это оценка достоверности этих данных. Генератор получает знания из шума, полученного из набора примеров, в то время как дискриминатор различает искусственные и подлинные образцы. После обучения модели аномалии могут быть выявлены путем сравнения реального сетевого трафика и сгенерированного трафика, тем самым любое существенное отклонение указывает на аномалию. Дискриминатор оценивает эти отклонения, отмечая шаблоны трафика, которые не соответствуют изученному ранее нормальному распределению. Этот подход применяется для обеспечения надежной сетевой безопасности в динамических средах, в частности, в областях, где используется синтез изображений, перевод иностранных языков с помощью технологий искусственного интеллекта и обнаружение аномалий.

Закключение. В ходе работы были рассмотрены современные методы глубокого обучения в области обнаружения аномалий. Описанные методы позволяют значительно усилить защиту против атак нулевого дня, распределенного отказа в обслуживании (DDoS) и др. В настоящее время в области обнаружения аномалий сосредоточены на разработке эффективных и точных моделей глубокого обучения, которые бы обеспечивали баланс между улучшенной производительностью и повышенной интерпретируемостью. Ведется активная разработка гибридных систем (ансамблей) где одновременно используются несколько вариантов обучения модели, достигая тем самым еще более точных результатов в обнаружении отклонений.

Список литературы:

1. Kohli, M., Chhabra, I. A comprehensive survey on techniques, challenges, evaluation metrics and applications of deep learning models for anomaly detection. *Discov Appl Sci* 7, 784 (2025). [Электронный ресурс]. – Режим доступа: <https://doi.org/10.1007/s42452-025-07312-7>.
2. Как устроено глубокое обучение нейросетей [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/articles/918188/>.

КВАДРАТУРНАЯ АМПЛИТУДНАЯ МОДУЛЯЦИЯ (QAM) КАК ОСНОВА СОВРЕМЕННЫХ ВЫСОКОСКОРОСТНЫХ СИСТЕМ СВЯЗИ: АНАЛИЗ УЯЗВИМОСТИ К ОШИБКАМ СИНХРОНИЗАЦИИ

Егоров В.А., студент гр.461401

Белорусский государственный университет информатики и радиоэлектроники¹
г. Минск, Республика Беларусь

Фильченкова – старший преподаватель каф. ЗИ

Аннотация. В данной работе проводится сравнительный анализ квадратурной амплитудной модуляции (QAM) как основы современных систем высокоскоростной передачи данных, таких как Wi-Fi и 5G. Рассматриваются принципы формирования сигнала и использование кода Грея для минимизации битовых ошибок. Основное внимание уделено исследованию устойчивости QAM различного порядка (16, 64, 256) к ошибкам синхронизации фазы и амплитуды в сравнении с QPSK. На основе полученных зависимостей BER определены границы применимости QAM в условиях зашумленного канала и рассинхронизации

Ключевые слова. Квадратурная амплитудная модуляция (QAM), сигнальное созвездие, битовая ошибка (BER), синхронизация фазы, амплитудная ошибка.

Квадратурная амплитудная модуляция (QAM) представляет собой метод передачи информации, сочетающий в себе элементы амплитудной (ASK) и фазовой (PSK) манипуляций. Основным принципом заключается в модуляции двух ортогональных несущих – обычно синусоидальной и косинусоидальной составляющих, называемых синфазной (I) и квадратурной (Q) компонентами. Результирующий сигнал $s(t)$ математически описывается уравнением [1]:

$$s(t) = I_n \cos(2\pi f_c t) - Q_n \sin(2\pi f_c t). \quad (1)$$

Ключевым преимуществом QAM является высокая спектральная эффективность. За счет формирования сигнального созвездия, где каждая точка соответствует уникальной кодовой комбинации, QAM позволяет передавать n бит за один символ, где $M = 2^n$ (M – порядок модуляции). Это обеспечивает кратное увеличение пропускной способности канала в фиксированной полосе частот без расширения занимаемого спектра.

При распределении важно, чтобы небольшой всплеск шума на стороне приемника не привел к большому количеству ошибок в битах. Такое может случиться, если присвоить последовательные значения битов смежным символам. Поэтому для минимизации ошибок важно использовать код Грея при распределении бит. Распределение бит для 16-QAM [2] показано на рисунке 1.

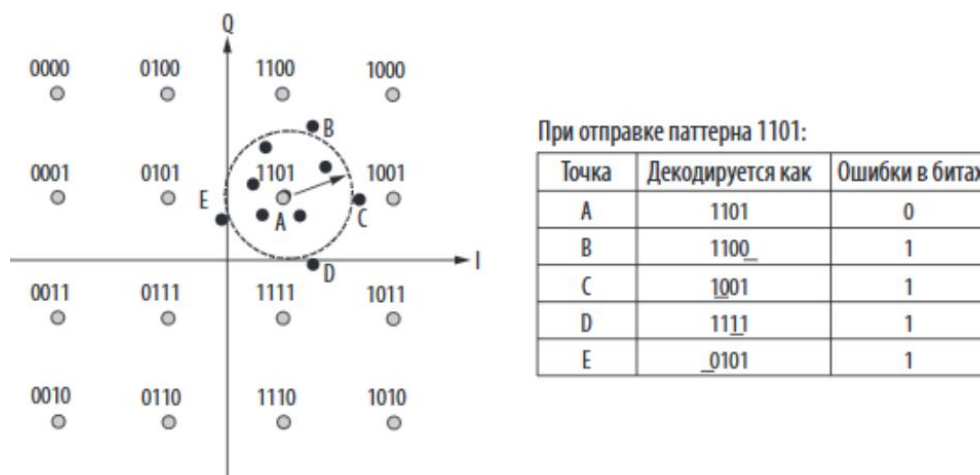


Рисунок 1 – Созвездие 16-QAM модуляции

Добавим аддитивный белый шум в канал связи. Для наглядности добавим шум так, чтобы отношение сигнал/шум (SNR) было равно 30. При этом показатель BER стремится к 0. Кроме шума в каналах связи также возникают ошибки синхронизации фазы и амплитуды, что также негативно сказывается при демодуляции сигнала. Визуализации переданных данных с ошибками синхронизации по фазе на 10 градусов (рисунок 2а) и по амплитуде в 0.7 (рисунок 2б) с учетом воздействия аддитивного белого шума.

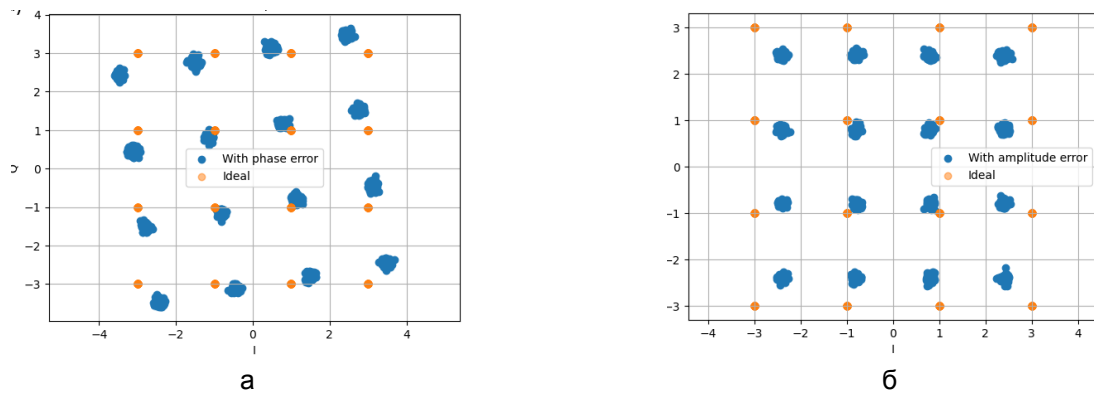


Рисунок 2 – Визуализация полученных точек при демодуляции с ошибкой синхронизации фазы на 10 градусов (а); и амплитуды в 0,8 раза (б)

Построим графики зависимости ошибки приема BER в зависимости от коэффициентов рассинхронизации фазы и амплитуды. Из графика зависимости ошибки BER от ошибки синхронизации амплитуды (рисунок 3, а) видно, что оптимальное отклонение амплитуды фазы составляет от 0,75 до 1.7 раз (при SNR=30).

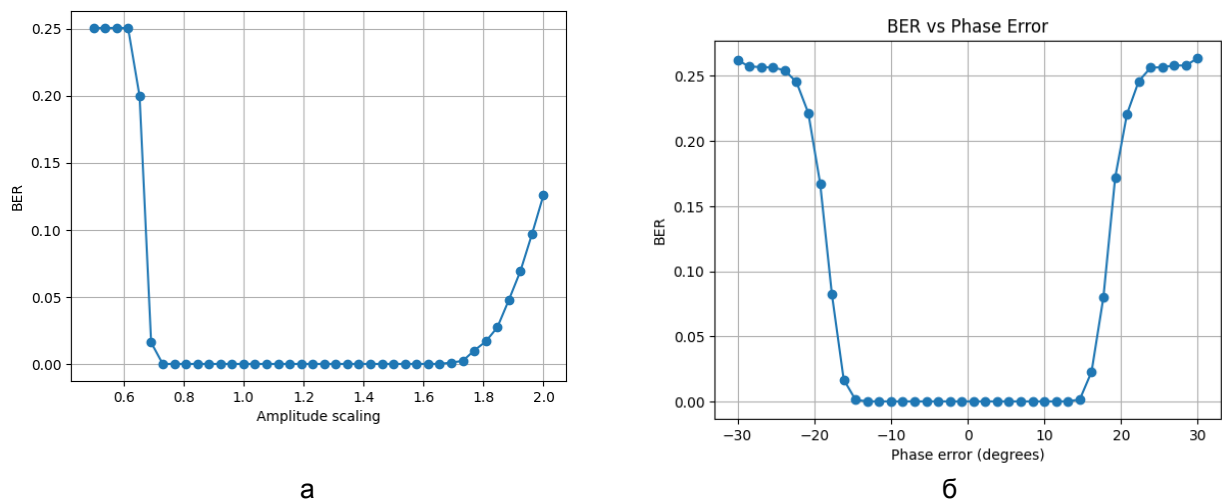


Рисунок 3 – Зависимость ошибки приема (BER) от отклонения амплитуды (а) и отклонения фазы (б)

Из графика зависимости ошибки BER от ошибки синхронизации фазы, изображенного на рисунке 3, б, видно, что допустимое отклонение фазы, при SNR=30, не превышает 15 градусов.

Но в настоящих системах связи редко встречаются случаи ошибки синхронизации только фазы или только амплитуды, поэтому стоит рассмотреть систему, на которую действует одновременно отклонение и фазы, и амплитуды. Значение ошибки приема BER в зависимости от ошибки синхронизации фазы и амплитуды изображены на рисунке 5.

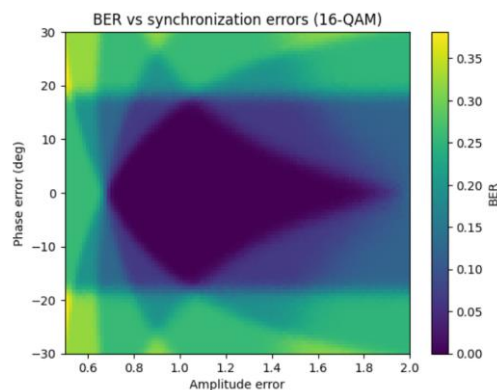


Рисунок 5 – Зависимость ошибки приема (BER) от отклонения фазы и амплитуды для 16-QAM

Сравним полученный график с аналогичным, построенным для QPSK (квадратурной фазовой модуляции). Тепловая карта зависимости ошибки приема BER от ошибки синхронизации амплитуды и фазы представлен на рисунке 6.

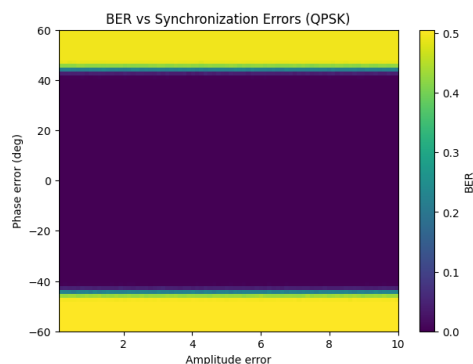


Рисунок 6 – Зависимость ошибки приема (BER) от отклонения фазы и амплитуды для QPSK

При анализе и сравнении рисунков 5 и 6 видно, что QPSK устойчива к ошибкам синхронизации амплитуды и допускает отклонение ошибки и устойчив к ошибке синхронизации фазы вплоть до отклонения в 40 градусов. 16-QAM в свою очередь предоставляет возможность передать за промежуток времени в два раза больше информации, но и устойчивость к ошибкам синхронизации у квадратурной амплитудной модуляции ниже.

Нарастивая разрядность QAM модуляции (64-QAM, 1024-QAM), устойчивость к ошибкам синхронизации становится значительно ниже, что видно из рисунка 7.

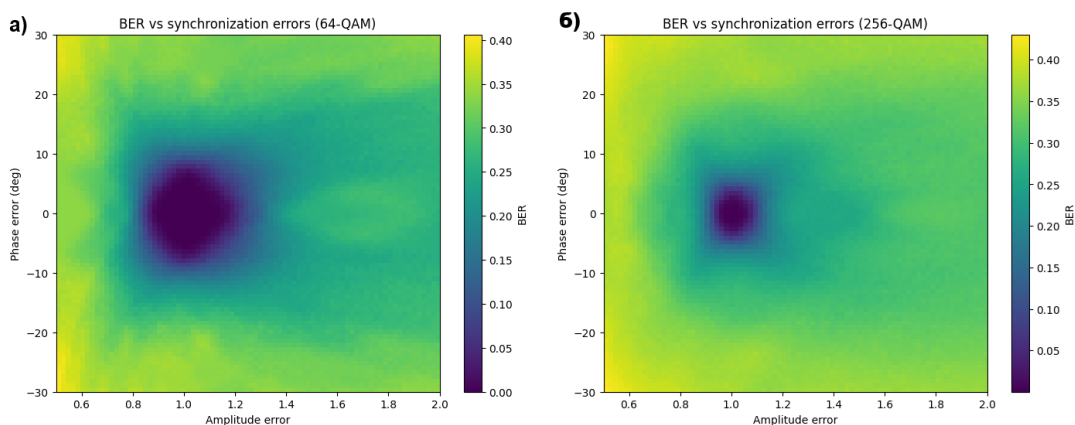


Рисунок 7 – Зависимость ошибки приема (BER) от отклонения фазы и амплитуды для а) 64-QAM; б) 256-QAM

Современные технологии и стандарты всё чаще применяют квадратурную амплитудную модуляцию. На её основе работают такие технологии как Wi-Fi (EIII 802.11ac/ax), 4G-LTE, 5G, которые способны обеспечить высокую пропускную способность. Но такие системы уязвимы к ошибкам синхронизации и зашумления канала связи [3].

Таким образом, если канал связи защищен от сильного воздействия помех, а модулятор и демодулятор синхронизированы, тогда QAM модуляция – хорошее решение. Когда стоит вопрос о передаче сигнала в условиях сильного шума и возможных ошибках синхронизации, стоит воздержаться от использования квадратурной амплитудной модуляции в пользу более простых, но помехоустойчивых видов модуляции.

Список использованных источников:

1. Сергиенко А. Б. Цифровая обработка сигналов : учебник для вузов. – СПб. : Питер, 2002.. – 608 с.
2. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Н. Фимстер, Д. Уэзеролл. – 6-е изд. – Санкт-Петербург : Питер, 2024. - 992 с.
3. Цифровая связь: теоретические основы и практическое применение / Бернард Скляр. - 2-е изд.. – Москва [и др.] : Вильямс, 2017. - 1099 с.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ ГЕНЕРАЦИИ ОДНОРАЗОВЫХ ПАРОЛЕЙ

Каршакевич В.М., студент гр.567001

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

*Бойправ О.В. – канд. тех. наук, доцент,
заведующий кафедрой защиты информации*

Аннотация. Статья посвящена комплексному исследованию современных технологий генерации одноразовых паролей (One-Time Password), которые в настоящее время широко используются для повышения эффективности процесса аутентификации пользователей в информационных системах. В рамках этого исследования проведен анализ алгоритмов HOTP (HMAC-Based One-Time Password Algorithm), TOTP (Time-based One-Time Password), а также методов, используемых для передачи одноразовых паролей. Представлены рекомендации по совершенствованию систем генерации одноразовых паролей, разработанные с учетом результатов проведенного исследования.

Ключевые слова. одноразовый пароль, HOTP, TOTP, аутентификация, информационная безопасность, двухфакторная аутентификация.

Информационные системы на данный момент используют повсеместно: они помогают хранить данные, автоматизировать рутину в бизнесе, налаживать электронный документооборот, управлять ресурсами компании, а также оказывать услуги онлайн. Одним из ключевых методов защиты информации, обрабатываемой в информационных системах, является аутентификация их пользователей.

Многие устоявшиеся методы аутентификации, использующие статические пароли, имеют ряд недостатков, такие как уязвимости каналов передачи одноразовых паролей, возможность реализации атак перехвата и воспроизведения, зависимость некоторых алгоритмов от синхронизации времени, а также необходимость хранения секретных ключей на серверной стороне. Кроме того, существенную угрозу представляют атаки социальной инженерии, при которых пользователь может самостоятельно передать одноразовый пароль злоумышленнику. Такого рода исследования позволяют не только определить проблемные участки, но также найти метод для улучшения.

Цель работы – выполнить анализ уязвимостей современных систем генерации одноразовых паролей и по результатам этого анализа предложить пути совершенствования таких систем.

Для достижения поставленной цели были поставлены следующие задачи:

- анализ современных алгоритмов генерации одноразовых паролей;
- исследование основных угроз и атак на системы генерации одноразовых паролей;
- оценка криптографической стойкости одноразовых паролей;
- сравнительный анализ методов генерации одноразовых паролей;
- разработка рекомендаций по совершенствованию систем генерации одноразовых паролей.

Характеристики атак на системы генерации одноразовых паролей представлены ниже.

Атаки перехвата (eavesdropping) направлены на получение одноразового пароля в процессе его передачи по каналу связи. Несмотря на ограниченный срок действия одноразового пароля, злоумышленник может использовать его в реальном времени, особенно при реализации атаки типа «man-in-the-middle». В этом случае безопасность системы зависит не только от алгоритма генерации одноразового пароля, но и от защищенности канала передачи [1].

Атаки воспроизведения (replay attacks) заключаются в повторном использовании перехваченного пароля. Большинство систем генерации одноразовых паролей защищены от данного типа атак благодаря одноразовому характеру паролей, однако при наличии временного окна (например, в алгоритме TOTP) существует вероятность успешного повторного использования в пределах допустимого интервала. Дополнительную угрозу создают атаки с опережением по времени (time-shift attacks), когда злоумышленник искусственно рассинхронизирует время на устройстве жертвы и сервере [2].

Существенную угрозу представляют атаки на серверную сторону. В случае компрометации базы данных злоумышленник может получить доступ к секретным ключам (в алгоритмах HOTP и TOTP), что позволяет ему генерировать валидные одноразовые пароли. Это является одним из наиболее критичных недостатков классических систем генерации одноразовых паролей, так как делает скомпрометированным весь будущий сеанс аутентификации [3].

Отдельную категорию составляют атаки социальной инженерии, включая фишинг. Даже при использовании одноразового пароля пользователь может быть обманут и самостоятельно передать одноразовый пароль злоумышленнику. Особенно опасны фишинговые сайты, которые в реальном времени проксируют трафик между жертвой и легитимным сервисом (атака «человек посередине» с перехватом сессии), что позволяет злоумышленнику использовать полученный одноразовый пароль мгновенно, до его истечения.

Большинство одноразовых паролей передаются через SMS, мессенджеры или электронную почту. Протокол SS7 (Signaling System № 7), используемый в сотовой связи, имеет фундаментальные уязвимости, позволяющие злоумышленникам перенаправлять SMS с одноразовыми паролями на свои устройства без физического доступа к SIM-карте жертвы. Таким образом, даже криптографически стойкий алгоритм генерации пароля теряет свою эффективность при использовании небезопасного канала доставки [4].

Таким образом, анализ модели угроз показывает, что повышение безопасности систем генерации одноразовых паролей требует комплексного подхода, включающего как совершенствование алгоритмов генерации, так и защиту каналов передачи и пользовательских сценариев.

Криптографическая стойкость систем генерации одноразовых паролей во многом определяется длиной пароля и используемыми алгоритмами. Как правило, одноразовые пароли представляют собой числовые значения длиной от 6 до 8 символов. Общее количество возможных комбинаций можно оценить как:

$$N = 10^d, \quad (1)$$

где d – количество цифр в пароле.

Для шестизначного одноразового пароля количество возможных значений составляет $10^2 = 1000000$. При отсутствии ограничений на количество попыток это делает систему уязвимой к перебору (brute force). Однако на практике применяются механизмы ограничения числа попыток и временные задержки, что существенно снижает вероятность успешной атаки.

Вероятность угадывания одноразового пароля за одну попытку определяется как:

$$P = \frac{1}{10^d} \quad (2)$$

При наличии ограничения на число попыток k , вероятность успешной атаки может быть оценена как:

$$P_k = \frac{k}{10^d} \quad (3)$$

Однако современные распределенные атаки (например, с использованием ботнетов) позволяют злоумышленникам обходить ограничения на количество попыток, распределяя запросы между различными IP-адресами. В связи с этим увеличение длины одноразового пароля (например, до 8-10 символов) становится необходимой, но не достаточной мерой.

Дополнительным фактором является энтропия секретного ключа. В алгоритмах HOTP и TOTP безопасность напрямую зависит от стойкости ключа K и используемой хеш-функции (например, SHA-1, SHA-256). При использовании современных криптографических примитивов вероятность подбора ключа остается пренебрежимо малой [3].

В случае хеш-цепочек безопасность определяется стойкостью хеш-функции к преобразованию (preimage resistance) и коллизиям. Использование современных функций (например, SHA-256) обеспечивает высокий уровень защиты при условии корректной реализации [5].

Сравнение рассмотренных методов позволяет выделить их ключевые характеристики с точки зрения безопасности и практической применимости.

Алгоритмы HOTP и TOTP отличаются простотой реализации и широким распространением, однако требуют хранения секретного ключа на сервере. Это делает их уязвимыми при компрометации серверной базы данных. Кроме того, алгоритм TOTP критически зависит от точности синхронизации времени. При расхождении часов сервера и клиента более чем на допустимый интервал (обычно 30–60 секунд) аутентификация становится невозможной без ручного вмешательства.

Методы на основе хеш-цепочек, напротив, минимизируют необходимость хранения секретных данных на сервере, что повышает устойчивость к утечкам. Однако они уступают по удобству использования из-за необходимости управления цепочками и их ограниченной длины. После исчерпания цепочки требуется повторная инициализация, что снижает удобство для пользователя.

С точки зрения устойчивости к атакам можно отметить, что: алгоритм HOTP уязвим к рассинхронизации счетчика; алгоритм TOTP зависит от точности времени и подвержен атакам с использованием временных окон; хеш-цепочки ограничены по ресурсу использования и требуют сложного механизма восстановления; все методы подвержены атакам перехвата при отсутствии защищенного канала.

Таким образом, ни один из подходов не является универсальным решением, что подтверждает необходимость разработки комбинированных моделей, компенсирующих недостатки друг друга.

Реализация комбинированной системы генерации одноразовых паролей требует учета ряда практических аспектов.

Безопасная инициализация. Во-первых, необходимо обеспечить безопасную инициализацию системы, включая генерацию исходного секретного значения и начального элемента хеш-цепочки. Инициализация должна происходить в защищенной среде (например, с использованием протокола

TLS 1.3) с проверкой подлинности сервера, чтобы исключить возможность внедрения злоумышленником собственных параметров в процессе первоначальной настройки [6].

Выбор функции вывода ключей (KDF). Во-вторых, важным является выбор функции вывода ключей. Она должна обладать свойствами устойчивости к атакам перебора (brute-force) и обеспечивать равномерное распределение выходных значений. В качестве таких функций могут использоваться PBKDF2, HKDF или Argon2. Argon2 рекомендуется к использованию в новых системах благодаря устойчивости к атакам с использованием GPU и ASIC [4].

Производительность и масштабируемость. В-третьих, необходимо учитывать производительность системы. Добавление нескольких факторов (хеш-цепочка, время, идентификатор сессии) в процесс генерации одноразового пароля увеличивает вычислительную нагрузку. Для высоконагруженных систем критически важно использовать эффективные алгоритмы или распределение вычислений.

Защита от атак повторного воспроизведения. Также следует уделить внимание защите от атак повторного воспроизведения. Для этого одноразовый пароль должен быть привязан не только к времени, но и к конкретной сессии или контексту аутентификации. Это может быть реализовано путем включения дополнительного параметра (например, идентификатора сессии или уникального nonce) в функцию генерации. Такой подход делает перехваченный пароль бесполезным для злоумышленника.

На основе проведенного анализа предлагаются следующие рекомендации по усовершенствованию системы генерации одноразовых паролей.

1. Отказ от SMS как канала доставки. В случае высоких требований к безопасности (финансовый сектор, государственные информационные системы) следует использовать push-уведомления в защищенных приложениях или аппаратные токены, исключающие перехват через уязвимости SS7.

2. Многофакторность генерации. Генерировать одноразовый пароль на основе комбинации трех факторов: секретного ключа (хранящегося в защищенном элементе TPM на устройстве пользователя), временной метки (ограниченной окном в 15-30 секунд) и идентификатора сессии.

3. Защита серверной стороны. Секретные ключи на сервере не должны храниться в открытом виде. Использование аппаратных модулей безопасности (HSM) или методов разделения секрета (threshold cryptography) позволяет исключить компрометацию всей системы при взломе одной из баз данных [3].

4. Адаптивная политика ограничений. Внедрение адаптивных механизмов блокировки, которые увеличивают задержку при неудачных попытках не линейно, а экспоненциально, а также учитывают геолокацию и поведенческие факторы пользователя.

Дальнейшие исследования могут развиваться по следующим направлениям.

1. Интеграция с биометрией. Одним из перспективных направлений является интеграция одноразовый пароль с биометрическими факторами аутентификации, что позволяет создать многоуровневые системы защиты. Биометрические данные могут выступать в роли фактора владения (после первичной регистрации) или использоваться для динамической генерации ключа.

2. Аппаратные средства безопасности. Другим направлением является использование аппаратных средств, таких как токены безопасности (U2F/WebAuthn) и Trusted Platform Module (TPM), для хранения секретных данных и выполнения криптографических операций. В отличие от программных одноразовых паролей-генераторов, аппаратные средства исключают возможность извлечения ключа даже при заражении устройства пользователя вредоносным ПО.

3. Применение машинного обучения. Кроме того, интерес представляет применение методов машинного обучения для выявления аномалий в процессе аутентификации. Это позволяет дополнительно повысить уровень безопасности за счет анализа поведения пользователя (тайминг нажатия клавиш, характерные местоположения, типичные устройства).

4. Постквантовая криптография. Наконец, развитие постквантовой криптографии может оказать влияние на алгоритмы генерации одноразовых паролей. Алгоритмы, основанные на цепочках хешей (которые устойчивы к квантовым атакам в большей степени, чем асимметричные схемы), могут стать основой для будущих стандартов аутентификации в постквантовый период [5].

Список использованных источников:

1. HOTP: An HMAC-Based One-Time Password Algorithm / D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, O. Ranen // RFC 4226. – 2005. – 34 p.
2. TOTP: Time-Based One-Time Password Algorithm / D. M'Raihi, S. Machani, M. Pei, J. Rydell // RFC 6238. – 2011. – 14 p.
3. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes / J. Bonneau, C. Herley, P. C. van Oorschot, F. Stajano // Proceedings of the IEEE Symposium on Security and Privacy. – 2012. – P. 553–567.
4. Digital Identity Guidelines: Authentication and Lifecycle Management / P. A. Grassi, M. E. Garcia, J. L. Fenton // NIST Special Publication 800-63B. – 2017. – 77 p.
5. Post-quantum cryptography / D. J. Bernstein, T. Lange // Nature. – 2017. – Vol. 549, No. 7671. – P. 188–194.
6. The Transport Layer Security (TLS) Protocol Version 1.3 / E. Rescorla // RFC 8446. – 2018. – 160 p.

РАЗРАБОТКА ОБУЧАЮЩЕЙ ИГРЫ ДЛЯ ФОРМИРОВАНИЯ НАВЫКОВ ПО ЗАЩИТЕ ОТ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Клиндухов Я.А., Мажаева С.Д.

Национальный детский технопарк, г. Минск, Республика Беларусь

*Бойправ О.В. – канд. тех. наук, доцент,
заведующий кафедрой защиты информации*

Аннотация. В статье выявлены основные проблемы разработки обучающих игр для подготовки специалистов по информационной безопасности: баланс обучения и геймплея, моделирование угроз, интеграция актуальных таксономий, оценка эффективности и техническая реализация. Предложен алгоритм создания игры, состоящий из девяти шагов. Описана реализация игры на языке программирования Python. Результаты апробации обучающей игры показали прирост среднего балла более чем на 20%, что подтверждает эффективность предложенного подхода.

Ключевые слова. обучающие игры, разработка обучающих игр, алгоритм создания обучающих игр, Cyber Kill Chain, моделирование угроз информационной безопасности, подготовка специалистов в области информационной безопасности.

В условиях стремительной цифровизации всех сфер жизни Республики Беларусь наблюдается значительный рост угроз информационной безопасности [1–3]. Согласно исследованиям Ponemon Institute, 75% инцидентов в более чем 310 компаниях по всему миру связаны именно с ошибками пользователей информационных систем. В таких условиях появляется значительный разрыв между техническими возможностями программных средств защиты информации и реальными навыками пользователей по их применению. Одним из наиболее эффективных инструментов преодоления этого разрыва выступают обучающие игры, однако их разработка сопряжена с рядом системных проблем, без решения которых обучающая игра теряет как образовательную, так и игровую ценность. Целью данной работы является выявление ключевых проблем разработки обучающих игр по информационной безопасности, предложение алгоритма их преодоления и апробация полученного решения.

Под обучающей игрой будем понимать компьютерную программу, которая разработана специально для обучения определенным предметам или навыкам [4]. Отличие обучающей игры от компьютерной заключается в получении обучающимися новых специальных знаний, наличии четкой учебной цели и педагогического результата, в то время как компьютерная игра фокусируется на развлечении, хотя и может иметь побочный образовательный эффект.

Также, обучающие игры имеют эффективное применение в области информационной безопасности, так как они позволяют моделировать реальные угрозы информационной безопасности, формируя необходимые практические и теоретические навыки. Большинство таких игр носят симуляционный характер, моделируя обучающемуся ситуацию, похожую на реальную. Особенностью таких симуляторов является возможность генерации конкретных угроз информационной безопасности, таких как внедрение вредоносного кода в процессы, использование легитимных учетных записей, почтовый фишинг и другие. Такой подход обеспечивает высокую заинтересованность обучающегося в процессе, позволяя добиться высокой эффективности обучения в короткие сроки. Кроме того, специалистам по защите информации часто требуется поиск неординарных решений, а игровые технологии способствуют развитию творческого потенциала и стратегического мышления, необходимого для решения задач проектирования и защиты информационных систем.

На основе анализа литературных данных и собственного опыта разработки обучающей игры выделены пять основных проблем, возникающих при создании обучающих игр в области информационной безопасности. Первая проблема – это баланс между обучением и геймплеем. Чрезмерное преобладание теории снижает степень заинтересованности игрой, в то время как избыточная игровая составляющая без требуемого образовательного наполнения не формирует нужных знаний и навыков.

Вторая проблема заключается в правильном моделировании реальных угроз – слишком упрощенные сценарии не дают практических навыков, что ограничивает их применение в учебном процессе. Третья проблема связана с интеграцией актуальных моделей атак: большинство существующих обучающих игр используют устаревшие или разрозненные данные об угрозах информационной безопасности и не имеют привязки к общепризнанным базам знаний, таким как MITRE ATT&CK.

Четвёртая проблема касается оценки эффективности обучения – без встроенных механизмов тестирования и сбора метрик практически невозможно измерить прирост знаний после прохождения игры. Из-за этого игрок может перейти к последующим этапам игры, не получив и не закрепив

полученные знания. Наконец, пятая проблема носит технический характер и связана с выбором языка программирования и фреймворка, которые должны обеспечивать быструю разработку, кроссплатформенность и работу на ограниченных вычислительных ресурсах. Для системного решения перечисленных проблем разработан и апробирован алгоритм создания обучающей игры по информационной безопасности, состоящий из девяти этапов, приведенный на рисунке 1.



Рисунок 1 – Алгоритм создания обучающей игры в области информационной безопасности

Первым шагом идёт анализ целевой аудитории, в ходе которого определяется уровень подготовки будущих игроков – школьники, студенты или действующие сотрудники. Вторым шагом является выбор модели угроз. Третьим шагом определяется жанр игры: на основе анализа литературы, наиболее эффективным оказался жанр симулятора, поскольку он позволяет максимально приблизить ситуацию к реальной работе специалиста.

Четвёртый шаг – разработка сценария, включающего детальную проработку сюжетной линии игры, роли персонажей, интерфейса пользователя и разбиение на дни или уровни сложности. Пятый шаг предполагает выбор программных средств разработки: языка программирования, конкретного фреймворка, системы управления базами данных и графических средств. Шестой шаг – реализация игровых механик, а именно разработанный геймплей должен сочетать в себе баланс графической составляющей и реализации выбранных угроз. Седьмым шагом внедряются обучающие элементы: встроенная справочная система, например в виде браузера, тесты для самопроверки и контекстные подсказки.

Восьмой шаг является рекомендуемым всем обучающим играм, в которых реализуются атаки на информационные системы, и заключается в интеграции модели нарушителя Cyber Kill Chain: каждая учебная угроза должна быть привязана к конкретному этапу цепочки атаки [5]. Девятым, заключительным шагом алгоритма выступает апробация разработанной игры и оценка её эффективности с помощью тестирования до и после прохождения.

Модель Cyber Kill Chain, предложенная компанией Lockheed Martin, описывает семь последовательных этапов кибератаки: разведка, вооружение, доставка, эксплуатация, установка, получение управления и действие нарушителя. В разработанной нами игре каждая учебная угроза сопоставляется с конкретным этапом этой цепочки. Например, фишинговая атака относится к этапу доставки, поскольку злоумышленник доставляет вредоносную ссылку или вложение. Использование легитимных учётных записей соответствует этапу эксплуатации, когда нарушитель уже получил доступ к системе и использует штатные средства. Внедрение вредоносного кода в процессы операционной системы относится к этапу установки. Такая привязка позволяет игроку не просто выбирать средство защиты, а осознанно понимать, на каком этапе развития атаки применяется то или иное программное средство – межсетевой экран, антивирус, SIEM-система или средство резервного копирования.

Для практической реализации описанного алгоритма был выбран язык программирования Python версии 3.14.0 и фреймворк Pygame версии 2.5.0, что позволило создать игровой проект, не требующий больших вычислительных ресурсов. Жанр игры определён как симулятор практических задач специалиста отдела информационной безопасности организации. Сюжет игры следующий: игрок выступает в роли нового сотрудника отдела информационной безопасности вымышленной компании «ТехноПро», и все действия происходят внутри интерфейса персонального компьютера, состоящего из различных программ, с которыми игроку предстоит взаимодействовать – SIEM-система, антивирусная программа, система анализа трафика и другие. Игра состоит из четырёх дней, причём алгоритм каждого дня един и соответствует этапам модели Cyber Kill Chain. Сначала одна из программных систем персонального компьютера уведомляет игрока об обнаружении нестандартного поведения некоторого процесса и просит выявить его среди легитимных процессов. После выявления вредоносного процесса начинается расследование угрозы, при котором игроку требуется детально изучить признаки угрозы, алгоритм её работы и методы борьбы. Важно отметить, что с каждым днём угрозы информационной безопасности меняются и их уровень возрастает, последовательно проходя этапы Cyber Kill Chain от доставки до действий нарушителя. После выполнения всех этапов обучающей игры игрок проходит тестирование по теме отражённой атаки, после чего ему выводится количество правильных ответов и, при необходимости, рекомендация повторения теоретического материала во встроенном интернет-браузере, где собраны сведения об всех угрозах из матрицы MITRE ATT&CK.

Для количественной оценки эффективности разработанной обучающей игры было проведено тестирование среди 38 учащихся Национального детского технопарка по образовательным направлениям «лазерные технологии», «электроника и связь», «информационные и компьютерные технологии» и «инженерная экология». Методика апробации включала сбор первичных знаний по теме угроз информационной безопасности в виде тестирования с выбором из четырёх вариантов ответов, всего десять вопросов, поэтому оценка осуществлялась по десятибалльной системе. Затем участникам было предложено полностью пройти игру, после чего они повторно прошли те же самые десять вопросов для выявления вторичных знаний. Результаты тестирования до прохождения игры представлены на рисунке 2, а результаты после тестирования представлены на рисунке 3.

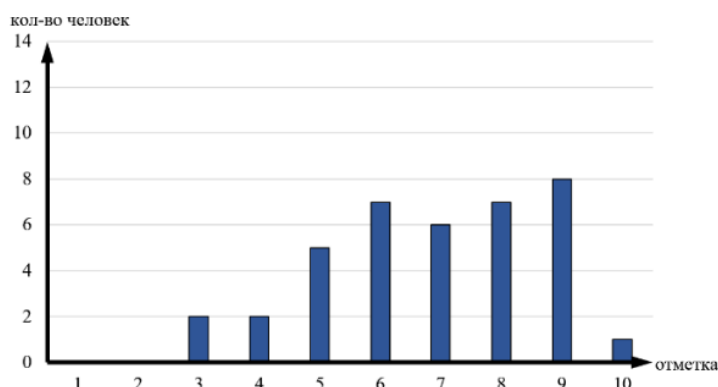


Рисунок 2 – Распределение оценок до прохождения обучающей игры

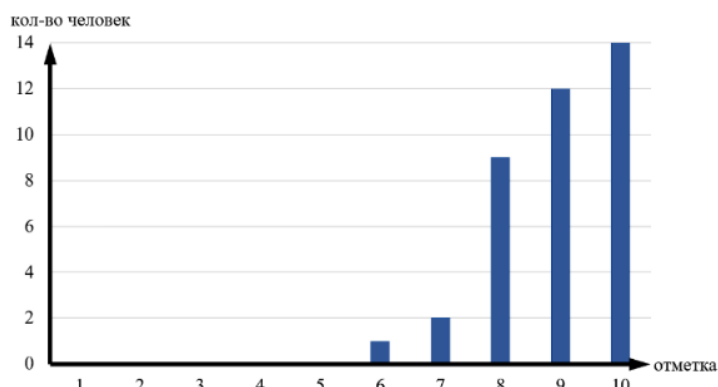


Рисунок 3 – Распределение оценок после прохождения обучающей игры

Результаты тестирования показали, что до прохождения игры средний балл составил 6,87, тогда как после прохождения игры средний балл повысился до 8,95. Таким образом, прирост среднего балла составил 2,08, что говорит об увеличении среднего балла более чем на 20%. Полученные результаты свидетельствуют о высокой эффективности разработанной обучающей игры.

Кроме того, отзывы участников исследования говорят о высоком уровне заинтересованности обучающей игрой, что выгодно отличает её среди других видов обучающих материалов.

В ходе проведённого исследования были выявлены пять ключевых проблем разработки обучающих игр в области информационной безопасности: баланс между обучением и геймплеем, адекватное моделирование реальных угроз, интеграция актуальных моделей атак, оценка эффективности обучения и техническая реализация. Для преодоления этих проблем предложен и апробирован формализованный девятишаговый алгоритм создания обучающей игры, обязательным элементом которого выступает интеграция модели Cyber Kill Chain. Разработанный на основе этого алгоритма симулятор практических задач специалиста отдела информационной безопасности позволил реализовать интерактивный подход к обучению, где каждая угроза привязана к конкретному этапу цепочки атак. Результаты экспериментальной апробации, проведённой среди учащихся Национального детского технопарка, подтвердили высокую эффективность разработанной обучающей игры: прирост среднего балла успеваемости составил более 20%. Таким образом, обучающие игры, созданные по предложенному алгоритму, могут быть эффективным средством для подготовки специалистов в области защиты информации, обеспечивая высокую вовлечённость обучающихся и развивая аналитическое и стратегическое мышление.

Список использованных источников:

1. Барило К. С., Нестеренков С. Н., Бегляк Е. В. (2025) Криптографические методы защиты информации в сфере электронного документооборота. *Технические средства защиты информации*. 66–69.
2. Мырадов П. С., Мырадов П. С. (2025) Технические средства защиты информации: современные технологии, методы и перспективы. *Технические средства защиты информации*. 260–263.
3. Дроздов М. М., Прудник А. М. (2017) Анализ состояния и методология обеспечения безопасности информационных систем. *Технические средства защиты информации*. 15–16.
4. Рябинин Н. С. (2025) Многофункциональный веб-сервис для тестирования и интерактивных игр с использованием искусственного интеллекта. *Радиотехника и электроника*. 171–175.
5. Борботько Т. В., Бойправ О. В., Тимофеев А. М. (2025) Основы информационной безопасности. Минск, Издательство «БГУИР».

СИНЕРГЕТИЧЕСКИЙ ЭФФЕКТ ПРИ КОМБИНИРОВАНИИ РАЗНОРОДНЫХ КИБЕРАТАК

Ковалевич М.А., студент гр.361401

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Мокеров В.С. – ассистент каф. ЗИ

Аннотация. В работе выполнен теоретический анализ синергетического эффекта при комбинировании разнородных кибератак. Показано, что эффективность композитных атак превышает сумму эффективностей отдельных компонентов, что противоречит традиционным аддитивным моделям. Выявлен эффект композитного перехода – существование пар атак, безопасных по отдельности, но критических в комбинации. Предложена классификация типов синергии по механизму взаимодействия. На основе анализа реальных примеров обоснована необходимость перехода от изолированных средств защиты к кросс-слойной корреляции событий в системах мониторинга безопасности.

Ключевые слова. кибератаки, синергетический эффект, композитные атаки, корреляция событий.

Синергия в кибератаках возникает при объединении различных методов (технических, социальных, психологических), где совокупный эффект превышает сумму действий по отдельности. Ключевые механизмы включают многоступенчатые (APT) атаки, комбинирование фишинга с эксплойтами, использование ботнетов для усиления DDoS, и одновременное воздействие на инфраструктуру и персонал [1].

Ключевым недостатком большинства систем безопасности является отсутствие корреляции разнородных событий. Каждый инцидент анализируется автономно, что исключает возможность обнаружения многоступенчатых атак, проявляющихся только через последовательность событий различных типов.

Синергетический эффект при комбинировании разнородных кибератак возникает вследствие четырех основных механизмов. Первый – ослабление защиты: злоумышленники отключают системы логирования и очищают журналы событий, что снижает эффективность средств обнаружения [2]. Второй – отвлечение внимания: DDoS-атаки служат прикрытием для кражи данных или повышения привилегий, перегружая центры мониторинга безопасности [3]. Третий – сокрытие следов: использование легитимных инструментов ОС (Living Off the Land) и отключение логирования веб-серверов позволяют маскировать вредоносную активность [4]. Четвертый – обход разных слоев защиты: антивирус, файрвол и DLP работают изолированно, а комбинированная атака использует разрывы между ними [5].

Для рассмотрения синергии в кибератаках были выбраны следующие виды кибератак: фишинг, Pass-the-Hash, DDoS, эксфильтрация данных, отключение логирования, эксплуатация уязвимости. В таблице 1 представлена эффективность кибератак по отдельности и в комбинации.

Фишинг представляет собой метод социальной инженерии, при котором злоумышленник создает поддельное электронное письмо, веб-сайт или сообщение, имитирующее легитимную организацию (банк, корпоративный портал, сервис электронной почты). Жертву побуждают перейти по вредоносной ссылке, открыть зараженное вложение или ввести свои учетные данные на поддельной странице. В результате фишинг позволяет злоумышленнику получить доступ к учетным данным жертвы или установить вредоносное программное обеспечение на ее компьютере. Pass-the-Hash (PtH) – это техническая атака, при которой злоумышленник использует хеш пароля пользователя для аутентификации на удаленных системах. В операционных системах Windows хеши паролей хранятся в памяти процесса LSASS или на диске в файле SAM. PtH позволяет атакующему, имеющему хеш, подключаться к другим компьютерам в сети, выдавая себя за легитимного пользователя. Фишинг и PtH образуют последовательную цепочку. Сначала фишинговая атака позволяет получить доступ к рабочей станции и извлечь хеш пароля. Затем, имея хеш, злоумышленник применяет PtH для аутентификации на других компьютерах в сети – серверах, рабочих станциях коллег, контроллерах домена. Каждый новый скомпрометированный компьютер дает новые хеши, что позволяет двигаться дальше.

DDoS-атака (Distributed Denial of Service) – это атака, при которой злоумышленник использует сеть зараженных устройств (ботнет) для отправки огромного количества запросов к целевой системе. Цель – перегрузить вычислительные ресурсы, пропускную способность канала или сетевые сервисы, сделав их недоступными для легитимных пользователей. DDoS-атака генерирует десятки тысяч оповещений в секунду, перегружая центры мониторинга безопасности (SOC). Эксфильтрация данных – это несанкционированное копирование, передача или выгрузка конфиденциальной информации за пределы контролируемой сети. Злоумышленник может использовать легитимные протоколы (HTTP, HTTPS, DNS, FTP), облачные хранилища или скрытые каналы связи. Эксфильтрация требует времени (особенно при больших объемах данных) и создает аномальный

сетевой трафик, который может быть обнаружен DLP-системами, анализаторами трафика или специалистами SOC. DDoS-атака запускается одновременно с эксфильтрацией или незадолго до нее. Массовый поток оповещений от DDoS перегружает SOC – специалисты вынуждены обрабатывать тысячи ложных срабатываний, отвлекаться на восстановление доступности сервисов. На этом фоне эксфильтрация данных остается незамеченной, так как ее трафик теряется в общем шуме. Кроме того, аномалии, связанные с эксфильтрацией, могут быть ошибочно отнесены к последствиям DDoS.

Отключение логирования – это действие, при котором злоумышленник изменяет настройки системы аудита, останавливает службы журналирования, очищает существующие журналы событий или удаляет логи веб-серверов. Цель – уничтожить доказательства своей активности и предотвратить фиксацию последующих действий. Это действие может быть выполнено через скомпрометированную учетную запись, с использованием штатных средств ОС или вредоносного ПО. Эксплуатация уязвимости (exploitation) – это использование программной ошибки, недостатка конфигурации или слабости в реализации для получения несанкционированного доступа, повышения привилегий, выполнения произвольного кода или обхода механизма безопасности. Эксплуатация может привести к полной компрометации системы. Злоумышленник сначала отключает систему логирования или очищает журналы событий. Это действие может быть выполнено удаленно через скомпрометированную учетную запись. После того как логирование отключено, он эксплуатирует уязвимость – но записать эту эксплуатацию уже некому. Система не фиксирует ошибки, не сохраняет данные о созданных процессах, не регистрирует сетевые подключения.

Таблица 1 – Эффективность реализации кибератак

Вид кибератаки	Оценка эффективности	Ограничения	Эффект
Фишинг	До 5%	Только одна рабочая станция	Дает начальный доступ и хеш пароля
Pass-the-Hash	До 10%	Требует предварительно скомпрометированный хеш	Использует хеш для перемещения по сети
DDoS	До 5%	Не дает доступа к данным	Создает шум и отвлекает SOC
Эксфильтрация	До 15%	Обнаруживается по трафику	Кража данных
Отключение логов	0%	Само по себе безопасно	Не дает права доступа
Эксплуатация уязвимости	До 25%	Оставляет следы в логах	Кибератака со следами

Обобщая рассмотренные примеры, можно выделить четыре основных типа синергии по механизму взаимодействия, результат отображен в таблице 2. К первому типу по механизму взаимодействия относится последовательная синергия, при которой одна атака создает условия, необходимые для проведения другой атаки. Результат первой атаки является предпосылкой для второй: атакующий выстраивает цепочку действий, где каждый шаг расширяет его возможности и приближает к конечной цели. Без первого шага второй невозможен или бессмыслен. Классический пример – комбинация фишинга и Pass-the-Hash. Последовательная синергия характеризуется жесткой зависимостью между атаками и четкой временной последовательностью.

Второй тип – маскировочная синергия, при которой одна атака скрывает следы или отвлекает внимание от другой атаки. Атакующий использует диверсионную атаку как прикрытия для скрытой операции. Примером служит комбинация DDoS-атаки и эксфильтрации данных. Маскировочная синергия не требует жесткой зависимости между атаками – они могут выполняться параллельно, но эффект достигается именно за счет маскировки.

Третий тип – обходная синергия, при которой атаки воздействуют на разные слои защиты, обходя каждый из них по отдельности. Современные системы безопасности изолированы: антивирусные средства проверяют файлы, межсетевые экраны контролируют трафик, DLP-системы анализируют содержимое, а средства защиты от фишинга проверяют ссылки. Каждый из этих инструментов эффективен в своей области, но не способен видеть картину целиком. Обходная синергия использует разрывы между этими слоями: одна атака обходит один слой защиты, а другая атака – другой слой. Классический пример – комбинация отключения логирования и эксплуатации уязвимости.

Четвертый тип – параллельная синергия, при которой несколько атак проводятся одновременно и усиливают друг друга. В отличие от последовательной синергии, здесь нет жесткой зависимости по времени – атаки выполняются параллельно, и их совокупный эффект превышает сумму эффектов каждой по отдельности за счет взаимного усиления. Пример – одновременное проведение атаки на отказ в обслуживании (DDoS) и атаки на подбор паролей (брутфорс). DDoS перегружает систему аутентификации, замедляя ее работу, что затрудняет блокировку брутфорс-атаки по превышению

лимита неудачных попыток. В свою очередь, брутфорс-атака создает дополнительную нагрузку, усугубляя эффект DDoS. Параллельная синергия наиболее опасна в распределенных системах, где ресурсы ограничены и конкурируют между собой.

Таблица 2 – Классификация синергии по механизму взаимодействия

Тип синергии	Механизм
Последовательная	А создает условия для В
Маскировочная	А скрывает следы В
Обходная	Атаки обходят разные слои защиты
Параллельная	Атаки усиливают друг друга одновременно

Для решения проблемы синергии в кибератаках необходим переход от изолированных средств защиты к кросс-слоистой корреляции событий. Этот подход предполагает централизованный сбор данных из всех доступных источников: сетевых журналов (файрволы, IDS/IPS, NetFlow), логов конечных точек (Windows Event Log, EDR, системный аудит), событий аутентификации (Active Directory, VPN), оповещений DLP, а также контекстуальной информации об активах, уязвимостях и пользователях. Все эти разнородные данные анализируются совместно в единой системе, что позволяет устанавливать связи между событиями, которые по отдельности выглядят безобидными.

В случае с фишингом и Pass-the-Hash корреляция связывает фишинговое событие (переход по ссылке) с последующей подозрительной аутентификацией с того же хоста, выявляя латеральное перемещение атакующего. При комбинации DDoS и эксфильтрации данных система фиксирует начало DDoS-атаки и автоматически повышает приоритет мониторинга исходящего трафика; обнаружение аномального объема данных в тот же период формирует инцидент «кража под прикрытием DDoS». В случае с отключением логирования и эксплуатацией уязвимости система после фиксации отключения аудита переводит актив в режим повышенного наблюдения за альтернативными источниками (сетевой трафик, запуски процессов); любая аномальная активность после этого интерпретируется как высоковероятная эксплуатация, не оставившая следов в логах. Только такой комплексный подход способен своевременно обнаруживать комбинированные кибератаки, использующие синергетический эффект.

Список использованных источников:

1. Security Vision : [сайт]. – Мск., 2023-2026. – URL: <https://www.securityvision.ru/blog/kiberataki-chast-1-tehnicheskie-instrumenty-i-sposoby-realizatsii/> (дата обращения: 05.04.2026).
2. Fortinet : [сайт]. – Sunnyvale, 2025-2026. – URL: <https://www.fortinet.com/blog/threat-research/uncovering-hidden-forensic-evidence-in-windows-mystery-of-autologger> (дата обращения: 05.04.2026).
3. Imperva : [сайт]. – San Mateo, 2023-2026. – URL: <https://www.imperva.com/blog/why-attackers-target-the-financial-services-industry/> (дата обращения: 05.04.2026).
4. Gurufocus : [сайт]. – Austin, 2024-2026. – URL: <https://www.gurufocus.com/news/2422355/honeywell-report-reveals-silent-residency-is-driving-escalating-cyber-threat-for-industrial-and-critical-infrastructure-facilities> (дата обращения: 05.04.2026).
5. ITworld: [сайт]. – Мск., 2026-2026. – URL: <https://www.it-world.ru/news-company/5tj379eqtns484o0kwscko0cococwwg.html> (дата обращения: 05.04.2026).

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ХЕШИРОВАНИЯ

Ковалевич М.А., Филиппченко К.В., студенты гр.361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Тимофеев А.М. – канд. техн. наук, доцент

Аннотация. Произведен сравнительный анализ алгоритмов хеширования ГОСТ 34.11-2018, СТБ 34.101.77-2016, SHA-256 и BLAKE2. С учетом критериев сравнения была сформирована оценка уровня информационной безопасности приведенных алгоритмов. На основе анализа был разработан программный модуль HashComparator, который сравнивает скорость вычисления криптографических хешей SHA-256 и BLAKE2b для любого заданного файла и рекомендует более быстрый алгоритм. Код решает задачу объективного выбора оптимального алгоритма хеширования для конкретного файла в зависимости от времени выполнения – важного критерия в приложениях, работающих с большими объемами данных.

Ключевые слова. сравнительный анализ, оценка уровня информационной безопасности, алгоритм хеширования, ГОСТ 34.11-2018, СТБ 34.101.77-2016, SHA-256, BLAKE2.

Криптографические хеш-функции – это математический алгоритм, преобразовывающий произвольный массив данных в состоящую из букв и цифр строку фиксированной длины.

ГОСТ 34.11-2018 – это межгосударственный стандарт, который описывает криптографическую функцию хеширования «Стрибог» (Streebog), является обязательным для использования в системах криптографической защиты информации на территории России. Алгоритм также известен как «Стрибог» и поддерживает два уровня безопасности – 256 бит и 512 бит фиксированной длины. Основная сфера применения включает обеспечение целостности данных, проверку подлинности информации, а также является неотъемлемой частью процедур формирования и проверки электронной цифровой подписи (ЭЦП) по ГОСТ 34.10-2018. Документ действует с 1 июня 2019 года, а его разработчиками выступили Центр ФСБ России и компания «ИнфоТекС» [1].

В Республике Беларусь государственным стандартом, который описывает алгоритмы хеширования, стандартизированные в Республике Беларусь, является Bash. Полное название стандарта – СТБ 34.101.77-2016 «Информационные технологии и безопасность. Алгоритмы хеширования». Настоящий стандарт определяет семейство криптографических алгоритмов хеширования, предназначенных для контроля целостности и необратимого сжатия данных. Алгоритмы хеширования настоящего стандарта отличаются уровнем стойкости l . Это натуральное число, кратное 16 и не превосходящее 256. Алгоритм уровня l вычисляет хеш-значения длины $2l$, обрабатывая входные слова блоками длины $1536 - 4l$. Уровни $l = 128$, $l = 192$ и $l = 256$ являются стандартными, им следует отдавать предпочтение [2].

Алгоритм хеширования BLAKE2 предназначен для обеспечения высокой скорости хеширования при сохранении высокого уровня безопасности, и он может быть использован в различных приложениях, таких как аутентификация, проверка целостности данных и многие другие криптографические задачи [3].

Алгоритм хеширования SHA-256, входящий в семейство SHA-2, является одним из самых популярных и надежных алгоритмов. Он генерирует фиксированный 256-битный хэш, что делает его устойчивым к атакам на коллизии и подбор. SHA-256 широко используется в блокчейн-системах, сертификатах SSL/TLS, а также для проверки целостности файлов [4].

Сравнительный анализ перечисленных алгоритмов осуществлялся по следующим критериям: скорость вычисления хеша, коллизионная стойкость, лавинный эффект, длина хеша, криптостойкость, равномерность распределения, вычисление алгоритма. Выбранные критерии для сравнения хеш-алгоритмов являются общепринятыми в криптографическом анализе и системной инженерии. Скорость вычисления определяет применимость алгоритма в реальных системах с ограниченными ресурсами. Коллизионная стойкость представляет собой фундаментальное требование, вытекающее из определения криптографической хеш-функции, и при её нарушении алгоритм считается скомпрометированным. Лавинный эффект характеризует качество перемешивания входных данных и необходим для предотвращения статистического и дифференциального криптоанализа. Длина хеша напрямую влияет на стойкость к атакам полного перебора и парадокса дней рождений, при этом современные стандарты предписывают минимальную длину 256 бит. Криптостойкость включает устойчивость к атакам удлинения сообщения, что критически важно для использования в HMAC. Равномерность распределения обеспечивает статистическую независимость выхода от входа. Способ вычисления выбран для анализа архитектурных особенностей, влияющих на аппаратную оптимизацию и устойчивость к различным классам атак. Результат сравнительного анализа представлен в таблице 1.

Таблица 1 – Обзор алгоритмов хеширования

Критерии для сравнения	ГОСТ 34.11-2018	СТБ 34.101.77-2016	SHA-256	BLAKE2
Скорость вычисления	100 МБ/с для 1 потока	150 МБ/с для 1 потока	200-400 МБ/с для 1 потока	200-400 МБ/с для 1 потока
Коллизийная стойкость	$2^{n/2}$, n-длина хэша	$2^{n/2}$, n-длина хэша	$2^{n/2}$, n-длина хэша	$2^{n/2}$, n-длина хэша
Лавинный эффект	S-блоки, P-преобразование, L-преобразование, 12 раундов	Sponge- конструкция и раундовая функция bash-f	Основа на ARX, функции перемешивания, 64 раунда	Основа на ARX функция перемешивания G, 10/12 раундов
Длина хэша	512 бит, 256 бит	512 бит, 384 бита, 256 бит	256 бит	512 бит, 256 бит
Криптостойкость	Устойчивость к Length Extension (спец.конструкция)	Устойчивость к Length Extension	–	Устойчивость к Length Extension (изначально заложено)
Равномерность распределения	Равномерность обеспечивается SPN-структурой	Sponge- конструкция с перестановкой bash-f (24 раунда)	Равномерность обеспечивается ARX- архитектурой	Равномерность обеспечивается ARX- архитектурой
Вычисление	Разбиение на блоки по 512 бит, 12 раундов преобразований, финальное преобразование	Sponge- конструкция: абсорбция блоков сообщения в 1536- битное состояние через XOR с последующей 24- раундовой перестановкой bash-f, затем сквиз хэша длиной 2l бит (256/384/512).	Разбиение на блоки, создание расписания ключей, 64 раунда сжатия	Инициализация состояния (матрица 4x4), функция сжатия G, раунды перемешивания

На основе представленных данных все четыре алгоритма обеспечивают приемлемый уровень информационной безопасности, однако между ними есть существенные различия. По коллизийной стойкости все алгоритмы соответствуют теоретическому пределу $2^{n/2}$ и не имеют явных уязвимостей. Ключевым дифференцирующим фактором выступает устойчивость к атакам удлинения сообщения: ГОСТ 34.11-2018, СТБ 34.101.77-2016 и BLAKE2 устойчивы к данному классу атак, тогда как SHA-256 уязвим, что снижает его безопасность при использовании в протоколах типа HMAC. По лавинному эффекту SHA-256 с 64 раундами обеспечивает наибольший консервативный запас прочности, проверенный временем, тогда как ГОСТ с 12 раундами и BLAKE2 с 10-12 раундами могут иметь меньший запас, хотя их архитектуры (SPN и ARX соответственно) считаются стойкими. По длине хэша SHA-256 предлагает только 256 бит, тогда как остальные алгоритмы поддерживают 512 бит, что обеспечивает значительно более высокую стойкость к атакам на квантовых компьютерах.

Выбор SHA-256 и BLAKE2 для разработанной программы обоснован их широкой доступностью для конечных пользователей и отсутствием необходимости в дополнительных криптографических библиотеках. Оба алгоритма входят в стандартную библиотеку hashlib языка Python, что обеспечивает кроссплатформенную совместимость и простоту развертывания без установки стороннего программного обеспечения. SHA-256 присутствует во всех современных операционных системах и языках программирования. BLAKE2 включен в стандартную библиотеку Python начиная с версии 3.6, что делает его доступным. На рисунке 1 представлена блок-схема разработанного программного модуля.

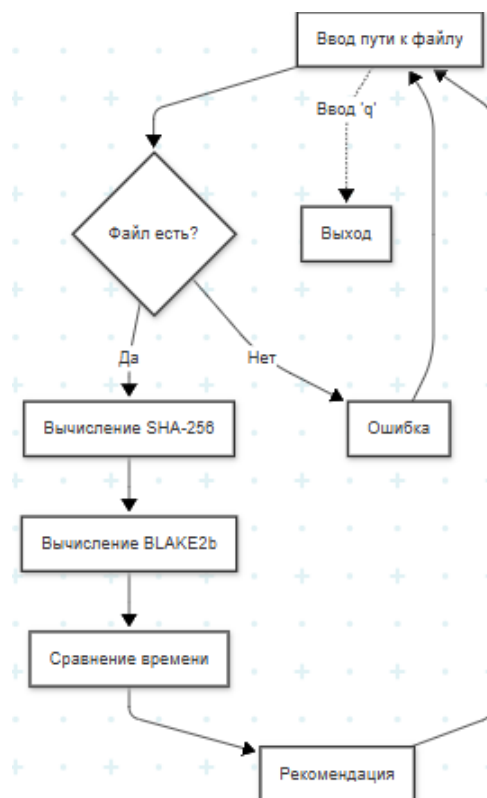


Рисунок 1 – Блок-схема программного модуля HashComparator

Разработанная программа представляет собой инструмент для эмпирического сравнения производительности двух криптографических хеш-функций (SHA-256 и BLAKE2b) на произвольном файле, выбранном пользователем. Листинг модуля включает определение класса HashComparator, который инкапсулирует логику вычисления хешей, замера времени и формирования рекомендации. При инициализации объекта сохраняется путь к целевому файлу и инициализируется пустой словарь results для накопления результатов измерений. Методы calculate_hash_sha256 и calculate_hash_blake реализуют измерение времени выполнения соответствующих алгоритмов с использованием высокоточного таймера time.perf_counter, что позволяет минимизировать погрешности, связанные с системными вызовами. Чтение файла осуществляется блоками по 4096 байт, что обеспечивает баланс между скоростью ввода-вывода и потреблением оперативной памяти. Вычисленный хеш возвращается в шестнадцатеричном формате вместе с затраченным временем. Метод run_analysis последовательно вызывает оба измерительных метода, выводя на экран информацию об анализируемом файле (его имя и размер в байтах), а также промежуточные результаты для каждого алгоритма. После завершения замеров вызывается метод get_recommendation, который находит алгоритм с минимальным временем выполнения, выводит его название и значение времени, а также формирует отсортированную по скорости таблицу сравнения.

Таким образом, наивысший уровень безопасности демонстрируют ГОСТ 34.11-2018, BLAKE2 и СТБ 34.101.77-2016 как современные стандартизированные алгоритмы с поддержкой 512-битного хеша и устойчивостью к удлинению сообщения, тогда как SHA-256, несмотря на широкое распространение, уступает по ряду криптографических свойств. Выбор SHA-256 и BLAKE2 для программного модуля обусловлен их наличием в стандартной библиотеке Python, что обеспечивает доступность для пользователей без установки дополнительного ПО.

Список использованных источников:

1. Электронный фонд правовых и нормативно-технических документов : [сайт]. – Мск., 2019-2026. – URL: <https://docs.cntd.ru/document/1200161707> (дата обращения: 03.04.2026).
2. Википедия : [сайт]. – Мн., 2016-2026. – URL: [https://ru.wikipedia.org/wiki/Bash_\(хэш-функция\)](https://ru.wikipedia.org/wiki/Bash_(хэш-функция)) (дата обращения: 03.04.2026).
3. Server Flow : [сайт]. – Мск., 2025-2026. – URL: <https://serverflow.ru/blog/stati/sovremennye-algoritmy-kheshirovaniya-ot-sha-256-do-argon2/> (дата обращения: 03.04.2026).
4. Хабр : [сайт]. – Мск., 2023-2026. – URL: <https://habr.com/ru/articles/729260/> (дата обращения: 03.04.2026).

АМПЛИТУДНО-ФАЗОВАЯ МОДУЛЯЦИЯ КАК СРЕДСТВО ПОВЫШЕНИЯ СКРЫТНОСТИ ПЕРЕДАЧИ ДАННЫХ

Колесник Н.В., студент гр.461401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Фильченкова Т. М. – старший преподаватель каф. ЗИ

Аннотация. В работе исследуется применение совместной амплитудно-фазовой модуляции для повышения скрытности передачи информации в системах электрической связи. Рассмотрены принципы формирования комбинированных сигналов, построены математические модели амплитудно-фазовой модуляции, проведён анализ спектральной и энергетической эффективности. Выполнено моделирование в среде Python с построением осциллограмм, спектров и диаграмм созвездий. Проведена оценка сложности перехвата и демодуляции сигналов. Разработаны рекомендации по применению комбинированной модуляции в системах защищенной связи.

Ключевые слова: амплитудно-фазовая модуляция, QAM, спектральная эффективность, BER, скрытность передачи.

В современных системах электрической связи наряду с обеспечением пропускной способности и помехоустойчивости важное значение имеет повышение скрытности передачи информации. Одним из базовых методов модуляции является амплитудная модуляция, отличающаяся простотой реализации, однако обладающая рядом ограничений, связанных с низкой спектральной эффективностью и относительной лёгкостью обнаружения сигнала. Более сложным и эффективным методом является совместная амплитудно-фазовая модуляция, позволяющая увеличить информационную ёмкость сигнала и усложнить его структуру, что потенциально повышает уровень защищённости передачи.

Цель данной научно-исследовательской работы: изучить амплитудно-фазовую модуляцию с точки зрения их эффективности и возможности повышения скрытности передачи данных.

Совместная амплитудно-фазовая модуляция (Quadrature Amplitude Modulation, QAM) позволяет повысить спектральную эффективность и усложнить структуру сигнала, что затрудняет его перехват и анализ без знания параметров модуляции. При этом методе передачи информации изменяются сразу два параметра несущего сигнала: его амплитуда и фаза. В общем виде сигнал с амплитудно-фазовой модуляцией может быть представлен как

$$s(t) = A(t)\cos(\omega_c t + \varphi(t)),$$

где $A(t)$ – изменяющаяся во времени амплитуда (амплитудная модуляция); $\varphi(t)$ – изменяющаяся во времени фаза (фазовая модуляция); ω_c – несущая частота.

То есть состоит из двух квадратурных несущих, модулированных по амплитуде многоуровневыми последовательностями импульсов (рисунок 1).

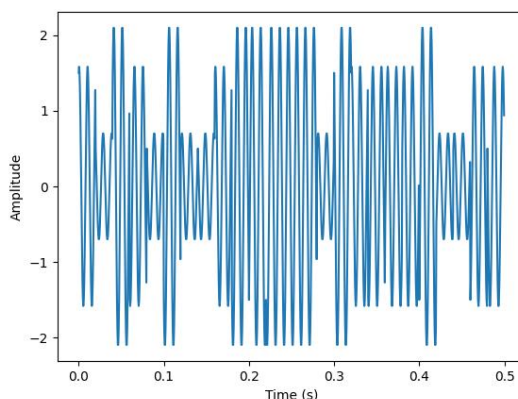


Рисунок 1 – Осциллограмма 16-QAM во временной области

Геометрически сигналы при квадратурной амплитудной модуляции могут быть представлены в виде точек в двумерном сигнальном пространстве, образующих так называемое сигнальное созвездие. Количество точек в созвездии определяется порядком модуляции M и соответствует числу возможных символов сигнала. С увеличением порядка модуляции возрастает плотность расположения точек. На рисунке 2 представлены сигнальные созвездия различных вариантов КАМ [1].

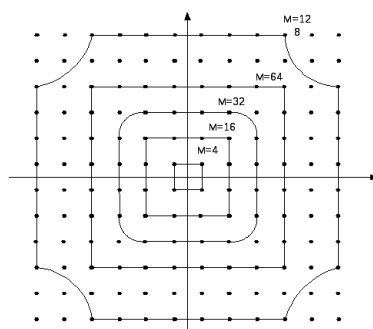


Рисунок 2 – Сигнальное созвездие

Преимущества QAM заключаются в высокой спектральной эффективности, усложненной структуре сигнала и отсутствии выраженной несущей линии в спектре (рисунок 3).

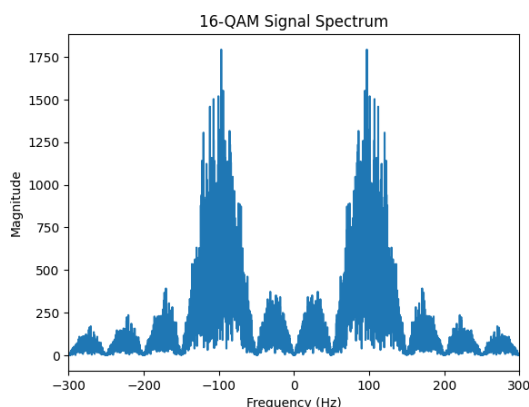


Рисунок 3 – Спектр 16-QAM

Оценка эффективности методов модуляции проводится по двум основным критериям: спектральной и энергетической эффективности. Эти параметры позволяют определить рациональность использования полосы частот и требуемый уровень мощности для обеспечения заданного качества передачи.

В случае амплитудно-фазовой модуляции полоса сигнала определяется скоростью символов, а не битовой скоростью напрямую. Поэтому при одинаковой полосе частот QAM позволяет передавать значительно больший объем информации. Следовательно спектральная эффективность QAM значительно выше, увеличивается информационная плотность сигнала и полоса используется более рационально [3].

Энергетическая эффективность характеризуется требуемым отношением сигнал/шум (SNR) для обеспечения заданной вероятности битовой ошибки (BER).

Для QAM требуется когерентная демодуляция, необходима синхронизация по фазе и при увеличении порядка модуляции требуется более высокий SNR (рисунок 4).

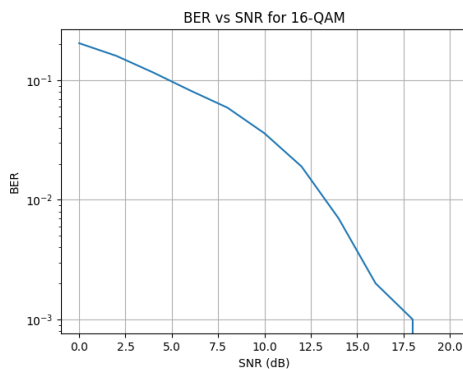


Рисунок 4 – График BER для АФМ

В программной реализации все этапы были реализованы с использованием библиотеки NumPy и пакета matplotlib.

Для исследования сложности перехвата и дешифрования АФМ-сигнала была создана таблица 1, в которой приведено описание по различным критериям.

Таблица 1 – Анализ сложности перехвата и дешифрования сигналов АФМ.

Критерий анализа	Амплитудно-фазовая модуляция
Обнаружение сигнала	Требуется спектральный анализ. Несущая подавлена или неясна
Структура сигнала	Отсутствует выраженная структура огибающей
Метод демодуляции	Требуется когерентный приемник
Требования к синхронизации	Необходима фазовая и частотная синхронизация
Оценка фазы	Требуется точная оценка фазы
Требования к знаниям о сигнале	Требуется знание схемы кодирования и карты созвездия
Устойчивость к анализу	Более высокая
Общая сложность перехвата и дешифрования	Средняя или высокая

QAM-сигналы характеризуются большей сложностью анализа вследствие необходимости когерентного приема, точной фазовой синхронизации и знания параметров модуляции.

На основе проведенного теоретического анализа, математического моделирования и исследования сложности перехвата сигналов можно сформулировать следующие практические рекомендации по применению амплитудно-фазовой модуляции в системах защищенной связи:

1. Использование АФМ предпочтительно в цифровых системах передачи данных, где требуется высокая спектральная эффективность и увеличение информационной плотности сигнала при ограниченной полосе частот.

2. Для повышения скрытности передачи рекомендуется применять модуляции с подавленной несущей (DSB-SC, QAM), поскольку отсутствие выраженной несущей линии в спектре затрудняет обнаружение сигнала средствами спектрального анализа [2].

3. Целесообразно использовать модуляции более высокого порядка (16-QAM, 64-QAM и выше) в сочетании с контролем SNR канала. Это позволяет увеличить объем передаваемой информации и усложнить структуру сигнала для потенциального перехватчика.

Таким образом, были рассмотрены принципы амплитудно-фазовой модуляции, построены их математические модели и выполнено моделирование сигналов; установлено, что QAM обладает значительно более высокой спектральной эффективностью по сравнению с АМ, однако требует более высокого отношения сигнал/шум и сложной синхронизации; показано, что АФМ требует когерентного приема и знания параметров модуляции, что усложняет его перехват и анализ.

Список использованных источников:

1. Амплитудно-фазовая модуляция [Электронный ресурс]. – Режим доступа: <https://clck.ru/3SMrsd> – Дата доступа: 05.03.2026.
2. Типы амплитудной модуляции [Электронный ресурс]. – Режим доступа: <https://clck.ru/3SBdUK>. – Дата доступа: 01.03.2026
3. Шерстюков, С. Я. Способ повышения спектральной эффективности радиосигналов с амплитудно-фазовой модуляцией / С. Я. Шерстюков, С. С. Печников // Вестник Воронежского института МВД России. – 2019. - №2. – С. 155 – 165.

СРАВНЕНИЕ РЕКУРРЕНТНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБРАБОТКИ РЕЧЕВЫХ СИГНАЛОВ

Коржова И.А., магистрант гр. 467241

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Зельманский О.Б. – канд. тех. наук, доцент

Аннотация. В работе рассматривается применение рекуррентных нейронных сетей для обработки речевых сигналов. Проведено сравнительное исследование архитектур RNN, LSTM и GRU при анализе признаков речевых сигналов, полученных методом мел-частотных кепстральных коэффициентов (MFCC). Выполнено обучение моделей на наборе аудиоданных и проведена оценка качества их работы по метрикам точности и функции потерь. Полученные результаты позволяют определить эффективность различных архитектур рекуррентных нейронных сетей при обработке речевой информации

Ключевые слова: Обработка речевых сигналов; Нейронные сети; Рекуррентные нейронные сети; RNN; LSTM; GRU; MFCC; Машинное обучение; Анализ речи; Защита информации.

Современные системы обработки речевых сигналов широко применяются в различных областях информационных технологий, включая системы распознавания речи, голосовые интерфейсы и средства анализа аудиоданных. Особую актуальность задачи обработки речевых сигналов приобретают в области технической защиты информации, где требуется анализ и обработка речевых данных для выявления возможных угроз безопасности. Речевой сигнал представляет собой сложную временную последовательность, содержащую информацию о фонетических особенностях речи. Для эффективного анализа таких сигналов применяются методы извлечения признаков, одним из наиболее распространённых среди которых являются мел-частотные кепстральные коэффициенты (MFCC). Данные признаки позволяют представить аудиосигнал в компактной форме, удобной для дальнейшей обработки алгоритмами машинного обучения. В последние годы для анализа последовательных данных активно применяются рекуррентные нейронные сети. К числу наиболее распространённых архитектур относятся классические рекуррентные сети (RNN), а также их модификации – Long Short-Term Memory (LSTM) и Gated Recurrent Unit (GRU). Эти модели способны учитывать временные зависимости в последовательностях данных, что делает их эффективными при обработке речевых сигналов.

Целью данной работы является сравнительный анализ эффективности различных архитектур рекуррентных нейронных сетей при обработке признаков речевых сигналов.

В рамках исследования была проведена сравнительная оценка эффективности рекуррентных нейронных сетей для обработки речевых сигналов.

В качестве исходных данных использовался открытый корпус речевых записей Common Voice (русскоязычный сегмент). Для проведения эксперимента была сформирована подвыборка объёмом 300 аудиофайлов. Небольшой объём выборки обусловлен ограничениями вычислительных ресурсов и используется для демонстрационного сравнительного анализа архитектур. Данные были перемешаны и разделены на обучающую и тестовую выборки в соотношении 80/20. В качестве упрощённой задачи классификации, позволяющей провести сравнительную оценку архитектур, использовалась бинарная разметка на основе длины текстовой транскрипции: записи с длиной предложения менее 50 символов относились к классу 0, остальные – к классу 1. Выбор длины текстовой транскрипции в качестве метки класса обусловлен тем, что данная характеристика косвенно отражает степень контекстной зависимости речевого сигнала. Длинные предложения содержат больше разнообразных фонетических окружений и требуют удержания контекста на более протяжённых временных интервалах, что близко к условиям задачи выделения аллофонов, где контекст играет определяющую роль. Таким образом, способность нейронной сети различать фрагменты с разной длительностью контекста является необходимым условием для последующего решения целевой задачи – формирования базы аллофонов на основе речи конкретного диктора.

Предварительная обработка данных включала:

- приведение аудиосигналов к частоте дискретизации 16 кГц;
- извлечение признаков на основе мел-частотных кепстральных коэффициентов (MFCC);
- формирование входных последовательностей фиксированной длины.

В качестве признакового представления использовались MFCC-векторы размерности 40 на временной шаг. Для обеспечения единообразия входных данных все последовательности были приведены к длине 200 временных шагов путём обрезания или дополнения нулями.

Для решения задачи бинарной классификации были реализованы три архитектуры рекуррентных нейронных сетей:

- классическая рекуррентная нейронная сеть (RNN);
- сеть с долгой краткосрочной памятью (LSTM);

– рекуррентная сеть с управляемыми вентилями (GRU).

Каждая модель имела следующую структуру: рекуррентный слой с 64 скрытыми нейронами (batch_first=True), за которым следует полносвязный слой с 2 выходными нейронами. Для классификации использовался последний временной шаг выходной последовательности рекуррентного слоя.

Обучение моделей проводилось с использованием следующих параметров:

- оптимизатор Adam с коэффициентом скорости обучения 0.001;
- функция потерь CrossEntropyLoss;
- размер батча 16;
- количество эпох обучения 20.

В таблице 1 представлены основные метрики качества классификации для исследуемых архитектур: доля правильных ответов (Accuracy), полнота (Recall), точность (Precision) и F1-мера. Все метрики приведены в макроусреднении (macro-average).

Таблица 1 – Сравнение эффективности архитектур

Архитектура	Доля правильных ответов (Accuracy)	Полнота (Recall)	Точность (Precision)	F1-мера (F1-score)
RNN	0,70	0,70	0,77	0,68
LSTM	0,91	0,91	0,91	0,91
GRU	0,91	0,91	0,92	0,91

На рисунке 1 представлена динамика функции потерь (loss) в процессе обучения для всех трёх моделей. По оси абсцисс отложены эпохи обучения, по оси ординат – значение функции потерь.

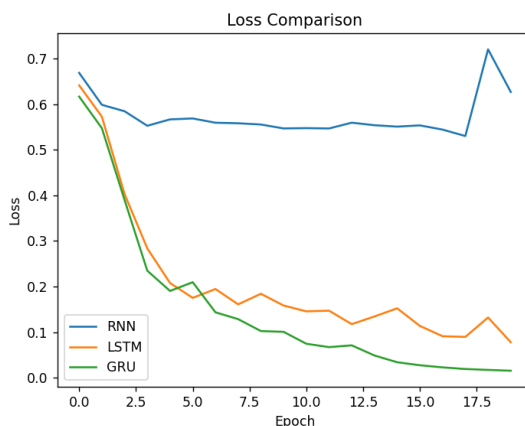


Рисунок 1 – Сравнение динамики функции потерь при обучении RNN, LSTM и GRU

Анализ полученных результатов позволяет сделать следующие наблюдения:

– модель RNN демонстрирует медленную сходимость и нестабильное поведение, что обусловлено проблемой исчезающего градиента, характерной для классических рекуррентных архитектур;

– модель LSTM характеризуется плавным и устойчивым снижением функции потерь, достигая высокой точности (91%) к 6-й эпохе;

– модель GRU обеспечивает наиболее быстрое снижение ошибки на ранних этапах обучения, показывая сопоставимые с LSTM финальные результаты (91%).

Полученные результаты показывают, что классическая архитектура RNN уступает более современным модификациям при обработке речевых сигналов. Это связано с ограниченной способностью RNN учитывать долгосрочные зависимости во временных рядах, что подтверждается теоретическими положениями, описанными в работах [1, 2].

Модель LSTM продемонстрировала стабильное обучение и высокое качество классификации (Accuracy = 0.91). Благодаря механизму вентилей LSTM эффективно сохраняет контекстную информацию на протяжении длительных временных интервалов, что делает её особенно подходящей для анализа речевых сигналов, характеризующихся сложной временной структурой.

Модель GRU показала сопоставимое качество с LSTM (Accuracy = 0.91) и более высокую скорость сходимости на начальных этапах обучения. Однако наблюдается более агрессивное снижение функции потерь, что может косвенно свидетельствовать о возможной склонности к переобучению при недостаточном объёме данных. Упрощённая архитектура GRU по сравнению с LSTM позволяет достичь сопоставимой точности при меньшем количестве параметров, что является преимуществом при ограниченных вычислительных ресурсах.

В результате проведённого исследования установлено, что использование рекуррентных нейронных сетей позволяет эффективно обрабатывать речевые сигналы на основе MFCC-признаков.

Сравнительный анализ показал, что архитектуры LSTM и GRU значительно превосходят классическую RNN по всем рассмотренным метрикам точности и стабильности обучения. Модель LSTM обеспечивает наилучший баланс между точностью и стабильностью, в то время как GRU демонстрирует более быструю сходимость на начальных этапах обучения.

Полученные результаты могут быть использованы при разработке систем защиты речевой информации. В контексте формирования базы аллофонов и генерации акустических помех применение LSTM-архитектур позволяет создавать персонализированные речевые профили, которые могут применяться для защиты конфиденциальных переговоров путём наложения адаптированных аллофонных структур на речевой сигнал диктора. Это открывает перспективы для дальнейших исследований в области создания активных средств акустической защиты информации.

Список использованных источников:

1. Hochreiter, S. Long Short-Term Memory / S. Hochreiter, J. Schmidhuber // *Bioinf.jku.at*, 1997. – С. 1–10.
2. Graves, A. Framewise Phoneme Classification with Bidirectional LSTM and Other Neural Network Architectures / A. Graves, J. Schmidhuber // *Cs.toronto.edu*, 2005. – С. 45–52.
3. Cho, K. Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation / K. Cho [u др.] // *Arxiv.org*, 2014. – С. 1–15.
4. Vaswani, A. Attention Is All You Need / A. Vaswani [u др.] // *Arxiv.org*, 2017. – С. 1–15.
5. Panayotov, V. LibriSpeech: An ASR Corpus Based on Public Domain Audio Books / V. Panayotov [u др.] // *Arxiv.org*, 2015. – С. 1–5.
6. Baevski, A. wav2vec 2.0: A Framework for Self-Supervised Learning of Speech Representations / A. Baevski [u др.] // *Arxiv.org*, 2020. – С. 1–12.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕРВЕРНОЙ ИНФРАСТРУКТУРЫ НА БАЗЕ ФРЕЙМВОРКА KTOR ДЛЯ АНАЛИЗА ОПЕРАТИВНОЙ ОБСТАНОВКИ

Кочеров Р.С., студент гр.230501

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Супрун Ф.Н. – преподаватель

Аннотация. Одной из перспективных платформ для построения высоконагруженных сервисов является асинхронный фреймворк Ktor, созданный на языке Kotlin. Он позволяет создавать масштабируемые сервисы, но требует тщательного проектирования защитных механизмов на всех уровнях: от приёма сетевых запросов до хранения данных в базах. В данной статье рассматривается комплексный подход к обеспечению безопасности Ktor-сервера для органов внутренних дел Республики Беларусь с акцентом на моделирование угроз, реализацию концепции нулевого доверия, защиту от SQL-инъекций, управление токенами доступа и противодействие DDoS-атакам.

Ключевые слова. Безопасность, Ktor, серверная защита, модель угроз, Zero Trust, SQL-инъекции, Exposed, JWT, аутентификация, авторизация, DDoS.

В современном мире происходит активное внедрение цифровых технологий во все сферы деятельности государства, включая правоохранительные органы. Этот процесс получил название цифровая трансформация - переход от традиционных бумажных и ручных методов работы к автоматизированным информационным системам, основанным на компьютерной обработке данных. Для органов внутренних дел Республики Беларусь цифровая трансформация означает создание и использование информационно-аналитических систем - программных комплексов, которые собирают, хранят, обрабатывают и анализируют большие объёмы информации о правонарушениях, преступлениях, участниках процессов и оперативной обстановке.

Однако цифровизация порождает новые уязвимости. Информация, циркулирующая в таких системах, часто относится к категории ограниченного доступа: это персональные данные граждан (фамилии, адреса, паспортные данные, биометрические сведения), служебная информация о расследованиях, оперативные сводки. Поэтому одновременно с внедрением систем необходимо обеспечить их защиту от несанкционированного доступа, утечек, искажения или уничтожения данных. В Республике Беларусь действует Закон «О персональных данных», а также ведомственные нормативные акты, которые устанавливают обязательные требования к обработке и защите такой информации. Соблюдение этих требований является не просто технической задачей, а юридической обязанностью.

Прежде чем строить защиту, необходимо знать какие угрозы могут нарушить работу сервера или завладеть полезной информацией. В информационной безопасности выделяется такое понятие, как модель угроз - систематизированное описание всех возможных опасностей, их источников, способов реализации и потенциального ущерба. Модель угроз разрабатывается для конкретной системы с учётом её архитектуры, данных и условий эксплуатации.

Для ведомственной информационной системы, работающей в органах внутренних дел можно выделить следующие риски:

Внешние атаки на сетевой периметр. Сетевой периметр – это граница между внутренней защищённой сетью органов и внешней средой. Злоумышленник, находящийся снаружи, может попытаться проникнуть внутрь через уязвимости в сетевых сервисах, например, через веб-приложение сервера.

Попытки несанкционированного доступа через уязвимости веб-приложений. Веб-приложение – это программа, работающая на сервере и взаимодействующая с пользователями через браузер или мобильное приложение. Если в коде есть ошибки, злоумышленник может использовать их, чтобы получить доступ к данным или выполнить запрещённые команды.

Компрометация учётных записей сотрудников. Компрометация означает, что злоумышленник каким-то образом завладел логином и паролем сотрудника и теперь может действовать от его имени.

Превышение должностных полномочий. Даже легальный пользователь может намеренно или случайно выполнить операции, на которые у него нет.

Случайные или преднамеренные утечки информации. Это может быть как злой умысел сотрудника, который копирует данные на флешку, так и случайная ошибка - отправка отчёта не по адресу.

Особую опасность представляют внутренние угрозы, то есть исходящие от самих сотрудников или обслуживающего персонала. Внутренние угрозы считаются более сложными для предотвращения, потому что человек уже имеет легальный доступ к системе и знает её особенности. Кроме того, в больших ведомствах работает много людей с разными уровнями допуска, что увеличивает вероятность ошибок или злоупотреблений.

В ответ на перечисленные риски современная практика информационной безопасности предлагает подход Zero Trust. Концепция «нулевого доверия» пересматривает рабочие процессы на основе

отсутствия доверия к любому пользователю перед началом каждой операции. Для этого система должна автоматически проводить процедуру аутентификации и авторизации пользователя, прежде чем предоставить ему доступ к какому-либо приложению, базе данных или другим ресурсам компании. Кроме того, в процессе работы с приложениями и данными статус авторизации каждого пользователя постоянно перепроверяется [1].

В архитектуре Ktor-сервера принцип нулевого доверия реализуется через многоступенчатую проверку каждого запроса к API. Каждый запрос, прежде чем получить доступ к бизнес-логике или к базе данных, проходит следующие этапы:

1. Аутентификация – проверка, действительно ли пользователь тот, за кого себя выдаёт с помощью пароля, логина и токена.

2. Авторизация – проверка, имеет ли аутентифицированный пользователь право выполнять именно эту операцию.

3. Валидация входных данных – проверка, что данные, присланные пользователем, имеют правильный формат, не содержат вредоносного кода и находятся в допустимых пределах.

Только после успешного прохождения всех трёх этапов запрос передаётся на обработку. Ни один запрос не получает доступа к данным или функциям без полного подтверждения своих полномочий. Такой подход особенно важен для распределённых систем, где сотрудники работают с удалённых автоматизированных рабочих мест, планшетов патрульных экипажей или мобильных терминалов.

SQL-инъекция – это один из самых распространённых и опасных видов атак на веб-приложения, работающие с реляционными базами данных. Реляционная база данных – это способ организации данных в виде таблиц, связанных между собой. Для управления такими базами данных используется язык SQL (Structured Query Language – структурированный язык запросов). Программа формирует SQL-команды, чтобы найти, добавить, изменить или удалить данные.

Уязвимость SQL-инъекции возникает, если разработчик напрямую вставляет в текст SQL-команды данные, введённые пользователем. Например, представьте, что программа строит запрос так:

```
"SELECT * FROM users WHERE login = '" + userInput + "'".
```

Если злоумышленник в поле ввода напишет ' OR '1'='1, то получится запрос:

```
SELECT * FROM users WHERE login = '' OR '1'='1'.
```

Условие '1'='1' всегда истинно, поэтому база данных вернёт всех пользователей, и злоумышленник может войти в систему без пароля. Ещё более опасные варианты позволяют удалять таблицы, читать чужие данные или выполнять произвольные команды на сервере.

В Ktor-сервере для работы с базами данных используется библиотека Exposed. Exposed основана на параметризованных запросах. Вместо того чтобы вставлять пользовательский ввод прямо в текст SQL-команды, программист пишет шаблон запроса, где вместо данных ставятся специальные метки-параметры. Затем значения параметров передаются драйверу базы данных отдельно от текста команды. Драйвер – это программа-посредник между приложением и базой данных, которая отвечает за безопасную подстановку данных. В результате даже если злоумышленник попытается внедрить вредоносный код, драйвер интерпретирует его как обычную строку данных, а не как часть SQL-команды. В проекте категорически запрещено формировать SQL-запросы через конкатенацию строк, то есть склеивание кусочков текста с помощью оператора + или аналогичных методов. Такой подход считается грубейшим нарушением стандартов безопасной разработки.

Для контроля качества кода используется статический анализатор – программа, которая проверяет исходный код без его запуска, ищет потенциально опасные конструкции. В проекте применяется инструмент detekt с набором правил безопасности. Если анализатор находит запрещённый способ формирования запроса, он блокирует сборку проекта, то есть не позволяет создать рабочую версию программы, пока ошибка не исправлена.

Для подтверждения личности пользователя и разграничения его прав доступа в системе используется стандарт JSON Web Tokens.

JWT состоит из трёх частей, разделённых точками:

1. Заголовок – содержит информацию о том, как подписан токен.
2. Полезная нагрузка – набор утверждений о пользователе: его идентификатор, роль, уникальный номер токена, время выдачи и истечения срока действия.

3. Подпись – результат криптографического преобразования заголовка и полезной нагрузки с использованием секретного ключа [2].

В Ktor интеграция с JWT выполняется через официальный плагин. Токены подписываются асимметричным алгоритмом RS256. Асимметричный алгоритм означает, что используются два ключа: закрытый и открытый. Закрытый ключ хранится на сервере в защищённом хранилище секретов. Этим ключом сервер подписывает токены. Открытый ключ используется для проверки подписи – его можно распространять свободно, потому что с его помощью нельзя подделать подпись, а только проверить её подлинность. Если злоумышленник попытается изменить полезную нагрузку токена, подпись станет недействительной, и сервер отклонит такой токен.

Проверка прав доступа происходит на каждом маршруте сервера. Система проверяет не только срок действия токена, но и наличие у роли пользователя разрешения на выполнение запрошенной операции. Рядовой сотрудник милиции не может просматривать документы для руководства, а аналитик не может вносить изменения в оперативные данные. Такой подход соответствует принципу наименьших привилегий – каждому пользователю выдаётся ровно тот минимум прав, который необходим ему для выполнения его служебных обязанностей, и не более того.

Если токен украден, то злоумышленник сможет выдавать себя за легального пользователя в течение всего срока действия токена. Чтобы минимизировать ущерб от такой кражи, в системе реализована двухуровневая схема с двумя видами токенов:

Токен доступа (access token) – короткоживущий, его срок действия составляет не более 15 минут. Он используется для каждого запроса к API. Если токен украден, злоумышленник сможет использовать его только в течение этого короткого окна.

Токен обновления (refresh token) – может действовать часы или дни. Он предназначен исключительно для получения нового токена доступа, когда старый истекает. Токен обновления хранится на сервере в связке с идентификатором устройства и отпечатком браузера. Это позволяет серверу убедиться, что запрос на обновление токена приходит с того же устройства, с которого выполнялся вход.

Для принудительного отзыва токенов, то есть немедленной отмены их действия до истечения срока, может использоваться высокопроизводительное хранилище Redis. Redis – это база данных, размещаемая в памяти, которая используется, в основном, в роли кеша, находящегося перед другой, центральной базой данных, вроде MySQL или PostgreSQL. Кеш, основанный на Redis, помогает улучшить производительность приложений. Он эффективно использует скорость работы с данными, характерную для памяти, и смягчает нагрузку центральной базы данных приложения [3]. В нашем случае в Redis хранится чёрный список идентификаторов токенов, которые были отозваны.

Доступность – одно из трёх основных свойств информационной безопасности. Оно означает, что система должна быть работоспособна и отвечать на запросы пользователей в любое необходимое время. Для правоохранительных органов недоступность информационной системы может иметь критические последствия: невозможно проверить человека по базам данных, зарегистрировать заявление, получить оперативную сводку.

Одним из самых серьёзных способов нарушить доступность является DDoS-атака (Distributed Denial of Service – распределённая атака типа «отказ в обслуживании»). Злоумышленник использует сеть из множества заражённых компьютеров и направляет от них огромное количество запросов на сервер жертвы. Сервер не справляется с нагрузкой, начинает тормозить, а затем полностью перестаёт отвечать. Для противодействия DDoS на уровне Ktor-приложения реализован плагин Rate Limiting. Этот плагин подсчитывает, сколько запросов приходит от одного IP-адреса или от одного пользователя за единицу времени, например, за секунду или минуту. Если количество превышает установленный лимит, последующие запросы отклоняются.

Валидация – это процесс проверки того, что данные, присланные пользователем, соответствуют ожидаемому формату, типу, диапазону значений и не содержат недопустимых символов. Валидация выполняет две функции: защита от ошибок – предотвращает попадание в базу данных некорректных данных; защита от атак – отсеивает попытки внедрения вредоносного кода. Необходимо обеспечить проверку соответствия JSON-схем, формата полей, диапазона значений. Некорректные или потенциально опасные запросы отклоняются ещё до того, как достигнут бизнес-логики. Это снижает риск эксплуатации уязвимостей на уровне приложения, поскольку вредоносные данные просто не доходят до мест, где они могли бы причинить вред.

Таким образом, при построении защищённого Ktor-сервера для информационных систем органов внутренних дел применяется архитектура на основе принципа нулевого доверия с многоступенчатой проверкой каждого запроса к API (аутентификация, авторизация, валидация). Для защиты от SQL-инъекций используются параметризованные запросы через библиотеку Exposed, категорически запрещена конкатенация строк, а качество кода контролируется статическим анализатором defekt. Аутентификация и разграничение доступа реализованы на основе JWT с асимметричной подписью RS256, применяется двухуровневая схема с короткоживущими токенами доступа (15 минут) и токенами обновления, принудительный отзыв токенов осуществляется через высокопроизводительное хранилище Redis. Доступность сервиса обеспечивается механизмом ограничения частоты запросов (Rate Limiting), а валидация входных данных по JSON-схемам позволяет отклонять некорректные и опасные запросы до попадания в бизнес-логику.

Список использованных источников:

1. Kaspersky [Электронный ресурс]. URL: <https://www.kaspersky.ru/resource-center/definitions/zero-trust> (дата обращения: 02.04.2026).
2. Wikipedia [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/JSON_Web_Token (дата обращения: 02.04.2026).
3. Хабр [Электронный ресурс]. URL: <https://habr.com/ru/companies/wunderfund/articles/685894> (дата обращения: 01.04.2026).

АКТУАЛЬНЫЕ ВОПРОСЫ ИЗМЕНЕНИЯ ЗАКОНОДАТЕЛЬСТВА РЕСПУБЛИКИ БЕЛАРУСЬ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Лукашевич З.Ю., студент гр.361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Тимофеев А.М. – канд. техн. наук, доцент

Аннотация. Статья посвящена анализу несоответствия между широким кругом субъектов информационных отношений, закреплённых в Законе Республики Беларусь № 455-3, и ограниченным субъектным составом административной ответственности, установленным статьями 23.11 и 23.12 КоАП РБ. Рассматривается бланкетный характер ст. 41 Закона № 455-3 и последствия введения новых норм кибербезопасности Законом № 91-3 от 12 июля 2025 г. Особое внимание уделяется причинам и правовым последствиям исключения из сферы административной ответственности Республики Беларусь, административно-территориальных единиц, иностранных государств и международных организаций.

Ключевые слова: Кибербезопасность, критически важные объекты информатизации, КВОИ, административная ответственность, КоАП РБ, Закон № 455-3, Указ № 40, субъекты ответственности.

В современных условиях стремительного развития информационных технологий и постоянного роста киберугроз обеспечение кибербезопасности критически важных объектов информатизации (КВОИ) приобретает стратегическое значение для национальной безопасности Республики Беларусь. Принятие Законом Республики Беларусь от 12 июля 2025 г. № 91-3 новых статей 23.11 и 23.12 Кодекса об административных правонарушениях стало важным шагом в формировании эффективного правового механизма защиты национальной критической инфраструктуры. Однако введение данных норм выявило существенное несоответствие между широким кругом субъектов информационных отношений, установленным Законом № 455-3, и ограниченным субъектным составом административной ответственности, предусмотренным ст. 1.8 КоАП РБ. Актуальность исследования обусловлена необходимостью научного осмысления причин такого законодательного решения и его влияния на эффективность правоприменительной практики.

Закон Республики Беларусь от 10 ноября 2008 г. № 455-3 «Об информации, информатизации и защите информации» (далее – Закон № 455-3) является базовым нормативным правовым актом, регулирующим отношения в сфере создания, использования и защиты информации. Он распространяется на широкий круг субъектов: физических лиц, юридических лиц, государственных органов, а также иностранных государств и международных организаций. Статья 41 Закона № 455-3 носит бланкетный характер и отсылает к другим законодательным актам при привлечении к ответственности за нарушения.

С 17 июля 2025 года Законом Республики Беларусь от 12 июля 2025 г. № 91-3 «Об изменении кодексов по вопросам административной ответственности» в главу 23 КоАП РБ «Административные правонарушения в области связи и информации» были добавлены специальные нормы – статья 23.11 (нарушение требований по кибербезопасности обычных объектов информационной инфраструктуры) и статья 23.12 (нарушение требований по кибербезопасности критически важных объектов информатизации – КВОИ).

Следует отметить, что в марте 2026 года Палатой представителей был принят во втором чтении ещё один законопроект с аналогичным названием. Одобрен Советом Республики 02.04.2026 и ожидает подписания Президента. Данный документ вносит корректировки в существующие нормы, усиливает профилактическую составляющую и уточняет процедуры, однако не затрагивает вновь введённые статьи 23.11 и 23.12.

Основной проблемой нового правового регулирования стало существенное несоответствие между субъектами, указанными в Законе № 455-3, и субъектами административной ответственности, предусмотренными ст. 1.8 КоАП РБ. Согласно последней, административную ответственность несут только физические лица (включая должностных) и юридические лица (включая иностранные юридические лица). Республика Беларусь, административно-территориальные единицы, иностранные государства и международные организации как суверенные субъекты международного права исключены из числа субъектов административной ответственности.

Закон № 455-3 охватывает все информационные системы и ресурсы. Однако Указ Президента Республики Беларусь № 40 «О кибербезопасности» вводит чёткое разделение: обычные объекты информационной инфраструктуры (ОИИ) и критически важные объекты информатизации (КВОИ). КВОИ – это объекты, нарушение или прекращение функционирования которых может причинить существенный ущерб национальным интересам Республики Беларусь. Такие объекты регистрируются в Государственном реестре КВОИ по строгим критериям. Для обычных ОИИ применяется ст. 23.11 КоАП РБ, для КВОИ – более строгая ст. 23.12.

Согласно ст. 1.8 КоАП РБ административную ответственность несут физические лица и юридические лица (включая иностранные юридические лица). Иностранные государства и международные организации как суверенные субъекты международного права не являются субъектами административной ответственности по КоАП РБ. Вопросы в их отношении решаются в дипломатическом порядке или через нормы международного права. КВОИ являются национальными объектами Республики Беларусь, поэтому иностранное государство или международная организация не может выступать их прямым владельцем. Иностранные юридические лица несут ответственность на общих основаниях.

В КоАП РБ отсутствует отдельная специальная норма, посвящённая исключительно государственным органам. Статьи 23.11 и 23.12 сформулированы универсально и применяются к юридическим лицам в целом. Государственный орган или государственная организация подпадает под действие этих статей и может быть оштрафована как юридическое лицо. Наиболее жёсткий механизм ответственности для государственного сектора предусмотрен Указом Президента Республики Беларусь № 40 «О кибербезопасности» (подп. 3.14–3.15 п. 3). Руководитель государственного органа несёт персональную ответственность за обеспечение кибербезопасности и обязан назначить заместителя, ответственного за это направление. Персональная ответственность реализуется преимущественно через дисциплинарные меры (вплоть до увольнения) и, в тяжёлых случаях, через уголовные статьи 425 и 428 УК РБ.

Республика Беларусь как суверенное государство и административно-территориальные единицы (области, районы, города) не являются субъектами административной ответственности по КоАП РБ (ст. 1.8). Государство не может само себя привлекать к административной ответственности. В случае нарушений на КВОИ, находящихся в ведении республиканских или местных органов, ответственность наступает в отношении юридического лица (государственного органа или организации) и должностных лиц по ст. 23.12 и ст. 24.58 КоАП РБ, а также через персональную дисциплинарную и уголовную ответственность руководителей.

Таким образом, законодатель Республики Беларусь, руководствуясь принципами риск-ориентированного и пропорционального регулирования, сознательно ограничил круг субъектов административной ответственности по статьям 23.11 и 23.12 КоАП РБ. Выявленное несоответствие между широким перечнем субъектов информационных отношений, закреплённых в Законе № 455-З, и ограниченным субъектным составом административной ответственности не является правовым пробелом. Напротив, оно отражает взвешенную и последовательную государственную политику, направленную на обеспечение максимальной защиты критически важных объектов информатизации как национальных активов.

Критически важные объекты информатизации, будучи стратегическими элементами национальной инфраструктуры, не могут становиться предметом самопривлечения государства к административной ответственности. Вопросы же ответственности иностранных государств и международных организаций традиционно разрешаются в рамках дипломатических механизмов и норм международного права. Такой подход позволяет эффективно защищать критическую информационную инфраструктуру, не нарушая фундаментальных принципов государственного суверенитета и международных иммунитетов.

В заключение необходимо подчеркнуть, что выбранный законодателем дифференцированный подход к ответственности за нарушения требований кибербезопасности КВОИ полностью отвечает задачам обеспечения национальной безопасности в условиях цифровизации. Он позволяет государству сосредоточить ресурсы и контроль именно на тех объектах, сбой в работе которых может иметь критические последствия для страны, одновременно избегая излишнего административного давления на субъектов, не представляющих системной угрозы. Такой механизм делает законодательство более гибким, эффективным и соответствующим современным международным стандартам регулирования кибербезопасности.

Список использованных источников:

1. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (в ред. от 2025 г.).
2. Кодекс Республики Беларусь об административных правонарушениях (в ред. Закона № 91-З от 12.07.2025).
3. Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности».
4. Закон Республики Беларусь от 12 июля 2025 г. № 91-З «Об изменении кодексов по вопросам административной ответственности».

ОБРАЗОВАТЕЛЬНЫЙ ХАБ ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Маршалова К.Ц., Биюмен Е.А., студенты гр.361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук, доцент

Аннотация. Разработана обучающая CTF-платформа в формате Point-and-Click квеста на базе движка Unity 6. Архитектура объединяет внутриигровой ролевой интерфейс и практическое решение задач в физической операционной системе (ОС) пользователя. Навигация включает локации с неигровыми персонажами (NPC) для выдачи заданий и виртуальный «хаб». Хаб представляет собой терминал, интегрирующий модули управления квестами, мониторинга глобального рейтинга (Leaderboard) и верификации CTF-флагов. Базовая механика заключается в экспорте тренировочных артефактов (PCAP-дампов, криптографических контейнеров) на реальный ПК. Обучающийся анализирует артефакты с помощью профессиональных утилит информационной безопасности, возвращая найденный флаг в клиент игры.

Ключевые слова. обучающий хаб, защита информации, геймификация, Unity, Capture The Flag, кибербезопасность, неигровые персонажи, системное администрирование, анализ артефактов.

Разрабатываемый хаб представляет собой интерактивный обучающий комплекс, реализованный в формате Point-and-Click квеста. В качестве базовой среды разработки выбран кроссплатформенный игровой движок Unity 6. Выбор 2D-перспективы продиктован необходимостью минимизации когнитивной нагрузки на пространственное ориентирование: обучающийся не тратит ресурсы на управление камерой в трехмерном пространстве, концентрируя внимание исключительно на аналитических и технических задачах. Для обеспечения высокого качества визуализации при низких системных требованиях задействован конвейер рендеринга Universal Render Pipeline (URP), позволяющий реализовать ресурсоэффективное динамическое освещение и постобработку, стилизующие интерфейс под жанр киберпанк.

Фундаментальным отличием предложенного хаба от классических образовательных симуляторов (киберполигонов) является отказ от внутренней программной эмуляции операционных систем и специализированного программного обеспечения. Платформа функционирует по гибридной модели взаимодействия. Игровой клиент берет на себя роль интерактивного распределителя задач (Task Manager), системы нарратива и контроллера прогресса, тогда как непосредственный анализ уязвимостей и работа с артефактами осуществляются на стороне физической хост-машины обучающегося (например, в среде ОС Kali Linux). Схематическое представление потоков данных в рамках гибридной архитектуры приведено на рисунке 1.



Рисунок 1 – Схема взаимодействия игрового клиента и физической операционной системы обучающегося

Программная архитектура приложения обладает высокой степенью модульности и декомпозирована на три ключевых компонента, взаимодействие между которыми реализуется через систему диспетчеризации событий UnityEvents и двумерные физические коллайдеры (Box Collider 2D).

1. Модуль пространственной навигации и генерации квестов. Игровое пространство разделено на тематические локации (галерея, библиотека, серверная и др.). Получение заданий формата Capture The Flag (CTF) интегрировано в систему ветвящихся диалогов с неигровыми персонажами (NPC). Программная логика диалоговой системы спроектирована с использованием паттерна ScriptableObjects. Данное архитектурное решение выносит данные о квестах за пределы исполняемого кода, позволяя масштабировать банк заданий, добавлять новые сценарии и корректировать тексты диалогов через инспектор Unity без необходимости перекомпиляции проекта. Подобный нарративный подход эффективно эмулирует начальные этапы аудита безопасности – социальную инженерию и сбор информации (Reconnaissance) [1].

2. Модуль экспорта артефактов и интеграции с ОС. Данный модуль является связующим звеном между игровой симуляцией и реальной практикой. При акцептовании задания от NPC скрипты платформы инициируют выгрузку тренировочного файла-артефакта. На программном уровне

используется функционал пространства имен System.IO, обеспечивающий бинарное копирование файлов (защитных в ресурсы игры или загружаемых с удаленного сервера) в пользовательскую директорию (например, Downloads) на физическом диске компьютера. В качестве учебных артефактов могут выступать:

- дампы сетевого трафика в формате .pcap для анализа протоколов;
- бинарные исполняемые файлы (.exe, .elf) для базового реверс-инжиниринга;
- зашифрованные криптографические контейнеры и дампы оперативной памяти;
- фрагменты скомпрометированного исходного кода.

Типичный сценарий выполнения лабораторной задачи реализуется в четыре этапа. На первом этапе обучающийся получает от NPC сюжетную информацию о перехваченном сетевом трафике (легенда задания). На втором этапе игровая платформа аппаратно экспортирует файл дампа на рабочий стол игрока. На третьем этапе обучающийся сворачивает окно игры, запускает профессиональный анализатор протоколов (например, Wireshark) в своей реальной ОС, производит фильтрацию пакетов, декодирует полезную нагрузку и извлекает искомые данные. На финальном этапе полученный ответ форматируется в стандартный CTF-флаг [2].

3. Модуль виртуального хаба и рейтинговой верификации. Вектор возврата в игру осуществляется через личную комнату главного героя (виртуальный хаб). В хабе реализован интерфейс персонального компьютера (терминала), выполняющий функцию личного кабинета обучающегося. Через данный терминал студент вводит найденный флаг. Проверка валидности флага производится не путем прямого сравнения строк в коде, а через сопоставление криптографических хэш-сумм (например, алгоритмом SHA-256). Это полностью исключает возможность извлечения правильных ответов путем реверс-инжиниринга исходного кода самого образовательного хаба.

Дополнительно в виртуальном терминале интегрирована система мониторинга академического прогресса и глобальная рейтинговая таблица (Leaderboard). За каждое корректно выполненное задание системе начисляются баллы, формирующие позицию студента в рейтинге. Для поддержания объективного соревновательного баланса в платформе реализована система динамического ценообразования задач (Dynamic Scoring).

Суть данного алгоритма заключается в постепенном снижении стоимости задания пропорционально количеству обучающихся, успешно его решивших. При этом стоимость снижается не бесконечно, а лишь до установленного минимального порога, гарантирующего получение базовых баллов даже при позднем решении. Для дополнительного стимулирования соревновательной активности предусмотрен статический бонус за первоочередное решение задачи – «First Blood» (первая кровь), который не зависит от общей статистики прохождений.

Математическая модель расчета итогового количества рейтинговых баллов (R), начисляемых обучающемуся за сдачу флага, описывается следующей формулой:

$$R = \max(P_{\min}, P_{\max} - ((P_{\max} - P_{\min}) / S_{\text{decay}}) \cdot N) + \text{FB}, \quad (1)$$

где $P_{\max}$ – начальная (максимальная) стоимость задания в баллах; $P_{\min}$ – минимальный порог баллов, ниже которого стоимость задания не опускается; N – текущее количество пользователей, успешно решивших данную задачу; S_{decay} – пороговое количество решений, при достижении которого стоимость задания фиксируется на минимальном уровне; FB – статический бонус «First Blood», принимающий заданное значение строго для первого решившего и равный 0 для всех последующих.

Наличие динамической рейтинговой системы выступает критически важным фактором внутренней мотивации обучающихся. Алгоритм автоматически балансирует сложность: задачи, которые решают все, быстро теряют в «цене», в то время как действительно сложные артефакты остаются высокобалльными, объективно отражая технические компетенции лидеров таблицы.

Таким образом, интеграция подлинного инструментария аудита информационной безопасности в логику 2D-квеста позволяет трансформировать рутинный образовательный процесс в исследовательскую работу. Механика экспорта артефактов в синергии с динамическим CTF-рейтингом обеспечивает бесшовный переход от академической теории к прикладной практике системного администрирования.

Список использованных источников:

1. Геймификация в образовательном процессе подготовки специалистов по защите информации / А.А. Шелупанов [и др.] // *Безопасность информационных технологий*, 2021. – Т. 28. – № 2. – С. 115-125.
2. Образовательный хаб для подготовки специалистов в области защиты информации / К.Ц. Маршалова, Е.А. Биюмен // *Технические средства защиты информации 2026*. – С. 318–321.

МЕТОДИКА ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ ДЛЯ ПОДРАЗДЕЛЕНИЙ КИБЕРБЕЗОПАСНОСТИ

Михайловский С.Г., студенты гр.461403

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук, доцент

Аннотация. В статье рассматривается роль методики тестирования на проникновение в деятельности подразделений кибербезопасности. Раскрываются ключевые этапы разработанной методики: разведка, сканирование, анализ уязвимостей, эксплуатация, закрепление в системе и нагрузочное тестирование. Особое внимание уделяется современным инструментальным средствам, включая AI-first сканеры, технологии эксплуатации уязвимостей и автоматизации обработки данных. Подход ориентирован на практическое использование атакующими и защищающими командами для объективной оценки защищенности корпоративных информационных систем.

Ключевые слова. тестирование на проникновение, пентест, методика, эксплуатация уязвимостей, импланты, C2-каналы, автоматизация, AI-безопасность, команда кибербезопасности, Red Team, Blue Team.

Современные корпоративные информационные системы представляют собой сложные распределенные комплексы с облачными платформами, виртуализацией, микросервисами и множеством внешних интеграций. В условиях роста кибератак обеспечение информационной безопасности требует регулярной оценки эффективности средств защиты, ключевым инструментом которой выступает тестирование на проникновение. В крупных организациях функции могут быть разделены между «красными» (Red Team) и «синими» (Blue Team) командами, а эффективное взаимодействие между ними невозможно без формализованной методики. Настоящая статья посвящена разработке комплексной методики тестирования на проникновение, включающей этапы проведения, инструментальное обеспечение на базе AI-first сканеров и автоматизацию. Предлагаемый подход ориентирован на практическое применение подразделениями кибербезопасности для объективной оценки защищенности корпоративных информационных систем [1].

Разработанная методика базируется на модели Cyber Kill Chain и включает шесть последовательных этапов, обеспечивающих полноту охвата всех стадий атаки: от сбора информации до закрепления в системе.

Этап планирования и подготовки, формализует цели, объем и правила взаимодействия. Определяются объекты оценки: внешний периметр (веб-приложения, шлюзы), внутренняя инфраструктура (серверы приложений, БД, СХД), сетевая архитектура (VLAN, межсетевые экраны, микросегментация), человеческий фактор. На данном этапе формируется команда, распределяются роли, разрабатывается план взаимодействия с заказчиком, включая информирование о критических находках и механизмы экстренного прекращения тестирования.

Этап разведки делится на пассивные и активные методы, при этом пассивная разведка включает анализ IP-адресов, DNS-имен, соцсетей, архивов сайтов с использованием theHarvester (сбор email и поддоменов), Maltego (визуальный анализ связей), Shodan (поиск устройств в глобальной сети). Активная разведка, это этап сканирование портов, определение версий сервисов, определение топологии сети. Автоматизация обеспечивается скриптами, которые выполняют последовательный запуск OSINT-инструментов, парсинг данных, формирование списков активных хостов и подготовку отчетов для импорта в другие системы [2].

Этап сканирования и анализа уязвимостей, обеспечивается применением Masscan, который позволяет осуществлять высокоскоростное обнаружение активных узлов и портов (до миллионов пакетов в секунду). Nmap выполняет детальный анализ версий сервисов, ОС и специализированные скрипты безопасности. Nmap с набором скриптов vulners автоматически сопоставляет версии ПО с CVE и оценивает критичность по CVSS. AI-first сканер MEDUSA (открытая платформа, 76+ анализаторов, 7300+ правил) выявляет классические уязвимости (SQL-инъекции, XSS) и риски AI-компонентов, LLM-интеграций. Преимущества сканера AI-first в снижении ложных срабатываний до 74 %, контекстная приоритизация рисков, поддержка более 42 языков (Python, JavaScript, Terraform, Docker, конфигурации AI-агентов) [3].

Этап эксплуатации уязвимостей и закрепления в системе позволяет моделировать действия злоумышленника. Как правило, эксплуатация выполняется с использованием публичных эксплоитов Metasploit для получения начального shell-доступа. Ключевое отличие методики в обязательном закрепление в системе для оценки способности средств защиты обнаруживать активность после получения доступа. Для этого используется платформа Sliver, позволяющая генерировать импланты на сервере C2 с обфускацией, что делает каждый экземпляр уникальным, усложняя сигнатурный анализ. Архитектура импланта включает ядро агента на Go, поддерживает протоколы C2 (HTTPS,

DNS, mTLS, WireGuard), модульная структура снижает вероятность обнаружения. После установления C2 выполняются сбор информации, повышение привилегий и горизонтальное перемещение для оценки сетевой сегментации и принципа минимальных привилегий.

Этап тестирования устойчивости и доступности, проводится на трех уровнях модели OSI: сетевом (hping3 для реализации SYN-flood, UDP-flood или проверки межсетевых экранов, IPS, SYN Cookies), транспортном (thc-ssl-dos для проверки устойчивости TLS/SSL к атакам, связанным с повторным согласованием соединения, выявление некорректных конфигураций веб-серверов), прикладном (siege для нагрузочного тестирования веб-сервисов, оценки кэширования, балансировщиков, отказоустойчивости). Автоматизация достигается скриптами, стандартизирующими параметры тестирования и формирующими сводные отчеты [3].

Этап анализа результатов и формирования рекомендаций, базируется на документировании уязвимостей с указанием методов эксплуатации, использованных инструментов и доказательной базы (логи C2, скриншоты). Формируется матрица рисков по CVSS с учетом бизнес-контекста. Предлагаются меры по совершенствованию СЗИ (формируется дорожная карта повышения защищенности).

Реализация представленной методики требует применения систематизированного набора инструментов, охватывающих все этапы тестирования. В таблице 1 представлены основные категории инструментов и их роль в методике.

Таблица 1 – Инструменты обеспечения методики тестирования на проникновение

Категория	Инструменты	Назначение
Базовая платформа	Kali Linux	Унифицированная операционная среда с предустановленным набором инструментов безопасности
Разведка и OSINT	theHarvester, Maltego, Shodan	Сбор информации из открытых источников, визуальный анализ связей, поиск устройств и сервисов
Сканирование портов	Masscan, Nmap	Высокоскоростное обнаружение активных узлов, детальное определение версий и операционных систем
Анализ уязвимостей	Nmap (скрипт vulners), MEDUSA	Поиск известных уязвимостей (CVE), AI-first статический анализ кода и конфигураций
Эксплуатация уязвимостей	Metasploit Framework	Выполнение эксплойтов, автоматизация атак
Закрепление и C2	Sliver	Генерация имплантов, управление каналами C2, пост-эксплуатация
Нагрузочное тестирование	hping3, thc-ssl-dos, siege	SYN-флуд, SSL renegotiation, нагрузочное тестирование веб-приложений
Социальная инженерия	GoPhish	Моделирование фишинговых кампаний, оценка человеческого фактора
Автоматизация процессов	Скрипты Python/Bash	Автоматизация сбора данных, обработки результатов, формирования отчетов

В ходе разведки скрипты последовательно собирают данные через OSINT-инструменты, фильтруют результаты, формируют списки активных хостов, поддоменов и email-адресов, готовят структурированные отчеты (JSON, XML) для импорта в системы анализа. Обеспечивается воспроизводимость и сравнительный анализ изменений атакуемой поверхности.

Скрипты выполняют двухэтапное сканирование: высокоскоростное обнаружение активных узлов Masscan, затем детальный анализ Nmap с определением версий и поиском уязвимостей. Результаты агрегируются в единый отчет. Дополнительно инициируется сканирование AI-first сканером MEDUSA, который выявляет уязвимости в коде и конфигурациях, снижая ложные срабатывания до 74 % [2].

Нагрузочное тестирование реализуется скриптами, последовательно запускающими различные типы атак (SYN-флуд, атаки на TLS/SSL, нагрузочное тестирование веб-сервисов), собирающими метрики производительности и формирующими сводные отчеты. Стандартизация параметров обеспечивает воспроизводимость результатов и сравнение показателей до и после изменений [3].

Скрипты агрегируют результаты всех этапов, формируют матрицу рисков с оценкой критичности уязвимостей и готовят итоговый отчет для передачи заказчику и интеграции с системами управления уязвимостями. Это сокращает время подготовки документов и обеспечивает единообразие результатов при повторных тестированиях.

Разработанная методика тестирования на проникновение повышает эффективность Red Team и Blue Team.

Для Red Team она обеспечивает системность, воспроизводимость и накопление знаний. Автоматизация высвобождает ресурсы для нестандартных задач, требующих глубокого понимания архитектуры.

Для Blue Team результаты тестирования позволяют приоритизировать устранение уязвимостей и настраивать системы обнаружения инцидентов. Автоматизированная отчетность ускоряет идентификацию критических рисков.

Взаимодействие команд строится на совместном планировании. Информированное тестирование оценивает не только возможность эксплуатации уязвимостей, но и способность службы ИБ их своевременно обнаружить. Совместный анализ предоставляет детальную информацию о методах, инструментах и тактиках для настройки систем обнаружения.

Особую ценность имеет этап закрепления в системе с использованием платформы Sliver. Развертывание обфусцированного импланта и установление скрытого канала C2 подтверждает неспособность средств защиты блокировать полиморфные нагрузки, доказывая необходимость поведенческого анализа и XDR. DNS-туннелирование для управления и эксфильтрации данных выявляет недостаточную глубину анализа служебных протоколов сетевой защитой [2].

Разработанная методика представляет собой систематизированный подход к оценке защищенности корпоративных информационных систем, интегрирующий ключевые этапы тестирования на проникновение, современные инструментальные средства и автоматизацию процессов. Ее реализация обеспечивает системность и воспроизводимость оценки, объективную оценку эффективности средств защиты, выявление не только наличия уязвимостей, но и реальной возможности их эксплуатации, формирование обоснованных рекомендаций.

Для команд Red Team и Blue Team методика создает основу системной работы и накопления знаний, а автоматизация позволяет сосредоточиться на сложных задачах. Для подразделений кибербезопасности результаты становятся объективной основой приоритизации защитных мероприятий и оценки эффективности внедренных средств.

Список использованных источников:

1. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение. – СПб: Университет ИТМО, 2018. – 45 с.
2. Парасрам Ш. Kali Linux. Тестирование на проникновение и безопасность / Шива Парасрам. – Москва : ДМК Пресс, 2021. – 432 с.
3. Efe A. A risk assessment on usage of Kali tools to hack and manipulate web-based MIS and ERP applications // *Yönetim Bilişim Sistemleri Dergisi*. – 2025. – Vol. 11, № 1. – P. 62–80.

АМПЛИТУДНО-ИМПУЛЬСНАЯ И ШИРОТНО-ИМПУЛЬСНАЯ МОДУЛЯЦИИ В СИСТЕМАХ УПРАВЛЕНИЯ И ЗАЩИТЫ ИНФОРМАЦИИ

Осадчий И.В., студент гр.461401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Фильченкова Т.М. – старший преподаватель каф. ЗИ

Аннотация. В работе исследуются импульсные методы модуляции амплитудно-импульсная (АИМ) и широтно-импульсная модуляция (ШИМ). Проведено моделирование формирования ШИМ-сигнала и выполнен анализ его временных и спектральных характеристик. Показано наличие спектральных составляющих на частоте информационного сигнала и гармониках несущей. Также выполнена оценка помехоустойчивости при воздействии аддитивного белого шума и исследована зависимость вероятности битовой ошибки от отношения сигнал/шум. Результаты подтверждают устойчивость ШИМ-сигнала к шумовым воздействиям и возможность его применения в системах управления и передачи данных.

Ключевые слова. Широтно-импульсная модуляция, амплитудно-импульсная модуляция, ШИМ-сигнал, спектральный анализ, коэффициент заполнения, помехоустойчивость, аддитивный белый шум, отношение сигнал/шум, вероятность битовой ошибки, цифровая передача сигналов.

В условиях стремительного развития цифровых технологий и роста объемов передаваемой информации особую актуальность приобретают методы преобразования аналоговых сигналов в форму, пригодную для цифровой обработки и передачи по каналам связи. Современные системы дистанционного управления, автоматизации технологических процессов, робототехники и беспилотных летательных аппаратов требуют высокой надёжности, помехоустойчивости и защищённости каналов передачи управляющих сигналов. В этой связи импульсные методы модуляции занимают важное место в теории электрической связи и практике построения телекоммуникационных систем. Амплитудно-импульсная и широтно-импульсная модуляции относятся к числу базовых способов представления аналоговой информации в импульсной форме. Они широко применяются в системах управления электроприводами, источниках вторичного электропитания, преобразователях энергии, а также в каналах передачи управляющих воздействий.

Амплитудно-импульсная модуляция представляет собой способ кодирования информации, при котором амплитуда периодически повторяющихся импульсов изменяется пропорционально мгновенному значению аналогового сигнала, тогда как их длительность и период повторения остаются постоянными [1].

$$U_{\text{АИМ}}(t) = U(1 + m \sin \Omega t) \left(\frac{1}{Q} + \sum_{k=1}^{\infty} \frac{2}{k\pi} \sin \frac{k\pi}{Q} \cos k\omega_1 t \right), \quad (1)$$

где U – амплитуда сигнала; m – коэффициент глубины модуляции; k – коэффициент пропорциональности; Q – скважность сигнала.

Такой подход обеспечивает простоту реализации и позволяет осуществлять дальнейшее квантование сигнала, однако делает систему чувствительной к амплитудным помехам, что особенно критично в условиях зашумлённых каналов связи.

Широтно-импульсная модуляция основана на ином принципе: амплитуда импульсов фиксирована, а информационным параметром является их длительность. Коэффициент заполнения определяется как отношение длительности импульса к периоду повторения [1].

$$U_{\text{ШИМ}}(t) = U \left(\frac{\tau + \Delta\tau \sin \Omega t}{T_1} + \frac{2}{\pi} \sum_{k=1}^{\infty} \frac{1}{k} \sin \left(k\pi \frac{\tau + \Delta\tau \sin \Omega t}{T_1} \right) \cos k\omega_1 t \right), \quad (2)$$

где U – амплитуда сигнала; τ – длительность импульса; $\Delta\tau$ – максимальное приращение ширины импульса.

Благодаря тому, что информация переносится во временную область, ШИМ обладает большей устойчивостью к амплитудным искажениям и широко применяется в системах управления электроприводами, импульсных источниках питания, а также в каналах дистанционного управления беспилотными летательными аппаратами.

Для исследования характеристик сигналов было выполнено моделирование в среде Python. В качестве модулирующего сигнала использована синусоида частотой 50 Гц. На основе дискретизации

был сформирован АИМ-сигнал, представляющий собой последовательность импульсов с амплитудой, пропорциональной значению исходного сигнала в моменты отсчёта. На рисунке 1 приведена осциллограмма исходного аналогового сигнала и осциллограмма сигнала АИМ.

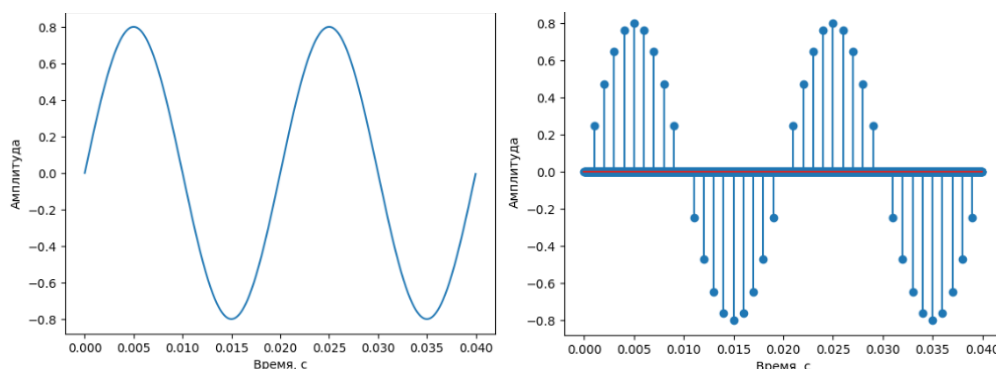


Рисунок 1 – Осциллограмма исходного аналогового сигнала и осциллограмма сигнала АИМ

Далее был реализован процесс формирования ШИМ-сигнала методом сравнения аналогового сигнала с пилообразным опорным напряжением. Демодуляция осуществлялась с помощью цифрового фильтра нижних частот. Полученный сигнал после фильтрации повторяет форму исходной синусоиды с допустимой погрешностью, что подтверждает корректность модели и принцип восстановления аналоговой информации из ШИМ-последовательности [2]. На рисунке 2 показана осциллограмма ШИМ-сигнала и осциллограмма демодулированного ШИМ сигнала.

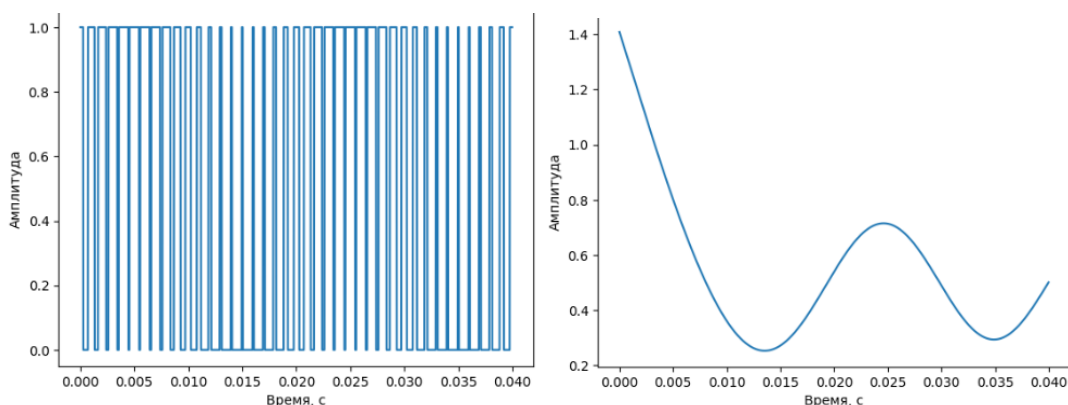


Рисунок 2 – Осциллограмма ШИМ-сигнала и осциллограмма демодулированного ШИМ сигнала

Спектральный анализ ШИМ-сигнала показал наличие выраженной составляющей на частоте информационного сигнала, а также спектральных линий на частоте несущей и её гармониках. Расширение спектра по сравнению с исходным сигналом обусловлено импульсной природой модуляции. Дополнительно была проведена оценка помехоустойчивости путём моделирования аддитивного белого шума и расчёта зависимости вероятности битовой ошибки от отношения сигнал/шум. Полученный график демонстрирует снижение вероятности ошибки при увеличении отношения сигнал/шум, что подтверждает устойчивость ШИМ к шумовым воздействиям. При высоких значениях отношения сигнал/шум вероятность ошибки стремится к нулю, что делает данный метод перспективным для применения в системах управления, требующих высокой надёжности передачи команд. На рисунке 3 представлен амплитудный спектр ШИМ-сигнала и показана зависимость вероятности битовой ошибки от отношения сигнал/шум.

С точки зрения информационной безопасности канал ШИМ представляет особый интерес. Поскольку информация закодирована во временной длительности импульсов, незначительное изменение их ширины может использоваться для скрытого внедрения дополнительных данных. Такие изменения могут быть практически незаметны для стандартных алгоритмов управления, но при этом позволяют реализовать скрытый канал передачи информации [3]. Это создаёт потенциальную угрозу для систем дистанционного управления дронами, промышленными объектами и элементами критической инфраструктуры. Внедрение скрытых команд или управляющих последовательностей через модификацию коэффициента заполнения может привести к нарушению устойчивости системы или выполнению несанкционированных действий.

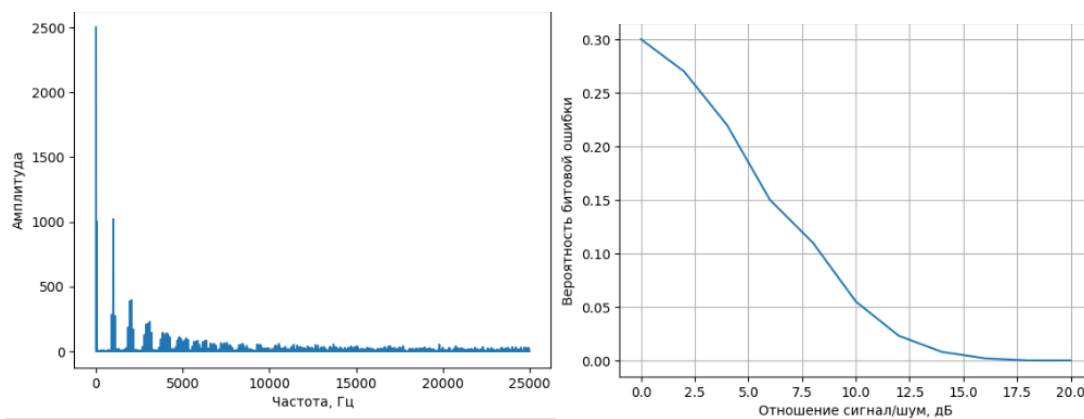


Рисунок 3 – Амплитудный спектр ШИМ-сигнала
и зависимость вероятности битовой ошибки от отношения сигнал/шум

Для обнаружения подобных искажений предложен метод контроля целостности сигнала, основанный на статистическом анализе длительности импульсов. В процессе работы системы принимается последовательность импульсов ШИМ за заданный интервал наблюдения, после чего для каждого импульса определяется его длительность t_i и период повторения T_i . На основании этих параметров для каждого периода вычисляется коэффициент заполнения, который определяется выражением:

$$Di = \frac{t_i}{T_i}. \quad (3)$$

После определения коэффициентов заполнения для всей последовательности из N импульсов вычисляется их среднее значение:

$$\bar{D} = \frac{1}{N} \sum_{i=1}^N Di. \quad (4)$$

Далее определяется дисперсия коэффициентов заполнения, характеризующая степень отклонения длительностей импульсов от среднего значения:

$$\sigma^2 = \frac{1}{N} \sum_{i=1}^N (Di - \bar{D})^2. \quad (5)$$

Полученное значение дисперсии сравнивается с эталонным значением σ^2 , соответствующим нормальному режиму функционирования системы. Если разность между текущим и эталонным значением дисперсии превышает допустимый порог, то фиксируется возможное нарушение целостности передаваемого сигнала. Дополнительно может применяться спектральный анализ последовательности импульсов, позволяющий выявлять появление побочных гармоник, возникающих при систематическом изменении длительности импульсов. Для повышения уровня защиты системы возможно использование криптографических методов контроля, например формирование цифровой подписи пакетов импульсов или вычисление контрольной хеш-суммы последовательности коэффициентов заполнения, что позволяет обнаруживать несанкционированные изменения параметров сигнала.

Таким образом, проведённое исследование показало, что амплитудно-импульсная и широтно-импульсная модуляции являются эффективными методами представления аналоговой информации в импульсной форме, при этом ШИМ обладает большей помехоустойчивостью и энергетической эффективностью. Одновременно временная природа кодирования создаёт потенциальные возможности для скрытого внедрения информации, что требует разработки специализированных методов контроля целостности. Полученные результаты подтверждают необходимость комплексного подхода к защите каналов связи, сочетающего методы теории электрической связи и инструменты информационной безопасности.

Список использованных источников:

1. Сорока, Н. И. Телемеханика. Линии связи и безопасность устройств и сетей: учеб. пособие / Н. И. Сорока, Г. А. Кривинченко, Е. В. Тарасюк. – Минск: БГУИР, 2023. – 240 с.
2. Баскаков, С. И. Радиотехнические цепи и сигналы: учеб. пособие для вузов / С. И. Баскаков. – М.: Высшая школа, 2000. – 462 с.
3. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – 2-е изд. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

МЕТОДЫ АКТИВНОЙ И ПАССИВНОЙ ЗАЩИТЫ ОТ АТАК ТИПА BADUSB НА ОСНОВЕ ЭМУЛЯЦИИ HID-УСТРОЙСТВ

Погирейчик В.В., студент гр.361402

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Мокеров В.С. – ассистент каф. ЗИ

Аннотация. Статья посвящена исследованию методов активной и пассивной защиты от атак типа BadUSB, основанных на эмуляции HID-устройств. Анализируются достоинства и недостатки существующих подходов к обнаружению подмены класса USB-устройства. Рассматриваются пассивные методы, включающие анализ дескрипторов устройств и мониторинг событий ввода, а также активные меры, такие как блокировка системных интерпретаторов, фильтрация HID-отчётов и ограничение доступа для неподтверждённых устройств. Обосновывается эффективность гибридной модели защиты, не требующей использования специализированного оборудования.

Ключевые слова. кибербезопасность, BadUSB, USB-устройство, USB, атака, программное обеспечение, защита, пользователь.

В мире кибербезопасности существует множество угроз, и некоторые из них используют маскировку под безобидные устройства. Одной из таких угроз является BadUSB – атака, при которой вредоносное программное обеспечение загружается на USB-устройство, заставляя его вести себя как другое, более опасное устройство. Чаще всего это эмуляция клавиатуры (HID – Human Interface Device), которая может выполнять команды, вводить текст или даже запускать вредоносные скрипты без ведома пользователя.

Суть атаки BadUSB заключается в том, что злоумышленник перезаписывает прошивку USB-контроллера устройства. Это означает, что устройство перестает быть просто «флешкой» или «мышкой» и может имитировать любое другое HID-устройство. Наиболее распространенные сценарии включают:

Эмуляция клавиатуры, при котором устройство может "печатать" команды, которые запускают вредоносные программы, скачивают файлы, изменяют настройки системы или даже удаляют данные. Это происходит настолько быстро, что пользователь может даже не заметить, что что-то происходит.

Эмуляция сетевой карты, при котором устройство может создавать виртуальную сетевую карту, через которую злоумышленник может перехватывать трафик или получать доступ к сети.

Эмуляция USB-модема, при котором устройство позволяет злоумышленнику получить доступ к интернету через зараженное устройство.

Главная опасность BadUSB заключается в его невидимости. Антивирусное программное обеспечение часто не может обнаружить вредоносную прошивку, так как она находится на аппаратном уровне, а не в файловой системе.

Защита от BadUSB требует комплексного подхода, сочетающего пассивные и активные меры.

Пассивная защита направлена на минимизацию вероятности заражения устройства BadUSB. Одним из методов является ограничение использования неизвестных USB-устройств. Политика «не подключать ничего, кроме доверенных устройств» – это самый простой, но эффективный метод. USB-порты могут быть физически заблокированы или отключены на уровне BIOS. Создание списка разрешённых USB-устройств позволяет блокировать любое устройство, не входящее в данный перечень. Использование специализированного оборудования включает применение USB-дата-блокеров, которые физически блокируют передачу данных через USB-порт, допуская только зарядку подключённых устройств. USB-фильтры – это некоторые аппаратные решения могут фильтровать USB-трафик, блокируя подозрительные команды или типы устройств. Регулярное обновление прошивок и программного обеспечения является необходимым условием защиты, для чего важно поддерживать в актуальном состоянии операционную систему и драйверы. Это требуется для обнаружения и нейтрализации некоторых видов вредоносного ПО, которое может быть установлено после успешной эмуляции HID [1].

В основе подхода минимизация поверхности атаки через блокировку системных интерпретаторов, в основании которого лежит принцип минимизации привилегий и ограничения доступа к критическим системным интерпретаторам.

Поскольку атаки на базе эмуляции HID-устройств опираются на автоматизированный ввод последовательности символов для вызова командных оболочек, блокировка исполняемых файлов powershell.exe и cmd.exe через системный реестр или групповые политики нивелирует вектор атаки. При подключении вредоносного устройства и попытке инициализации командного сценария операционная система блокирует запуск целевого процесса, руководствуясь установленными правилами ограничения программного обеспечения. Таким образом, даже при успешной эмуляции клавиатуры и воспроизведении полезной нагрузки, выполнение деструктивного кода становится

невозможным из-за отсутствия доступного интерпретатора в пользовательской сессии, что представлено на рисунке 1. Данный метод демонстрирует эффективность превентивных мер, направленных на сужение поверхности атаки без использования специализированных аппаратных средств защиты.

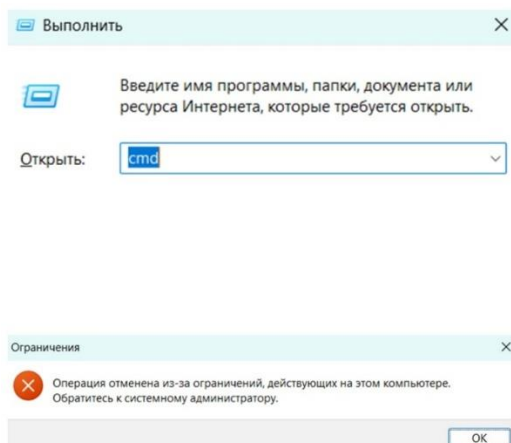


Рисунок 1 – Результат блокировки интерпретаторов

Активная защита – это обнаружение и реагирование на вредоносные воздействия. Активная защита направлена на выявление и нейтрализацию уже активных атак BadUSB. Мониторинг поведения USB-устройств – это анализ HID-событий. Системы мониторинга могут отслеживать события, генерируемые HID-устройствами [2].

Специализированное программное обеспечение может анализировать последовательность и тип генерируемых HID-событий, сравнивая их с типичным поведением доверенных устройств. Для обнаружения аномалий нужны системы обнаружения вторжений и системы управления информацией и событиями безопасности, которые могут быть настроены на выявление аномального поведения USB-устройств. Использование специализированного программного обеспечения для обнаружения BadUSB. Это сканирование прошивки USB-контроллеров. Существуют инструменты, которые пытаются обнаружить модифицированную прошивку на USB-контроллерах. Эмуляция «ловушек» – это создание виртуальных USB-устройств или портов, которые при подключении к ним подозрительного устройства будут генерировать предупреждения, не позволяя выявить атакующего, не подвергая реальные системы риску. Контроль целостности прошивки – это цифровые подписи прошивок. USB-устройства должны иметь прошивки с цифровыми подписями от доверенных производителей. Системы могут проверять эти подписи перед разрешением устройству работать в полном режиме. Однако, это требует поддержки со стороны производителей и не является широко распространенной практикой для всех типов USB-устройств. [3].

Важные серверы и рабочие станции должны быть максимально изолированы от внешних USB-устройств. Разделение сети на более мелкие сегменты может ограничить распространение вредоносного ПО, если атака BadUSB все же произойдет.

Атаки BadUSB представляют собой серьезную угрозу, поскольку они используют доверие к обычным устройствам и действуют на аппаратном уровне, что затрудняет их обнаружение. Комплексный подход, сочетающий пассивные меры предотвращения и активные методы обнаружения и реагирования, является ключом к эффективной защите. Внедрение строгих политик использования USB-устройств, использование специализированного оборудования и программного обеспечения, а также постоянное обучение пользователей помогут минимизировать риски и обеспечить безопасность цифровой среды от этой невидимой угрозы.

Список использованных источников:

1. Полежаев П.Н., Малахов А.К., Сагитов А.М. «Ахиллесова пята» USB-устройств: атака и защита // *Философские проблемы информационных технологий и киберпространства*. 2015. № 1(9). С. 106–117.
2. Агуров П.В. *Интерфейс USB. Практика использования и программирования*. СПб. : БХВ-Петербург, 2004. 576 с.
3. Петин В.А. *Проекты с использованием контроллера Arduino*. СПб. : БХВ-Петербург, 2015. 448 с.

ОЦЕНКА ЗАЩИЩЕННОСТИ И ПРАКТИЧЕСКИЕ МЕТОДЫ ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ КОРПОРАТИВНЫХ МЕЖСЕТЕВЫХ ЭКРАНОВ НА ПРИМЕРЕ CHECK POINT T-110

Седляр А.С., Боздаг Бора, студенты гр.361402

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Белоусова Е.С. – канд. техн. наук, доцент

Аннотация. В работе проведена комплексная оценка защищенности аппаратного межсетевого экрана корпоративного класса Check Point T-110. Описан процесс развертывания испытательного стенда и инициализации устройства в ОС Gaia. Проведен анализ устойчивости системы к ряду критических уязвимостей, включая CVE-2024-24919 и CVE-2024-6387. В ходе экспериментально-практического исследования выявлены условия реализации атаки типа IP-спуфинг при стандартных настройках политик безопасности. Предложены практические методы эксплуатации данной уязвимости и алгоритм ее нейтрализации с использованием встроенных механизмов Anti-Spoofing. Полученные результаты могут быть использованы при проектировании защищенных корпоративных сетей.

Ключевые слова. Информационная безопасность, межсетевой экран, Check Point T-110, ОС Gaia, оценка защищенности, уязвимость, CVE, сетевая атака, IP-спуфинг, эксплуатация уязвимостей, Anti-Spoofing, сетевой периметр, аудит безопасности.

Актуальность защиты периметра корпоративных сетей в современных условиях обусловлена постоянным усложнением киберугроз, что требует внедрения высоконадежных решений для обеспечения информационной безопасности. Одним из признанных лидеров на рынке средств сетевой защиты выступает оборудование компании Check Point Software Technologies, межсетевые экраны которой широко применяются для глубокой фильтрации трафика и предотвращения вторжений. Целью данной работы является проведение комплексного аудита безопасности аппаратного межсетевого экрана Check Point T-110 для оценки уровня его устойчивости к актуальным векторам атак.

В качестве объекта исследования рассматривается аппаратный межсетевой экран Check Point T-110, функционирующий под управлением специализированной операционной системы Gaia R80.40. Испытательный стенд был развернут путем аппаратного сброса устройства до заводских настроек и первоначальной инициализации через консоль FTW (First Time Wizard), при этом управление конфигурацией осуществлялось посредством клиентского программного обеспечения SmartConsole. С целью всестороннего аудита безопасности проведена проверка устойчивости объекта к актуальным угрозам путем выявления ряда критических уязвимостей, зафиксированных в базе CVE [1]. В ходе тестирования попытки эксплуатации CVE-2024-24919, связанной с произвольным чтением файлов (Path Traversal), а также CVE-2023-28130, допускающей внедрение команд через механизмы обработки DNS, не увенчались успехом. Отсутствие реализации данных векторов атак обусловлено спецификой конфигурации испытательного стенда, в частности, ограничением доступа к веб-интерфейсу управления, что минимизирует поверхность атаки. Аналогичные результаты были получены при анализе защищенности от уязвимости CVE-2024-6387 (regreSSHion). Исследование показало, что в операционной системе Gaia задействована версия OpenSSH 7.2p1, которая не входит в диапазон версий, подверженных данной бреши в защите, что свидетельствует об устойчивости системы к удаленной эксплуатации в процессе аутентификации. Дополнительно была проанализирована вероятность проведения атаки типа DLL Hijacking через клиентское приложение SmartConsole (CVE-2020-6024). Установлено, что используемая сборка программного обеспечения уже содержит необходимые исправления, блокирующие возможность подмены динамических библиотек. В итоге проведенная оценка подтвердила эффективность встроенных механизмов защиты и актуальность применяемых патчей безопасности для рассматриваемого оборудования.

Несмотря на устойчивость системы к известным программным уязвимостям, было выдвинуто предположение о возможности обхода защиты на сетевом уровне через IP-спуфинг. Теоретической основой реализации атаки данного типа является преднамеренная подмена адреса источника в IP-пакете с целью обхода политик контроля доступа или имитации трафика от доверенного узла сети [2]. Для практической проверки уязвимости использовалась сетевая утилита hping3 в ОС Kali Linux, предназначенная для генерации произвольных пакетов и анализа сетевых стеков. В ходе эксперимента с помощью hping3 был сформирован ICMP-пакет, в котором посредством параметра -a был указан IP-адрес, принадлежащий сегменту доверенной внутренней сети. При этом пакет физически отправлялся со стороны внешнего интерфейса межсетевого экрана. Тестирование показало, что при стандартной конфигурации политик безопасности устройство беспрепятственно пропускает поддельные пакеты, если они формально соответствуют разрешающим правилам фильтрации. Вследствие отсутствия автоматического сопоставления физического интерфейса получения пакета с его исходным адресом становится возможным проведение несанкционированного сканирования от имени легитимного хоста (рисунок 1).

```

└─$ sudo hping3 -S -a 10.0.0.1 -p 80 192.168.31.154 -c 1
HPING 192.168.31.154 (eth0 192.168.31.154): S set, 40 headers + 0 data bytes
— 192.168.31.154 hping statistic —

```

Рисунок 1 – Реализация атаки IP-спуфинг с использованием утилиты hping3

В отличие от угроз, связанных с программными ошибками в коде сервисов (CVE), нейтрализация выявленной проблемы требует не установки патчей, а корректной архитектурной настройки параметров безопасности. В среде SmartConsole для устранения данной уязвимости была задействована функция Anti-Spoofing [3]. Исправление конфигурации осуществлялось согласно следующему алгоритму: в свойствах конкретного сетевого интерфейса в разделе “Topology” активировался механизм “Perform Anti-Spoofing based on interface topology”, после чего указывалась конкретная сеть, закрепленная за данным интерфейсом (рисунок 2). Вследствие активации указанных настроек и последующей инсталляции политики межсетевой экран начал выполнять проверку соответствия входящего интерфейса и адреса источника пакета. Повторная попытка генерации трафика посредством hping3 привела к немедленной блокировке пакетов на уровне ядра ОС Gaia. Это позволяет обеспечить целостность сетевого периметра и исключить возможность эксплуатации доверительных отношений между узлами сети на основе IP-адресации [4].

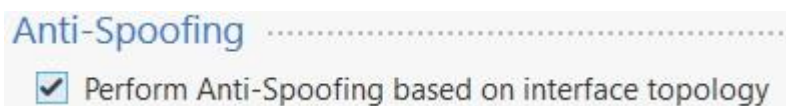


Рисунок 2 – Активация функции Anti-Spoofing в среде SmartConsole

Проведенное исследование показало, что аппаратный межсетевой экран Check Point T-110 обладает высоким уровнем базовой защищенности на уровне ядра операционной системы и используемых версий программных компонентов, что подтверждается устойчивостью устройства к ряду актуальных критических уязвимостей (CVE). В то же время выявлено, что обеспечение безопасности от сетевых атак, связанных с подменой идентификационных данных (IP-спуфинг), требует обязательной экспертной настройки политик сетевой топологии и ручной активации механизмов Anti-Spoofing администратором. В итоге гарантированная защита корпоративного периметра достигается только при сочетании штатных обновлений безопасности и корректной конфигурации функций контроля трафика.

Список использованных источников:

1. CVE - CVE [Электронный ресурс] / CVE Program. – Режим доступа: <https://www.cve.org/>. – Дата доступа: 06.04.2026.
2. IP Spoofing: что это и как работает [Электронный ресурс] / АО «Лаборатория Касперского». – Режим доступа: <https://www.kaspersky.ru/resource-center/threats/ip-spoofing>. – Дата доступа: 07.04.2026.
3. Check Point Security Gateway Support for Anti-Spoofing [Electronic resource] / Check Point Support Center. – Mode of access: <https://support.checkpoint.com/results/sk/sk180814>. – Date of access: 07.04.2026.
4. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. пособие / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2020. – 992 с.

ОСОБЕННОСТИ РЕАЛИЗАЦИИ НЕЙРОСЕТЕЙ НА ПЛАТФОРМАХ STM32/CORTEX-M ДЛЯ ЗАДАЧ ОБНАРУЖЕНИЯ ЗАКЛАДНЫХ УСТРОЙСТВ ИМПУЛЬСНО-РЕФЛЕКТОРНЫМ МЕТОДОМ

Сурвило И.С., магистрант гр.467241

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Петров С.Н. – канд. техн. наук, доцент

Аннотация. В статье рассматривается применение нейросетевых технологий для обнаружения закладных устройств импульсно-рефлекторным методом. Особое внимание уделено реализации на микроконтроллерах STM32 в парадигме TinyML. Описаны этапы разработки: сбор и разметка данных, выбор архитектуры нейросети (свёрточные, рекуррентные или временные сети), квантование и обрезка моделей. Представлена конфигурация периферии (АЦП, таймер, DMA) для синхронизированного сбора данных. Ключевыми инструментами выступают TensorFlow Lite for Microcontrollers, CMSIS-NN и STM32CubeAI.

Ключевые слова. Обнаружение закладных устройств, импульсно-рефлекторный метод, нейросетевые технологии, TinyML, STM32, добротность, обработка временных рядов, сверточные нейронные сети, CMSIS-NN, TensorFlow Lite for Microcontrollers, STM32CubeAI.

Задача обнаружения закладных устройств с использованием импульсно-рефлекторного метода представляет собой специфическую область радиофизического контроля, где нейросетевые технологии могут значительно повысить точность и надежность обнаружения. Основная идея метода заключается в облучении исследуемой области зондирующими электромагнитными импульсами и анализе отраженных сигналов. Эффективность метода для обнаружения ЗУ обусловлена их конструктивными особенностями, а именно наличием высокодобротных антенных систем. Добротность, или Q-фактор, является ключевым параметром, характеризующим способность колебательного контура эффективно накапливать и отдавать энергию при резонансе. Антенные системы большинства ЗУ работают в узком диапазоне частот, что делает их чувствительными к воздействию зондирующего сигнала, частота которого совпадает с их собственной резонансной частотой. Когда зондирующий импульс попадает на контур с высокой добротностью, в нем наводятся токи с резко возрастающей амплитудой, что приводит к значительному увеличению мощности отраженного сигнала. Полезный сигнал представляет собой сложный временной сигнал, содержащий прямой отклик от резонансного контура ЗУ, форма которого зависит от резонансной частоты, Q-фактора и степени затухания. Чем выше Q-фактор, тем медленнее затухают колебания после воздействия короткого импульса, создавая длинную осциллирующую часть на графике сигнала. Этот уникальный временной профиль является основным диагностическим признаком наличия ЗУ. Входной сигнал для нейросети всегда будет содержать фоновый электромагнитный шум окружающей среды, а также отражения от других металлических предметов и поверхностей. Классические подходы, основанные на простых пороговых значениях или быстром преобразовании Фурье, часто оказываются неэффективными в условиях сложного шумового фона, так как они плохо различают форму сигнала. Исходя из этого нейросеть, особенно архитектуры, предназначенные для обработки временных рядов, становится эффективным инструментом. Сверточная нейронная сеть может выделять локальные признаки формы сигнала, такие как крутизна фронта или период колебаний, в то время как рекуррентные сети могут улавливать временные зависимости между различными участками сигнала [1].

Для успешного обучения нейросетевой модели критически важно правильно сформировать обучающий набор данных, который должен быть максимально разнообразным и покрывать все возможные сценарии. Набор должен состоять из трех основных классов сигналов:

- сигналы наличия ЗУ от различных типов устройств на разных частотах и с разными параметрами Q-фактора, в том числе за препятствиями;
- сигналы отсутствия ЗУ, включающие чистый фоновый шум помещения и отражения от стационарных объектов;
- сигналы шума и помех от других радиоустройств для повышения устойчивости модели.

Методология сбора данных может быть как экспериментальной, так и основанной на моделировании, позволяющем быстро сгенерировать большие объемы данных. После сбора данных требуется их обработка и нормализация: обрезка до фиксированной длины, масштабирование до единого диапазона и разметка по классам. Качество разметки напрямую влияет на итоговую точность модели.

Выбор и последующая оптимизация архитектуры нейронной сети являются центральными этапами разработки решения для обнаружения закладных устройств на микроконтроллерах семейства STM32. Устройства данного класса характеризуются жесткими ограничениями по объему оперативной памяти, флэш-памяти и вычислительной производительности, поэтому применение глубоких и широких моделей, обученных на графических процессорах для облачных задач, абсолютно невозможно. TinyML предлагает комплекс методов для адаптации нейросетевых моделей под эти условия, позволяя запускать модели машинного обучения непосредственно на устройстве с минимальными ресурсами. Учитывая, что

входными данными являются одномерные временные ряды, наиболее перспективны архитектуры, специально разработанные для обработки последовательных данных [2]. Сверточные нейронные сети эффективны для обработки временных рядов, способны автоматически извлекать локальные признаки из сигнала, а легковесные вариации с использованием сверток с разделением глубины значительно сокращают количество параметров и вычислительную сложность. Рекуррентные нейронные сети и их вариации LSTM и GRU изначально предназначены для работы с последовательными данными и способны улавливать долгосрочные временные зависимости, однако могут быть более ресурсоемкими. Временные сверточные сети сочетают лучшие свойства CNN и RNN, используя свертки с расширенными ядрами для получения большого окна восприятия без увеличения глубины сети, и часто демонстрируют лучшую производительность по сравнению с RNN. Главным инструментом в TinyML является квантование – преобразование весов и активаций нейронной сети из 32-битных чисел с плавающей запятой в 8-битные целочисленные представления. Квантование дает три ключевых преимущества: резкое сокращение размера модели в четыре раза, значительное ускорение вычислений за счет аппаратной поддержки SIMD-инструкций в процессорах Cortex-M, а также снижение потребления энергии, что критически важно для автономных устройств.

Существует два подхода к квантованию. Квантование после обучения просто в реализации, но может привести к заметной потере точности. Квантование с учетом обучения, при котором в процессе обучения модели искусственно имитируется эффект квантования, заставляет сеть привыкнуть к работе с целочисленными значениями и обычно приводит к гораздо меньшей потере точности. Современные фреймворки, такие как TensorFlow Lite, предоставляют инструменты для обоих подходов. Помимо квантования, для дальнейшего сжатия модели используются обрезка – процесс удаления незначительных весов из сети, что экономит память и время вычислений. Эти техники часто комбинируются: модель сначала оптимизируется для поиска легкой архитектуры, затем к ней применяется квантование и обрезка. Инструменты, такие как STM32Cube.AI, интегрируют часть этих процессов и позволяют генерировать код для оптимизированных моделей, которые затем выполняются с использованием высокооптимизированных библиотек CMSIS-NN.

Успешная реализация нейросетевой модели для обнаружения скрытых устройств на микроконтроллерах невозможна без глубокого понимания аппаратных возможностей целевой платформы и доступного программного инструментария. Экосистема STM32 предоставляет целостное решение для разработчиков, включая широкий спектр 32-битных ARM Cortex-M процессоров, оптимизированные математические библиотеки и мощные средства автоматической генерации кода. Для задач обнаружения ЗУ наиболее интересны высокопроизводительные серии, такие как STM32H7 и более новые STM32N6. Процессоры Cortex-M7 способны работать с частотой до 480-550 МГц, предоставляя значительную вычислительную мощность. Серия STM32N6 идет еще дальше, предлагая встроенные нейронные процессоры, специально спроектированные для ускорения операций нейронных сетей, которые могут выполнять прогнозирование квантованных моделей с высокой скоростью и крайне низким энергопотреблением, освобождая основной процессор для других задач. Самая важная часть аппаратной поддержки TinyML – это наличие оптимизированных математических библиотек CMSIS-DSP и CMSIS-NN [2].

CMSIS-DSP содержит множество функций для цифровой обработки сигналов, таких как быстрое преобразование Фурье, цифровые фильтры и матричные операции, оптимизированные для процессоров Cortex-M с поддержкой операций с плавающей и фиксированной запятой.

CMSIS-NN – это специализированная библиотека, содержащая высокооптимизированные ядра для основных операций нейронных сетей: свертки, полносвязные слои, пулинг и активационные функции. Эти ядра написаны на ассемблере для конкретных моделей Cortex-M и используют все доступные аппаратные возможности для достижения максимальной производительности.

На программном уровне центральное место занимает TensorFlow Lite for Microcontrollers – открытый фреймворк от Google, специально разработанный для запуска моделей машинного обучения на устройствах с ограниченными ресурсами, предоставляющий среду выполнения, управляющую памятью и выполняющую операции модели. TensorFlow Lite for Microcontrollers по умолчанию использует CMSIS-NN в качестве движка для выполнения вычислений на Cortex-M процессорах. Для упрощения разработки STMicroelectronics создала X-CUBE-AI – пакет расширения для STM32CubeIDE, который берет на вход предварительно обученную и оптимизированную модель в формате TensorFlow Lite или ONNX и автоматически генерирует готовый к использованию С-код. Процесс генерации включает создание С-структур, описывающих архитектуру сети, генерацию массивов данных с весами и смещениями, генерацию С-функций для прогнозирования с вызовом ядер CMSIS-NN, а также предоставление простого API.

Процесс разработки нейросетевого приложения для обнаружения скрытых устройств на платформе STM32 представляет собой четко структурированную последовательность этапов.

Первый этап – обучение модели в среде высокопроизводительных вычислений на Python с использованием TensorFlow и Keras. На этом этапе выбирается исходная архитектура, показывающая хорошие результаты на обучающем наборе данных, проводится обучение до достижения приемлемого

уровня точности, при необходимости проводится квантование с учетом обучения. По завершении обучения модель сохраняется в нативном формате фреймворка.

Второй этап – оптимизация и преобразование модели с помощью TensorFlow Lite Converter, который конвертирует модель в формат TensorFlow Lite. Именно на этом этапе происходит основное квантование весов и активаций из 32-битных чисел с плавающей запятой в 8-битные целые числа. Конвертер позволяет указать тип входных данных и предоставляет возможность использовать файл с эталонными данными для калибровки, что помогает минимизировать потерю точности. Результатом является файл «.tflite», содержащий архитектуру и параметры модели в целочисленном представлении [2].

Третий этап – генерация кода с помощью инструмента X-CUBE-AI. Пользователь загружает файл «.tflite» в мастер-конфигуратор, инструмент анализирует архитектуру модели, рассчитывает необходимый объем памяти, проверяет возможность размещения модели в памяти целевого микроконтроллера и генерирует набор C-файлов и заголовочных файлов, содержащих массивы с квантованными весами, заготовки функций инференса и API для инициализации, загрузки входных данных и получения результатов.

Четвертый этап – интеграция и разработка приложения. Сгенерированные файлы добавляются в проект микроконтроллера. Основной код приложения инициализирует периферийные модули: АЦП, таймеры и DMA для настройки сбора данных. По сигналу от таймера, синхронизированному с моментом отправки зондирующего импульса, АЦП начинает преобразование отраженного сигнала, данные передаются через DMA напрямую в буфер в оперативной памяти без нагрузки на центральный процессор. Когда буфер заполняется, программа вызывает функцию прогнозирования, сгенерированную X-CUBE-AI, которая копирует данные в буфер ввода нейронной сети и последовательно выполняет все операции, используя оптимизированные ядра CMSIS-NN с целочисленной арифметикой.

После завершения вычислений в выходном буфере находится массив вероятностей для каждого класса, приложение считывает его, определяет класс с максимальной вероятностью и принимает решение.

Для микроконтроллеров STM32 существует стандартная и чрезвычайно эффективная конфигурация периферийных модулей: синхронизированный сбор данных с помощью АЦП, таймера и DMA. Эта конфигурация позволяет минимизировать нагрузку на центральный процессор и обеспечить сбор данных с высокой частотой дискретизации, что критически важно для корректного анализа формы отраженного импульса. Таймер настраивается для генерации регулярных событий с необходимой частотой, которые служат триггером для АЦП, запуская преобразование аналогового напряжения в цифровое значение, и могут использоваться для генерации самого зондирующего импульса, что обеспечивает точную синхронизацию. АЦП конфигурируется для работы в режиме непрерывного сканирования канала. DMA настраивается на чтение регистра данных АЦП и автоматическую запись этих данных в заранее выделенный массив в оперативной памяти, позволяя центральному процессору свободно выполнять другие задачи или находиться в спящем режиме. Только по завершении сбора всей временной последовательности DMA генерирует прерывание, и ЦП передает собранный массив данных на вход нейросетевой модели для анализа. Качество входных данных зависит от разрядности АЦП (чем выше разрядность, тем больше динамический диапазон), скорости АЦП (максимальная частота дискретизации определяет плавность фиксации формы сигнала) и точности тактового генератора (любые флуктуации частоты таймера приведут к некорректной временной шкале). Для дополнительного анализа в частотной области можно использовать функции FFT из библиотеки CMSIS-DSP, преобразующие временной ряд в массив амплитуд и фаз различных частотных составляющих, что может быть полезно для выделения частотных признаков, менее выраженных во временной области. Управление памятью является важным аспектом: буфер для хранения сырых данных АЦП должен быть точно рассчитан на требуемую длительность сигнала, память под веса модели выделяется статически из расчетов X-CUBE-AI, память для промежуточных активаций также выделяется статически и является одним из главных источников потребления RAM.

На данный момент технология TinyML является единственным жизнеспособным подходом для решения поставленной задачи на ресурсограниченных микроконтроллерах, а центральным технологическим стеком является связка TensorFlow Lite for Microcontrollers, библиотеки CMSIS-NN и инструмента STM32CubeAI. При выборе аппаратной платформы стоит отдать предпочтение моделям с процессорами Cortex-M7 или новейшим Cortex-M85 с встроенным нейронным процессором, обеспечивающим максимальную производительность и энергоэффективность для прогнозирования нейронных сетей.

Список использованных источников:

1. Сурвило, И.С. Импульсно-рефлекторный метод обнаружения закладных радиоустройств / И.С. Сурвило, С.Н. Петров // Технические средства защиты информации : материалы XXIII Международной научно-технической конференции / Белорусский государственный университет информатики и радиоэлектроники [и др.] ; редкол.: О. В. Бойправ [и др.]. – Минск, 2025. – С. 303–307.
2. Йодиче, Дж. TinyML. Книга рецептов / Дж. Йодиче. – М.: ДМК Пресс, 2023. – 298 с.

ИССЛЕДОВАНИЕ СКРЫТНОСТИ СИГНАЛОВ С РАЗЛИЧНЫМИ ВИДАМИ МАНИПУЛЯЦИЯМИ НА ОСНОВЕ АНАЛИЗА ИХ СПЕКТРАЛЬНЫХ ХАРАКТЕРИСТИК

Фам Тхи Хонг Ньунг, студентка гр.461403

Михайловский Д.А., студент гр.461403

Белорусский государственный университет информатики и радиоэлектроники¹
г. Минск, Республика Беларусь

Фильченкова Т.М. – старший преподаватель каф. ЗИ

Аннотация. Исследуется метод распознавания сигналов ASK, FSK и BPSK в условиях экстремально низкого отношения сигнал/шум ($SNR < -15$ дБ). Предложена модель на основе анализа пик-фактора (PAPR) как ключевого параметра для выявления энергетических различий между модуляциями. Установлено, что статистическое усреднение PAPR позволяет эффективно классифицировать сигналы даже при доминирующем влиянии шумов.

Ключевые слова. Цифровая модуляция, скрытность передачи, ASK, FSK, BPSK, спектральная плотность мощности, PAPR, распознавание сигналов.

В современных условиях развития инфокоммуникационных технологий вопросы обеспечения информационной безопасности выходят на первый план. Одним из ключевых аспектов защиты информации является скрытность передачи данных – способность сигнала оставаться незамеченным средствами радиоэлектронной разведки. Даже при использовании современных методов модуляции сигнал может быть обнаружен на основе анализа его энергетических и спектральных характеристик. Исследование скрытности сигналов с различными видами манипуляции является актуальной научно-технической задачей [1].

Практическая значимость данной проблематики обусловлена широким спектром прикладных задач. В области радиоэлектронной борьбы системы обнаружения сигналов применяются для выявления несанкционированных каналов связи, подавления вражеских систем управления и защиты собственных коммуникаций. В гражданской сфере аналогичные методы используются операторами связи для мониторинга радиочастотного спектра и выявления нелегальных передатчиков. В системах критической инфраструктуры – на объектах энергетики, транспорта и государственного управления – обеспечение скрытности каналов передачи данных является обязательным требованием к защищённым коммуникациям [2]. Кроме того, развитие технологий интернета вещей и беспилотных систем порождает новые требования к малозаметной передаче телеметрии и командных сигналов в условиях радиоэлектронного противодействия.

В работе рассматриваются три основных типа цифровой модуляции: амплитудная (ASK), частотная (FSK) и фазовая (BPSK). Для оценки скрытности сигнала необходимо проанализировать распределение его мощности по частоте. Чем равномернее распределена мощность и чем менее выражены дискретные составляющие в спектре, тем сложнее обнаружить сигнал на фоне шумов.

Теоретический анализ спектральной плотности мощности на основе теоремы Винера–Хинчина показал (1 – ASK, 2 – PSK, 3 – FSK):

$$G_s^{ASK}(f) = \frac{A^2 T}{16} \times [\text{sinc}^2(\pi(f - f_c) T)] + \frac{A^2}{16} \delta(f - f_c), \quad (1)$$

$$G_s^{PSK}(f) = \frac{A^2 T}{4} \times [\text{sinc}^2(\pi(f - f_c) T)], \quad (2)$$

$$G_s^{FSK}(f) = \frac{A^2 T}{16} \times [\text{sinc}^2(\pi(f - f_1) T) + \text{sinc}^2(\pi(f - f_2) T)] + \frac{A^2}{16} [\delta(f - f_1) + \delta(f - f_2)], \quad (3)$$

где f_c – несущая частота, T – длительность одного бита, A – амплитуда [3].

Спектр ASK содержит дискретную составляющую на несущей частоте, что обуславливает его низкую скрытность [4]. BPSK характеризуется подавленной несущей – отсутствие дискретных пиков обеспечивает лучшую маскировку. FSK имеет два пика на частотах логических уровней, что также демаскирует сигнал.

Практическое моделирование в среде MATLAB подтвердило теоретические выводы. На рисунке 1 представлены спектры сигналов ASK, BPSK и FSK.

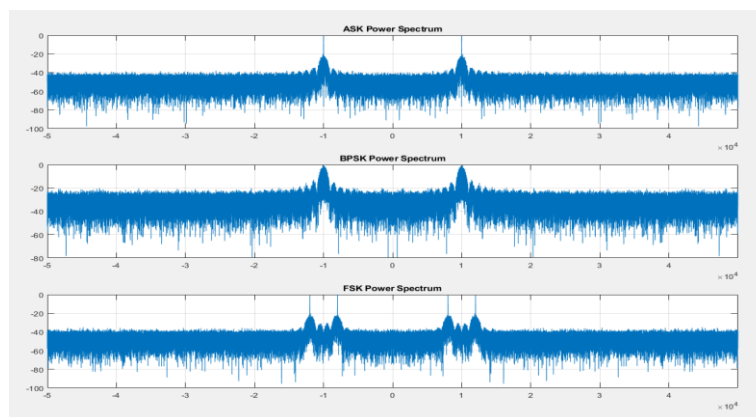


Рисунок 1 – Спектры сигналов ASK, BPSK и FSK

Сравнительный анализ спектральных характеристик представлен в таблице 1.

Таблица 1 – Сравнение спектров различных видов манипуляции

№	Характеристика	ASK	BPSK	BFSK
1	Наличие несущей	Есть (яркий пик)	Нет (подавлена)	Есть (два пика)
2	Ширина спектра	Узкая ($2/T$)	Узкая ($2/T$)	Широкая ($\Delta f + 2/T$)
3	Скрытность	Низкая	Высокая	Средняя / Низкая
4	Энергетическая эффективность	Низкая	Высокая	Средняя

Для распознавания сигналов в условиях экстремально низкого отношения сигнал/шум ($\text{SNR} = -20$ дБ) предложена модель на основе анализа пик-фактора (PAPR – Peak-to-Average Power Ratio). PAPR вычисляется как отношение мгновенной пиковой мощности к средней мощности в скользящих временных окнах [5]:

$$\text{PAPR}_{\text{dB}} = 10 \log\left(\frac{\max |s(t)|^2}{E[|s(t)|^2]}\right). \quad (5)$$

Для преодоления доминирующего влияния белого шума применяется статистическое усреднение значений PAPR по нескольким символьным интервалам. Экспериментальные результаты показали четкое разделение типов модуляции: ASK: $\text{PAPR} \approx 14.00$ дБ; FSK: $\text{PAPR} \approx 12.93$ дБ; BPSK: $\text{PAPR} \approx 12.27$ дБ.

На основе этих различий устанавливаются адаптивные решающие пороги для классификации сигналов. Данный подход позволяет проводить точную идентификацию без необходимости сложной временной и фазовой синхронизации, что особенно важно в условиях ограниченных вычислительных ресурсов.

Таким образом, проведенное исследование подтвердило, что анализ PAPR является надежным инструментом для обнаружения сигналов в сильно зашумленной среде. Наивысшую скрытность продемонстрировал сигнал BPSK благодаря стабильной амплитуде и низкому пик-фактору. Полученные результаты имеют практическую значимость для систем радиоразведки и обнаружения нелегальных каналов связи. Предложенный метод классификации на основе адаптивных решающих порогов по значениям PAPR отличается низкой вычислительной сложностью и не требует предварительной синхронизации по времени и фазе, что делает его пригодным для реализации на встраиваемых платформах с ограниченными ресурсами – в частности, на программно-определяемых радиосистемах и специализированных ПЛИС. Это открывает перспективы для его интеграции в портативные комплексы радиомониторинга и автономные системы обнаружения.

Список использованных источников:

1. Digital Modulation Techniques [Электронный ресурс]: <https://www.geeksforgeeks.org/electronics-engineering/digital-modulation-techniques/>. – Дата доступа: 27.02.2026
2. Signal Encoding Techniques [Электронный ресурс]: <https://www.ccs.neu.edu/home/rtraj/Courses/6710/S10/Notes/SignalsPropagation.pdf>. – Дата доступа: 28.02.2026.
3. Differences between analog and digital modulation methods [Электронный ресурс]: https://en.intwww.de/index.php?title=Modulation_Methods/Linear_Digital_Modulation&direction=prev&oldid=46327. – Дата доступа: 27.02.2026.
4. Digital Modulation [Электронный ресурс]: <https://www.rose-hulman.edu/class/ee/Ferguson/curtiss/Chapter%207%20Digital%20Modulation.pdf>. – Дата доступа: 01.03.2026.
5. Technical identification of digital signals [Электронный ресурс]: https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.1600-2-201508-S!!PDF-E.pdf. – Дата доступа: 01.03.2026.

ПРОГРАММНЫЙ МОДУЛЬ ЗАЩИТЫ HL7-СООБЩЕНИЙ: АНАЛИТИЧЕСКИЙ ОБЗОР ЛИТЕРАТУРНЫХ ИСТОЧНИКОВ

Фомин Д.А., магистрант гр. 467241

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Зельманский О.Б. – канд. тех. наук, доцент

Аннотация. В статье представлен аналитический обзор проблем обеспечения информационной безопасности при обмене медицинскими данными в стандарте HL7. Рассмотрены уязвимости протоколов HL7, связанные с отсутствием шифрования, аутентификации и контроля целостности. Проанализированы существующие подходы к защите: ручная проверка, брандмауэры, сегментация сети и VPN, а также современные научно-технические решения на основе шифрования и технологий распределенных реестров. Обоснована необходимость разработки специализированного программного модуля.

Ключевые слова: HL7; защита медицинских данных; информационная безопасность; шифрование; Twofish; Electronic Health Records; уязвимости; анализ угроз; межсетевые экраны.

Стандарт HL7 (Health Level 7) является доминирующим протоколом для обмена электронными медицинскими записями (EHR) в информационных системах здравоохранения. Однако, как отмечается в современных исследованиях, его широкое распространение сопряжено с серьезными проблемами безопасности. Таким образом для выявления основных угроз и обоснования подхода к разработке программного модуля защиты HL7-сообщений необходимо провести аналитический обзор литературных источников и существующих решений.

Критический анализ литературы показывает, что стандарт HL7 был разработан без учета современных требований безопасности. В работе [1] подчеркивается необходимость внедрения эффективных схем шифрования и иерархического контроля доступа. Однако, как показывают источники, фундаментальные проблемы протокола заключаются в отсутствии нативной поддержки шифрования (данные передаются в открытом виде), слабой или отсутствующей аутентификации (злоумышленник может подключиться к порту TCP 2575) и отсутствии встроенных механизмов проверки целостности сообщений, что делает возможным атаки «человек посередине» с подменой клинических данных, таких как диагнозы или дозировки лекарств.

В исследовании [2] подчеркивается, что технологии защиты медицинских данных должны обеспечивать три основных требования: конфиденциальность (доступ к данным только авторизованных лиц), целостность (защита от несанкционированного изменения) и доступность (обеспечение доступа к данным при лечении пациентов). HL7 в чистом виде не удовлетворяет ни одному из этих требований, что делает необходимым применение дополнительных средств защиты.

Современные исследования подтверждают актуальность этих угроз. В обзоре [3] отмечается, что методы машинного обучения, внедряемые в медицину, сами становятся мишенью для атак, что требует разработки устойчивых и безопасных конвейеров обработки данных, включая этап очистки и валидации входных HL7-сообщений. Кроме того, как указано в отчете CVE-2024-52807, даже современные инструменты для работы с HL7 FHIR подвержены классическим уязвимостям, таким как внедрение XML External Entity (XXE), что может привести к раскрытию данных сервера. Это доказывает, что проблема защиты актуальна для всех поколений стандарта.

В исследовании Хасельхорста [4] представлен детальный анализ методов защиты HL7-интерфейсов, который включает как традиционные, так и специализированные подходы.

Ручная проверка (manual validation) является простейшим методом, позволяющим сверять количество сообщений на отправляющей и принимающей сторонах. Однако, как справедливо отмечается, этот метод не масштабируется и не обеспечивает проверки содержания сообщений.

Хостовые межсетевые экраны (host-based firewalls) могут ограничить круг систем, имеющих доступ к HL7-порту, и предотвратить DoS-атаки путём исчерпания максимального количества соединений. Тем не менее, они не защищают данные от перехвата и не препятствуют ARP-spoofing-атакам.

Сегментация сети (network segmentation) ограничивает видимость HL7-интерфейсов с менее защищённых сегментов сети, что является важной мерой defence-in-depth. Однако интерфейсный движок по своей природе должен взаимодействовать с системами из разных сетей, а сами данные по-прежнему передаются в открытом виде.

VPN и SSH-туннелирование обеспечивают шифрование передаваемых данных. Особый интерес представляет SSH-туннелирование, которое требует минимальных изменений в существующей HL7-инфраструктуре и может быть реализовано с помощью встроенных средств операционных систем. При этом HL7-данные остаются зашифрованными даже при успешной ARP-spoofing-атаке.

Технологии распределённых реестров (blockchain) рассматриваются в систематическом обзоре [5] как средство обеспечения неизменяемости и аудируемости транзакций с медицинскими данными. Однако авторы отмечают такие ограничения, как высокая вычислительная сложность и задержки, что затрудняет применение в реальном времени.

Проведённый аналитический обзор литературных источников подтверждает, что проблема защиты HL7-сообщений остаётся актуальной и нерешённой. Существующие подходы – от нормативного регулирования (HIPAA) до технологий blockchain и машинного обучения – имеют свои достоинства, но не предоставляют готового, производительного и совместимого решения для HL7-инфраструктур. Обоснована необходимость разработки специализированного программного модуля, который станет предметом дальнейших исследований.

Список использованных источников:

1. Вора Дж., Италия П., Танвар С., Тьяги С., Кумар Н., Обайда М.С., Сяо К.Ф. Обеспечение конфиденциальности и безопасности электронных медицинских карт. В сборнике: Труды Международной конференции по компьютерным, информационным и телекоммуникационным системам (CITS). – Кольмар, Франция, – 2018 г. – С. 1-5.
2. Мбониханкуйе С., Нкунзimana А., Ндагиджимана А. Технология безопасности медицинских данных: соответствие требованиям HIPAA. Беспроводная связь и мобильные вычисления. – 2019. – С. 1-7.
3. Кайюм А., Кадир Дж., Билал М., Аль-Фукаха А. Безопасное и устойчивое машинное обучение для здравоохранения: обзор. IEEE Reviews in Biomedical Engineering. 2020. – Т. 14. – С. 156-180.
4. Даллас Хазелхорст, Взлом интерфейсов данных HL7 в медицинских средах: атака и защита – ахиллесова пята здравоохранения [Электронный ресурс]. – Режим доступа: <https://linuxincluded.com/hl7-medical-attacking-defending/>: 24.02.2025.
5. Агбо К.С., Махмуд Х., Эклунд Дж.М. Технология блокчейн в здравоохранении: систематический обзор. Healthcare. 2019. Т. 7. № 2. – 56 с.

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ БЕЛАРУСИ И СТРАН ЕВРОПЕЙСКОГО СОЮЗА

Шерышев Р.В., студент гр. 561402

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Пухир Г.А. – старший преподаватель каф. ЗИ

Аннотация. В работе рассматриваются подходы к регулированию деятельности организаций в сфере защиты информации в Республике Беларусь и странах Европейского Союза. Анализируется белорусская модель лицензирования, основанная на разрешительном принципе, а также европейская практика аккредитации и надзора, применяемая при работе с государством и критической инфраструктурой. Выявляются ключевые различия между двумя системами: лицензированием как обязательным условием осуществления деятельности в Беларуси и дифференцированным подходом в странах ЕС.

Ключевые слова. Регулирование деятельности, скрытность передачи, ASK, FSK, BPSK, спектральная плотность мощности, PAPER, распознавание сигналов.

Информация в современных условиях превратилась в один из ключевых стратегических ресурсов, требующих надежной защиты. Деятельность по обеспечению информационной безопасности связана с высокой степенью ответственности, поскольку специализированные методы и средства защиты, оказавшись в распоряжении злоумышленников, могут быть использованы для нанесения ущерба критически важной инфраструктуре. В условиях трансграничного обмена данными особое значение приобретает анализ международных подходов к регулированию этой сферы. Сравнение белорусской модели лицензирования с европейскими механизмами сертификации, аккредитации и надзора позволяет выявить различные способы минимизации рисков, обусловленных двойственным характером знаний и технологий в области защиты информации.

В Республике Беларусь регулирование деятельности в сфере защиты информации исторически развивается на основе лицензирования, а также обязательной сертификации и аттестации средств и систем защиты информации. Формирование национальной системы законодательства о лицензировании началось с Постановления Совета Министров Республики Беларусь от 16 октября 1991 г. № 386. В настоящее время отношения в сфере лицензирования регулируются Законом Республики Беларусь от 14 октября 2022 г. № 213-З «О лицензировании», который определяет общие подходы к лицензируемым видам деятельности и порядок их осуществления. Вопросы, связанные с деятельностью в области защиты информации, дополнительно регулируются Указом Президента Республики Беларусь от 16 февраля 2012 г. № 71 «О порядке лицензирования видов деятельности, связанных со специфическими товарами (работами, услугами)», устанавливающим особенности лицензирования деятельности, связанной с криптографической защитой информации и средствами негласного получения информации.

Лицензирование деятельности по технической и криптографической защите информации, включая применение электронной цифровой подписи, осуществляет Оперативно-аналитический центр при Президенте Республики Беларусь. В части средств криптографической защиты государственных секретов и средств негласного получения информации соответствующие полномочия возложены на Комитет государственной безопасности.

В Европейском союзе отсутствует единое обязательное государственное лицензирование всей деятельности по защите информации. Регулирование осуществляется через сочетание сертификации, стандартов, национального надзора и общеевропейских нормативных актов, прежде всего GDPR и NIS2. GDPR устанавливает правила обработки персональных данных для организаций, работающих с данными граждан ЕС, независимо от места их нахождения. Он предусматривает обязанности по назначению ответственного за защиту данных в предусмотренных случаях, проведению оценки рисков и внедрению мер безопасности, но не требует получения обязательной государственной лицензии.

Директива NIS2, принятая в 2022 году, усилила требования к кибербезопасности организаций в критически важных секторах ЕС, включая энергетику, транспорт, банковский сектор, здравоохранение и государственное управление. Она обязывает организации внедрять меры управления рисками, обеспечивать защиту цепочек поставок, поддерживать непрерывность деятельности и своевременно уведомлять о значимых инцидентах. В ряде случаев предусмотрена и повышенная ответственность руководства за соблюдение требований кибербезопасности. [1]

Деятельность по защите информации также опирается на международные стандарты, в частности на: ISO/IEC 27001:2022 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования»; ISO/IEC 27002:2022 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление информационной безопасностью»;

ISO/IEC 27005:2022 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по управлению рисками информационной безопасности».

В государствах ЕС существуют национальные особенности регулирования защиты информации, обусловленные историческими, управленческими факторами и требованиями национальной безопасности. Общим принципом является дифференциация требований в зависимости от статуса организации и характера обрабатываемых данных. Для коммерческих компаний, не связанных с госорганами и критической инфраструктурой, обязательное получение разрешений в сфере информационной безопасности обычно не требуется; их деятельность регулируется GDPR и NIS2. Обязательная аккредитация, сертификация или признание со стороны национального регулятора необходима при работе с госзаказчиками, объектами критической инфраструктуры или особо чувствительными данными. Однако в отдельных странах такие требования распространяются на криптографические средства и поставщиков, выполняющих государственные контракты. [2]

В Германии функции профильного регулятора выполняет Федеральное ведомство по информационной безопасности (BSI). Оно ведет механизмы признания и оценки компетентности поставщиков и решений в сфере ИТ-безопасности, а в отдельных случаях устанавливает дополнительные требования для работы с государственными структурами и операторами критической инфраструктуры. Для деятельности, связанной с криптографической защитой информации в государственных системах, могут применяться дополнительные процедуры согласования и аккредитации.

Во Франции головным органом выступает Национальное агентство безопасности информационных систем (ANSSI). Для работы с государственными заказчиками и в чувствительных секторах оно применяет механизмы квалификации и сертификации, подтверждающие техническую компетентность и надежность поставщиков. Криптографические продукты, предназначенные для защиты государственной информации, подлежат обязательной сертификации в установленном порядке.

В Нидерландах надзор в сфере информационной безопасности распределён между несколькими государственными структурами. Ключевую роль играет Национальный центр кибербезопасности (NCSC), который анализирует угрозы, координирует реагирование и даёт рекомендации по защите цифровой инфраструктуры. В сфере персональных данных действует Управление по защите данных (AP), контролирующее соблюдение GDPR. Обязательные процедуры признания, согласования или аккредитации, как правило, применяются прежде всего при работе с государственными органами и объектами критической инфраструктуры, тогда как коммерческий сектор в основном действует в рамках общеевропейского регулирования без дополнительных административных барьеров.

В Испании ключевую роль играет Национальный криптологический центр (CCN), который связан с формированием и применением требований к безопасности информационных систем в государственном секторе. Каталог продуктов и услуг безопасности (CPSTIC) используется как ориентир при выборе средств защиты информации для государственных органов и объектов критической инфраструктуры. Для систем, работающих с информацией ограниченного распространения, применяется Национальная схема безопасности (ENS), а сертификация соответствия осуществляется через уполномоченные и аккредитованные органы.

В Польше национальная система регулирования строится вокруг Закона о национальной системе кибербезопасности (UKSC), который устанавливает требования для операторов ключевых сервисов и объектов критической инфраструктуры. Надзорные функции распределены между несколькими государственными институтами: Научно-академическая компьютерная сеть (NASK) участвует в координации и технической поддержке, Агентство внутренней безопасности (ABW) играет важную роль в вопросах государственной и криптографической безопасности, а Министерство национальной обороны отвечает за оборонный сектор.

Проведенный анализ показывает принципиальные различия в подходах к регулированию деятельности в сфере защиты информации в Республике Беларусь и Европейском союзе. Белорусская модель строится на более централизованном государственном контроле, где лицензирование, сертификация и аттестация выступают ключевыми механизмами допуска к деятельности. Европейская модель, напротив, основана на стандартизации, последующем надзоре и усиленной ответственности без единой системы обязательного лицензирования. Выбор той или иной модели определяется национальными приоритетами: в первом случае акцент делается на государственную безопасность и контроль, во втором – на развитие рынка при высоких требованиях к соблюдению правил. В дальнейшем системы защиты информации, вероятно, будут все активнее сочетать элементы риск-ориентированного подхода, что позволит повысить устойчивость критической инфраструктуры в условиях роста глобальных киберугроз.

Список использованных источников:

1. Kianpour, M., Earls Davis, P.A. & Windekilde, I.M. *Digital sovereignty in practice: analyzing the EU's NIS2 directive*. *Int. J. Inf. Secur.* 24, 167 (2025)
2. Верхелст Э., Ваутерс Я. *Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС // Вестник международных организаций: образование, наука, новая экономика*. 2020, Т. 15, № 2. – С. 105-124.

МЕТОДИКА ОБНАРУЖЕНИЯ LOTL-АТАК ПРИ ПОМОЩИ SIEM-СИСТЕМЫ WAZUH

Шумченя М.А., Лукашик Л.А., студенты гр. 361402

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Мокеров В.С. – ассистент каф. ЗИ

Аннотация. Статья посвящена исследованию методов обнаружения атак класса Living off the Land (LoL) с использованием SIEM-системы Wazuh. Рассмотрена техника эксплуатации легитимной утилиты mshta.exe в контексте тактики Defense Evasion согласно классификации MITRE ATT&CK. Экспериментально установлено, что штатные механизмы Wazuh не обеспечивают обнаружение данной угрозы без разработки специализированных правил корреляции. Предложена методика составления XML-правил, подтвержденная практической апробацией. Полученные результаты свидетельствуют о необходимости регулярного расширения базы правил корреляции как обязательного условия обеспечения киберустойчивости информационных систем.

Ключевые слова. Living off the Land, LolBins, mshta.exe, SIEM, Wazuh, правила корреляции, MITRE ATT&CK.

В современных условиях значительную проблему для систем обнаружения вторжений представляет использование легитимных системных утилит в вредоносных целях, известных как LolBins. (Living Off the Land Binaries and Scripts). LolBins – это термин, используемый в кибербезопасности для обозначения легитимных исполняемых файлов, скриптов или утилит, уже доступных на компьютере пользователя, с помощью которых хакеры выполняют различные вредоносные действия. Вместо того чтобы загружать вредоносные файлы с внешних источников, злоумышленники используют инструменты, которые уже находятся в системе. Таким образом они избегают обнаружения антивирусными программами или другими системами обеспечения безопасности [1].

Данный метод имеет много преимуществ с точки зрения злоумышленника:

- злонамеренная деятельность сочетается с повседневной сетевой и административной деятельностью;
- инструменты, уже установленные на компьютерах, с меньшей вероятностью запускают защиту конечных точек;
- нет необходимости тратить время и ресурсы на разработку собственных вредоносных инструментов;
- такая активность не дает очевидных показателей компрометации, что затрудняет отслеживание вредоносной активности и сравнение атак между организациями;
- многие компании не могут собрать и хранить информацию о мониторинге сети и повседневной сетевой активности достаточно подробно, поэтому невозможно отслеживать эволюцию атаки в реальном времени. Это делает предотвращение атак и смягчение их последствий чрезвычайно сложным [2].

Инструменты Windows, полезные для злоумышленников, обычно называются LolBins или LOLBAS (LOLbinaries and scripts). Наиболее популярными являются PowerShell и rundll32 [3].

Данные инструменты изначально входят в состав операционной системы и предназначены для выполнения административных задач, что позволяет злоумышленникам использовать их для обхода механизмов сигнатурного обнаружения и снижения вероятности выявления подозрительной активности.

В рамках данной работы был проведен эксперимент, направленный на анализ эффективности обнаружения подобных техник средствами системы мониторинга безопасности Wazuh [4].

Wazuh является наиболее широко распространенной платформой кибербезопасности с открытым исходным кодом, объединяющей XDR (Extended Detection and Response) и SIEM (Security Information and Event Management) в одном решении. Он анализирует данные безопасности по конечным точкам, облакам и сетям для обнаружения угроз, реагирования на инциденты и обеспечения соответствия, помогая организациям укреплять свою безопасность посредством непрерывного мониторинга и автоматизации.

Wazuh отслеживает параметры системы и конфигурации приложений, чтобы убедиться, что они соответствуют политикам безопасности, стандартам и/или руководствам по усовершенствованию систем безопасности. Агенты Wazuh проводят периодическое сканирование для выявления неправильных конфигураций или пробелов в безопасности в конечных точках, которые могут быть использованы субъектами угроз. Кроме того, есть возможность настроить эти проверки конфигурации, тем самым адаптируя их, чтобы должным образом соответствовать потребностям организации. Оповещения о безопасности включают рекомендации по лучшей конфигурации с соблюдением нормативных требований [5].

В качестве исследуемой утилиты была выбрана mshta, применяемая для реализации сценария загрузки и последующего исполнения вредоносного файла [6]. mshta - Microsoft HTML (HyperText Markup Language) Application Host. Программа используется для запуска .hta (HTML Application) файлов. Выполнение этого процесса не критично для операционной системы. Однако, если удалить этот файл, это может оказать влияние на стабильную работу Windows. Если запущенное HTML приложение зависло или работает нестабильно, его можно безопасно уничтожить, используя диспетчер задач.

mshta также предоставляет злоумышленникам гибкость для встраивания полезной нагрузки скрипта в любой законный формат файла. Например, характерно встраивать контент HTA в законные двоичные файлы Microsoft (пример - DIALER.EXE). Злоумышленники просто добавляют вредоносный контент HTA в конец файла и mshta.exe сканирует файл до тех пор, пока он не найдет действительное содержимое скрипта HTA. Злоумышленники знают, что полезная нагрузка с меньшей вероятностью будет первоначально обнаружена, если она встроена в законный файл [7].

В MITRE ATT&CK mshta фигурирует в тактике Defense Evasion, Sub-technique of: T1218 [8].

В целях нашей работы, мы сначала эксплуатировали mshta, не написав правила корреляции.

Правила корреляции для Wazuh имеют синтаксис XML (eXtensible Markup Language). При написании правил руководствовались документацией на официальном сайте Wazuh [9] [10].

«mshta.exe http://192.168.100.110:8000/test.hta» – команда, при помощи которой мы имитировали атаку.

Далее после прописания данной команды, смотрели логи Sysmon [11]. На рисунке 1 приведено изображение события.

```
Process Create:
RuleName: -
UtcTime: 2026-04-04 17:36:37.620
ProcessGuid: {ead290b2-4c25-69d1-8001-00000000b00}
ProcessId: 3356
Image: C:\Windows\System32\mshta.exe
FileVersion: 11.00.19041.5794 (WinBuild.160101.0800)
Description: Microsoft (R) HTML Application host
Product: Internet Explorer
Company: Microsoft Corporation
OriginalFileName: MSHTA.EXE
CommandLine: mshta.exe http://192.168.100.110:8000/test.hta
CurrentDirectory: C:\Users\Leonid\
User: DESKTOP-MFS1JDI\Leonid
LogonGuid: {ead290b2-48b7-69d1-0ba0-030000000000}
LogonId: 0x3A00B
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: MD5=B8ED3F70700C22AEE6BBF961879EA99,SHA256=
=F8A2FD36FDC35AA8E7E678576A2ECC5D7B3FE6383E73101508E5D7B49443D153,IMPHASH=
482D661ACB78B36340AF7BEB797951EE
ParentProcessGuid: {ead290b2-4969-69d1-cd00-00000000b00}
ParentProcessId: 6224
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\Windows\system32\cmd.exe"
```

Рисунок 1 – Лог Sysmon

В это же время таких же событий на SIEM нет. На рисунке 2 мы можем видеть, что диапазон времени целые сутки, однако, сработки по mshta мы не видим.

1,472 hits					
Apr 3, 2026 @ 20:37:10 808 - Apr 4, 2026 @ 20:37:10 909					
Export Formatted Reset view 737 available fields Columns Density 1 fields sorted Full screen					
timestamp	agent.name	rule.description	rule.level	rule.id	
Apr 4, 2026 @ 20:35:54.711	Windows	CIS Microsoft Windows 10 Enterprise Benchmark v4.0.0: Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'.	3	19009	
Apr 4, 2026 @ 20:35:54.896	Windows	CIS Microsoft Windows 10 Enterprise Benchmark v4.0.0: Ensure 'Enforce password history' is set to '24 or more password(s)'.	3	19009	
Apr 4, 2026 @ 20:35:28.271	Windows	Software protection service scheduled successfully.	3	60842	
Apr 4, 2026 @ 20:35:13.104	Windows	Windows Logon Success	3	60106	
Apr 4, 2026 @ 20:34:53.896	Windows	Executable dropped in Windows root folder	6	92217	

Рисунок 2 – События на SIEM

Далее настроили правила и после повторной имитации атаки, зайдя на SIEM, увидели событие 14 уровня, которое свидетельствует о том, что правило работает. На рисунке 3 представлено правило, на рисунке 4 представлено событие на Wazuh.

```

<group name="lolbins, windows, sysmon, ">
  <!-- EID 1: Process Create -->
  <rule id="230001" level="12">
    <if_group>sysmon_event1</if_group>
    <field name="win.eventdata.image" type="pcr2">(?!)(certutil\.exe$</field>
    <field name="win.eventdata.commandLine" type="pcr2">(?!)(urlcache|decode|encode|ping|verify)</field>
    <description>LOLBin: certutil - $(win.eventdata.commandLine)</description>
    <mitre><id>T1105</id><id>T1140</id></mitre>
  </rule>

  <rule id="230002" level="14">
    <if_group>sysmon_event1</if_group>
    <field name="win.eventdata.image" type="pcr2">(?!)(mshta\.exe$</field>
    <field name="win.eventdata.commandLine" type="pcr2">(?!)(https?|ftp|\\\\|vbscript|javascript)</field>
    <description>LOLBin: mshta выполняет удалённый контент - $(win.eventdata.commandLine)</description>
    <mitre><id>T1218.005</id></mitre>
  </rule>

```

Рисунок 3 – Правило корреляции

1,510 hits				
Apr 3, 2026 @ 20:47:13.356 - Apr 4, 2026 @ 20:47:13.356				
timestamp	agent.name	rule.description	rule.level	rule.id
Apr 4, 2026 @ 20:47:04.556	Windows	OS Microsoft Windows 10 Enterprise Benchmark v4.0.0: Ensure 'Minimum password length' is set to '14 or more character(s)'.	3	19009
Apr 4, 2026 @ 20:47:04.533	Windows	OS Microsoft Windows 10 Enterprise Benchmark v4.0.0: Ensure 'Minimum password age' is set to '1 or more day(s)'.	3	19008
Apr 4, 2026 @ 20:46:47.977	Windows	LOLBin: mshta сетевое подключение - 192.168.100.110:8000	14	230010
Apr 4, 2026 @ 20:46:46.629	Windows	LOLBin: mshta запускает удалённый контент - mshta.exe http://192.168.100.110:8000/test.htm	14	230002

Рисунок 4 – События на Wazuh

Таким образом, можно сделать вывод о том, что регулярное написание правил корреляции крайне необходимо для повышения киберустойчивости информационной системы. Также, необходимо учитывать, что злоумышленники могут использовать легитимные утилиты для своих целей.

Список использованных источников:

1. LoLBins [Электронный ресурс]. – Режим доступа: <https://www.securitylab.ru/glossary/lolbins/> – Дата доступа: 03.04.2026.
2. Как подготовиться к LotL- атакам на [Электронный ресурс]. – Режим доступа: <https://www.kaspersky.co.uk/blog/lotl-attacks-detection-hardening-guidance/27389/> – Дата доступа: 03.04.2026.
3. Cybercriminals' top LoLBins [Электронный ресурс]. – Режим доступа: <https://www.kaspersky.com/blog/most-used-lolbins/42180/> – Дата доступа: 03.04.2026.
4. The Open Source Security Platform [Электронный ресурс]. – Режим доступа: <https://wazuh.com/> – Дата доступа: 03.04.2026.
5. One unified platform for complete protection [Электронный ресурс]. – Режим доступа: <https://wazuh.com/platform/overview/> – Дата доступа: 03.04.2026.
6. mshta.exe [Электронный ресурс]. – Режим доступа: <https://www.reviversoft.com/ru/processes/mshta.exe?ncr=1> – Дата доступа: 03.04.2026
7. Why do adversaries use Mshta? [Электронный ресурс]. – Режим доступа: <https://redcanary.com/threat-detection-report/techniques/mshta/> – Дата доступа: 03.04.2026.
8. System Binary Proxy [Электронный ресурс]. – Режим доступа: <https://attack.mitre.org/techniques/T1218/005/> – Дата доступа: 03.04.2026.
9. Rules Syntax [Электронный ресурс]. – Режим доступа: <https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/rules.html> – Дата доступа: 03.04.2026.
10. Regular Expression Syntax [Электронный ресурс]. – Режим доступа: <https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/regex.html> – Дата доступа: 03.04.2026.
11. Sysmon версии 15.2 [Электронный ресурс]. – Режим доступа: <https://learn.microsoft.com/ru-ru/sysinternals/downloads/sysmon> – Дата доступа: 03.04.2026.

ИНТЕГРАЦИЯ МОДЕЛИ МАШИННОГО ОБУЧЕНИЯ В МЕЖСЕТЕВОЙ ЭКРАН CHUWALL

Яниславский К.О., Мартинкевич Д.М.

Учреждение образования «Национальный детский технопарк»,
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук, доцент

Аннотация. В данной работе рассматривается подход обнаружения и блокировки кибератак на уровне межсетевого экрана CHUWALL с использованием алгоритмов машинного обучения. Обосновывается выбор библиотеки CatBoost и фреймворка NFStream для анализа сетевого трафика в реальном времени. Приводятся результаты сравнительного анализа моделей и итогового тестирования системы.

Ключевые слова. Межсетевой экран, анализ трафика, модель машинного обучения, библиотека CatBoost, фреймворк NFStream, методы машинного обучения случайный лес (Random Forest) и градиентный бустинг (Gradient Boosting).

Традиционные средства сетевой защиты ограничиваются использованием классических методов анализа трафика, однако на фоне стремительной эволюции киберугроз и появления новых векторов кибератак подобные методы защиты утрачивают свою эффективность, что требует внедрения интеллектуальных систем анализа трафика. В данной работе рассматривается разработка и проверка эффективности применения модуля на базе модели машинного обучения, интегрированного в межсетевой экран CHUWALL, для активного противодействия киберугрозам.

Для обеспечения высокой производительности межсетевого экрана CHUWALL [1] была выбрана бинарная классификация сетевых потоков: легитимный трафик (Benign) и вредоносный трафик (Attack). Был выбран подход машинного обучения с учителем (Supervised Learning), который обусловлен возможностью использования заранее размеченных наборов данных, что позволяет обучить модель выявлять скрытые закономерности, характерные для различных типов кибератак.

Для выбора программного обеспечения, которое позволит модели эффективно обрабатывать большие потоки сетевых данных в реальном времени, было проведено сравнение различных библиотек и методов машинного обучения (таблица 1).

Таблица 1 – Сравнение библиотек для обучения модели

Критерий	Scikit-learn (Random Forest, Gradient Boosting)	Pytorch/TF (Deep Learning)	XGB/CatBoost (Gradient Boosting)
Скорость обучения	Средняя	Низкая	Высокая
Скорость работы	Очень высокая	Низкая	Средняя
Точность	Средняя	Высокая	Очень высокая
Сложность внедрения	Низкая	Высокая	Средняя
Основные задачи в ИБ	Быстрый поиск аномалий по готовым признакам, обнаружение известных кибератак	Анализ сырых пакетов и зашифрованного трафика, обнаружение zero-day атак	Максимальная точность в определении кибератак
Устойчивость к выбросам	Средняя	Низкая	Высокая

Сравнительный анализ показал, что классические методы случайного леса и градиентного бустинга обеспечивают высокую скорость работы, в то время как метод глубокого обучения хотя и эффективен для выявления zero-day кибератак и имеет высокую точность, однако для анализа большого потока трафика на межсетевом экране он не подходит из-за своей низкой скорости работы, а также требования значительных вычислительных ресурсов. На основании полученных данных исследование было сужено до сравнения двух наиболее эффективных для поставленных задач методов машинного обучения: Random Forest и Gradient Boosting (таблица 2).

Результаты сравнения показывают преимущество библиотеки CatBoost при реализации градиентного бустинга. Тем не менее, выбор между методами Random Forest и Gradient Boosting неоднозначен. В связи с этим было принято решение об обучении двух моделей на идентичном датасете с последующим их сравнением в равных условиях при выполнении реальных задач. Такой подход позволил оценить и сравнить эффективность выбранных методов не только по теоретическим критериям, но и по результатам тестирования в условиях имитации кибератак.

Таблица 2 – Сравнение методов машинного обучения

Критерий	Scikit-Learn [2] (Random Forest)	Scikit-Learn (Gradient Boosting)	CatBoost [3] (Gradient Boosting)
Скорость обучения	Средняя (только CPU)	Низкая (только CPU)	Высокая (поддержка GPU)
Скорость работы	Высокая	Высокая	Самая высокая
Потребление ресурсов	Среднее	Среднее	Низкое
Склонность к переобучению	Низкое	Среднее	Низкая (использование Order ed Boosting)

На основе сравнения, представленного в таблице 3, в качестве основы для обучения модели был выбран датасет NF-CSE-CIC-IDS2018-v2 [4], который содержит актуальные признаки сетевых потоков в формате Netflow (фреймворка, который в дальнейшем был использован для передачи информации о сессии модели). Первоначально обучения проводились на полном наборе данных, однако значительный дисбаланс классов (соотношение легитимного трафика к атакам составляло примерно 5:1) приводил к неверным предсказаниям обеих моделей. Поэтому был применен метод случайного понижающего сэмплирования, который позволил обеспечить оптимизацию процесса обучения и устранить значительный дисбаланс классов. Исходный объем легитимных сессий был сокращен до 3 млн записей, выбранных случайным образом. Это позволило достичь соотношения классов, близкого к 1:1, что положительно сказалось на результатах моделей.

Таблица 3 – Сравнение датасетов для обучения моделей

Название датасета	Количество легитимных сессий	Количество кибератак	Количество классов кибератак	Год создания
NF-CSE-CIC-IDS2018-v2	16 249 186	2 644 522	15	2018
NF-UNSW-NB15-v2	2 295 222	95 053	9	2015
NF-ToN-IoT-v2	609 391	769 883	9	2019
NF-BoT-IoT-v2	13 859	586 196	4	2018

Классификация сессий осуществляется на основе 27 статистических характеристик потока: длительность соединения, общее количество и длина переданных пакетов, временные интервалы между пакетами и др.

В ходе экспериментов сравнивались модели Random Forest (Scikit-Learn) и Gradient Boosting (CatBoost), обученные на идентичном сокращенном датасете NF-CSE-CIC-IDS2018-v2. Модели тестировались в одинаковых условиях и анализировали одинаковые сохраненные дампы трафика с различными кибератаками. Результаты тестирования и сравнения моделей представлены в таблицах 4–5.

Таблица 4 – Классификация модели, обученной методом Random Forest

	Precision	Recall	F1-score
Метод Random Forest			
Без кибератак	0,97	0,98	0,98
С кибератаками	0,98	0,97	0,97
Метод Gradient Boosting			
Без кибератак	0,98	1,00	0,99
С кибератаками	1,00	0,97	0,98

Таблица 5 – Сравнение уровней уверенности моделей в кибератаках

Кибератака	Scikit-Learn	CatBoost
DoS UDP	35,33%	94,68%
DoS TCP	26,0%	96,79%
SSH BruteForce	27,33%	89,37%
Port Scan	28%	93,85%

Проведенный сравнительный анализ показал значительное превосходство второй модели Gradient Boosting (CatBoost), из-за чего она и была выбрана для интеграции в межсетевой экран и анализа трафика в реальном времени. Программная реализация выполнена на языке Python с использованием фреймворка NFStream.

Алгоритм работы модуля состоит из следующих этапов:

1. Захват трафика на сетевом интерфейсе в реальном времени. Модуль настроен на анализ исключительно входящих сетевых соединений, что позволяет минимизировать влияние ложноположительных срабатываний на исходящий трафик внутренней сети и работу доверенных сервисов.

2. Извлечение признаков потока и передача их в модель CatBoost.

3. Расчет вероятности, что сессия является кибератакой. Если уверенность модели больше 50%, то инициируется блокировка.

4. IP-адрес атакующего заносится в список nftables и все последующие пакеты блокируются.

5. Автоматическая разблокировка по истечении установленного интервала времени.

В качестве сценария проверки работы разработанного модуля анализа трафика моделью машинного обучения и его эффективности в реальных условиях была реализованна DoS-атака на внешний интерфейс межсетевого экрана, при отключенных остальных модулях защиты. Кибератака включала в себя генерацию интенсивного потока TCP-пакетов с использованием сетевого инструмента hping3. В ходе тестирования, представленного на рисунке 1, модуль, работающий в реальном времени, успешно проанализировал сетевые потоки, классифицировал их как аномальные и идентифицировал атакующий узел. В соответствии с заложенной логикой, при превышении порога уверенности модели (Threshold 0,50), система мгновенно занесла IP-адрес нарушителя в правила фильтрации nftables, что подтвердило эффективность разработанного механизма защиты.

```
ОБНАРУЖЕНА УГРОЗА: 192.168.100.10 -> 192.168.100.2 | Уверенность: 91.42%
ОБНАРУЖЕНА УГРОЗА: 192.168.100.10 -> 192.168.100.2 | Уверенность: 91.67%
ОБНАРУЖЕНА УГРОЗА: 192.168.100.10 -> 192.168.100.2 | Уверенность: 91.51%
ОБНАРУЖЕНА УГРОЗА: 192.168.100.10 -> 192.168.100.2 | Уверенность: 91.93%
```

Рисунок 1 – Обнаружение кибератаки моделью

Таким образом, было проведено сравнение различных библиотек и методов для обучения моделей как теоретически, так и практически. Интеграция модели машинного обучения в процесс фильтрации трафика позволяет межсетевому экрану выявлять необычные угрозы, которые могут преодолеть все предыдущие этапы проверки. Применение CatBoost совместно с NFStream обеспечивает необходимую скорость работы, достаточную для анализа сетевых потоков в режиме реального времени.

Список использованных источников:

1. Маршрутизатор с функциями анализа сетевого трафика / Е. С. Белоусова, В. Л. Мальцев, Д. М. Мартинкевич, К. О. Яниславский // Будущее через исследования : сборник материалов I Республиканской конференции молодых ученых, г. Минск, 29 января 2026 г. – Минск : БГТУ, 2026. – С. 52–57.
2. Scikit-learn : [сайт]. – 2026. – URL: <https://scikit-learn.org> (дата обращения: 28.03.2026).
3. CatBoost: unbiased boosting with categorical features / L. Prokhorenkova, G. Gusev, A. Vorobev, A. V. Dorogush, A. Gulin // Journal of Machine Learning Research. – 2011. – P. 2825-2830.
4. Datasets NF-CSE-CIC-IDS-2018-v2. База данных The University of Queensland. [сайт] – URL: <https://espace.library.uq.edu.au/view/UQ:e9636b7> (дата обращения: 02.03.2026).

СЕКЦИЯ «СИСТЕМЫ И СЕТИ ИНФОКОММУНИКАЦИЙ»

УДК 004.932

ОЦЕНКА ЭФФЕКТИВНОСТИ СОВРЕМЕННЫХ ДЕТЕКТОРОВ ОБЪЕКТОВ В ЗАДАЧАХ ОДНОВРЕМЕННОЙ ЛОКАЛИЗАЦИИ, КАРТОГРАФИРОВАНИЯ И ТРЕКИНГА (SLAMOT)

Левоненко И.И., Робачевский А.Д., магистранты гр. 567001

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Цветков В.Ю. – д-р техн. наук, профессор

Аннотация. В работе проводится сравнительный анализ современных детекторов объектов, применяемых в задачах одновременной локализации, картографирования и трекинга объектов (SLAMOT). Цель статьи – определить, какие архитектуры детекции обеспечивают наилучший баланс между точностью, скоростью и устойчивостью в условиях динамических сцен, характерных для мобильной робототехники и автономных систем. В качестве сравниваемых моделей рассматриваются одностадийные и многостадийные детекторы: семейство YOLO, SSD, Faster R-CNN, а также OWL как представитель современных универсальных моделей обнаружения. Для каждой архитектуры оцениваются метрики качества детекции, вычислительная эффективность, способность корректно отслеживать объекты во времени и влияние на стабильность SLAMOT-пайплайна. Результаты экспериментов позволяют определить наиболее подходящие модели для интеграции в системы SLAMOT и сформулировать рекомендации по выбору детектора в зависимости от требований к производительности и точности.

Ключевые слова. SLAMOT, детекция объектов, компьютерное зрение, одностадийные и многостадийные детекторы, оценка эффективности, автономные системы.

Введение

В условиях стремительного развития автономных робототехнических систем методы искусственного интеллекта перестали быть исключительно теоретическими моделями и превратились в ключевой инструмент обеспечения восприятия и навигации в реальном мире. Главную роль в этом процессе играют модели компьютерного зрения на основе глубоких нейронных сетей, способные извлекать высокоуровневые признаки из визуальных данных и выявлять сложные нелинейные зависимости, недоступные традиционным алгоритмам обработки изображений. Однако для достижения полноценной автономности роботам недостаточно лишь распознавать объекты или строить карту окружающего пространства. Необходима интеграция этих процессов в рамках задач одновременной локализации, картографирования и трекинга объектов (SLAMOT), где детекция объектов становится не вспомогательной функцией, а критическим компонентом системы восприятия [1,2].

Использование нейронных сетей в SLAMOT-системах позволяет отказаться от жёстко заданных алгоритмических правил и опираться на обученные модели, способные адаптироваться к динамическим, частично наблюдаемым и слабоструктурированным условиям реального мира. Актуальность исследования определяется необходимостью поиска оптимального компромисса между точностью детектирования, устойчивостью трекинга и вычислительной эффективностью, особенно в условиях ограниченных ресурсов бортовых вычислительных платформ. Одностадийные детекторы, такие как YOLO [3] и SSD [4], демонстрируют высокую скорость работы, что делает их привлекательными для мобильных роботов. Однако их влияние на стабильность SLAMOT-пайплайна и качество построения карт требует систематического анализа. Многостадийные архитектуры, например Faster R-CNN [5], обеспечивают более высокую точность, но уступают в производительности, что также ставит вопрос об их применимости в реальном времени. Дополнительный интерес представляет использование современных универсальных моделей, таких как OWL-ViT [6], способных выполнять zero-shot детекцию и расширять возможности системы без дополнительного обучения. Рассмотрение подобных моделей в сравнительном анализе даёт возможность исследовать эффективность подходов, поддерживающих обнаружение объектов вне заранее заданного набора категорий, и оценить их влияние на адаптивность SLAMOT-систем к новым или ранее неизвестным объектам. Это особенно важно в контексте автономных платформ, работающих в непредсказуемых и быстро меняющихся условиях окружающей среды.

Целью настоящей работы является комплексная оценка эффективности современных детекторов объектов в контексте их интеграции в SLAMOT-системы. Для достижения этой цели анализируется влияние архитектурных особенностей детекторов на устойчивость локализации, проводится классификация подходов к включению семантической информации в карты окружения, исследуются метрики производительности в условиях ограниченных вычислительных ресурсов, а

также рассматриваются современные программные инструменты для развертывания нейросетевых моделей на бортовых вычислительных устройствах.

Теоретические аспекты семантического восприятия в задачах SLAMOT

Семантическое восприятие является критически важным компонентом современных автономных систем, поскольку позволяет робототехнической платформе переходить от геометрического представления пространства к его интерпретации на уровне объектов. В математической формулировке задача семантического восприятия заключается в построении отображения:

$$\psi: I \rightarrow S, \quad (1)$$

где I – пространство входных сенсорных данных (изображений); а S – пространство семантических меток.

В контексте SLAMOT (Simultaneous Localization, Mapping, and Object Tracking) данная интерпретация становится фундаментом для повышения устойчивости локализации за счёт фильтрации динамических объектов и улучшения ассоциации данных. Результатом работы детектора объектов является набор кортежей

$$D = \{(b_i, c_i, p_i)\}_{i=1}^N, \quad (2)$$

где $b_i = (x_i, y_i, w_i, h_i)$ – координаты ограничивающей рамки; c_i – метка класса; p_i – вероятность обнаружения.

Эффективность последующих процессов трекинга и построения семантической карты напрямую зависит от точности и частоты обновления множества D , что определяется архитектурой нейронной сети.

Современные детекторы объектов эволюционируют в направлении оптимизации компромисса между точностью и вычислительной сложностью, разделяясь на одностадийные и многостадийные архитектуры. Одностадийные модели, к классу которых относятся семейства YOLO и SSD, реализуют принцип плотного прогнозирования (dense prediction), выполняя регрессию координат и классификацию объектов за один прямой проход сети. Функция потерь в таких архитектурах обычно формируется как взвешенная сумма ошибок классификации и локализации:

$$L = \lambda_{cls} L_{cls} + \lambda_{loc} L_{loc}, \quad (3)$$

где L_{loc} часто базируется на метрике IoU (Intersection over Union):

$$IoU(b, \hat{b}) = \frac{|b \cap \hat{b}|}{|b \cup \hat{b}|}, \quad (4)$$

или её модификациях CloU/DIoU, улучшающих сходимость регрессии границ. Преимуществом данного подхода является линейная вычислительная сложность относительно размера входного тензора и минимальная задержка вывода, что делает такие модели предпочтительными для мобильных роботов с ограниченным энергопотреблением. Однако отсутствие этапа верификации регионов может приводить к снижению точности на сложных сценах с высокой окклюзией, что потенциально влияет на устойчивость трекинга в динамической среде.

Многостадийные архитектуры, представленные семейством R-CNN (в частности, Faster R-CNN), используют двухэтапный процесс, включающий генерацию регионов интереса (Region Proposal Network – RPN) и последующую классификацию предложенных областей. Математически это разделяет задачу на минимизацию функции потерь предложений

$$L_{RPN} = L_{cls}^{RPN} + L_{loc}^{RPN}, \quad (5)$$

и функцию потерь детекции:

$$L_{det} = L_{cls}^{det} + L_{loc}^{det}, \quad (6)$$

что позволяет достигать более высокой точности за счёт анализа регионов с высоким разрешением. Такие модели демонстрируют высокую эффективность при детекции мелких объектов и в условиях сложного фона благодаря механизму ROI Align. Однако их вычислительная сложность существенно выше из-за последовательного характера обработки и операций выборки регионов. В системах SLAMOT реального времени использование таких архитектур часто ограничено частотой кадров, но

они служат важным ориентиром при сравнительном анализе, позволяя оценить предельное качество детектирования при наличии достаточных вычислительных ресурсов.

Отдельное направление развития представляют универсальные модели открытого словаря (open-vocabulary), такие как OWL-ViT, основанные на трансформерных архитектурах и механизме самовнимания (Self-Attention). Ключевым элементом данных моделей является механизм внимания, вычисляемый как

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V, \quad (7)$$

где Q – матрица запросов (*query*), содержащая векторы, описывающие, какую информацию каждый элемент последовательности стремится получить от других элементов; K – матрица ключей (*key*), представляющая векторы признаков, по которым определяется релевантность элементов относительно запросов; V – матрица значений (*value*), содержащая информацию, которая агрегируется на выходе механизма внимания; QK^T – матрица скалярных произведений запросов и ключей, определяющая степень соответствия между элементами последовательности; $\sqrt{d_k}$ – коэффициент масштабирования, где d_k – размерность векторов ключей; используется для стабилизации значений $softmax$ и предотвращения чрезмерного роста градиентов; $softmax(\cdot)$ – нормализующая функция, преобразующая оценки внимания в вероятностное распределение весов;

Это позволяет модели устанавливать глобальные зависимости между участками изображения и текстовыми эмбедами классов без фиксации конечного набора категорий. Способность работать с текстовыми запросами и обнаруживать новые категории через вычисление косинусного сходства в пространстве признаков делает такие модели перспективными для SLAMOT-систем, функционирующих в непредсказуемых условиях. Несмотря на высокие вычислительные затраты, возможность адаптации к новым объектам без дообучения (zero-shot detection) открывает новые возможности для расширения семантического картографирования в долгосрочной перспективе.

Экспериментальная оценка эффективности детекторов объектов в SLAMOT-системах

Экспериментальная оценка эффективности детекторов в конвейере SLAMOT проведена для моделей, представляющих различные архитектурные парадигмы: одностадийных детекторов YOLOv8n и SSD (lite320/300), многостадийной архитектуры Faster R-CNN ResNet50 FPN, а также трансформерной модели открытого словаря OWL-ViT. Выбор данного набора обусловлен необходимостью анализа компромисса между вычислительной сложностью и точностью семантического восприятия в условиях ограниченных ресурсов мобильных платформ. Сравнение архитектур осуществляется по совокупности измеряемых характеристик: время инференса (*inference latency*), характеризующее быстродействие модели при обработке единичного кадра; потребление памяти (*memory footprint*), отражающее объем оперативной и видеопамати, необходимый для выполнения прямого прохода; и размер модели (*model size / parameters count*), определяющий требования к хранению и передаче весовых коэффициентов. Данные метрики позволяют количественно оценить вычислительную сложность каждой архитектуры и её пригодность для развёртывания на ресурсоограниченных платформах, используемых в системах SLAMOT.

Непосредственное тестирование проводилось в рамках стандартизированного протокола, обеспечивающего воспроизводимость результатов. Первоначальный порог уверенности (*confidence threshold*) устанавливался на уровне 0.5, что соответствовало минимальной вероятности 50% корректной классификации объекта согласно выходному распределению модели. В случае отсутствия детекций, удовлетворяющих данному критерию, применялась адаптивная стратегия понижения порога с дискретным шагом до достижения содержательно валидных результатов, при этом нижняя граница поиска фиксировалась на нулевом значении.

В качестве основных метрик временной эффективности регистрировались медианное время инференса, характеризующее центральную тенденцию задержек обработки единичного кадра, а также робастная оценка вариативности – медианное абсолютное отклонение (MAD, Median Absolute Deviation), дополненное экстремальными значениями минимального и максимального времени выполнения. Указанные статистики вычислялись после предварительной фазы стабилизации (*warmup*), включавшей 10 итераций прогона модели на репрезентативном входном тензоре, что позволяло минимизировать влияние кэширования, динамической компиляции и инициализации вычислительного графа на итоговые замеры.

Характеристики ресурсоёмкости моделей включали пиковое потребление оперативной памяти (RAM) и видеопамати (VRAM), фиксируемое в процессе выполнения прямого прохода, общее количество обучаемых параметров, а также оценочный размер модели в мегабайтах. Для архитектуры OWL-ViT размер вычислялся теоретически на основе произведения количества параметров на размерность представления весов в формате float32 (4 байта), тогда как для остальных детекторов применялся прямой замер размера сериализованного файла весов. Все замеры памяти отражали максимальное потребление в течение цикла инференса, что обеспечивало

консервативную оценку требований к аппаратным ресурсам при развёртывании в условиях ограниченной памяти.

На рисунке 1 приведены изображения, использованные для тестирования нейросетевых моделей.



Рисунок 1 – Тестовые изображения

На рисунке 2 представлен результат обработки используя Faster R-CNN ResNet50 FPN.

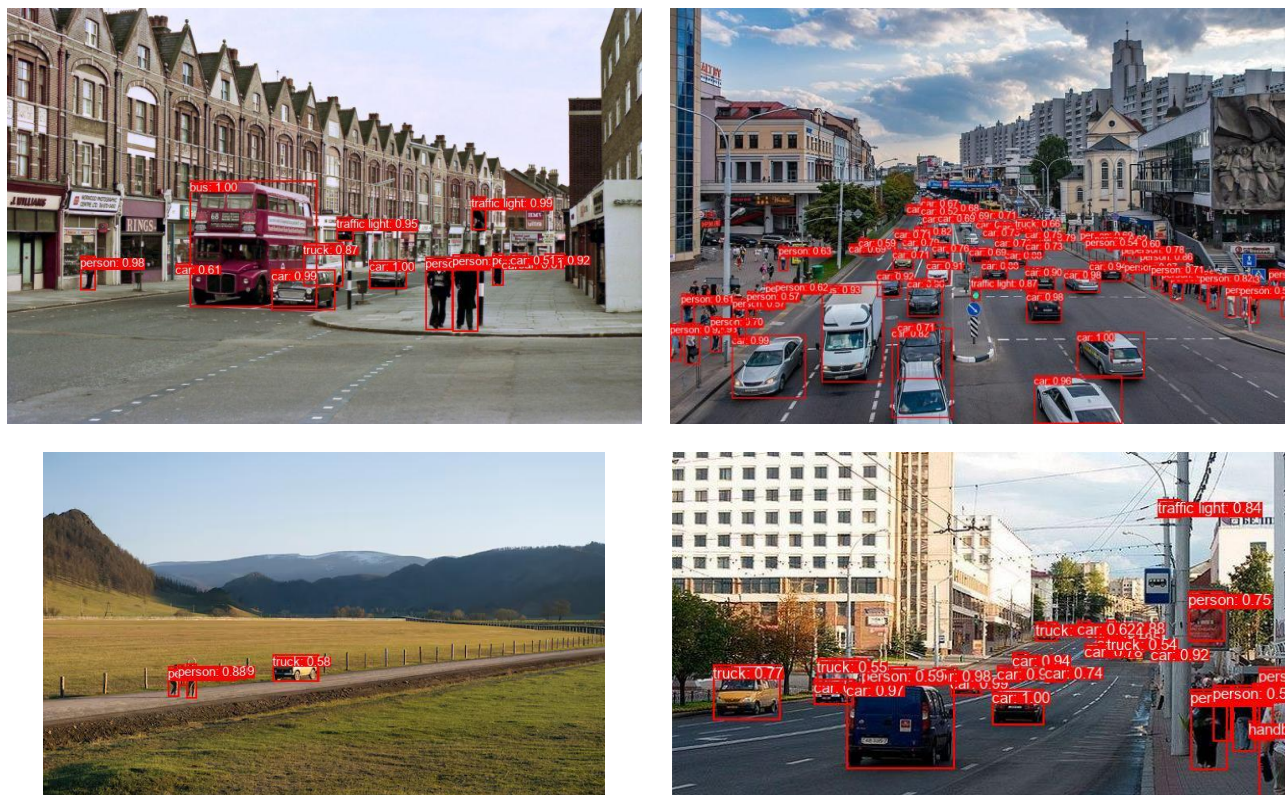


Рисунок 2 – Результат детектирования объектов с использованием Faster R-CNN.

На рисунке 3 представлен результат обработки изображений используя OWL-ViT.

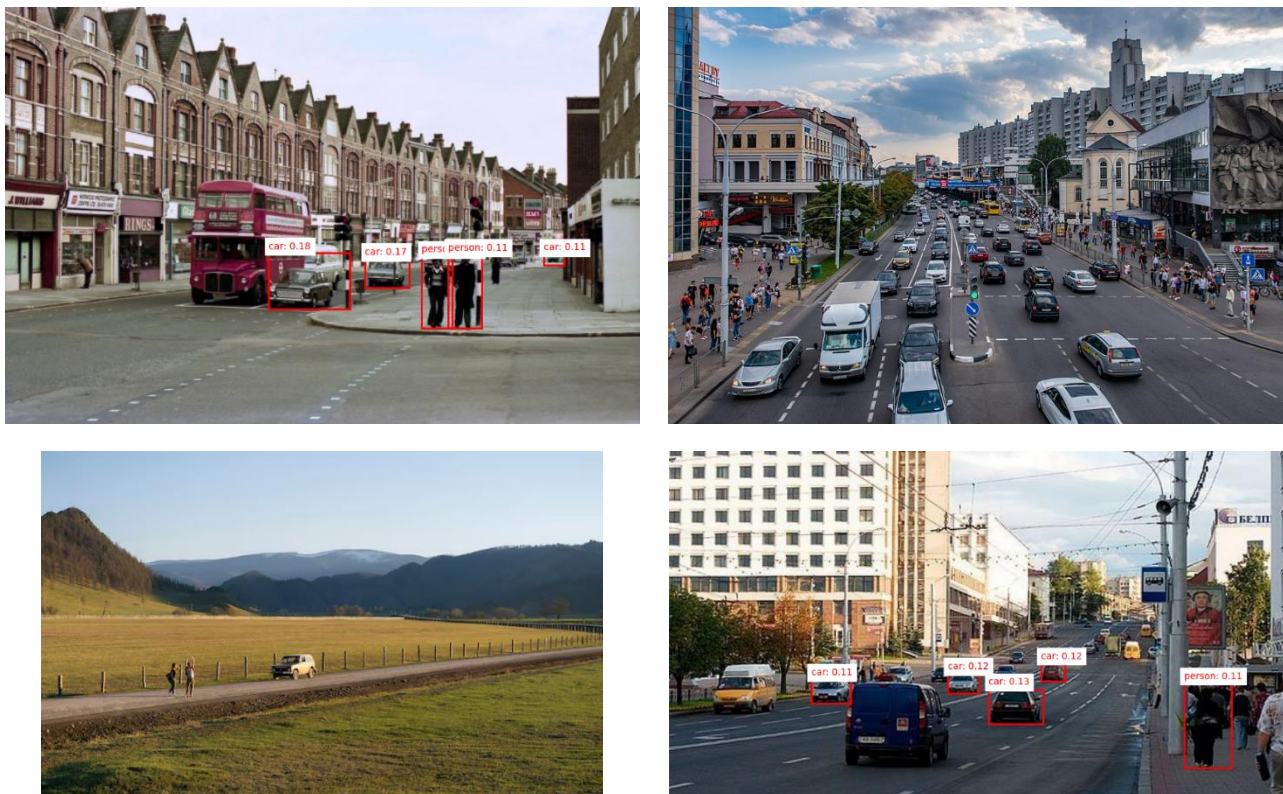


Рисунок 3 – Результат детектирования объектов с использованием OWL-ViT

На рисунке 4 представлен результат обработки изображений используя YOLOv8n.

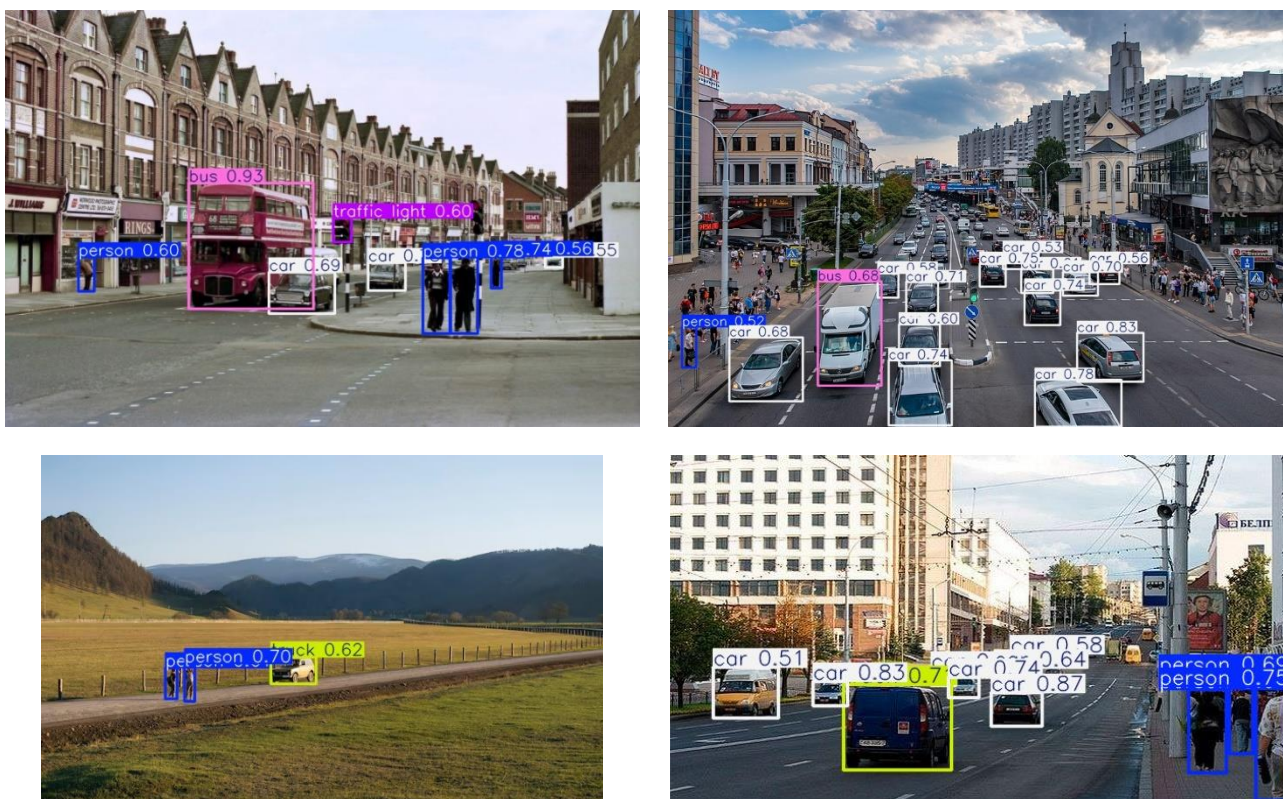


Рисунок 4 – Результат детектирования объектов с использованием YOLOv8n

На рисунке 5 представлен результат обработки изображений используя SSD (lite320).

Таблица 1 – Сводная таблица результатов детекторов объектов

Модель	Архитектура	Порог уверенности	Время инференса (медиана), с	Количество параметров, 10^6	Размер, МБ	Потребление RAM, МБ
YOLOv8n	One-stage	0,50	0,0198	3,16	6,25	672,30
SSDLite320	One-stage	0,20	0,0574	3,44	13,41	678,41
SSD300	One-stage	0,20	0,2080	35,64	135,99	891,25
OWL-ViT	Vision Transformer	0,00	0,3213	153,23	584,53	1212,10
Faster R-CNN	Two-stage	0,20	1,2483	41,76	159,79	1617,13

Экспериментальные замеры производительности пяти архитектур детекции объектов, выполненные на центральном процессоре при обработке четырех изображений схожего разрешения, продемонстрировали выраженную иерархию вычислительной эффективности, коррелирующую с архитектурной сложностью моделей.

Наиболее высокую скорость инференса показала модель YOLOv8n с медианным временем обработки кадра 19.8 мс и минимальным отклонением ($MAD = 1.6$ мс), что подтверждает эффективность одностадийных детекторов с оптимизированной архитектурой для задач реального времени. При этом модель характеризуется наименьшим объемом параметров (3.16 млн) и размером весов (6.25 МБ), а также умеренным потреблением оперативной памяти (672 МБ). Качественный анализ результатов детекции выявил, что YOLOv8n обеспечивает приемлемый уровень локализации объектов, достаточный для большинства практических задач, несмотря на отдельные случаи пропуска малоразмерных или частично окклюзированных целей.

Модели семейства SSD продемонстрировали ожидаемый компромисс между точностью и быстродействием: облегченная архитектура SSDLite320 MobileNetV3 обеспечила время инференса 57.4 мс при сохранении компактности (3.44 млн параметров), тогда как более емкая версия SSD300 VGG16 потребовала 208 мс на кадр, что объясняется увеличением глубины сети и количества параметров до 35.64 млн. В аспекте качества детекции модель SSD300 VGG16 превзошла облегченную модификацию, демонстрируя более стабильное выделение объектов сложной формы, однако уступила YOLOv8n в точности локализации границ. Архитектура SSDLite320 заняла промежуточное положение, показав результаты, сопоставимые с базовыми требованиями к системам навигации в условиях ограниченных вычислительных ресурсов.

Трансформерная модель открытого словаря OWL-ViT, несмотря на значительное количество параметров (153.23 млн) и наибольший расчетный размер весов (584.53 МБ), показала время инференса 321.3 мс, что существенно быстрее двухстадийной архитектуры Faster R-CNN. Однако качественная оценка результатов детекции выявила существенные ограничения данной модели в рамках проведенного эксперимента: на тестовых изображениях наблюдалось критически низкое количество корректных детекций. Вероятной причиной данного явления выступает чувствительность архитектуры открытого словаря к формулировке текстовых запросов – семантическое несоответствие между промптами и визуальным содержанием кадров могло привести к подавлению большинства предсказаний механизмом пост-обработки. Таким образом, применение OWL-ViT требует тщательной инженерии запросов и, потенциально, адаптации пороговых стратегий под конкретную предметную область.

Наибольшее время обработки (1.248 с на кадр) и потребление ресурсов (1617 МБ RAM) зафиксировано для Faster R-CNN ResNet50 FPN, что согласуется с теоретическими ожиданиями для двухстадийных архитектур: необходимость последовательного выполнения региональной предложения и классификации существенно увеличивает вычислительную нагрузку. Тем не менее, именно данная модель продемонстрировала наивысшее качество детекции: точное выделение границ объектов, устойчивая работа при вариативном освещении и минимальное количество ложных срабатываний. Это подтверждает актуальность двухстадийных подходов для задач, где приоритетом является максимальная точность семантического восприятия, а временные задержки допустимы в рамках оффлайн-обработки или пост-анализа.

Все замеры производительности осуществлялись в условиях предварительной стабилизации вычислительного конвейера, для чего перед началом регистрации временных метрик выполнялась серия из десяти итераций прогона модели на репрезентативном входном тензоре (warmup-фаза). Данная процедура необходима для минимизации систематических погрешностей, вызванных «холодным» стартом: инициализацией вычислительного графа фреймворка, динамической компиляцией ядер (в случае использования бэкендов типа TorchScript или ONNX Runtime), заполнением кэшей процессора первого и второго уровня, а также установлением стационарного режима распределения оперативной памяти. Все замеры производительности осуществлялись в условиях предварительной стабилизации вычислительного конвейера, для чего перед началом

регистрации временных метрик выполнялась серия из десяти итераций прогона модели на репрезентативном входном тензоре (waгmип-фаза). Данная процедура необходима для минимизации систематических погрешностей, вызванных «холодным» стартом: инициализацией вычислительного графа фреймворка, динамической компиляцией ядер (в случае использования бэкендов типа TorchScript или ONNX Runtime), заполнением кэшей процессора первого и второго уровня, а также установлением стационарного режима распределения оперативной памяти.

Заключение

В данной работе была произведена комплексная оценка эффективности современных архитектур детекции объектов в контексте их глубокой интеграции в сложные системы одновременной локализации, картографирования и трекинга (SLAMOT). Полученные экспериментальные данные демонстрируют выраженную прямую корреляцию между возрастающей архитектурной сложностью нейронных моделей и их снижающейся вычислительной эффективностью на стандартном оборудовании. Одностадийные детекторы, в частности легковесная версия YOLOv8n, обеспечивают наиболее оптимальный баланс высокой скорости обработки и приемлемой точности для критичных задач реального времени, требующих минимальной задержки отклика системы. В противоположность им, двухстадийные архитектуры, такие как Faster R-CNN ResNet50, демонстрируют наивысшее качество детекции и точность локализации границ, однако ценой существенного увеличения времени инференса и потребления оперативной памяти, что объективно ограничивает их применение исключительно сценариями оффлайн-анализа или постобработки данных на мощных серверах. Модели открытого словаря, представленные трансформером OWL-ViT, несмотря на значительную теоретическую гибкость в работе с произвольными текстовыми запросами, показали в текущих условиях низкую практическую эффективность без тщательной инженерии промптов и адаптации пороговых стратегий под конкретную предметную область. Кроме того, тестирование на центральном процессоре выявило критическую важность оптимизации памяти для всех моделей, так как избыточное потребление RAM может дестабилизировать работу основного конвейера SLAM. Таким образом, для развёртывания на ресурсограниченных мобильных платформах и встраиваемых системах рекомендовано приоритетное использование лёгких одностадийных детекторов, в то время как более сложные архитектуры целесообразно применять для задач семантического обогащения карт, где приоритетом является максимальная точность восприятия окружающей среды, а не минимальная задержка обработки видеопотока.

Список использованных источников:

1. Cadena, C., Carlone, L., Carrillo, H. et al. Past, Present, and Future of Simultaneous Localization and Mapping: Toward the Robust-Perception Age // *IEEE Transactions on Robotics*. – 2016. – Vol. 32, No. 6. – P. 1309–1332.
2. Zhong, F., Wang, Y., Chen, X. et al. SLAMOT: A Survey on Simultaneous Localization, Mapping and Object Tracking // *arXiv preprint arXiv:2303.09331*. – 2023. – 42 p.
3. Redmon, J., Divvala, S., Girshick, R., Farhadi, A. You Only Look Once: Unified, Real-Time Object Detection // *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. – 2016. – P. 779–788.
4. Liu, W., Anguelov, D., Erhan, D. et al. SSD: Single Shot MultiBox Detector // *European Conference on Computer Vision (ECCV)*. – 2016. – P. 21–37.
5. Ren, S., He, K., Girshick, R., Sun, J. Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks // *Advances in Neural Information Processing Systems (NeurIPS)*. – 2015. – Vol. 28.
6. Minderer, M., Gritsenko, A., Stone, A. et al. Simple Open-Vocabulary Object Detection with Vision Transformers // *European Conference on Computer Vision (ECCV)*. – 2022. – P. 728–755.

UDC 004.932

PERFORMANCE EVALUATION OF STATE-OF-THE-ART OBJECT DETECTORS FOR SIMULTANEOUS LOCALIZATION, MAPPING, AND OBJECT TRACKING (SLAMOT)

I.I. Levonenko, A.D. Robachevsky

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

V.Yu. Tsviatkou – Doctor of Engineering, professor

Annotation. This paper presents a comparative benchmark study of modern object detection architectures employed in Simultaneous Localization, Mapping, and Object Tracking (SLAMOT) pipelines. The primary objective is to identify which detection frameworks achieve the optimal trade-off between accuracy, inference latency, and robustness under dynamic scene conditions typical of mobile robotics and autonomous systems. The evaluated models encompass both single-stage detectors (YOLO family, SSD variants) and two-stage architectures (Faster R-CNN), alongside OWL-ViT as a representative of contemporary open-vocabulary, transformer-based detection paradigms. For each architecture, we assess detection quality metrics, computational efficiency (inference time, memory footprint, parameter count), temporal tracking consistency, and the impact on overall SLAMOT pipeline stability. Experimental results enable the identification of the most suitable models for integration into resource-constrained SLAMOT systems and provide actionable guidelines for detector selection based on application-specific requirements for real-time performance and semantic perception accuracy.

Keywords. SLAMOT, object detection, computer vision, single-stage and two-stage detectors, performance benchmarking, autonomous systems.

УДК 621.374.4:621.3.029.6

МОДУЛЬ УМНОЖИТЕЛЯ ЧАСТОТЫ В ДИАПАЗОНЕ 18-40 ГГц

Кийко В.В.

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Ланин В.Л. – д-р техн. наук, профессор

Аннотация. Данная работа посвящена разработке модуля умножителя частоты для диапазона 18–40 ГГц, используемого в современных радиотехнических системах для получения стабильных сигналов миллиметрового диапазона. Основная проблема, решаемая в устройстве – подавление паразитных гармоник, возникающих из-за нелинейности активных элементов, для обеспечения спектральной чистоты выходного сигнала. Для эффективной фильтрации во всем рабочем диапазоне предлагается архитектура с банком перекрывающихся полосовых фильтров, настроенных на выделение второй гармоники и подавление нежелательных частотных составляющих.

Ключевые слова: умножитель частоты, миллиметровый диапазон, гармоники, полосовой фильтр, спектральная чистота.

Введение. Развитие современных радиотехнических систем требует генерации и обработки сигналов в миллиметровом диапазоне волн. Такие системы применяются в радиолокации, спутниковой связи, телекоммуникациях пятого поколения и измерительной технике. Одним из важных элементов подобных систем являются устройства умножения частоты, позволяющие получать сигналы более высокого диапазона из стабильных источников более низкой частоты [1].

Умножители частоты широко используются при построении гетеродинов, синтезаторов частоты и передающих трактов СВЧ-устройств. Одним из наиболее распространённых типов является умножитель частоты, который формирует сигнал с удвоенной частотой входного сигнала.

Однако эффективность работы таких устройств существенно зависит от режимов управления активными элементами, параметров согласования и уровня входной мощности. Поэтому задача оптимизации параметров управления умножителем частоты является актуальной.

Структура умножителя частоты и его основные параметры

Умножитель частоты основан на использовании нелинейных свойств активных или пассивных элементов. При воздействии гармонического сигнала [2]:

$$V_{in} = V_0 \cos(\omega t), \quad (1)$$

где V_{in} – входное напряжение, V_0 – амплитуда сигнала, ω – круговая частота, t – время.
на нелинейный элемент возникает ток, содержащий высшие гармоники:

$$I(t) = a_1 \cos(\omega t) + a_2 \cos(2\omega t) + a_3 \cos(3\omega t) + \dots, \quad (2)$$

где $I(t)$ – ток через нелинейный элемент, a_1 , a_2 , a_3 – амплитуды гармоник, ω – круговая частота входного сигнала, t – время.

Полезным сигналом в данном случае является вторая гармоника:

$$f_{out} = 2f_{in}, \quad (3)$$

где f_{out} – частота выходного сигнала, f_{in} – частота входного сигнала.

Структурная схема умножителя частоты приведена на рисунке 1.

Одной из основных проблем умножителей частоты является появление паразитных гармоник, возникающих вследствие нелинейных свойств активных элементов. Помимо полезной второй гармоники $2f_{in}$, в спектре выходного сигнала присутствуют компоненты с частотами $3f_{in}$, $4f_{in}$ и выше. Наличие таких составляющих ухудшает спектральную чистоту сигнала и может приводить к помехам в соседних частотных каналах.

Для подавления нежелательных гармоник в умножителе используется банк полосовых фильтров, настроенных на выделение полезной гармоники и подавление остальных спектральных составляющих.

На рисунке 2 представлена структурная схема банка полосовых фильтров, включённых в тракт выходного сигнала умножителя частоты.

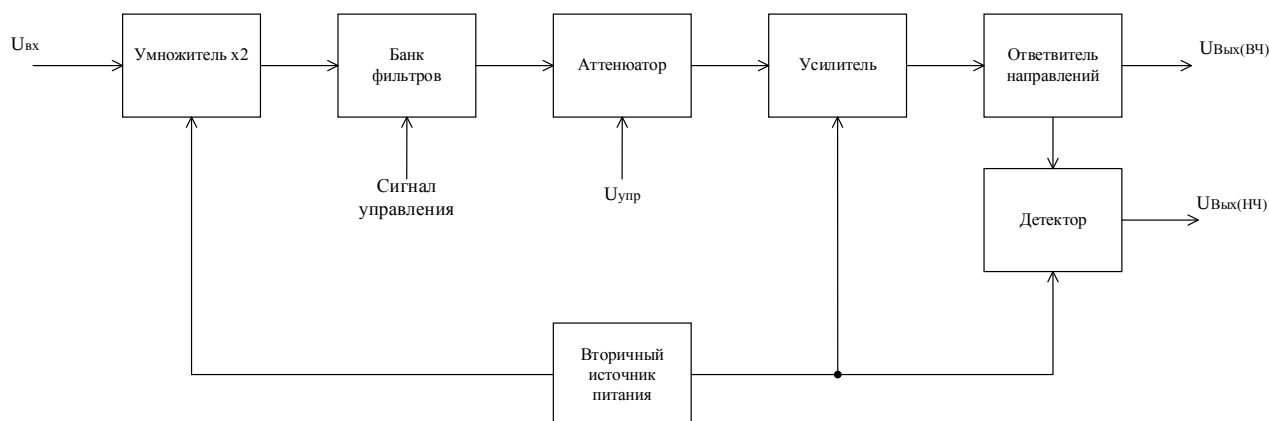


Рисунок 1 – Структурная схема умножителя частоты

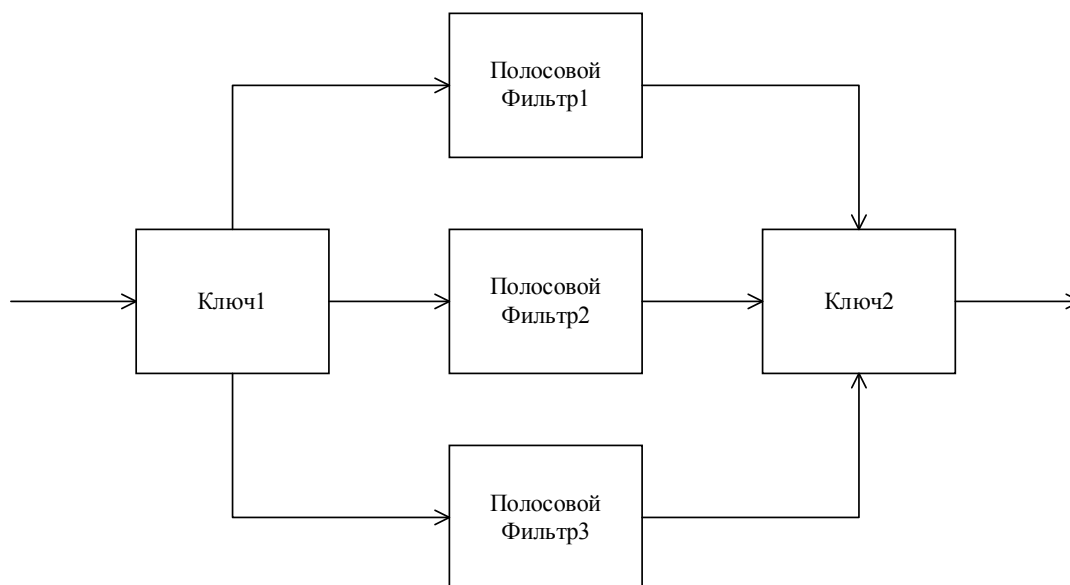


Рисунок 2 – Банк полосовых фильтров

Банк фильтров представляет собой набор полосовых, включённых в тракт выходного сигнала умножителя частоты. Основной задачей этих фильтров является выделение сигнала с частотой $f_{out} = 2f_{in}$ в диапазоне 18-40" ГГц".

При этом фильтры обеспечивают подавление следующих гармоник:

- входной частоты f_{in} ;
- третьей гармоники $3f_{in}$;
- четвёртой и более высоких гармоник.

Таким образом, полезная гармоника проходит через фильтр практически без ослабления, тогда как паразитные составляющие значительно подавляются.

Использование нескольких фильтров позволяет повысить избирательность и уменьшить уровень паразитных сигналов на выходе устройства.

При проектировании банка фильтров необходимо учитывать следующие параметры:

- коэффициент передачи в полосе пропускания;
- уровень подавления вне полосы;
- коэффициент отражения;
- ширину полосы пропускания [3].

Эффективная фильтрация гармоник затруднена из-за широкополосной природы умножителя. Например, при входном сигнале с частотой 10 ГГц генерируются гармоники на частотах 20, 30, 40 и 50 ГГц. Для чистого выделения желаемой второй гармоники на частоте 20 ГГц полосовой фильтр должен резко подавлять сигнал на частоте 30 ГГц (третья гармоника), пропуская при этом сигнал на частоте 20 ГГц. Но если выходной сигнал смещается в сторону частот 26+ ГГц, тот же фильтр становится неэффективным.

Идеальная архитектура использует перекрывающиеся полосовые фильтры с полосой пропускания около 33%, например: 18 – 24 ГГц; 24 – 32 ГГц; 32 – 40 ГГц.

Такая конфигурация позволяет лучше контролировать подавление гармоник, особенно на краях полосы пропускания. Дополнительная фильтрация поможет полностью подавить основную и третью гармоники во всем диапазоне выходного сигнала.

Список литературы

1. Jeon, Y. *Front-End Module of 18–40 GHz Ultra-Wideband Receiver for Electronic Warfare System* / Y. Jeon [et al.] // *Journal of Electromagnetic Engineering and Science*. – 2018. – Vol. 18, No. 3. – P. 188-198.
2. Фомин, Н. Н. *Радиотехнические устройства СВЧ на синхронизированных генераторах* / Н. Н. Фомин, В. С. Андреев, Э. С. Воробейчиков ; под ред. Н. Н. Фомина. – Москва : Радио и связь, 1991. – 192 с.
3. Клименко, Д. В. Особенности разработки банка фильтров сантиметрового диапазона на основе GaAs pHEMT-технологии / Д. В. Клименко, А. Б. Никитин, А. А. Строганов, И. А. Цикин // *Информатика, телекоммуникации и управление*. – 2023. – Т. 16, № 3. – С. 7-17.

UDC 621.374.4:621.3.029.6

MODULE OF FREQUENCY MULTIPLIER IN THE RANGE OF 18-40 GHZ

Kiyko V.V.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Scientific adviser: Lanin V.L. – Dr. Tech. Sciences, prof.

Annotation This work is devoted to the development of a frequency multiplier module for the 18–40 GHz range, used in modern radio systems to obtain stable millimeter-wave signals. The main problem solved in the device is the suppression of spurious harmonics arising from the nonlinearity of active elements to ensure the spectral purity of the output signal. For effective filtering over the entire operating range, an architecture with a bank of overlapping bandpass filters tuned to extract the second harmonic and suppress unwanted frequency components is proposed.

Keywords. frequency multiplier, millimeter-wave range, harmonics, bandpass filter, spectral purity.

УДК 004.9:794.5

ИГРОВАЯ ИНДУСТРИЯ КАК СФЕРА ИТ И ИКТ. СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Мацкевич В. В., студент гр. 361401

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Чепикова В. В. – старший преподаватель

Аннотация. В статье рассматривается игровая индустрия как важная часть сферы информационных технологий и информационно-коммуникационных технологий. Анализируются структура и технологическая основа индустрии видеоигр, а также её экономическое значение на мировом рынке. Особое внимание уделяется состоянию игровой индустрии в Республике Беларусь, её проблемам и ограничениям развития. Также исследуются перспективы развития отрасли и потенциал Беларуси в сфере разработки видеоигр.

Ключевые слова. Игровая индустрия, видеоигры, информационные технологии, ИТ, ИКТ, цифровая экономика, разработка игр, game development, издательство игр, publishing, платформы распространения, цифровые платформы, киберспорт, esports, игровые сервисы, облачный гейминг, cloud gaming, искусственный интеллект, AI, VR, AR, метавселенные, игровые движки, программирование, сетевые технологии, интернет-инфраструктура, мобильный гейминг, рынок видеоигр, экономика игр, ИТ-сектор Беларуси, Парк высоких технологий, ПВТ, аутсорсинг, стартапы, инвестиции, экспорт ИТ-услуг, кадровый потенциал, разработчики игр, цифровые технологии.

В условиях стремительной цифровизации экономики особую роль начинает играть индустрия видеоигр, которая в последние десятилетия превратилась из развлекательного сегмента в полноценную высокотехнологичную отрасль. Игровая индустрия объединяет разработку программного обеспечения, компьютерную графику, сетевые технологии и цифровые коммуникации, что делает её важной частью сферы информационных технологий (ИТ) и информационно-коммуникационных технологий (ИКТ). Благодаря широкому распространению интернета, мобильных устройств и цифровых платформ видеоигры стали одним из наиболее динамично развивающихся сегментов мировой цифровой экономики.

Актуальность исследования данной темы обусловлена тем, что индустрия видеоигр демонстрирует устойчивый рост и оказывает значительное влияние на развитие технологических и экономических процессов. По данным аналитических исследований, мировой рынок видеоигр в 2024 году оценивался примерно в 274–300 млрд долларов США, а в ближайшие годы ожидается дальнейшее увеличение объёма рынка до более чем 700 млрд долларов к 2034 году [1]. Такой рост обусловлен развитием мобильного гейминга, распространением высокоскоростного интернета, а также увеличением аудитории игроков по всему миру.

Помимо экономической значимости, игровая индустрия играет важную роль в развитии современных технологий. Разработка видеоигр стимулирует развитие компьютерной графики, алгоритмов искусственного интеллекта, сетевых сервисов и облачных вычислений. В частности, технологии искусственного интеллекта используются для создания интеллектуального поведения игровых персонажей, генерации игровых миров и анализа поведения пользователей. Одновременно с этим развитие графических движков, виртуальной и дополненной реальности (VR/AR) способствует появлению новых форм интерактивного контента и расширяет возможности применения игровых технологий в других областях – образовании, медицине и моделировании сложных систем [2].

В последние годы игровая индустрия также стала важным драйвером инноваций в области сетевых технологий и цифровых платформ. Массовые многопользовательские онлайн-игры, облачный гейминг и игровые сервисы требуют высокопроизводительной инфраструктуры передачи данных и обработки информации, что напрямую связано с развитием ИКТ-сектора [3]. Таким образом, игровая индустрия представляет собой не только культурное и развлекательное явление, но и значимый элемент современной технологической экосистемы.

Особый интерес представляет развитие игровой индустрии в отдельных странах, включая государства с развитым ИТ-сектором. Республика Беларусь является одним из заметных центров разработки программного обеспечения в Восточной Европе и обладает значительным кадровым потенциалом в области информационных технологий. В связи с этим исследование состояния и перспектив развития игровой индустрии в Беларуси является актуальным как с научной, так и с практической точки зрения.

Целью данной статьи является анализ игровой индустрии как сферы ИТ и ИКТ, а также исследование её современного состояния и перспектив развития в Республике Беларусь.

Игровая индустрия представляет собой совокупность экономических и технологических процессов, связанных с созданием, распространением и коммерциализацией цифровых интерактивных развлечений. Она включает разработку программного обеспечения для видеоигр,

создание графических и звуковых компонентов, маркетинг, распространение и поддержку игровых продуктов. В современном понимании игровая индустрия является частью более широкой сферы информационных технологий и цифровых медиа, поскольку её функционирование напрямую связано с программированием, обработкой данных, компьютерной графикой и сетевыми коммуникациями.

Современная структура игровой индустрии состоит из нескольких ключевых сегментов [4]:

- Разработка игр (game development). Данный сегмент включает процесс создания игровых продуктов: проектирование игровой механики, разработку программного кода, создание графики, анимации, звуковых эффектов и тестирование игры. Разработчики используют различные языки программирования, инструменты моделирования и специализированные игровые движки для реализации игровых проектов;

- Издательство игр (publishing). Издатели выполняют функции финансирования, маркетинга и продвижения игровых проектов. Они обеспечивают выпуск игр на различных платформах, проводят рекламные кампании и организуют распространение продукта на международных рынках;

- Платформы распространения. Распространение видеоигр осуществляется через цифровые платформы и магазины приложений, а также через консольные и компьютерные экосистемы. Развитие цифровых платформ позволило значительно упростить доступ пользователей к игровому контенту и ускорить процесс распространения игр на глобальном рынке;

- Киберспорт (esports). Киберспорт представляет собой организованные соревнования по видеоиграм между профессиональными игроками или командами. Данный сегмент индустрии активно развивается и формирует отдельную экономическую экосистему, включающую турниры, трансляции, спонсорство и рекламные контракты. По данным аналитических исследований, мировой рынок киберспорта демонстрирует устойчивый рост и может достигнуть десятков миллиардов долларов в ближайшие годы;

- Игровые сервисы и экосистемы. К этому сегменту относятся облачные игровые платформы, подписочные сервисы, системы микротранзакций, игровые сообщества и стриминговые сервисы. Они обеспечивают долгосрочное взаимодействие пользователей с игровыми продуктами и формируют дополнительные источники дохода для разработчиков и издателей.

Функционирование игровой индустрии базируется на широком спектре современных информационных технологий, которые обеспечивают создание, обработку и передачу цифрового контента. Сюда входят [4]:

- Игровые движки. Игровой движок представляет собой программную платформу, предназначенную для разработки видеоигр. Он включает набор инструментов для работы с графикой, физикой, анимацией и звуком. Использование игровых движков значительно ускоряет процесс разработки и позволяет создавать сложные интерактивные виртуальные среды;

- Программирование. Разработка видеоигр требует применения различных языков программирования и технологий разработки программного обеспечения. Программный код обеспечивает реализацию игровой логики, взаимодействие пользователя с игровым миром и работу различных игровых систем;

- Искусственный интеллект. Технологии искусственного интеллекта широко применяются для создания поведения неигровых персонажей, адаптации сложности игры и анализа поведения игроков. Использование алгоритмов машинного обучения также позволяет улучшать игровые механики и повышать уровень реалистичности игровых миров;

- Облачные технологии. Облачные вычисления используются для хранения игровых данных, обработки больших объемов информации и реализации облачного гейминга. Благодаря облачным платформам пользователи могут запускать современные игры без необходимости использования мощного оборудования;

- Сетевые технологии. Онлайн-игры требуют стабильных и высокоскоростных сетевых соединений, позволяющих миллионам пользователей одновременно взаимодействовать в виртуальных мирах. Развитие сетевых протоколов и серверных технологий позволило создать масштабные многопользовательские игровые проекты.

Игровая индустрия тесно связана со сферой информационно-коммуникационных технологий. Основой её функционирования является развитая интернет-инфраструктура, обеспечивающая передачу данных между игровыми серверами и пользователями. Кроме того, важную роль играют мобильные сети, благодаря которым мобильные игры стали одним из крупнейших сегментов рынка. Значительное значение имеют онлайн-сервисы, такие как игровые магазины, стриминговые платформы и социальные сети для игроков. Они обеспечивают коммуникацию пользователей, распространение контента и формирование игровых сообществ.

Игровая индустрия является одной из наиболее быстрорастущих отраслей цифровой экономики. По данным аналитических исследований, мировой рынок видеоигр в 2024 году оценивался примерно в 274 млрд долларов, а к 2034 году его объем может превысить 720 млрд долларов, демонстрируя среднегодовые темпы роста около 10 % [1].

Рост отрасли обусловлен несколькими факторами:

- Увеличением числа пользователей видеоигр по всему миру;

- Развитием мобильного гейминга;
- Распространением высокоскоростного интернета;
- Развитием облачных игровых сервисов и цифровых платформ.

Кроме того, игровая индустрия оказывает значительное влияние на рынок труда в сфере информационных технологий. Разработка видеоигр требует специалистов различных направлений: программистов, дизайнеров, художников, аналитиков данных, специалистов по кибербезопасности и маркетингу. Таким образом, индустрия формирует большое количество рабочих мест и способствует развитию человеческого капитала в ИТ-секторе.

Дополнительным экономическим сегментом индустрии является киберспорт, который развивается как самостоятельная отрасль цифровой экономики. По оценкам аналитиков, рынок киберспорта может вырасти с нескольких миллиардов долларов в настоящее время до десятков миллиардов в течение следующего десятилетия, что связано с ростом аудитории, увеличением спонсорских контрактов и развитием онлайн-трансляций [5].

Таким образом, игровая индустрия представляет собой значимый элемент современной ИТ-экономики, оказывающий влияние на технологическое развитие, рынок труда и глобальные цифровые коммуникации.

В последние два десятилетия Республика Беларусь сформировала достаточно развитый сектор информационных технологий, который стал одним из ключевых драйверов экономического роста страны. ИТ-индустрия Беларуси ориентирована преимущественно на экспорт программного обеспечения и цифровых услуг, что позволяет интегрировать национальную экономику в глобальный рынок информационных технологий. По оценкам аналитиков, экспорт ИКТ-услуг в 2021 году достиг примерно 3,2 млрд долларов США, что составило около 7,5 % общего экспорта страны и около 5 % валового внутреннего продукта. В 2025 году экспорт ИКТ-услуг достиг примерно 2,1 млрд долларов США, что составило около 2% валового внутреннего продукта [6].

Одним из ключевых факторов развития ИТ-сектора в Беларуси стало создание специальной экономической зоны – Парка высоких технологий (ПВТ), который был основан в 2005 году для стимулирования развития программной индустрии. ПВТ предоставляет резидентам льготный налоговый режим, благоприятные условия для ведения бизнеса и поддержку международного сотрудничества.

Благодаря деятельности Парка высоких технологий ИТ-сектор Беларуси демонстрировал устойчивый рост. Количество компаний-резидентов ПВТ постоянно увеличивалось, а экспорт программного обеспечения и компьютерных услуг значительно вырос. К 2025 году в ПВТ насчитывается более 1000 компаний, в которых работало свыше 60 тысяч специалистов. Для сравнения, экспорт услуг компаний-резидентов ПВТ достиг 2,7 млрд долларов в 2022 году, что составило почти 30 % экспорта всех услуг страны. Экспорт услуг компаний-резидентов ПВТ превысил 2 млрд долларов в 2025 году, что составляет 2 % ВВП страны [7].

Беларусь известна на международном уровне игровой индустрии благодаря нескольким крупным компаниям, занимающимся разработкой видеоигр. Одной из наиболее известных является компания Wargaming, основанная в Минске. Она получила мировую известность благодаря созданию многопользовательской онлайн-игры World of Tanks, которая стала одним из самых успешных проектов в жанре массовых онлайн-игр. Помимо Wargaming, в Беларуси были основаны и другие студии разработки игр, такие как Vizion Games и Melsoft Games, специализирующиеся преимущественно на мобильных играх и социальных игровых проектах. Эти компании создают проекты для международного рынка и сотрудничают с зарубежными издателями и платформами распространения.

Значительная часть белорусских игровых студий работает в формате **аутсорсинга**, выполняя заказы крупных международных компаний. В рамках таких проектов специалисты участвуют в разработке графики, программного кода, игровых механик и тестировании программного обеспечения. Беларусь стала привлекательной площадкой для аутсорсинговых проектов благодаря высокому уровню подготовки специалистов и относительно низким издержкам разработки. Кроме того, многие белорусские компании участвуют в международных проектах и сотрудничают с ведущими мировыми разработчиками программного обеспечения, что способствует обмену опытом и развитию национальной индустрии разработки игр.

Одним из ключевых факторов развития игровой индустрии в Беларуси является высокий уровень подготовки специалистов в области информационных технологий. Система высшего образования страны включает ряд университетов, готовящих специалистов по направлениям программирования, компьютерной графики, информационных систем и программной инженерии. К числу ведущих образовательных учреждений относятся Белорусский государственный университет, Белорусский государственный университет информатики и радиоэлектроники, Белорусский государственный университет и Белорусский национальный технический университет. Эти университеты обеспечивают подготовку специалистов в области программирования, системного анализа, информационных технологий и разработки программного обеспечения.

Дополнительную роль в развитии кадрового потенциала играет образовательная инфраструктура Парка высоких технологий. На базе ПВТ функционируют образовательные программы и курсы, направленные на развитие навыков программирования, разработки программного обеспечения и управления ИТ-проектами. Белорусские разработчики обладают высоким уровнем квалификации в таких областях, как программирование, разработка программного обеспечения, компьютерная графика, искусственный интеллект и анализ данных. Благодаря этому специалисты из Беларуси востребованы на международном рынке труда и активно участвуют в глобальных технологических проектах [8].

ИТ-индустрия оказывает значительное влияние на экономику Республики Беларусь, в том числе через экспорт программного обеспечения и цифровых услуг. Основная часть продукции ИТ-компаний ориентирована на зарубежные рынки, что способствует притоку валютных средств в экономику страны. Более 90 % программного обеспечения, созданного компаниями-резидентами ПВТ, экспортируется за пределы Беларуси [7].

Развитие ИТ-сектора способствует созданию новых рабочих мест. В компаниях-резидентах Парка высоких технологий работают десятки тысяч специалистов, а число занятых в отрасли продолжает увеличиваться [7].

Хотя точную долю игровой индустрии в структуре ИТ-экспорта определить сложно, игровые компании занимают заметное место среди разработчиков программного обеспечения. Они создают продукты, ориентированные на глобальный рынок цифровых развлечений, что способствует росту экспорта и повышению международной конкурентоспособности белорусской ИТ-индустрии.

Таким образом, игровая индустрия в Беларуси развивается в тесной связи с национальным ИТ-сектором и опирается на развитую инфраструктуру, высококвалифицированные кадры и экспортную ориентацию экономики. Эти факторы формируют основу для дальнейшего роста и интеграции белорусских компаний в мировой рынок цифровых технологий.

Несмотря на значительный потенциал и высокий уровень развития ИТ-сектора, игровая индустрия Республики Беларусь сталкивается с рядом проблем и ограничений, которые оказывают влияние на темпы её роста и конкурентоспособность на международном рынке. К основным факторам, сдерживающим развитие отрасли, относятся отток квалифицированных специалистов, ограниченный доступ к инвестициям, влияние международных санкций и относительно небольшое количество крупных игровых студий и издателей.

Существенное влияние на развитие ИТ-сектора и игровой индустрии оказали международные санкции и изменение геополитической ситуации. Ограничения, введённые рядом стран в отношении белорусской экономики, затруднили доступ компаний к международным рынкам, финансовым инструментам и технологическим партнёрам. Некоторые технологические компании приняли решение о переносе своих офисов или регистрации бизнеса в других странах для сохранения доступа к глобальному рынку. Это также привело к частичному перемещению игровых студий и специалистов за пределы Беларуси.

Несмотря на наличие талантливых специалистов и успешных проектов, в Беларуси относительно небольшое количество крупных игровых студий и издателей, способных создавать масштабные международные проекты. Большая часть компаний работает в сегменте мобильных игр, социальных игр или выполняет аутсорсинговые задачи для зарубежных разработчиков. Отсутствие большого числа крупных издательских компаний ограничивает возможности продвижения игровых продуктов на мировом рынке. В мировой игровой индустрии издатели играют ключевую роль в финансировании разработки, маркетинге и распространении игр. Без поддержки крупных издателей даже качественные проекты могут испытывать трудности с выходом на международный рынок и привлечением широкой аудитории.

Ещё одной важной проблемой является ограниченный доступ к инвестиционным ресурсам. Разработка современных видеоигр требует значительных финансовых вложений, особенно в случае создания крупных проектов класса AAA. Однако в Беларуси венчурная экосистема находится на относительно ранней стадии развития, а количество крупных инвестиционных фондов, специализирующихся на финансировании игровых стартапов, остаётся ограниченным. Многие белорусские студии вынуждены искать финансирование за рубежом или работать в формате аутсорсинга, выполняя отдельные этапы разработки для иностранных компаний. Такой формат сотрудничества позволяет поддерживать занятость специалистов, однако ограничивает возможности создания собственных масштабных игровых проектов и национальных брендов в игровой индустрии.

Также среди проблем для развития ИТ-индустрии Беларуси стоит отметить отток высококвалифицированных кадров за пределы страны. Для игровой индустрии этот фактор особенно критичен, поскольку разработка видеоигр требует специалистов высокого уровня подготовки – программистов, дизайнеров, художников, специалистов по компьютерной графике и искусственному интеллекту. Потеря значительной части квалифицированных кадров может замедлить развитие новых проектов и уменьшить возможности создания крупных игровых студий внутри страны.

Таким образом, развитие игровой индустрии в Республике Беларусь сдерживается рядом экономических, кадровых и институциональных факторов. Решение этих проблем требует

комплексного подхода, уже реализуемого государством, включающего развитие инвестиционной инфраструктуры, поддержку технологических стартапов, сохранение кадрового потенциала и расширение международного сотрудничества в сфере информационных технологий,

Игровая индустрия продолжает активно развиваться благодаря внедрению новых технологий, расширению цифровых платформ и росту аудитории пользователей по всему миру. Перспективы дальнейшего развития отрасли связаны как с технологическими инновациями, так и с экономическими и организационными факторами, включая появление новых бизнес-моделей и расширение международного сотрудничества.

Одним из ключевых направлений развития игровой индустрии являются технологии виртуальной и дополненной реальности (VR/AR). Использование данных технологий позволяет создавать более реалистичные и интерактивные игровые среды, что значительно повышает уровень погружения пользователя в виртуальный мир. VR- и AR-технологии находят применение не только в индустрии развлечений, но и в образовании, медицине и профессиональном обучении. По прогнозам аналитиков, мировой рынок VR и AR может превысить 450 млрд долларов к 2030 году, что свидетельствует о значительном потенциале развития этих технологий [9].

Другим важным направлением развития является облачный гейминг. Облачные игровые сервисы позволяют пользователям запускать современные игры на удалённых серверах без необходимости использования мощного локального оборудования. Это расширяет доступ к игровому контенту и делает видеоигры более доступными для широкой аудитории. Развитие облачных вычислений и высокоскоростных интернет-сетей способствует росту популярности таких сервисов [3].

Значительное влияние на развитие игровой индустрии оказывает искусственный интеллект. Алгоритмы машинного обучения используются для создания более реалистичного поведения персонажей, генерации игровых уровней и анализа поведения игроков. Кроме того, искусственный интеллект может применяться для автоматизации процессов разработки, тестирования и оптимизации игровых проектов.

Перспективным направлением также является развитие метавселенных – цифровых виртуальных пространств, в которых пользователи могут взаимодействовать друг с другом, участвовать в различных видах деятельности и создавать собственный контент. Игровые платформы рассматриваются как одна из основ формирования метавселенных, поскольку они уже обладают необходимой технологической инфраструктурой и большим количеством пользователей [10].

Экономические перспективы игровой индустрии во многом связаны с ростом аудитории игроков и развитием новых бизнес-моделей. Одним из наиболее быстрорастущих сегментов рынка является мобильный гейминг. Благодаря широкому распространению смартфонов и мобильного интернета мобильные игры стали наиболее массовым сегментом игровой индустрии. По данным аналитических исследований, на мобильные игры приходится более 50 % мировых доходов игровой индустрии [2].

Важной тенденцией является также развитие независимых студий разработки игр (indie-студий). Современные инструменты разработки и цифровые платформы распространения позволяют небольшим командам создавать и распространять собственные игровые проекты без необходимости сотрудничества с крупными издателями. Это способствует повышению разнообразия игрового контента и стимулирует инновации в отрасли.

Кроме того, значительные перспективы связаны с международным сотрудничеством и реализацией глобальных проектов. Игровая индустрия является по своей природе международной, поскольку разработчики, издатели и пользователи могут находиться в разных странах. Международные проекты позволяют объединять ресурсы, обмениваться опытом и расширять рынки сбыта игровых продуктов.

Несмотря на существующие ограничения, Республика Беларусь обладает рядом факторов, которые могут способствовать дальнейшему развитию игровой индустрии. Одним из таких факторов является высокий уровень подготовки специалистов в сфере информационных технологий. Наличие квалифицированных программистов, дизайнеров и специалистов по компьютерной графике создаёт благоприятные условия для формирования новых игровых студий и стартапов.

Перспективным направлением является развитие стартапов в области разработки видеоигр. Небольшие команды разработчиков могут создавать инновационные игровые проекты, ориентированные на глобальный рынок цифровых развлечений. Поддержка стартапов со стороны технологических парков, акселераторов и инвестиционных фондов может способствовать формированию новых компаний в игровой индустрии.

Также важным фактором развития может стать сотрудничество с зарубежными компаниями. Участие белорусских разработчиков в международных проектах позволяет получать доступ к современным технологиям, инвестициям и мировым рынкам. Такое сотрудничество может реализовываться как в формате аутсорсинга, так и через совместную разработку игровых продуктов.

Не менее важным направлением является развитие образовательных программ, направленных на подготовку специалистов в области разработки видеоигр. Включение в учебные программы университетов дисциплин, связанных с игровым программированием, компьютерной графикой и

дизайном игр, может способствовать формированию нового поколения специалистов для игровой индустрии.

Таким образом, перспективы развития игровой индустрии связаны с внедрением новых технологий, расширением международного сотрудничества и развитием образовательной инфраструктуры. При эффективном использовании имеющихся ресурсов Республика Беларусь может не только сохранять, но и укреплять свои позиции на мировом рынке разработки программного обеспечения и цифровых развлечений.

Игровая индустрия в современном мире является одной из наиболее динамично развивающихся отраслей цифровой экономики и важной частью сферы информационных технологий и информационно-коммуникационных технологий. В ходе проведенного исследования было установлено, что индустрия видеоигр представляет собой сложную технологическую и экономическую систему, включающую разработку программного обеспечения, цифровые платформы распространения, игровые сервисы, а также быстро развивающийся сегмент киберспорта.

Анализ структуры игровой индустрии показал, что её развитие тесно связано с использованием современных информационных технологий, включая игровые движки, технологии программирования, искусственный интеллект, облачные вычисления и сетевые решения. Развитие этих технологий способствует созданию более сложных и реалистичных игровых проектов, а также расширяет возможности применения игровых технологий в других сферах, таких как образование, медицина и моделирование сложных процессов.

В ходе исследования также было установлено, что мировой рынок видеоигр демонстрирует устойчивый рост. Увеличение количества пользователей цифровых развлечений, распространение мобильных устройств, развитие высокоскоростного интернета и появление новых форм интерактивного контента способствуют расширению масштабов отрасли. Игровая индустрия становится важным драйвером инноваций в сфере ИТ и ИКТ и оказывает значительное влияние на развитие цифровой инфраструктуры и рынка труда.

Особое внимание в статье было уделено анализу состояния игровой индустрии в Республике Беларусь. Проведенный анализ показал, что страна обладает развитым ИТ-сектором, который сформировался благодаря благоприятной институциональной среде, включая деятельность Парка высоких технологий, а также наличие квалифицированных специалистов в области программирования и разработки программного обеспечения. Белорусские компании, такие как разработчики известных онлайн-игр и мобильных игровых проектов, внесли заметный вклад в развитие мирового рынка видеоигр и укрепили репутацию страны как одного из центров разработки программного обеспечения в Восточной Европе.

Несмотря на существующие ограничения, Республика Беларусь сохраняет значительный потенциал для дальнейшего развития игровой индустрии. Высокий уровень подготовки специалистов, развитая ИТ-инфраструктура, а также участие белорусских компаний в международных проектах создают благоприятные условия для формирования новых игровых студий и стартапов. Дополнительные возможности для роста отрасли могут быть связаны с развитием образовательных программ, расширением международного сотрудничества и внедрением современных технологий, таких как виртуальная и дополненная реальность, облачный гейминг и искусственный интеллект.

Таким образом, игровая индустрия представляет собой перспективное направление развития ИТ и ИКТ-сектора, способное оказывать значительное влияние на экономическое и технологическое развитие государств. При эффективном использовании имеющихся ресурсов и создании благоприятных условий для развития инновационного предпринимательства Республика Беларусь может укрепить свои позиции на мировом рынке разработки программного обеспечения и цифровых развлечений.

Список использованных источников:

1. Video Games Market Size and Forecast 2025 to 2034 [Электронный ресурс]. – Режим доступа: <https://www.precedenceresearch.com/video-game-market>. – Дата доступа: 10.03.2026.
2. Video Game Industry Statistics and Facts [Электронный ресурс]. – Режим доступа: <https://www.statista.com/topics/868/video-games/>. – Дата доступа: 10.03.2026.
3. Cloud Gaming Market Size And Share Analysis: Growth, Trends, Forecast (2026-2031) [Электронный ресурс]. – Режим доступа: <https://www.mordorintelligence.com/industry-reports/cloud-gaming-market>. – Дата доступа: 10.03.2026.
4. Newman J. Videogames / James Newman. – London: Routledge, 2013. – 27 с.
5. Esports Market Size, Share and Trends 2026 to 2035 [Электронный ресурс]. – Режим доступа: <https://www.precedenceresearch.com/esports-market>. – Дата доступа: 10.03.2026.
6. Внешняя торговля услугами [Электронный ресурс]. – Режим доступа: <https://www.belstat.gov.by/ofitsialnaya-statistika/realny-sector-ekonomiki/vneshnyaya-torgovlya/vneshnyaya-torgovlya-uslugami/>. – Дата доступа: 10.03.2026.
7. Цифры и факты [Электронный ресурс]. – Режим доступа: <https://park.by/http/facts/>. – Дата доступа: 10.03.2026.
8. ИТ-образование и ИТ-индустрия [Электронный ресурс]. – Режим доступа: <https://www.park.by/education/about/>. – Дата доступа: 10.03.2026.
9. Virtual Reality (VR) – Statistics & Facts [Электронный ресурс]. – Режим доступа: <https://www.statista.com/topics/2532/virtual-reality-vr/>. – Дата доступа: 10.03.2026.
10. What is the Metaverse? [Электронный ресурс]. – Режим доступа: <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-metaverse>. – Дата доступа: 10.03.2026.

UDC 004.9:794.5

GAMING INDUSTRY AS A SPHERE OF IT AND ICT. STATUS AND DEVELOPMENT PROSPECTS IN THE REPUBLIC OF BELARUS

V. V. Matskevich

*Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus*

V. V. Chepikova – Senior Lecturer

Abstract. This article examines the gaming industry as an important part of the information technology and information and communications technology sectors. It analyzes the structure and technological foundation of the video game industry, as well as its economic significance in the global market. Particular attention is paid to the state of the gaming industry in the Republic of Belarus, its problems, and development constraints. It also examines the industry's development prospects and Belarus's potential for video game development.

Keywords. Gaming industry, video games, information technology, IT, ICT, digital economy, game development, game publishing, publishing, distribution platforms, digital platforms, eSports, gaming services, cloud gaming, artificial intelligence, AI, VR, AR, metaverses, game engines, programming, network technologies, internet infrastructure, mobile gaming, video game market, gaming economy, IT sector of Belarus, High-Tech Park, HTP, outsourcing, startups, investments, IT service exports, human resources, game developers, digital technologies.

УДК 519.872

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ СЕТЕВЫХ ТОПОЛОГИЙ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ТЕОРИИ МАССОВОГО ОБСЛУЖИВАНИЯ

Бондарь А.В., Вабищевич А.С., Михайлов К.В., Позняк В.М., студенты гр. 361402

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Полуян Т.В. – ассистент

Аннотация. В статье проведено сравнительное моделирование и анализ характеристик качества обслуживания для двух архитектур беспроводных сетей: самоорганизующейся (Ad-hoc) и иерархической кластерной. Исследование выполнено на модели сети из девяти узлов с помощью аппарата замкнутых сетей массового обслуживания. Для аналитической оценки применены методы глобального баланса, Гордона-Ньюэлла, Бузена и анализа средних значений (MVA), а результаты верифицированы имитационным моделированием в среде NS-3. В результате установлены предельные значения пропускной способности и характер зависимости задержки от нагрузки для каждой топологии, а также проведен сравнительный анализ точности и применимости использованных аналитических методов. Показано, что кластерная организация обеспечивает лучшую управляемость трафиком и является предпочтительной для масштабируемых систем.

Ключевые слова. Сети массового обслуживания, групповая маршрутизация, метод глобального баланса, метод Гордона-Ньюэлла, пропускная способность, алгоритм Бузена, метод анализа средних значений.

Современные системы передачи данных требуют точного прогнозирования характеристик качества обслуживания ещё на этапе проектирования. Для решения этой задачи широко применяется математический аппарат сетей массового обслуживания (СМО), который доказал свою эффективность при расчете характеристик инфокоммуникационных систем любой размерности. Именно аналитическое моделирование на основе теории массового обслуживания позволяет получить гарантированные оценки производительности системы еще на ранних стадиях ее проектирования, существенно снижая риски архитектурных ошибок [1]. Особую актуальность приобретает выбор корректного метода аналитического моделирования, способного адекватно описывать замкнутые и разомкнутые системы с ограниченными буферами.

В данной работе исследована модель сети из 9 узлов, организованных в топологию «решетка». Целью исследования является сравнительный анализ эффективности двух режимов организации связи – Ad-Hoc и Группового – а также верификация результатов имитационного моделирования в среде NS-3 с помощью теоретических методов теории очередей.

Исследуемая система представляет собой сеть, состоящую из 9 узлов, расположенных в форме решетки (3x3). Каждый узел оснащен буфером ёмкостью 3 пакета, что необходимо для предотвращения потерь данных при пиковых нагрузках.

В работе рассматриваются два режима функционирования сети. Первый режим основан на принципах самоорганизующейся (Ad-Hoc) сети, для которой характерна полная децентрализация. В данной архитектуре все узлы обладают равным статусом и автономно устанавливают соединения друг с другом, формируя динамическую топологию. С функциональной точки зрения, такая сеть эмулирует плоскую структуру локальной вычислительной сети (LAN), где механизм маршрутизации реализуется в распределенном виде, основываясь на непосредственной связности между смежными узлами.

Второй рассматриваемый режим представляет собой иерархическую кластерную модель. В ее рамках узлы агрегируются в логические группы – в данной конфигурации, в три кластера по три узла в каждом. Ключевым элементом данной архитектуры является выделение в каждом кластере ведущего узла (Cluster Head). На данный узел возлагаются специализированные функции, включая агрегацию внутригруппового трафика и организацию всей межгрупповой маршрутизации. Иерархическая организация с выделением кластеров является фундаментальным методом повышения производительности, позволяющим минимизировать накладные расходы на поддержание таблиц маршрутизации и локализовать широковещательный трафик в пределах групп [2]. Таким образом, коммуникация между различными кластерами осуществляется не напрямую, а исключительно через назначенные ведущие узлы, выступающие в роли шлюзов. Подобная логическая сегментация, обеспечивающая контролируемое взаимодействие между изолированными группами, концептуально близка к принципам построения виртуальных локальных сетей (VLAN).

Нагрузка на сеть λ_i задается одинаковой для каждого узла. В качестве инструмента имитационного моделирования выбран симулятор NS-3, позволяющий реализовать детализированные сценарии обмена пакетами и собрать статистику по задержкам и пропускной способности.

Для оценки производительности сети и верификации результатов симуляции применялись четыре фундаментальных метода теории телетрафика.

Был рассмотрен метод глобального баланса (Global Balance), основанный на составлении и решении системы уравнений равновесия для марковской цепи, описывающей состояния системы. Данный метод, где для каждого состояния S_i сумма интенсивностей выходящих потоков приравнивается к сумме интенсивностей входящих потоков, обеспечивает наиболее точные результаты для марковских процессов. Однако его недостатком является «комбинаторный взрыв» при росте числа узлов и емкости буферов, что делает его вычислительно затратным для крупных сетей. В контексте данного исследования этот метод показал наиболее оптимистичные оценки пропускной способности.

Для анализа замкнутой сети массового обслуживания с экспоненциальным обслуживанием применялся метод Гордона-Ньюэлла (Gordon-Newell). Результатом метода является мультипликативный вид (product-form solution) стационарного распределения вероятностей состояний сети:

$$P(n_1, n_2, \dots, n_M) = \frac{1}{G(N)} \prod_{i=1}^M f_i(n_i), \quad (1)$$

где $G(N)$ – нормализующая константа.

Это позволяет оценить стационарные вероятности без решения полной системы уравнений глобального баланса, хотя прямое вычисление $G(N)$ представляет вычислительную сложность.

Для эффективного вычисления этой константы использовался метод (алгоритм) Бузена (Buzen's Algorithm), также известный как алгоритм свертки. Он заменяет прямое суммирование по всем состояниям рекуррентным соотношением:

$$g(n, m) = g(n, m - 1) + X_m \cdot g(n - 1, m), \quad (2)$$

где X_m – коэффициент нагрузки узла m .

Использование алгоритма Бузена позволяет существенно снизить вычислительную сложность с экспоненциальной до полиномиальной, что было критически важно для анализа сети из 9 узлов. В проведенном эксперименте данный метод продемонстрировал более консервативную оценку пропускной способности по сравнению с методом глобального баланса.

Четвертым методом стал анализ средних значений (Mean Value Analysis, MVA) – итерационный алгоритм, позволяющий вычислять средние характеристики сети (время ожидания, длину очереди) без явного нахождения вероятностей состояний. Алгоритм базируется на теореме прибытия и законе Литтла. Для узла i среднее время пребывания заявки T_i при наличии k заявок в системе выражается через среднюю длину очереди L_i при $k-1$ заявках:

$$T_i(k) = \frac{1}{\mu_i} (1 + L_i(k - 1)), \quad (3)$$

MVA интуитивно понятен и широко используется в инженерной практике. На графиках результатов данный метод занимает промежуточное положение, обеспечивая баланс между точностью и вычислительной сложностью [3].

Сравнительные графики, иллюстрирующие зависимости пропускной способности (Throughput) и задержки (Delay) от интенсивности входной нагрузки λ для обоих режимов сети, представлены на рисунке 1.

Проведенный анализ графиков на рисунке 1 позволяет сделать следующие выводы относительно характеристик исследуемых сетевых режимов.

Анализ пропускной способности показывает, что для обоих режимов работы сети характерно насыщение максимальной пропускной способности при увеличении нагрузки. При этом модель Ad-Нос демонстрирует более резкий выход на асимптоту: метод глобального баланса прогнозирует для неё предельную пропускную способность около 4.5 Мбит/с при высоких нагрузках, тогда как метод Бузена даёт более консервативную нижнюю оценку – около 3.8 Мбит/с. Для групповой сети наблюдается схожая тенденция, однако насыщение наступает плавнее, что обусловлено структурными ограничениями, вносимыми иерархией. Эти ограничения наиболее корректно отражены методом анализа средних значений (MVA), кривая которого занимает промежуточное положение между оптимистичной оценкой глобального баланса и консервативной оценкой метода Бузена.

Анализ задержки выявляет принципиальные различия в поведении сетей. В режиме Ad-Нос задержка растёт экспоненциально при приближении нагрузки к критическому значению (около 3.5 – 4 пакетов/сек), что объясняется высокой конкуренцией равноправных узлов за среду передачи и интерференцией в плотной решётке. В групповом режиме график задержки имеет более выраженную нелинейность с характерным «коленом».

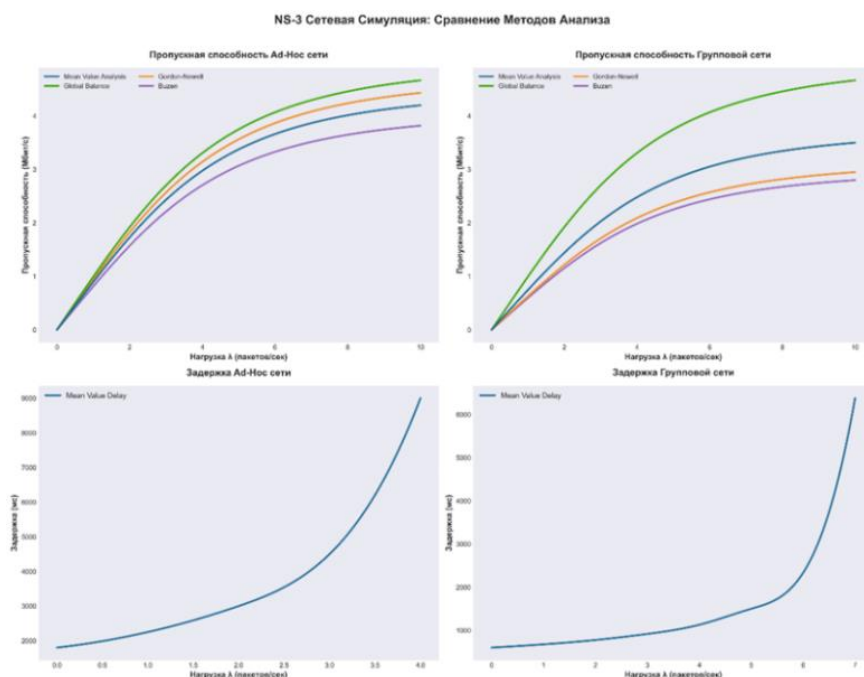


Рисунок 1 – Графики зависимости пропускной способности (Throughput) и задержки (Delay) от интенсивности входной нагрузки λ (пакетов/сек)

При малых нагрузках групповая структура вносит небольшую дополнительную задержку из-за необходимости агрегации трафика в кластерах, однако при высоких нагрузках (выше 6 пакетов/сек) наблюдается резкий скачок задержки. При этом важным преимуществом групповой архитектуры является её лучшая устойчивость и более низкий рост задержки в диапазоне средних нагрузок, что достигается за счёт иерархической организации и управления трафиком через главные узлы.

Проведенное исследование показало, что выбор топологии сети существенно влияет на её производительность. Групповой режим (кластерный) является более предпочтительным для масштабируемых систем, так как обеспечивает лучшую управляемость потоками данных, хотя и вносит дополнительные задержки на уровне главных узлов групп.

Установленная закономерность подтверждается результатами моделирования, которое не только позволило количественно оценить характеристики, но и выявило значимые различия в точности и применимости различных математических подходов к оценке производительности.

Сравнительный анализ методов моделирования выявил, что их выбор должен определяться конкретными задачами проектирования и требуемой точностью оценки. Каждый из рассмотренных подходов – метод глобального баланса, алгоритм Бузена и анализ средних значений (MVA) обладает специфическими сильными сторонами, делающими его оптимальным в определенном контексте.

Метод глобального баланса, демонстрируя высокую теоретическую точность, подходит исключительно для малых или концептуальных систем. Его фундаментальное ограничение, а именно: «комбинаторный взрыв» вычислительной сложности, делает его неприменимым для моделирования крупномасштабных топологий. Как показали результаты, в контексте сложных структур, таких как кластерная сеть, метод систематически переоценивает пропускную способность. Эта оптимистичность обусловлена тем, что полная система уравнений равновесия в меньшей степени учитывает косвенные эффекты иерархической маршрутизации и конфликты доступа, которые в полной мере проявляются при имитационном моделировании. Таким образом, его основная роль заключается в верификации других моделей и анализе базовых случаев.

В противоположность этому, алгоритм Бузена предоставляет надежную, консервативную оценку, формирующую нижнюю границу производительности системы. Его ключевым преимуществом является полиномиальная сложность вычислений на основе рекуррентных соотношений, которая обеспечивает вычислительную устойчивость даже для сетей с десятками узлов. Прогнозируемые с его помощью значения пропускной способности, как было установлено в ходе анализа, являются минимально гарантированными. Это делает данный метод незаменимым инструментом на этапе инженерного проектирования, когда требуется заложить эксплуатационный запас и гарантировать выполнение параметров качества обслуживания при наихудших сценариях нагрузки, обеспечивая отказоустойчивость проектируемой инфраструктуры.

Метод анализа средних значений (MVA) продемонстрировал себя как наиболее сбалансированный и практически ориентированный инструмент, особенно эффективный для оценки задержек в замкнутых сетях массового обслуживания. Его итерационный алгоритм, основанный на теореме прибытия, позволяет напрямую и с высокой точностью вычислять ключевые для оператора

средние показатели (время отклика и длину очереди) без ресурсоемкого расчета полного распределения вероятностей состояний. Как следствие, MVA обеспечивает реалистичный прогноз, занимая промежуточное положение между оптимистичными и консервативными оценками. Наибольшая ценность метода проявилась при анализе нелинейного поведения задержки в групповой топологии, где он точно воспроизвел характерное точку резкого нелинейного роста (перегиба) на кривой, что подтверждает его адекватность для моделирования систем с иерархической структурой.

Важным результатом работы стала успешная интеграция аналитического и имитационного моделирования. Применение инструментария симулятора NS-3 в связке со скриптовым языком Python для визуализации позволило не только подтвердить корректность аналитических расчетов, но и наглядно продемонстрировать расхождения между методами. Имитационное моделирование выступило в качестве независимого арбитра, количественно подтвердившего общие тенденции, предсказанные теорией, и обеспечило наглядное представление результатов для принятия проектных решений.

Таким образом, синергия рассмотренных методов формирует комплексную методологию проектирования. Для оценки гарантированных параметров качества обслуживания целесообразно использовать алгоритм Бузена, для оперативного анализа средних характеристик и задержек – метод MVA, а для верификации моделей на начальных этапах – метод глобального баланса. Имитационное моделирование в NS-3 завершает этот цикл, обеспечивая практическую проверку и визуализацию.

Список использованных источников:

1. Вишневецкий, В. М. Теоретические основы проектирования компьютерных сетей / В. М. Вишневецкий. – Москва: Техносфера, 2003. – 512 с.
2. Столлингс, В. Беспроводные линии связи и сети / В. Столлингс. – Москва: Вильямс, 2003. – 640 с.
3. Кокорева, Е.В. Анализ показателей качества обслуживания систем мобильной связи четвертого поколения / Е.В. Кокорева // Программные системы и вычислительные методы. – 2018. – № 3. – С. 35-44. – DOI: 10.7256/2454-0714.2018.3.26920.

UDC 519.872

COMPARATIVE ANALYSIS OF NETWORK TOPOLOGY PERFORMANCE USING QUEUING THEORY METHODS

Bondar A.V., Vabishchevich A. S., Mikhailov K. V., Pozniak U. M.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Poluyan T.V. – Assistant

Annotation. The article provides comparative modeling and analysis of quality of service characteristics for two wireless network architectures: self-organizing (Ad-hoc) and hierarchical cluster. The study was performed on a nine-node network model using a closed-loop queuing network. The methods of global balance, Gordon-Newell, Buzen and mean value analysis (MVA) were used for the analytical assessment, and the results were verified by simulation modeling in the NS-3 environment. As a result, the bandwidth limits and the nature of the load-delay dependence for each topology were established, as well as a comparative analysis of the accuracy and applicability of the analytical methods used. It is shown that cluster organization provides better traffic management and is preferable for scalable systems.

Keywords. Queuing networks, group routing, global balance method, Gordon-Newell method, throughput, Buzen algorithm, average value analysis method.

OSINT-ТЕХНОЛОГИИ В ЗАДАЧАХ ВЫЯВЛЕНИЯ ПОВЕРХНОСТИ АТАК КОРПОРАТИВНЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

Лапина С.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Насонова Н.В. – д-р техн. наук, доцент

Аннотация. Рассматривается применение OSINT-технологий для выявления внешней поверхности атак корпоративных инфокоммуникационных систем. Сформулирована гипотеза о том, что использование OSINT при инвентаризации и верификации ресурсов позволяет точнее выявлять внешние точки входа и сопоставлять их с архитектурой сети организации. Предложена трёхэтапная методика исследования, включающая сбор открытых сведений о ресурсах, формирование карты поверхности атак и её сопоставление с сегментами корпоративной сети. На примере компании показана практическая ценность подхода для специалистов по информационной безопасности, мониторинга и подготовки данных для классификации систем.

Ключевые слова. OSINT, корпоративная инфокоммуникационная система, VPN, DMZ, SOC.

Современные корпоративные инфокоммуникационные системы изменяются быстрее, чем внутренние реестры ресурсов и эксплуатационная документация. Организации публикуют веб-сервисы, тестовые стенды, каналы удалённого доступа и облачные интеграции, однако эти изменения не всегда своевременно отражаются во внутреннем учёте. В результате возникает разрыв между тем, как система описана внутри организации, и тем, как она выглядит для внешнего наблюдателя. Для специалистов по информационной безопасности это критично, поскольку атакующий начинает именно с открытой разведки: изучает домены, поддомены, сертификаты, VPN-шлюзы, почтовую инфраструктуру и иные признаки публикации сервисов [1].

Поверхность атаки корпоративной инфокоммуникационной системы определяется как совокупность всех доступных для воздействия извне и из смежных контуров ресурсов, интерфейсов, сервисов, учётных записей, каналов связи и точек интеграции, через которые потенциально может быть реализована атака. Её выявление включает инвентаризацию ресурсов, анализ сетевой архитектуры и периметра, проверку внешней доступности узлов и сервисов, а также поиск потенциально уязвимых точек взаимодействия между локальными, удалёнными и облачными сегментами.

Применение OSINT-технологий, включающее накопление и анализ данных, полученных из открытых источников в интернете, в процессах инвентаризации и верификации ресурсов позволяет построить более полную и актуальную карту внешней поверхности организации, чем при опоре только на внутренние описания. При этом OSINT рассматривается не как единственный способ инвентаризации, а как средство её дополнения и проверки за счёт независимого анализа внешне наблюдаемых ресурсов.

Методика выявления и картирования внешней поверхности атаки корпоративной инфокоммуникационной системы с использованием OSINT (рисунок 1) представляет собой трёхэтапный процесс инвентаризации внешних ресурсов, их классификации по типам сервисов и сопоставления с архитектурой корпоративной сети для оценки потенциальных точек внешнего воздействия. На первом этапе собираются открытые сведения о внешних ресурсах: домены и поддомены, публичные IP-адреса, TLS-сертификаты, почтовые записи, точки VPN-доступа. Для этого могут использоваться Amass и theHarvester для поиска доменов и поддоменов, crt.sh и SecurityTrails для анализа DNS-, MX- и сертификатных данных, а также Shodan и Censys для выявления опубликованных сервисов и их сетевых признаков. На втором этапе ресурсы группируются по функциональным категориям: веб-доступ, почта, удалённый доступ, интеграционные сервисы. На третьем этапе результаты сопоставляются с архитектурной моделью корпоративной сети: определяется, в каком периметровом сегменте расположен внешний сервис, куда он должен передавать трафик, какие внутренние сегменты и средства мониторинга затрагиваются.

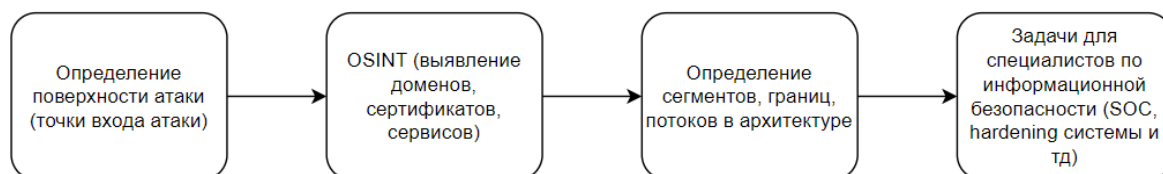


Рисунок 1 – Последовательность выявления поверхности атак с помощью OSINT в корпоративной инфокоммуникационной системе

На практике основной результат исследования состоит не в получении списка доменных имён, а в построении проверяемой модели внешнего периметра. Предложенная методика была апробирована на модели корпоративной инфокоммуникационной системы страховой компании. Для компании были выделены публичные веб-сервисы, почтовая инфраструктура и канал VPN-доступа. Каждая внешняя точка входа сопоставлялась с конкретным сетевым сегментом: клиентский портал относился к DMZ WEB, VPN-шлюз – к DMZ VPN, почтовый узел – к DMZ MAIL. Далее определялись допустимые потоки во внутренний контур: DMZ WEB – SERVER APP – DB LAN, DMZ VPN – SERVER APP и SERVER INFRA, а журналы всех периметровых компонентов направлялись в SEC LAN. Такое сопоставление позволило актуализировать контекстную схему корпоративной сети, выделить критичные границы доверия и уточнить перечень системных контуров, присутствующих в архитектуре [3].

Для повышения наглядности результаты целесообразно представлять не только в виде схемы, но и в виде компактной таблицы соответствий (таблица 1).

Таблица 1 – Сопоставление внешних ресурсов с архитектурной моделью корпоративной инфраструктуры

Внешний актив	Назначение	Сетевой сегмент	Внутренняя точка назначения
client-portal.company.by	Клиентский веб-доступ	DMZ WEB	SERVER APP
vpn.company.by	Удаленный доступ филиалов	DMZ VPN	SERVER APP / SERVER INFRA
mail.company.by	Почтовый обмен	DMZ MAIL	Mail system
api.company.by	Интеграционный сервис	DMZ WEB	SERVER APP

Построенная таблица показывает, что исследование с использованием OSINT может быть непосредственно преобразовано в инженерные артефакты для специалистов по информационной безопасности. Если внешний сервис существует, но не имеет места в архитектурной модели, это означает наличие неучтённого ресурса либо устаревшей документации. Если же ресурс отражён в схеме, но не имеет владельца, допустимого маршрута и источника логов, то организация получает зону повышенного риска, которую сложно контролировать и защищать.

На основе построенной карты внешней поверхности и уточнённой архитектурной модели были выделены ключевые системные контуры: веб-канал обслуживания, корпоративные сервисы, прикладные бизнес-сервисы и контур мониторинга. Для каждого контура определялись виды обрабатываемых данных, допустимые потоки и требования к мониторингу, что создаёт основу для последующего отнесения систем к классам типовых ИС по требованиям регулятора [2].

Таблица 2 – Выделение информационных систем по данным внешнего периметра и архитектурной модели

ИС	Ключевые данные	Размещение	Практический результат
ИС-1 Веб-канал	ПД клиентов, учетные записи	DMZ WEB, SERVER APP, DB LAN	Контроль публикации порталов и API
ИС-2 Корпоративная инфраструктура	Учетные записи, почта, файлы	SERVER INFRA, MGMT LAN	Уточнение состава сервисов удаленного доступа
ИС-3 Бизнес-логика	Договоры, обращения, вложения	SERVER APP, DB LAN, FILE SRV	Понимание критичных потоков к данным
ИС-4 Киберцентр	Логи, телеметрия, инциденты	SEC LAN, BACKUP LAN	Определение источников событий и мониторинга

Анализ результатов показывает, что OSINT целесообразно рассматривать как постоянный процесс подразделения информационной безопасности, а не как разовую исследовательскую процедуру. Его практическая ценность проявляется в трёх направлениях: выявление теневых и забытых ресурсов, проверка полноты архитектурной документации, повышение качества мониторинга в SOC. При этом OSINT не заменяет внутренний аудит и требует верификации со стороны владельцев систем, однако в качестве первичного средства контроля внешнего периметра позволяет быстрее обнаруживать расхождения между реальной внешней поверхностью корпоративной инфокоммуникационной системы и её формальным описанием.

Список использованных источников:

1. Makrushin, A. *Attack Surface Analysis and Monitoring using Open-Source Intelligence* / A. Makrushin. – 2022.
2. О внесении изменений в приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 : приказ ОАЦ от 30.12.2021 № 195.
3. *Information security, cybersecurity and privacy protection – Information security controls : ISO/IEC 27002:2022.*

УДК 004.7:004.056

ГИБРИДНАЯ АРХИТЕКТУРА: ИНТЕГРАЦИЯ БЛОКЧЕЙНА И EDGE COMPUTING В УПРАВЛЕНИИ БЕСПИЛОТНЫМ ТРАНСПОРТОМ

Алмаждуб М.А., магистрант гр. 567001

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Вишняков В.А. – д.т.н., профессор

Аннотация. В статье рассматривается гибридная архитектура управления беспилотным транспортом, основанная на интеграции технологий блокчейн и edge computing. Предложена многоуровневая модель Edge–Fog–Cloud, в которой обработка данных распределяется между бортовыми вычислительными системами, наземными узлами и облачной инфраструктурой. Такой подход позволяет обеспечить минимальные задержки обработки данных (менее 5 мс на edge-уровне), повысить отказоустойчивость системы и устранить единую точку отказа. Использование блокчейна обеспечивает целостность данных, доверие между участниками и автоматизацию взаимодействия за счет смарт-контрактов.

Ключевые слова: блокчейн, edge computing, беспилотный транспорт, V2X, децентрализация.

Введение

Современные системы управления беспилотным транспортом сталкиваются с рядом критических ограничений. Основной проблемой является использование централизованных архитектур, в которых отказ одного узла может привести к остановке всей системы [1].

Как показано в документе (стр. 2), централизованные решения подвержены следующим рискам:

- наличие единой точки отказа;
- уязвимость к атакам (MITM, spoofing);
- высокие задержки при передаче данных;
- отсутствие отказоустойчивости.

При этом требования к системам беспилотного транспорта крайне жесткие: решения должны приниматься в реальном времени, а любая задержка может привести к критическим ошибкам.

Цель данной статьи – исследование гибридной архитектуры, объединяющей edge computing и блокчейн, как способа устранения указанных ограничений.

Основная часть

В современных системах управления беспилотным транспортом ключевую роль играет необходимость обработки больших объемов данных в реальном времени при одновременном обеспечении высокой надежности и безопасности. Бортовые системы автономных транспортных средств непрерывно генерируют потоки данных от сенсоров (камеры, LiDAR, радары), которые должны быть обработаны с минимальной задержкой. Использование централизованных облачных решений в таких условиях приводит к увеличению времени отклика и создает критическую зависимость от доступности сети [2]. Кроме того, централизованная архитектура формирует единую точку отказа, что делает систему уязвимой к сбоям и кибератакам.

Дополнительной проблемой является обеспечение доверия между участниками сети. В распределенной среде беспилотного транспорта взаимодействуют различные устройства и системы, принадлежащие разным субъектам. Отсутствие доверенной среды может привести к подмене данных, атакам типа spoofing или перехвату управляющих команд [3]. Классические механизмы защиты не всегда способны обеспечить необходимый уровень безопасности, особенно в условиях высокой динамики сети.

С другой стороны, применение блокчейн-технологий в чистом виде также имеет ограничения. К ним относятся высокая задержка подтверждения транзакций, ограниченная пропускная способность и значительные вычислительные затраты. Это делает традиционные блокчейн-системы (особенно с алгоритмами консенсуса типа Proof-of-Work) непригодными для задач, требующих обработки данных в режиме реального времени. Таким образом, возникает необходимость поиска архитектурного решения, способного объединить преимущества различных подходов и компенсировать их недостатки.

Таким решением является гибридная архитектура, основанная на интеграции edge computing и блокчейн [4]. В рамках данного подхода вычислительные задачи распределяются между несколькими уровнями системы, что позволяет оптимизировать обработку данных и повысить общую эффективность.

Гибридная архитектура включает три уровня: Edge, Fog и Cloud. На уровне Edge выполняются бортовые вычисления непосредственно на транспортных средствах. Этот уровень отвечает за обработку сенсорных данных, локальный анализ дорожной обстановки и принятие оперативных решений. Благодаря размещению вычислительных ресурсов вблизи источника данных достигается

минимальная задержка (менее 5 мс), что является критически важным для систем управления движением [1–2]. Кроме того, edge-уровень обеспечивает автономность работы системы в случае потери связи с внешними узлами.

Уровень Fog представляет собой промежуточный слой между edge-устройствами и облачной инфраструктурой. Он включает наземные узлы, такие как дорожные станции (RSU), локальные серверы и центры обработки данных регионального уровня. Основными функциями данного уровня являются агрегация данных, предварительная обработка информации и координация взаимодействия между транспортными средствами. На этом уровне также может выполняться частичная валидация транзакций и взаимодействие с блокчейн-сетью, что позволяет снизить нагрузку на глобальную систему и повысить ее масштабируемость.

На уровне Cloud осуществляется централизованная аналитика, хранение данных и выполнение смарт-контрактов. В отличие от традиционных облачных решений, данный уровень интегрирован с блокчейн-сетью, что обеспечивает децентрализованное хранение информации и ее криптографическую защиту. Блокчейн позволяет гарантировать неизменяемость данных, их проверяемость и прозрачность взаимодействия между участниками системы. Смарт-контракты автоматизируют выполнение правил и процессов, исключая необходимость участия доверенного посредника [3].



Рисунок 1 – Многоуровневая архитектура Edge–Fog–Cloud

Ключевым преимуществом гибридной архитектуры является разделение функций между уровнями системы. Обработка данных, требующая минимальных задержек, выполняется на edge-уровне, тогда как задачи обеспечения безопасности и доверия реализуются с использованием блокчейн-технологий. Такой подход позволяет преодолеть ограничения классических распределенных систем и достичь баланса между производительностью, безопасностью и масштабируемостью.

Использование edge computing позволяет существенно снизить нагрузку на сеть и уменьшить объем передаваемых данных за счет их предварительной обработки. Это особенно важно в условиях высокой плотности транспортных потоков, где количество генерируемых данных может достигать значительных величин. В свою очередь, блокчейн обеспечивает надежную защиту информации, предотвращая ее подмену или несанкционированное изменение.

Дополнительным преимуществом является повышение отказоустойчивости системы. В гибридной архитектуре отсутствует единый центр управления, что исключает возможность полной остановки системы при выходе из строя одного из узлов. Распределенная структура сети позволяет сохранять работоспособность даже в условиях частичных отказов или атак.

Гибридный подход также способствует повышению масштабируемости системы. Добавление новых транспортных средств или вычислительных узлов не требует значительных изменений архитектуры, что позволяет эффективно расширять систему по мере роста нагрузки.

Важным аспектом реализации данной архитектуры является возможность эффективной координации групп беспилотных аппаратов, что особенно актуально при управлении роевыми структурами в динамических городских условиях [5]. В таких сценариях использование Edge-уровня позволяет минимизировать время реакции на изменение траекторий соседних транспортных средств, в то время как блокчейн-платформа обеспечивает доверенную среду для обмена телеметрией и предотвращает атаки, направленные на подмену координат или перехват управления. Кроме того, создание подобной децентрализованной инфраструктуры способствует укреплению цифрового суверенитета и технологической независимости критических транспортных систем [6]. Это делает их устойчивыми к потенциальным сбоям глобальных облачных сервисов и повышает общую надежность национального сегмента интернета вещей в условиях внешних киберугроз. Реализация протоколов безопасного совместного использования данных на стыке Edge-вычислений и блокчейна позволяет не только оптимизировать распределение трафика, но и сформировать прозрачную базу для аудита

действий автономных систем, что критически важно для юридического разграничения ответственности при возникновении дорожных инцидентов.

Заключение

Таким образом, интеграция блокчейн и edge computing формирует основу для построения интеллектуальных транспортных систем нового поколения, способных обеспечивать безопасное, надежное и эффективное управление беспилотным транспортом в условиях реального времени.

Список литературы

1. Смирнов, Д. В., Кузнецов, М. А. «Гибридные архитектуры блокчейн-Edge: новые парадигмы для децентрализованных автономных систем». Сборник научных трудов «Цифровые Инновации в Транспорте», Том 7, № 1, 2023, с. 25-39.
2. Сидоров, А. Н., Козлова, О. И. «Оптимизация обработки данных в автономных транспортных средствах с использованием Edge Computing». Труды Международной конференции «Передовые Технологии в Транспорте», Москва, 2021, с. 112-120.
3. Иванов, С. А., Петрова, Е. В. «Применение технологии блокчейн для обеспечения безопасности данных в беспилотных летательных аппаратах». Журнал «Распределенные Системы и Кибербезопасность», № 3, 2022, с. 45-58.
4. Wang, H., Li, X. "Blockchain-Enabled Secure Data Sharing in Edge Computing for IoT". IEEE Internet of Things Journal, Vol. 8, Issue 1, 2021, pp. 248-259.
5. Волков, В. П., Зайцева, Н. Д. «Координация роев беспилотных аппаратов: обзор и перспективы гибридных подходов». Журнал «Искусственный Интеллект и Робототехника», Том 15, № 2, 2020, с. 78-91.
6. Лебедев, Г. М., Соколова, Л. С. «Вопросы цифрового суверенитета и независимости инфраструктуры критических объектов в эпоху автономных систем». Монография. Издательство «Техносфера», 2024, 280 с.

UDC 004.7:004.056

HYBRID ARCHITECTURE: INTEGRATION OF BLOCKCHAIN AND EDGE COMPUTING IN AUTONOMOUS TRANSPORT MANAGEMENT

Almajdoub M.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Vishniakov V.A. – Doctor of Technical Sciences, Professor

Annotation. The article examines a hybrid architecture for autonomous transport management based on the integration of blockchain and edge computing technologies. A multi-level Edge–Fog–Cloud model is proposed, in which data processing is distributed between onboard computing systems, ground nodes, and cloud infrastructure. This approach ensures minimal latency (less than 5 ms at the edge level), improves system fault tolerance, and eliminates a single point of failure. The use of blockchain provides data integrity, trust between participants, and automation of interactions through smart contracts.

Keywords. Blockchain, edge computing, autonomous transport, V2X, decentralization

УДК 004.738

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА АДАПТИВНОГО МОНИТОРИНГА КАЧЕСТВА ВОСПРИЯТИЯ ИНФОКОММУНИКАЦИОННЫХ УСЛУГ

Элтарabili М.С., магистрант гр.567001

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лагутин А.Е. – канд. тех. наук, доцент

Аннотация. В статье рассматриваются методы разработки интеллектуальной системы адаптивного мониторинга качества восприятия (QoE) инфокоммуникационных услуг. Особое внимание уделяется моделям оценки QoE с использованием методологий ITU-T и алгоритмов машинного обучения. Рассматриваются механизмы реального времени адаптации мониторинга, методы сбора и обработки метрик качества на основе нейронных сетей, а также применение многофакторной интеллектуальной обработки данных. Отдельно проводится анализ особенностей реализации клиентской части системы на платформе Flutter/Dart. Показано, что комплексное применение современных методов искусственного интеллекта позволяет значительно повысить точность оценки качества восприятия и эффективность управления инфокоммуникационными услугами в реальном времени.

Ключевые слова: качество восприятия, QoE, адаптивный мониторинг, инфокоммуникационные услуги, машинное обучение, нейронные сети, ITU-T, Flutter, Dart.

Введение

Моделирование качества восприятия инфокоммуникационных услуг. Одним из наиболее важных этапов разработки интеллектуальных систем мониторинга является анализ и моделирование качества восприятия. Для систематизации моделей широко применяются рекомендации ITU-T и методы машинного обучения [1, 2].

Модели QoE (рисунок 1) включают шесть основных категорий оценки: субъективные (MOS – Mean Opinion Score), объективные (PESQ, POLQA), гибридные и предиктивные на основе машинного обучения. Рекомендации ITU-T (P.800, GSTR-5GQoE) позволяют классифицировать параметры восприятия и прогнозировать удовлетворённость пользователей ещё на этапе проектирования архитектуры системы.

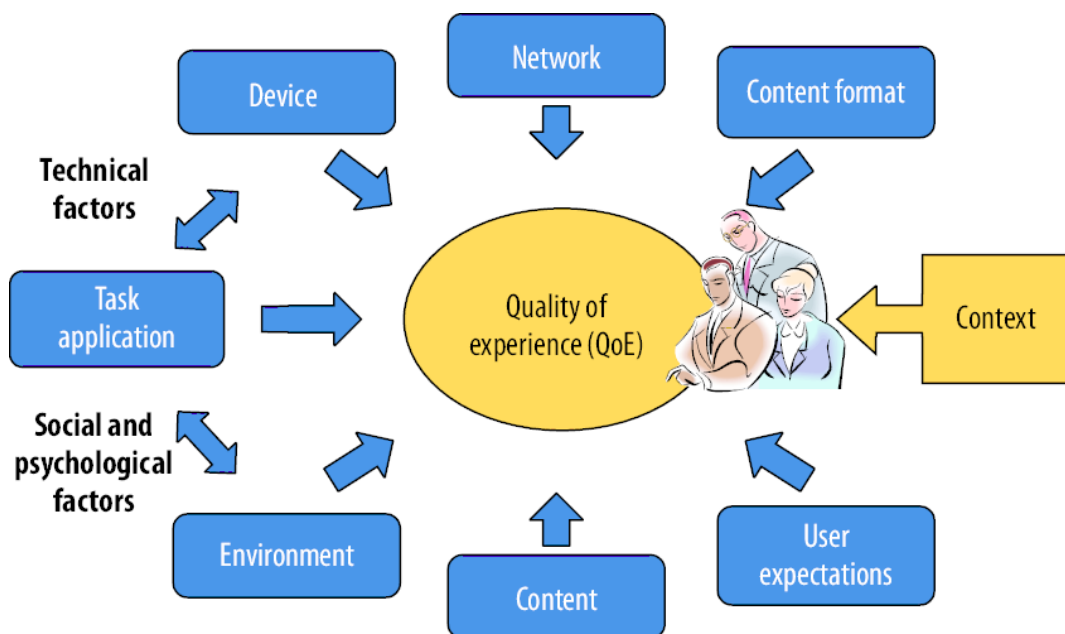


Рисунок 1 – Модель оценки качества восприятия QoE

Методология ITU-T представляет собой международный стандарт анализа качества восприятия мультимедийных услуг. Наиболее известным документом является серия рекомендаций по QoE, содержащая перечень наиболее распространённых метрик [1], включая задержку, джиттер, потери пакетов, разрешение видео и поведенческие характеристики пользователя. Применение моделей машинного обучения (нейронные сети, градиентный бустинг) позволяет переходить от статических оценок к динамическому прогнозированию QoE в реальном времени.

Методы адаптивного мониторинга качества восприятия

В инфокоммуникационных системах обрабатываются различные категории метрик качества восприятия: сетевые параметры (задержка, пропускная способность), контекстные данные (устройство, геолокация) и субъективные отзывы пользователей. Для обеспечения адаптивности мониторинга необходимо применять комплекс мер на основе искусственного интеллекта. К основным принципам относятся точность, оперативность и масштабируемость оценки [3, 8].

Одним из основных методов является использование протоколов сбора данных в реальном времени с применением *HTTPS* и *TLS*-шифрования для защищённой передачи метрик. Дополнительной мерой является агрегация данных на краю сети (*edge computing*) и облачная обработка. Также рекомендуется использовать систему динамического разграничения частоты мониторинга на основе текущего уровня *QoE*.

Важным аспектом является реализация механизмов интеллектуальной обработки, обеспечивающих адаптацию параметров мониторинга в зависимости от контекста. При этом необходимо применять принцип минимизации нагрузки на устройство пользователя, согласно которому мониторинг активизируется только при необходимости.

Дополнительно следует учитывать требования нормативно-правовых актов в области обработки пользовательских данных, включая прозрачность сбора метрик и получение согласия.

Не менее важной мерой является организация мониторинга и журналирования событий *QoE*. Ведение логов позволяет выявлять аномалии и оперативно корректировать параметры услуг.

Также рекомендуется применять методы обезличивания данных, что снижает риск компрометации пользовательской информации. В совокупности перечисленные меры формируют многоуровневую адаптивную систему мониторинга, обеспечивающую высокий уровень точности оценки *QoE* в инфокоммуникационных услугах.

Механизмы интеллектуальной обработки и адаптации

Для обеспечения эффективного адаптивного мониторинга необходимо реализовать надёжные механизмы интеллектуальной обработки данных. Интеллектуальная обработка позволяет прогнозировать *QoE*, а адаптация определяет динамическое изменение параметров системы. Разграничение этих процессов является важным условием построения эффективной архитектуры.

Одним из наиболее распространённых подходов является использование моделей машинного обучения [5]. Они позволяют прогнозировать качество восприятия на основе сетевых параметров без необходимости передачи больших объёмов сырых данных. В рамках данного подхода применяются нейронные сети и алгоритмы градиентного бустинга, которые предоставляют точные предсказания в реальном времени. Это особенно актуально для кроссплатформенных систем, где клиентское приложение взаимодействует с сервером через *API*.

В современных системах часто применяются гибридные модели на основе *LSTM* и *Transformer* для временных рядов [6]. Такие модели обеспечивают высокую точность прогнозирования и позволяют снижать нагрузку на сеть за счёт предиктивной адаптации. Однако при использовании *ML*-моделей необходимо учитывать риски переобучения и применять механизмы их защиты, такие как валидация на реальных данных и использование безопасных алгоритмов обучения.

Для повышения уровня адаптивности рекомендуется применять контекстно-зависимую обработку (*context-aware adaptation*). В этом случае система корректирует частоту мониторинга и набор метрик в зависимости от контекста, включая сетевые условия, тип услуги и поведение пользователя. Использование адаптивных алгоритмов существенно повышает эффективность, даже в условиях изменяющейся среды.

Дополнительно в современных системах применяются методы федеративного обучения, при которых модель обучается на устройстве пользователя без передачи сырых данных. При обнаружении аномалий система может автоматически корректировать параметры услуг.

Также важным элементом является защита моделей и их безопасное хранение на стороне клиента. Рекомендуется использовать защищённые хранилища и избегать передачи моделей по незащищённым каналам. На стороне сервера необходимо реализовать проверку актуальности моделей и механизм их обновления.

Таким образом, комплексное применение моделей машинного обучения, контекстной адаптации и федеративного обучения позволяет обеспечить высокий уровень интеллектуальности кроссплатформенных систем мониторинга и эффективно управлять качеством восприятия инфокоммуникационных услуг. На рисунке 2 представлена схема адаптивного мониторинга (*ML* + контекстная адаптация) – поток обработки данных.

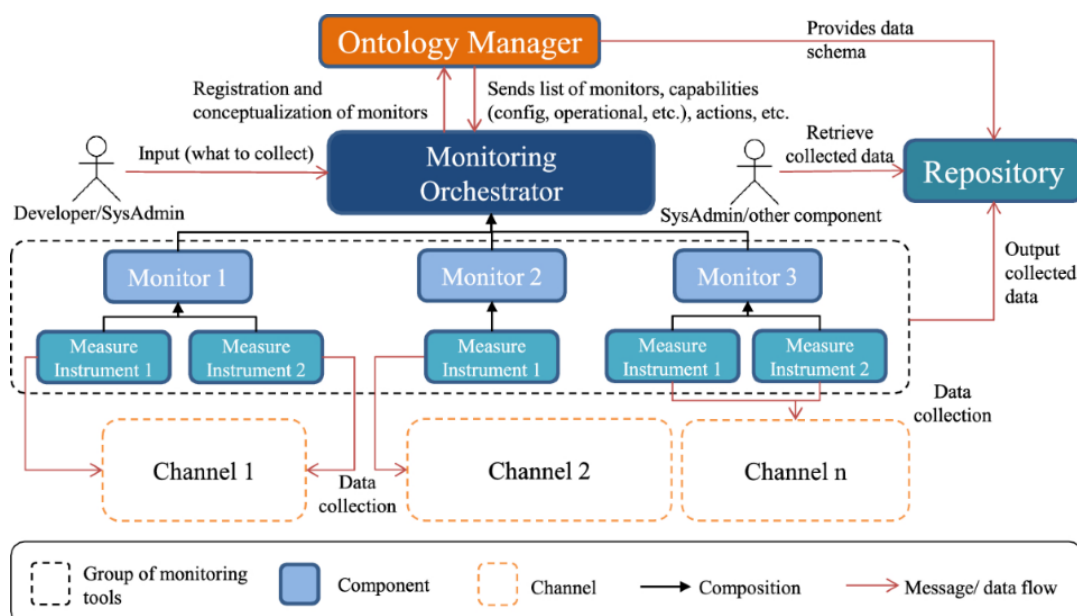


Рисунок 2 – Схема адаптивного мониторинга (ML + контекстная адаптация) – поток обработки данных

Анализ особенностей реализации кроссплатформенных приложений мониторинга на платформе Flutter/Dart

Платформа Flutter широко используется для разработки кроссплатформенных приложений мониторинга QoE [4]. Несмотря на преимущества, связанные с высокой производительностью и удобством разработки, подобные приложения могут сталкиваться с особенностями реализации, влияющими на точность мониторинга. Одной из распространённых проблем является высокое потребление ресурсов при сборе метрик в реальном времени. Для предотвращения подобных проблем рекомендуется использовать оптимизированные API и background-процессы, а также избегать избыточного сбора данных. Кроме того, необходимо регулярно проводить анализ производительности программного обеспечения, используя методы статического и динамического профилирования [4, 7]. В таблице 1 приведены основные особенности реализации и методы их оптимизации.

Таблица 1 – Основные особенности реализации Flutter/Dart-приложений мониторинга QoE и методы оптимизации

Особенность	Описание	Методы оптимизации
Высокое потребление батареи	Постоянный сбор сетевых метрик в фоне	Оптимизация background-процессов, использование WorkManager
Задержка обработки данных	Реальное время обработки больших объёмов метрик	Локальное предобучение моделей ML, кэширование
Несовместимость API	Различия в доступе к системным метрикам на Android/iOS	Пакет flutter_plugin для кроссплатформенного доступа
Перехват сетевого трафика	Передача метрик QoE может быть подвержена задержкам	Certificate pinning, оптимизация HTTPS
Обратная инженерия кода	Возможность анализа логики мониторинга	Обфускация кода, минимизация чувствительной логики
Недостаточный анализ производительности	Проблемы с FPS и точностью остаются незамеченными	Статический и динамический профилинг, Firebase Performance Monitoring

Заключение

В условиях активной цифровизации инфокоммуникационной сферы обеспечение адаптивного мониторинга качества восприятия становится одной из ключевых задач разработки программных систем [1, 2]. Применение моделей ITU-T и методов машинного обучения позволяет выявлять и прогнозировать параметры QoE на ранних этапах. Использование современных механизмов интеллектуальной адаптации, включая нейронные сети и контекстно-зависимые алгоритмы, значительно повышает точность оценки [5, 6, 8]. Комплексное применение технологий реального времени, edge-вычислений и кроссплатформенной реализации позволяет создать надёжную интеллектуальную систему адаптивного мониторинга качества восприятия инфокоммуникационных услуг.

Список использованных источников:

- 1 ITU-T Recommendation P.10/G.100. Vocabulary for performance and quality of service. – ITU, 2022. – [Электронный ресурс]. – Режим доступа: <https://www.itu.int>.
- 2 Machine Learning for QoE Management in Future Wireless Networks / Various authors. – 2021. – [Электронный ресурс]. – Режим доступа: <https://www.researchgate.net/publication/355381291>.
- 3 Stallings W. Cryptography and Network Security: Principles and Practice. – Pearson Education, 2017.
- 4 Flutter Performance Monitoring / Flutter Documentation. – [Электронный ресурс]. – Режим доступа: <https://docs.flutter.dev/perf>.
- 5 GSTR-5GQoE: QoE requirements for real-time multimedia services over 5G networks / ITU-T. – 2022. – [Электронный ресурс]. – Режим доступа: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-QOS-2022-1-PDF-E.pdf.
- 6 JSON Web Token (JWT) (RFC 7519) / Jones M., Bradley J., Sakimura N. – IETF. – 2015. – [Электронный ресурс]. – Режим доступа: <https://datatracker.ietf.org/doc/html/rfc7519> (адаптировано для ML-моделей).
- 7 OWASP Mobile Security Testing Guide / OWASP. – [Электронный ресурс]. – Режим доступа: <https://owasp.org/www-project-mobile-security-testing-guide/>.
- 8 Bishop M. Computer Security: Art and Science. – Boston: Addison-Wesley, 2018.
- 9 Android Performance Monitoring / Android Developers. – [Электронный ресурс]. – Режим доступа: <https://developer.android.com>.
- 10 ISO/IEC 27001 Information Security Management Systems / ISO. – 2022. – [Электронный ресурс]. – Режим доступа: <https://www.iso.org/isoiec-27001-information-security.html>.

UDC 004.738

INTELLIGENT SYSTEM FOR ADAPTIVE MONITORING OF THE QUALITY OF PERCEPTION OF INFOCOMMUNICATION SERVICES

Eltarabily M.S.

Belarusian State University of Informatics and Radioelectronics1, Minsk, Republic of Belarus

Lagutin A.E. – PhD in Technical Sciences, Associate Professor

Abstract. The article analyzes methods for developing an intelligent system for adaptive monitoring of the quality of experience (QoE) in infocommunication services. Special attention is paid to QoE evaluation models using ITU-T methodologies and machine learning algorithms. The paper discusses real-time adaptation mechanisms, data collection and processing methods based on neural networks, as well as the implementation of cross-platform technologies. The study shows that a comprehensive AI approach significantly improves the accuracy of quality perception assessment and the efficiency of infocommunication service management.

Keywords: quality of experience, QoE, adaptive monitoring, infocommunication services, machine learning, neural networks, ITU-T, Flutter, Dart.

УДК 004.7:004.056

ПОВЫШЕНИЕ ОТКАЗОУСТОЙЧИВОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Скиб А.И., магистрант гр. 567001

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Лагутин А.Е. – канд. тех. наук, доцент

Аннотация. В статье рассматриваются основные способы повышения отказоустойчивости в компьютерных сетях. Описаны подходы, направленные на обеспечение непрерывности работы сетевой инфраструктуры при сбоях оборудования, каналов связи и программного обеспечения. Рассматриваются методы резервирования, кластеризации, балансировки нагрузки и динамической маршрутизации. Сделан вывод о необходимости комплексного подхода для обеспечения высокой доступности сети.

Ключевые слова: отказоустойчивость, сеть, резервирование, кластер, маршрутизация, балансировка нагрузки.

Введение

Современные компьютерные сети выступают фундаментом цифровой инфраструктуры любой организации [1–2]. От их стабильной работы зависит функционирование корпоративных информационных систем, облачных сервисов и критически важных бизнес-процессов. В условиях высоких требований к непрерывности предоставления услуг (SLA) даже кратковременные сетевые сбои приводят к существенным финансовым и репутационным потерям [3].

Современные корпоративные стандарты требуют обеспечения уровня доступности сети (High Availability) не ниже «четырёх девяток» (99,99 %), что допускает простой не более 52,6 минут в год, а для критических систем 99,999 % (около 5 минут простоя в год) [4]. Одной из главных проблем при проектировании таких сетей является устранение «единых точек отказа» (Single Point of Failure, SPOF) узлов или каналов, выход из строя которых приводит к неработоспособности всей системы.

Цель данной статьи – систематизация и анализ методов повышения отказоустойчивости компьютерных сетей с оценкой их эффективности в современных инфраструктурах.

Методы

Исследование базируется на анализе научно-технической литературы, международных стандартов (RFC), а также рекомендаций ведущих производителей сетевого оборудования (Cisco Validated Design). В работе применен метод сравнительного анализа для оценки технических характеристик различных протоколов резервирования и архитектурных решений. Критериями оценки выступили время сходимости (восстановления связи), сложность внедрения и способность обеспечивать заданные метрики RTO (Recovery Time Objective).

Примечание. При подготовке текста использовался искусственный интеллект исключительно для улучшения стилистики и перевода аннотации на английский язык под строгим контролем автора.

Результаты анализа

Базовым подходом к устранению SPOF является аппаратное резервирование и мультихоминг (подключение к нескольким независимым провайдерам) [5]. Дублирование физических линков и узлов формирует основу для работы логических механизмов отказоустойчивости.

На сетевом уровне широкое применение находят протоколы резервирования первого шлюза (FHRP), в частности VRRP (Virtual Router Redundancy Protocol) [6].

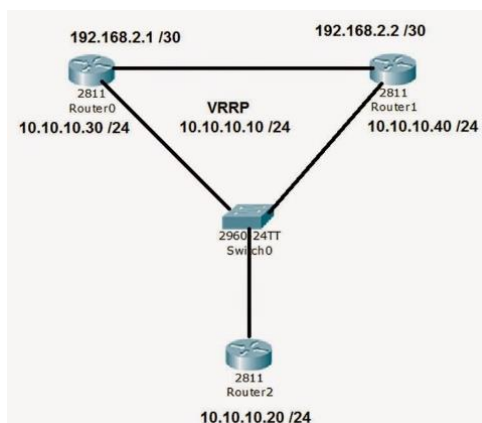


Рисунок 1 – Схема работы протокола VRRP

Архитектура VRRP (рис. 1) строится по принципу кластера «master-slave» (режим active/passive). Маршрутизаторы объединяются в логическую группу с общим виртуальным IP-адресом. Основной узел (Master) обрабатывает весь трафик, а резервный (Slave) находится в режиме ожидания, непрерывно получая служебные сообщения (heartbeat). При падении мастера резервный узел автоматически (обычно в течение 1–3 секунд) перехватывает виртуальный IP- и MAC-адрес, восстанавливая маршрутизацию незаметно для конечных узлов. Для серверов и межсетевых экранов применяется кластеризация.

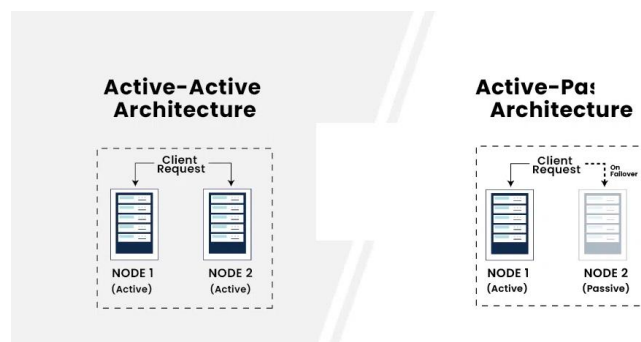


Рисунок 2 – Архитектура отказоустойчивых кластеров (Active-Passive и Active-Active)

В режиме Active-Passive логика аналогична VRRP, тогда как в режиме Active-Active (рис. 2) все узлы кластера одновременно обрабатывают трафик, что требует применения механизмов балансировки нагрузки (Load Balancing, например, HAProxy, Nginx или аппаратных ADC) [7]. Балансировщик распределяет запросы и автоматически исключает упавший узел из пула маршрутизации.

Особую роль играет динамическая маршрутизация (OSPF, BGP). В отличие от статических маршрутов, динамические протоколы способны автоматически перестраивать таблицу маршрутизации при падении линка [8–9]. Сходимость OSPF при правильной настройке таймеров может составлять менее секунды.

Для систематизации проанализированных подходов была составлена сравнительная таблица (Таблица 1).

Таблица 1 – Сравнительная характеристика методов повышения отказоустойчивости

Метод	Принцип действия	Преимущества	Недостатки	Среднее время восстановления
VRRP (Active/Passive)	Перехват виртуального IP резервным маршрутизатором при сбое основного	Простота настройки, прозрачность для хостов	Простаивание ресурсов резервного узла (Slave)	1–3 секунды
Кластер Active/Active	Распределение нагрузки между всеми узлами с автоматическим исключением сбойных	Максимальная утилизация ресурсов, высокая производительность	Сложность настройки синхронизации состояний (stateful)	Миллисекунды – секунды
Динамическая маршрутизация (OSPF)	Автоматический перерасчет метрик и путей при изменении топологии	Масштабируемость, учет состояния каналов на всей сети	Требует вычислительных ресурсов для работы алгоритма SPF	< 1 секунды (с BFD)
Мультихоминг + BGP	Подключение к разным ISP с анонсированием автономной системы	Защита от аварий на стороне провайдера	Высокая стоимость, сложная настройка политик маршрутизации	10–90 секунд

Анализ эффективности

Анализ показывает, что ни один из методов по отдельности не гарантирует доступность на уровне 99,99 %. Использование только динамической маршрутизации защищает сеть от обрыва оптики, но не спасет от падения шлюза по умолчанию на стороне локальных хостов (здесь необходим

VRRP). В свою очередь, VRRP не защитит от перегрузки сервиса (здесь нужен балансировщик и кластер Active/Active).

Современным трендом в повышении отказоустойчивости является внедрение программно-определяемых сетей (SDN) [10] и микросервисных архитектур (например, на базе Kubernetes) [11], где функции сетевого управления отделены от передачи данных. Это позволяет контроллеру SDN мгновенно перенаправлять потоки при обнаружении деградации каналов, снижая RTO практически до нуля.

Кроме того, при оценке эффективности выбранной стратегии необходимо учитывать не только скорость переключения (Failover Time), но и сохранение целостности сессий пользователей. В современных мультиоблачных и гибридных инфраструктурах классических методов резервирования становится недостаточно из-за задержек на трансграничных каналах связи. Внедрение интеллектуальных систем мониторинга, работающих в связке с протоколами BFD (Bidirectional Forwarding Detection), позволяет сократить время обнаружения обрыва линка до нескольких миллисекунд, что критически важно для передачи голоса (VoIP) и потокового видео. Также стоит отметить, что избыточность инфраструктуры неизбежно ведет к усложнению администрирования: увеличение числа активных узлов в кластере Active-Active повышает вероятность возникновения ошибок конфигурации. Таким образом, баланс между максимальной отказоустойчивостью и операционной простотой системы является основной задачей сетевого инженера при проектировании масштабируемых сетей.

Заключение

Таким образом, повышение отказоустойчивости компьютерных сетей требует комплексного подхода. Использование только одного метода не обеспечивает полной защиты от сбоев. Наиболее эффективным является сочетание резервирования, кластеризации, балансировки нагрузки и динамической маршрутизации.

Современные сети должны проектироваться с учетом возможных отказов и предусматривать механизмы автоматического восстановления. Это позволяет обеспечить непрерывность работы сервисов и повысить надежность всей информационной инфраструктуры.

Список литературы

1. Таненбаум Э., Уэзеролл Д. *Компьютерные сети*. 5-е изд. СПб.: Питер, 2012. 960 с.
2. Олифер В. Г., Олифер Н. А. *Компьютерные сети. Принципы, технологии, протоколы*. 6-е изд. СПб.: Питер, 2020. 1008 с.
3. Kurose J. F., Ross K. W. *Computer Networking: A Top-Down Approach*. 8th ed. Pearson, 2021. 864 p.
4. Cisco Systems. *Enterprise Campus 3.0 Architecture: Overview and Framework*. Cisco Validated Design (CVD), 2023. [Электронный ресурс]. URL: https://www.cisco.com (дата обращения: 26.03.2026).
5. Chen, M., et al. "BGP Multihoming and Fast Reroute Mechanisms for Enterprise Networks." *IEEE Transactions on Network and Service Management*, vol. 22, no. 2, 2025, pp. 210-225.
6. RFC 5798. *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*. Internet Engineering Task Force (IETF), 2010.
7. Smith, R., Jones, T. "Evaluating Load Balancing Algorithms in Active-Active High Availability Clusters." *Springer Journal of Network and Systems Management*, vol. 32, no. 4, 2024, pp. 55-78.
8. Дойл Дж., Кэрролл Д. *Маршрутизация TCP/IP*. Том 1. 2-е изд. М.: Вильямс, 2006. 800 с.
9. Иванов А. С., Петров В. В. *Сравнительный анализ протоколов динамической маршрутизации при построении отказоустойчивых сетей* // *Вестник инфокоммуникационных технологий*. 2025. Т. 12. № 2. С. 34-41.
10. Zhang, Y., et al. "High Availability in Software-Defined Networking: A Comprehensive Survey." *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, 2023, pp. 450-485.
11. Li, X., Wang, H. "Reliability Analysis of Kubernetes-based Microservice Architectures in Edge Computing." *Elsevier Future Generation Computer Systems*, vol. 142, 2024, pp. 112-125.

UDC 004.7:004.056

IMPROVING FAULT TOLERANCE IN COMPUTER NETWORKS

Skib A.I.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Lagutin A.E. – PhD in Technical Sciences, Associate Professor

Annotation. The article considers the main methods of improving fault tolerance in computer networks. The approaches aimed at ensuring continuous operation of network infrastructure in case of failures of equipment, communication channels and software are described. The methods of redundancy, clustering, load balancing and dynamic routing are analyzed. The result of the study is the conclusion that a comprehensive approach is required to achieve high availability and reliability of modern networks.

Keywords: fault tolerance, computer networks, redundancy, clustering, load balancing, routing

УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ VPN (IPSEC VS OPENVPN VS WIREGUARD) ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ

Пурус А.О., Голубев А.А., студенты гр.568403

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Чепикова В.В. – старший преподаватель

Аннотация. В работе представлен сравнительный анализ трех основных протоколов виртуальных частных сетей: IPsec, OpenVPN и WireGuard. Рассмотрены особенности их архитектуры, механизмы шифрования, производительность и удобство настройки. Выявлены сильные и слабые стороны каждого протокола, а также даны рекомендации по их применению в различных сценариях использования.

Ключевые слова. VPN, IPsec, OpenVPN, WireGuard, безопасность данных, сравнение протоколов, шифрование, производительность.

Введение

В современном цифровом мире защита передаваемых данных становится одной из приоритетных задач. Виртуальные частные сети (VPN) предоставляют возможность безопасного соединения между удаленными узлами через публичные сети, такие как Интернет [1]. На сегодняшний день существует множество протоколов VPN, каждый из которых имеет свои особенности, преимущества и недостатки. Наиболее распространенными являются IPsec, OpenVPN и WireGuard.

Цель данной работы – провести сравнительный анализ этих трех протоколов по ключевым критериям: безопасность, производительность, удобство настройки и совместимость. Результаты исследования помогут сделать обоснованный выбор протокола в зависимости от конкретных требований к защите данных и условиям эксплуатации.

Обзор протоколов VPN

IPsec (Internet Protocol Security) – это набор протоколов для защиты IP-трафика, который работает на сетевом уровне модели OSI [2]. Стандарт был разработан IETF (Internet Engineering Task Force) и включает два основных протокола: AH (Authentication Header) для аутентификации и ESP (Encapsulating Security Payload) для шифрования и аутентификации [6]. Для управления ключами используется протокол IKE (Internet Key Exchange), который прошел эволюцию от IKEv1 до более совершенного IKEv2 [10].

IPsec широко применяется в корпоративной среде для построения site-to-site VPN и обеспечивает высокий уровень безопасности [5]. Протокол имеет встроенную поддержку в большинстве операционных систем и сетевых устройств, что упрощает его внедрение в существующую инфраструктуру [2].

OpenVPN – это открытое программное решение, которое использует протоколы SSL/TLS для обеспечения безопасности [1]. В отличие от IPsec, OpenVPN работает на прикладном уровне и может использовать как TCP, так и UDP в качестве транспорта [9].

Ключевая особенность OpenVPN – его гибкость. Протокол может работать через любой порт, включая 443 (стандартный порт HTTPS), что позволяет обойти многие сетевые ограничения и межсетевые экраны [9]. OpenVPN поддерживает широкий спектр криптографических алгоритмов, включая AES-256-GCM, ChaCha20-Poly1305 и другие [5].

WireGuard – это современный протокол VPN, который появился в 2015 году и быстро завоевал популярность благодаря своей простоте и высокой производительности [4]. Протокол встроен непосредственно в ядро Linux и состоит всего из 4000 строк кода (для ядерной реализации), что значительно упрощает его аудит безопасности [8].

WireGuard использует современные криптографические алгоритмы: ChaCha20 для шифрования, Poly1305 для аутентификации, Curve25519 для обмена ключами и BLAKE2s для хеширования [4]. Такой ограниченный, но тщательно подобранный набор алгоритмов исключает возможность ошибочной конфигурации [5].

Сравнительный анализ

1. **Безопасность.** Все три рассматриваемых протокола обеспечивают высокий уровень безопасности при правильной настройке. Однако существуют важные различия в их подходах. IPsec предоставляет надежную защиту на сетевом уровне, используя проверенные временем механизмы шифрования [10]. Протокол поддерживает множество криптографических алгоритмов, включая AES-GCM, ChaCha20-Poly1305 и различные методы аутентификации [2]. Однако сложность конфигурации IPsec

может приводить к ошибкам, снижающим уровень безопасности [9]. OpenVPN, основанный на SSL/TLS, обеспечивает надежную защиту при использовании актуальных версий библиотеки OpenSSL [1]. В 2025 году исследователями были выявлены потенциальные уязвимости, связанные с атаками на начальный вектор инициализации (IV), однако для современных версий протокола разработаны эффективные методы защиты [3]. Основным преимуществом OpenVPN является возможность тонкой настройки параметров безопасности [5]. WireGuard отличается минималистичным дизайном и использованием только современных, проверенных криптографических примитивов [4]. Малый объем кода значительно снижает вероятность наличия необнаруженных уязвимостей [8]. Отсутствие необходимости в управлении сертификатами также упрощает безопасное развертывание [5]. Однако некоторые эксперты отмечают, что ограниченный набор криптографических алгоритмов может стать недостатком в случае обнаружения уязвимости в одном из них [4].

2. Производительность. Производительность VPN-протоколов критически важна для обеспечения комфортной работы пользователей и эффективной передачи данных. IPsec демонстрирует хорошую производительность благодаря работе на сетевом уровне и встроенной поддержке в ядре операционной системы [2]. При использовании аппаратного ускорения шифрования IPsec способен обеспечивать высокую пропускную способность, что делает его предпочтительным для site-to-site соединений [5]. OpenVPN традиционно считается наименее производительным среди рассматриваемых протоколов [5]. Это связано с тем, что он работает в пользовательском пространстве, что требует дополнительных копирований данных между ядром и пользовательским режимом [9]. Двойное шифрование (на уровне TLS и на уровне туннеля) также увеличивает вычислительную нагрузку на процессор [1]. WireGuard признан лидером по производительности [5]. Работа в ядре Linux в сочетании с оптимизированными алгоритмами шифрования позволяет достигать более высокой скорости передачи данных при меньшей задержке по сравнению с конкурентами [4]. Статистический характер протокола (отсутствие необходимости поддерживать постоянное состояние соединения) также положительно влияет на производительность [8].

3. Удобство настройки и эксплуатации. Сложность настройки VPN напрямую влияет на вероятность ошибок конфигурации и время развертывания. IPsec считается наиболее сложным в настройке протоколом [9]. Администратору необходимо определить политики шифрования, настроить обмен ключами, маршрутизацию и правила межсетевого экрана [2]. В больших корпоративных сетях это требует высокой квалификации специалистов [5]. OpenVPN предлагает баланс между гибкостью и сложностью. Настройка осуществляется через конфигурационные файлы и не требует глубокого понимания работы протоколов безопасности [1]. Наличие готовых шаблонов и скриптов упрощает развертывание [9]. Однако использование стороннего клиентского ПО может создавать дополнительные сложности [5]. WireGuard отличается максимальной простотой [4]. Для настройки требуется всего несколько строк конфигурации: указать приватный ключ, порт и список пиров с их публичными ключами и IP-адресами [8]. Отсутствие необходимости в управлении сертификатами и сложных протоколах обмена ключами делает WireGuard доступным даже для начинающих администраторов [5].

4. Совместимость и обход ограничений. Возможность работы в различных сетевых условиях критична для удаленного доступа.

IPsec может испытывать трудности при работе через NAT (трансляцию сетевых адресов) из-за использования фиксированных портов и протоколов [2]. Хотя современные реализации поддерживают NAT-Traversal, это добавляет сложности в настройку [10]. OpenVPN обладает наилучшей способностью обходить сетевые ограничения [9]. Возможность использования TCP-порта 443 позволяет маскировать VPN-трафик под обычный HTTPS, что делает его практически неотличимым для систем глубокого анализа трафика [1]. WireGuard использует только UDP и фиксированный порт (по умолчанию 51820), что может создавать проблемы в сетях с жесткими политиками фаервола [5]. Однако благодаря своей простоте и современной архитектуре, WireGuard успешно работает через NAT в большинстве случаев [4]. Сводные результаты сравнительного анализа представлены в таблице 1.

Таблица 1 – Сравнение характеристик протоколов VPN

Критерий	IPsec	OpenVPN	WireGuard
Уровень работы	Сетевой	Прикладной	Сетевой
Криптография	AES, ChaCha20 и др. [2]	AES, ChaCha20 и др. [2]	ChaCha20, Poly1305, Curve25519 (фиксированный набор) [4]
Производительность	Высокая [5]	Средняя [9]	Очень высокая [4]
Сложность настройки	Высокая [9]	Средняя [5]	Низкая [8]
Обход NAT/фаерволов	Средний [10]	Отличный [1]	Хороший [4]
Поддержка платформ	Встроенная во все ОС [2]	Требуется сторонний клиент [5]	Встроена в ядро Linux, клиенты для всех ОС [4]
Размер кодовой базы	Крупный	Крупный	Малый (~4000 строк) [8]

Заключение

Проведенный сравнительный анализ позволяет сделать вывод, что выбор протокола VPN зависит от конкретных требований и условий эксплуатации.

IPsec остается оптимальным выбором для корпоративных site-to-site соединений, где требуется надежность, стандартизация и встроенная поддержка в сетевом оборудовании [2]. Несмотря на сложность настройки, этот протокол предоставляет все необходимые механизмы для построения защищенных каналов между офисами и дата-центрами [5].

OpenVPN является универсальным решением, особенно подходящим для удаленного доступа в условиях строгих сетевых ограничений [9]. Возможность работы через порт 443 делает его незаменимым в странах с жесткой интернет-цензурой или в корпоративных сетях с ограниченным выходом в интернет [1].

WireGuard представляет собой будущее VPN-технологий [4]. Сочетание высокой производительности, современных криптографических алгоритмов и простоты настройки делает его лучшим выбором для большинства современных сценариев использования, особенно в облачных и IoT-средах [5]. Ожидается, что с расширением поддержки WireGuard в различных операционных системах и сетевых устройствах его популярность будет только расти [8].

Рекомендуется использовать WireGuard для новых проектов, требующих высокой производительности и простоты развертывания, OpenVPN – для обхода строгих сетевых ограничений, а IPsec – в корпоративных средах с существующей инфраструктурой, построенной на этом протоколе [5].

Список использованных источников:

- 1 noBGP. Compare VPN Protocols and an Alternative [Электронный ресурс]. – 2025. – Режим доступа: <https://www.nobgp.com/info/compare-vpn-protocols>. – Дата доступа: 21.03.2026.
- 2 Libreswan Project. Implemented Standards: IKE and IPsec RFCs [Электронный ресурс]. – 2025. – Режим доступа: https://libreswan.org/wiki/Implemented_Standards. – Дата доступа: 21.03.2026.
- 3 IETF. RFC 4301: Security Architecture for the Internet Protocol [Электронный ресурс]. – 2005. – Режим доступа: <https://datatracker.ietf.org/doc/html/rfc4301>. – Дата доступа: 21.03.2026.
- 4 IETF. RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2) [Электронный ресурс]. – 2014. – Режим доступа: <https://datatracker.ietf.org/doc/html/rfc7296>. – Дата доступа: 21.03.2026.
- 5 Telnyx. The Best VPN for IoT Security: OpenVPN vs. IPsec vs. WireGuard [Электронный ресурс]. – 2025. – Режим доступа: <https://telnyx.com/resources/ipsec-vs-openvpn-vs-wireguard>. – Дата доступа: 21.03.2026.
- 6 OpenVPN Inc. OpenVPN Reference Manual [Электронный ресурс]. – 2024. – Режим доступа: <https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/>. – Дата доступа: 21.03.2026.
- 7 WireGuard LLC. WireGuard Documentation [Электронный ресурс]. – 2025. – Режим доступа: <https://www.wireguard.com/documentation/>. – Дата доступа: 21.03.2026.
- 8 Donenfeld J.A. WireGuard: Next Generation Kernel Network Tunnel // Proceedings of the 2017 Network and Distributed System Security Symposium (NDSS). – San Diego, 2017. – P. 1-12.
- 9 OpenVPN Security Overview. OpenVPN Security Architecture [Электронный ресурс]. – 2024. – Режим доступа: <https://openvpn.net/security-overview/>. – Дата доступа: 21.03.2026.
- 10 WireGuard Security Audit. WireGuard Formal Verification and Security Audit Report [Электронный ресурс]. – 2020. – Режим доступа: <https://www.wireguard.com/audit/>. – Дата доступа: 21.03.2026.

UDC 004.056

COMPARATIVE ANALYSIS OF VPN PROTOCOLS (IPSEC VS OPENVPN VS WIREGUARD) FOR SECURE DATA TRANSMISSION

Purus A.O., Golubev A.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Chepikova V.V. – senior lecturer

Annotation. The paper presents a comparative analysis of three main virtual private network protocols: IPsec, OpenVPN and WireGuard. The features of their architecture, encryption mechanisms, performance and ease of configuration are considered. The strengths and weaknesses of each protocol are identified, as well as recommendations for their use in various usage scenarios.

Keywords. VPN, IPsec, OpenVPN, WireGuard, data security, protocol comparison, encryption, performance.

ЭТИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАНИИ

Масейчик Е.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пилушко А.А. – научн. рук, канд. техн. наук, доцент

Аннотация. В данном ответе рассматриваются этические проблемы, обусловленные внедрением систем искусственного интеллекта в современный образовательный процесс.

Ключевые слова. Искусственный интеллект, образовательный процесс, гуманистические ценности.

Искусственный интеллект не является нейтральным инструментом: его применение формирует новые социальные практики, влияет на когнитивные стратегии и изменяет характер взаимодействия между человеком и технологией. В этих условиях возрастает значение этики искусственного интеллекта как системы принципов, регулирующих разработку и использование алгоритмических решений в образовательном процессе.

В основе этики искусственного интеллекта лежат следующие нормативные принципы: принцип справедливости, принцип прозрачности, принцип подотчетности, принцип приоритета человека, принцип защиты персональных данных [1], [2].

Применение искусственного интеллекта в образовательном процессе сопровождается комплексом взаимосвязанных этических проблем.

К основным относятся:

- трансформация академической добросовестности;
- риск алгоритмической дискриминации;
- угроза конфиденциальности данных;
- смещение роли преподавателя;
- зависимость обучающихся от алгоритмов;
- непрозрачность решений;
- коммерциализация образовательной среды.

Данные вызовы требуют системного регулирования и разработки комплексных этических стандартов, обеспечивающих баланс между технологическим развитием и сохранением гуманистических оснований образования.

Перспективным направлением является внедрение принципов этического проектирования при разработке образовательных платформ.

Этическое проектирование предполагает: прозрачность логики алгоритмов, возможность объяснения результатов, наличие человеческого контроля; минимизацию сбора персональных данных; защиту информации от несанкционированного доступа.

Данные требования направлены на формирование доверия к цифровым инструментам и обеспечение их соответствия гуманистическим ценностям образования [3].

Перспективный анализ позволяет выделить несколько ключевых тенденций: усиление регулирования генеративных технологий, внедрение механизмов алгоритмического аудита, расширение программ цифровой грамотности, интеграция этики искусственного интеллекта в образовательные стандарты, развитие гибридных моделей обучения, сочетающих цифровые и традиционные формы.

Данные тенденции отражают стремление обеспечить устойчивое развитие образовательного процесса в условиях технологической трансформации.

Таким образом, гармоничное внедрение искусственного интеллекта в образование возможно при соблюдении баланса между инновационным развитием и сохранением гуманистических ценностей. Этические принципы приоритета человека, справедливости, прозрачности и ответственности должны стать основой цифровой трансформации образовательного процесса. Реализация данных принципов обеспечивает не только технологическую эффективность, но и сохранение сущностного назначения образования как процесса формирования личности и развития критического мышления.

Список литературы:

1. А. И. Минаков. Искусственный интеллект и нейросети в образовании. // учебник. – 2024. – URL: https://dksta.ru/ff/iskusstvennyj_intellekt.pdf – (дата обращения: 17.03.2026).
2. А. Я. Рыженков. Организационно-правовые и этические аспекты использования искусственного интеллекта // Law and Order DonSTU. – 2025. – URL: <https://www.lawandorder-donstu.ru/jour/article/view/84/0> – (дата обращения: 17.03.2026).
3. А. В. Ильина, Ю. Ю. Калинина [и др.] Этические аспекты использования искусственного интеллекта в образовательной сфере // GIEF Journal.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОВОДНЫХ, БЕСПРОВОДНЫХ И ЯЧЕИСТЫХ СЕТЕЙ

Бродович Б.Е.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лагутин А.Е. – канд. тех. наук, доцент

В работе проведен сравнительный анализ архитектур проводных, беспроводных и ячеистых сетей. Рассмотрены преимущества и недостатки каждого типа передачи данных. Особое внимание уделено перспективам развития ячеистых топологий в условиях Интернета вещей. Выявлено, что гибридные решения обеспечивают наилучшую отказоустойчивость.

Современные телекоммуникационные системы требуют гибкого подхода к организации сетевой инфраструктуры. Традиционно выделяют проводные и беспроводные технологии [1]. Проводные сети обеспечивают высокую стабильность и скорость, однако ограничивают мобильность узлов. Беспроводные сети решают проблему мобильности, но подвержены интерференции и затуханию сигнала.

Для оценки пропускной способности канала используется формула Шеннона:

$$C = B \cdot \log_2(1 + S/N) \quad (1),$$

где C – пропускная канала, бит/с; B – ширина полосы, Гц; S/N – отношение сигнал/шум.

Ячеистые сети (Mesh) представляют собой топологию с динамической связью между узлами, где каждое устройство может выступать как в роли конечного пункта, так и ретранслятора данных. Ключевое преимущество такой архитектуры – способность к самоорганизации и автоматическому восстановлению маршрута при отказе отдельных узлов, что обеспечивает высокую отказоустойчивость системы.

Для оценки качества канала в Mesh-сетях применяется метрика:

где LQI – индикатор качества связи; RSSI – уровень принимаемого сигнала; SNR – отношение сигнал/шум.

В зависимости от назначения выделяют три типа узлов:

- Router – участвует в маршрутизации трафика;
- End Device – конечное устройство с минимальным энергопотреблением;
- Border Router – обеспечивает связь Mesh-сети с внешними инфраструктурами.

Преимущества Mesh-топологий включают масштабируемость, отсутствие единой точки отказа и гибкость развёртывания. Ограничениями являются возможный рост задержки при многоузловой маршрутизации и повышенные требования к ресурсам устройств.

Таким образом, ячеистые сети являются оптимальным решением для распределённых систем Интернета вещей, где важны надёжность связи и энергоэффективность

Таблица 1 – Сравнительная характеристика сетей

№п/п	Тип сети	Скорость	Надёжность
1	Проводная	Высокая	Высокая
2	Беспроводная	Средняя	Средняя
3	Ячеистая	Зависит от узла	Высокая

Таким образом, выбор технологии зависит от конкретных задач развёртывания. Для стационарных объектов предпочтительны проводные решения, для мобильных – беспроводные, а для распределённых систем IoT – ячеистые структуры [3].

Список использованных источников:

1. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. пособие / В.Г. Олифер, Н.А. Олифер. – СПб. : Питер, 2016. – 992 с..
2. Wireless Mesh Networks: A Survey / I.F. Akyildiz [et al.] // Computer Networks, 2005. – P. 445-487.
3. Интернет вещей: архитектура и протоколы / А.В. Смирнов [и др.] // Вестник БГУИР, 2020. – С. 15-22.

СОВРЕМЕННЫЕ МНОГОКАНАЛЬНЫЕ ПРИЕМНИКИ СВЧ-ДИАПАЗОНА: КЛАССИФИКАЦИЯ И ОБЛАСТИ ПРИМЕНЕНИЯ

Шапошникова Н.П.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гусинский А.В. – д-р техн. наук, профессор

В статье рассматриваются современные многоканальные приемники СВЧ-диапазона 1–20 ГГц. Приведена классификация устройств по способу построения (параллельные, сканирующие, матричные) и назначению (измерительные, поисковые, разведывательные). Описана типовая структура, включающая узлы опорного генератора, гетеродина, синтезатора, переноса частоты и предварительного усиления. Определены основные области применения: радиомониторинг, радиотехническая разведка и измерительные системы.

Многоканальные приемные устройства (МПУ) являются основой современных радиотехнических измерительных систем, используемых в радиомониторинге и радиотехнической разведке. Эффективность решения задач обнаружения и измерения параметров радиосигналов напрямую зависит от технического уровня и метрологического обеспечения МПУ. Диапазон частот 1–20 ГГц представляет наибольший интерес в связи с насыщенностью этого диапазона средствами связи, радиолокации и навигации.

По способу построения МПУ подразделяются на параллельные (одновременный прием по всем каналам), сканирующие (последовательный опрос каналов) и матричные (комбинированные). По назначению выделяют измерительные, поисковые и разведывательные приемники.

Типовая структура МПУ включает узел опорного генератора (УОГ), узел гетеродина (УГ), узел синтезатора (УС), узел переноса частоты (УПЧ) и узел предварительного усиления (УПУ). Наличие функции определения вида модуляции расширяет функциональные возможности устройства.

Основные области применения МПУ охватывают широкий круг задач, требующих одновременного приема и обработки сигналов в диапазоне 1–20 ГГц. В системах радиомониторинга эти устройства используются для непрерывного контроля радиоэфира с целью выявления несанкционированных излучений, обеспечения электромагнитной совместимости (ЭМС) и поддержания работоспособности сетей связи. Благодаря многоканальной структуре, такие приемники позволяют одновременно вести наблюдение за несколькими частотными каналами, что критически важно для оперативного обнаружения кратковременных сигналов и помех. В сфере радиотехнической разведки многоканальные приемники выступают в качестве ключевого элемента станций перехвата и пеленгации. Их применение направлено на сбор и анализ информации об источниках радиоизлучения (РЛС, станции активных помех, системы навигации и связи противника) в условиях плотной и сложной сигнальной обстановки. Параллельные и матричные архитектуры МПУ обеспечивают здесь высокую вероятность обнаружения сигналов с псевдослучайной перестройкой рабочей частоты (ППРЧ) и позволяют вести точное определение угловых координат (пеленгование) источников в реальном масштабе времени. Отдельную нишу занимают измерительные системы – анализаторы спектра, векторные анализаторы цепей и специализированные измерительные комплексы. В них МПУ применяются для прецизионного определения параметров сигналов (несущая частота, уровень мощности, вид модуляции, фазовые шумы) с высокой метрологической достоверностью. Использование многоканальной структуры в таких системах позволяет реализовывать корреляционные методы измерений, существенно повышающие динамический диапазон и чувствительность по сравнению с одноканальными решениями. Таким образом, выбор конкретного типа МПУ – измерительного, поискового или разведывательного – напрямую диктуется спецификой решаемых задач, требуемой скоростью обзора частотного диапазона и необходимыми метрологическими характеристиками.

Заключение. Современные МПУ представляют собой сложные многоканальные системы с высокой степенью интеграции узлов. Для обеспечения достоверности результатов измерений необходим метрологический контроль каждого узла (УОГ, УГ, УС, УПЧ, УПУ) с использованием обоснованных методов и средств измерений. Полученные результаты обосновывают актуальность разработки специализированных методик исследования метрологических характеристик МПУ.

Список использованных источников:

1. Фомин, Н.Н., Бугаев, А.В. Радиоприемные устройства. – М.: Горячая линия – Телеком, 2022. – 320 с.
2. Дворяшин, Б.В. Основы метрологии и радиоизмерения. – М.: Радиотехника, 2021. – 320 с.
3. Боев С.Ф. Радиофотонный приемный канал СВЧ диапазона с оптическим гетеродинированием // Журнал радиоэлектроники. – 2015. – №2.

МЕТОДЫ ОПТИМИЗАЦИИ АГРЕГАЦИИ СОБЫТИЙ В СИСТЕМАХ REAL-TIME BIDDING ПРИ ВЫСОКИХ НАГРУЗКАХ

Анциферова Е.И., магистрант гр.467041

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Давыдова Н.С. – канд. тех. наук, доцент

Аннотация. В работе представлен аналитический обзор методов оптимизации агрегации событий в системах Real-Time Bidding в условиях высоких нагрузок. Рассматриваются структурные особенности RTB-логов и ключевые проблемы их обработки, обусловленные высокой интенсивностью поступления и значительными объемами данных. Систематизированы современные подходы к агрегации, включая потоковую обработку, методы предварительной агрегации и применение колоночных хранилищ данных. Проведён сравнительный анализ преимуществ и ограничений рассматриваемых решений. Полученные результаты могут быть использованы при проектировании масштабируемых систем обработки данных в рекламных платформах.

Ключевые слова. Real-Time Bidding, RTB-логи, агрегация событий, потоковая обработка данных, предварительная агрегация, колоночные базы данных, ClickHouse, Apache Kafka, высоконагруженные системы, масштабируемость, аналитика данных.

Современный рынок цифровой рекламы характеризуется стремительным ростом объемов обрабатываемых данных и повышением требований к скорости принятия решений. Системы Real-Time Bidding (RTB), обеспечивающие программную закупку рекламных мест в режиме реального времени, генерируют десятки миллионов событий в секунду, что создаёт значительные вызовы для инфраструктуры обработки и анализа данных. Согласно отчётам аналитических агентств, глобальный объём транзакций в RTB-экосистеме превысил 500 миллиардов запросов в сутки, при этом средняя задержка на обработку одного запроса не должна превышать 100 миллисекунд [1].

В условиях таких нагрузок традиционные методы агрегации и аналитики данных оказываются неэффективными, что обуславливает необходимость разработки и применения специализированных подходов к оптимизации обработки событий.

Ключевой задачей RTB-платформ является агрегация разнородных событий – показов (impressions), кликов (clicks), конверсий (conversions) и биддинговых запросов – с целью формирования аналитических метрик в режиме, близком к реальному времени.

При этом система должна обеспечивать не только высокую пропускную способность, но и точность расчётов, масштабируемость и отказоустойчивость. Актуальность исследования определяется следующими факторами:

- Экспоненциальный рост объемов данных. Количество рекламных запросов увеличивается на 40–50% ежегодно, что требует постоянной модернизации систем обработки.
- Жёсткие требования к задержкам. Рекламодатели и аналитики нуждаются в оперативном доступе к метрикам эффективности кампаний для принятия управленческих решений.
- Сложность архитектур. Гетерогенность источников данных, распределённая природа систем и необходимость обеспечения консистентности данных усложняют проектирование решений.
- Экономическая эффективность. Оптимизация процессов агрегации напрямую влияет на инфраструктурные затраты платформ.

Real-Time Bidding представляет собой автоматизированную систему программной закупки рекламы, функционирующую на основе аукционных механизмов в режиме реального времени. Типичная RTB-экосистема включает ряд ключевых компонентов [2], среди которых SSP (платформа на стороне издателя), DSP (платформа на стороне рекламодателя), рекламная биржа (Ad Exchange), координирующая процесс торгов, а также DMP, обеспечивающая управление данными для таргетинга.

Процесс обработки рекламного запроса включает последовательность этапов, начиная с формирования запроса на участие в аукционе (bid request), содержащего информацию о пользователе и контексте. Далее DSP-платформы формируют и отправляют ставки, после чего проводится аукцион, чаще всего по модели second-price auction, определяется победитель и осуществляется показ рекламного объявления. В случае взаимодействия пользователя фиксируются события клика и конверсии. Существенным ограничением является требование к времени обработки: полный цикл должен укладываться в 100–120 миллисекунд.

RTB-системы генерируют различные типы событий, включая запросы на участие в аукционе, ставки, показы, клики и конверсии [1]. Эти события отличаются как по частоте возникновения, так и по объёму и структуре данных. Наиболее массовыми являются bid requests и ставки, достигающие миллионов событий в секунду, тогда как клики и конверсии происходят значительно реже, но обладают высокой ценностью с точки зрения аналитики. Каждое событие содержит набор атрибутов,

таких как идентификаторы пользователей, параметры рекламных кампаний, временные метки и контекст размещения.

Данные, формируемые в RTB-системах, характеризуются значительными объемами, высокой скоростью поступления и разнообразием форматов. Объем логов может достигать десятков или сотен терабайт в сутки, а в крупных системах – вплоть до петабайтных масштабов. Поток событий отличается неравномерностью нагрузки, обусловленной временными факторами, а сами данные имеют множество версий схем. Дополнительную сложность представляет временная специфика обработки: события могут поступать с задержкой, нарушать хронологический порядок и требовать учета как времени генерации, так и времени обработки. Кроме того, данные между различными типами событий связаны, что требует выполнения операций объединения и построения пользовательских сессий.

Указанные особенности определяют высокие требования к системам агрегации данных. Такие системы должны обеспечивать обработку миллионов событий в секунду при минимальной задержке формирования аналитических показателей. Важным аспектом является точность вычислений в условиях неполных и запаздывающих данных, а также способность системы масштабироваться с ростом нагрузки. Не менее значимыми являются требования отказоустойчивости и поддержки гибких аналитических запросов. Совокупность этих факторов обуславливает необходимость применения специализированных методов оптимизации агрегации, рассматриваемых в дальнейшем.

Одной из центральных проблем агрегации RTB-событий является обеспечение минимальных задержек между моментом возникновения события и его отражением в агрегированных метриках. Анализ показывает, что задержка складывается из нескольких компонентов:

$$T_{total} = T_{network} + T_{ingestion} + T_{processing} + T_{storage} + T_{query}$$

где $T_{network}$ – задержка передачи данных по сети (10–50 мс), $T_{ingestion}$ – время приёма данных в систему обработки (20–100 мс), $T_{processing}$ – время вычисления агрегатов (100 мс – 10 сек), $T_{storage}$ – запись результатов (50–500 мс), T_{query} – выполнение аналитических запросов (100 мс – 5 сек).

Высокая интенсивность записи событий создает существенную нагрузку на системы хранения данных. При выполнении агрегации непосредственно на уровне базы данных возникает эффект усиления записи (write amplification), при котором обработка каждого события приводит к множественным операциям обновления. Дополнительно наблюдается конкуренция за блокировки (lock contention), обусловленная параллельным обновлением агрегатов, что снижает общую производительность системы. Существенное влияние оказывает и необходимость поддержания индексов для выполнения многомерных аналитических запросов, что увеличивает стоимость операций записи в несколько раз.

Вертикальное масштабирование, предполагающее увеличение мощности отдельных серверов, ограничено физическими возможностями оборудования и сопровождается нелинейным ростом стоимости. Горизонтальное масштабирование через шардинг или партиционирование сталкивается с рядом проблем: выполнение кросс-партиционных запросов требует координации между узлами, данные распределяются неравномерно (data skew), когда отдельные кампании генерируют значительно больше событий, а перераспределение данных при добавлении новых узлов создает дополнительные накладные расходы. Кроме того, точность агрегатов усложняется из-за поступления событий вне хронологического порядка (out-of-order events), что требует ретроактивных корректировок и создает компромисс между полнотой данных и актуальностью метрик.

Потоковая обработка данных основана на концепции непрерывной обработки событий по мере их поступления, в противовес традиционной пакетной обработке накопленных данных. Формально, поток событий можно представить как бесконечную последовательность:

$$S = \{e_1, e_2, e_3, \dots, e_n, \dots\},$$

где каждое событие $e_i = (\text{key}, \text{value}, \text{timestamp})$.

Агрегация в потоковой модели выполняется инкрементально:

$$A_t = f(A_{t-1}, e_t),$$

где A_t – состояние агрегата в момент t , f – функция обновления.

Далее представлены современные технологические платформы для потоковой обработки данных, широко применяемые в системах Real-Time Bidding, с анализом их возможностей по обеспечению высокой производительности, низкой задержки и масштабируемости.

Apache Kafka представляет собой клиентскую библиотеку для создания распределённых потоковых приложений. Она поддерживает stateful processing через RocksDB, гарантирует идемпотентность операций при сбоях и позволяет строить обработку данных в виде

топологий «источник → процессор → приёмник». Производительность при простой агрегации может достигать до 10^6 событий в секунду на узел.

Apache Flink обеспечивает низколатентную обработку с поддержкой семантики event-time, включая механизмы Watermarks для отслеживания времени событий, гибкое управление состояниями через различные backend'ы и асинхронное создание снимков состояния для восстановления. Flink эффективно обрабатывает события вне хронологического порядка с задержкой менее 100 мс.

Apache Spark Streaming использует микробатчинговый подход и абстракцию непрерывной таблицы. Задержка обработки варьируется от 100 мс в режиме continuous до нескольких секунд в micro-batch режиме, при этом обеспечивается высокая пропускная способность потоков данных.

Сравнительный анализ технологических платформ расположен в таблице 1.

Таблица 1 – Сравнение параметров технологических платформ

Платформа	Задержка	Пропускная способность	Управление состоянием	Сложность
Kafka Streams	10–100 мс	10^6 /сек/узел	RocksDB	Низкая
Flink	5–50 мс	10^6 /сек/узел	Flexible	Средняя
Spark Streaming	100 мс – 5 сек	10^7 /сек/кластер	In-memory/RDD	Средняя

Потоковая обработка обеспечивает непрерывное вычисление агрегатов по мере поступления событий, что позволяет минимизировать задержки и оперативно получать аналитические показатели. Каждое событие рассматривается как элемент бесконечной последовательности, а агрегаты обновляются инкрементально, что исключает необходимость ожидания полного набора данных. Этот подход позволяет обрабатывать миллионы событий в секунду и обеспечивает поддержку out-of-order событий, что критично для точности аналитики.

Предварительная агрегация заключается в раннем сворачивании данных на этапе их поступления. Суть метода состоит в том, чтобы на уровне edge-узлов или промежуточных сервисов формировать частичные агрегаты, которые затем передаются в центральное хранилище. Это позволяет значительно уменьшить объём передаваемых данных и снизить нагрузку на основную систему агрегации. Для повышения эффективности предварительной агрегации применяются иерархические структуры, в которых данные агрегируются сначала по секундам, затем по минутам, часам и дням. Такой подход обеспечивает возможность выполнения запросов различной временной глубины без необходимости пересчёта всех событий с нуля.

Использование оконных функций позволяет формировать агрегаты за фиксированные временные интервалы или по сессиям пользователей. В RTB-системах применяются непересекающиеся окна, скользящие окна и динамические сессионные окна, что обеспечивает гибкость при вычислении показателей в реальном времени. Особое внимание уделяется обработке опоздавших событий, когда события поступают не в хронологическом порядке. Для этого применяются механизмы отслеживания времени событий, допускаются периоды задержки обработки и реализуются стратегии ретроактивного пересчёта агрегатов, что позволяет поддерживать баланс между полнотой данных и оперативностью метрик.

Колоночные базы данных являются эффективным инструментом для аналитики больших потоков данных. В отличие от традиционных строковых СУБД, данные хранятся по столбцам, что улучшает компрессию, снижает объём считываемых данных и ускоряет выполнение запросов. Среди популярных решений для RTB-систем выделяются ClickHouse, Druid, BigQuery и Amazon Redshift. Они обеспечивают высокую пропускную способность вставки данных, поддержку распределённых вычислений и эффективную обработку аналитических запросов с минимальными задержками. Важным элементом является возможность использования материализованных представлений и агрегатных кубов, что позволяет заранее вычислять ключевые показатели и уменьшать время отклика на запросы аналитиков.

Для обеспечения масштабируемости и равномерного распределения нагрузки применяется партиционирование и шардирование данных. Временное партиционирование позволяет разделять данные по дням, неделям или месяцам, что упрощает архивирование и ускоряет выборку по времени. Хеш-шардирование распределяет данные между узлами на основе ключей, что позволяет минимизировать узкие места при высоких нагрузках. Гибридные стратегии, сочетающие временное и хеш-шардирование, позволяют обеспечить баланс между эффективностью хранения и быстродействием запросов. Кроме того, динамическое создание и поддержка партиций позволяет адаптировать систему к растущим объёмам данных без остановки работы платформы.

Применение описанных методов в комплексе позволяет RTB-системам достигать высокой пропускной способности, минимальных задержек при агрегации событий и точности аналитических показателей, что обеспечивает поддержку оперативного принятия решений в условиях высоких нагрузок.

В работе рассмотрены ключевые методы оптимизации агрегации событий в системах Real-Time Bidding при высоких нагрузках. Проведённый анализ показал, что традиционные подходы к обработке

данных оказываются недостаточно эффективными для обеспечения минимальных задержек и высокой пропускной способности в условиях миллионов событий в секунду.

Потоковая обработка данных позволяет обрабатывать события непрерывно, обеспечивая низкую латентность и поддержку событий вне хронологического порядка. Предварительная агрегация и использование материализованных представлений позволяют существенно снизить нагрузку на центральные хранилища и ускорить формирование аналитических метрик. Применение колоночных баз данных, а также партиционирование и шардирование данных обеспечивает масштабируемость системы и эффективность выполнения многомерных запросов.

Комплексное использование перечисленных подходов позволяет RTB-платформам достигать баланса между точностью вычислений, скоростью обработки и экономической эффективностью инфраструктуры. Полученные результаты могут быть использованы при проектировании и развитии высоконагруженных систем обработки данных в цифровой рекламе, а также служат основой для дальнейших исследований в области оптимизации агрегации потоковых событий.

Список использованных источников:

1. Zhu, F., & Iyer, B. *Intermediation in Electronic Marketplaces: A Case of Real - Time Bidding*. Information Systems Research, 2018.
2. Hill, S., & Fulgoni, G. *RTB Is Not Enough: Understanding the Role of Consumer Data in Digital Advertising*. Journal of Advertising Research, 2015.

UDC 005.591.1

METHODS FOR OPTIMIZING EVENT AGGREGATION IN REAL-TIME BIDDING SYSTEMS UNDER HIGH LOADS

Antsiferova E.I.

*Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus*

Davydova N.S. –PhD in Engineering, Associate Professor

Abstract. This paper presents an analytical review of methods for optimizing event aggregation in Real-Time Bidding systems under high loads. It examines the structural features of RTB logs and key processing challenges associated with high incoming data and significant volumes. It systematizes modern aggregation approaches, including stream processing, pre-aggregation methods, and the use of columnar data warehouses. A comparative analysis of the advantages and limitations of the solutions under consideration is provided. The results can be used in the design of scalable data processing systems for advertising platforms.

Keywords: Real-Time Bidding, RTB logs, event aggregation, streaming data processing, pre-aggregation, columnar databases, ClickHouse, Apache Kafka, high-load systems, scalability, data analytics

УДК 621.396.4

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАТУХАНИЯ СИГНАЛА В ГЕТЕРОГЕННЫХ СЕТЯХ СОТОВОЙ СВЯЗИ НА ОСНОВЕ ИЗМЕРЕНИЙ RSSI В ГОРОДСКИХ УСЛОВИЯХ МИНСКА

Родионов М.А., магистрант гр.467041

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Аксенов В.А. – старший преподаватель,

Астровский И.И. – кандидат технических наук, доцент

Аннотация. В работе представлены результаты практических измерений уровня принимаемого сигнала (RSSI) в сетях LTE г. Минска. Измерения выполнены в 64 точках трёх характерных локаций с различной плотностью застройки. Расстояния от точек замера до базовых станций рассчитаны по формуле гаверсинусов. Экспериментальные данные сопоставлены с логарифмической моделью затухания; определены коэффициенты затухания n для каждой зоны. Выявлена зависимость качества покрытия от типа городской среды и плотности размещения базовых станций.

Ключевые слова. гетерогенные сети, LTE, RSSI, затухание сигнала, формула гаверсинусов, коэффициент затухания, планирование сетей связи, многолучевое распространение, хэндовер, городская среда, практические измерения, качество сигнала.

Введение

Стремительный рост объёмов мобильного трафика и ужесточение требований к качеству обслуживания обуславливают необходимость постоянного совершенствования инфраструктуры сотовой связи. Согласно прогнозам 3GPP, глобальный мобильный трафик ежегодно возрастает более чем на 40 %, что требует существенного увеличения плотности сетевой инфраструктуры [1]. Современные сети мобильной связи строятся по гетерогенному принципу (HetNet): они объединяют макросоты, микросоты и пикосоты, работающие в различных частотных диапазонах и образующие перекрывающиеся зоны покрытия [2].

Эффективное планирование HetNet невозможно без точных моделей распространения радиоволн, верифицированных на реальных данных. Классические модели – Hata-COST 231, ITU-R P.1411 и 3GPP TR 38.901 – описывают средние потери пути в типовых городских условиях, однако их применимость к конкретным районам требует экспериментальной проверки [3, 4].

Целью настоящей работы является верификация логарифмической модели затухания сигнала и определение эмпирических коэффициентов затухания для трёх типологически различных локаций г. Минска на основе практических измерений RSSI в сети LTE.

Для достижения цели решены следующие задачи: сбор данных RSSI в 64 точках трёх локаций; расчёт расстояний между точками замера и базовыми станциями; статистический анализ данных; оценка коэффициентов затухания методом наименьших квадратов; сравнение с теоретическими значениями по ITU-R P.1411 и 3GPP TR 38.901.

Методика исследования

Полевые измерения проводились с использованием смартфона с установленным приложением Network Cell Info (Android), которое обеспечивает доступ к параметрам Radio Interface Layer (RIL): идентификатору соты (CID), уровню принимаемого сигнала RSSI (дБм) и географическим координатам. Для повышения достоверности в каждой точке выполнялось три последовательных измерения с последующим усреднением, что позволяет снизить влияние быстрых замираний Рэлея [5].

Исследование охватило три характерные локации г. Минска, различающиеся типом застройки и функциональным назначением. На проспекте Дзержинского собрано 22 точки измерений (жилая многоэтажная застройка, базовая станция CID 17926). В районе Ботанического сада – 14 точек (открытая парковая зона с густой древесной растительностью, CID 17920). На проспекте Независимости – 28 точек (плотная смешанная застройка, зафиксировано переключение между пятью сотами: CID 17949, 17924, 17923, 17971, 26843). Общее количество точек измерений составило 64.

Для расчёта геодезического расстояния между точкой замера и антенной базовой станции применялась формула гаверсинусов [6]:

$$d = 2 \cdot R \cdot \arcsin \left(\sqrt{\sin^2 \left(\frac{\varphi_2 - \varphi_1}{2} \right) + \cos(\varphi_1) \cdot \cos(\varphi_2) \cdot \sin^2 \left(\frac{\lambda_2 - \lambda_1}{2} \right)} \right),$$

где d – расстояние между точками; R – радиус Земли (6371 км); φ_1, λ_1 – широта и долгота антенны; φ_2, λ_2 – широта и долгота точки измерения.

Она обеспечивает погрешность не более 0,3 % при расстояниях до 1 км. На рисунках 1, 2 и 3 приведено расположение антенн и точек замера на карте Минска в районах Парка Челюскинцев, проспекта Независимости и станции метро Петровщина.

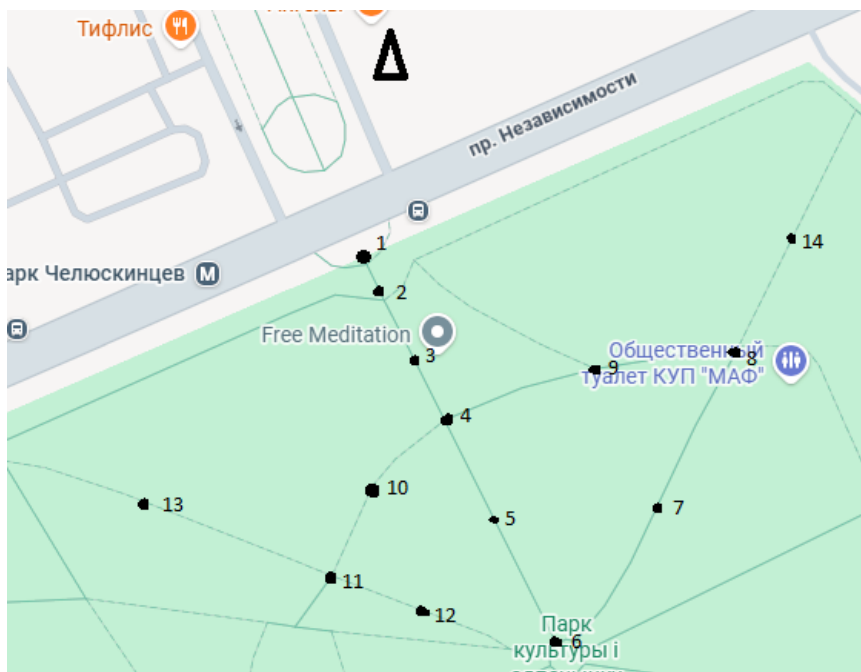


Рисунок 1 – Расположение антенн (▲) и точек замера (●) на карте Парка Челюскинцев

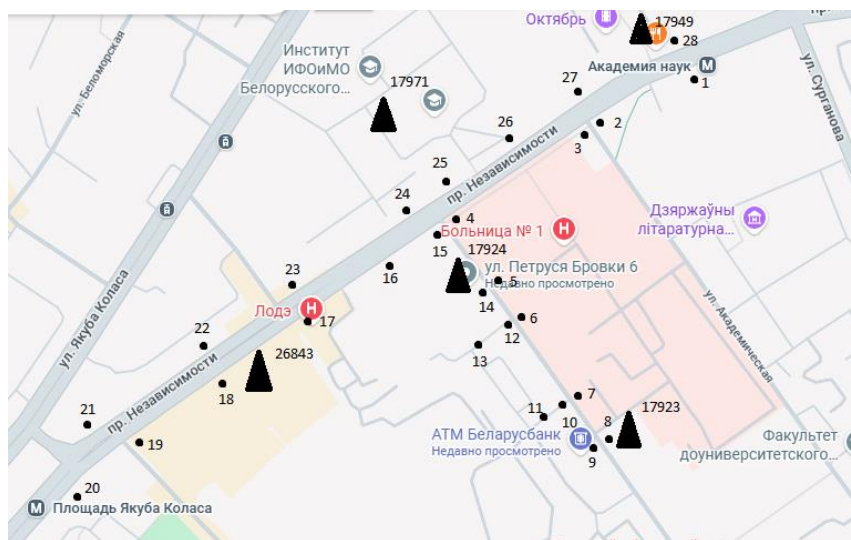


Рисунок 2 - Расположение антенн (▲) и точек замера (●) на карте проспекта Независимости

Для анализа зависимости RSSI от расстояния использована стандартная логарифмическая модель потерь пути [3, 4]:

$$\text{RSSI}(d) = P_0 - 10 \cdot n \cdot \lg\left(\frac{d}{d_0}\right),$$

где P_0 – уровень сигнала на опорном расстоянии $d_0 = 1$ м; n – коэффициент затухания (для свободного пространства $n = 2$; для городской среды $n = 2,5-5,0$ по ITU-R P.1411 [3]).

Параметры P_0 и n определялись методом наименьших квадратов по выборке каждой локации отдельно. Коэффициент детерминации R^2 использовался для оценки адекватности модели.

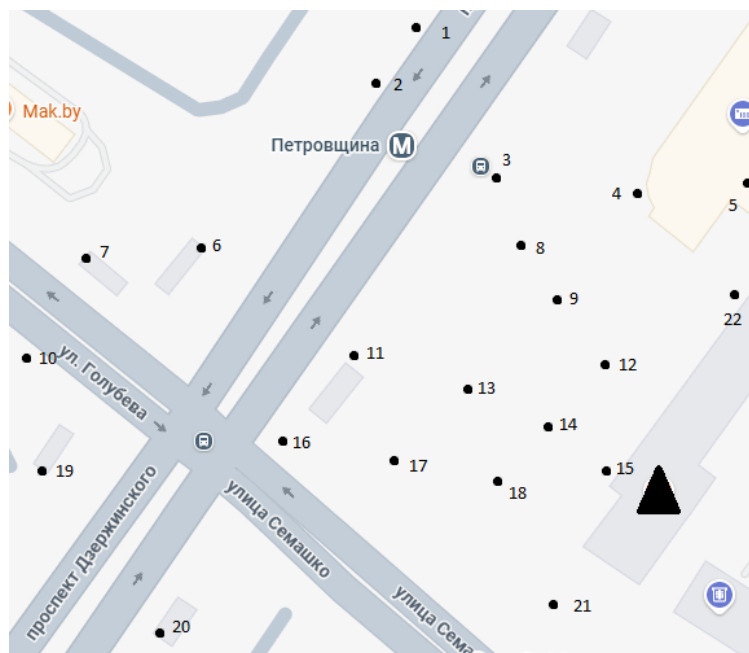


Рисунок 2 - Расположение антенн (▲) и точек замера (●) на карте ст. м. Петровщина

Результаты и обсуждение

По результатам обработки 64 точек измерений получены статистические характеристики уровня сигнала по локациям, приведённые в таблице 1.

Таблица 1 – Статистика измерений параметров сигнала RSSI

Локация	Точек	Среднее, дБм	Min, дБм	Max, дБм	Стд. откл., дБ	Ср. расст., м
Пр. Дзержинского	22	-91,8	-112	-70	14,4	~100
Ботанический сад	14	-92,9	-109	-69	12,5	307
Пр. Независимости	28	-81,7	-102	-66	9,0	~120

Из данных таблицы 1 следует, что лучшее покрытие зафиксировано на проспекте Независимости (средний RSSI -81,7 дБм, $\sigma = 9,0$ дБ). Высокая плотность базовых станций и эффективный хэндовер между пятью сотами обеспечивают стабильный приём: 67,9 % точек имеют уровень «отличный» (-65...-75 дБм) или «хороший» (-75...-85 дБм). Минимальное стандартное отклонение подтверждает равномерность покрытия в этом районе.

На проспекте Дзержинского (средний RSSI -91,8 дБм, $\sigma = 14,4$ дБ) наблюдается наибольший разброс значений. Высокое стандартное отклонение обусловлено чередованием участков с прямой видимостью (LOS) и зонами теневого экранирования (NLOS) плотной жилой застройкой. Доля точек с «отличным» и «хорошим» уровнем составляет 40,9 %.

В Ботаническом саду (средний RSSI -92,9 дБм, среднее расстояние до антенны 307 м) зафиксировано наибольшее удаление от базовой станции и значительное затухание вследствие поглощения сигнала кроной деревьев. Доля критического покрытия (ниже -105 дБм) составляет 21,4 %, что указывает на необходимость установки дополнительных микро- или пикосот.

Коэффициент затухания $n = 2,8$ для Ботанического сада находится в нижней части диапазона ITU-R P.1411 для открытых городских зон, что объясняется относительно свободным распространением сигнала на большей части маршрута. Значимая корреляция ($r = -0,707$, $p < 0,01$, метод Пирсона) свидетельствует о доминирующей роли расстояния в формировании затухания при отсутствии крупных зданий-экранов.

На проспекте Дзержинского и проспекте Независимости корреляция r - d незначима ($p > 0,05$), что обусловлено различными причинами. На Дзержинского резкие перепады RSSI в соседних точках связаны с многолучевым распространением в плотной застройке. На проспекте Независимости хэндовер между пятью сотами устраняет монотонное нарастание потерь с расстоянием, характерное для однотипной модели [2]. Тем не менее значения $n = 3,2$ и $n = 3,5$ хорошо согласуются с рекомендациями 3GPP TR 38.901 для сценария UMa (Urban Macro) [4].

Заключение

В работе проведены практические измерения RSSI в 64 точках трёх локаций г. Минска и выполнен их сравнительный анализ с логарифмической моделью затухания. Установлены закономерности.

В зоне плотной застройки с высокой плотностью базовых станций (пр. Независимости) наблюдается наилучшее покрытие (средний RSSI = -81,7 дБм) при минимальном разбросе ($\sigma = 9,0$ дБ) благодаря эффективному хэндоверу в гетерогенной сети.

В открытой парковой зоне (Ботанический сад) установлена значимая корреляция RSSI с расстоянием ($r = -0,707$, $p < 0,01$), коэффициент затухания $n = 2,8$ соответствует нижней границе диапазона ITU-R P.1411; 21,4 % точек имеют критический уровень покрытия, что требует установки пикосот с интервалом не более 150 м.

В жилой многоэтажной застройке (пр. Дзержинского) значительный разброс ($\sigma = 14,4$ дБ) и слабая корреляция $r-d$ ($p > 0,05$) обусловлены многолучевым распространением; доля удовлетворительного и выше покрытия составляет 40,9 %, что свидетельствует о необходимости оптимизации антенных систем макросоты.

Полученные значения n (2,8–3,5) согласуются с рекомендациями ITU-R P.1411 и 3GPP TR 38.901 для сценариев городской застройки, что подтверждает применимость логарифмической модели как инструмента экспресс-верификации планировочных расчётов.

Результаты работы могут быть использованы операторами сотовой связи для корректировки моделей планирования с учётом локальной специфики городской среды Минска, а также в качестве базы данных для верификации ПО радиосетевого планирования.

Список использованных источников:

1. 3GPP TR 38.901. Study on channel model for frequencies from 0.5 to 100 GHz. – V17.0.0. – 2022. – 105 p.
2. 3GPP TS 36.104. Base Station (BS) radio transmission and reception (LTE). – V17.10.0. – 2023. – 84 p.
3. ITU-R P.1411-10. Propagation data and prediction methods for the planning of short-range outdoor radiocommunication systems. – Geneva : ITU, 2019. – 66 p.
4. Rappaport, T. S. Wireless Communications: Principles and Practice / T. S. Rappaport. – 2nd ed. – Upper Saddle River : Prentice Hall PTR, 2002. – 707 p.
5. Parsons, J. D. The Mobile Radio Propagation Channel / J. D. Parsons. – 2nd ed. – Chichester : Wiley, 2000. – 436 p.
6. Sinnott, R. W. Virtues of the Haversine / R. W. Sinnott // Sky and Telescope. – 1984. – Vol. 68, № 2. – P. 159.
7. Давыдов, А. В. Планирование сетей мобильной связи / А. В. Давыдов. – М. : Горячая линия – Телеком, 2021. – 312 с.
8. Парамонов, А. И. Модели распространения радиоволн в системах мобильной связи / А. И. Парамонов // Телекоммуникации. – 2020. – № 6. – С. 42–48.

UDC 621.396.4

COMPARATIVE ANALYSIS OF SIGNAL ATTENUATION IN HETEROGENEOUS CELLULAR NETWORKS BASED ON RSSI MEASUREMENTS IN MINSK URBAN ENVIRONMENT

Rodionov M.A.

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Aksenov V.A. – senior lecturer

Astrovskii I.I. – Phd in Engineering

Annotation. The paper presents the results of practical RSSI measurements in LTE networks across 64 measurement points in three characteristic locations of Minsk. Distances from measurement points to base stations were calculated using the haversine formula. Experimental data were compared with the logarithmic path-loss model; attenuation exponents were derived for each zone via least-squares fitting. The dependence of coverage quality on urban morphology and base-station density was established.

Keywords. heterogeneous networks, LTE, RSSI, signal attenuation, haversine formula, path loss exponent, network planning, multipath propagation, handover, urban environment, practical measurements, signal quality.

УДК 654.09

РОЛЬ МАППИНГА В ПРОЕКТИРОВАНИИ И ЭКСПЛУАТАЦИИ СОВРЕМЕННЫХ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ

Романюк Я.С., магистрант гр.567041

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Насонова Н.В. – д-р техн. наук, профессор

Аннотация. В докладе исследуется роль маппинга в проектировании и эксплуатации современных инфокоммуникационных сетей. Цель работы - продемонстрировать, как методы маппинга повышают эффективность проектирования, мониторинга и обслуживания сетевых инфраструктур, а также способствуют обеспечению их надёжности и масштабируемости.

Ключевые слова: Маппинг; инфокоммуникационные сети; проектирование сетей; эксплуатация сетей; коэффициент готовности; утилизация каналов; пропускная способность.

Современные инфокоммуникационные сети представляют собой сложные распределённые системы, требующие эффективных инструментов проектирования и эксплуатации. Маппинг - визуализация топологии и состояния сети – становится критически важным инструментом для решения этих задач.

Цель доклада – показать, как методы маппинга повышают эффективность проектирования, мониторинга и обслуживания сетевых инфраструктур, а также способствуют обеспечению их надёжности и масштабируемости.

Задачи исследования:

- проанализировать применение маппинга на всех этапах жизненного цикла сети;
- оценить количественный эффект от внедрения маппинга;
- привести математические модели для расчёта ключевых показателей сети.

1. Маппинг на этапе проектирования

На этапе проектирования маппинг выступает ключевым инструментом для создания эффективной и надёжной инфокоммуникационной сети. Он позволяет не просто визуализировать планируемую структуру, но и провести количественную оценку её параметров, выявить потенциальные проблемы ещё до развёртывания оборудования.

Основные задачи маппинга на этапе проектирования:

- моделирование топологии сети (физической и логической) до развёртывания;
- расчёт пропускной способности каналов с учётом текущей и прогнозируемой нагрузки;
- оптимизация расположения коммутационного и активного оборудования;
- прогнозирование зон покрытия для беспроводных сегментов сети (Wi-Fi, сотовые сети);
- планирование резервирования и отказоустойчивости;
- оценка масштабируемости решения – возможности расширения без кардинальной перестройки.

1.1. Расчёт пропускной способности

Ключевым параметром при проектировании является пропускная способность канала. Она рассчитывается по формуле Шеннона [1]:

$$C = B \cdot \log_2 (1 + \text{SNR}), \quad (1)$$

где C – пропускная способность (бит/с); B – полоса пропускания (Гц); SNR – отношение сигнал/шум (безразмерная величина).

Эта формула позволяет оценить теоретический максимум пропускной способности канала и выбрать оборудование с соответствующими характеристиками. На практике реальная пропускная способность будет ниже из-за накладных расходов протоколов, помех и асимметрии трафика.

1.2. Прогнозирование зоны покрытия беспроводных сетей

Для беспроводных сетей (Wi-Fi, 5G) важно рассчитать зону покрытия точки доступа или базовой станции. Радиус зоны покрытия определяется по формуле Фрииса [2]:

$$R = (4\pi)^2 P_{\text{t}} P_{\text{r}} G_{\text{t}} G_{\text{r}} \lambda, \quad (2)$$

где R – радиус зоны покрытия (м); P_{t} – мощность передатчика (Вт); G_{t} , G_{r} – коэффициенты усиления передающей и приёмной антенн; λ – длина волны (м); P_{rmin} – минимальная мощность сигнала на приёмнике (Вт).

На практике радиус сокращается из-за препятствий (стены, мебель), интерференции и загруженности диапазона.

1.3. Оптимизация топологии и резервирование

Маппинг позволяет смоделировать различные варианты топологии (звезда, кольцо, mesh) и оценить их по критериям:

– задержки:

$$T_{total} = \sum n T_{prop,i} + T_{proc,i},$$

– отказоустойчивость: вероятность отказа сети с резервированием рассчитывается как:

$$P_{fail} = 1 - \prod (1 - p_i), \quad (3)$$

где P_{fail} – вероятность отказа всей системы; p_i – вероятность отказа узла i .

Для критически важных сегментов проектируют резервированные маршруты (LAG, MPLS TE), что снижает P_{fail} .

1.4. Планирование кабельной инфраструктуры

При проектировании структурированной кабельной системы (СКС) маппинг помогает:

– рассчитать длину трасс с учётом стандартов (максимум 90 м для горизонтальной подсистемы);

– определить количество портов коммутаторов и патч-панелей;

– спланировать маркировку и документирование соединений.

Задержка распространения сигнала в кабеле рассчитывается как:

$$T_{prop} = vL, \quad (4)$$

где T_{prop} – задержка распространения (с); L – длина кабеля (м); v – скорость сигнала в среде (для витой пары $\sim 2 \times 10^8$ м/с).

1.5. Инструменты для проектирования с маппингом

Для реализации маппинга на этапе проектирования используют:

– Специализированное ПО: AutoCAD (для планов помещений), Visio (логические схемы), Lucidchart (онлайн-моделирование).

– Сетевые симуляторы: GNS3, Cisco Packet Tracer (тестирование топологий без оборудования).

– ГИС-платформы: ArcGIS, QGIS (для городских сетей - привязка к местности).

– Системы управления конфигурациями: NetBox (учёт оборудования, IP-адресация).

– Инструменты для расчёта радиопокрытия: TamoGraph, Ekahau (моделирование Wi-Fi).

1.6. Практический пример: проектирование кампусной сети университета

Задача: обеспечить проводной и беспроводной доступ для 5 000 пользователей в 10 зданиях.

Этапы с применением маппинга:

– Сбор требований: 1 Гбит/с на этаж, Wi-Fi 6 в аудиториях, резервирование магистралей.

– Моделирование топологии: ядро (L3-коммутаторы) – распределение (стеки L2+) – доступ (PoE-коммутаторы).

– Расчёт пропускной способности по формуле (1): для магистралей 10 Гбит/с (с запасом 40 %).

– Расчёт зон покрытия Wi-Fi по формуле (2): размещение точек доступа с перекрытием 20 %.

– Оптимизация: резервирование связей между коммутаторами распределения (MLAG).

– Документирование: схемы в Visio и база данных оборудования в NetBox.

Этот раздел демонстрирует, что маппинг на этапе проектирования – не просто рисование схем, а инженерный процесс с математическим обоснованием решений. Он снижает риски ошибок, оптимизирует затраты и закладывает основу для эффективной эксплуатации сети.

2. Маппинг при развёртывании и эксплуатации

При развёртывании сети маппинг помогает:

– планировать прокладку кабелей;

– маркировать оборудование на карте;

– документировать соединения;

– контролировать соответствие проекта и реализации.

В процессе эксплуатации маппинг обеспечивает:

– визуализацию трафика в реальном времени;

– диагностику сбоев (трассировка маршрута);

– управление конфигурациями;

– отчётность для аудита.

Важным показателем является утилизация канала - доля используемой пропускной способности:

$$U=R\lambda\cdot L, \quad (5)$$

где U – утилизация канала (безразмерная величина или %); λ – интенсивность трафика (пакетов/с); L – средняя длина пакета (бит); R – пропускная способность канала (бит/с).

Если $U>0,8$ (80 %), канал считается перегруженным и требует модернизации.

Коэффициент готовности сети показывает, какую часть времени система функционирует корректно:

$$A=MTBF+MTTR\cdot MTBF, \quad (6)$$

где A – коэффициент готовности (безразмерная величина или %); MTBF (Mean Time Between Failures) – среднее время наработки на отказ (ч); MTTR (Mean Time to Repair) – среднее время восстановления (ч).

Маппинг позволяет выявить «узкие места» с низким коэффициентом готовности и спланировать резервирование.

3. Маппинг для модернизации и масштабирования

При масштабировании сети маппинг помогает:

- анализировать узкие места (карты утилизации ресурсов);
- планировать добавление новых узлов;
- тестировать изменения на модели;
- мигрировать сервисы с минимальной потерей доступности.

Время восстановления после сбоя (RTO - Recovery Time Objective) можно оценить по формуле:

$$RTO=T_{detect}+T_{diag}+T_{repair}+T_{test}, \quad (7)$$

где T_{detect} – время обнаружения сбоя (с); T_{diag} – время диагностики (с); T_{repair} – время устранения неисправности (с); T_{test} – время тестирования работоспособности (с).

Вероятность отказа сети с резервированием рассчитывается как:

$$P_{fail}=1-\prod (1-p_i), \quad (8)$$

где P_{fail} – вероятность отказа всей системы; p_i – вероятность отказа узла i .

Маппинг резервированных маршрутов позволяет минимизировать P_{fail} за счёт выбора альтернативных путей.

Практические результаты внедрения маппинга.

Анализ кейсов внедрения систем маппинга (SolarWinds, Cisco DNA Center, NetBox) показывает следующие результаты [3, 4]:

- сокращение времени поиска неисправностей с 4 часов до 30 минут (на 87 %);
- уменьшение ошибок при конфигурации на 60 % за счёт визуализации;
- повышение прозрачности управления ресурсами (единый источник данных для всех отделов);
- снижение затрат на модернизацию на 25 % благодаря точному планированию.

Маппинг является неотъемлемым инструментом проектирования и эксплуатации современных инфокоммуникационных сетей. Его применение:

- повышает эффективность проектирования за счёт моделирования и расчёта параметров;
- улучшает мониторинг и диагностику в процессе эксплуатации;
- снижает затраты на масштабирование и модернизацию;
- увеличивает надёжность и доступность сетевых сервисов.

Перспективные направления развития – интеграция маппинга с искусственным интеллектом для предсказания сбоев и автоматизация построения карт на основе потоковых данных.

Список использованных источников:

1. Shannon, C. E. A Mathematical Theory of Communication // Bell System Technical Journal. – 1948. – Vol. 27. – С. 379–423, 623–656.
2. Friis, H. T. A Note on a Simple Transmission Formula // Proceedings of the IRE. – 1946. – Vol. 34, No. 5. – С. 254–256.
3. SolarWinds Network Topology Mapper: User Guide. – SolarWinds, 2023.
4. Cisco DNA Center: Design and Deployment Guide. – Cisco Systems, 2022.

УДК 005.216.1

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ БЕСПИЛОТНЫХ СИСТЕМ ЧЕРЕЗ СОВМЕСТНОЕ УПРАВЛЕНИЕ ЭНЕРГОПОТРЕБЛЕНИЕМ И ПОДСИСТЕМАМИ ВИДЕОНАБЛЮДЕНИЯ

Воронович Д.Ю., Максак М.Ю.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Вишняков В.А. – д-р техн. наук, профессор

Аннотация. В статье рассматривается проблема разработки комплексной системы управления беспилотным автомобилем, основанной на технологии IoT. Актуальность исследования обусловлена необходимостью перехода от изолированных бортовых систем к интегрированной экосистеме, где подсистемы энергопитания и технического зрения функционируют согласованно. Предложена архитектура, объединяющая интеллектуальное управление энергопотреблением и системы видеонаблюдения с элементами компьютерного зрения. Особое внимание уделено взаимосвязи между нагрузкой на вычислительные узлы обработки видеопотока и стратегией распределения энергии, а также вопросам информационной безопасности передачи данных. Результаты исследования демонстрируют, что совместная оптимизация алгоритмов управления питанием и видеоконтролем позволяет повысить автономность, безопасность и адаптивность беспилотных транспортных средств в условиях современной транспортной инфраструктуры.

Ключевые слова. Беспилотные автомобили, энергопитание, компьютерное зрение, безопасность передачи данных.

Развитие автономных транспортных средств является одним из стратегических направлений современной транспортной инфраструктуры. В условиях роста требований к безопасности, энергоэффективности и интеллектуализации логистических процессов, беспилотные автомобили всё чаще рассматриваются не как изолированные технические системы, а как интегрированные элементы единой интеллектуальной транспортной экосистемы на базе технологий IoT [1]. Особую роль в обеспечении функциональности таких систем играют подсистемы технического зрения и энергоменеджмента, которые традиционно проектируются отдельно, что снижает общую эффективность транспортного средства.

Системы видеонаблюдения и компьютерного зрения формируют основу для восприятия окружающей среды и принятия решений в реальном времени [2]. Однако обработка видеопотоков и работа нейросетевых алгоритмов требуют значительных вычислительных ресурсов, что напрямую влияет на энергопотребление бортовой сети. В то же время, интеллектуальные системы управления питанием, ориентированные на оптимизацию зарядки и распределения энергии, часто не учитывают динамическую нагрузку со стороны периферийных датчиков и вычислительных модулей [3]. Отсутствие координации между подсистемами энергопитания и видеоконтроля приводит к неоптимальному расходу заряда батареи и снижению автономности АТС в сложных условиях эксплуатации.

Дополнительную актуальность приобретают вопросы информационной безопасности и надёжности передачи данных. В условиях, когда видеопотоки используются для критически важных решений, а система питания взаимодействует с внешней инфраструктурой, обеспечение целостности и доступности информации становится неотъемлемой частью архитектуры системы. Это особенно важно в свете требований по защите персональных данных и технических регламентов безопасности колёсных транспортных средств [4].

В рамках данного исследования предлагается многоуровневая архитектура комплексной системы управления беспилотным автомобилем, основанная на технологиях IoT. Основная идея заключается в объединении подсистем энергопитания и видеонаблюдения в единый информационно-управляющий контур, что позволяет оптимизировать распределение ресурсов в реальном времени.

На сенсорном уровне размещаются источники данных и исполняющие устройства. К ним относятся камеры технического зрения, датчики тока и напряжения бортовой сети, блок управления батареей и вычислительные модули. Важной особенностью является наличие единого IoT-шлюза, который агрегирует данные от разнородных источников [5].

Сетевой уровень обеспечивает передачу данных между компонентами системы. Для связи внутри автомобиля используется шина Controller Area Network, обеспечивающая детерминированную передачу критических данных, таких как показания датчиков напряжения. Для передачи видеопотоков и телеметрии во внешнюю инфраструктуру применяются беспроводные протоколы и легковесные протоколы прикладного уровня, такие как MQTT.

Уровень приложений реализует логику управления. Здесь функционируют алгоритмы компьютерного зрения (детекция объектов, построение маршрута) и алгоритмы энергоменеджмента. В отличие от традиционных подходов, где эти подсистемы работают изолированно, в предложенной

архитектуре реализован обратный канал влияния: данные о вычислительной нагрузке систем зрения передаются в модуль управления питанием.

Взаимодействие подсистем организовано следующим образом. Модуль видеонаблюдения формирует запрос на вычислительные ресурсы в зависимости от сложности дорожной сцены. Эта информация передается в интеллектуальный контроллер питания, который корректирует режимы работы батареи и распределение энергии между двигателем и бортовой электроникой. Данные о состоянии заряда батареи могут влиять на работу видеосистемы, например, снижая частоту кадров или разрешение потока при критическом уровне энергии для продления автономности [3]. Такая интеграция позволяет реализовать адаптивные сценарии работы. Например, при обнаружении препятствия системой зрения приоритет энергии временно отдается вычислительному блоку для экстренного расчета траектории, а при движении по трассе с хорошим освещением нагрузка на камеры снижается в пользу экономии заряда.

Таким образом, предложенная архитектура обеспечивает не только сбор и обработку данных, но и интеллектуальное управление ресурсами автомобиля на основе комплексного анализа состояния как энергетической системы, так и системы восприятия окружающей среды.

Модель взаимодействия подсистем и алгоритм управления ресурсами

Для описания зависимости энергопотребления от нагрузки систем технического зрения введем целевую функцию оптимизации. Пусть E_{total} – общее доступное энергопотребление на текущем участке маршрута, E_{drive} – энергия, необходимая для движения, E_{comp} – энергия на вычислительные задачи. Тогда ограничение имеет вид:

$$E_{comp} \leq E_{total} - E_{drive} - E_{reserve}, \quad (1)$$

где $E_{reserve}$ – резервный запас энергии для нештатных ситуаций.

Энергопотребление вычислительного модуля E_{comp} напрямую зависит от параметров видеопотока. Его можно представить как функцию от частоты кадров FPS, разрешения Res и сложности алгоритма детекции Alg:

$$E_{comp} = k_1 \cdot FPS \cdot Res + k_2 \cdot C_{alg}, \quad (2)$$

где k_1, k_2 – коэффициенты, определяемые архитектурой вычислительной платформы.

Сложность алгоритма C_{alg} варьируется в зависимости от дорожной сцены. Например, движение по трассе в дневное время требует меньше вычислительных ресурсов, чем движение в плотном городском потоке ночью. Система видеонаблюдения оценивает сложность сцены и передает эту метку в контроллер питания. На основе полученных данных реализуется алгоритм динамического распределения ресурсов [5].

Результаты имитационного моделирования

Для оценки эффективности предложенной архитектуры и алгоритма управления ресурсами было проведено имитационное моделирование. Моделировался сценарий движения беспилотного автомобиля по городскому маршруту протяженностью 10 км с переменной дорожной обстановкой (открытая трасса, плотный городской трафик, ночное время).

В качестве метрик эффективности использовались:

- общее энергопотребление системы E_{total} ;
- точность детекции объектов Acc_{det} ;
- время автономной работы T_{auto} .

Сравнивались два подхода: базовый (независимая работа подсистем видео и питания) и предложенный (интегрированное управление с адаптивной настройкой параметров видеопотока).

Таблица 1 – Сравнение эффективности подходов

Метрика	Базовый подход	Предложенный подход	Улучшение
E_{total} , Вт·ч	145,2	118,7	18,3%
Acc_{det} , %	94,1	93,8	–0,3%
T_{auto} , мин	87	106	+21,8%

Как видно из таблицы, предложенный подход позволяет сократить общее энергопотребление на 18,3% при незначительном снижении точности детекции, что находится в пределах допустимой погрешности. Прирост времени автономной работы составляет почти 22%, что является существенным преимуществом для практического применения [6].

В работе решена задача интеграции подсистем энергоснабжения и видеонаблюдения беспилотного автомобиля в рамках единой IoT-архитектуры. Предложен алгоритм адаптивного

управления ресурсами, динамически корректирующий параметры видеопотока в зависимости от сложности сцены и уровня заряда батареи. Результаты имитационного моделирования подтвердили эффективность разработанного подхода: применение алгоритма позволяет сократить общее энергопотребление на 18,3% при незначительном снижении точности детекции объектов (0,3 п.п.), что находится в пределах допустимой погрешности. Прирост времени автономной работы составляет почти 22%, что является существенным преимуществом для практического применения беспилотных платформ в условиях городской и сельской местности.

Список использованных источников:

1. Вишняков В. А., Максак М. Ю. Концепция, модель, примеры систем Интернета вещей для эффективного электроснабжения // Технологии передачи и обработки информации : материалы Междунар. науч.-техн. семинара, Минск, апр. 2025 г. / Белорус. гос. ун-т информатики и радиоэлектроники. – Минск : БГУИР, 2025. – С. 37–41.
2. Сиротко С. И., Ма Ц., Зорько М. И. [и др.]. Модели одновременной локализации и построения карты открытого пространства БЛА с помощью многокамерной видеосистемы // Технологии передачи и обработки информации : материалы Междунар. науч.-техн. семинара, Минск, апр. 2025 г. – Минск : БГУИР, 2025. – С. 7–14.
3. Хаджинова Н. В., Савоневская М. О., Столярова В. В. [и др.]. Алгоритмы мультиагентного доступа к каналам мобильной связи (5G, 6G) для минимизации задержек в условиях Интернета вещей // Технологии передачи и обработки информации : материалы Междунар. науч.-техн. семинара, Минск, апр. 2025 г. – Минск : БГУИР, 2025. – С. 67–72.
4. Крагель В. А., Романюк М. В. Перспективы использования мобильных сетей нового поколения в Интернете вещей // Технологии передачи и обработки информации : материалы Междунар. науч.-техн. семинара, Минск, апр. 2025 г. – Минск : БГУИР, 2025. – С. 183–187.
5. Бегляк Е. В., Марцинкевич В. А. Современные протоколы аутентификации и авторизации в беспроводных сетях // Технологии передачи и обработки информации : материалы Междунар. науч.-техн. семинара, Минск, апр. 2025 г. – Минск : БГУИР, 2025. – С. 168–175.
6. Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» [Электронный ресурс]. – Режим доступа: <https://pravo.by/document/?guid=12551&p0=H12100099>. – Дата доступа: 15.03.2025.

UDC 005.216.1

IMPROVING THE EFFICIENCY OF UNMANNED SYSTEMS THROUGH JOINT MANAGEMENT OF ENERGY CONSUMPTION AND VIDEO SURVEILLANCE SUBSYSTEMS

Voronovich D.Yu., Maksak M.Yu.

*Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus*

V.A. Vishnyakov – Doctor of Technical Sciences, Professor

Abstract. This article examines the development of an integrated control system for a self-driving car based on IoT technology. The relevance of the study stems from the need to transition from isolated onboard systems to an integrated ecosystem where power supply and computer vision subsystems operate in concert. An architecture is proposed that integrates intelligent power management and video surveillance systems with computer vision elements. Particular attention is paid to the relationship between the load on computing nodes processing the video stream and the energy distribution strategy, as well as issues of data transmission security. The study's results demonstrate that joint optimization of power management and video monitoring algorithms can improve the autonomy, safety, and adaptability of autonomous vehicles in today's transportation infrastructure.

Keywords: autonomous vehicles, power supply, computer vision, data security.

КРОСС-МОДАЛЬНЫЙ ПЕРЕНОС ЗНАНИЙ КАК ФАКТОР РАЗВИТИЯ ЛОГИЧЕСКОГО РАССУЖДЕНИЯ В ЯЗЫКОВЫХ МОДЕЛЯХ

Оруджев М.М.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Масейчик Е.А. – ассистент

В данной работе рассматривается феномен кросс-модального переноса знаний (cross-modal transfer learning) в контексте больших языковых и мультимодальных моделей. Утверждается, что включение видеоданных в процесс предобучения систематически улучшает способность моделей к логическому рассуждению в текстовых задачах – эффект, не объяснимый исключительно увеличением объема текстового корпуса.

Принятая парадигма в масштабировании языковых моделей предполагает, что повышение когнитивных способностей ИИ достигается посредством увеличения объема обучающих текстов [1]. Однако, накопленные эмпирические данные свидетельствуют как раз об обратном: разнообразие модальностей, но отнюдь не масштаб однородных данных, является в большей степени фундаментальным фактором для развития общих способностей к рассуждению.

Основным эмпирическим подтверждением данного тезиса служит работа [2], представившая модель MERLOT, предобученную на 180 миллионах видеофрагментов с транскриптами. Авторы зафиксировали значимое улучшение показателей модели на текстовых бенчмарках в области здравого смысла (HellaSwag, VCR) в сравнении с текстовыми базовыми линиями аналогичного масштаба. Авторы именно таким образом интерпретируют этот результат, а именно: видеопоследовательности обеспечивают модель темпоральными причинно-следственными структурами, то есть «законами мира». В явном виде вывести их из текста крайне сложно. В системе VideoBERT получены подобные результаты [3]. Совместное обучение по видео вместе с текстом повысило точность заполнения масок в языковых задачах, тем самым косвенно указывая на обогащение семантических репрезентаций.

В то же самое время модель CLIP показала, что контрастивное обучение на парах изображение-текст формирует семантически намного более плотные представления в сравнении с обучением на одном из каналов, а в работе о системе Gato показали, что единая мультимодальная политика, обученная на разнородных задачах (включая игровые видеоданные), демонстрирует способность к zero-shot генерализации на новые текстовые задачи, а это свидетельствует о переносе абстрактных структур рассуждения.

С когнитивно-научной точки зрения, этот эффект в целом согласуется с теорией embodied cognition: концептуальные репрезентации укоренены в перцептивном опыте и также в моторном опыте. Во время наблюдения моделью за физикой движения объектов, столкновений, гравитации, она формирует неявные каузальные схемы, которые затем активируются при решении текстовых задач на рассуждение. Йошуа Бенджио вместе с другими в теории глубоких представлений предположили, что признаки должны отражать основные факторы вариативности наблюдаемых данных, при этом видеоданные делают эти факторы (движение, время, причинность) явными для модели.

Полученные результаты ставят под сомнение саму идею насчет «текстоцентричной» гипотезы масштабирования. Логическое мышление отчасти является эмерджентным продуктом мультимодального восприятия. Значит, достичь artificial general intelligence можно не увеличением текстовых данных, а созданием систем, которые объединяют разные типы данных в общие причинно-следственные модели мира.

Cross-modal transfer learning являет собой не технический артефакт, а скорее основной механизм для формирования общего интеллекта. Обучение с помощью видео улучшает текстовую логику, потому что предоставляет моделям доступ к структурам реального мира. В чисто лингвистическом пространстве подобные структуры оказываются недоступными для модели.

Список использованных источников:

1. *Scaling laws for neural language models* / J. Kaplan [et al.] // *arXiv preprint*. – 2020. – arXiv:2001.08361.
2. *MERLOT: Multimodal neural script knowledge models* / R. Zellers [et al.] // *Advances in Neural Information Processing Systems (NeurIPS)*. – 2021. – Vol. 34. – P. 23634–23651.
3. *VideoBERT: A joint model for video and language representation learning* / C. Sun [et al.] // *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)*. – 2019. – P. 7464–7473.

МНОГОФАКТОРНАЯ АУТЕНТИФИКАЦИЯ (MFA) КАК БАЗОВЫЙ МЕТОД ЗАЩИТЫ КОРПОРАТИВНОЙ СЕТИ

Жуков Н.А., студент гр.568403

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Чепикова В.В. – старший преподаватель.

Аннотация. В работе представлен комплексный анализ многофакторной аутентификации (MFA) как фундаментального элемента безопасности корпоративных сетей. Рассмотрены современные векторы атак, направленные на обход традиционных методов MFA, включая атаки «злоумышленник в середине» (AitM) и «усталость от MFA» (MFA Fatigue). Обоснована необходимость перехода к фишингоустойчивым методам на базе протоколов FIDO2 и WebAuthn. Даны практические рекомендации по интеграции MFA в архитектуру «нулевого доверия» (Zero Trust).

Ключевые слова. Многофакторная аутентификация, MFA, информационная безопасность, корпоративная сеть, Zero Trust, AitM, MFA Fatigue, FIDO2, биометрия.

Введение

В современном цифровом мире защита передаваемых данных и корпоративных ресурсов становится одной из приоритетных задач. Традиционные сетевые экраны (firewalls) и виртуальные частные сети (VPN) долгое время служили основой корпоративной безопасности, создавая защищенный периметр вокруг внутренних ресурсов. Однако в условиях стремительной децентрализации ИТ-инфраструктуры, массовой миграции сервисов в облачные среды и повсеместного перехода на удаленный и гибридный форматы работы традиционная модель безопасности, основанная на защите периметра, окончательно утратила свою эффективность. Сегодня сотрудники получают доступ к конфиденциальной коммерческой информации с различных устройств, включая личные (BYOD), и из неконтролируемых публичных сетей. В этой новой реальности парадигма безопасности сместилась от защиты сети к защите данных и строгой идентификации пользователей. Концепция «нулевого доверия» (Zero Trust Architecture, ZTA) предполагает, что ни одному субъекту или устройству нельзя доверять по умолчанию, независимо от их физического или логического местоположения. В основе этой архитектуры лежит непрерывная проверка личности пользователя, где многофакторная аутентификация (MFA) выступает уже не как дополнительная опция, а как фундаментальный, базовый механизм защиты корпоративного контура [1]. Цель данной работы – провести анализ многофакторной аутентификации как базового метода защиты, рассмотреть уязвимости традиционных подходов перед современными угрозами и определить наиболее эффективные способы внедрения фишингоустойчивых решений в корпоративную среду.

Эволюция угроз и кризис парольной защиты

Исторически сложилось так, что основным методом идентификации пользователей в информационных системах выступала парольная защита. Тем не менее, на сегодняшний день пароли представляют собой наиболее уязвимое звено в архитектуре кибербезопасности. Статистические данные ведущих аналитических агентств показывают, что подавляющее большинство успешных кибератак начинается именно с компрометации учетных данных. Проблема усугубляется человеческим фактором: пользователи склонны применять легко угадываемые пароли или повторно использовать одни и те же комбинации для доступа к различным корпоративным и личным сервисам. Даже при внедрении строгих политик сложности паролей злоумышленники активно применяют методы социальной инженерии, фишинг, атаки полного перебора (brute-force) и подстановку ранее утекших учетных данных (credential stuffing). В связи с этим Национальным институтом стандартов и технологий США (NIST) и Европейским агентством по кибербезопасности (ENISA) в рамках требований директивы NIS2 настоятельно рекомендуется отказ от использования исключительно парольной защиты для доступа к критически важной инфраструктуре [2, 3].

Принципы и классификация факторов MFA

В основе многофакторной аутентификации лежит довольно простой принцип: чтобы подтвердить свою личность, пользователю недостаточно предъявить что-то одно. Нужно предоставить как минимум два независимых доказательства. Смысл такого подхода очевиден – если злоумышленник подсмотрит пароль или каким-то образом украдет токен, система все равно его не пропустит, поскольку у него не окажется второго ключа к учетной записи. На практике все эти доказательства (или факторы) принято делить на три большие группы:

То, что мы держим в голове, или фактор знания. Сюда относятся привычные всем пароли, короткие PIN-коды, а также ответы на контрольные вопросы.

То, что находится у нас в руках – фактор владения. Это может быть как обычный смартфон, на который приходит SMS или где работает генератор кодов (например, приложение TOTP), так и специализированное оборудование вроде аппаратных USB-ключей и смарт-карт.

То, кем мы физически являемся, то есть неотъемлемые свойства человека. Речь идет о биометрии: отпечатках пальцев, геометрии лица или рисунке радужной оболочки глаза [4]. Скопировать или передать кому-то такие данные крайне проблематично. Кроме того, современные корпоративные системы все чаще смотрят не только на то, что вводит пользователь, но и на контекст его действий. Технологии адаптивной аутентификации (Adaptive MFA) умеют анализировать, из какой геопозиции происходит попытка входа, в какое время суток, насколько надежно само устройство и не отличается ли сетевое поведение сотрудника от его привычных паттернов.

Современные векторы атак на системы MFA

Несмотря на то, что внедрение базовой MFA критически повышает уровень защищенности, не все ее методы обеспечивают одинаковую степень защиты от современных изощренных кибератак. Выделяют два основных вектора атак на системы многофакторной аутентификации: Первый вектор – атаки типа «злоумышленник в середине» (Adversary-in-the-Middle, AitM). В данном сценарии атакующий разворачивает прокси-сервер, который перехватывает трафик между жертвой и легитимным сервисом. Жертва переходит по ссылке на поддельный сайт. При вводе логина, пароля и одноразового кода (например, из SMS), прокси-сервер в реальном времени передает эти данные на целевой ресурс. После успешной аутентификации сервис выдает легитимный маркер сеанса (session cookie), который перехватывается злоумышленником. Получив маркер, атакующий обходит защиту MFA. Второй вектор – атака типа «усталость от MFA» (MFA Fatigue или Prompt Bombing). Данная техника применяется, когда в качестве второго фактора используются Push-уведомления. Атакующий, заполучив пароль жертвы, инициирует десятки запросов на авторизацию подряд, обычно в ночное время. Непрерывный поток уведомлений вызывает раздражение у пользователя, который в конечном итоге подтверждает запрос, чтобы прекратить спам.

Сравнительный анализ методов аутентификации

Для выбора оптимального решения необходимо оценивать методы MFA по уровню предоставляемой безопасности, устойчивости к описанным атакам и удобству для конечного пользователя. В таблице 1 представлен сравнительный анализ основных методов.

Таблица 1 – Сравнительный анализ методов многофакторной аутентификации

Метод аутентификации	Уровень безопасности	Защита от фишинга (AitM)	Защита от MFA Fatigue	Удобство пользователя
SMS / Email OTP	Низкий	Нет (перехват)	Да (неприменимо)	Высокое
TOTP	Средний	Нет (перехват)	Да (неприменимо)	Среднее
Push-уведомления	Средне-Высокий	Нет(если без контекста)	Нет	Очень высокое
Аппаратные ключи (FIDO2)	Наивысший	Да (криптографическая привязка)	Да (требует физ. контакта)	Среднее (нужен токен)
Биометрия	Высокий	Да	Да	Высокое

Сравнительный анализ методов аутентификации

Для надежной защиты корпоративной сети от современных угроз организациям необходимо переходить к фишингоустойчивым методам MFA. Наиболее эффективным решением является использование протоколов WebAuthn и FIDO2. Аппаратные ключи безопасности (например, YubiKey) или платформенные аутентификаторы используют криптографию с открытым ключом, которая криптографически привязана к конкретному домену (URL-адресу). Если пользователь попадает на фишинговый сайт, ключ просто не выдаст валидный ответ, что делает атаки AitM технически невозможными.

Для успешного внедрения MFA в корпоративную среду рекомендуется:

1 Использовать политики условного доступа (Conditional Access): запрашивать MFA с учетом контекста (необычный IP-адрес, новое устройство, доступ к критичным данным).

2 Ограничить Push-уведомления: внедрить функцию «сопоставления чисел» (Number Matching) для защиты от MFA Fatigue.

3 Защитить привилегированные учетные записи (PAM): администраторы должны в обязательном порядке использовать аппаратные ключи безопасности (FIDO2).

Заключение

Многофакторная аутентификация перестала быть опциональным элементом и перешла в разряд базовых требований безопасности для любой корпоративной сети. Однако полагаться на устаревшие методы, такие как SMS, в условиях изощренных атак больше нельзя. Стратегия безопасности должна строиться на внедрении фишингоустойчивой MFA, грамотном управлении доступом на основе контекста и обучении сотрудников, что в совокупности обеспечивает надежный фундамент архитектуры Zero Trust.

Список использованных источников:

- Rose, S. *Zero Trust Architecture* : NIST Special Publication 800-207 / S. Rose [et al.]. – Gaithersburg : National Institute of Standards and Technology, 2020. – 59 p.
- Grassi, P. A. *Digital Identity Guidelines: Authentication and Lifecycle Management* : NIST Special Publication 800-63B / P. A. Grassi [et al.]. – Gaithersburg : National Institute of Standards and Technology, 2017. – 81 p.
- Cybersecurity roles and skills for NIS2 Essential and Important Entities* / European Union Agency for Cybersecurity (ENISA). – Athens : ENISA, 2025. – 45 p.
- Бритвина, В. В. Сравнительный анализ методов аутентификации: от паролей до биометрии и FIDO2 / В. В. Бритвина, С. А. Бердников // Вестник науки. S– 2025. – Т. 1, № 1. – С. 112-118.

UDC 004.056.53

MULTIFACTOR AUTHENTICATION (MFA) AS A BASIC METHOD OF CORPORATE NETWORK SECURITY

Zhukov N.A.

*Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus*

Chepikova V.V. – senior lecturer

Abstract. This paper presents a comprehensive analysis of multi-factor authentication (MFA) as a fundamental element of corporate network security. It examines modern attack vectors aimed at bypassing traditional MFA methods, including man-in-the-middle (AitM) attacks and MFA fatigue. It also substantiates the need to transition to phishing-resistant methods based on the FIDO2 and WebAuthn protocols. Practical recommendations for integrating MFA into a Zero Trust architecture are provided.

Keywords: Multi-factor authentication, MFA, information security, corporate network, Zero Trust, AitM, MFA fatigue, FIDO2, biometrics.

DYNAMIC CHANNEL MODELING AND PERFORMANCE ANALYSIS FOR UAV COMMUNICATIONS

Chi Zhang

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Jun Ma – Assistant

Abstract. A stepwise dynamic channel model for UAV communications is developed, integrating AWGN, Rayleigh fading, distance-dependent path loss, and velocity-dependent Doppler shift. BPSK and QPSK performances are compared under LOS/NLOS scenarios. Results show BER increases with distance and velocity, with QPSK more sensitive. Modulation switching thresholds are identified, and an interactive GUI is presented.

Keywords. UAV channels, AWGN, OFDM.

The increasing use of UAVs demands reliable air-to-ground links, but UAV channels are highly dynamic. This work builds a comprehensive model: UAV flies at 100 m altitude, 20 m/s, from (0,0,100) to (1000,0,100). Ground station at origin. Free-space path loss:

$$PL(d)=20\log_{10}(d)+20\log_{10}(f_c)-147, 55, f_c=2.4 \text{ GHz.}$$

Doppler shift:

$$f_d(t) = \frac{v_r(t)}{\lambda}, v_r(t) = \frac{x(t)v}{d(t)}.$$

NLOS adds flat Rayleigh fading $h_{ray}(t) = \frac{1}{\sqrt{2}}(N(0,1) + jN(0,1))$, BPSK/QPSK evaluated.

Simulation in MATLAB follows AWGN → Rayleigh → dynamic PL+Doppler → combined model. Table 1 lists parameters. GUI (Figure 1) allows real-time adjustment. Figure 2 shows BER vs. distance: QPSK degrades faster. Figure 3 shows BER vs. velocity: threshold ~30 m/s. Figure 4 compares modulations: in LOS, BPSK needs ~7 dB for BER=10⁻³, QPSK ~10 dB; in NLOS both worsen ~12 dB. Recommendations: SNR<10 dB → BPSK, 10–22 dB → QPSK, >22 dB → higher-order.

Table 1 – Simulation parameters

Parameter	Value
Carrier frequency f_c	2.4 GHz
UAV velocity v	20 m/s
UAV altitude	100 m
Flight distance range	0 – 1000 m
Symbol rate R_s	1 kHz
Reference distance	100 m
Reference SNR range	0 – 30 dB
Number of symbols	50,000

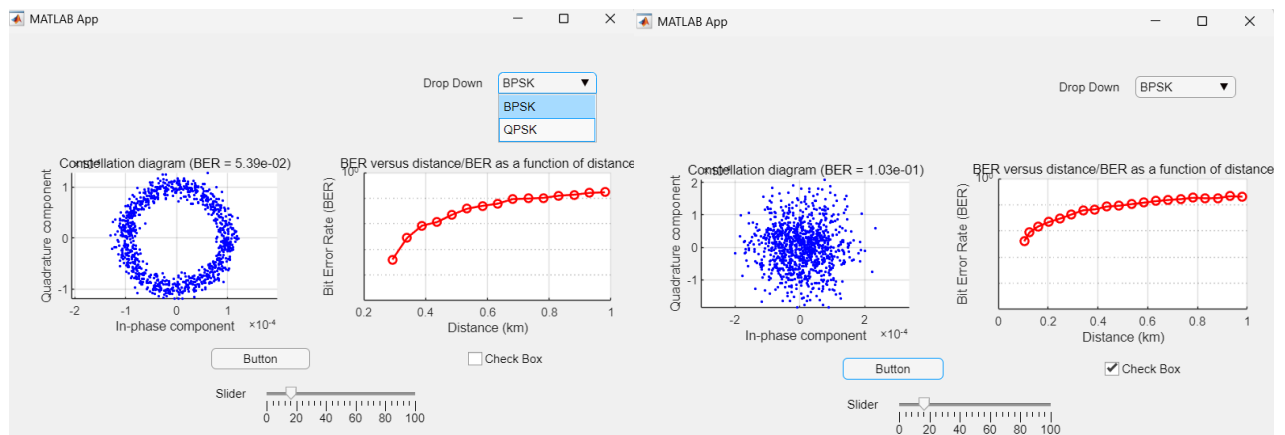


Figure 1 – GUI for UAV channel simulation (insert screenshot)

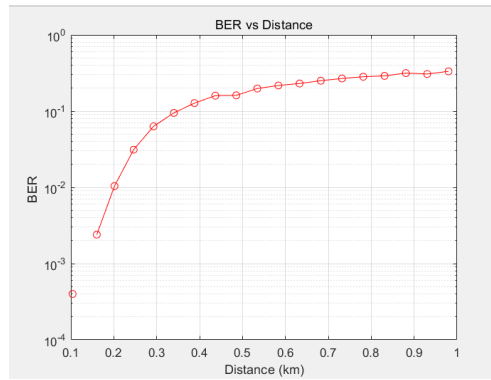


Figure 2 – BER vs. distance (BPSK & QPSK, LOS, SNR_{ref}=30 dB)

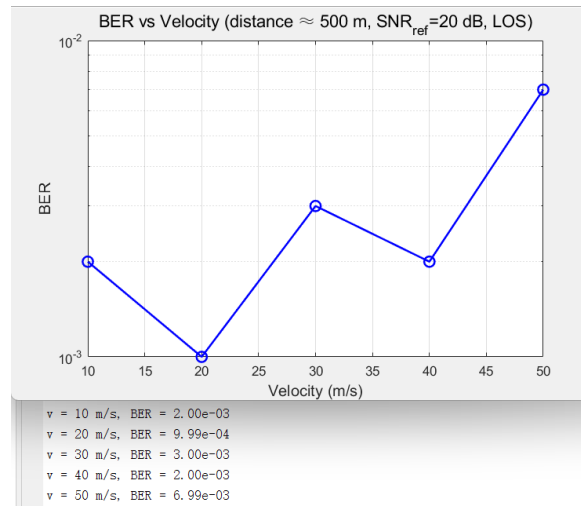


Figure 3 – BER vs. velocity (BPSK, fixed distance ≈500 m, SNR_{ref}=20 dB, LOS)

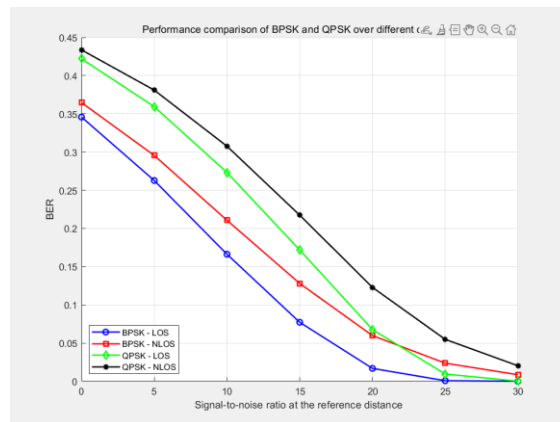


Figure 4 – BER vs. reference SNR (BPSK & QPSK, LOS & NLOS)

This work provides a dynamic channel model, quantifies distance/velocity impacts, gives modulation guidelines, and offers an interactive GUI. Future work includes urban scenarios and OFDM.

References:

1. W. Khawaja et al., *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2361-2391, 2019.
2. D. W. Matolak and R. Sun, *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 26-44, 2017.
3. X. Lin et al., *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 204-210, 2018.

DEEP LEARNING-BASED SKELETON EXTRACTION

Jiarou Wang

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Jun Ma – Assistant

Abstract. This paper presents BlumNet, a deep learning framework for object skeleton extraction based on graph component detection. It decomposes skeletons into curves, endpoints and junctions, uses a multi-branch network and joint loss, then reconstructs topologically consistent skeletons. Experiments on the SK1491 dataset show that BlumNet avoids breaks and false branches, outperforms U-Net and SkeletonNetV2, and achieves high accuracy and structural consistency.

Keywords. Deep learning methods, skeleton curves, skeleton reconstruction module.

Introduction

Skeleton extraction is a key task in computer vision for shape analysis, medical imaging, recognition and 3D reconstruction. A skeleton is a compact, single-pixel medial axis that preserves topology and geometry. Traditional methods based on morphology and distance transformation are sensitive to noise and produce broken or messy skeletons. Most deep learning methods treat skeleton extraction as segmentation and do not model graph structure explicitly, leading to topological inconsistency. This paper implements and evaluates BlumNet, which detects skeleton graph components instead of segmenting pixels, to improve precision and structural integrity.

BlumNet is a multi-branch framework built on graph component detection. It includes three parts:

1. Backbone feature extraction network: modified ResNet-50 with deformable convolution to capture multi-scale features and adapt to thin, curved skeletons.

2. Three parallel detection branches: for skeleton curves, endpoints and junction nodes, which predict confidence maps and heatmaps.

3. Skeleton reconstruction module: threshold filtering, non-maximum suppression, component association and post-processing to form a clean single-pixel skeleton.

The total loss function combines segmentation loss, heatmap regression loss and bounding box regression loss with weights $\alpha=1.0$, $\beta=1.0$, $\gamma=0.5$ for joint optimization.

Experiments were carried out on the SK1491 dataset with 1491 manually annotated shape images. Images were resized to 256×256 and split 8:1:1 for training, validation and testing. The model was implemented in PyTorch and trained on an NVIDIA RTX 2080Ti GPU using the Adam optimizer for 200 epochs. Total training time was 15 h 38 min 28 s; average inference time per image was 0.1744 s.

Visual results in Figure 1 show that BlumNet produces complete, single-pixel skeletons without breaks or false branches, matching the ground truth closely.

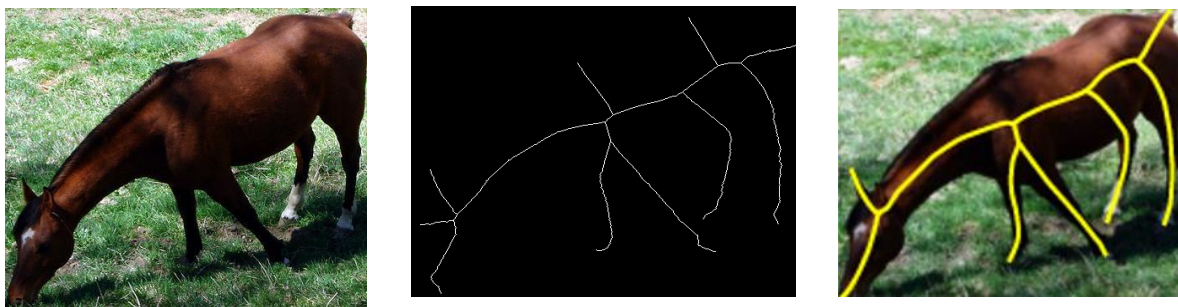


Figure 1 – Visual comparison of skeleton extraction results: a – input image; b – ground truth; c – BlumNet result

Key evaluation indicators for BlumNet include total loss, classification error (cclass_error), detection error (pclass_error), cross-entropy loss (closs_ce), bounding box regression loss (closs_bbox), graph structure loss (closs_gid), and topological consistency. The training process curves of BlumNet are shown in Figure 2.

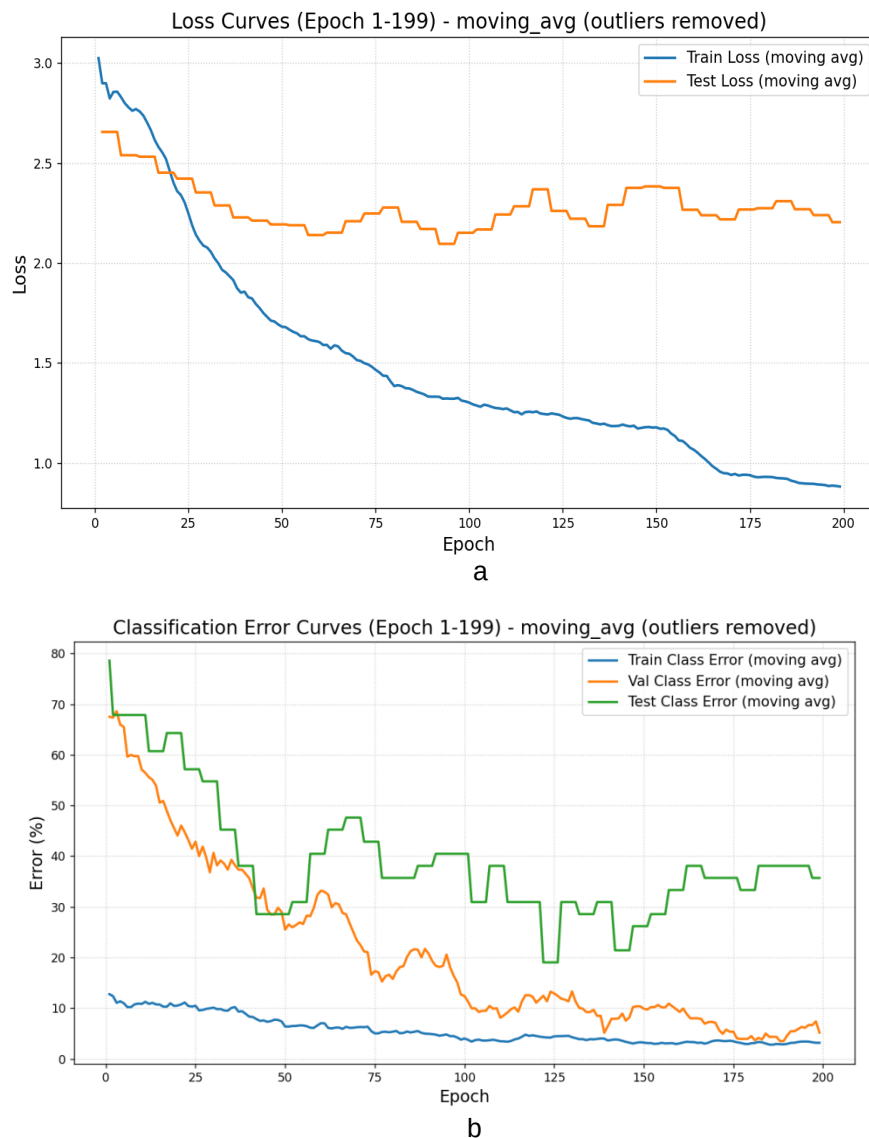


Figure 2 – Loss and Classification Error Curves of BlumNet: a – loss curve; b – classification error curve

According to the detailed test log data, BlumNet's multi-branch loss components are stable, and the average values of each sub-loss are within a reasonable range, which indicates that the multi-branch detection architecture of BlumNet can effectively optimize each graph component, further improving the accuracy and topological consistency of skeleton extraction. For example, the average `class_ce_0~4` of BlumNet is 0.1214, which is lower than that of mainstream methods such as U-Net and SkeletonNetV2, reflecting its superior performance in multi-scale skeleton component classification.

Conclusion

BlumNet effectively improves skeleton extraction by modeling skeletons as graph components. It solves the problems of fracture, false branches and topological inconsistency in traditional methods. Limitations include longer inference time than U-Net and lower accuracy on very small or complex shapes. Future work will focus on lightweight design and multi-scale attention to enhance speed and generalization.

References:

1. Rosenfeld A., Kak A. *Digital Picture Processing*. Academic Press, 1976.
2. Ronneberger O., Fischer P., Brox T. U-Net: Convolutional Networks for Biomedical Image Segmentation. *Proc. MICCAI*, 2015, pp. 234–241.
3. Xu G. et al. SkeletonNetV2: Structure-Aware Skeleton Extraction. *International Journal of Computer Vision*, 2021, vol. 129, pp. 2467–2486.
4. Zhang Y., Sang L., Yang C. BlumNet: Graph Component Detection for Object Skeleton Extraction. *Proc. ACM MM*, 2022, pp. 5527–5536.
5. Soille P. *Morphological Image Analysis: Principles and Applications*. Springer, 2006.

VEHICLE-MOUNTED VISION-LIDAR INTERMEDIATE FUSION PERCEPTION ALGORITHM BASED ON DYNAMIC DBSCAN AND ADAPTIVE WEIGHTS

Xinyu Zhang, student gr.363411

Belarusian State University of Informatics and Radioelectronics, Republic of Belarus

Jun Ma – Assistant

Abstract. To address issues in autonomous vehicles (AVs) scenarios such as insufficient robustness of single-sensor perception, unstable long-distance point cloud clustering results, and the difficulty of fixed-weight fusion strategies in adapting to the physical characteristics of sensors, this paper proposes a decision-level mid-level fusion perception algorithm based on YOLOv8 visual detection and dynamic DBSCAN point cloud clustering. The algorithm uses the KITTI dataset as a verification platform, complements multi-modal information from vehicle-mounted cameras and LiDAR, and improves the reliability of target detection and distance estimation under different distances and densities through dynamic clustering parameters, distance-adaptive weights, and clustering quality-driven confidence calculation. While ensuring lightweight and real-time performance, it effectively reduces missed detections and false detections, making it suitable for vehicle-mounted embedded perception systems.

Keywords. Autonomous vehicles, sensor fusion, dynamic DBSCAN.

Introduction

With the rapid development of AVs, environment perception has put forward higher requirements for system safety and reliability. Visual sensors have low cost and rich semantic information, but they are susceptible to factors such as illumination, occlusion, and weather, and their positioning accuracy for long-distance targets is limited. LiDAR can directly obtain 3D spatial information, and has stable measurement of target positions and contours, with obvious accuracy advantages especially at close distances [1]. However, its point clouds quickly become sparse as distance increases, making long-distance clustering difficult. Traditional perception schemes mostly rely on a single sensor, which is difficult to meet the perception needs of full-distance and multi-target in complex urban scenes. Multi-sensor fusion has become the mainstream technical route to improve system robustness, which can be divided into data layer, feature layer, and decision layer according to the fusion stage. Decision layer fusion has the characteristics of small computational load, strong modularity, and convenient engineering deployment, making it suitable for on-board real-time systems. Existing decision layer fusion methods still have several shortcomings: point cloud clustering often uses DBSCAN with fixed parameters [2], which cannot adapt to the point cloud distribution that is dense at close range and sparse at long range, confidence fusion mostly adopts fixed weights, which cannot dynamically allocate the confidence of vision and LiDAR according to the target distance, LiDAR confidence is mostly manually hard-coded, lacking correlation with the actual clustering quality. To address these issues, this paper constructs a complete vision-LiDAR fusion process, and proposes dynamic adaptive mechanisms in three key links: point cloud clustering, weight allocation, and confidence calculation, to improve the perception performance across all distance segments.

Methodology

The fusion perception system proposed in this paper adopts a modular pipeline architecture, which mainly includes an image reading and visual detection module, a point cloud reading and preprocessing module, a dynamic DBSCAN clustering module [3], a camera-lidar calibration and spatial projection module, an adaptive weight fusion module, and a result visualization module. The system takes single-frame synchronized images and point clouds as input. First, it completes 2D target detection through YOLOv8 to obtain target boxes, categories, and visual confidence. At the same time, it denoises and filters the point clouds by range, uses dynamic parameters to complete clustering, and obtains 3D target centers and laser confidence. With the help of calibration parameters, the laser clustering centers are projected onto the image plane to complete the spatial matching between detection boxes and clusters. Finally, adaptive weight fusion is performed according to the target distance, and the fused target category, detection box, distance, confidence, and working mode are output, realizing the complementary advantages of vision and lidar.

The visual detection module is based on the YOLOv8n network. It filters key target categories such as pedestrians, bicycles, cars, motorcycles, buses, and trucks from the KITTI dataset, ensuring detection accuracy while controlling computational costs. The module's output includes the target's 2D bounding box, category probability, and visual confidence, providing stable 2D semantic and positional information for subsequent fusion. Point cloud preprocessing and dynamic clustering are among the core innovations of this paper. First, distance and height filtering are applied to the original point cloud to retain the effective observation range and preserve the point cloud at the bottom of the vehicle, thereby reducing missed detections at close range. Traditional DBSCAN uses fixed parameters, which makes it difficult to adapt to the

density differences between near and far point clouds [2]. My research uses the median of point cloud distances as a reference to dynamically calculate the clustering radius and the minimum number of samples, enabling stricter clustering for close-range point clouds and looser clustering for long-range point clouds, which significantly improves clustering integrity and noise resistance. At the same time, laser confidence is dynamically generated based on the number of points in the cluster, and the confidence increases with the number of effective points, more truly reflecting the reliability of the cluster. The spatial projection and matching module use KITTI calibration parameters to convert the laser cluster center from the laser coordinate system to the camera coordinate system, and then projects it onto the image pixel plane. By determining whether the projected point falls within the detection box and selecting the cluster closest to the center of the box to complete the matching, accurate association between 2D detection and 3D clustering is achieved.

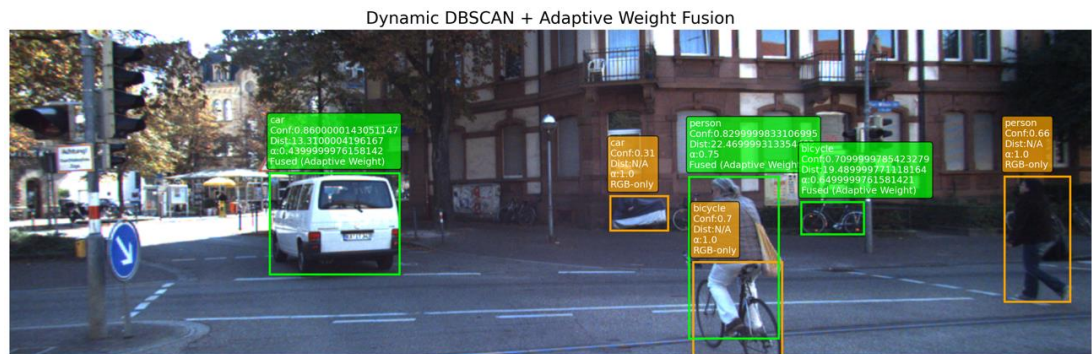


Figure 1 – Result of objective detection

The adaptive weight fusion mechanism is another core innovation of this research. It dynamically allocates the confidence weights of vision and LiDAR according to the target distance. For short distance, it reduces the visual weight and increases the LiDAR weight to make full use of the high-precision advantage of LiDAR. For long distance, it increases the visual weight and decreases the LiDAR weight to make up for the clustering instability caused by sparse point clouds. For targets with no matching laser clusters, visual results are adopted with a confidence penalty, marked as a pure visual mode, ensuring that the system can still output usable results when point clouds fail. This strategy makes the fusion confidence more in line with physical significance and improves the detection reliability in long-distance and occluded scenarios.

Evaluation

The experiments were conducted based on the KITTI dataset, using single-frame synchronized images and point cloud data to verify the effectiveness of the algorithm on a general computing platform. The main evaluation metrics included rate, and the fusion effect was visually compared with the help of visualization results. The experimental results show that compared with fixed-parameter DBSCAN and fixed-weight fusion, the dynamic strategy proposed in this paper performs better in all distance segments, with more complete clustering at close range, more stable targets at long range, more reasonable fusion confidence, and significantly improved overall system robustness. The visualization results distinguish fusion targets from pure visual targets by different colors, clearly displaying target categories, distance, confidence level, and fusion weights, which facilitates intuitive evaluation of the system's working status. Quantitative results are summarized in Table 1.

Table 1 – Quantitative Overview

Methods	Recall	Precision	DistErr	FPS
RGB	83.6	86.1	1.79	44.2
LiDAR	79.5	82.3	0.88	36.8
Fixed DBSCAN	87.1	88.5	1.16	22.4
Dynamic DBSCAN+adaptive	92.8	91.7	0.64	20.1

The proposed dynamic DBSCAN clustering strategy significantly improves the recall rate to 92.8%, which is 5.7% higher than the fixed-weight fusion method. This demonstrates the effectiveness of the adaptive parameter mechanism in handling sparse point clouds at long distances. Regarding distance estimation accuracy, the proposed method achieves the lowest average error of 0.64 meters, representing a 44.8% reduction compared to the fixed-weight fusion (1.16m). This validates the adaptive weight logic, where LiDAR confidence is weighted more heavily at close ranges and RGB confidence at long ranges.

Figure 2 (Accuracy vs Distance) further illustrates the superiority of the proposed system across all distance ranges. Especially in the range of 80-100 meters, the proposed system maintains over 70% accuracy, while other methods drop below 40%. This confirms the robust fusion capability in extreme long-range scenarios.

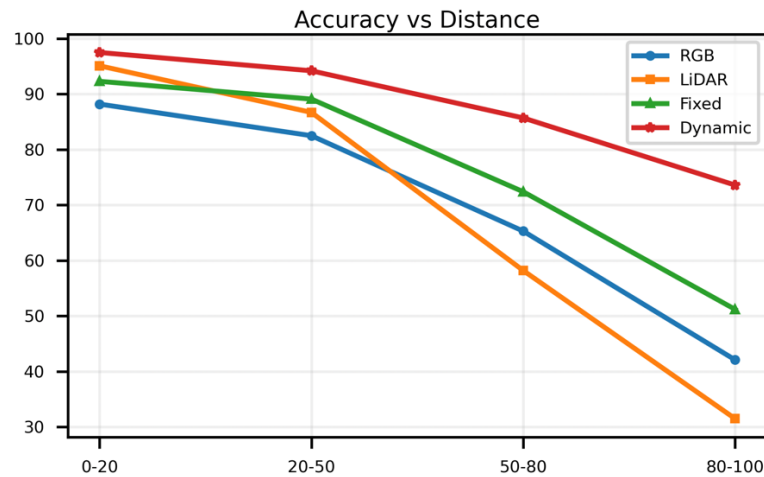


Figure 2 – Accuracy Curve for Different Distance Segments

Although the inference speed (20.1 FPS) is slightly lower than single-modality methods, it still meets the real-time requirement for autonomous driving perception.

Conclusion

In conclusion, this research proposes a vision-lidar decision-level intermediate fusion algorithm for Avs. Through dynamic DBSCAN clustering, distance-adaptive weight fusion, and clustering quality-driven laser confidence calculation, it effectively solves the problems of traditional methods such as fixed parameters, rigid weights, and disconnection between confidence and actual quality. The system has a high degree of modularity, lightweight computation, and strong real-time performance, making it suitable for deployment on vehicle-mounted embedded platforms. It can provide stable and reliable target perception results in urban roads, multi-target, and mixed near-far distance scenarios.

Reference:

1. M. Nawaz, J. K. T. Tang, K. Bibi, S. Xiao, H. P. Ho, and W. Yuan, *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 5, pp. 3228–3243, May 2024.
2. S. Chen, X. Li, S. Ma, S. Wang, and X. Ren, *IEEE Trans Instrum Meas*, vol. 74, 2025.
3. Y. Kong, L. Yan, G. Zhao, D. Liu, and H. Yang, *SAFEPROCESS 2023, Institute of Electrical and Electronics Engineers Inc.*, 2023.

SEMANTIC COMMUNICATION SYSTEM FOR VEHICLE DETECTION BASED ON CNN ENCODER AND SUPERNET ARCHITECTURE

Qikai Wang

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Jun Ma – Assistant

Abstract. This paper proposes a semantic communication system for vehicle detection tasks over noisy wireless channels. A CNN-based semantic encoder is designed to compress image features at multiple compression ratios (CH4, CH8, CH16), transmitting only task-relevant information rather than raw pixel data. To reduce model redundancy, a Supernet architecture with shared encoder weights is introduced, supporting all three compression ratios within a single model trained using the Sandwich Rule strategy. Experiments are conducted under AWGN channel conditions across five SNR levels (0-30 dB), evaluated using six detection metrics via the YOLOv12 framework on a multi-class vehicle dataset of 5,171 training images. Results demonstrate that at 0 dB SNR, the traditional transmission method suffers catastrophic performance collapse, while the semantic CH16 encoder retains $mAP@0,5 = 0,414$ (a reduction of only 8,2% from its 30 dB performance). Furthermore, Supernet_K16 achieves $mAP@0,5 = 0,618$ at 0 dB, compared to 0,627 for the independently trained CH16, a gap of only 1,4%, demonstrating that a single Supernet can effectively replace three independent models with negligible performance loss.

Keywords. Semantic communication, vehicle detection, YOLOv12, CNN encoder, supernet, AWGN channel, compression ratio.

Introduction. The rapid proliferation of intelligent transportation systems (ITS) has driven growing demand for reliable vehicle detection over wireless communication channels. In bandwidth-constrained or high-noise environments, conventional image transmission methods degrade significantly because they transmit the full raw pixel stream regardless of its task relevance. When channel quality is poor, compressed JPEG artifacts and AWGN noise corrupt pixel values irreversibly before reaching the inference engine, causing catastrophic detection failure.

Semantic communication offers a fundamentally different paradigm: instead of transmitting the image, only the features necessary to accomplish the downstream task are encoded and sent. This approach can provide strong robustness to channel noise because the encoder learns compact, task-aware representations that are far less sensitive to moderate channel distortion than raw RGB values.

In this work, we design a CNN-based semantic encoder for vehicle detection and systematically evaluate its robustness across five SNR levels under AWGN conditions. We further introduce a Supernet architecture that unifies three compression ratios (CH4, CH8, CH16) into a single model, reducing deployment overhead while preserving detection performance [1, 4].

System Model. The proposed semantic communication pipeline consists of four components: (i) a CNN semantic encoder E , (ii) an AWGN channel simulation, (iii) a CNN semantic decoder D , and (iv) a pre-trained and frozen YOLOv12 object detector. Given an input image x , the encoder maps it to a compact feature vector z where $C \in \{4, 8, 16\}$ is the channel dimension corresponding to compression ratios CH4, CH8, and CH16 respectively. The compressed feature is then corrupted by additive white Gaussian noise: $\hat{z} = z + n$, $n \sim N(0, \sigma^2 I)$ (1), where the noise variance σ^2 is determined by the target SNR level. The decoder D reconstructs a feature representation which is passed to the frozen YOLOv12 detector to produce bounding box predictions. For the traditional baseline, the raw image is JPEG-compressed, pixel values are directly corrupted by AWGN, and the noisy image is forwarded to YOLOv12 without any semantic encoding.

Supernet Architecture. Training three independent semantic encoders for CH4, CH8, and CH16 is computationally redundant. We therefore design a SupernetSemanticCodec that shares encoder and decoder backbone weights across all three sub-networks, differing only in the final channel projection layer[3,4]. Training is performed using the Sandwich Rule strategy: in each iteration, the largest sub-network ($K=16$), the smallest sub-network ($K=4$), and a randomly sampled intermediate sub-network ($K=8$) are each evaluated and their gradients accumulated before a single optimizer step. This ensures all sub-networks receive balanced gradient updates. The Supernet was trained for 50 epochs on an NVIDIA RTX 4090, completing training in approximately 53 minutes – the same wall-clock time as a single independent encoder.

Experiments. 1. Dataset and Setup: Experiments are conducted on a multi-class vehicle aerial image dataset containing 5,171 training images with annotations for cars, trucks, buses, SUVs, and motorcycles. Each semantic encoder is trained for 50 epochs. Evaluation is performed on a held-out validation set under five SNR conditions: {30, 20, 10, 5, 0} dB. Six metrics are reported: $mAP@0,5$, $mAP@0,5:0,95$, Precision, Recall, F1 Score, and Average Detection Count.

2. Semantic vs. Traditional Transmission: Figure 1 shows the $mAP@0,5$ curves for Traditional transmission and the three semantic encoders across SNR levels. The traditional method achieves the highest $mAP@0,5$ at 30 dB (0,511), but collapses sharply below 10 dB, reaching only 0,003 at 0 dB. In contrast, CH16 degrades gracefully, retaining 0,414 at 0 dB – a relative decrease of only 8,2% from its 30 dB performance (0,451).

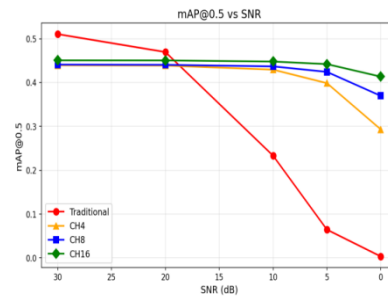


Figure 1 – mAP@0.5 vs SNR: Traditional vs semantic encoders (CH4/CH8/CH16)

Table 1 presents the complete quantitative evaluation. At 0 dB, CH16 achieves $mAP@0.5 = 0.414$ compared to Traditional 0.003, a 138 $\times$ improvement. CH8 and CH4 show progressively lower performance as the compression ratio increases.

Table 1 – Full evaluation results across SNR levels

Method	SNR(dB)	mAP@0.5	Prec.	Recall	F1
Traditional	30	0.511	0.713	0.852	0.776
Traditional	10	0.233	0.741	0.465	0.572
Traditional	0	0.003	0.787	0.009	0.018
CH16	30	0.451	0.718	0.802	0.758
CH16	10	0.448	0.721	0.798	0.757
CH16	0	0.414	0.721	0.758	0.739

3. Supernet vs. Independent Models: Figure 2 compares the Supernet sub-networks (dashed lines) against independently trained encoders (solid lines) across all SNR levels. Supernet_K16 tracks CH16_Indep closely, with a maximum gap of 1.4% at 0 dB (0.618 vs 0.627). Table 2 provides a focused comparison at 0 dB SNR. The Supernet replaces three independent models with one, at approximately 67% parameter cost reduction, with minimal performance degradation.

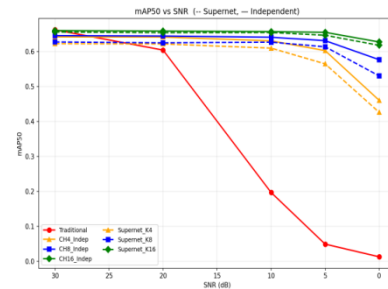


Figure 2 – mAP@0.5 vs SNR: Supernet sub-networks vs independent encoders

Table 2 – Comparison at 0 dB SNR: Supernet vs. independent encoders

Model	SNR(dB)	mAP@0.5	Prec.	Recall	F1
CH4_Indep	0	0.461	0.581	0.444	0.503
Supernet_K4	0	0.426	0.547	0.416	0.473
CH16_Indep	0	0.627	0.679	0.580	0.626
Supernet_K16	0	0.618	0.686	0.567	0.621

Conclusion. This paper presents a semantic communication system for vehicle detection that demonstrates strong robustness to AWGN channel noise. The proposed CNN semantic encoder (CH16) reduces $mAP@0.5$ degradation from 99.4% (Traditional) to 8.2% at 0 dB SNR. The Supernet architecture with Sandwich Rule training further consolidates three compression-ratio variants into a single model, with Supernet_K16 achieving only 1.4% lower $mAP@0.5$ than its independently trained counterpart at 0 dB. Future work will investigate adaptive compression ratio selection based on estimated channel quality, incorporation of attention mechanisms in the semantic encoder, and end-to-end joint optimization of the encoder-decoder-detector pipeline.

References:

1. Aoki T., Ohka S., Shiozawa D., Ogawa Y., Sakagami T. // *Engineering Proceedings*. 2019. Vol. 51. P. 44–55.
2. Hu Y., Xu L., Shen X., Jin L. // *Applied Optics*. 2021. Vol. 60. P. 9396–9403.
3. Wang D., Li Y., Pu Y. // *Sensors*. 2024. Vol. 24. P. 1307–1321.
4. Sun Y., Chen W., Li F., Gu Z., Feng L., Guo D. and Cai H. // *IEEE Transactions on Instrumentation and Measurement*. 2023 Feb. Vol. 72. P. 1–11.

COMPARISON OF DSO AND ORBSLAM3 IN INDOOR ENVIRONMENTS USING MONOCULAR VISUAL SLAM

Qiyao Yang

*Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus*

Jun Ma – Assistant

Abstract. This thesis presents a comparative study of ORB-SLAM3 and DSO in indoor environments. We first validate the local implementation on public datasets, then analyze self-recorded sequences from four perspectives: trajectory behavior, summary statistics, average per-frame runtime, and mapping visualization. The results show that ORB-SLAM3 is stronger in pose estimation and real-time efficiency, while DSO provides more informative semi-dense map appearance. Both methods degrade under low light and strong highlights, but with different failure modes, indicating clear complementarity. The study also notes key limitations, including the absence of ground truth for custom data, limited run repetitions, and acquisition choices that increase loop-closure difficulty. Future work will expand scene coverage and sample size, improve the evaluation protocol, and explore a hybrid framework that combines the strengths of both approaches. **Keywords:** semantic communication, vehicle detection, YOLOv12, CNN encoder, supernet, AWGN channel, compression ratio.

Keywords. DSO, ORB-SLAM3, monocular SLAM, indoor localization, photometric calibration, TUM RGB-D, EuRoC MAV, self-recorded data.

Introduction

Visual Simultaneous Localization and Mapping (SLAM) is a fundamental technology in robotics and computer vision that enables devices to estimate their ego-motion and simultaneously reconstruct the structure of unknown environments from image sequences [1]. It has found widespread applications in areas such as autonomous driving, indoor mobile robotics, augmented reality (AR), and virtual reality (VR). Among these, indoor environments are particularly important due to the growing demand for indoor robot navigation, warehouse automation, and AR-based indoor guidance systems. However, indoor scenes pose significant challenges for visual SLAM due to their diverse textures, varying illumination conditions, and potential dynamic objects [2].

Two prominent open-source visual SLAM systems are Direct Sparse Odometry (DSO) [3] and ORB-SLAM3 [4], representing direct and feature-based methods, respectively. DSO minimizes photometric errors without feature extraction, making it advantageous in low-texture or motion-blurred environments [3]. ORB-SLAM3 supports monocular, stereo, RGB-D, and visual-inertial modes, using ORB features for tracking, mapping, and loop closure to achieve high accuracy and robustness [4]. Their monocular versions are particularly attractive for low-cost and easy-to-deploy applications.

Experiments

To further characterize the computational cost of our self-collected sequences, we report the average per-frame tracking time of ORB-SLAM3 and DSO (mode = 0 / mode = 1) on the 509 and corridor scenarios under day and night illumination. The statistics show that ORB-SLAM3 remains near 8.3–9.2 ms per frame in all four conditions and is substantially faster than DSO; both DSO configurations span 19.2–28.9 ms per frame, i.e., roughly 2.5–3× the ORB-SLAM3 timings. This gap is consistent with the differing computational structures: DSO forms photometric residuals over many high-gradient samples inside a sliding window and performs iterative optimization, yielding a larger per-frame problem; ORB-SLAM3 relies mainly on feature extraction, matching, and comparatively light backend updates, and therefore exhibits lower time cost on our hardware and image-resolution settings.

Within DSO, mode = 1 is never faster than mode = 0 across all scenes; the largest gap appears on the corridor day sequence (≈ 25.0 ms/frame vs. 28.9 ms/frame), suggesting that disabling fixed photometric calibration and relying on online affine brightness compensation may increase the number of optimization variables or iterations and thus raise the average latency. Day–night changes barely affect ORB-SLAM3, whose curve is almost flat; DSO decreases to some extent at night on both 509 and the corridor, with a more pronounced drop on corridor night. This may reflect fewer reliable gradients under low light, changes in keyframe triggering, or a smaller active set of residuals in the window, shrinking each optimization step and lowering the per-frame average. Lower latency must not be equated with higher accuracy; interpretation should be combined with trajectory continuity, mapping density, and failure rates reported elsewhere.

Overall, the figure quantifies—in terms of wall-clock cost—the price of denser geometric and photometric modeling: ORB-SLAM3 is more lightweight per frame, whereas DSO trades higher per-frame cost for richer direct-map information, with mode = 0 slightly favoring average efficiency over mode = 1.

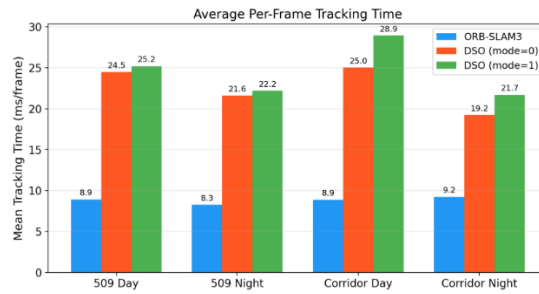


Figure 1 – Average Per-Frame Tracking Time of ORB-SLAM3 and DSO Under Different Scenarios

Table 3 – Five-time Average Measured Performance on Corridor Sequence

Metric	ORB-SLAM3 (Day/Night)	DSO mode=0 (Day/Night)	DSO mode=1 (Day/Night)
Input Frames	1805 / 1861	1804 / 1860	1804 / 1860
Output Poses	248 / 206	279 / 208	289 / 212
Average Points per Frame	212.4 / 214.3	2639.8 / 2631.0	2707.2 / 2667.9

Table 2 – Five-time Average Measured Performance on Classroom 509 Sequence

Metric	ORB-SLAM3 (Day/Night)	DSO mode=0 (Day/Night)	DSO mode=1 (Day/Night)
Input Frames	2302 / 1551	2301 / 1550	2301 / 1550
Output Poses	322 / 201	352 / 268	362 / 272
Average Points per Frame	252.1 / 218.7	2404.9 / 2065.1	2436.1 / 2035.0

Conclusion

The experiments first complete a baseline validation of the local implementation on public datasets, then turn to self-recorded sequences. This order gives the subsequent claims a clear traceability: the public benchmarks check that the pipeline, parameters, and runtime environment are sound; the custom sequences expose how the algorithms behave in realistic indoor settings. Following this protocol, the paper compares methods along four dimensions—trajectory shape, summary statistics, average per-frame time, and mapping visualization—to form a relatively complete evaluation framework.

On the self-recorded data, ORB-SLAM3 and DSO show a fairly clear division of roles. ORB-SLAM3 is overall stronger in pose estimation and trajectory stability: when illumination and texture are favorable, the estimated path aligns better with the actual motion and global consistency is easier to maintain. DSO tends to produce visually richer maps with more structural detail; its semi-dense output makes scene contours and local texture easier to perceive. Neither is free of failure modes: ORB-SLAM3 is more prone to tracking loss and map resets under night conditions and strong specular highlights; without loop closure, DSO can drift more noticeably and may also fail when facing very bright regions. The paper therefore does not frame the comparison as a simple winner–loser ranking, but as complementary strengths in localization robustness versus map interpretability.

In terms of computational cost, ORB-SLAM3's average per-frame tracking time is lower than DSO's throughout, consistent with the different front-end workload and optimization scales of feature-based and direct formulations. That suggests ORB-SLAM3 is more likely to meet tight latency budgets, whereas DSO trades higher per-frame cost for denser scene expression. Taken together with the trajectory and mapping results, system design should trade off localization stability, runtime, and map detail in a task-driven way rather than relying on a single score.

References:

1. Cadena C., Carlone L., Carrillo H. et al. // *IEEE Transactions on Robotics*. 2016. Vol. 32. P. 1309–1332.
2. Mur-Artal R., Tardós J. D. // *IEEE Transactions on Robotics*. 2017. Vol. 33. P. 1067–1080.
3. Engel J., Koltun V., Cremers D. // *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2018. Vol. 40. P. 184–197.
4. Mur-Artal R., Campos C. // *IEEE Transactions on Robotics*. 2021. Vol. 37. P. 1874–1890.

UAV-TO-SATELLITE IMAGE GEO-LOCALIZATION VIA DUAL-BRANCH DEEP LEARNING: A COMPARATIVE STUDY OF RESNET-18 AND MLP-MIXER

Qinghan Yu

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Jun Ma – Assistant

Abstract. UAV-to-satellite cross-view geo-localization is an important technology for autonomous navigation in GNSS-denied environments. However, large differences in viewpoint, scale, and distortion between UAV and satellite images make feature matching difficult. This paper presents a dual-branch deep learning framework and compares two backbone architectures, ResNet-18 and MLP-Mixer, under the same bidirectional InfoNCE training objective. Experiments on the UAV-Visloc dataset show that MLP-Mixer achieves better retrieval performance than ResNet-18, reaching Recall@1 of 74.09% versus 72.40%, with consistent improvements at Recall@5 and Recall@10. Ablation results further show that independent branches are important for handling the domain gap between UAV and satellite imagery. The results indicate that pure MLP architectures have strong potential for cross-view geo-localization when combined with contrastive learning.

Keywords. Cross-view geo-localization, UAV-satellite images, ResNet-18, MLP-Mixer, contrastive learning.

Introduction

UAV-to-satellite cross-view geo-localization provides an effective solution for positioning in GNSS-denied environments by matching low-altitude UAV images with high-altitude satellite images. This task is challenging because the two views differ significantly in perspective, scale, rotation, and visual appearance. Although CNN-based and Transformer-based methods have been widely studied, pure MLP architectures remain less explored in this scenario.

In this paper, we adopt a dual-branch framework for UAV-satellite image matching and compare two representative backbone networks, ResNet-18 and MLP-Mixer, under the same contrastive learning setting. The goal is to evaluate their retrieval accuracy and analyze whether pure MLP architectures can serve as competitive alternatives to CNNs in cross-view geo-localization. Experimental results show that MLP-Mixer consistently outperforms ResNet-18 on the UAV-Visloc dataset.

Method

The proposed framework uses two independent branches to process UAV and satellite images separately, which helps address the large domain gap between the two views. Each branch employs either ResNet-18 or MLP-Mixer as the feature extractor. The extracted features are then passed through a projection head to generate 256-dimensional normalized embeddings.

$$\mathcal{L}_{d \rightarrow s} = -\frac{1}{B} \sum_{i=1}^B \log \frac{\exp(\mathbf{z}_{d,i}^\top \mathbf{z}_{s,i} / \tau)}{\sum_{j=1}^B \exp(\mathbf{z}_{d,i}^\top \mathbf{z}_{s,j} / \tau)}$$

The model is trained using bidirectional InfoNCE loss, which pulls matched UAV-satellite pairs closer in the embedding space while pushing unmatched pairs apart. During inference, cosine similarity is computed between the UAV query embedding and all satellite gallery embeddings, and the gallery images are ranked according to similarity. Retrieval performance is evaluated by Recall@1, Recall@5, and Recall@10.

Experiments

Experiments are conducted on the UAV-Visloc dataset containing 768 UAV-satellite image pairs. The dataset is split into 80% training and 20% validation using a fixed random seed. All models are trained for 80 epochs with the AdamW optimizer. The embedding dimension is set to 256, and retrieval performance is measured by Recall@1, Recall@5, and Recall@10.

The main comparison results are shown in Table 1. MLP-Mixer achieves better performance than ResNet-18 across all evaluation metrics. In particular, MLP-Mixer improves Recall@1 from 72.40% to 74.09%, Recall@5 from 87.50% to 88.41%, and Recall@10 from 90.49% to 92.45%. These results suggest that the global token-mixing mechanism of MLP-Mixer is effective for modeling spatial correspondences between UAV and satellite views.

Table 1

Model	R@1	R@5	R@10
ResNet-18 (Baseline)	72,40%	87,50%	90,49%
MLP-Mixer (Baseline)	74,09%	88,41%	92,45%

To validate the importance of the dual-branch design, we further compare independent branches with shared weights. The results in Table 2 show that independent branches are clearly more effective, especially for ResNet-18. When shared weights are used, ResNet-18 drops from 72.40% to 49.35% in Recall@1, indicating that forcing UAV and satellite images into a single feature extractor significantly reduces retrieval performance. Although MLP-Mixer is less sensitive to weight sharing, the independent-branch setting still gives the best result. This confirms that separate feature extraction pathways are necessary for handling the domain gap between the two image modalities.

Table 2

Model	Independent Branches	Shared Weights	$\Delta R@1$
ResNet-18	72,40%	49,35%	-23,05%
MLP-Mixer	74,09%	72,79%	-1,30%

Visualization

This advantage is also reflected in qualitative retrieval results. As shown in Figure 1, MLP-Mixer more consistently ranks the correct satellite image at the top positions, whereas ResNet-18 is more likely to confuse visually similar but geographically different locations. These examples demonstrate that MLP-Mixer learns more discriminative representations for practical cross-view retrieval.

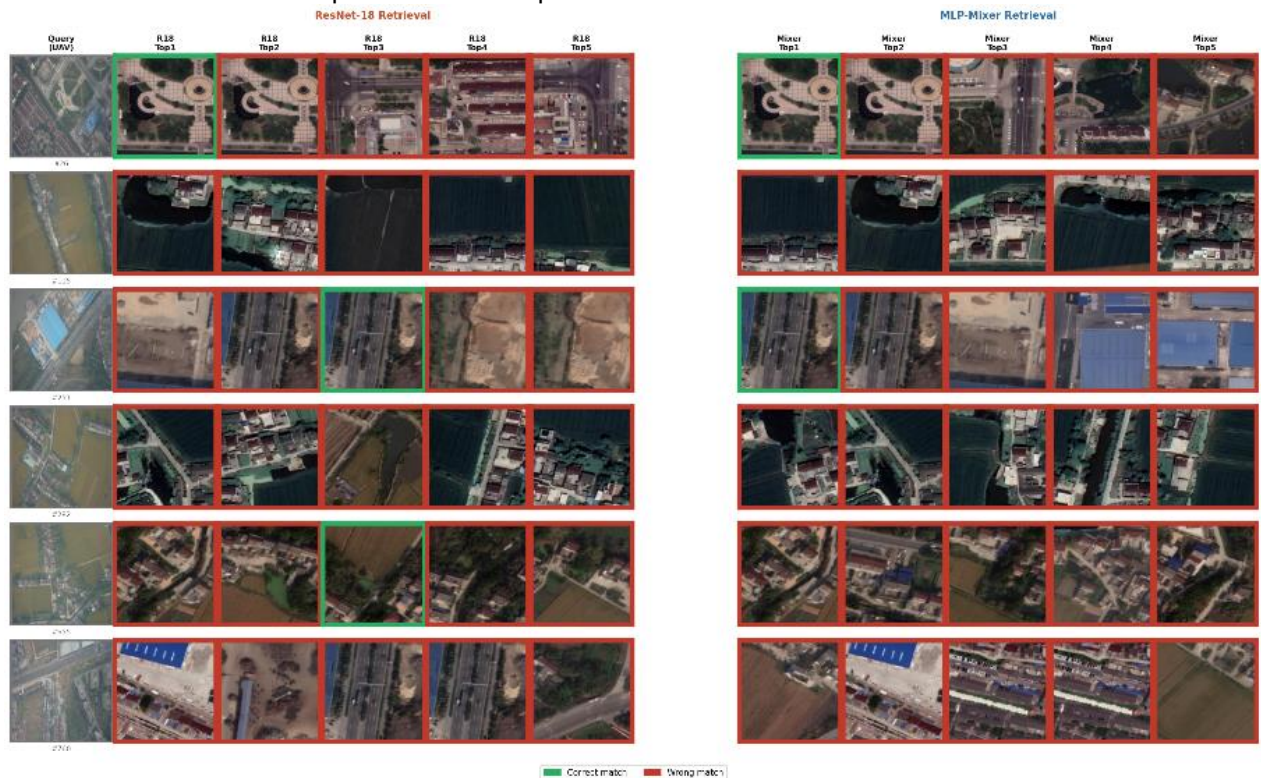


Figure 1 – The visualization results

Conclusion

This paper presents a compact comparative study of ResNet-18 and MLP-Mixer for UAV-to-satellite cross-view geo-localization under a dual-branch contrastive learning framework. Experimental results show that MLP-Mixer achieves consistently better retrieval performance than ResNet-18 on the UAV-Visloc dataset. In addition, the ablation study demonstrates that independent branches are essential for effective cross-view matching. These findings indicate that pure MLP architectures are promising for UAV-satellite geo-localization and deserve further investigation in larger-scale and more diverse datasets.

References:

- 1 K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, Las Vegas, NV, USA, 2016, pp. 770–778.
- 2 I. Tolstikhin, N. Houlsby, A. Kolesnikov, L. Beyer, X. Zhai, T. Unterthiner, J. Yung, A. Steiner, D. Keysers, J. Uszkoreit, M. Lucic, and A. Dosovitskiy, "MLP-Mixer: An all-MLP architecture for vision," in *Advances in Neural Information Processing Systems (NeurIPS)*, vol. 34, 2021, pp. 24261–24272.
- 3 T. Chen, S. Kornblith, M. Norouzi, and G. Hinton, "A simple framework for contrastive learning of visual representations," in *Proc. Int. Conf. Machine Learning (ICML)*, vol. 119, 2020, pp. 1597–1607.
- 4 Y. Shi, L. Liu, X. Yu, and H. Li, "Spatial-aware feature aggregation for image based cross-view geo-localization," in *Advances in Neural Information Processing Systems (NeurIPS)*, vol. 32, 2019, pp. 10090–10100.
- 5 S. Zhu, M. Shah, and C. Chen, "TransGeo: Transformer is all you need for cross-view image geo-localization," in *Proc. IEEE/CVF Conf. Computer Vision and Pattern Recognition (CVPR)*, 2022, pp. 1162–1171.
- 6 Z. Zheng, Y. Wei, and Y. Yang, "University-1652: A multi-view multi-source benchmark for drone-based geo-localization," in *Proc. ACM Int. Conf. Multimedia (ACM MM)*, 2020, pp. 1395–1403.

A COMPARATIVE STUDY OF ERROR-CORRECTING CODES FOR MULTI-CELL UPSETS IN MEMORIES: CLC AND OPCOSA

Lin Wei

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Jun Ma – assistant

Annotation. With semiconductor scaling, memories are more vulnerable to radiation-induced Multiple Cell Upsets (MCU). This paper compares two 2D error-correcting codes: CLC and OPCoSA. It analyzes their coding structures and evaluates error correction ability, hardware overhead, and reliability via synthesis and fault injection. Experiments show CLC has moderate cost and decent performance. OPCoSA optimizes redundancy to cut hardware overhead while keeping strong correction. This study helps choose suitable ECCs for space memories under resource and reliability constraints.

Keywords. Matrix ECC, PCoSA, CLC and OPCoSA Algorithms.

Error Correction Code Principles and Structures: It is a two-dimensional matrix ECC that arranges data and redundant bits in rows and columns. Taking CLC (16,40) as an example, 16 data bits form a 4×4 matrix. An (8,4) extended Hamming code is applied row-wise to generate check and parity bits, and column parity is computed to form a 40-bit codeword [1]. This structure supports single-bit and multi-bit error correction. CLC includes variants (16,39) and (16,54) and supports Standard and Extended modes [2]. This work focuses on CLC (16,40). OPCoSA is an optimized product code derived from PCoSA [3, 4]. It arranges 16 data bits in a matrix and applies extended Hamming codes to both rows and columns to generate check and parity bits. Compared with PCoSA, OPCoSA removes the parity-on-parity region, shortening the codeword to 48 bits with 32 redundant bits, reducing redundancy by 33%. Although the minimum Hamming distance decreases to 7, the decoding algorithm still ensures strong MCU correction [3].

Experimental Setup: Hardware Implementation Gate-level circuits of CLC (16,40) and OPCoSA (48,16) are implemented in Logisim, including encoder, decoder, Hamming code modules, error injection, and correction output units. The results as show in Figures 1. Designs are then translated to Verilog and implemented on Xilinx Virtex-7 XC7V485TFFG1157-1 (28 nm CMOS) in Vivado. Error Correction Evaluation Fault injection is performed to simulate 1–8 adjacent errors to mimic MCU. Monte Carlo simulations are run for each pattern, and correction rates are counted under identical conditions for fairness. Hardware Overhead Metrics Overhead is evaluated using Vivado synthesis and power analysis: Resource utilization: Slice LUTs, registers, IOBs, BUFGCTRL, Power: total on-chip power, dynamic power, static power, Thermal parameters: junction temperature, thermal resistance, margin.

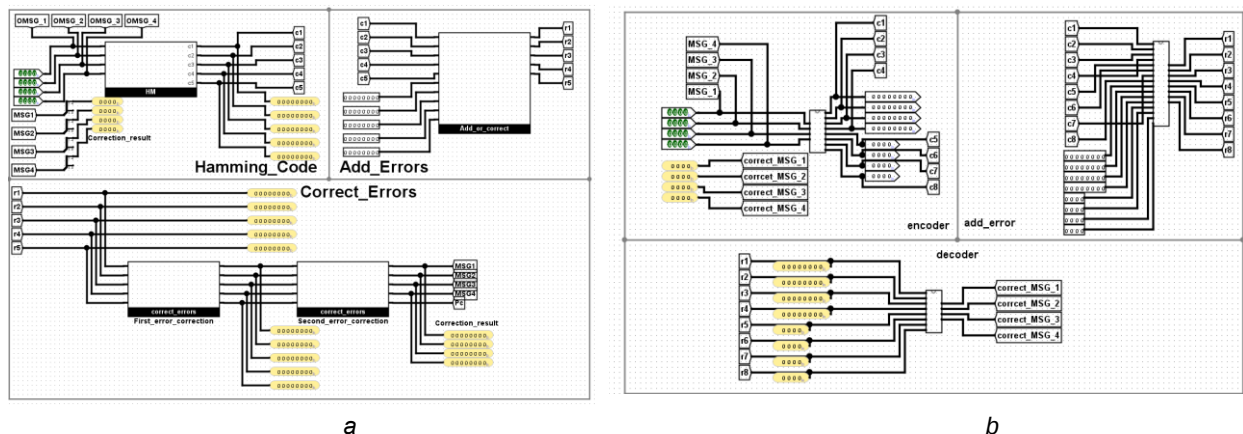


Figure 1 – Gate - level circuit schematic of the algorithm: a – gate - level circuit implementation of CLC; b – gate - level circuit implementation of OPCoSA

Results and Discussion: Error Correction Capability Both codes achieve 100% correction for 1–3 bit errors. At 4-bit errors, OPCoSA remains 100% while CLC drops to 48.69%. For 5-bit and 6-bit errors, OPCoSA reaches 53% and 35%, outperforming CLC (33.58%, 22.58%). OPCoSA supports full-codeword error correction, while CLC only corrects within information bits. **Special Error Scenarios** In ≤4-bit burst errors, OPCoSA corrects 100% vs. 75.5% for CLC. For >4-bit bursts, OPCoSA achieves 44% vs. 24% for CLC. In 36 typical space radiation patterns and 3×3 MCU mode, OPCoSA corrects 100% of errors, while CLC reaches only 75%–78%. **Hardware Overhead** CLC uses 752 LUTs, 251 registers, and 5.2 W. OPCoSA uses 1454 LUTs, 475 registers, and 7.6 W, approximately twice the overhead. The difference comes from longer codewords and more complex decoding. Experimental results as shown in Figures 2. and Figures 3.

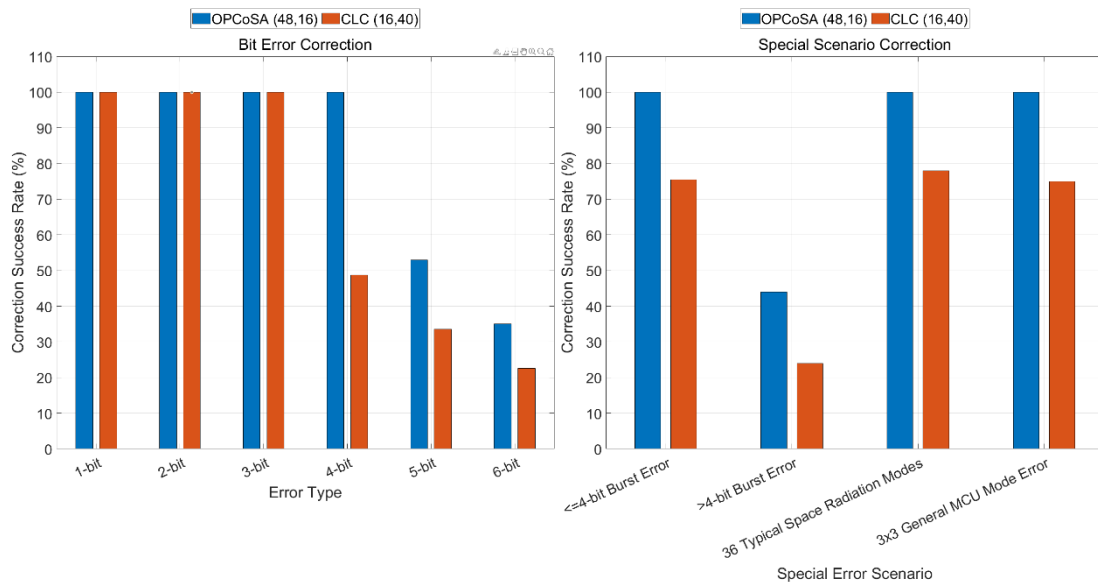


Figure 2 – Comparison of Error Correction Rates (%) Between CLC and OPCoSA Algorithms

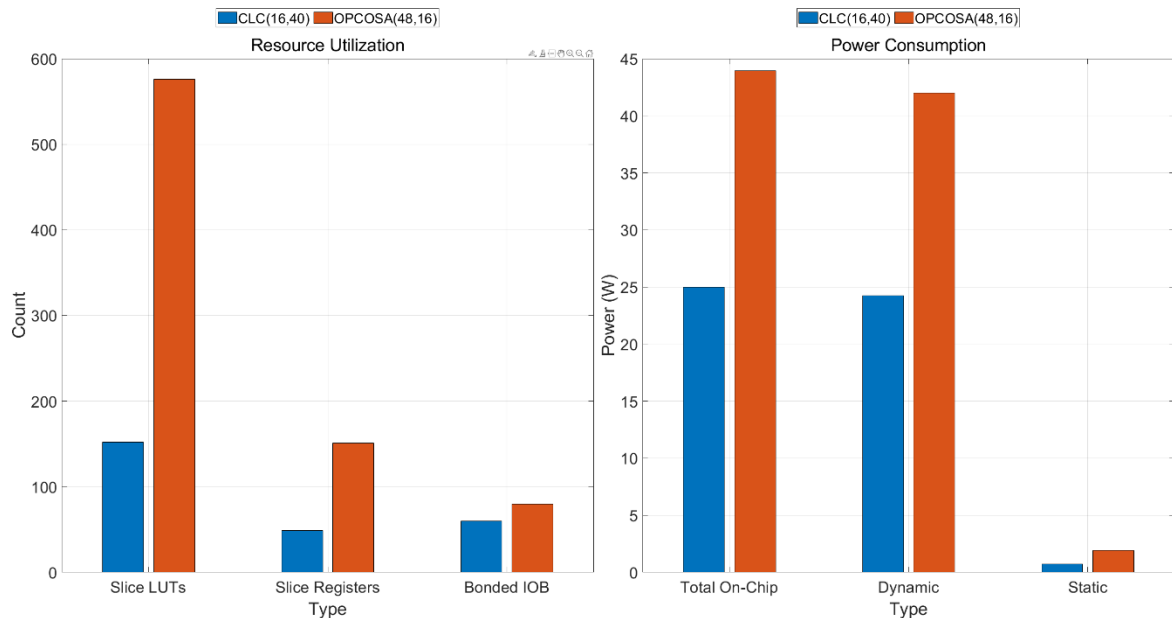


Figure 3 – Comparison of Hardware Overhead Between CLC and OPCoSA Algorithms

Conclusion: OPCoSA are both effective 2D ECCs for MCU mitigation. CLC provides low hardware cost and is suitable for resource-constrained systems with small MCU errors. OPCoSA delivers significantly stronger correction under 4-bit and complex multi-bit errors, supports full-codeword protection, and is more robust for high-reliability space applications despite higher overhead. Limitations include simplified fault injection, 28 nm FPGA only, and no voltage/temperature variation. Future work will extend evaluation to real radiation environments and advanced processes.

References:

1. H. Castro, J. Silveira, A. Coelho, F. Silva, P. Magalhaes, and O. Lima, "A correction code for multiple cells upset in memory devices for space applications," in *Proc. IEEE Int. New Circuits Syst. Conf. (NEWCAS)*, 2016, pp. 1–4.
2. F. Silva, J. Silveira, C. Marcon, F. Vargas, and O. Lima Jr., "An Extensible Code for Correcting Multiple Cell Upset in Memory Arrays," *J. Electron. Test.*, vol. 34, no. 4, pp. 417–433, Aug. 2018.
3. D. Freitas, J. Silveira, C. Marcon, L. Naviner, and J. Mota, "OPCoSA: an Optimized Product Code for space applications," *Microelectron. Reliab.*, vol. 128, art. no. 114430, 2022.
4. D. Freitas et al., "PCoSA: A Product Code for Space Applications".

A REVIEW OF COLLABORATIVE OPTIMIZATION OF TASK ALLOCATION AND PATH PLANNING IN MULTI-ROBOT SYSTEMS

Xinyue Shao

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Jun Ma – Assistant

Abstract. Multi-robot systems are widely used in intelligent manufacturing, smart logistics and unmanned systems with high robustness and parallel operation capability. Task allocation and path planning are the core of collaborative decision-making, but their joint optimization is challenged by dynamic environments, communication constraints and heterogeneous conflicts. This paper defines the Co-MAPF problem, compares three system architectures, classifies mainstream algorithms, and summarizes the development trend of collaborative optimization for multi-robot systems.

Keywords. Multi-robot systems; Task allocation; Path planning; Collaborative optimization; Communication constraints; Deep reinforcement learning

Introduction

Multi-robot systems are key to meeting the requirements of large-scale, high-precision operations in aerospace, smart warehousing and urban inspection [1 – 3]. The core of collaboration lies in task allocation and path planning. Early sequential “allocate-then-plan” methods lead to suboptimal solutions and deadlock [4]. In recent years, joint optimization of task allocation and path planning has become a research hotspot. This paper systematically reviews collaborative optimization technologies, and clarifies the research status and development characteristics of this field.

Problem Definition

Collaborative Multi-Agent Path Finding (Co-MAPF) extends the classical MAPF by integrating task allocation. The workspace is represented as an undirected graph $G = (V, E)$, and the agent set $A = \{a_1, \dots, a_k\}$ corresponds to tasks τ_i with start s_i and goal g_i . The optimization objectives include total makespan, energy consumption and number of completed tasks. Co-MAPF realizes active collaboration instead of passive collision avoidance, emphasizing real-time interaction and dynamic decision-making.

System Architectures

Multi-robot systems adopt centralized, distributed and hybrid architectures, as shown in Table 1.

Table 1 – Comparison of three system architectures

Architecture Type	Advantages	Disadvantages	Applicable Scenarios
Centralized	Global optimal, high path quality	High computation, single point failure	Small-scale static systems
Distributed	Strong robustness, good scalability	Local optima, complex protocols	Large-scale dynamic swarms
Hybrid	Balance optimality and flexibility	Complex interfaces, communication bottlenecks	Large-scale complex tasks

Search-Based Algorithms

Typical algorithms include HCA*, CO-WHCA* and CBS. CBS uses high-level conflict management and low-level path planning to ensure optimality, but computational complexity grows exponentially with the number of agents. TC-CBS enhances the coupling of task allocation and path planning.

Sampling-Based Algorithms

RRT, PRM and Multi-RRT* are suitable for high-dimensional spaces. They support distributed asynchronous planning and reduce centralized computation load, but path quality and convergence speed are uncertain.

Intelligent Optimization Algorithms

Genetic algorithm, PSO and ACO solve nonlinear multi-objective problems. DAC-GA and AFSA-PSO balance global convergence and local search, but require parameter tuning and have high computation costs.

Learning-Based Algorithms

Deep reinforcement learning (DRL) and graph neural networks (GNN) adapt to dynamic environments. The CTDE framework realizes centralized training and decentralized execution. GNN improves communication efficiency and handles dynamic topology.

Communication-Aware Joint Optimization

Communication constraints (bandwidth, delay, packet loss) are integrated into the planning model. “Task-Control-Communication” co-design couples trajectory planning and communication optimization, improving system robustness under limited bandwidth.

Conclusion

Task allocation and path planning are developing from separate design to deep joint optimization. The research field has formed a complete technical system including problem modeling, architecture design and algorithm implementation. Centralized, distributed and hybrid architectures adapt to different application scenarios, while search-based, sampling-based, intelligent optimization, learning-based and communication-aware algorithms provide effective solutions for collaborative optimization. The continuous integration of communication, control and artificial intelligence will further promote the practical application of multi-robot collaborative systems in complex real-world scenarios.

Core Challenges

1. Trade-off between real-time performance and algorithm scalability.
2. Adaptive capacity to dynamic environments and uncertainties.
3. Collaborative robustness under communication constraints.
4. Efficient deep coupling mechanism for task allocation and path planning.
5. Coordination of heterogeneous robots and large-scale swarms.

References:

1. Xiong J, Zhang W, Xiong Z, et al. *Journal of System Simulation*, 2025, 37(12): 3033 – 3049.
2. Zhang Z, Mao J, Tan H. *Acta Automatica Sinica*, 2024, 50(1): 21 – 41.
3. D'Andrea R. *IEEE Transactions on Automation Science and Engineering*, 2012, 9(4): 638 – 639.
4. Greshler N, Gordon O, Salzman O. *2021 International Symposium on Multi-Robot and Multi-Agent Systems, IEEE*, 2021: 20 – 28.

ARTIFICIAL NOISE AIDED PHYSICAL LAYER SECURITY FOR LEO SATELLITE COMMUNICATIONS

Can Wang

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Jun Ma – Assistant

Abstract. Low Earth Orbit (LEO) satellite communications are vulnerable to eavesdropping over open wireless links. This paper proposes a simplified artificial noise (AN)-aided physical layer security scheme. A system model with a multi-antenna LEO satellite, a single-antenna ground user, and multiple eavesdroppers is built under shadowed-Rician fading and imperfect channel state information. AN is projected into the null space of the legitimate channel to avoid interference, and fixed power allocation is adopted for low complexity. Simulations show the scheme achieves better secrecy rate and secrecy outage probability than traditional methods, suitable for resource-constrained LEO satellite systems.

Keywords: LEO satellite communication; physical layer security; artificial noise; null space projection; power allocation.

Introduction

LEO satellite networks provide low-latency global coverage but are vulnerable to eavesdropping. Traditional encryption is impractical due to limited on-board resources [1, 2]. Physical layer security (PLS) using artificial noise can achieve secure transmission without complex key management [3]. However, existing AN schemes are overly complex for LEO platforms [4]. This paper presents a low-complexity AN-aided PLS scheme for LEO satellites.

System Model

The system consists of a 4-antenna LEO satellite, a single-antenna ground user, and two single-antenna eavesdroppers. Channels follow shadowed-Rician fading with imperfect channel state information:

$$\widehat{h}_b = h_b + e, \sigma_e^2 = 0.01 \quad (1)$$

The transmitted signal is expressed as:

$$\mathbf{x} = \mathbf{w}s + \mathbf{v}n \quad (2)$$

where s is the information symbol, $\mathbf{w}$ is the MRT beamforming vector, n is the artificial noise, and $\mathbf{v}$ is the AN vector orthogonal to the legitimate channel.

Artificial Noise Scheme Design. Null Space AN Generation: The AN vector $\mathbf{v}$ is constructed in the null space of $\widehat{\mathbf{h}}_b$, satisfying $\widehat{\mathbf{h}}_b^H \mathbf{v} = 0$. For 4 transmit antennas, the null space has 3 dimensions:

$$\mathbf{v} = \mathbf{U}_{null} \mathbf{u} \quad (3)$$

where $\mathbf{U}_{null}$ is the null space matrix of $\widehat{\mathbf{h}}_b$, and $\mathbf{u}$ is a random vector.

Power Allocation: Total satellite power constraint: $\|\mathbf{w}\|^2 + \|\mathbf{v}\|^2 \leq P_{max}$. Fixed power allocation ($\alpha = 0.5$):

$$\|\mathbf{w}\|^2 = 0.5P_{max}, \|\mathbf{v}\|^2 = 0.5P_{max} \quad (4)$$

This strategy ensures low computational complexity and easy implementation.

Performance Evaluation

The main metrics are secrecy rate and SOP. Simulation parameters: LEO altitude 1000 km, $P_{max}=23$ dBm, carrier frequency 2 GHz.

Table 1 – Simulation parameters

Parameter	Value
LEO altitude	1000 km
P_{max}	23 dBm
Carrier frequency	2 GHz
Noise spectral density	-174 dBm/Hz

The proposed scheme is compared with “Traditional AN” and “No AN”. Results (Fig. 1) show it achieves higher secrecy rate and lower SOP with lower computational cost.

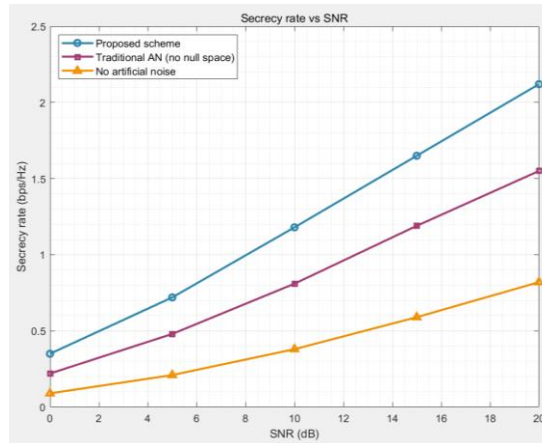


Figure 1 – Secrecy rate vs SNR

The secrecy outage probability (SOP) performance of the three schemes is presented in Figure 2.

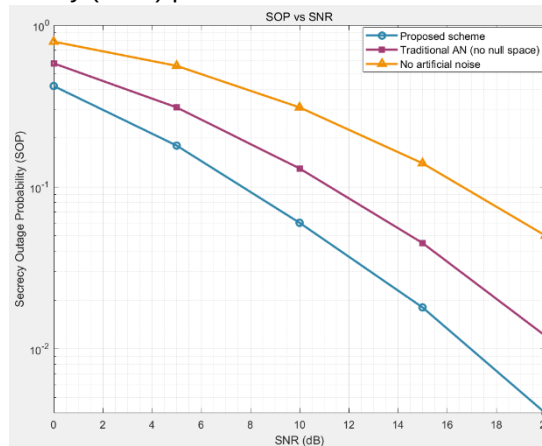


Figure 2 – SOP vs SNR

As shown in the figures, the proposed scheme achieves the highest secrecy rate across all SNR values and the lowest SOP, outperforming both traditional AN and no-AN baselines. The fixed power allocation ensures low computational complexity, making the scheme suitable for resource-constrained LEO satellite systems.

Conclusion

This paper proposes a simplified artificial noise-aided physical layer security scheme suitable for LEO satellite communications. Aiming at the problems of limited resources and vulnerable eavesdropping of open wireless links in LEO satellites, the scheme projects artificial noise into the null space of the legitimate user's channel, which can effectively suppress eavesdroppers while avoiding interference to legitimate communications. Meanwhile, a fixed power allocation strategy is adopted to simplify the implementation process of the scheme, which significantly improves the physical layer security of communication links on the premise of ensuring low computational complexity. Simulation results verify the performance superiority of the proposed scheme over the traditional schemes without artificial noise and with artificial noise without null space projection from two core indicators of secrecy rate and secrecy outage probability. The scheme can be effectively adapted to resource-constrained LEO satellite communication systems and has good engineering application value.

References:

1. Niu H. et al. // 2025.
2. Kim S. H., Lee J. W., Lee I. T. // *Proc. IEEE Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*. 2024. P. 112–116.
3. Kumar R., Arnon S. // *Electronics*. 2024. Vol. 13. No. 22. doi: 10.3390/electronics13224414.
4. Talgat A., Wang R., Kishk M. A., Alouini M.-S. // 2024.

PERFORMANCE ANALYSIS OF LS AND LMMSE CHANNEL ESTIMATION FOR 5G NR OFDM SYSTEMS OVER TIME-VARYING FADING CHANNELS

Shuo Wang

Belarusian State University of Informatics and Radioelectronics Minsk, Republic of Belarus

Jun Ma – Assistant

Abstract. Accurate and efficient acquisition of Channel State Information (CSI) is crucial for reliable data transmission using Orthogonal Frequency Division Multiplexing (OFDM) in 5G NR (New Radio) systems. Focusing on the 5G NR physical layer standards, this paper constructs a complete OFDM baseband transmission link and conducts an in-depth performance comparison and theoretical analysis of block pilot-based Least Squares (LS) and Linear Minimum Mean Square Error (LMMSE) channel estimation algorithms. A first-order autoregressive (AR1) model is employed to simulate slow and fast fading environments at different mobility speeds. A strictly discrete frequency-domain autocorrelation matrix is derived to address the errors of continuous integral approximation in traditional LMMSE.

Keywords. OFDM; Channel Estimation; LMMSE; Time-domain Linear Interpolation; Time-varying Fading.

Introduction

The OFDM is the core modulation technology for 5G NR downlink, and it is highly sensitive to CSI accuracy. Pilot symbol insertion enables CSI acquisition, while traditional LS estimation is simple but susceptible to Additive White Gaussian Noise (AWGN). The LMMSE algorithm achieves optimal frequency-domain smoothing using second-order channel statistics with higher complexity and reliance on accurate autocorrelation matrix. This paper focuses on performance comparison of LS and LMMSE under time-varying fading channels, and verifies the effectiveness of time-domain linear interpolation for fast fading channel tracking.

System Model

A 5G NR-compliant OFDM baseband transmission system is constructed. At the transmitter, input bit stream is 16-QAM modulated, mapped onto N_{fft} orthogonal subcarriers with block pilots, and transformed to time domain via IFFT. Cyclic Prefix (CP) is appended to mitigate Intersymbol Interference (ISI). At the receiver, CP is removed and FFT is performed after synchronization, with frequency-domain received signal obtained on each subcarrier.

A first-order autoregressive (AR1) model is adopted to generate time-varying multipath Rayleigh fading channel for different terminal mobility speeds. The time-domain channel impulse response h_t for each OFDM symbol is expressed as: $h_t = \alpha h_{t-1} + \sqrt{1 - \alpha^2} \cdot w_t$, where w_t is independent complex Gaussian random process, and α is time correlation coefficient affected by terminal mobility speed (Doppler shift). ($\alpha=1$) represents slow fading (block fading), while $\alpha=0.985$ represents fast fading with significant channel variation within a single Slot.

Pilot Structure Design Common OFDM pilot patterns include Block Pilot, Comb Pilot and Lattice Pilot (Scattered Pilot). Block pilot structure is adopted in this simulation to adapt to 5G NR Slot format (14 symbols per Slot). Pilots are inserted at the 1st and 8th symbol positions to enable effective tracking of time-varying channels in subsequent processing, which provides anchor points for channel estimation and interpolation.

Channel Estimation Algorithms

The LS algorithm aims to minimize the squared error between received signal and expected signal. At block pilot positions, the frequency-domain channel response estimated by LS can be directly obtained via zero-forcing formula, which features low complexity and easy implementation but poor anti-noise performance due to direct AWGN propagation.

Based on LS estimation, LMMSE algorithm uses channel frequency-domain autocorrelation matrix R_{hh} and system noise variance to smooth estimates via Wiener Filtering, with its weight matrix designed for optimal estimation. Traditional R_{hh} adopts integral approximation with continuous power delay profile, which has mismatch with actual discrete FFT sampling.

A strictly discrete correlation formula is derived based on discrete uniform multipath power distribution to eliminate the approximation error. For arbitrary subcarriers, the elements of discrete autocorrelation matrix are calculated with accurate discrete frequency-domain correlation characteristics, which improves the estimation accuracy of LMMSE algorithm.

Sample-and-hold strategy suffices for slow fading, while fast fading causes severe Channel Aging. Time-domain linear interpolation is employed for fast fading scenarios: using estimates from the 1st and 8th pilot symbols, intermediate data symbols are interpolated and the 9th to 14th symbols are extrapolated, recovering the entire slot's time-varying channel matrix to track dynamic channel changes.

Table 1 – 5G NR OFDM Simulation Parameter Settings

Parameter Name	Parameter Value
FFT Size (N_{fft})	512
Cyclic Prefix Length (N_{cp})	22
Number of Symbols per Slot (N_{sym})	14
Modulation Scheme	16-QAM / QPSK
Pilot Position (Symbol Index)	1, 8
Maximum Multipath Delay (τ_{max})	16

Algorithm Performance Evaluation

In slow fading environment, the channel remains static within a Slot. LMMSE algorithm significantly outperforms traditional LS algorithm in MSE across the entire SNR range, reducing estimation error by approximately one order of magnitude in low SNR region. LS is susceptible to AWGN contamination, while LMMSE exploits the low-rank nature of frequency-domain autocorrelation matrix to achieve optimal smoothing and noise suppression.

In BER performance, LMMSE maintains stable parallel gain in medium-to-high SNR region. The BER convergence in extremely low SNR is caused by system "ceiling effect", where background white noise on data symbols dominates total error and masks the gain from improved channel estimation.

Two typical fast fading scenarios are simulated: quasi-static/low-speed fading ($\alpha=0.999$) and high-mobility fast fading ($\alpha=0.985$). For low-speed fast fading, channel evolution within one slot is extremely slow, and time-domain linear interpolation can fit the minor linear drift with high precision. BER of both LS+Interpolation and LMMSE+Interpolation schemes decreases continuously with increasing SNR without obvious Error Floor, with LMMSE gaining better performance from excellent subspace noise reduction at pilot anchor points.

For high-mobility fast fading (highway/high-speed rail environments), BER curves stop descending and fall into severe error floor effect when SNR exceeds 20 dB. The root cause is the geometric mismatch of interpolation model: AR1 channel model causes drastic nonlinear fluctuations between pilot intervals, and first-order linear interpolation can only depict macroscopic linear trends, incapable of tracking high-frequency random fluctuations. In high SNR region, "nonlinear interpolation residual" becomes the dominant interference source that cannot be eliminated by increasing transmission power.

Conclusion

Targeting 5G NR standard, this paper evaluates LS and LMMSE channel estimation algorithms based on block pilot architecture for OFDM systems over time-varying fading channels. By adopting strictly discrete autocorrelation matrix, LMMSE algorithm comprehensively outperforms LS in MSE due to excellent subspace noise reduction capability, and provides stable parallel BER gain in medium-to-high SNR region. The low-SNR BER convergence of both algorithms is driven by the system-level ceiling effect of data symbol background noise.

Time-domain linear interpolation is highly effective for quasi-static and low-speed fading environments, but fails to track drastic nonlinear channel fluctuations in high-mobility fast fading scenarios, resulting in severe high-SNR error floor. These findings indicate the necessity of dynamic DMRS configurations in 5G networks: for extreme mobility scenarios, denser time-domain pilot structures (e.g., comb pilots) or higher-order dynamic tracking algorithms (e.g., Kalman filtering) should be adopted by sacrificing partial spectral efficiency to break through the physical limit of linear interpolation.

References:

1. 3GPP. NR; Physical channels and modulation. 3GPP TS 38.211 version 15.2.0 Release 15, 2018.
2. Edfors O., Sandell M., Van de Beek J. J. // IEEE Transactions on Communications. 1998. Vol. 46. P. 931–939.
3. Coleri S., Ergen M., Puri A. // IEEE Transactions on Broadcasting. 2002. Vol. 48. P. 223–229.
4. Proakis J. G., Salehi M. Digital Communications. McGraw-Hill, 2008.
5. Zhou E., Zhao Z. Research on Channel Estimation Algorithms in Broadband Mobile Communication Systems. Beijing: Publishing House of Electronics Industry, 2012.
6. Lin J. Research on Channel Estimation Technology for OFDM System and Exploration of the LS algorithm Implementation. Master's thesis, Beijing Jiao tong University, 2020

UDC621.391

MULTI-SENSOR FUSION FOR MOBILE ROBOT PERCEPTION

Bin Zhang, student gr.363411

Belarusian State University of Informatics and Radioelectronics¹, Minsk, Republic of Belarus

Jun Ma – Assistant

Annotation. This paper presents a multi-sensor fusion perception system to overcome key limitations of single-line LiDAR in mobile robots, including pose drift, vertical blind zones, and poor robustness against transparent surfaces or sensor failures. The proposed architecture integrates LiDAR-IMU tightly-coupled odometry, RGB-D camera-based 3D mapping using ORB-SLAM2, and ultrasonic near-field detection. The design is expected to improve positioning accuracy and environmental awareness in indoor scenarios. The work is currently at the design phase, with physical implementation planned for future research.

Keywords. 2D LiDAR, Raspberry Pi, Obstacle Avoidance, Indoor Mobile Robot, LiDAR SLAM.

Introduction

With the rapid development of AI and sensor technologies, mobile robots have expanded from industrial automation to healthcare, logistics, and domestic service [1]. LiDAR has become a core navigation sensor due to its high accuracy and fast response [2]. Within ROS2 [3], low-cost mobile robot development has become a research hotspot. Single-line LiDAR offers high accuracy, good real-time performance, and low cost. However, relying solely on it for both obstacle avoidance and mapping presents several limitations. First, it only obtains 2D planar information, missing low-height or suspended obstacles, and has a near-field blind zone. Second, pure LiDAR odometry lacks motion priors, making it prone to pose drift during rapid motion. Third, it has blind zones for glass and mirrors, struggles with dynamic objects, and suffers from single points of failure. To validate these limitations, a distributed control platform with upper and lower computers was constructed. The upper computer (Raspberry Pi 4B, ROS2 Humble) handles LiDAR data, obstacle avoidance, and visualization. The lower computer (Arduino Uno) receives speed commands, performs inverse kinematics for Mecanum wheels, and controls four DC motors via an L293D driver module. Figure 1 shows the system hardware architecture.

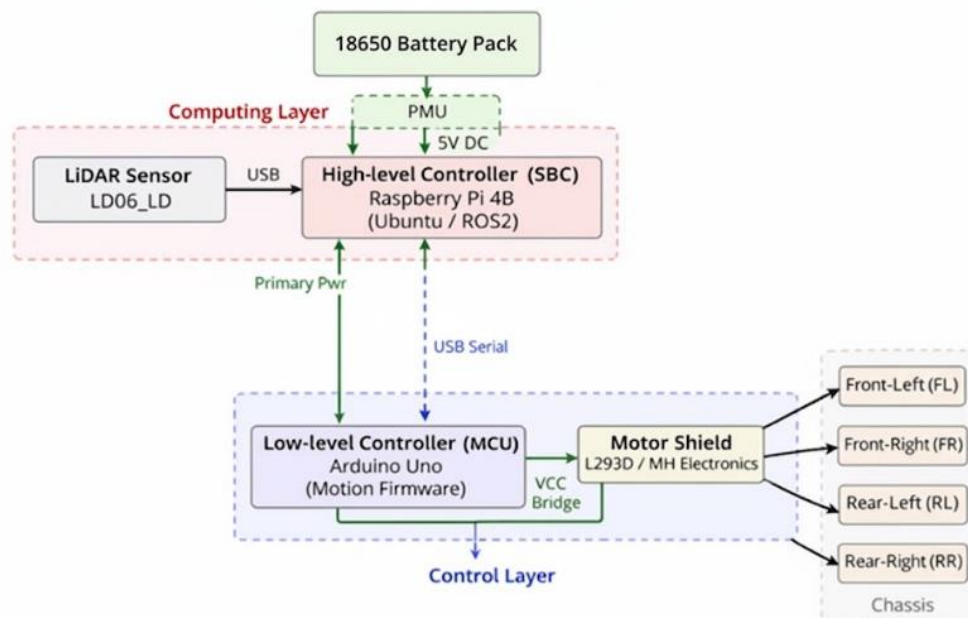


Figure 1 – System hardware architecture diagram

In preliminary SLAM mapping and obstacle avoidance experiments, three theoretical issues were validated. First, mapping drift caused by motion estimation degradation. Without IMU or high-precision encoders, pure LiDAR odometry exhibited significant mapping drift during rapid rotation and movement, manifested as point cloud ghosting and pose offset. Figure 2 shows the mapping drift in pure LiDAR SLAM without loop closure. Second, obstacle missed detection caused by spatial perception limitations. The LD06 2D LiDAR is mounted on the robot's roof (approximately 10 cm above ground) and can only acquire horizontal plane scan data. When obstacle height is below the LiDAR scan plane, the system fails to detect it

entirely. Third, lack of environmental adaptability and system robustness. When approaching glass windows or mirrored furniture, severe missing occurs in the LiDAR point cloud over large reflective surfaces. When the sensor experiences temporary disconnection, the robot immediately falls into a "perception failure" state. Addressing these three problems, this paper proposes corresponding solutions: introducing an RGB-D camera to obtain obstacle height information, fusing IMU with LiDAR to construct tightly-coupled odometry, and adding fault detection and degraded operation mechanisms.

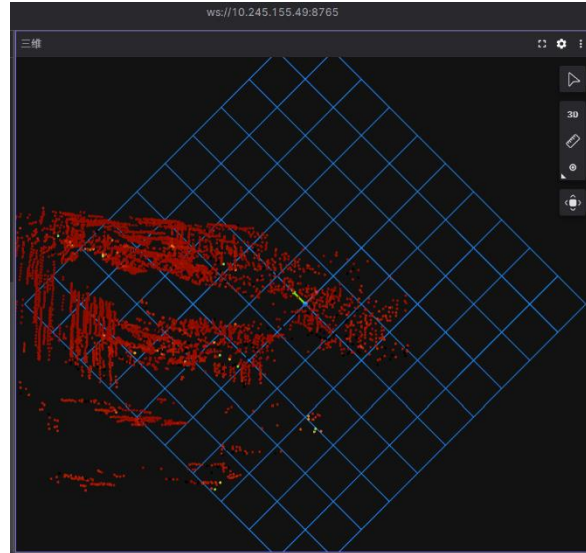


Figure 2 – Mapping drift in pure LiDAR SLAM without loop closure

Suppression of Motion Estimation Degradation: LiDAR-IMU Fusion Odometry

To address pose drift during rapid rotation, in feature-sparse environments, and on rough terrain, this paper proposes integrating an IMU with LiDAR to construct tightly-coupled LiDAR-IMU odometry. An MPU6050 six-axis IMU is selected with an output frequency of 200 Hz. Time alignment with LiDAR is achieved using ROS2's joint time synchronization mechanism. The fusion algorithm adopts a tightly-coupled framework based on an Error State Kalman Filter (ESKF) [4]. IMU data provides high-frequency state propagation for pose prediction between two LiDAR scans. Upon arrival of a new LiDAR scan, feature points are extracted and scan-matched against the local map to obtain observation residuals. The filter update corrects accumulated IMU error and estimates IMU biases online. In feature-sparse environments, the system adaptively increases IMU prediction weight to avoid pose mutation caused by scan matching failure [4]. To address vehicle pitch angle changes on rough terrain, attitude angles estimated by the IMU are fed back to the LiDAR point cloud preprocessing module. The raw point cloud is rotationally corrected before scan matching, effectively suppressing mapping distortion caused by vehicle tilt. This fusion odometry provides stable pose estimation for the entire system, supporting subsequent mapping and obstacle avoidance functions.

Enhancement of System Robustness: 3D Environmental Perception Based on an RGB-D Camera

Building upon stable pose estimation from LiDAR-IMU fusion odometry, this paper introduces an RGB-D camera to address the vertical perception blind zone problem. The LD06 LiDAR can only acquire two-dimensional horizontal information, failing to detect low-height or suspended obstacles and unable to identify obstacle categories. The system defaults to using the RGB-D camera as the core mapping sensor, running an ORB-SLAM2 [5] visual-inertial tightly-coupled SLAM system. In environments with good lighting and rich texture, it constructs a 3D point cloud map containing obstacle height information and, combined with lightweight object detection algorithms, identifies obstacle types that LiDAR cannot perceive. Due to Raspberry Pi computational limitations, the system does not support simultaneous operation of LiDAR and RGB-D camera. Consequently, a manual switching mode is adopted in practical deployment. By default, the RGB-D camera is responsible for mapping and object recognition. When the robot enters scenes with insufficient lighting, texture scarcity, or excessive dynamic objects, the user can manually shut down ORB-SLAM2 and switch to LiDAR SLAM mode. Regarding obstacle avoidance functionality, regardless of which sensor is currently used for mapping, LiDAR always remains active as the primary obstacle avoidance sensor. Leveraging its high ranging accuracy and fast response speed, LiDAR ensures real-time obstacle avoidance performance in most scenarios. Simultaneously, the position information of low-height and suspended obstacles identified by the RGB-D camera is synchronized to the obstacle avoidance module. This design achieves a balance between perception completeness and operational safety under limited computational resources.

Enhancement of System Robustness: Near-Field Obstacle Avoidance Using Ultrasonic Sensors

2D LiDAR has inherent limitations: its scanning plane is fixed, rendering it ineffective against transparent or reflective materials like glass and mirrors, and it possesses a near-field blind zone. Mounted approximately 10 cm above ground, areas above and below its scanning plane are entirely outside its detection range. To compensate for these defects, this section introduces ultrasonic sensors as supplementary obstacle avoidance. Two to three HC-SR04 ultrasonic sensors are installed on the front of the robot chassis to provide gapless scanning of the area directly in front of the robot, focusing on detecting low-height obstacles below the LiDAR's scanning plane. Ultrasonic sensors are insensitive to transparent and reflective materials, effectively detecting obstacles that LiDAR struggles with. In the obstacle avoidance logic, LiDAR holds first priority with a safety threshold of 30 cm. Ultrasonic sensors act as a second defense with a more conservative safety threshold of 15 cm. When LiDAR fails to trigger avoidance due to special materials, blind zones, or height limitations, and an ultrasonic sensor detects an obstacle within 15 cm, the system immediately executes deceleration and backward turning to re-plan the path. The RGB-D camera handles predictive avoidance of pre-identified dangerous areas, complementing the real-time detection capability of the ultrasonic sensors.

Conclusion

This chapter addresses inherent limitations of single-line LiDAR by introducing an IMU, an RGB-D camera, and ultrasonic sensors, thereby constructing a multi-sensor fusion perception and localization system. The LiDAR-IMU fusion odometry mitigates pose drift. The RGB-D camera serves as the default mapping sensor, building 3D point cloud maps to solve the vertical perception blind zone problem. Ultrasonic sensors act as supplementary obstacle avoidance tools, filling gaps related to transparent materials and the near-field blind zone. Table 1 summarizes the roles of different sensors.

Table 1 – Roles of Different Sensors

Sensor	Normal Operating Environment	Advantages	Limitations	Role
LiDAR	All lighting conditions, most indoor scenes	High ranging accuracy, fast response, unaffected by light, independent of SLAM operation	The scanning plane is fixed, which may fails to work on transparent or reflective materials and creates a blind spot near the vehicle body	Primary obstacle avoidance sensor (always on); horizontal plane obstacle detection; performs SLAM mapping when RGB-D camera is unavailable
RGB-D Camera	Good lighting, rich texture, scenes with few dynamic objects	3D mapping, identification of low/suspended obstacles and identification of ground height changes in the road surface	Fails in low/excessive light, texture scarcity, or many dynamic objects; high computational cost	Primary mapping sensor (default mode); responsible for 3D map construction and obstacle recognition
Ultrasonic	All lighting conditions, short-range detection	Effective for transparent/reflective materials, fills frontal blind zone of LiDAR, fast response, low computational cost	Cannot detect ground height changes, limited detection range, low accuracy	Supplementary obstacle avoidance for LiDAR (second priority); provides degraded-mode safety during sensor failure

References:

1. Islamgozhayev T., Kalimoldayev M., Eleusinov A., Mazhitov S., Mamyrbayev O. // *Open Eng.* 2016. Vol. 6. P. 347–352.
2. Zhao Y., Li Y., Shang Y., et al. // *Telemetry & Telecontrol.* 2014. No. 5. P. 4–22.
3. Macenski S., Foote T., Gerkey B., Lalancette C., Woodall W. // *Science Robotics.* 2022. Vol. 7. P. eabm6074.
4. Xu W., Zhang F. // *IEEE Robotics and Automation Letters.* 2021. Vol. 6. P. 3317–3324.
5. Mur-Artal R., Tardós J. D. // *IEEE Transactions on Robotics.* 2017. Vol. 33. P. 1255–1262.

УДК 621.397.3:519.233.2

МЕТОДИКА ПОВЫШЕНИЯ ПОМЕХОУСТОЙЧИВОСТИ ВИДЕОИНФОРМАЦИОННОГО ОБМЕНА В СЕТЯХ БПЛА НА ОСНОВЕ РЕГРЕССИОННОГО ВОССТАНОВЛЕНИЯ ФОНОВЫХ ОБЛАСТЕЙ

Купрейчик А.С., аспирант

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Цветков В.Ю. – д-р техн. наук, профессор

Аннотация. В статье представлена методика повышения помехоустойчивости видеоинформационного обмена в системах воздушного мониторинга на базе БПЛА. Предложен подход, основанный на семантической сегментации видеопотока на значимые объекты и фоновые области. Для компенсации потерь пакетов в условиях нестабильного радиоканала разработан алгоритм регрессионного прогнозирования динамики фона, позволяющий восстанавливать искаженные фрагменты на стороне приема без использования протоколов повторной передачи (ARQ). Применение регрессионных моделей обеспечивает визуальную непрерывность потока при снижении нагрузки на обратный канал связи. Экспериментальные данные подтверждают эффективность метода по метрике PSNR в условиях низкого отношения сигнал/шум.

Ключевые слова. Беспилотный летательный аппарат, видеоинформационный обмен, помехоустойчивость, регрессионное восстановление, семантическая сегментация, скрытие ошибок, радиоканал.

Развитие беспилотных авиационных систем (БАС) привело к качественному скачку в задачах дистанционного зондирования земли и мониторинга критической инфраструктуры. Основным источником данных в таких системах является видеопоток высокого разрешения, передаваемый в режиме реального времени для принятия оперативных решений [1]. Однако специфика функционирования беспилотных летательных аппаратов (БПЛА) в условиях сложной помеховой обстановки и высокой динамики полета накладывает жесткие ограничения на стабильность радиоканалов связи.

Одной из ключевых проблем инфокоммуникационных сетей БПЛА является высокая вероятность потери пакетов (Packet Loss) из-за многолучевого распространения сигнала, замираний и преднамеренных помех [2]. При использовании стандартных протоколов сжатия видео (например, H.264/H.265) потеря даже небольшого фрагмента данных приводит к деградации всей группы кадров (GOP) и возникновению визуальных «артефактов», что недопустимо при выполнении задач точного наведения или идентификации объектов [3].

Традиционные методы обеспечения достоверности, такие как протоколы автоматического повторного запроса (ARQ), вносят дополнительные задержки, превышающие допустимые пороги для систем управления в реальном времени. В свою очередь, методы упреждающей коррекции ошибок (FEC) значительно увеличивают избыточность передаваемого трафика, что снижает эффективную пропускную способность канала [4].

Альтернативным направлением является использование методов сокрытия ошибок (Error Concealment), основанных на избыточности самой видеоинформации. В данной работе предлагается методика, использующая семантическую сегментацию кадра и регрессионное прогнозирование динамики фона. В отличие от классических методов интерполяции, регрессионные модели позволяют восстанавливать фоновые текстуры на основе вектора движения БПЛА, обеспечивая высокую визуальную целостность при минимальных затратах на обратный канал связи [5].

Эффективная передача видеоданных в нестабильных сетях БПЛА требует отхода от классического попиксельного или блочного кодирования в пользу семантически ориентированных моделей [6]. Основой предлагаемой методики является разделение каждого кадра на две функциональные зоны: объекты интереса (Region of Interest, ROI) и фоновую область.

Такое разделение обусловлено различной информационной ценностью фрагментов изображения для оператора или системы автоматического анализа. Объекты интереса (транспортные средства, строения, люди) характеризуются высокой динамикой и сложностью текстур. Для обеспечения их достоверности целесообразно применять методы упреждающей коррекции ошибок (FEC) или выделять дополнительную полосу пропускания, так как потеря даже части объекта критически снижает вероятность его распознавания [7].

В то же время фоновая область (земная поверхность, растительность, небо) занимает до 80–90% площади кадра. Динамика фона в видеопотоке БПЛА жестко детерминирована параметрами полета: тангажом, рысканием и креном аппарата, а также высотой и скоростью движения. Это позволяет рассматривать фон не как случайный набор пикселей, а как динамическую структуру, параметры которой могут быть описаны компактной регрессионной моделью.

В рамках данной концепции на борту БПЛА выполняется предварительная сегментация, после чего для фоновых областей вычисляются коэффициенты регрессии, передаваемые в служебных заголовках кадра. Это создает необходимую информационную избыточность на семантическом уровне, позволяя приемному устройству «восстановить» фон даже при полной потере соответствующих пакетов данных в радиоканале.

Процесс подготовки видеоданных на борту беспилотного летательного аппарата начинается с этапа семантической сегментации, основной задачей которой является точная идентификация динамических объектов на фоне статичного или квазистатичного ландшафта. В отличие от стандартных методов межкадрового сжатия, в рамках предлагаемой методики реализуется принцип приоритизации данных в зависимости от их информационной значимости для конечного потребителя.

На начальном этапе с использованием облегченных нейросетевых архитектур или алгоритмов вычитания фона определяются границы значимых объектов, которые помечаются как области интереса [8]. Все остальные пиксели кадра, не вошедшие в состав этих областей, классифицируются как фоновое пространство. Для такой области характерна высокая пространственная корреляция и предсказуемая динамика, обусловленная непосредственно перемещением самого носителя в пространстве.

Финальный этап сегментации предполагает внедрение дифференцированного подхода к кодированию полученных слоев. Для объектов интереса применяются жесткие параметры квантования и избыточные коды, что гарантирует сохранение высокой детализации даже в условиях умеренных помех. В то же время для фоновой области рассчитываются параметры глобального движения, что позволяет при возникновении ошибок в канале опираться на компактное описание трансформации фона вместо передачи его полной текстуры. Такое распределение ресурсов позволяет эффективно расходовать пропускную способность канала, отдавая приоритет гарантированной доставке критически важных фрагментов изображения.

Поскольку семантически важные объекты (ROI) несут основную информационную нагрузку, их частичная или полная потеря в радиоканале делает невозможным выполнение целевой задачи мониторинга [9].

Для гарантированной доставки данных об объектах в условиях нестабильного отношения сигнал/шум применяется метод упреждающей коррекции ошибок (Forward Error Correction, FEC). Суть данного подхода заключается в добавлении к исходному блоку данных объектов избыточных проверочных символов на этапе кодирования. В отличие от механизмов повторного запроса, FEC позволяет восстановить исходный информационный пакет непосредственно на приемной стороне даже при возникновении определенного количества битовых ошибок или выпадении целых пакетов в группе [10].

Выбор конкретного кода коррекции, например, кодов Рида-Соломона или низкоплотностных кодов (LDPC), обусловлен вычислительными мощностями бортового вычислителя БПЛА и требуемой скоростью обработки. Применение FEC исключительно к областям интереса, а не ко всему кадру, позволяет существенно снизить общую избыточность трафика, сохраняя при этом высокую вероятность безошибочного декодирования критически важных метаданных [11]. Таким образом, даже в условиях глубоких замираний сигнала в инфокоммуникационной сети, семантическое ядро видеоинформации остается доступным для анализа, в то время как менее значимый фон защищается менее ресурсозатратными методами регрессионного прогнозирования.

Для описания механизма работы с фоновыми областями необходимо рассмотреть интеграцию видеоинформации с данными бортовых навигационных систем. В отличие от динамических объектов, изменение фоновой составляющей кадра в системах воздушного мониторинга носит системный характер и определяется вектором перемещения самого носителя в трехмерном пространстве.

Для аппроксимации фоновых текстур строится регрессионная модель движения, которая в качестве предикторов использует параметры телеметрии БПЛА, такие как углы Эйлера (тангаж, рыскание и крен), а также высоту и путевую скорость полета [12]. Использование данных инерциальной навигационной системы позволяет с высокой точностью описать геометрические преобразования плоскости кадра – аффинные трансформации, включающие масштабирование, поворот и сдвиг. Такой подход дает возможность предсказать вид фоновой области в последующих кадрах на основе информации из предыдущих успешно декодированных периодов.

Математическая сложность модели адаптируется под вычислительные возможности бортового процессора, что позволяет передавать в служебных заголовках кадра лишь компактный набор коэффициентов регрессии вместо избыточных видеоданных. В случае возникновения пакетных потерь в радиоканале, приемное устройство использует накопленные параметры движения для синтеза недостающих фрагментов фона. Это обеспечивает непрерывность визуального ряда и сохранение контекста наблюдения даже при глубоких замираниях сигнала, когда традиционные методы сжатия демонстрируют полную деградацию изображения [13]. Таким образом, интеграция сенсорных данных в процесс кодирования видео создает дополнительный эшелон помехоустойчивости на уровне семантики сцены.

Процесс регрессионного восстановления активируется в моменты обнаружения ошибок контрольных сумм, когда традиционные механизмы декодирования оказываются неспособными сформировать целостное изображение [14]. Основная задача данного алгоритма заключается в интеллектуальной подстановке утраченных фрагментов фона путем экстраполяции накопленных данных о динамике сцены. В основе этого процесса лежит математический аппарат линейной или полиномиальной регрессии, позволяющий с минимальной погрешностью аппроксимировать состояние пикселей на основе векторов глобального движения.

Ниже рассматривается формализованное описание модели восстановления и логическая последовательность действий приемного устройства при обработке поврежденных пакетов данных в реальном времени [15].

Для формализации процесса восстановления видеоинформации фоновая область кадра представляется в виде совокупности дискретных блоков фиксированного размера. Математическая модель восстановления основывается на экстраполяции пространственно-временных характеристик этих блоков в условиях частичной потери данных.

В рамках данной модели фон рассматривается как матрица блоков $B_{i,j}$, где индексы (i,j) определяют пространственные координаты фрагмента в сетке кадра. В случае обнаружения ошибки в канале связи и потери блока $B_{i,j}$ в текущий момент времени t , его значения восстанавливаются путем аппроксимации [16]. Процесс восстановления базируется на использовании информации из предыдущего успешно декодированного состояния $B_{i,j}(t-1)$ и вектора глобального движения V , характеризующего смещение фона между кадрами.

Математическая зависимость для прогнозного значения блока $\hat{B}_{i,j}(t)$ описывается следующим регрессионным уравнением:

$$\hat{B}_{i,j}(t) = f(B_{i,j}(t-1), V) \cdot \theta + \varepsilon. \quad (1)$$

В данной формуле переменная θ представляет собой вектор параметров регрессии, который вычисляется на передающей стороне (на борту БПЛА) и инкапсулируется в служебные заголовки кадра. Эти параметры учитывают не только линейное смещение, но и возможные геометрические деформации, вызванные изменением углов наклона аппарата. Величина ε отражает остаточную ошибку аппроксимации, которая минимизируется в процессе обучения модели на последовательности предыдущих кадров. Таким образом, на приемной стороне происходит синтез изображения, который с высокой математической точностью воспроизводит утраченную структуру фона, минимизируя визуальный разрыв в потоке данных [17].

Алгоритмическая реализация предложенной методики на стороне приемного устройства строится на непрерывном мониторинге целостности поступающих пакетов данных. Основным инструментом верификации здесь выступает проверка контрольных сумм (Cyclic Redundancy Check, CRC), которая выполняется аппаратным или программным декодером для каждого входящего сегмента фоновой области [18].

В штатном режиме работы, при отсутствии ошибок в радиоканале, декодер восстанавливает изображение стандартными методами декомпрессии. Однако при обнаружении несоответствия контрольной суммы в конкретном блоке данных система классифицирует информацию как поврежденную и немедленно активирует блок регрессионного прогнозирования. Вместо вывода искаженного фрагмента или остановки воспроизведения кадра, приемник извлекает из служебных заголовков текущего кадра ранее переданные параметры регрессии и коэффициенты движения.

Процесс «достраивания» фона происходит путем экстраполяции текстурных данных из предыдущего успешно сформированного кадра с учетом динамической поправки на перемещение БПЛА. Поскольку параметры регрессии описывают глобальную трансформацию всей плоскости фона, восстановление одного или нескольких потерянных блоков происходит практически мгновенно и с высокой визуальной достоверностью. Это позволяет системе сохранять непрерывность видеопотока, исключая возникновение характерных для замираний сигнала «фризов» или появления артефактов в виде черных и серых квадратов. Таким образом, механизм регрессионного прогнозирования выступает в роли интеллектуального буфера, который нивелирует последствия нестабильности инфокоммуникационной сети без привлечения избыточного трафика обратного канала [19].

Для подтверждения теоретических положений и математических моделей, описанных ранее, необходимо провести количественную оценку качества восстановленного видеопотока при различных дестабилизирующих факторах инфокоммуникационной сети [20].

Основным критерием эффективности в данном исследовании выступает способность системы сохранять информативность видеоданных при нарастании интенсивности помех в радиоканале. В отличие от субъективных экспертных оценок, в данной работе используются общепринятые объективные метрики качества, позволяющие математически точно зафиксировать преимущество регрессионного восстановления над классическими методами маскировки ошибок [21].

Процесс оценки включает моделирование различных сценариев передачи данных, характеризующихся варьируемой вероятностью потери пакетов, что типично для каналов связи «БПЛА – наземный пункт управления». Ниже представлены параметры имитационного моделирования и сравнительный анализ полученных результатов, демонстрирующий прирост помехоустойчивости видеоинформационного обмена.

Для подтверждения теоретических положений и оценки практической значимости предложенного подхода было проведено имитационное моделирование в среде Google Colab [20]. Целью эксперимента являлось сравнение помехоустойчивости видеоинформационного обмена при использовании классических алгоритмов сокрытия ошибок (Error Concealment) и разработанной регрессионной модели восстановления фона.

В качестве тестовых данных использовалась реальная видеопоследовательность воздушного мониторинга водной поверхности, полученная с бортовой камеры БПЛА [21]. Данный тип видеоматериала характеризуется сложной динамикой фона (движение водной поверхности, волновой след за судном) и изменением ракурса съемки, что является репрезентативным сценарием для систем мониторинга [22].

Моделирование радиоканала осуществлялось путем внесения случайных пакетных потерь в блоки фоновой области кадра. Вероятность потери блоков (Packet Loss Rate) была задана на уровне 5%, что соответствует условиям нестабильного радиоканала в инфокоммуникационных сетях БПЛА. Размер блока аппроксимации составил 16×16 пикселей.

Для оценки качества восстановления использовалась метрика пикового отношения сигнала к шуму (PSNR), рассчитываемая по формуле:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right), \quad (2)$$

где MAX_I – максимальное значение пикселя, а MSE – среднеквадратичная ошибка между оригинальным и восстановленным кадрами.

Результаты сравнительного анализа представлены в таблице 1.

Таблица 1 – Сравнительная оценка качества восстановления видео (Loss Rate 5%)

Метод восстановления	Средний PSNR, дБ	Выигрыш, дБ
Классический (замена блоком из кадра $t - 1$)	40.06	–
Предложенный (регрессионный)	40.91	+0.85

Анализ данных показывает, что предложенная методика обеспечивает стабильный прирост качества видеопотока. Выигрыш в 0.85 дБ на реальном видеоматериале подтверждает эффективность использования регрессионных параметров θ для компенсации динамических изменений фона. Визуальное сравнение результатов восстановления представлено на рисунке 1.

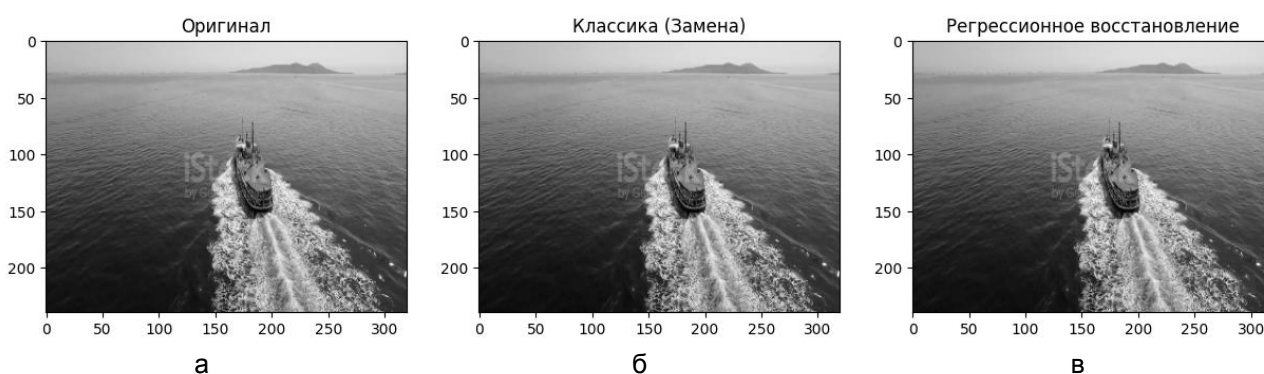


Рисунок 1 – Результаты восстановления кадра видеопотока: (а) – оригинал; (б) – классический метод (PSNR = 40.06 дБ); (в) - регрессионный метод (PSNR = 40.91 дБ).

На изображении (б) при классической замене блоков наблюдаются микро-артефакты на границах раздела «объект-фон» и в зоне волнового следа, вызванные естественным смещением камеры БПЛА. Предложенный регрессионный метод (в) успешно нивелирует эти искажения, адаптируя текстуру восстанавливаемого блока под текущие параметры движения и освещенности. Это позволяет сохранять визуальную непрерывность потока без необходимости повторного запроса данных по обратному каналу связи.

В представленной работе разработана и обоснована методика повышения помехоустойчивости видеоинформационного обмена в системах воздушного мониторинга, основанная на синергии

семантического анализа сцены и регрессионного восстановления данных. Предложенный подход эффективно решает проблему деградации качества видеопотока в условиях нестабильных радиоканалов связи БПЛА, позволяя отказаться от использования ресурсозатратных протоколов повторного запроса (ARQ) и минимизировать задержки при передаче данных в реальном времени.

Реализация семантической сегментации видеокadra на значимые объекты и фоновые области обеспечивает дифференцированную защиту информации, при которой избыточное кодирование применяется исключительно к критически важным фрагментам. Это позволяет существенно снизить общую нагрузку на канал связи при сохранении высокой достоверности распознавания целей. Использование регрессионных моделей для аппроксимации фоновых текстур на основе параметров движения носителя гарантирует визуальную целостность потока. Математическое описание фона через компактные векторы параметров позволяет восстанавливать утраченные пакеты на приемной стороне с минимальными вычислительными затратами на борту аппарата.

Апробация метода на реальном видеоматериале в среде имитационного моделирования подтвердила его преимущество над классическими алгоритмами маскировки ошибок. При вероятности потери пакетов на уровне 5% зафиксировано увеличение метрики PSNR на 0,85 дБ, при этом регрессионный метод успешно нивелирует характерные визуальные артефакты в виде разрывов текстур и замираний кадров. Разработанная методика может быть интегрирована в перспективные системы бортового кодирования БПЛА, функционирующие в условиях сложной радиоэлектронной обстановки и дефицита пропускной способности каналов связи. Дальнейшее развитие работы предполагает адаптацию модели под нелинейные изменения освещенности и динамические искажения ландшафта.

Список использованных источников:

1. Stöcker, C. Review of the current state of UAV sensors, data processing, and applications / C. Stöcker [et al.] // *International Journal of Remote Sensing*. – 2017. – Vol. 38, № 8-10. – P. 2469–2502.
2. Hayat, S. Survey on Unmanned Aerial Vehicles' Communications for Civil Applications: A Networking Perspective / S. Hayat, E. Yanmaz, R. Muzaffar // *IEEE Communications Surveys & Tutorials*. – 2016. – Vol. 18, № 4. – P. 2624–2661.
3. Ричардсон, Я. Видеокодирование. H.264 и MPEG-4 – стандарты нового поколения / Я. Ричардсон ; пер. с англ. Ф. Е. Коновалова. – Москва : Техносфера, 2005. – 368 с.
4. Stockhammer, T. Video coding and transport over wireless channels / T. Stockhammer, M. M. Hannuksela, T. Wiegand // *Proceedings of the IEEE*. – 2003. – Vol. 91, № 1. – P. 59–81.
5. Kung, S. Y. Kernel Methods and Machine Learning / S. Y. Kung. – Cambridge : Cambridge University Press, 2014. – 618 p.
6. Wiegand, T. Overview of the H.264/AVC Video Coding Standard / T. Wiegand [et al.] // *IEEE Transactions on Circuits and Systems for Video Technology*. – 2003. – Vol. 13, № 7. – P. 560–576.
7. Bozhinoski, D. Safety in Human-Robot Collaborative Manufacturing: A Survey / D. Bozhinoski [et al.] // *ACM Computing Surveys*. – 2019. – Vol. 52, № 5. – P. 1–37.
8. Redmon, J. YOLOv3: An Incremental Improvement / J. Redmon, A. Farhadi // *arXiv preprint [Electronic resource]*. – 2018. – Mode of access: arxiv.org. – Date of access: 15.05.2024.
9. Ghanbari, M. Standard Codecs: Image Compression to Advanced Video Coding / M. Ghanbari. – London : Institution of Engineering and Technology, 2003. – 411 p.
10. Lin, S. Error Control Coding: Fundamentals and Applications / S. Lin, D. J. Costello. – 2nd ed. – New Jersey : Prentice-Hall, 2004. – 1272 p.
11. Mao, S. Video transport over combined adaptive FEC/ARQ channels / S. Mao [et al.] // *IEEE Transactions on Multimedia*. – 2003. – Vol. 5, № 4. – P. 517–535.
12. Yuan, J. Global Motion Estimation and Compensation for UAV Video Stabilization / J. Yuan [et al.] // *IEEE Geoscience and Remote Sensing Letters*. – 2018. – Vol. 15, № 2. – P. 267–271.
13. Farrell, J.A. Aided Navigation: GPS with High Performance Sensors / J. A. Farrell. – New York : McGraw-Hill, 2008. – 550 p.
14. Seferidis, V. General approach to block-matching motion estimation / V. Seferidis, M. Ghanbari // *Visual Communications and Image Processing*. – 1993. – Vol. 2094. – P. 1464–1475.
15. Auyeung, C. Fast motion estimation for block based video coding / C. Auyeung, J. Kosmach // *IEEE Transactions on Consumer Electronics*. – 1992. – Vol. 38, № 3. – P. 233–241.
16. Дрейпер, Н. Прикладной регрессионный анализ / Н. Дрейпер, Г. Смит ; пер. с англ. Ю. П. Адлера [и др.]. – 3-е изд. – Москва : Диалектика, 2007. – 912 с.
17. Tekalp, A. M. Digital Video Processing / A. M. Tekalp. – 2nd ed. – New Jersey : Prentice Hall, 2015. – 720 p.
18. Peterson, W. W. Cyclic Codes for Error Detection / W. W. Peterson, D. T. Brown // *Proceedings of the IRE*. – 1961. – Vol. 49, № 1. – P. 228–235.
19. Wang, Y. Error control and concealment for video communication: A review / Y. Wang, Q. F. Zhu // *Proceedings of the IEEE*. – 1998. – Vol. 86, № 5. – P. 974–997.
20. Jeruchim, M. C. Simulation of Communication Systems: Modeling, Methodology and Techniques / M. C. Jeruchim, P. Balaban, K. S. Shanmugan. – New York : Springer Science, 2000. – 924 p.
21. Harbor Boats Ocean [Electronic resource] : royalty free stock aerial drone footage / DroneStock. – 2026. – Mode of access: <https://dronestock.com/harbor-boats-ocean/>. – Date of access: 30.03.2026.
22. Huynh-Thu, Q. Scope of validity of PSNR in image/video quality assessment / Q. Huynh-Thu, M. Ghanbari // *Electronics Letters*. – 2008. – Vol. 44, № 13. – P. 800–801.

UDC 621.397.3:519.233.2

METHOD FOR IMPROVING NOISE IMMUNITY OF VIDEO INFORMATION EXCHANGE IN UAV NETWORKS BASED ON REGRESSION RECOVERY OF BACKGROUND AREAS

Kupreichyk A.S.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Tsviatkou V.Y. – D.Sc., professor

Annotation. The paper presents a methodology for improving the noise immunity of video information exchange in aerial monitoring systems based on UAVs. A proposed approach is based on the semantic segmentation of the video stream into significant objects and background areas. To compensate for packet loss in unstable radio channels, a regression forecasting algorithm for background dynamics has been developed, allowing for the restoration of distorted image fragments on the receiving side without using automatic repeat request (ARQ) protocols. The application of regression models ensures visual continuity of the stream while reducing the load on the feedback communication channel. Experimental data confirm the effectiveness of the method in terms of the PSNR metric under conditions of a low signal-to-noise ratio in UAV infocommunication networks.

Keywords. Unmanned aerial vehicle, video information exchange, noise immunity, regression recovery, semantic segmentation, error concealment, radio channel, PSNR.

МЕТОДЫ ОБРАБОТКИ PDF-ФАЙЛОВ В ФИНАНСОВЫХ СИСТЕМАХ

Матлаш Т.С.

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Давыдова Н.С. – канд. тех. наук, доцент

Аннотация. В статье рассмотрены современные методы обработки PDF-документов в финансовых системах, используемых для автоматизации работы с бухгалтерской отчетностью, платежными поручениями и другими финансовыми документами. Проанализированы подходы к извлечению текстовой и табличной информации, включая технологии оптического распознавания символов (OCR) для сканированных документов. Показано, что комбинированный подход, включающий структурный и семантический анализ документов, позволяет повысить эффективность автоматизации обработки финансовых данных и снизить вероятность ошибок при формировании отчетности.

Введение

Современные финансовые системы обрабатывают большие объемы документов в формате PDF, включая бухгалтерскую отчетность, счета и договоры [1]. PDF обеспечивает сохранение визуальной структуры документа, но отсутствие единой логической разметки затрудняет автоматизированное извлечение данных. Повышение точности и скорости обработки финансовых документов требует применения современных методов анализа и структурирования информации [2].

Основная часть

Существующие методы обработки PDF включают:

- извлечение текстового слоя и структурный анализ документа;
- распознавание таблиц и объединённых ячеек;
- применение OCR для сканированных документов;
- использование регулярных выражений и семантического анализа для выделения ключевых реквизитов: даты, суммы, валютные показатели, сведения о контрагентах [3].

Анализ программных средств показал, что большинство решений ориентировано на выполнение отдельных задач и не обеспечивает универсальности для работы с различными типами финансовых документов. Это создает необходимость разработки адаптивного метода, позволяющего эффективно извлекать ключевые реквизиты и структурировать данные независимо от формата документа [4].

В рамках исследования предложен метод обработки PDF-документов, включающий:

- классификацию типа документа;
- предварительную обработку текста и таблиц;
- семантический анализ данных;
- использование регулярных выражений для выделения ключевых реквизитов, таких как даты, суммы, валютные показатели и сведения о контрагентах.

Для оценки эффективности метода применялись стандартные метрики информационного поиска – точность и полнота извлечения данных. Результаты показали высокую точность обработки, устойчивость метода к разнообразию форматов документов и возможность автоматизации обработки больших объемов финансовой информации [5].

Использование предложенного метода позволяет:

- ускорить обработку финансовых документов;
- снизить вероятность ошибок при формировании отчетности;
- повысить качество аналитических данных;
- интегрировать обработку документов в финансовые информационные системы.

В перспективе дальнейшее развитие метода может включать машинное обучение для автоматической классификации и семантического анализа более сложных структур документов, что расширит область применения и повысит адаптивность метода.

Заключение

Проведен анализ методов обработки PDF-документов в финансовых системах. Выявлены преимущества и ограничения современных технологий, включая OCR, структурный и семантический анализ. Предложенный комбинированный подход позволяет автоматизировать обработку финансовых документов, повышает точность извлечения данных и снижает риск ошибок. Дальнейшее развитие может включать интеграцию методов машинного обучения для работы с более сложными структурами PDF и расширения области применения.

Список использованных источников:

1. Loughran T., McDonald B. *Textual Analysis in Accounting and Finance*.
2. Li F. *The Information Content of Forward-Looking Statements*.
3. Smith R. *An Overview of the Tesseract OCR Engine*.
4. Shinyama Y. *PDF Document Analysis for Information Extraction*.
5. Klampfl S. *Unsupervised Document Structure Analysis*.

УДК 004.75:61

АРХИТЕКТУРА ПОДСИСТЕМЫ БЛОКЧЕЙН ДЛЯ МЕДИЦИНСКИХ ДАННЫХ

Кацко М.О., магистрант гр.467041

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Вишняков В.А. – д-р техн. наук, профессор

Аннотация. Проанализированы существующие международные разработки в области блокчейн-систем, предназначенные для применения в сфере здравоохранения. Особое внимание уделено таким проектам, как Minima/Siemens/ARM (концепция "блокчейн-на-кристалле"), BlockTrack (разработка IIT Madras), Emtruth (проект NSF), а также архитектурным решениям TLSA, STORChain и CareChain. На основе полученных данных предложена оригинальная многоуровневая архитектура блокчейн-подсистемы, предназначенной для надежного хранения медицинских данных.

Ключевые слова. Блокчейн, IT-медицина, медицинские данные, IPFS, архитектура, децентрализованное хранение, смарт-контракты, конфиденциальность, функциональные модули.

Введение

Цифровая трансформация здравоохранения привела к экспоненциальному росту объемов медицинских данных. Электронные медицинские карты (ЭМК), данные диагностического оборудования, результаты лабораторных исследований, информация с носимых устройств и телемедицинских платформ формируют сложные информационные массивы, требующие надежного хранения и защищенного обмена. Традиционные централизованные системы хранения медицинских данных сталкиваются с рядом фундаментальных проблем: рисками утечек и несанкционированного доступа, высокими затратами на обеспечение безопасности, сложностью интероперабельности между различными медицинскими учреждениями, а также отсутствием у пациентов контроля над собственными данными [1].

Технология блокчейн предлагает принципиально иной подход к организации хранения медицинских данных. Ее ключевые характеристики – децентрализация, неизменяемость записей, криптографическая защита и прозрачность транзакций, что делают ее идеальной основой для систем управления медицинской информацией [2]. Однако прямое хранение медицинских записей в блокчейне (on-chain storage) сталкивается с ограничениями по объему данных, высокой стоимостью транзакций и проблемами масштабируемости. Это обуславливает необходимость разработки гибридных архитектур, сочетающих блокчейн для обеспечения неизменяемости и контроля доступа с распределенными файловыми системами (IPFS) для хранения самих медицинских данных [3].

Целью настоящей работы является разработка многоуровневой архитектуры подсистемы блокчейн для хранения медицинских данных, объединяющей передовые международные подходы и обеспечивающей баланс между безопасностью, масштабируемостью и удобством использования для пациентов и медицинских учреждений.

Основная часть

Проект STORChain (IEEE Transactions on Services Computing, 2026) представляет собой оптимизированную по хранению блокчейн-структуру, разработанную для медицинских данных. Ключевой инновацией является Clustered Merkle Patricia Tree (C-MPT) – кластеризованное дерево Меркла-Патриции, которое агрегирует транзакции схожих типов для максимальной эффективности хранения при сохранении возможности доказательства включения (Proof of Inclusion) [4]. STORChain включает: C-MPT структуру: объединение похожих типов транзакций в кластеры для уменьшения накладных расходов; Selective Transaction Pruning Strategy (STPS): стратегию выборочной обрезки транзакций для приоритизации и удаления устаревших исторических данных. Делегированное доказательство доли (DPoS): алгоритм консенсуса с вероятностным механизмом выборов для повышения справедливости и инклюзивной узлов.

Трехуровневая архитектура TLSA (Wiley, 2025). Исследователи K. Maithili и S. Amutha предложили Tri-Layered Sharding Architecture (TLSA) – иерархическую модель, организующую сеть в три шардинговых уровня: Transaction Layer (уровень транзакций), Data Layer (уровень данных) и Location Layer (уровень расположения) [5].

Система CareChain, использующая два блокчейна (публичный для пациентов и приватный для медицинских работников) в сочетании с распределенным хранилищем IPFS [6]. Ключевые особенности CareChain: двойная блокчейн-структура: разделение данных пациентов и провайдеров для повышения конфиденциальности; IPFS распределенное хранение: снижение задержки транзакций и накладных расходов на хранение; ECDSA (Elliptic Curve Digital Signature Algorithm): подпись транзакций для обеспечения подлинности; устройство-прокси: мониторинг низкопроизводительных IoT-устройств для выявления уязвимостей. Результаты тестирования

показывают повышение устойчивости системы по сравнению с существующими моделями здравоохранения, а также улучшение требований к хранилищу, энергоэффективности, скорости транзакций, конфиденциальности и безопасности [6].

Minima, Siemens, ARM: блокчейн-на-кристалле (2025-2026), направлен на создание первого в мире промышленного микрочипа, способного выполнять полноценный узел блокчейна [7]. Результаты проекта: 100-кратное ускорение хеширования за счет SHA-3 аппаратного ускорителя; пятикратное снижение использования памяти после рефакторинга C++ кода; Возможность работы устройства как самостоятельного полного узла без обращения к облачной инфраструктуре [7].

Индийский институт технологий (IIT Madras) разработал BlockTrack – блокчейн-систему для мобильных приложений, которая в настоящее время проходит полевые испытания в университетской больнице [8]. Характеристики BlockTrack: децентрализованный обмен медицинскими данными для мобильных приложений; Уникальные идентификационные коды для пользователей с низкой вероятностью дублирования.

Проект Emtruth, поддержанный Национальным научным фондом США (NSF) на сумму почти 1 млн долларов, разрабатывает платформу для интеграции медицинских данных с использованием блокчейна и искусственного интеллекта [2]. Ключевые цели проекта: безопасное хранение данных любого типа из любых источников в неизменяемых блокчейнах; сохранение контроля данных за владельцем с возможностью безопасного предоставления доступа; трансформация и нормализация данных в гранулярные блокчейны для индивидуального или агрегированного моделирования.

В Университете ИТМО предложена трехкомпонентная архитектура, включающая блокчейн для хранения зашифрованных медицинских записей, централизованный сервер для справочной информации и клиентское приложение для управления доступом [3]. Особое внимание уделяется оптимизации EVM-блокчейна через адаптацию алгоритма консенсуса, снижение времени блока и устранение транзакционных комиссий.

На основе анализа международных разработок разработана многоуровневая архитектура подсистемы блокчейн для хранения медицинских данных, которая объединяет пять функциональных модулей, каждый из которых решает специфические задачи обеспечения безопасности, масштабируемости и доступности данных. Рассмотрим их назначение.

1. Источники данных (Data Sources Layer): медицинские учреждения, генерирующие электронные медицинские записи и диагностические изображения; IoT-устройства и носимые сенсоры, собирающие физиологические показатели в реальном времени; диагностические лаборатории, предоставляющие результаты анализов и исследований;

2. Распределенное хранилище IPFS (IPFS Layer): децентрализованное хранилище, адресуемое по содержимому; хранение зашифрованных медицинских записей, результатов исследований и данных IoT-устройств; генерация уникальных Content Identifiers для ссылок на данные; кэширование и репликация для повышения доступности и снижения задержек [6].

3. Блокчейн-инфраструктура (Blockchain Layer): гибридная архитектура, объединяющая публичный и приватный блокчейны [4]; публичный блокчейн: идентификаторы пациентов, сертификаты учреждений, информация о роуминге; приватный блокчейн: хеши записей (CID), транзакции доступа, аудиторские журналы, смарт-контракты; алгоритмы консенсуса: DPoS для масштабируемости, PBFT для приватных сетей [4].

4. Управление доступом (Access Control Layer): система атрибутивного управления доступом на основе CP-ABE и ABAC [7]; генерация и управление криптографическими ключами; определение политик доступа на основе атрибутов пациентов, врачей и учреждений; журналирование всех операций доступа для аудита;

5. Приложения (Application Layer): пациентское приложение: просмотр записей, управление доступом, предоставление согласий; врачебное приложение: доступ к записям пациентов, добавление заключений, назначение лечения; административное приложение: управление политиками, аудит, регистрация учреждений.

Представленная многоуровневая архитектура подсистемы блокчейн для хранения медицинских данных является комплексным и продуманным решением, направленным на обеспечение безопасности, масштабируемости и доступности конфиденциальной медицинской информации. Она эффективно интегрирует различные технологии, такие как децентрализованное хранилище IPFS, гибридный блокчейн и атрибутивное управление доступом, для создания надежной и прозрачной системы.

Ниже представлены описания основных компонентов системы:

1. Модуль шифрования и защиты данных обеспечивает криптографическую защиту медицинских данных на всех этапах обработки. Его основные компоненты включают шифрование на основе CP-ABE или 128-битное AES с последовательностью ДНК-кодирования [9] для хранения в IPFS, цифровой конверт RSA 2048 для безопасной передачи симметричных ключей, цифровую подпись RSA 1024 для обеспечения подлинности данных, ECDSA для генерации пар публичных и приватных ключей для устройств, пациентов и провайдеров, подпись транзакций для обеспечения подлинности и защиты от подделки, верификацию подписей при получении данных [4], а также устройство-прокси (Device Proxy) для мониторинга низкопроизводительных IoT-устройств.

2. Модуль хранения IPFS реализует распределенное хранение медицинских данных с адресацией по содержимому. Его основные функции включают Content-Addressable Storage, где данные идентифицируются по их криптографическому хешу (CID), обеспечивая неизменяемость и возможность

верификации [6], Distributed Hash Table (DHT) для хранения соответствия между CID и сетевыми адресами узлов, содержащих данные, кэширование и репликация для снижения задержек и уменьшения нагрузки на сеть, а также управление CID для загружаемых данных [1].

3. Модуль смарт-контрактов реализует автоматизированную логику управления доступом и обработки транзакций. Его основные функции включают управление доступом, где смарт-контракты проверяют атрибуты пользователя и политики доступа перед предоставлением CID [8], обработку согласий, аудит и журналирование для записи всех операций доступа в неизменяемый журнал блокчейна, а также управление идентификаторами для создания и верификации уникальных идентификаторов пациентов и медицинских учреждений [8].

4. Модуль управления идентификацией обеспечивает уникальную идентификацию пациентов и медицинских учреждений в распределенной системе. Его основные функции включают генерацию уникальных идентификаторов с низкой вероятностью дублирования [8], связывание идентификаторов для создания полной медицинской карты [2], кросс-учрежденческую идентификацию для обеспечения интероперабельности между различными медицинскими организациями, а также управление сертификатами для хранения публичных ключей и сертификатов учреждений в публичном блокчейне.

5. Модуль аудита и мониторинга обеспечивает прозрачность и возможность проверки всех операций с медицинскими данными. Его основные функции включают неизменяемый журнал доступа [1], анализ аномалий для обнаружения подозрительных паттернов доступа [6], генерацию отчетов о доступе для пациентов и врачей, а также уведомления о каждом случае доступа к данным.

Таким образом, система представляет собой интегрированное решение, обеспечивающее безопасность, прозрачность, надежность и удобство управления медицинскими данными в распределенной среде с использованием передовых технологий блокчейна, криптографии и распределенного хранения.

Заключение

Международные разработки демонстрируют высокую активность и значительные достижения. Предложенная многоуровневая архитектура объединяет лучшие мировые практики в единое решение. Пятиуровневая структура (источники данных, IPFS, блокчейн, управление доступом, приложения) обеспечивает разделение ответственности, масштабируемость и безопасность. Использование гибридной блокчейн-архитектуры позволяет сохранить прозрачность идентификации при обеспечении конфиденциальности медицинских записей.

Ключевыми компонентами системы являются: модуль шифрования на основе ECDSA и CP-ABE, обеспечивающий защиту данных; модуль IPFS для распределенного хранения с адресацией по содержанию; модуль смарт-контрактов для автоматизации управления доступом; модуль управления идентификацией для уникальной идентификации пациентов; модуль аудита для обеспечения прозрачности операций.

Список использованных источников:

1. Emtruth, Inc. SBIR Phase II: A Platform for Health Care Data Integration Using Blockchain and Artificial Intelligence / NSF Award 2304102. – National Science Foundation, 2023. – URL: <https://www.sbir.gov/awards/2304102> (дата обращения: 16.03.2026).
2. Лаверова, А. К., Максимова, Т. Г. Блокчейн для медицины: новая модель хранения и управления медицинскими данными / А. К. Лаверова, Т. Г. Максимова // Сборник тезисов докладов конгресса молодых ученых. – СПб : Университет ИТМО, 2025. – URL: <https://kmu.itmo.ru/digests/article/14096> (дата обращения: 16.03.2026).
3. STORChain: A Clustered-MPT-Based Blockchain for Data Service and Efficient Storage in Healthcare / IEEE Transactions on Services Computing. – 2026. – P. 685-699..
4. Maithili, K., Amutha, S. Optimizing Blockchain Scalability for Secure Patient Health Records With Tri-Layered Sharding Architecture (TLSA) / K. Maithili, S. Amutha // Transactions on Emerging Telecommunications Technologies. – 2025.
5. CareChain: Secure and scalable dual blockchain and IPFS driven IoT ecosystem for next gen healthcare systems / Scientific Reports. – 2025.
6. Minima Achieves Major Breakthrough: Blockchain-on-Chip Is Here / Minima Global. – 15 December 2025. – URL: <https://minima.global/ru/post/minima-achieves-major-breakthrough-blockchain-on-chip-is-here> (дата обращения: 16.03.2026).
7. IIT Madras. IIT Madras Develops Blockchain-based Healthcare Information Systems for Mobile Apps / Principal Scientific Adviser, Government of India. – 2026. – URL: <https://www.psa.gov.in/article/iit-madras-develops-blockchain-based-healthcare-information-systems-mobile-apps/2744> (дата обращения: 16.03.2026).
8. Sanobar, A., Anwar, S. A secure and privacy preserving model for healthcare applications based on blockchain-layered architecture / A. Sanobar, S. Anwar // International Journal of Computers and Applications. – 2024. – P. 1206-1218.

UDC 004.75:61

ARCHITECTURE OF A BLOCKCHAIN SUBSYSTEM FOR MEDICAL DATA

Katsko M.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Vishnyakov V.A. – Doctor of Technical Sciences, professor

Annotation. Existing international developments in blockchain systems designed for healthcare applications have been analyzed. Particular attention has been paid to projects such as Minima/Siemens/ARM (the "blockchain-on-a-chip" concept), BlockTrack (developed by IIT Madras), Emtruth (an NSF project), as well as the architectural solutions TLISA, STORChain, and CareChain. Based on the obtained data, an original multi-layered architecture for a blockchain subsystem intended for reliable storage of medical data is proposed.

Keywords. Blockchain, IT medicine, medical data, IPFS, architecture, decentralized storage, smart contracts, privacy, functional modules.

UDC 004.93: 004.8

HYBRID TRANSFORMER-GRAPH NEURAL NETWORK FEATURE MATCHING BASED METHODOLOGY FOR ROBUST TEMPLATE OBJECT LOCALIZATION

Bach N.V.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Tsviatkou V.Yu. – Doctor of Technical Sciences, Professor

Annotation. This paper proposes a novel framework that combines transformer-based and graph neural network-based feature matching techniques for accurate template object localization. The proposed pipeline consists of four main components: a hybrid features matching module, a non-linear geometric transformation module, and a bounding box refinement module. By integrating the strengths of both global contextual understanding from transformers and structural relationship modeling from graph neural networks, the method achieves improved robustness and precision in detecting and localizing objects under challenging conditions.

Keywords. Graph neural network, feature matching, template object localization, hybrid neural network.

Introduction. Template object localization is fundamental in applications ranging from industrial inspection and autonomous navigation to augmented reality. Traditional keypoints methods for template object localization such as scale-invariant feature transform (SIFT) or oriented FAST and rotated BRIEF (ORB) often struggle with large viewpoint changes, non-rigid deformations, and varying illumination. To overcome these challenges, it is proposed a hybrid strategy that intelligently combines the complementary strengths of efficient local feature matching (ELOFTR) with transformer [1, 2] and SuperPoint–SuperGlue with graph neural network (GNN) [3, 4] for creating a more robust and versatile feature matching system that can adapt to different image characteristics and application requirements and improve the accuracy and efficiency of finding correspondences between features in images. This approach integrates the powerful representational capabilities of transformers with the structural awareness of GNNs to create robust and adaptable matching models. Transformer owing to using self-attention and global view mechanisms is effective and flexible at capturing long-range dependencies and contextual information within data sequences or feature sets, understanding of relationships between features and adapting to various matching tasks by adjusting their architecture and training objectives. GNN due to using structure awareness mechanism and local neighborhood aggregation operates on graph-structured data, effectively capturing structural relationships and dependencies between features based on their connections and aggregates information from neighboring nodes, allowing them learn local feature representations and identify clusters.

This project presents a novel pipeline that integrates transformer-based and graph-based feature matching to accurately localize objects in a source image given a template. To achieve robust and precise object localization, our framework intelligently combines the hybrid features matching module, non-linear geometric transformation module and bounding box processing and analysis module.

The hybrid features matching module can integrate multi feature matching modules, but in project we use two submodels: transformer-based matcher (ELOFTR) and GNN-based matcher (SuperPoint–SuperGlue) (Figure 1). Integration of the ELOFTR and SuperPoint–SuperGlue feature matching module to generate good keypoints is based on computing confidence score that estimates how likely the module outputs are correct.

Input Stage. The template image (visual prompt) annotated with an initial bounding box in the XYXY format, defining the object's spatial extent. The template and the source images are a resolution frame (460×512) or (1920×1080) with bit depth varying between 8 and 24 bits. The template and the source images to be recognized may exhibit multi-dimensional differences, such as varying spectral bands, platforms, sources, resolutions, or perspectives.

Hybrid Feature Matching Module. At the core of our pipeline, we combine a transformer-based matcher (ELOFTR) with a graph-based matcher (SuperPoint + SuperGlue) to harvest both dense, globally consistent correspondences and sparse, locally refined keypoints. ELOFTR first divides the template and source images into fixed-size patches, embeds each via a linear projection, and injects learned positional encodings. A coarse cross-attention stage then establishes rough matches, which a fine-grained refinement head sharpens to sub-pixel accuracy—each correspondence tagged with a confidence score. In parallel, SuperPoint detects salient 2D keypoints and computes 256-dimensional descriptors; SuperGlue builds a bipartite graph over template and source points, performs iterative cross-graph attention, and solves an optimal-transport problem to yield robust match pairs.

Non-linear geometric transformation module. In this module, we first prune and concatenate the keypoints correspondences generated by ELOFTR and SuperGlue. The retained matches are then used to robustly estimate a projective homography H through RANSAC algorithm, which automatically rejects

outliers. Finally, the four corners of the template's object bounding box are warped through H to yield a provisional object region in the source image, ready for downstream contour-based refinement.

Bounding-box refinement module. In the final stage, we refine the provisional bounding box by leveraging local edge and contour information to achieve precise object delineation. First, we extract a crop of the source image defined by the warped corners of the provisional box. This region is converted to grayscale and subjected to adaptive Gaussian thresholding, which dynamically segments foreground and background based on local intensity variations. From the resulting binary mask, we detect all connected contours and evaluate each by computing its area overlap with the provisional box. The contour exhibiting the maximum overlap is assumed to correspond to the target object's silhouette. Finally, we fit a minimum-area enclosing rectangle around this contour, and convert its corner coordinates into the standard XYYX format to produce the final, refined bounding box.

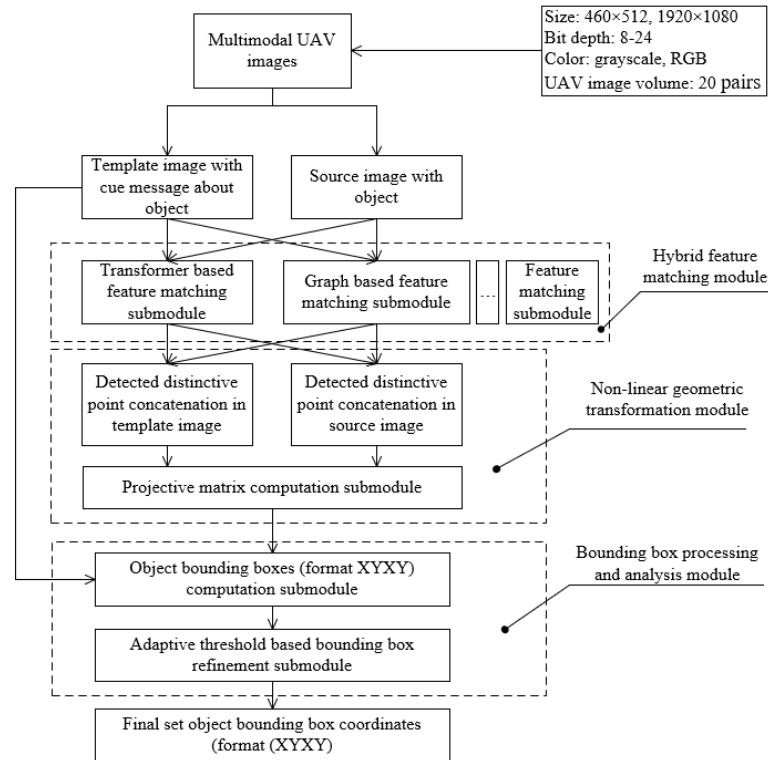


Figure 1 – Integrated modular feature matching structure

Estimation of the hybrid features matching module performance. Table 1 summarizes the average IoU-based score values (1) providing by using the ELoFTR and SuperPoint+SuperGlue matcher submodules and hybrid feature matching module on our test sets of 20 image pairs.

$$scorevalue = \begin{cases} 1 + (IoU - 0.75) \cdot 4, & 0.5 < IoU \leq 1.0 \\ 0, & 0.3 \leq IoU \leq 0.5 \\ -0.5, & IoU < 0.3 \end{cases} \quad (1)$$

Table 1 – Estimation of template object detection score values for submodules and hybrid module

Type of submodule	Score value
ELoFTR submodule	12.39
SuperPoint+SuperGlue submodule	5.6
Hybrid Feature Matching Module	15.6

It follows from Table 1 provides the score value of template object detection is increased from 3.21 to 10 score value with using the hybrid feature matching module for the given multimodal UAV images.

Figure 2 and Figure 3 present comparative results of different feature matching approaches under various image conditions. It can be observed that the hybrid feature matching module consistently achieves the most accurate object localization, with bounding boxes closely aligned to the target objects. In contrast, the SuperPoint+SuperGlue method shows lower precision due to limited global context, while ELoFTR provides better global matching but lacks fine localization accuracy. Overall, the results demonstrate that the hybrid approach effectively combines the strengths of both methods, leading to improved robustness and detection performance across different scenarios.

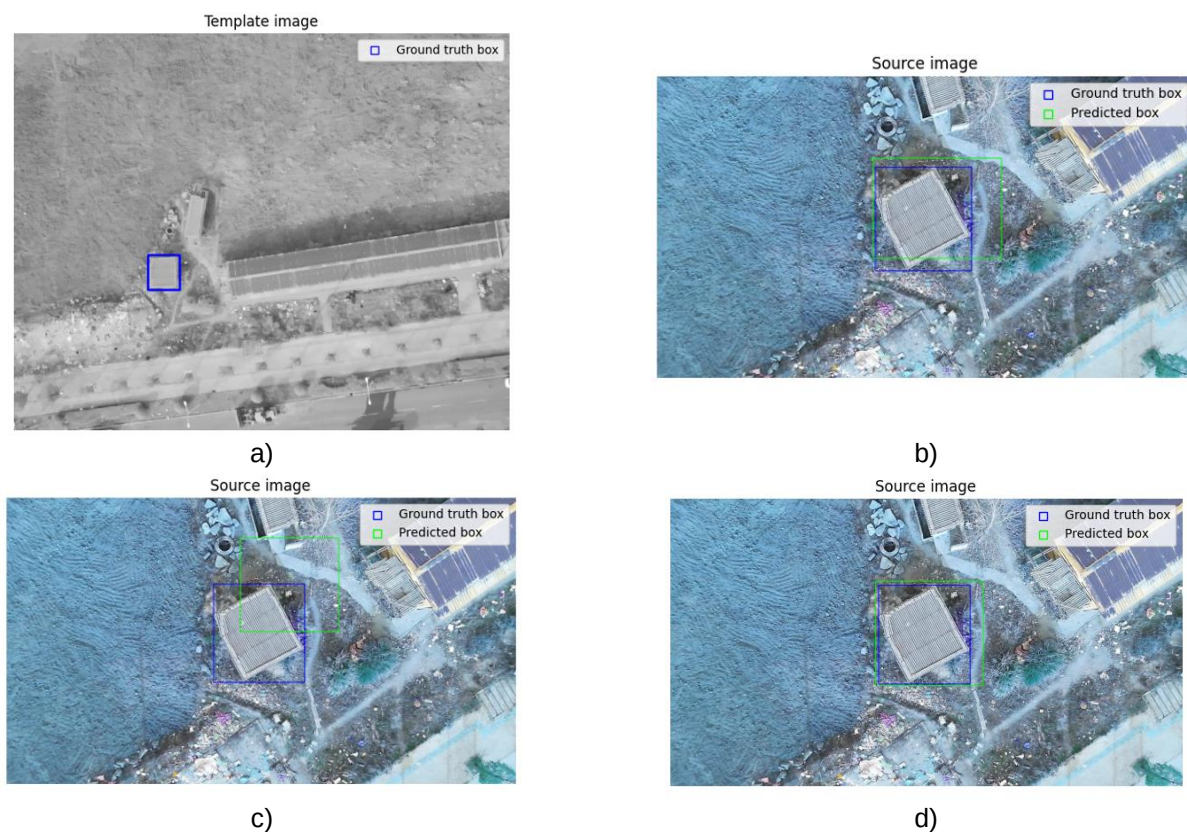


Figure 2 – Grayscale template (a) and color source images with detected object bounding box using hybrid feature matching module (b), only SuperPoint+SuperGlue submodule (c), only ELoFTR submodule (d)

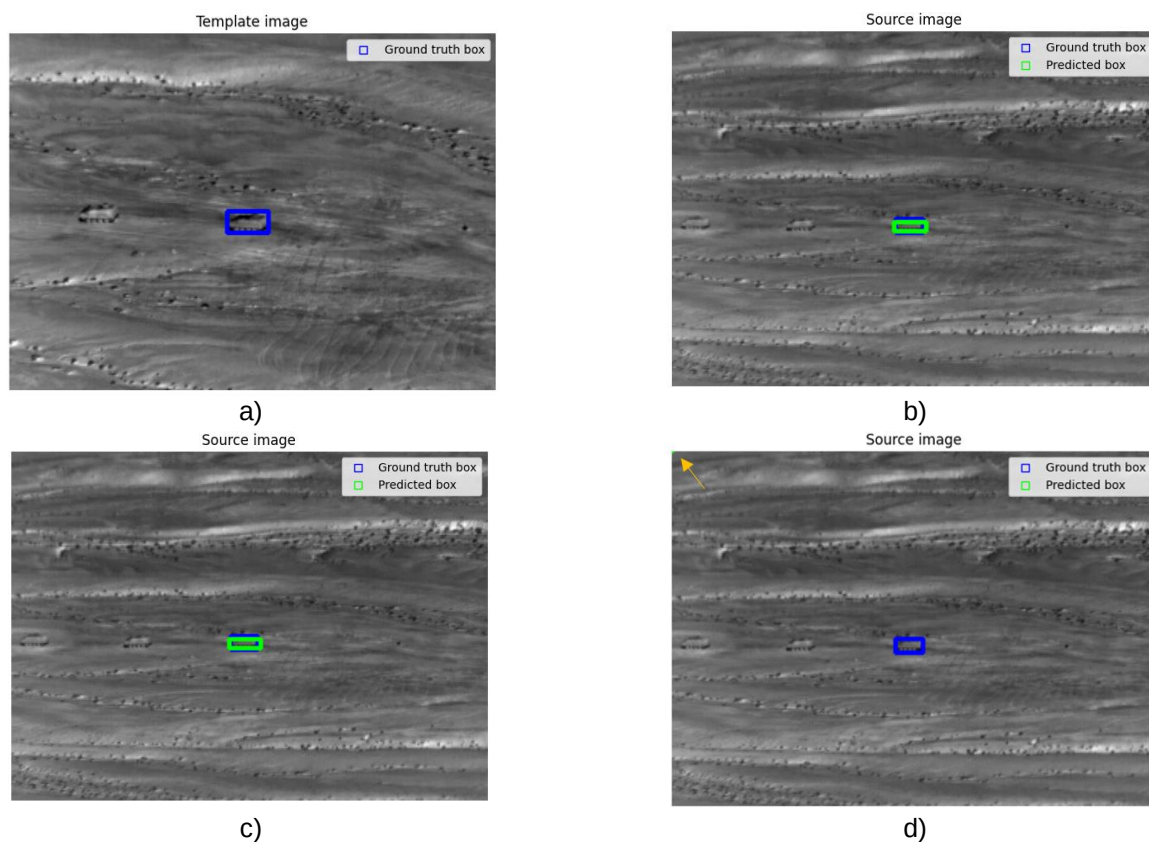


Figure 3 – Grayscale template (a) and source images with detected object bounding box using hybrid feature matching module (b), only SuperPoint+SuperGlue submodule (c), only ELoFTR submodule (d)

Visualization of bounding-box refinement module efficiency. The Figure 4 contains detected object image with (a) and without (b) using bounding box processing and analysis module.

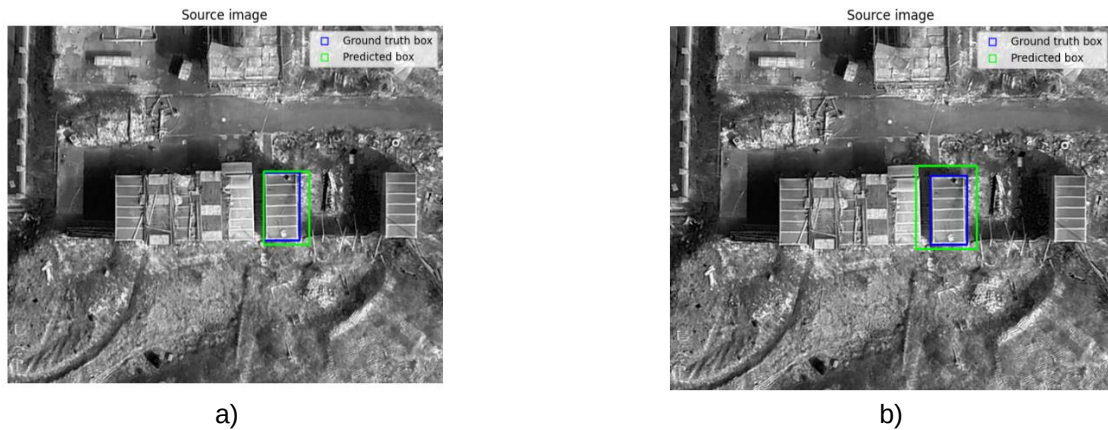


Figure 4 – Detected object bounding box with (a) and without (b) bounding box processing and analysis module

It follows from Figure 4 that bounding box processing and analysis module improves template object detection accuracy for the given multimodal UAV images.

Conclusion. In this paper, we proposed a hybrid object localization framework that integrates transformer-based and graph neural network-based feature matching with robust geometric transformation and contour-based bounding box refinement. By combining global contextual modeling and structural relationship learning, the proposed approach achieves high localization accuracy and robustness under challenging conditions such as scale variation and multimodal differences. Experimental results demonstrate that the hybrid feature matching module significantly outperforms individual methods, confirming the effectiveness of the overall pipeline.

References:

1. He, X. *Matchanything: Universal cross-modality image matching with large-scale pre-training* / H. Yu, S. Peng, D. Tan, Z. Shen, H. Bao, X. Zhou // *arXiv preprint arXiv*, 2025. – P. 2501.07556.
2. Wang, Y. *Efficient LoFTR: Semi-dense local feature matching with sparse-like speed* / X. He, S. Peng, D. Tan, and X. Zhou // *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2024. – P. 21666-21675.
3. Sarlin, P. E. *Superglue: Learning feature matching with graph neural networks* / DeTone, D., Malisiewicz, T., & Rabinovich, A. // *In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2020. – P. 4938-4947.
4. DeTone, D. *Superpoint: Self-supervised interest point detection and description* / T. Malisiewicz, A. Rabinovich // *In Proceedings of the IEEE conference on computer vision and pattern recognition workshops*, 2018. – P. 224-236.

TIME DELAY-PHASE HARMONIC MODEL OF TRANSMITTED LASER SIGNAL FOR GAS CONCENTRATION ESTIMATION

Bach N.V.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Tsviatkou V.Yu. – Doctor of Technical Sciences, Professor

Annotation. The proposed time delay-phase harmonic model takes into account absorption, scattering, and reflectance effects and the relationship between the phase shift and the time delay and the absorption pulse signal quality. The Levenberg–Marquardt algorithm is applied to define optimal model parameters, enabling an efficient and effective of gas concentration estimation process. Experimental results demonstrate a strong correlation between the harmonic ratio feature and methane concentration under varying laser power conditions. Furthermore, the phase shift effect on the absorption signal is investigated, revealing its impact on waveform symmetry and peak distribution. The proposed method has been proven to require only a few signal cycles for gas concentration estimation.

Keywords. Tunable diode laser absorption spectroscopy, gas concentration, Levenberg–Marquardt algorithm, harmonic model, time delay, phase shift.

Introduction. One of the most promising approaches for remote methane detection, even at extremely low concentrations, is optical methods. Tunable diode laser absorption spectroscopy (TDLAS) is among the most effective optical techniques for this purpose [1, 2]. There are three primary variations of TDLAS: direct absorption spectroscopy (DAS) [3, 4], wavelength modulation spectroscopy (WMS) [5, 6], and wavelength modulation-direct absorption spectroscopy (WM-DAS) [7, 8].

Direct absorption spectroscopy is the simplest form of TDLAS, requiring minimal equipment and offering straightforward alignment and data interpretation. However, its sensitivity is limited due to inherent uncertainty in the laser output signal measurements. On the other hand, wavelength modulation spectroscopy (WMS) overcomes this limitation by using harmonic detection technology, which enables higher modulation frequencies-sometimes reaching several hundred kHz-thereby improving sensitivity and eliminating baseline uncertainty. As a result, WMS is more resilient to low-frequency noise and offers enhanced measurement accuracy. This technology has been widely studied and implemented for gas property measurements.

Although WMS provides higher accuracy and sensitivity compared to direct absorption spectroscopy, it is more complex to implement due to the need for signal modulation and the use of lock-in amplifiers. The WM-DAS method combines the simplicity and calibration-free benefits of direct absorption spectroscopy with the high sensitivity and noise rejection capabilities of harmonic detection, making it a powerful and reliable technique for methane concentration estimation.

The goal of our paper is to develop harmonic models of the interaction laser light with gas for providing the trade-off between computational complexity, robustness and accuracy of gas concentration estimation. The key contributions of our paper can be summarized as follows:

- the proposed harmonic model of the absorption pulse signal is based on time delay and phase shift and optimal model parameter estimation influencing on the signal pulse quality related to gas concentration;
- the harmonic ratio feature of an extracted-and-formed absorption pulse defined by the ration of the sum of the even harmonic amplitudes of absorption pulse signal to the fundamental harmonic amplitude is proposed for estimating gas concentration.

Methodology of the harmonic model integration. Based on the analysis of the harmonic properties of the absorption pulse signal $I_{abs}(t, \lambda)$, the proposed time delay-phase harmonic model of this signal is defined as:

$$I_{abs}(t, \lambda, \Delta t, \varphi) = \sum_{k=1}^{K_H/2} (C_{2k}(\lambda) \sin(2\pi \cdot 2kf_1 \cdot (t + \Delta t) + \varphi)), \quad (1)$$

where $C_{2k} = \sqrt{A_{2k}^2 + B_{2k}^2}$ is the amplitude of the k -th even harmonics, Δt and φ are the time delay and phase shift of the absorption pulse signal influencing the position and shape of absorption pulses.

The absorption pulse signal $I_{abs}(t, \lambda, \Delta t, \varphi)$, fundamental harmonic signal $I_{RAW}^{f_1}(t)$, DC component $I_{DC}(t)$ and the attenuation coefficient K_{env} are computed by the Levenberg–Marquardt algorithm [9]. The Levenberg–Marquardt algorithm provides a trade-off between computational complexity and concentration accuracy.

Given a set of m empirical samples $(t, I_{tr}(t, \lambda, K_{env}))$ of independent and dependent variables, we find the optimal parameters β_{opt} from $\beta = \{A_1, B_1, I_{DC}, K_{env}\} \cup \{C_{2k}\}_{k=1, \dots, K_H}$ by using the objective function represented as:

$$\beta_{opt} = \underset{\beta}{\operatorname{argmin}} \sum_{t=1}^m \left(I_{tr}(t, \lambda, K_{env}) - \hat{I}_{tr}(t, \lambda, \beta) \right)^2, \quad (2)$$

where $\hat{I}_{tr}(t, \lambda, \beta) = \left(I_{DC}(t, \lambda) + I_{RAW}^{f_1}(t, \lambda) + I_{abs}(t, \lambda, \Delta t, \varphi) \right) \cdot K_{env}(\lambda)$ is the estimated transmitted laser intensity signal.

Values $\Delta t = \left(\arctan\left(\frac{B_{2k}}{A_{2k}}\right) - \varphi \right) / (2\pi \cdot 2kf_1)$ is defined from φ and $\{A_{2k}, B_{2k}\}$, which are computed by the objective function (2).

The harmonic ratio feature of absorption pulse A_{ab} is defined as the sum of the harmonic component's amplitudes of absorption pulse signal $I_{abs}(t, \lambda, \Delta t, \varphi)$ divided by the amplitude of the fundamental component $I_{RAW}^{f_1}(t, \lambda)$ for reducing systematic noise, represented as:

$$A_{ab}(\lambda) = \frac{\sum_{k=1}^{K_H/2} C_{2k}(\lambda)}{C_1(\lambda)}, \quad (3)$$

where $C_1 = \sqrt{A_1^2 + B_1^2}$ is the amplitude of the fundamental harmonic.

Estimation of the linear weight coefficients of the even harmonics. The Levenberg–Marquardt algorithm based on using the objective function (2) allows us to estimate the linear weight coefficients A_{2k} and B_{2k} (Table 1) for the most significant even harmonics $K_H = 7$.

Table 1 – Estimation of the linear weight coefficients (A and B) of the even harmonics under laser power 166 nW

Even harmonic indexes k	Methane gas concentration									
	100 ppm		250 ppm		540 ppm		1000 ppm		2000 ppm	
	A	B	A	B	A	B	A	B	A	B
2	-12580.3	-15060.3	-15949.8	-18362.2	-41067.3	-44922.1	-57938.1	-61931.8	-84645.2	-88710.2
4	-21423.6	493.9	-26671.6	784.3	-55775.1	2751.2	-76085.5	4227.8	-98583.9	5551.1
6	-4972.6	6505.5	-9722.10	12307.5	-19997.9	26414.4	-32743.2	42695.6	-48527.9	63852.8
8	1119.6	2610.1	1934.44	7812.8	4542.6	24875.2	7049.8	36113.5	11825.8	61218.7
10	3961.8	2352.2	6853.37	3801.7	12326.7	7339.7	22683.9	13926.6	37705.4	23071.7
12	4812.1	-1420.9	6224.06	-1600.9	13857.6	-3812.7	21908.2	-5800.3	33656.4	-9528.7
14	1140.3	-2185.3	2210.94	-5131.0	3209.2	-6334.2	5966.1	-11647.9	9882.9	-19649.9

Estimation of the phase shift value of absorption signal. Figure 1 shows influence of the phase shift values $(-\frac{\pi}{2}, -\pi, -\frac{\pi}{4})$ on the shape, amplitude and symmetry of the absorption pulses of signal $I_{abs}(t, \lambda, \Delta t, \varphi)$ using time delay-phase harmonic model.

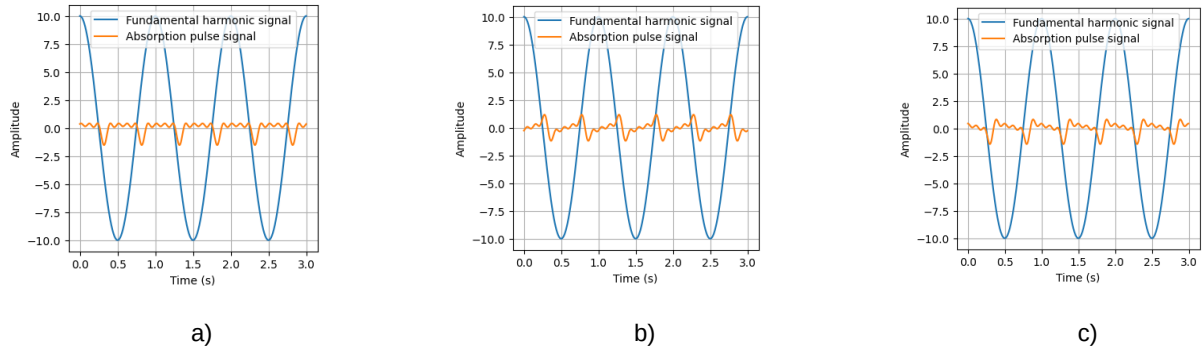


Figure 5 – Influence of the phase shift values on the absorption signal pulse parameter:

a) $\varphi = -\frac{\pi}{2}$, b) $\varphi = -\pi$, c) $\varphi = -\frac{\pi}{4}$

If $\varphi = -\frac{\pi}{2}$, then the positive part of the absorption pulse signal tends to flatten, while the negative part reaches two extrema within one fundamental period. If $\varphi < -\frac{\pi}{2}$, then the positive component skews higher on the right. If $\varphi > -\frac{\pi}{2}$, then the positive component shifts higher on the left, and the negative part does not reach its minimum value as in the case of $\varphi = -\frac{\pi}{2}$.

The optimal phase shift value of the absorption signal is determined to be $\varphi = -\frac{\pi}{2}$ due to the laser light absorption of the target gas.

Estimation of time delay value of the absorption pulse signal. After defining parameters A_{2k} , B_{2k} and φ , the parameter Δt is computed for the laser power of 166 nW (Table 2). It follows from Table 2 that the time delay of the second harmonic is equal to -5.58×10^{-5} s, while for the other harmonics, it is approximately equal to -6.60×10^{-6} s.

Estimation of gas concentration based on the time delay-phase harmonic model. Linear regression models of the relationship between the harmonic ratio feature A_{ab} and methane concentration

under the time delay of the second harmonic -5.58×10^{-5} s, and other harmonics -6.60×10^{-6} s, $\varphi = -\frac{\pi}{2}$ for the most significant even harmonics $K_H = 7$ are shown in Figure 2. Using the proposed time delay-phase harmonic model (1) and the objective function (2), we find the optimal parameters β_{opt} and then the harmonic ratio feature of absorption pulse A_{ab} corresponding to concentration under different laser powers.

Table 2 – Estimation of the time delay of the absorption pulse signal under a laser power of 166 nW

Time delay Δt (s) ($\times 10^{-6}$)	Even harmonic index k	Methane gas concentration				
		100 ppm	250 ppm	540 ppm	1000 ppm	2000 ppm
-55.8	2	-55.5	-55.7	-55.9	-56.0	-56.1
-6.60	4	-6.34	-6.37	-6.45	-6.47	-6.47
-6.60	6	-6.60	-6.56	-6.61	-6.60	-6.61
-6.60	8	-7.06	-6.73	-6.61	-6.63	-6.63
-6.60	10	-6.65	-6.69	-6.65	-6.62	-6.63
-6.60	12	-6.63	-6.58	-6.61	-6.59	-6.62
-6.60	14	-6.60	-6.68	-6.61	-6.60	-6.61

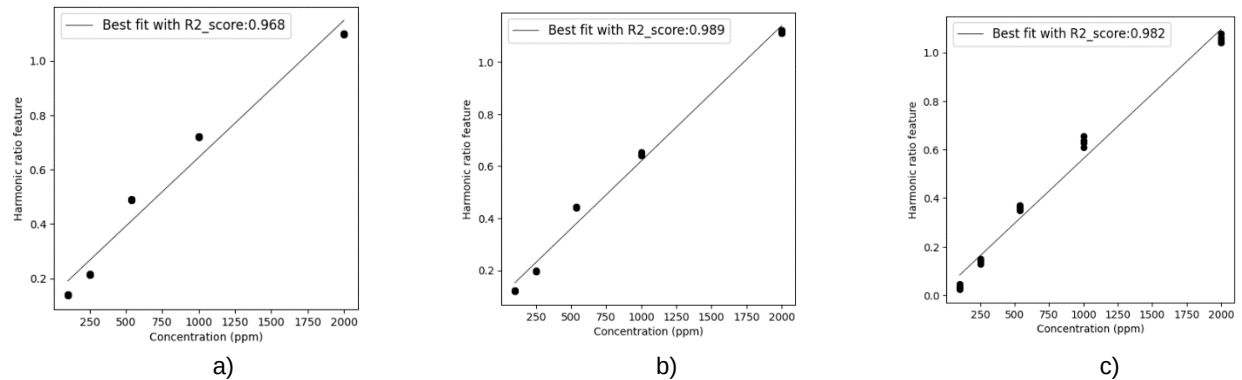


Figure 2 – Relationship between the harmonic ratio feature A_{ab} and methane concentration under different laser powers: a) 166 nW, b) 9 nW, and c) 2 nW

It follows from Figure 2 that the correlation coefficient R^2 under different laser powers is close to 1, which indicates a good fit between our observed and expected data. The time delay and phase shift values are not affected by variations in laser power. It is determined that the absorption signal energy is concentrated in the lower even harmonics.

Conclusion. The proposed method optimizes gas absorption parameters by an objective function used in the Levenberg–Marquardt algorithm. Experimental results demonstrate a strong correlation ($R^2 > 0.97$) between the harmonic ratio feature and methane concentration across different laser power changes, validating the robustness of the method. Additionally, the impact of phase shift on waveform symmetry and peak distribution is analyzed, highlighting its significance in signal interpretation. The time delay for the second harmonic is equal to -5.58×10^{-5} s, for higher harmonics it is approximately -6.60×10^{-6} s and a phase shift of $\varphi = -\frac{\pi}{2}$ allow us to reduce time complexity by decreasing the number of parameters in the proposed models.

References:

1. Nadezhdinsky, A.I. Preliminary results of an aircraft system based on near-IR diode lasers for continuous measurements of the concentration of methane, carbon dioxide, water and its isotope / Y.Y. Ponurovsky, Y.P. Shapovalov, I.P. Popov // *Applied Physics B*, 2012 Jun. –Vol. 109, iss. 6. –P. 505-510.
2. Ponurovskii, Y.Y. New possibilities for analyzing the biological role of hydrogen, methane and other biomarkers of gut microbiota activity using tunable diode laser absorption spectrometry and selective hydrogen and oxygen sensors / D.B. Stavrovskii, I.V.E. Shirokov, F.I. Romanikhin // *Optics and Spectroscopy*, 2024. –Vol. 132, iss. 2. –P. 303-309.
3. J. Wojtas, J. Aspect of the applications of cavity enhanced spectroscopy to nitrogen oxides detection / Z. Bielecki // *Sensors (Basel)*, 2013 Jun. –Vol. 13, iss. 6. –P. 7570-98.
4. Goldenstein, C. S. Diode laser measurements of linewidth and temperature-dependent lineshape parameters of H₂O-, CO₂-, and N₂-perturbed H₂O transitions near 2474 and 2482 nm / J. B. Jeffries, R. K. Hanson // *Journal of Quantitative Spectroscopy and Radiative Transfer*, 2013. –Vol. 130. –P. 100-111.
5. Yihong, W. Calibration-free wavelength modulation spectroscopy based on even-order harmonics / Z. Bin, L. Chang // *Opt. Express*, 2021. –Vol. 29. –P. 26618-26633.
6. Aветисов V. Hydrogen Sensor Based on Tunable Diode Laser Absorption Spectroscopy / O. Bjoroey, J. Wang, P. Geiser // *Sensors*, 2019. –Vol. 19, iss. 23. –P. 5313-5323.
7. Liang R. A Fourier-domain-based line shape recovery method used in direct absorption spectroscopy / F. Wang, Q. Xue, Q. Wang, J. Wu, Y. Cheng, Q. Li // *Spectrochimica Acta Part A: Molecular and Biomolecular Spectroscopy*, 2022. –Vol. 275. –P. 313-323.
8. Peng Z. Highly Sensitive, Calibration-Free WM-DAS Method for Recovering Absorbance—Part I / Y. Du, Y. Ding // *Sensors*, 2020. –Vol. 20, iss. 3. –P. 681-715.
9. Vugrin K. Confidence region estimation techniques for nonlinear regression in groundwater flow: Three case studies / L.P. Swiler, R.M. Roberts, N.J. Stucky- Mack and S.P. Sullivan // *Water Resources Research*, 2007. –Vol. 43, iss. 3. –P. 6313-6323.

СЕКЦИЯ «ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ СИСТЕМЫ»

УДК 621.317.78

МЕТОДИКА ОПРЕДЕЛЕНИЯ МЕТРОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК УСТРОЙСТВ СЛИЧЕНИЯ НАЦИОНАЛЬНОГО ЭТАЛОНА МОЩНОСТИ ЭЛЕКТРОМАГНИТНЫХ КОЛЕБАНИЙ

Доронина А.В., студент гр.467241

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Белошицкий А.П. – канд. техн. наук, доцент

Аннотация. В материалах доклада рассматривается разработанная методика определения метрологических характеристик (МХ) устройств сличения из состава национального эталона единицы мощности электромагнитных колебаний в диапазоне частот от 37,5 до 178,4 ГГц.

Ключевые слова. Методика, метрологические характеристики, устройства сличения, эталон, мощность, сверхвысокая частота.

Стремительное развитие современных радиотехнических комплексов, систем связи, радиолокации и навигации обусловило интенсивное освоение миллиметрового диапазона длин волн. На частотах свыше 37,5 ГГц прямое измерение традиционных электрических параметров, таких как ток и напряжение, становится технически нереализуемым из-за соизмеримости геометрических размеров измерительных цепей с длиной волны. В связи с этим фундаментальной энергетической характеристикой высокочастотного тракта выступает поглощаемая мощность электромагнитных колебаний [1]. Обеспечение достоверности и высокой точности измерения данного параметра является критически важной задачей при проектировании, производстве и эксплуатации современной СВЧ-аппаратуры.

В целях обеспечения единства измерений и метрологической прослеживаемости в расширенном частотном спектре на территории Республики Беларусь в рамках реализации государственной научно-технической программы был разработан Национальный эталон единицы мощности электромагнитных колебаний [2]. Созданный аппаратно-программный комплекс перекрывает диапазон частот от 37,5 до 178,4 ГГц.

Одними из основных функциональных элементов разработанного эталона выступают устройства сличения. Их основное назначение заключается в направленном разделении электромагнитной энергии для обеспечения прецизионного сравнения уровней мощности между первичным эталонным преобразователем и калибруемым средством измерений. Поскольку именно данные узлы осуществляют непосредственную передачу размера единицы физической величины в тракте, к стабильности их параметров предъявляются жесткие требования.

Неотъемлемым этапом ввода эталонного оборудования в эксплуатацию является экспериментальное подтверждение его метрологических характеристик. Возникает необходимость разработки и апробации методик определения параметров и характеристик отдельных функциональных устройств и блоков эталона. Целью настоящей работы является разработка методики экспериментального определения МХ устройств сличения, гарантирующей минимизацию инструментальных погрешностей и функциональную пригодность эталона.

Оборудование, подлежащее исследованию, представляет собой набор устройств сличения, выполненных на базе прямоугольных волноводов. Исходя из физических ограничений на распространение электромагнитной волны основного типа, рабочий диапазон частот эталона конструктивно разделен на поддиапазоны. Каждому поддиапазону соответствует отдельное устройство сличения с нормированным сечением волноводного тракта: УС-MBM-53, УС-MBM-78, УС-MBM-118 и УС-MBM-178, внешний вид которых представлен на рисунке 1.

Схемотехнически каждое устройство сличения включает в себя основной измерительный канал, предназначенный для транзита высокочастотного сигнала от источника к калибруемому средству измерений, и вспомогательный канал, служащий для ответвления нормированной части мощности на эталонный измеритель. Данная архитектура позволяет осуществлять непрерывный мониторинг уровня падающей мощности без существенного нарушения режима работы основного тракта.



Рисунок 1 – Внешний вид устройств сличения УС-MBM-53, УС-MBM-78, УС-MBM-118, УС-MBM-178

Для подтверждения пригодности устройств сличения к использованию в составе эталонного комплекса необходимо экспериментально определить их основные МХ. Первой характеристикой является коэффициент стоячей волны по напряжению (КСВН) измерительных портов основного и вспомогательного каналов в рабочем диапазоне частот, определяющий степень согласования устройства с подводящими линиями. Второй определяемой величиной выступает коэффициент передачи устройства сличения, количественно характеризующий вносимое ослабление при передаче сигнала между каналами.

Оценка качества согласования измерительных портов, выражаемая через КСВН, осуществляется методом прямых измерений с помощью измерителей КСВН панорамных Р2-120, Р2-121, РР2-01, Р2-123 по схеме, приведенной на рисунке 2.

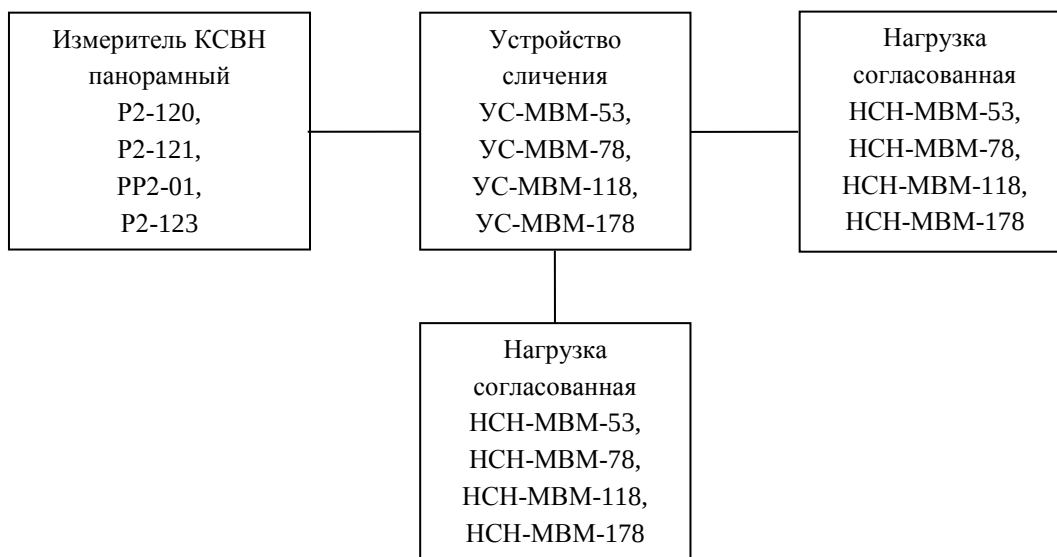


Рисунок 2 – Структурная схема измерения КСВН

Критически важным условием обеспечения требуемой точности и минимизации инструментальной погрешности является предотвращение возникновения паразитных резонансов в измерительном тракте. В связи с этим, при измерениях неподключенные к измерителю КСВН панорамному выходы устройства сличения должны быть соединены с нагрузками согласованными НСН-MBM-53, НСН-MBM-78, НСН-MBM-118, НСН-MBM-178 соответствующего сечения. Применение данных поглощающих элементов гарантирует полное рассеивание проходящей мощности и исключает влияние переотражений от свободных портов на итоговый результат.

Определение коэффициентов передачи основного и вспомогательного каналов устройства сличения осуществляется методом замещения по схеме, приведенной на рисунке 3. Для этого собирается измерительная цепь, включающая источник высокочастотного сигнала, поляризационный аттенюатор и измеритель поглощаемой мощности. На начальной стадии производится калибровка тракта: при отсутствии исследуемого устройства в цепи устанавливается опорный уровень мощности, при этом фиксируется начальное значение вносимого ослабления на поляризационном аттенюаторе A_{a1} .

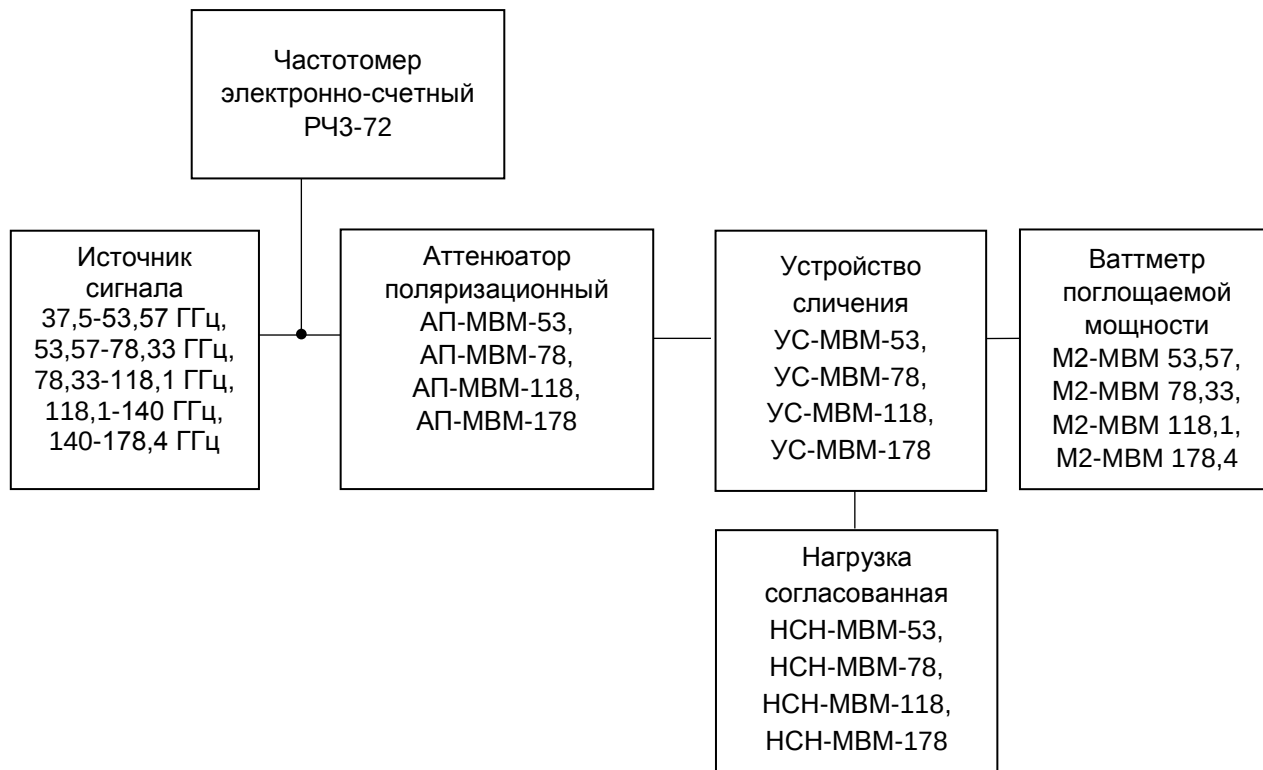


Рисунок 3 – Структурная схема измерения коэффициента передачи

Далее в разрыв измерительной цепи, непосредственно между поляризационным аттенюатором и ваттметром, подключается исследуемое устройство сличения. Вследствие внутренних электродинамических потерь в волноводном узле уровень мощности закономерно снижается. Для компенсации вносимых потерь ослабление поляризационного аттенюатора плавно уменьшается вплоть до точного восстановления первоначально зафиксированного показания ваттметра. Новое значение ослабления A_{a2} регистрируется в протоколе, после чего искомый коэффициент передачи вычисляется по следующей формуле:

$$K_n = A_{a1} - A_{a2}, \quad (1)$$

где K_n – коэффициент передачи устройства сличения на заданной частоте, дБ; A_{a2} – значение ослабления аттенюатора поляризационного после подключения устройства сличения для компенсации потерь, дБ; A_{a1} – начальное значение ослабления аттенюатора поляризационного, зафиксированное при калибровке опорного уровня, дБ.

Разрабатываемая методика определения МХ устройств сличения национального эталона мощности электромагнитных колебаний в диапазоне частот 37,5 – 178,4 ГГц позволяет экспериментально определить их количественные значения и оценить их вклад в общую неопределенность измерений, выполненных с помощью указанного эталона

Список использованных источников:

1. Измерение мощности СВЧ в диапазоне сантиметровых и миллиметровых волн / И.Ф. Бурак, А.В. Гусинский, Г.А. Шаров и др. – М.: Горячая линия – Телеком, 2018. – 328 с.
2. Инженерное образование в цифровом обществе: материалы Междунар. науч.-метод. конф. (Республика Беларусь, Минск, 14 марта 2024 года) В 2 ч. Ч.1 / редкол.: Е.Н. Шнейдеров [и др.]. – Минск : БГУИР, 2024. – С.298-301.

UDC 621.317.78

METHODOLOGY FOR DETERMINING THE METROLOGICAL CHARACTERISTICS OF COMPARISON DEVICES OF THE NATIONAL ABSORBED POWER STANDARD

Doronina A.V. gr. 467241

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Beloshitsky A.P. – PhD in Technical Sciences, Associate Professor

Annotation. The article discusses a scientifically based methodology for studying the technical and metrological characteristics (MC) of comparison devices that form the functional basis of the developed National Standard for the unit of electromagnetic oscillation power in the frequency range from 37.5 to 178.4 GHz. Based on approved test programs, the procedures for direct measurement of the voltage standing wave ratio and indirect measurement of the transmission coefficient are described. The presented algorithmic approach allows for a highly reliable evaluation of the parameters of microwave measuring paths, minimization of hardware errors, and provision of state uniformity of measurements when transferring the unit size.

Keywords. Comparison device, national standard, absorbed power, metrological characteristics, transmission coefficient, voltage standing wave ratio, millimeter wave band.

УДК 621.317.08

АППАРАТНО-ПРОГРАММНАЯ АРХИТЕКТУРА ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНОЙ СИСТЕМЫ С СЕТЕВЫМИ ВОЗМОЖНОСТЯМИ

Зокиров Д.Т., гр.426401

*Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь*

Гусинский А.В. – доктор технических наук, профессор

Аннотация. В докладе рассматривается разработанная аппаратно-программная архитектура информационно-измерительной системы (ИИС) с сетевыми возможностями, обеспечивающая метрологически корректную, надёжную и безопасную работу в условиях распределённых и дистанционных измерений, а также поддержку интеграции модулей искусственного интеллекта.

Ключевые слова. Аппаратно-программная архитектура, информационно-измерительная система, сетевые возможности, дистанционные измерения, метрологическая корректность.

Цель разработки – обеспечить метрологически корректную, удобную в эксплуатации и безопасную ИИС СВЧ диапазона с возможностью дистанционного управления, централизованного хранения результатов и интеграции ИИ-модулей. Основные требования включают учёт сетевых влияний в бюджете неопределённости, аппаратную синхронизацию времени, отказоустойчивость и встроенные механизмы безопасности. [1,2]

Ключевые принципы. Базовым требованием архитектуры является метрологическая корректность: все элементы сети и программного обеспечения учитываются при составлении бюджета неопределённости, а привязка ко времени выполняется аппаратными средствами (PTP/GPS) для минимизации вклада сетевой инфраструктуры в фазовые и временные погрешности. Для этого в метаданные каждого измерения включается информация об источнике времени и аппаратных timestamp.

Для обеспечения устойчивости к сбоям система проектируется с локальной буферизацией и возможностью автономной работы: при потере связи накопленные данные сохраняются в устойчивой очереди, что позволяет продолжать измерения без потери информации. После восстановления соединения механизм реплея гарантирует корректную и детерминированную доставку данных на центральный сервер.

Безопасность реализована по принципу «secure by default»: все каналы связи защищены mTLS/TLS, результаты подписываются цифровыми подписями, а операции фиксируются в журнале только для дозаписи (append-only) для последующего аудита. Ключи для подписи хранятся в HSM или защищённых элементах, что снижает риск компрометации.

Модульность и масштабируемость достигаются через строго определённые интерфейсы между аппаратными блоками (генератор, СВЧ тракт, FPGA/АЦП), контроллерами и сетевыми шлюзами. Каждый модуль имеет документированный API и набор метаданных, что облегчает замену, добавление или обновление компонентов и интеграцию внешних сервисов, включая модули искусственного интеллекта.

Технические требования. Коммуникационные интерфейсы устройств должны обеспечивать как минимум 1 GbE, при высоких нагрузках – предпочтительна поддержка 10 GbE; для выездных/полевых применений возможна опция Wi-Fi или LTE с учётом их влияния на метрологию. Важным требованием является аппаратная синхронизация времени: предпочтительны PTP с аппаратными timestamp'ами или GPS PPS; NTP допустим только для задач, не чувствительных к фазе.

Для управления системой рекомендуется применять REST/WebSocket через TLS, а для плотных потоков измерительных данных – двоичные протоколы (Protocol Buffers или Chunked TCP). Каждый пакет данных должен включать обязательные поля: идентификатор устройства, порядковый номер, метку времени и источник времени, полезные данные, сетевые метрики (RTT, loss, jitter), цифровую подпись и CRC для контроля целостности.

Локальная persistent-буферизация обязана покрывать минимум суточный объём измерений при типичной нагрузке, обеспечивая выживание при падении сети и возможность корректной повторной передачи данных после восстановления связи. Механизмы очереди должны выдерживать перезапуск приложения и аппаратные рестарты.

Требования к безопасности включают mTLS для связи прибор↔сервер, подписание результатов с ключами в HSM, append-only журнал аудита и регламент ротации ключей. Политики доступа реализуются через централизованные механизмы аутентификации и авторизации.

Ключевые показатели эффективности. Необходим контроль вклада сетевых факторов в расширенную неопределённость измерений – U_{net} должен быть ограничен на уровне, согласованном с категорией измерений. Ограничение по временной синхронизации выражается в допуске по offset, вычисляемом из допустимой фазовой ошибки по формуле $\Delta\phi = 2\pi f_{\text{max}} \Delta t$, что задаёт целевое значение Δt .

Сетевые операционные метрики включают медианный RTT (p50) порядка 50 ms для эффективной дистанционной калибровки; при RTT до 100 ms допускается работа с адаптивными алгоритмами. Приемлемый уровень потерь пакетов – до 0.5%; при превышении этого порога система переключается в режим повышенной усреднённости или локальной обработки. Допустимый RMS джиттера для фазочувствительных задач – порядка 5 ms.

Надёжность оценивается долей успешной доставки накопленных данных после восстановления сети (целевой показатель $\geq 99.9\%$) и временем выравнивания очереди (time-to-sync) не более 5 минут при стандартных объёмах записей.

Операционные метрики включают время отклика API (p95 < 200 ms, p99 < 1 s) и время установления удалённой сессии (handshake + readiness) в LAN менее 2 секунд. По безопасности – требования к подписанным файлам и ежегодной ротации ключей.

Поведение при авариях. При ухудшении качества сети система автоматически переводится в автономный режим: данные продолжают накапливаться локально и маркируются как «offline», при этом сохраняется информация о сетевых условиях в net_metrics. После восстановления соединения запускается упорядоченная передача накопленных данных с контролем целостности и подписи.

В случае потери синхронизации времени измерения помечаются, raw-данные сохраняются, генерируется уведомление для оператора и предпринимаются автоматические попытки восстановления PTP/GPS. Если синхронизация не восстанавливается, в отчётах фиксируется степень неопределённости, связанная с временным источником.

При обнаружении недействительной цифровой подписи или несоответствии CRC отправка пакета блокируется, инцидент попадает в журнал и администратор оповещается. Дополнительно инициируются процедуры расследования и, при необходимости, повторной верификации данных.

Требуемые при вводе в эксплуатацию тесты. Необходимо провести проверку пропускной способности (iperf3 для 1 GbE и 10 GbE), длительные тесты синхронизации времени (оценка offset и drift PTP/GPS в течение 24–72 часов), а также сценарии эмуляции сетевых сбоев с использованием netem (моделирование задержек, потерь, джиттера) для проверки корректности буферизации и восстановления данных. Тесты безопасности включают проверку конфигурации TLS/mTLS, валидацию схем подписи и базовый penetration testing.

Документы и артефакты поставки. Поставляемая документация должна включать спецификацию API (REST/WS), схемы protobuf/JSON, шаблон измерительного отчёта с полями net_metrics и подписи, скрипты для тестирования сети (netem, iperf3), чек-лист инсталляции, а также политику управления ключами и инструкции по обновлению ПО с процедурами rollback.

Предложенная архитектура сочетает строгие метрологические требования с практической эксплуатационной гибкостью: аппаратная привязка ко времени и гарантии целостности данных обеспечивают доверие к удалённым измерениям; локальная буферизация и адаптивные алгоритмы поддерживают непрерывность исследований в реальных сетевых условиях; предусмотренные механизмы безопасности и документооборот позволяют проводить аудит и верификацию результатов. Такая платформа упрощает интеграцию ИИ-модулей, масштабирование и дальнейшее развитие измерительных комплексов.

Список использованных источников:

1. Богуш В.А. Векторные анализаторы цепей сантиметрового и миллиметрового диапазонов длин волн / В.А. Богуш [и др.]. – Москва: Горячая линия–Телеком, 2019. – 328 с.
2. Зокиров Д. Т. Методики дистанционной калибровки информационно-измерительной системы СВЧ диапазона = Methodologies for distance calibration of microwave range information and measurement systems / Д. Т. Зокиров // Информационная безопасность : сборник материалов 61-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 21–25 апреля 2025 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2025. – С. 158–161.

УДК 621.396.946

СПУТНИКОВЫЙ ТЕРМИНАЛ СВЯЗИ VSAT

Коледа В.В., магистрант гр.567041

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гусинский А.В. – д-р техн. наук, профессор

Аннотация. В материалах доклада рассматриваются устройство и работа спутникового терминала связи с очень маленькой апертурой (VSAT), его структурная схема и технические характеристики.

Ключевые слова. Спутниковая связь, терминал, схема, технические характеристики.

Спутниковые системы связи (ССС) используются для передачи различных сигналов на протяженные расстояния. С момента своего появления спутниковая связь стремительно развивалась, и по мере накопления опыта, совершенствования аппаратуры, развития методов передачи сигналов произошел переход от отдельных линий спутниковой связи к локальным и глобальным системам. [1,2]

Терминал VSAT – это небольшая станция спутниковой связи с антенной, предназначенная, главным образом, для надежного обмена данными по спутниковым каналам. Она подключается напрямую к терминальному оборудованию пользователя, исполняя роль беспроводного модема.

Сеть спутниковой связи на базе VSAT включает в себя три основных элемента: центральная земная станция (при необходимости), спутник-ретранслятор и абонентские VSAT терминалы.

Центральная земная станция (ЦЗС) в сети спутниковой связи выполняет функции центрального узла и обеспечивает управление работой всей сети, перераспределение ее ресурсов, выявление неисправностей, тарификацию услуг сети и сопряжение с наземными линиями связи. Обычно ЦЗС устанавливается в узле сети, на который приходится наибольший трафик. Это может быть, например, главный офис или вычислительный центр компании в корпоративных сетях, или же крупный город в региональной сети.

Абонентский VSAT терминал включает в себя антенно-фидерное устройство, наружный внешний радиочастотный блок и внутренний блок (модем). Внешний блок представляет собой небольшой приемопередатчик или приемник. Внутренний блок обеспечивает сопряжение спутникового канала с терминальным оборудованием пользователя (компьютер, сервер локальной вычислительной сети, телефон, факс учрежденческой АТС и т.д.).

Спутники-ретрансляторы сети VSAT строятся на базе геостационарных спутников-ретрансляторов. Это позволяет максимально упрощать конструкцию абонентских терминалов и снабжать их простыми фиксированными антеннами без системы слежения за спутником. Спутник принимает сигнал от земной станции, усиливает его и направляет назад на Землю. Важнейшими характеристиками спутника являются мощность бортовых передатчиков и количество радиочастотных каналов (стволов или транспондеров) на нем. Для обеспечения работы через малогабаритные абонентские станции типа VSAT требуются передатчики с выходной мощностью около 5 Вт. Внешний вид спутникового терминала связи VSAT представлен на рисунке 1.

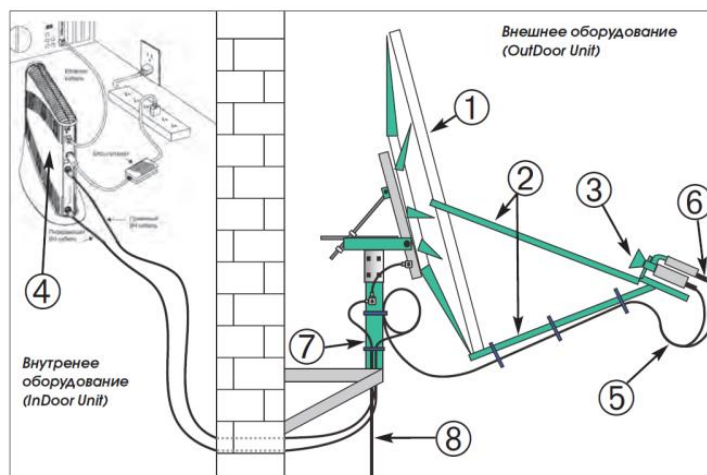


Рисунок 1 – Внешний вид терминала VSAT

Терминал VSAT состоит из следующих основных узлов и деталей:

- антенна (1) с облучателем (3) и штангами (2) для крепления приемопередатчика;
- спутниковый модем (4) с телефонным модулем или без него;
- радиочастотный кабель (5) с коннекторами (6);
- опора для крепления антенны (7) на здании или на земле;
- кабель заземления (8).

Терминал VSAT обеспечивает:

- работу от нескольких десятков до нескольких тысяч абонентов, под управлением одного хаба;
- подключение спутниковой станции непосредственно или через обычный коммутатор Ethernet к отдельному компьютеру или серверу; прямо к локальной компьютерной сети Ethernet; к маршрутизаторам, криптошлюзам, аппаратным сетевым экранам и т.п.; к шлюзам IP–телефонии; к веб–камерам и видеосерверам; к устройствам для прозрачной передачи данных по другим протоколам через сети IP (например, для протокола RS–232 – COM–серверы); к прочим устройствам с интерфейсом Ethernet;

- получение информации со скоростью до 54 Мбит/с и передачу информации до 30 Мсим/с.

Диапазон рабочих частот терминала VSAT:

- прием от 18,5 до 19,5 ГГц;
- передача от 28,7 до 29,5 ГГц.
- коэффициент стоячей волны по напряжению антенны, не более 1.3.
- коэффициент стоячей волны по напряжению приемного устройства: 1,3 – 1,5.

Структурная схема спутникового терминала VSAT представлена на рисунке 2.

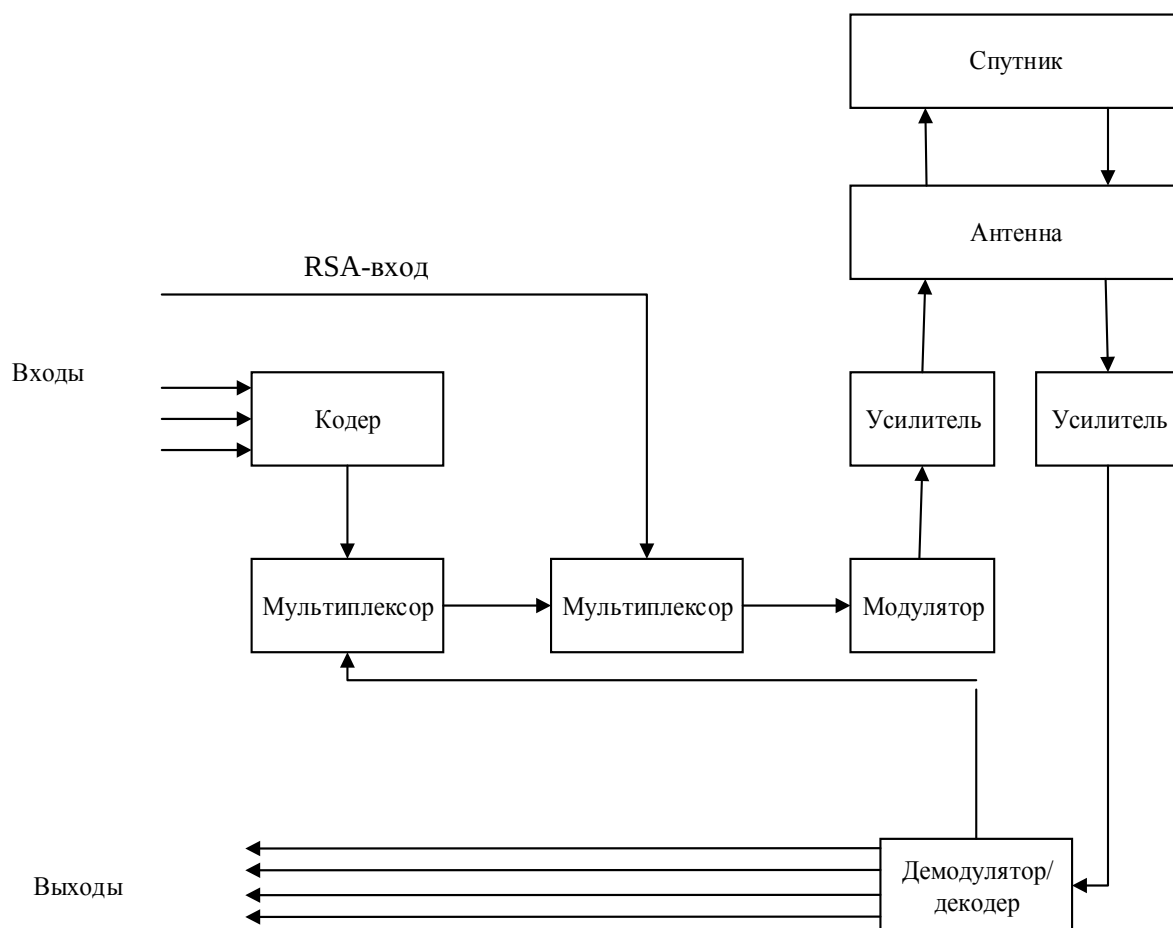


Рисунок 2 – Структурная схема спутникового терминала VSAT

Кодер предназначен для приема и выделения из однопрограммного или многопрограммного транспортного потока элементарных потоков изображения, звукового сопровождения, видеоинформации, декодирование выделенных потоков сигналов изображения, звукового сопровождения и видеоинформации.

Мультиплексоры предназначены для передачи по одной высокоскоростной линии связи нескольких менее скоростных потоков, а также вывода нескольких каналов из общего потока.

Модулятор предназначен для формирования сигнала по стандарту DVB-S в диапазоне частот 950...2150 МГц.

Сетевой коммутатор (Свитч) используется в сетях передачи пакетов данных для объединения нескольких сегментов и передачи данных от одного порта к другому на основе содержащейся в пакете информации.

Передающее устройство предназначено для систем СВЧ-диапазона спутниковой связи. Оно интегрировано с блоком питания, генератором фазовой автоподстройки, усилителем мощности и преобразователем частоты.

Приемное устройство обеспечивает минимальный коэффициент усиления 60 дБ с типичным коэффициентом шума ниже, чем 1,5 дБ.

Демодулятор/Декодер предназначен для обработки и преобразования цифровых сигналов транспортных потоков, полученных по различным каналам в виде DVB-S/S2/T/C или ASI в любой из требуемых интерфейсов: ASI, CVBS, HDMI или YPbPr. Каждый транспортный поток может содержать несколько телевизионных программ, программы радиовещания, интернет-данные. Позволяет эффективно обеспечить формирование и трансформацию цифровых телевизионных потоков и производить их маршрутизацию для дальнейшего приема телевизионных программ абонентским оборудованием.

Рассматриваемый спутниковый терминал связи обеспечивает безопасный и надёжный обмен данными по спутниковым каналам без необходимости специального обслуживания оборудования.

Список использованных источников:

1. Основы построения систем спутниковой связи/ М.С. Немировский, Б.Д. Локшин М.Д., Аронов Д.А.: Горячая линия – Телеком, 2024. – 432 с.
2. Спутниковые системы связи: Учебное пособие для вузов/ Сомов А.М.: Горячая линия – Телеком, 2025. – 243 с.

UDC 621.396.946

SATELLITE COMMUNICATION TERMINAL VSAT

Kaliada V.V. master's student gr. 567041

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

A.V. Gusinsky – Doctor of Technical Sciences, Professor

Annotation. The article discusses the design and operation of a satellite communication terminal VSAT, its structural diagram and technical characteristics.

Keywords. Satellite communication, terminal, diagram, technical characteristics.

УДК 004.056.53

МЕТОДЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ И ДОСТОВЕРНОСТИ ДАННЫХ В ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ ПРИБОРАХ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Маевский П.К., *курсант гр.333702*

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

*Брилевский В.И. – ассистент кафедры ИИС,
Магистр технических наук*

Аннотация. В статье исследуется уязвимость первичных преобразователей информационно-измерительных систем к атакам типа инъекции ложных данных (FDI). В условиях слияния корпоративных и технологических сетей на объектах критической инфраструктуры доказана недостаточность исключительно периметральной защиты. Обоснована неэффективность применения традиционных криптографических стандартов на полевом уровне из-за аппаратных ограничений. В качестве альтернативы предложен метод интеграции алгоритмов легковесной криптографии (на базе ARX-архитектуры) в микроконтроллеры измерительных приборов для вычисления имитовставки. Проведенный анализ вычислительных затрат подтверждает применимость подхода в системах жесткого реального времени.

Ключевые слова. Информационная безопасность, критическая информационная инфраструктура, легковесная криптография, имитовставка, ПЛК, инъекция ложных данных, микроконтроллеры.

Надежность функционирования современных автоматизированных систем управления технологическими процессами (АСУ ТП) в энергетическом, нефтехимическом и промышленном секторах Республики Беларусь фундаментально зависит от качества телеметрии, поступающей с нижнего (полевого) уровня. Информационно-измерительные приборы (ИИП) непрерывно формируют массивы данных о физических величинах, на основе которых программируемые логические контроллеры (ПЛК) и системы SCADA принимают автоматические решения. В связи с присвоением ключевым индустриальным объектам статуса критической информационной инфраструктуры (КИИ) [1] возникает острая необходимость пересмотра классической модели угроз. Парадигма изолированных технологических сетей окончательно утратила актуальность из-за внедрения концепций промышленного интернета вещей (IIoT). Это требует смещения фокуса от построения «непроницаемого» сетевого периметра к обеспечению безопасности конечных устройств (Endpoint Security).

Ретроспективный анализ инцидентов кибербезопасности в промышленном секторе демонстрирует эволюцию векторов целенаправленных атак (APT). Злоумышленники все чаще избегают лобовых атак на защищенные серверные сегменты, предпочитая компрометировать наименее защищенные звенья – непосредственно сенсорные узлы, термоэлектрические преобразователи и исполнительные механизмы. Проблема усугубляется тем, что подавляющее большинство эксплуатируемых сегодня интеллектуальных датчиков опираются на открытые промышленные протоколы (HART, Modbus RTU/TCP, Profibus-DP). Архитектура этих стандартов, заложенная десятилетия назад, не предусматривает криптографической аутентификации источника сообщений и контроля целостности пакетов на канальном и прикладном уровнях.

Такой структурный недостаток создает идеальную среду для реализации кибератак класса Sensor Spoofing и False Data Injection (FDI). Механика атаки FDI заключается не в отказе в обслуживании (DoS), а во внедрении математически выверенных, семантически корректных, но физически ложных показаний в измерительный канал. Например, при искажении профиля измерений термопарного преобразователя злоумышленник может транслировать в ПЛК заниженные значения температуры химического реактора. Контроллер, не имея математического аппарата для проверки подлинности пакета, воспримет данные как легитимные и инициирует открытие клапанов подачи реагентов, что неизбежно приведет к нештатной ситуации вплоть до техногенной катастрофы.

Для нейтрализации угрозы FDI императивом становится обеспечение неотрекаемости и целостности данных непосредственно «на борту» измерительного прибора, до момента попадания пакета в распределенную среду передачи. На практике реализация данного подхода сталкивается с жесткими ресурсными барьерами. Полевые сенсоры строятся на базе экономичных микроконтроллеров (MCU), обладающих крайне скудными вычислительными возможностями. Типовой узел характеризуется малым объемом оперативной памяти (SRAM), лимитированным ресурсом энергонезависимой памяти (Flash) и низкой тактовой частотой ради снижения энергопотребления. В таких условиях имплементация полновесных криптографических стандартов

(асимметричной криптографии RSA/ECC или тяжелых хеш-функций семейства SHA) ведет к недопустимым задержкам и нарушению детерминированности измерительного цикла.

Разрешение данного противоречия лежит в плоскости легковесной криптографии (Lightweight Cryptography, LWC) [2]. В качестве фундаментального защитного механизма для измерительного канала предлагается вычисление криптографической имитовставки (Message Authentication Code, MAC) на базе симметричных блочных шифров с уменьшенным размером блока и ключа.

Формулы (включая химические) выносятся отдельной строкой, отделяя пробельными строками с обеих сторон и нумеруют. Пояснения к формулам размещают без абзацного отступа начиная со строчной буквы, перечисление идет через точку с запятой:

$$C = M \parallel MAC(k, M), \quad (1)$$

где C – результирующий пакет телеметрии, передаваемый в промышленную сеть; M – бинарный массив полезной нагрузки (исходный результат измерения); k – секретный сессионный ключ шифрования, предварительно распределенный между сенсором и ПЛК; $\parallel$ – операция строковой конкатенации бит.

Высокая производительность LWC-алгоритмов достигается за счет специфической внутренней архитектуры. Передовые легковесные шифры строятся на базе концепции ARX (Addition, Rotation, XOR). Данная концепция использует исключительно комбинации простейших битовых операций: модульное сложение, циклический битовый сдвиг и побитовое исключающее ИЛИ. Аппаратная реализация АЛУ большинства промышленных микроконтроллеров выполняет любую из этих инструкций за один машинный такт.

Для объективной оценки применимости LWC было проведено профилирование затрат машинных тактов и потребления памяти для микроконтроллеров архитектуры ARM Cortex-M0/M3, являющихся отраслевым стандартом для современных ИИП. Результаты профилирования сведены в таблицу 1.

Рисунки располагаются в тексте, отделяются пробельной строкой. При необходимости можно размещать рисунки в невидимой таблице или в режиме обтекания текстом с левой стороны страницы. В тексте до рисунка в обязательном порядке должна содержаться ссылка на рисунок: схематическое представление образования металл-цитратного комплекса с алюминием приведено на рисунке 1.

Для объективной оценки применимости LWC было проведено профилирование затрат машинных тактов и потребления памяти для микроконтроллеров архитектуры ARM Cortex-M0/M3, являющихся отраслевым стандартом для современных ИИП. Результаты профилирования сведены в таблицу 1.

Таблица 1 – Сравнение вычислительной сложности криптоалгоритмов для MCU ИИП

№п/п	Криптографический алгоритм	Размер блока, бит	Затраты RAM, байт	Затраты Flash (ROM), байт	Время выполнения (на 16 МГц), мкс
1	AES-128 (классический стандарт)	128	416	3218	1240
2	Speck 64/128 (алгоритм LWC)	64	32	412	185
3	Simon 64/128 (алгоритм LWC)	64	36	450	210

Анализ эмпирических данных таблицы 1 наглядно демонстрирует, что симметричные LWC-алгоритмы снижают потребление оперативной памяти и процессорного времени на порядок по сравнению с классическим AES. Такая компактность позволяет интегрировать криптографический модуль непосредственно в жесткий измерительный цикл прибора, сохраняя детерминированную природу протоколов реального времени (Real-Time Systems).

Процедура верификации достоверности на принимающей стороне выполняется программируемым логическим контроллером. Контроллер принимает пакет C , разделяет его на полученное сообщение M_{revc} и полученную имитовставку MAC_{revc} . Далее ПЛК вычисляет эталонный MAC и сравнивает его с полученным путем операции побитового сложения по модулю 2:

$$V = MAC_{revc} \oplus MAC(k, M_{revc}), \quad (2)$$

где V – результирующий вектор верификации; $\oplus$ – логическая операция XOR.

Если $V = 0$, пакет математически признается достоверным и нескомпрометированным. Если $V \neq 0$, данные немедленно отбрасываются как результат кибератаки или сильной канальной помехи, а в SCADA-систему генерируется сигнал тревоги о попытке подмены данных.

Ключевым аспектом практической реализации предложенной архитектуры является подсистема управления ключевой информацией. Для автономных ИИП наиболее перспективным видится метод предварительного распределения ключей (Pre-shared key, PSK) на этапе пусконаладки, с периодической ротацией сессионных ключей на основе счетчиков измерений для предотвращения атак повторного воспроизведения (Replay Attacks).

Реализация рассмотренных методов защиты ИИП должна опираться на национальную нормативную базу. Следующим этапом исследований станет адаптация отечественных криптографических алгоритмов (СТБ 34.101.31) [3] под жесткие аппаратные ограничения микроконтроллеров. Использование стандартизованных решений (BeIT) позволит повысить безопасность измерительных каналов КИИ и обеспечит соответствие аппаратуры нормативным требованиям в условиях импортозамещения.

Список использованных источников:

1. О кибербезопасности [Электронный ресурс] : Указ Президента Республики Беларусь, 14 февр. 2023 г., № 40 // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: <https://pravo.by>. – Дата доступа: 14.03.2026.
2. Жуков, А. Е. Легковесная криптография. Часть 1 / А. Е. Жуков // Вопросы кибербезопасности. – 2015. – № 1(9). – С. 26–43.
3. Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности : СТБ 34.101.31-2020. – Введ. 01.09.21. – Минск : Госстандарт, 2020. – 66 с.

UDC 004.056.53

METHODS FOR ENSURING DATA INTEGRITY AND RELIABILITY IN INFORMATION-MEASURING DEVICES OF CRITICAL INFRASTRUCTURE

Mayeuski P.K.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Doronina A.V. – Assistant of the Department of Information and Measurement Systems

Annotation. The article investigates the vulnerability of primary converters of information-measuring systems to False Data Injection (FDI) attacks. In the context of the convergence of corporate and technological networks at critical infrastructure facilities, the insufficiency of purely perimeter-based protection is proven. The inefficiency of applying traditional cryptographic standards at the field level due to hardware limitations is substantiated. As an alternative, a method of integrating lightweight cryptography algorithms (based on ARX architecture) into the microcontrollers of measuring devices to calculate a message authentication code is proposed. The performed profiling of computational costs confirms the applicability of this approach in strict real-time systems.

Keywords. information security, critical information infrastructure, lightweight cryptography, MAC, PLC, False Data Injection, microcontrollers.

ПРИМЕНЕНИЕ НЕЙРОСЕТЕЙ ДЛЯ ЛИНЕАРИЗАЦИИ ТЕРМОЭДС ТЕРМОПАР КАК АЛЬТЕРНАТИВА ПОЛИНОМИАЛЬНОЙ МОДЕЛИ

Мороз А.С., аспирант

Белорусский национальный технический университет, Минск, Республика Беларусь

Тяловский А.К. – канд. тех. наук, доцент

Аннотация. Стандартные полиномиальные модели для линеаризации термопар дают систематическую погрешность до $\pm 0,05^\circ\text{C}$ даже при разбиении на поддиапазоны. Рациональные полиномиальные функции снижают ошибку до $\pm 0,01^\circ\text{C}$, но остаются статическими. В работе предлагается использование многослойного перцептрона (MLP) как альтернативы. Нейросеть обеспечивает единую модель для всего диапазона, потенциальную точность выше $0,001^\circ\text{C}$ и возможность адаптации под индивидуальные характеристики датчика, что открывает путь к интеллектуальным измерительным каналам.

Ключевые слова. Нейросети, MLP, термоЭДС, погрешности измерения температуры,

Термопары широко применяются для измерения температуры благодаря широкому диапазону измерения, надёжности и низкой стоимости. Однако их выходная термоЭДС (ТЭДС) изменяется с температурой лишь приблизительно линейно. Для получения точных значений требуется линеаризация – преобразование измеренной ТЭДС в температуру с учётом нелинейности характеристики термопары. Классическим подходом является использование полиномиальных моделей. Для термопары типа К предлагается полином девятого порядка с десятью коэффициентами, причём весь рабочий диапазон разбивается на три поддиапазона, для каждого из которых коэффициенты свои. Аппроксимация исходной зависимости «температура-ТЭДС» для термопар типа К приведена в документе NIST [1], а также в стандартах МЭК 60584, ASTM E230, ITS-90 [2] и ГОСТ Р 8.585-2001. Для преобразования измеренного значения термоЭДС применяется стандартная зависимость ТЭДС термопары от температуры, описываемая степенным рядом (1)

$$E(T) = a_0 + a_1T + a_2T^2 + \dots + a_nT^n, \quad (1)$$

где a_i – коэффициенты, определяемые материалами электродов.

Несмотря на широкое распространение, стандартные полиномы обладают существенными недостатками. Исходные данные в таблицах округлены до 1 мкВ (обратные таблицы до 1°C), что вносит погрешность квантования около $\pm 0,01^\circ\text{C}$. Однако систематическая ошибка самой полиномиальной аппроксимации оказывается значительно больше – до $\pm 0,03^\circ\text{C}$ (рисунок 1). На границах поддиапазонов возникают дополнительные осцилляции, ухудшающие точность.

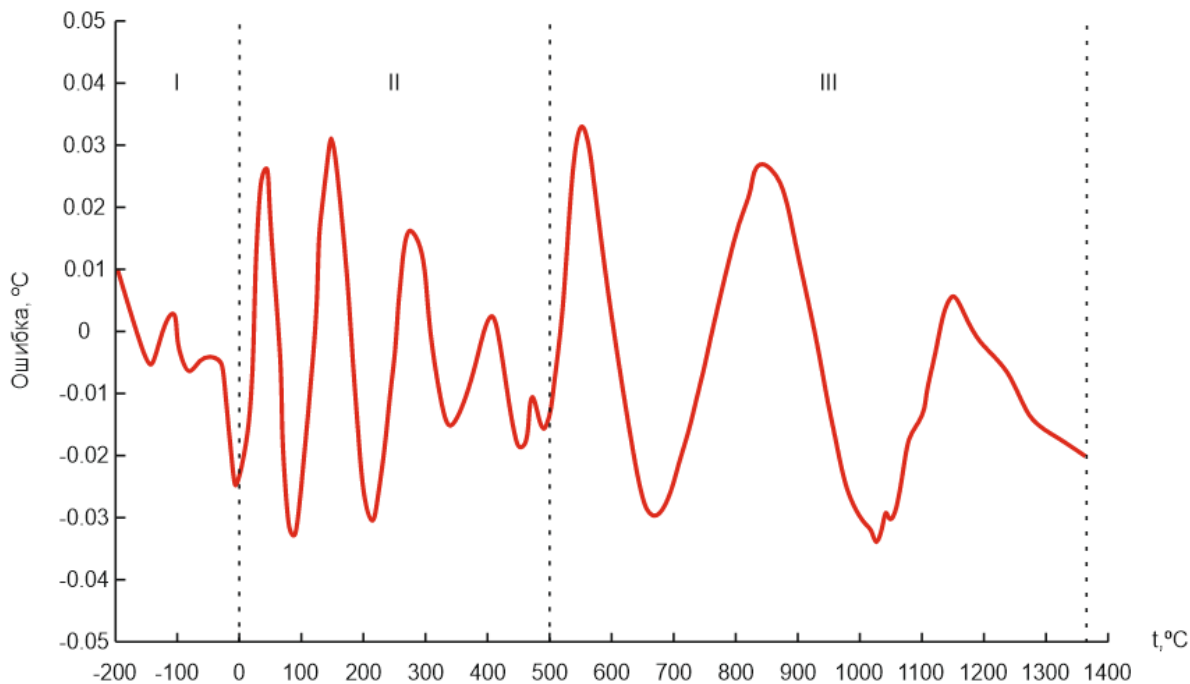


Рисунок 1 — Погрешности измерения температуры, возникающие при применении стандартного полинома 9-го порядка к калибровочным данным термопары типа К. Диапазоны; I от минус 200°C до 0°C ; II от 0°C до 500°C ; III от 500°C до 1372°C .

Более совершенной альтернативой классическим методам являются рациональные полиномиальные функции – отношение двух полиномов меньших порядков. Такая модель снижает систематическую ошибку до $\pm 0,01^\circ\text{C}$, что уже меньше погрешности квантования исходных данных, и не требует разбиения на поддиапазоны. Однако и рациональная функция остаётся статической: её коэффициенты рассчитываются один раз по усреднённым табличным данным и не учитывают индивидуальные особенности конкретного датчика, его дрейф или условия эксплуатации.

Альтернативой, позволяющей преодолеть эти ограничения, служат нейронные сети, в частности многослойный перцептрон (MLP) [3]. MLP является универсальным аппроксиматором, способным воспроизводить нелинейные зависимости с произвольно высокой точностью. При обучении на стандартных данных или на реальных экспериментальных измерениях MLP формирует единую для всего диапазона модель, свободную от разрывов на границах поддиапазонов. Благодаря нелинейным функциям активации сеть может улавливать тонкие особенности характеристики, которые не описываются рациональной функцией с фиксированной структурой. На рисунке 2 приведена погрешность, полученная при использовании многослойного перцептрона (MLP). Максимальная ошибка составила $\pm 0,005^\circ\text{C}$. Теоретически достижимая погрешность может быть снижена до уровня шума измерений (менее $0,001^\circ\text{C}$). Кроме того, MLP легко адаптируется под конкретный экземпляр датчика: достаточно провести индивидуальную калибровку и дообучить сеть. После обучения вычисления сводятся к матричным операциям, которые эффективно реализуются даже на микроконтроллерах.

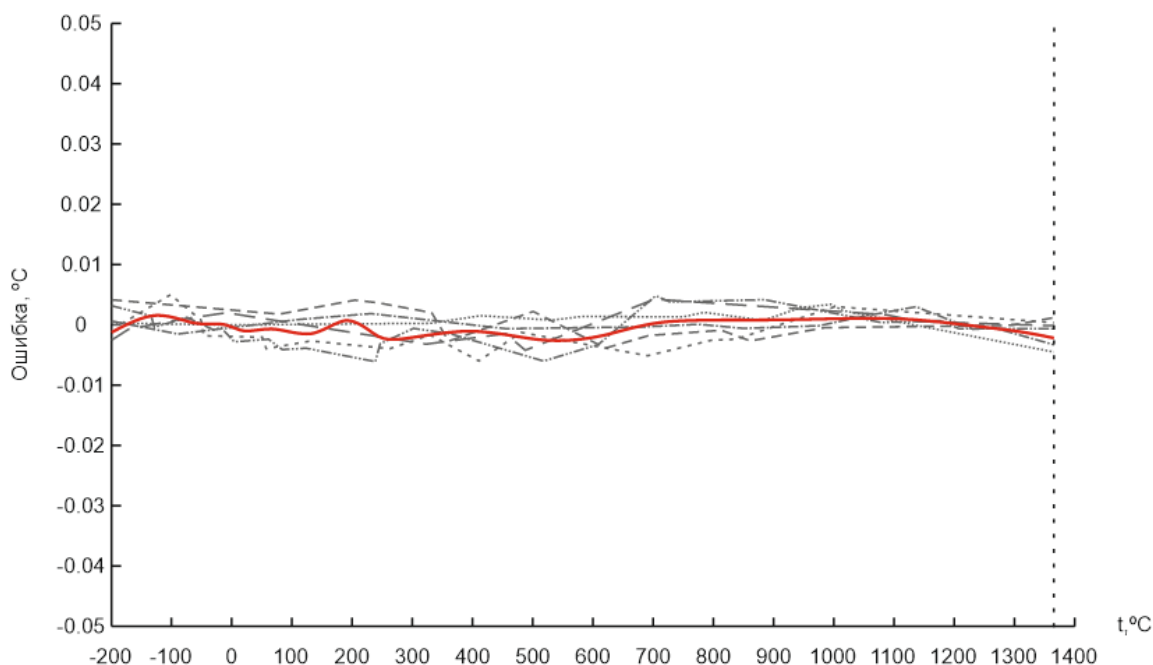


Рисунок 2 – Погрешность аппроксимации характеристики термодатчика типа К многослойным перцептроном (MLP).

Сравнение методов показывает, что стандартные полиномы дают ошибку $\pm 0,03^\circ\text{C}$ при десяти коэффициентах и разбиении на поддиапазоны; рациональная функция с девятью коэффициентами обеспечивает точность около $\pm 0,01^\circ\text{C}$; MLP при использовании двух скрытых слоёв (общее число весов – несколько сотен) потенциально способен достичь точности выше $0,001^\circ\text{C}$ с единой моделью для всего диапазона и возможностью учёта индивидуальных характеристик.

Таким образом, применение нейросетей типа MLP для линеаризации термодатчиков позволяет не только превзойти по точности классические полиномиальные модели, но и получить адаптивный инструмент, пригодный для создания «интеллектуальных» измерительных каналов с самокалибровкой и компенсацией дрейфа. Переход от статических математических аппроксимаций к нейросетевым решениям открывает новые возможности для повышения точности и надёжности термометрических систем.

Список использованных источников:

1. NIST Special Publication 250-35. Thermocouple Calibration. URL: <https://www.nist.gov>
2. Preston-Thomas, H., "The International Temperature Scale of 1990 (ITS90). *Metrologia* 27, 3-10 (1990). DOI:10.1088/0026-1394/27/1/002
3. Almeida, L.B. Multilayer perceptrons, in *Handbook of Neural Computation*, IOP Publishing Ltd and Oxford University Press, 1997. URL: <https://www.lx.it.pt/~lbalmeida/papers/AlmeidaHNC.pdf>

УДК 006.91:621.396.62

АНАЛИЗ МЕТОДОВ И СРЕДСТВ КОНТРОЛЯ МЕТРОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК МНОГОКАНАЛЬНЫХ ПРИЕМНЫХ УСТРОЙСТВ

Шапошникова Н.П., магистрант гр.567001

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Гусинский А.В. – д-р техн. наук, профессор

Аннотация. В статье проведен анализ методов и средств контроля метрологических характеристик многоканальных приемных устройств диапазона 1–20 ГГц. Рассмотрены основные контролируемые параметры: частота настройки, нестабильность, чувствительность, избирательность, фазовый шум, коэффициент усиления, динамический диапазон. Описаны прямые, косвенные и сравнительные методы контроля, а также средства измерений: анализаторы спектра, векторные анализаторы цепей, генераторы сигналов. Приведены требования при выборе измерительного оборудования для метрологических исследований МПУ. Результаты могут быть использованы при разработке методик контроля узлов приемного тракта.

Ключевые слова. Многоканальное приемное устройство, метрологические характеристики, методы контроля, средства измерений, нестабильность частоты, чувствительность, избирательность, фазовый шум, динамический диапазон.

Многоканальные приемные устройства (МПУ) являются ключевым элементом современных радиотехнических измерительных систем, применяемых в радиомониторинге, радиотехнической разведке и измерительной технике. От их метрологических характеристик (МХ) напрямую зависят достоверность обнаружения радиосигналов, точность измерения их параметров и, в конечном счете, эффективность функционирования всей системы.

В диапазоне частот 1–20 ГГц, насыщенном средствами связи, радиолокации и навигации, требования к метрологическому обеспечению МПУ особенно высоки. Многоканальная архитектура, включающая узлы опорного генератора (УОГ), гетеродина (УГ), синтезатора (УС), переноса частоты (УПЧ) и предварительного усиления (УПУ), предъявляет дополнительные требования к методам и средствам контроля, так как погрешности каждого узла вносят вклад в результирующую неопределенность измерений.

Для обеспечения пригодности МПУ к применению и принятия обоснованных решений по их допуску необходимо проведение метрологических исследований по специально разработанным и научно обоснованным методикам. Разработка таких методик требует тщательного анализа существующих методов измерения, выбора адекватных средств измерений (СИ) с учетом их точностных характеристик, а также оценки результирующей погрешности или неопределенности измерений.

Целью данной статьи является анализ существующих методов и средств контроля метрологических характеристик многоканальных приемных устройств, а также обоснование выбора средств измерений для проведения метрологических исследований МПУ в диапазоне частот 1–20 ГГц.

Контролируемые параметры многоканальных приемных устройств.

Метрологические характеристики МПУ представляют собой совокупность параметров, определяющих его способность выполнять измерительные задачи с требуемой точностью. Выбор номенклатуры контролируемых параметров базируется на функциональном назначении устройства, требованиях нормативной документации и особенностях построения многоканального тракта.

Частота настройки определяет диапазон принимаемых сигналов. Для МПУ диапазона 1–20 ГГц важнейшей характеристикой является абсолютная и относительная погрешность установки частоты, а также долговременная и кратковременная нестабильность. Нестабильность частоты обусловлена флуктуациями параметров УОГ и УГ и напрямую влияет на вероятность обнаружения сигналов с узкой полосой и точность измерения частоты. Контроль данного параметра включает оценку отклонений от номинального значения и анализ спектральных составляющих, характеризующих фазовые и частотные шумы.

Чувствительность МПУ – это минимальный уровень входного сигнала, при котором обеспечивается обнаружение сигнала с заданной вероятностью или достигается требуемое отношение сигнал/шум на выходе. В многоканальных устройствах чувствительность может варьироваться по каналам из-за различий в коэффициентах усиления УПУ и потерях в УПЧ. Контроль чувствительности позволяет оценить реальные возможности МПУ по приему слабых сигналов и выявить каналы с пониженной эффективностью.

Избирательность характеризует способность МПУ выделять полезный сигнал на фоне помех, расположенных по соседним и побочным частотам. В соответствии с ГОСТ 8.627-2013 контролируются следующие виды избирательности:

- избирательность по соседнему каналу – ослабление сигнала, отстроенного от частоты настройки на величину, равную ширине канала;
- избирательность по побочным каналам приема – ослабление сигналов на частотах зеркального канала, комбинационных составляющих и гармоник гетеродина;
- избирательность по интермодуляции – способность подавлять продукты нелинейного взаимодействия двух и более сигналов, попадающих в полосу пропускания.

Контроль избирательности особенно важен для МПУ, работающих в условиях плотной сигнальной обстановки.

Фазовый шум является одной из ключевых характеристик узлов формирования частот (УОГ и УГ). Он определяет флуктуации фазы выходного сигнала и проявляется в виде спектральных составляющих вблизи несущей частоты. В многоканальных приемниках фазовый шум влияет на:

- возможность обнаружения слабых сигналов вблизи мощных помех;
- когерентность обработки сигналов по каналам;
- точность измерения доплеровского сдвига частоты.

Измерение фазового шума проводится в частотной области с помощью анализаторов спектра или специализированных фазошумомеров.

Коэффициент усиления (КУ) определяет отношение амплитуды выходного сигнала к входному в линейном режиме работы. Контроль КУ проводится для узлов УПЧ и УПУ, а также для всего приемного тракта в целом. Важными характеристиками являются:

- неравномерность коэффициента усиления в рабочем диапазоне частот;
- идентичность коэффициентов усиления по каналам (для многоканальных устройств);
- стабильность усиления во времени и при изменении температуры.

Отклонения КУ приводят к погрешностям измерения уровня сигнала и нарушению балансировки каналов.

Динамический диапазон МПУ – это диапазон уровней входных сигналов, в пределах которого устройство сохраняет работоспособность с заданной точностью. Различают:

- по блокированию – максимальный уровень сигнала, при котором чувствительность не снижается более допустимого предела;
- по интермодуляции – диапазон уровней, в котором интермодуляционные искажения не превышают нормированного значения;
- общий динамический диапазон – отношение максимального неискажающего уровня сигнала к чувствительности.

Контроль динамического диапазона позволяет оценить способность МПУ работать одновременно с мощными и слабыми сигналами без потери избирательности и точности измерений.

Методы контроля. Для определения метрологических характеристик МПУ применяются различные методы измерений, выбор которых зависит от контролируемого параметра, требуемой точности, доступных средств измерений и особенностей построения МПУ.

Прямые методы основаны на непосредственном измерении контролируемого параметра с помощью соответствующего средства измерений. Например, частота настройки измеряется частотомером, уровень сигнала – анализатором спектра или измерителем мощности, коэффициент усиления – с помощью измерителя коэффициента передачи. Достоинством прямых методов является простота и наглядность, недостатком – необходимость использования высокоточных эталонных средств, погрешность которых должна быть существенно меньше допуска на контролируемый параметр.

Косвенные методы основаны на измерении вспомогательных величин, связанных с контролируемым параметром известной функциональной зависимостью. Например, фазовый шум оценивают по спектральной плотности мощности флуктуаций фазы, измеренной анализатором спектра с последующим пересчетом. Чувствительность определяют по отношению сигнал/шум при подаче на вход калиброванного сигнала. Косвенные методы часто применяются, когда прямое измерение параметра затруднено или требует специфического оборудования.

Сравнительные методы (методы сличения) предполагают сравнение контролируемого МПУ с эталонным устройством или с помощью эталонной меры. Они широко используются при поверке измерительных приемников в соответствии с ГОСТ 8.627-2013. Например, избирательность может быть определена сравнением уровней сигнала на выходе МПУ при настройке на полезный сигнал и при отстройке по частоте. Сравнительные методы позволяют компенсировать систематические погрешности средств измерений и повысить достоверность результатов.

Учитывая модульную структуру МПУ, целесообразно проводить контроль характеристик на уровне отдельных узлов. Это позволяет локализовать источник погрешностей и упрощает диагностику. Для каждого узла применяются специализированные методы:

- УОГ и УГ: измерение частоты, нестабильности, фазового шума, уровня выходной мощности;
- УС: оценка шага перестройки, времени установления частоты, спектральной чистоты;
- УПЧ: измерение коэффициента усиления, полосы пропускания, неравномерности АЧХ;

- УПУ: контроль коэффициента шума, динамического диапазона, линейности.

Такой подход соответствует современной практике метрологического обеспечения сложных радиоизмерительных систем.

Для реализации рассмотренных методов необходим комплекс средств измерений, обеспечивающих формирование испытательных сигналов, анализ параметров МПУ и обработку результатов. Выбор конкретных приборов определяется диапазоном частот (1–20 ГГц), требуемой точностью и функциональными возможностями.

Анализаторы спектра являются универсальными средствами для контроля большинства параметров МПУ:

- измерение чувствительности (по уровню шума);
- оценка избирательности (по ослаблению сигнала при отстройке);
- измерение фазового шума (методом прямой спектральной оценки);
- контроль уровня гармоник и побочных излучений;
- анализ динамического диапазона по интермодуляции.

Векторные анализаторы цепей (ВАЦ) используются для контроля СВЧ-трактов, входящих в состав УПЧ и УПУ. С их помощью измеряются:

- коэффициент передачи (S_{21}) и коэффициент отражения (S_{11});
- неравномерность АЧХ в полосе рабочих частот;
- фазовая характеристика и групповое время задержки;
- изоляция между каналами многоканального устройства.

Применение ВАЦ обеспечивает высокую точность калибровки и позволяет проводить измерения с погрешностью менее 0,1 дБ по амплитуде.

Для формирования испытательных сигналов используются генераторы сигналов (синтезаторы частот) с возможностью модуляции. Требования к генераторам:

- перекрытие диапазона 1–20 ГГц;
- низкий фазовый шум и высокий уровень спектральной чистоты;
- возможность задания амплитуды с высокой точностью (погрешность менее 0,5 дБ);
- наличие модуляции (АМ, ЧМ, ФМ, импульсной) для проверки функции определения вида модуляции.

Для высокоточного измерения частоты и оценки нестабильности применяются электронно-счетные частотомеры с внешним рубидиевым или водородным стандартом частоты. Они позволяют измерять абсолютную и относительную погрешность установок частоты, а также оценивать долговременную нестабильность. Для оценки кратковременной нестабильности (фазового шума) используются специализированные фазошумомеры или анализаторы сигналов с соответствующим программным обеспечением.

При выборе средств измерений для метрологических исследований МПУ необходимо учитывать:

- Диапазон частот – должен перекрывать рабочий диапазон МПУ (1–20 ГГц) с запасом для контроля побочных каналов.
- Погрешность измерений – должна быть не более 1/3 допуска на контролируемый параметр (в соответствии с общепринятой практикой).
- Функциональные возможности – наличие необходимых режимов (измерение фазового шума, анализ интермодуляции, поддержка внешней синхронизации).
- Совместимость – наличие стандартизованных интерфейсов (USB, LAN, GPIB) для автоматизации измерений.

Заключение. В результате проведенного анализа установлено, что контроль метрологических характеристик МПУ требует комплексного подхода, включающего выбор номенклатуры контролируемых параметров, применение соответствующих методов измерений и использование современных средств измерений.

Список использованных источников:

1. ГОСТ 8.627-2013. Государственная система обеспечения единства измерений. Приемники измерительные. Методика поверки. – М.: Стандартинформ, 2014. – 24 с.
2. МИ 2438-97. Радиоприемники измерительные. Методы и средства поверки. – М.: ВНИИФТРИ, 1997. – 40 с.
3. Дворяшин Б.В. Основы метрологии и радиоизмерения. – М.: Радиотехника, 2021. – 320 с.
4. Афонский А.А., Дьяконов В.П. Цифровые анализаторы спектра: метрология и применение. – М.: СОЛОН-Пресс, 2018. – 432 с.
5. Вострокнутов Н.Н. Цифровые измерительные устройства. Теория погрешностей, испытания, поверка: учеб. пособие. – М.: Академия стандартизации, метрологии и сертификации, 2018. – 288 с.
6. Иванов А.А., Петров С.В. Методика автоматизированного контроля параметров многоканальных приемных устройств // Известия вузов. Радиоэлектроника. – 2023. – № 4. – С. 45–52.
7. Сидоров В.Н., Кузнецов Д.А. Применение векторных анализаторов цепей для контроля СВЧ-трактов многоканальных приемников // Радиотехника. – 2022. – № 7. – С. 32–39.

UDC 006.91:621.396.62

ANALYSIS OF METHODS AND MEANS FOR CONTROL OF METROLOGICAL CHARACTERISTICS OF MULTICHANNEL RECEIVING DEVICES

Shaposhnikova N.P.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Gusinsky A.V. – Doctor of Technical Sciences, Professor

Annotation. This article analyzes methods and tools for monitoring the metrological characteristics of multichannel receivers in the 1–20 GHz range. Key monitored parameters include tuning frequency, instability, sensitivity, selectivity, phase noise, gain, and dynamic range. Direct, indirect, and comparative monitoring methods are described, as well as measurement tools such as spectrum analyzers, vector network analyzers, and signal generators. Requirements for selecting measuring equipment for metrological testing of multichannel receivers are presented. The results can be used in developing methods for monitoring receiver components.

Keywords. Multichannel receiving device, metrological characteristics, control methods, measuring instruments, frequency instability, sensitivity, selectivity, phase noise, dynamic range.