ЭКОНОМИКА И КАЧЕСТВО СИСТЕМ СВЯЗИ ***№ 3(33) / 2024***
Дата выхода: 19.09.2024

ISSN 2500-1833

Международный научно-практический электронный журнал
Основан в 2015 году, издается ежеквартально

Журнал включен в перечень рецензируемых научных изданий, рекомендуемых ВАК Минобрнауки России для публикации научных результатов, отражающих основное научное содержание кандидатских и докторских диссертаций

Учредитель *ООО «Научно-производственное предприятие «Информационные и Радио Технологии»*
Издатель *ООО «Научно-производственное предприятие «Информационные и Радио Технологии»*

Журнал публикует статьи, отражающие результаты исследований в соответствии со следующими разделами ГРНТИ:
06.00.00 – Экономика и экономические науки
20.00.00 – Информатика
28.00.00 – Кибернетика
47.00.00 – Электроника. Радиотехника
49.00.00 – Связь
81.93.29 – Информационная безопасность
82.00.00 – Организация и управление
90.00.00 – Метрология

Адрес редакции: *г. Москва, ул. Малая Тульская, д. 16, эт. 1. пом. I. ком. 20*

сайт: *http://journal-ekss.ru/* ***e-mail:*** *journal-ekss@mail.ru* ***тел:*** *+7 (495) 423-57-80*

СОДЕРЖАНИЕ

ЭКОНОМИКА И УПРАВЛЕНИЕ В ИНФОКОММУНИКАЦИЯХ. ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ГОСУДАРСТВА И ОБЩЕСТВА. ИНФОКОММУНИКАЦИОННЫЕ БИЗНЕС-ТЕХНОЛОГИИ

СИСТЕМЫ, СЕТИ И УСТРОЙСТВА СВЯЗИ. РАДИОТЕХНИКА. АНТЕННЫ. ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА. ПРИБОРЫ И МЕТОДЫ ИЗМЕРЕНИЯ. МЕТРОЛОГИЯ

ИНФОРМАЦИОННЫЕ СИСТЕМЫ, СЕТИ И ТЕХНОЛОГИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ

ЭКОНОМИКА И УПРАВЛЕНИЕ В ИНФОКОММУНИКАЦИЯХ. ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ГОСУДАРСТВА И ОБЩЕСТВА. ИНФОКОММУНИКАЦИОННЫЕ БИЗНЕС-ТЕХНОЛОГИИ

ЦИФРОВЫЕ ИНСТРУМЕНТЫ АВТОМАТИЗАЦИИ КАЗНАЧЕЙСКОЙ ФУНКЦИИ КОМПАНИИ

Е.Г. Кухаренко, *к.э.н., доцент, Московский технический университет связи и информатики, e.g.kukharenko@mtuci.ru;*
Е.А. Гуляева, *Московский технический университет связи и информатики, elenagulyaeva6a85@gmail.com.*

УДК 338.47

Аннотация. Казначейская функция предприятия связана с управлением денежными потоками и ликвидностью. Связанная с обработкой больших массивов неструктурированной информации и огромным количеством рутинных ручных операций деятельность департамента казначейства относится к приоритетным направлениям цифровизации современного предприятия. Решать поставленные задачи позволяет широкий спектр цифровых технологий и инструментов. Рассматриваются предложения по применению инструментов цифровизации бизнес-процессов казначейства крупных *IT*-компаний.

Ключевые слова: финансовая система; казначейская функция; финансовые бизнес-процессы; цифровые технологии; инструменты цифровизации

DIGITAL TOOLS FOR AUTOMATING THE TREASURY FUNCTION OF AN ENTERPRISE

Elena Kukharenko, *candidate of Economic Sciences, associate Professor, Moscow Technical University of Communications and Informatics;*
Gulyaeva Elena, *graduate student, Moscow Technical University of Communications and Informatics.*

Annotation. The treasury function of the enterprise is related to the management of cash flows and liquidity. Related to the processing of large amounts of unstructured information and a huge number of routine manual operations, the activities of the Treasury Department belong to the priority areas of digitalization of a modern enterprise. A wide range of digital technologies and tools allows you to solve these tasks. Proposals on the use of digitalization tools for business processes of the Treasury of large IT companies are being considered.

Keywords: financial system; treasury function; financial business processes; digital technologies; digitalization tools.

Введение

Важным условием успешного функционирования современной компании является скоординированная работа всех бизнес-процессов. Финансовые бизнес-процессы направлены на реализацию потребностей компании в финансовых ресурсах для обеспечения покрытия операционных затрат на осуществление производственно-хозяйственной деятельности, исполнения финансовых

обязательств и дальнейшего развития. Совокупность финансовых бизнес-процессов составляет финансовую систему предприятия или организации.

Важной составляющей финансовой системы являются технические средства управления финансами, то есть, современные средства вычислительной техники, телекоммуникации и различные технологии, применяемые для оптимизации и повышения эффективности деятельности не только финансовых структур, но и компании в целом. В условиях масштабной цифровизации экономики появляется все больше инструментов, которые позволяют автоматизировать рутинные задачи, сократить затраты времени и труда, минимизировать вероятность возникновения ошибок и повысить точность информации. Среди таких средств машинное обучение, робототехника и автоматизация, искусственный интеллект, интернет вещей, технологии больших данных и другие инструменты, успешно применяемые в различных отраслях и сферах деятельности [1-22]. Разнообразие инновационных решений актуализирует проблему выбора предприятием оптимального комплекса инструментов цифровизации.

Целью работы являлось исследование процессов цифровизации казначейской функции предприятия и разработка предложений по повышению их эффективности. В процессе исследования были решены следующие задачи:

- изучение деятельности казначейства, его роли и задач в финансовой структуре современной компании, типовых функций данного структурного подразделения;
- анализ возможностей существующих цифровых технологий и решений для автоматизации функций казначейства;
- анализ ключевых бизнес-процессов департамента казначейства крупных *IT*-компаний и выявление типовых проблем, отрицательно влияющих на эффективность деятельности данной структурной единицы;
- разработка предложений по применению инструментов цифровизации бизнес-процессов казначейства.

Казначейство в финансовой структуре компании

Финансовая работа компании ведется по трем ключевым направлениям (рис. 1) [23]. В процессе финансового планирования формируются финансовые планы, нацеленные на обеспечение компании необходимыми финансовыми ресурсами, улучшение финансового состояния и повышение эффективности ее деятельности. Оперативное управление связано с подготовкой и реализацией финансовых решений, их мониторингом, а также координацией финансовой работы структурных подразделений. Оценка эффективности деятельности компании, ее финансовых результатов, выявление отклонений и их причин, а также рекомендации по их предотвращению в будущих периодах осуществляется в ходе контроля и анализа.

Рисунок 1

Финансовая система компании включает два основных элемента: управляющую подсистему (субъект) и управляемую подсистему (объект), показанные на рис. 2 [24].

Рисунок 2

Организационная структура финансовой службы может быть различной в зависимости от размера компании, особенностей ее хозяйственной деятельности, организационно-правовой формы, целей и задач, поставленных перед компанией.

Управление денежными потоками – одно из наиболее приоритетных

направлений финансовой работы, особенно в условиях нестабильной финансовой ситуации. Поддержание стабильной платежеспособности является критичным фактором для любого бизнеса, поэтому возникает необходимость централизованного контроля за расходами, а также получением дополнительной прибыли от вложений свободных средств компании, то есть управлением ликвидностью.

В связи с этим распространенной практикой является введение в организационную структуру компании казначейства – специального департамента или отдела, предназначенного для управления денежными потоками. Задачами казначейства являются оперативное управление денежными потоками, организация эффективного взаимодействия с финансовыми институтами, минимизация расходов и финансовых рисков, максимизация доходности финансовых инвестиций. Казначейство, как правило, подчиняется напрямую финансовому директору и обеспечивает руководство необходимой информацией для принятия эффективных управленческих решений [25].

Введение в структуру финансовой системы компании департамента казначейства помогает устранить такие проблемы, как:

- несогласованность процедур управления финансовыми потоками компании, отсутствие единой политики;
- возникновение сложностей с формированием платежного календаря;
- задержка информации, недостаточная оперативность ее получения;
- вероятность возникновения финансовых рисков.

Работа казначейства в различных компаниях строится по-разному, но приоритетной задачей данного структурного подразделения является оперативное управление потоками финансовых средств компании. Для выполнения этой задачи казначейство выполняет ряд типовых функций (рис. 3) [26].

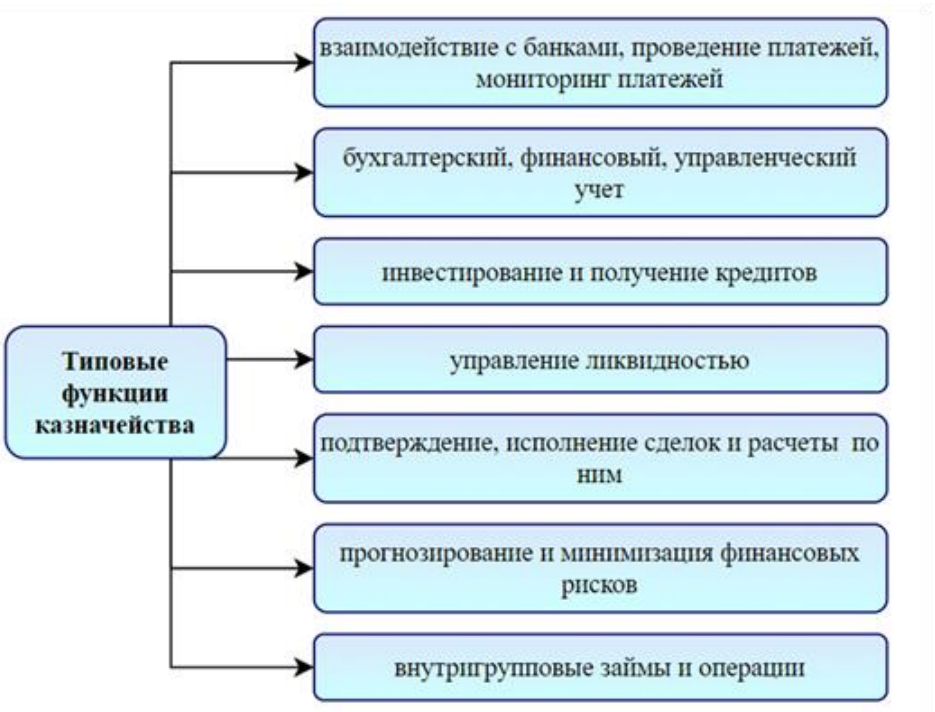


Рисунок 3

Процесс управления предприятием подразумевает активный обмен информацией всех его подразделений с внешней и внутренней средой.

Корректность, полнота, достоверность, а также своевременность получения необходимых данных являются залогом успеха компании в условиях современного бизнеса. Соответственно, информационное обеспечение становится одним из приоритетных направлений системы управления финансами предприятия.

Казначейства работают с огромными массивами информации, и эффективность их технической и аналитической деятельности в современных условиях напрямую связана с используемыми цифровыми инструментами.

Инструменты цифровизации финансовых бизнес-процессов

В условиях современного управления финансами и непрерывной цифровизации всех сфер деятельности расширяется спектр инструментов, которые помогают облегчить рутинные операции, сократить затраты времени и труда на выполнение ежедневных задач. Цифровизация финансовой системы касается не только финансовых отношений непосредственно, но и бизнес-процессов, процессов принятия управленческих решений, позволяя максимально оптимизировать их, что, в свою очередь, оказывает положительное влияние на эффективность деятельности компании.

Среди преимуществ цифровизации в сфере управления финансами можно выделить следующие аспекты. Сотрудники финансовых служб могут быть не привязаны к месту работы, так как с помощью цифровых продуктов вся необходимая информация всегда доступна. Многие специалисты отмечают значительное облегчение процесса документооборота, а также увеличение его эффективности ввиду исчезновения необходимости работы с бумажными документами. Цифровые технологии способны обеспечить оперативный доступ к информации в режиме реального времени. Таким образом, применение современных цифровых инструментов в сфере управления финансами компании позволяют значительно увеличить эффективность ее работы, а также оптимизировать затраты и повысить скорость принятия управленческих решений.

Глобально новые цифровые технологии можно разделить на следующие виды (рис. 4).

Рисунок 4

Технологии облачных вычислений основаны на предоставлении в аренду компаниям вычислительных платформ и приложений, инфраструктур, что

позволяет значительно повысить эффективность бизнеса, а также гибкость и оперативность. Технологии искусственного интеллекта представляют собой алгоритмы, в основе работы которых лежит имитация человеческого мышления. Технологии больших данных применяются для эффективной работы с большими объемами неструктурированной информации: ее хранения, обработки и анализа, а также управления ею. Интернет вещей – это различные устройства, объединенные между собой посредством взаимодействия с помощью беспроводной связи.

Искусственный интеллект (*AI – Artificial Intelligence*), как одна из самых перспективных и распространенных во многих сферах жизни технологий, успешно внедряется в деятельность компаний по ряду причин:

- использование *AI* обеспечивает информационную и экономическую безопасность вследствие возможности распознавания подозрительных сделок и мошеннических атак;
- применение *AI* увеличивает скорость обработки данных, снижая при этом риск возникновения ошибок, вызванных влиянием человеческого фактора;
- *AI* позволяет автоматизировать рутинные процессы, такие как генерирование документов, контроль различных показателей и т.п.;
- структурируя большой объем данных, описывающих каждый бизнес-процесс в компании, *AI* представляет собой действенный инструмент содействия принятию более обоснованных управленческих решений.

В финансовой деятельности технологии искусственного интеллекта позволяют решать задачи, связанные с прогнозированием и анализом рисков, проведением платежей, управлением ликвидностью, формированием управленческой и бухгалтерской отчетности.

Наиболее простым инструментом, составным элементом технологий искусственного интеллекта является роботизированная автоматизация процессов (*RPA – Robotic Process Automation*). *RPA* применяется в основном как инструмент оптимизации рутинных задач, которые можно построить в виде простого алгоритма. Решение этих задач выполняется роботом, что позволяет повысить производительность труда, так как робот в состоянии выполнить большее количество операций за то же время; снизить себестоимость за счет сокращения затрат рабочего времени, уделяемого сотрудником решению задачи; сократить количество ошибок [27, 28].

Примеры решения финансовых задач инструментами *RPA* приведены на рис. 5.

Роботизация помогает автоматизировать выполнение многих задач и оптимизировать бизнес-процессы, но достаточно примитивным образом на базовом уровне. Процессы *RPA* построены на базе строго определенных правил, в связи с чем возможности автоматизации посредством роботов ограничены. Более сложный спектр задач можно решить, совместив процессы *RPA* с машинным обучением и искусственным интеллектом.

Машинное обучение (*Machine Learning*) является разновидностью искусственного интеллекта. Под машинным обучением понимается класс методов искусственного интеллекта, предполагающих обучение в процессе решения задачи. Это, по сути, следующий шаг на пути к созданию искусственного интеллекта.

Рисунок 5

Искусственный интеллект расширяет возможности *RPA* и *ML* в решении финансовых задач, так как позволяет не просто автоматизировать множество процессов и задач, сделать этот процесс более осмысленным. Таким образом, роботизация, машинное обучение и искусственный интеллект являются тесно связанными между собой инструментами, несмотря на то, что рассматриваются как отдельные области.

Структурировать данные в пригодную для дальнейшего анализа форму позволяет еще один инструмент – системы класса *Business Intelligence (BI),* представляющие собой совокупность компьютерных инструментов и методов обработки информации. К достоинствам систем *BI* можно отнести такие возможности, как:

- обработка больших данных и их интерпретация в разрезе определенных факторов, которые являются ключевыми для конкретного вида анализа;
- принятие решения на основе результатов моделирования различных сценариев развития событий;
- объединение внутренних данных, полученных из источников внутри компании, с внешними, которые компания может получить от рынка, на котором она осуществляет свою деятельность.

Основное назначение *BI*-системы заключается в сведении данных воедино, их визуализация, что обеспечивает возможность их дальнейшей интерпретации и анализа.

В отличие от *Business Intelligence*, более сложный инструмент цифровизации *Big Data* способен обрабатывать большие объемы неструктурированной

информации. Предпосылкой появления этой технологии послужил стремительный рост объемов разного рода контента. Рост информации влечет за собой необходимость обработки ее с той скоростью, которая позволит не выходить за временные рамки проекта и своевременно принять меры в случае отклонения от показателей проекта. Информация может поступать в различном виде из различных источников, то есть в неструктурированном виде. Как правило, в общем потоке преобладает именно такой вид данных. Посредством *Big Data* эта информация обрабатывается, превращаясь на выходе в пригодную для дальнейшего анализа.

В сфере финансов технологии *Big Data* все шире применяются для анализа, планирования и прогнозирования различных финансовых показателей, выявления и оценки внешних рисков.

Еще одним не менее перспективным и востребованным инструментом является технология распределенного реестра - блокчейн. Данная технология позволяет оптимизировать множество разных бизнес-процессов, как, например, подтверждение подлинности сделок и товаров, контроль поставок товаров на протяжении всего пути, если речь идет о перевозках международного масштаба. Среди неоспоримых плюсов – децентрализованная организация хранения данных, что дает возможность сохранить их при возникновении сбоя на одной из машин. Также можно отметить такие положительные факторы, как скорость проведения транзакций, независимость от посредников, полную конфиденциальность [1,2].

В рамках финансовой деятельности компаний блокчейн может быть полезен при решении таких задач, как:

- *Формирование бизнес-процессов, технологических процессов*. Так как в результате изменения вводных, меняются и сами результаты, процесс может усложняться. Блокчейн помогает его оптимизировать, используя в качестве блока ранее достигнутые результаты.
- *Управление активами компании*. Выпуск токенов на базе технологии блокчейн, которые представляют реальные активы, обеспечивает прозрачность передачи прав на собственность.
- *Безопасность.* Блокчейн позволяет хранить зашифрованные данные, при этом сохраняя за пользователями возможность полностью контролировать принадлежащую им информацию.
- *Смарт-контракты*. Это программы, которые при выполнении условий сделки выполняются автоматически, что позволяет оптимизировать процесс, снизить риски и затраты.

Блокчейн помогает упростить платежные процессы, а также предоставляет дешевый способ отправки платежей, помогает в управлении поставками, но не является универсальным решением.

Рассмотренные выше цифровые решения позволяют автоматизировать отдельные функции казначейства. Помимо этого, для цифровизации процесса управления денежными потоками компании используют и комплексные решения.

Примером комплексного решения цифровизации казначейских функций являются мультибанковские платежные платформы. Они представляют собой платформенные решения, которые обеспечивают упрощенный доступ ко всем корпоративным счетам и операциям с ними, что позволяет сократить затраты труда и времени на сбор информации в онлайн-системах различных банков. Предпосылками к появлению мультибанковских платформ послужили такие факторы, как необходимость контролировать счета в разных банках; сложность адаптации к различным системам онлайн-банкинга, так как каждый банк использует свою платформу и единообразие в данном вопросе отсутствует;

потребность в экономии времени при оформление банковских переводов и др. Мультибанковские платформы позволяют оперативно получать агрегированную информацию об остатках средств на счетах компании и получать выписки; составлять различные финансовые отчеты; осуществлять сквозной контроль движения денежных средств в течение операционного дня; отправлять платежи контролировать их исполнение.

Схема работы казначейских агрегаторов стандартна и показана на рис. 6.

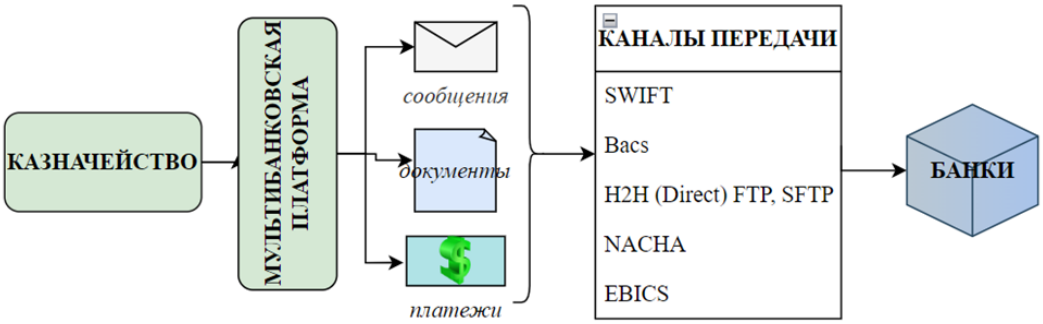


Рисунок 6

К комплексным решениям относится *ERP*-система (*ERP – Enterprise Resource Planning*) – платформа, построенная по модульному принципу и обеспечивающая управление всеми видами деятельности компании (рис. 7). Модули независимы друг от друга, что обеспечивает стабильную работу системы. Главным принципом работы *ERP*-системы является централизованный сбор информации, доступный любому сотруднику. *ERP* повышает эффективность деятельности компании за счет обеспечения прозрачности бизнес-процессов и улучшения коммуникации между подразделениями компании и внешними структурами. *ERP*-система настраивается под определенный функционал в соответствии со спецификой деятельности компании.

Рисунок 7

Еще одним комплексным решением для цифровизации финансовой системы компании является специализированная система управления казначейством (*TMS* –

Treasury Management System). *TMS* – это программное приложение, которое автоматизирует процесс управления финансовыми операциями компании (движение денежных средств, активы, инвестиции). *TMS* может быть установлена либо на сервере компании, либо же предоставляться провайдером в качестве облачного решения.

TMS настраивается под требования конкретной компании и позволяет реализовать функционал по управлению рисками, внутреннему банкингу, управлению финансовыми потоками, прогнозированию движения денежных средств, трейдинговым операциям, формированию разного рода отчетности, автоматизации платежей, обеспечению взаимосвязи банковских и *ERP*-систем.

Обобщив результаты анализа существующих технологий и решений с точки зрения охвата автоматизированных функций (рис. 8), можно сказать, что в распоряжении предприятия сегодня находится большой выбор цифровых инструментов для повышения эффективности работы казначейства и улучшению финансовой системы в целом.

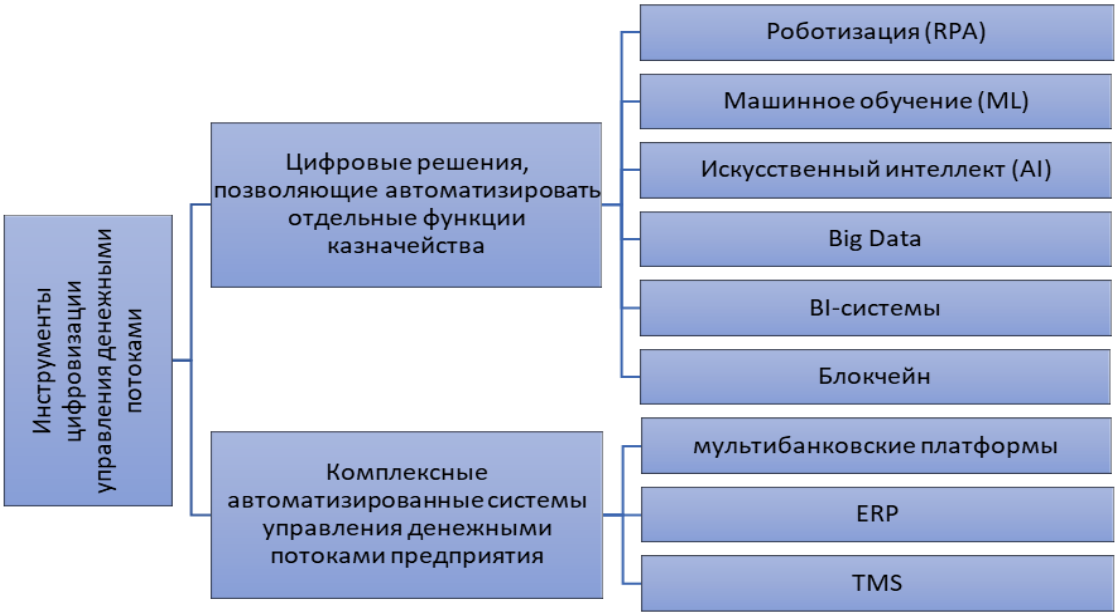


Рисунок 8

Технологии тесно связаны друг с другом и могут закрывать ряд схожих операций с разных сторон, а значит максимально повышать эффективность процессов при комплексном подходе в использовании. Однако выбор наилучших для конкретной компании решений зависит от масштабов и особенностей ее финансовой деятельности и совокупности затрат на внедрение цифровых инструментов.

Предложения по применению инструментов цифровизации бизнес-процессов казначейства

Анализ ключевых бизнес-процессов департамента казначейства позволяет нам выделить ряд типовых проблем, отрицательно влияющих на эффективность деятельности данной структурной единицы (рис. 9).

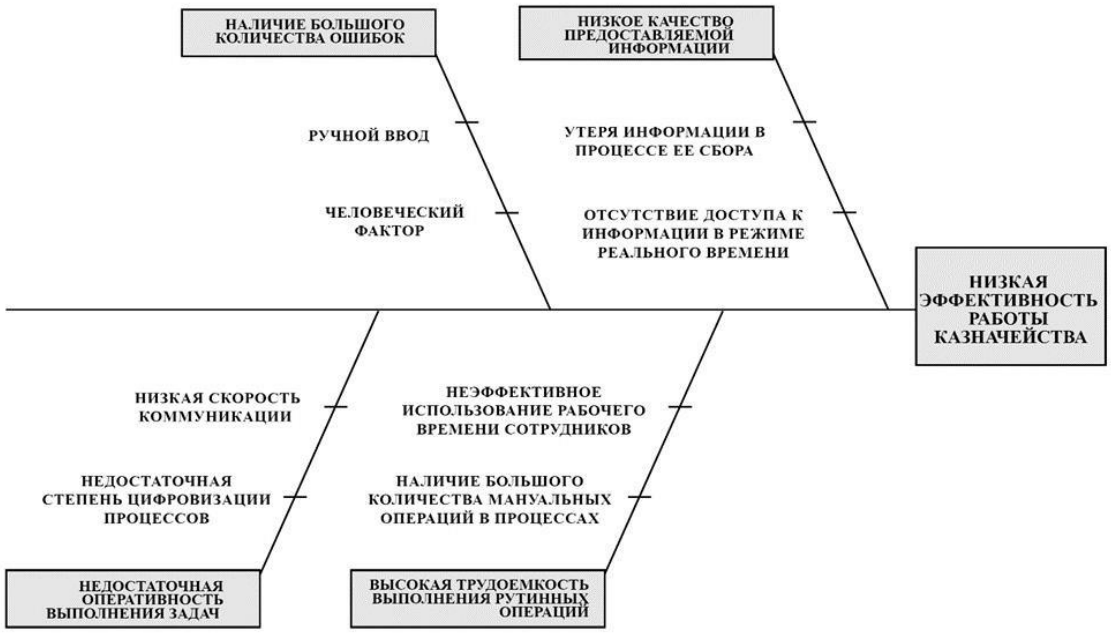


Рисунок 9

К неэффективной работе казначейства приводят, как правило, следующие факторы:

- низкое качество предоставляемой информации;
- большое количество ошибок;
- низкая оперативность выполнения задач;
- высокая трудоемкость выполнения рутинных операций.

Для устранения вышеупомянутых проблем необходимо наладить процесс сбора и обработки информации, минимизировать количество операций, выполняемых вручную, снизить трудоемкость выполнения рутинных задач, а также повысить оперативность выполнения задач, стоящих перед департаментом вследствие повышения производительности (рис. 10).

Рисунок 10

Обработка большого объема информации присуща, прежде всего, процессам управления ликвидностью и транзакционного учета. Базовой информацией для обоих процессов являются банковские выписки, содержащие информацию об остатках средств на счетах компании, а также обо всех транзакциях, совершаемых ежедневно всеми подразделениями во всех банках. Чем крупнее компания и шире масштабы ее деятельности, тем большее количество банковских счетов необходимо обрабатывать. Процесс растягивается во времени, возникает вероятность утери информации, а, следовательно, низкого качества ее предоставления.

Как было показано выше, максимально удобным инструментом для консолидации информации о движении и остатках денежных средств, являются мультибанковские платформы, решающие проблему оперативного сбора информации, обеспечивая при этом минимальную вероятность возникновения ошибки. С задачей же обработки и дальнейшего анализа информации (формирование отчетов и визуализация результатов в виде графиков и диаграмм) могут справиться *BI*-технологии. С их помощью можно анализировать финансовые показатели, а также оптимизировать процессы.

Основным процессом, наиболее значительно влияющим на эффективность деятельности отдела казначейства, является осуществление платежей. Данный процесс характеризуется наличием большого количества ручных операций, кросс-функциональной коммуникации, а, следовательно, высокой вероятностью возникновения ошибок ручного ввода, высокой трудоемкостью и задержками времени.

Для сокращения количества ошибок при вводе информации целесообразно минимизировать количество операций, осуществляемых вручную.

На этапе заведения счетов во внутренние системы и получения необходимых согласований оптимизацию процессов обеспечивают *CRM*-системы, которые могут существовать как самостоятельно, так и в качестве встроенного модуля *ERP*.

На этапе формирования списка платежей и проверки подтверждающих документов сотрудник казначейства сталкивается с довольно трудоемким процессом. Как правило, подтверждающие документы предоставляются в формате *pdf* тремя путями:

1) сохранение документов на сервере в папке для общего пользования;
2) сохранение документов в облаке;
3) документы направляются в запросе по электронной почте.

Сотрудник казначейства получает документы от других подразделений и в дальнейшем сравнивает с утвержденным реестром платежей. На этом этапе могут возникать такие проблемы, как утеря подтверждающих документов; допущение ошибок в платежных реквизитах; длительная обработка документов в виду их большого объема.

Данную проблему можно частично или полностью решить за счет внедрения автоматизации посредством *RPA*. Уровень сложности зависит от конкретно поставленной задачи. Роботы способны осуществлять поиск документов по папкам (например, по номеру счета/инвойса), группировать *pdf* -файлы в заданном порядке, распознавать текст, а также сверять данные в файлах разного формата – *.pdf* и *.xls*. При наличии оркестратора – инструмента, который управляет работой роботов, – данный процесс может быть реализован без непосредственного вмешательства человека, что позволит максимально устранить риск ошибок ручного ввода и прочих ошибок человеческого фактора.

Таким образом, *ERP* и *RPA* позволяют минимизировать количество ручных

операций, повысить оперативность решения поставленных перед казначейством задач и снизить трудоемкость рутинных операций.

Выбор инструментов цифровизации для компании – задача не простая. Цифровые проекты требуют значительных и инвестиций и связаны с высокими рисками. Не всем компаниям доступны имеющиеся на рынке продукты. Немаловажным фактором для принятия решения является и тенденция сокращения жизненного цикла технологий вследствие быстрого устаревания и вытеснения новыми более совершенными техническими решениями. Проведенное исследование позволило обобщить применимость различных инструментов для решения финансовых задач.

Экономический эффект от внедрения цифровых инструментов в финансовые бизнес-процессы рассчитать достаточно сложно. Это долгосрочный проект, требующий не только стартовых, но и регулярных последующих инвестиций, так как любое программное обеспечение требует постоянной доработки, оптимизации, обновления и технического обслуживания. Каждая компания, приняв решение оптимизировать свои бизнес-процессы посредством информационных технологий, работает тем самым на перспективу и вкладывает средства в повышение не только экономической эффективности, но, прежде всего, в улучшение качества реализации своей внутренней деятельности и выстраивание ее таким образом, чтобы рутинные задачи не отвлекали персонал от решения более значимых глобальных задач.

Заключение

Казначейские службы играют ключевую роль в управлении финансовыми активами компании. В их зоне ответственности находятся такие важные процессы как управление ликвидностью, поддержание и контроль стабильной платежеспособности компании, оперативное управление денежными средствами, а также приумножение пассивных доходов компании. Роль казначейства в компаниях трансформировалась в течение последних десятилетий. Теперь это не только отдел, выполняющий оперативные функции. Современное казначейство является стратегическим партнером бизнеса, оказывающим ему ежедневную поддержку во многих критически важных вопросах.

В рамках своего функционала казначейства ежедневно выполняют огромное количество рутинных задач, которые крайне важны для деятельности компании. Именно поэтому цифровизация бизнес-процессов казначейства крайне необходима.

В мировой практике существует огромное количество самых разных цифровых инструментов, позволяющих оптимизировать любые процессы. Для каждого инструмента существует свой набор задач, которые возможно максимально оптимизировать посредством его внедрения. Цифровые инструменты могут представлять собой как точечные решения, так и комплексные, системные, трансформирующие бизнес-процессы компании или определенного ее звена на глобальном уровне. Целесообразность внедрения того или иного инструмента зависит от предполагаемого масштаба трансформации бизнес-процессов, который, в свою очередь, зависит от размера компании. Внедрение оптимального набора современных цифровых технологий позволяет вывести автоматизацию на новый интеллектуальный уровень.

Литература

1. Gorodnichev M., Kukharenko A., Kukharenko E., Salutina T. Methods of developing systems based on bockchain. Conference of Open Innovation Association, FRUCT, 2019. – № 24. – С. 613-618.

2. Gorodnichev M.G., Kukharenko E.G., Salutina T.U., Moseva M.S., Kukharenko A.M. Features of the development of information systems for working with blockchain technology // В сборнике: Journal of Physics: Conference Series. International Scientific Conference «Conference on Applied Physics, Information Technologies and Engineering - APITECH-2019». Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations; Polytechnical Institute of Siberian Federal University, 2019. – С. 33039.
3. Kukharenko E., Yankevskiy A. Management of distributed medical information systems // В сборнике: Lecture Notes in Information Systems and Organisation. 3rd. Сер. «Digitalization of Society, Economics and Management - A Digital Strategy Based on Post-pandemic Developments», 2022. – С. 187-205.
4. Kukharenko E.G. Analysis of approaches to audiovisual interaction information systems creating in the context of digital transformation // В сборнике: Proceedings of the 2021 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», T and QM and IS 2021, 2021. – С. 880-882.
5. Kukharenko E.G., Alyushina S.G., Yankevskiy A.V. Innovative technologies monitoring the state of geographically distributed networks industrial facilities (using the example of pipeline transport) // В сборнике: Proceedings of the 2021 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», T and QM and IS 2021, 2021. – С. 883-887.
6. Kukharenko E.G., Korkunov I.A., Gorodnichev M.G., Salutina T.U. On the Introduction of Digital Economics in the Transport Industry // В сборнике: 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2019, (2019), RU, 8706797.
7. Kuzovkova T.A., Saliutina T.Y., Kukharenko E.G., Sharavova O.I. Mechanism of interconnected management of development of networks and platforms of the internet of things on the basis of evaluation of synergetic efficiency // В сборнике: 2020 Wave Electronics and its Application in Information and Telecommunication Systems, WECONF 2020, 2020. – С. 9131158.
8. Volodina E.E., Kukharenko E.G., Sukhodolskaya T.A. Innovative methods of spectrum management for the development of promising mobile networks // В сборнике: Proceedings of the 2021 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», T and QM and IS 2021, 2021. – С. 911-914.
9. Кухаренко Е.Г. Цифровые инструменты повышения эффективности деятельности компании инфокоммуникационной отрасли // Экономика и качество систем связи, 2022. – № 3 (25). – С.10-21.
10. Кузовкова Т.А., Салютина Т.Ю., Кухаренко Е.Г. Методические основы и результаты интегральной оценки цифрового развития экономики и общества // Электронный научный журнал «Век качества», 2019. – № 3. – С. 106-122.
11. Кузовкова Т.А., Салютина Т.Ю., Кухаренко Е.Г., Шаравова О.И. Механизм управления эффективностью применения цифровых технологий // Инновации в менеджменте, 2020. – № 2 (24). – С. 36-45.
12. Кухаренко А.М., Анохина М.Е. Роль единого информационного пространства предприятия в повышении эффективности бизнеса // В сборнике: Технологии информационного общества. Сборник трудов XII Международной отраслевой научно-технической конференции, 2018. – С.339-340.
13. Кухаренко Е.Г. Управление конкурентоспособностью компании на инфокоммуникационном рынке // В сборнике: Технологии информационного общества. Сборник трудов XII Международной отраслевой научно-технической конференции, 2018. – С. 346-347.

14. Кухаренко Е.Г., Аминев О. Мировой опыт цифровизации социальной сферы // В книге: Мобильный бизнес: Перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) XLIII международной конференции РАЕН. Москва, 2019. – С. 28-32.
15. Кухаренко Е.Г., Андержанова Г. CRM в телекоммуникациях как фактор повышения эффективности бизнеса // В сборнике: Технологии информационного общества. Сборник трудов XII Международной отраслевой научно-технической конференции, 2018. – С. 357-359.
16. Кухаренко Е.Г., Аношкина Е.С. Повышение эффективности управления регионом на основе информационно-телекоммуникационных технологий // В сборнике: Технологии информационного общества. Сборник трудов XII Международной отраслевой научно-технической конференции, 2018. – С. 354-356.
17. Кухаренко Е.Г., Карныгина Е.А. Анализ применения цифровых коммуникаций для продвижения банковских продуктов и услуг // В книге: Мобильный бизнес: Перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 48-й международной конференции. Москва, 2021. – С. 41-46
18. Кухаренко Е.Г., Карныгина Е.А. Стратегия продвижения банковских продуктов цифровой среде // В сборнике: технологии информационного общества. Сборник трудов XVI Международной отраслевой научно-технической конференции, 2022. – С. 192-194.
19. Кухаренко Е.Г., Николаева Е.А. Тенденции развития цифрового бизнеса в банковской сфере России // В сборнике: технологии информационного общества. Сборник трудов XV Международной отраслевой научно-технической конференции «Технологии информационного общества», 2021. – С. 264-265.
20. Кухаренко Е.Г., Синьянь Ц. Применение digital-инструментов в маркетинговой деятельности операторов подвижной связи КНР // В книге: Мобильный бизнес: Перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 47-й международной конференции. Москва, 2021. – С. 54-58.
21. Кухаренко Е.Г., Соломина Ю.Н. Трансформация моделей ведения бизнеса в условиях цифровизации // Экономика и качество систем связи, 2021. – № 2 (20). – С. 3-12.
22. Kukharenko E., Yankevskiy A. MANAGING THE DIGITALIZATION OF BUSINESS PROCESSES IN AN ORGANIZATION // В сборнике: E3S Web of Conferences. V International Scientific Forum on Computer and Energy Sciences (WFCES 2023), 2023. – С. 02027.
23. Самойличенко Е.Е., Самойличенко Н.В. Финансы предприятий. Часть 1. Финансовые аспекты организации производственно-хозяйственной деятельности предприятий: учебное пособие для студентов направления 38.03.01 «Экономика». Ярославль: Образовательная организация высшего образования (частное учреждение) «Международная академия бизнеса и новых технологий (МУБиНТ)», 2017. – 202 с.
24. Савченко Н.Л. Управление финансовыми ресурсами предприятия: учеб. пособие. М-во науки и высш. образования рос. Федерации, Урал. федер. ун-т. – Екатеринбург: Изд-во Урал. ун-та, 2019. – 164 с.
25. Кухаренко Е.Г., Гуляева Е.А. Инструменты цифровизации финансовой системы компании // В книге: Мобильный бизнес: Перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 49-й международной конференции. Москва, 2022. – С. 78-83.
26. Гуляева Е.А., Кухаренко Е.Г. Цифровизация финансовой системы компании // В сборнике: технологии информационного общества. Сборник трудов XVII

Международной отраслевой научно-технической конференции, 2023. – С. 155-158.
27. Маньков В.А., Кухаренко Е.Г. Применение технологических инноваций для цифровизации бизнес-процессов компании // В сборнике: технологии информационного общества. Сборник трудов XVI Международной отраслевой научно-технической конференции, 2022. – С. 195-197.
28. Маньков В.А., Кухаренко Е.Г. Технологии цифровизации бизнес-процессов инфокоммуникационной компании // В сборнике: технологии информационного общества. Сборник трудов XV Международной отраслевой научно-технической конференции «Технологии информационного общества», 2021. – С. 266-268.

ФАКТОРНЫЕ ОГРАНИЧЕНИЯ РАЗВИТИЯ БИЗНЕС-СРЕДЫ ЭКОСИСТЕМНОЙ НАПРАВЛЕННОСТИ В ОТРАСЛИ ИКТ

Е. В. Павлова, *к.э.н., Санкт-Петербургский государственный университет телекоммуникаций им. проф. Бонч-Бруевича, epavlova.pnd-9@yandex.ru.*

УДК 338

Аннотация. Трансформация экономических, политических, социальных аспектов предпринимательской деятельности посредством цифровых технологий привела к появлению новых организационных форм ведения бизнеса в российской экономике и в отрасли информационно-коммуникационных технологий (далее – ИКТ) в частности. Наряду с существующими и потенциальными преимуществами, которые несут в себе платформенные модели ведения бизнеса, во внешней среде появляются факторы, препятствующие дальнейшему развитию и распространению вышеуказанных предпринимательских цифровых платформ и экосистем отрасли ИКТ. В данной статье проведено исследование инвайроментальных факторов, ограничивающих развитие предпринимательских бизнес-единиц цифровой и экосистемной направленности в отрасли ИКТ.

Ключевые слова: информационно-коммуникационные технологии; отрасль ИКТ, цифровая платформа; бизнес-экосистема; критическая информационная инфраструктура; обеспечение информационной безопасности.

FACTORIAL CONSTRAINTS ON THE DEVELOPMENT OF AN ECOSYSTEM-ORIENTED BUSINESS ENVIRONMENT IN THE ICT INDUSTRY

E. V. Pavlova, *St. Petersburg State University of Telecommunications named after Prof. M. A. Bonch-Bruevich.*

Annotation. The transformation of the economic, political, and social aspects of entrepreneurial activity through digital technologies has led to the emergence of new organizational forms of doing business in the Russian economy and in the information and communication technology (hereinafter – *ICT*) industry in particular. Along with the existing and potential advantages that platform business models bring, factors appear in the external environment that hinder the further development and dissemination of the above-mentioned entrepreneurial digital platforms and ecosystems of the *ICT* industry. This article examines the environmental factors limiting the development of entrepreneurial business units of digital and ecosystem orientation in the *ICT* industry.

Keywords: information and communication technology; *ICT* industry; digital platform; business ecosystem; critical information infrastructure; information security.

Введение

Распространение экосистем в бизнес-среде российской экономики в целом и отрасли ИКТ, в частности, представляет собой закономерный этап развития Индустрии 4.0, так как масштабная цифровизация бизнес-процессов, происходящих на предприятиях всех отраслей экономики, привела к трансформации существующих моделей ведения бизнеса [1-2]. В основе функционирования любой экосистемы находится платформенная технология, так как экосистема представляет собой совокупность разнообразных онлайн-сервисов, объединенных между собой посредством единой цифровой платформы [3]. Цифровая платформа в отрасли ИКТ, в свою очередь, является базой экосистемы, так как обеспечивает беспрепятственный вход пользователя к любому его сервису посредством единого *ID*, так как на смену общественным идентификационным документам потребителя приходит персональный *ID* (с английского *identifier*), который является «единым паспортом» клиента в цифровом информационном пространстве [4].

Целью проведенного исследования, результаты которого отражены в статье, является идентификация факторов негативного влияния внешней среды на развитие и распространение цифровых экосистем в отрасли ИКТ.

Понятие термина «цифровая платформа»

Определение понятия «цифровая платформа» не приводится в нормативно-правовых актах, устанавливающих сущность, порядок работы и назначение государственных единых цифровых платформ, например, в социальной сфере, в сфере занятости и трудовых отношений «Работа в России», таких как «Одно окно экспортера», «ГосТех», «Госмаркет», «Национальная система пространственных данных», «Цифровая аналитическая платформа предоставления статистических данных» и др.[1]

Тем не менее в Постановлении Правительства РФ от 30 апреля 2019 г. № 529 «Об утверждении Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции» приводится определение «цифровой платформы», под которой понимается совокупность информационных технологий и технических средств, направленных на решение различных технологических задач и

[1] Постановление Правительства РФ от 13 мая 2022 г. N 867 «О единой цифровой платформе в сфере занятости и трудовых отношений «Работа в России» – URL: https://base.garant.ru/404612909/ (дата обращения: 11.05.2024).

Постановление Правительства РФ от 29 декабря 2023 г. N 2386 «О государственной информационной системе «Единая централизованная цифровая платформа в социальной сфере» – URL: https://base.garant.ru/408324253/ (дата обращения: 18.07.2024).

Постановление Правительства РФ от 30 ноября 2022 г. № 2194 «Об утверждении Положения о федеральной государственной информационной системе «Управление единой цифровой платформой Российской Федерации «ГосТех» и Положения о федеральной государственной информационной системе «Госмаркет» – URL: https://base.garant.ru/405875901/ (дата обращения: 10.06.2024).

Постановление Правительства РФ от 7 июня 2022 г. № 1040 «О федеральной государственной информационной системе «Единая цифровая платформа «Национальная система пространственных данных» – URL: https:// base.garant.ru/404817579/ (дата обращения: 15.06.2024).

Постановление Правительства РФ от 22 июня 2021 г. N 956 «О государственной информационной системе «Цифровая аналитическая платформа предоставления статистических данных» – URL: https://base.garant.ru/401391213/ (дата обращения: 01.08.2024).

взаимодействие субъектов экономической деятельности в промышленной сфере[2]. Данный термин не дает определение понятия «цифровая платформа» в широком смысле и может использоваться только применительно к предприятиям промышленной сферы деятельности [5].

В более широком смысле термин «цифровая платформа» раскрыт в докладе Центрального банка России от апреля 2021 г. о регулировании экосистемной модели ведения бизнеса, в котором поднимаются вопросы отрицательного влияния экосистем на общество в целом и конкурентную среду национальной экономики, рассматриваются вопросы нормативно-правового регулирования деятельности экосистем в Китае, Европейском Союзе и США и возможность адаптации данных законодательных практик применительно к российской экономике [6]. В вышеуказанном докладе под цифровой платформой понимается информационная система, функционирующая посредством сети интернет и обеспечивающая взаимодействие различных субъектов экономических отношений, представленных на ней, через процессы распределения и обмена товарами и услугами[3].

Так как цифровая платформа и электронные технологии являются ключевым ядром экосистемных форм ведения бизнеса отрасли ИКТ, то приоритетное значение в данных моделях уделяется вопросам, связанным с обеспечением информационной безопасности всех сервисов, компонентов и составных элементов платформы [7]. Обусловлена подобная необходимость значительными масштабами вовлечения в деятельность платформы ее субъектов-участников рынка ИКТ, к которым относятся группы разработчиков, потребителей и поставщиков услуг, а также наличием больших объемов персональных данных [8].

Взаимосвязь цифровых платформ отрасли ИКТ и объектов критической информационной инфраструктуры

Определение цифровой платформы как информационной системы и наличие значительного объема идентификационных данных пользователей приводит к тому, что разнообразные сегменты экосистемы, основанные на цифровых технологиях, становятся объектами критической информационной инфраструктуры (далее – КИИ). К объектам КИИ в соответствии с федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» относятся информационные системы, автоматизированные системы управления и информационно-телекоммуникационные сети[4]. Соответственно, государственные учреждения, госорганы и любые юридические лица, в том числе и бизнес-экосистемы, которые являются владельцами или арендаторами объектов КИИ, автоматически становятся субъектами КИИ [9].

В этой связи цифровые платформы бизнес-экосистем отрасли ИКТ попадают под действия положений и требований нормативно-правовых актов,

[2] Постановление Правительства РФ от 30 апреля 2019 г. N 529 «Об утверждении Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции» – URL: https://base.garant.ru/72237228/ (дата обращения: 15.07.2024).

[3] Экосистемы: подходы к регулированию / Доклад для общественных консультаций. Центральный банк Российской Федерации. Апрель 2021 г. – URL: https://cbr.ru/Content/Document/File/119960/Consultation_Paper_02042021.pdf (дата обращения: 29.07.2024).

[4] Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» – URL: https://base.garant.ru/71730198/ (дата обращения: 03.06.2024).

направленных на обеспечение безопасности объектов КИИ [10]. Определение критической информационной инфраструктуры также приведено в Федеральном законе от 26 июля 2017 г. № 187-ФЗ, который относит в данную категорию объекты КИИ, а также сети электросвязи, с помощью которых обеспечивается взаимодействие между данными объектами. Перечень отраслей КИИ достаточно обширен и согласно Государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации включает в себя следующие сферы: связь, топливно-энергетический комплекс, здравоохранение, оборонную промышленность, банковскую сферу, науку, горнодобывающую промышленность, атомную энергетику, химическую промышленность, транспорт, ракетно-космическую промышленность, энергетику, металлургическую промышленность и сферу регистрации прав на недвижимое имущество.

В качестве примера объектов КИИ негосударственных коммерческих предприятий экосистемной направленности в докладе Центрального банка Российской Федерации приводятся разнообразные цифровые сервисы экосистемы компании «Яндекс», так как на применении сервисов платформы «Яндекс.Карты», «Яндекс.Транспорт», «Яндекс.Навигатор» основано распределение дорожного трафика в Москве. Отнесение цифровых платформ и сервисов экосистем к объектам КИИ влечет за собой не право, а обязанность субъектов КИИ обеспечивать безопасность КИИ [11]. Под безопасностью КИИ следует понимать ее бесперебойное функционирование в период проведения компьютерной атаки и после ее завершения.

Мероприятия для обеспечения информационной безопасности цифровых платформ отрасли ИКТ как объектов критической информационной инфраструктуры

Для обеспечения безопасности КИИ от собственников экосистем требуется на постоянной и непрерывной основе проводить комплексные мероприятия по обеспечению информационной безопасности, внедрять на приоритетной основе меры по предотвращению компьютерных атак на экосистему в целом и ее участников в частности[5]. В соответствии с федеральным законом от 26 июля 2017 г. № 187-ФЗ под компьютерной атакой понимается специальная адресная процедура влияния на объекты КИИ и сетей электросвязи для вывода из строя вышеуказанных объектов либо нанесение ущерба безопасности их информационным данным, а под компьютерным инцидентом понимается событие, заключающееся в сбое или завершении работоспособности объекта или объектов КИИ, а также применяемой для их взаимосвязи сети электросвязи, или несоблюдении безопасности информационных данных вышеуказанных объектов по причине компьютерной атаки.

Функционирование экосистемы как субъекта КИИ налагает на нее следующие обязанности:

1) взаимодействие посредством НКЦКИ с ФСБ России в части обнаружения, предупреждения и ликвидации последствий компьютерных атак;

2) немедленное извещение о компьютерных инцидентах и атаках ФСБ России через НКЦКИ;

[5] Приказ Федеральной службы по техническому и экспортному контролю от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» – URL: https://base.garant.ru/71901880/ (дата обращения: 10.06.2024).

3) незамедлительное оповещение Центрального банка России о компьютерных инцидентах и атаках, если компания является банковской организацией или работает в финансовой сфере;

4) принятие комплекса мер по устранению влияния компьютерных атак по установленному ФСБ России алгоритму;

5) предоставление данных в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА) в соответствии с Приказом № 367, утвержденным ФСБ России[6];

6) взаимодействие с другими субъектами КИИ по вопросам обмена данными об атаках;

7) направление сотрудника компании в рабочую группу, создаваемую НКЦКИ из делегатов субъектов КИИ.

Для выполнения вышеуказанных обязанностей собственнику и менеджменту экосистемы как субъекту КИИ необходимо произвести комплекс следующих мероприятий:

1) подготовить защищенный канал межсетевого взаимодействия с НКЦКИ;

2) подключить предприятие к технической инфраструктуре НКЦКИ через личный кабинет;

3) провести инвентаризацию имеющихся на предприятии объектов КИИ: информационных систем, автоматизированных систем управления и информационно-телекоммуникационных сетей;

4) выполнить категорирование определенных в результате инвентаризации объектов КИИ, т. е. присвоить каждому объекту КИИ одну из четырех категорий[7];

5) провести согласование категории объектов КИИ с Федеральной службой по техническому и экспортному контролю;

6) осуществлять защитные меры, исходя из категории значимости объектов КИИ;

7) использовать специальные превентивные средства и средства элиминирования отрицательного воздействия атак;

8) обеспечить структурное подразделение по обеспечению информационной безопасности следующими специалистами:

- специалист по обнаружению компьютерных атак и инцидентов;
- специалист по обслуживанию средств;
- специалист по оценке защищённости;
- специалист по ликвидации последствий компьютерных инцидентов;
- специалист по установлению причин компьютерных инцидентов.

9) проводить тренировки и специальные киберучения работников на регулярной основе;

---

[6] Приказ ФСБ России от 24 июля 2018 г. N 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=443301 (дата обращения: 05.07.2024).

[7] Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» – URL: https://base.garant.ru/71876120/ (дата обращения: 22.05.2024).

10) проводить систематическое повышение квалификации ответственных сотрудников в сфере информационной безопасности;

11) обеспечить участие работников компании в специализированных соревнованиях по информационной безопасности;

12) разработать план, сценарии и инструкции по реагированию на инциденты, предупреждения и ликвидации последствий компьютерных атак.

Как видно из вышеперечисленного, реализация всех вышеизложенных мероприятий требует от экосистемы наличия значительных финансовых резервов денежных средств на проведение всего комплекса превентивных и итеративных мер по обеспечению информационной безопасности компонентов и сервисов экосистемы, что для владельцев локальных цифровых платформ, не связанных с крупным бизнесом и экосистемами, будет завышать стоимость предоставляемых ими услуг и снижать конкурентную привлекательность на клиентском рынке [12].

Ответственность и надзорная деятельность за выполнением требований по обеспечению безопасности цифровых платформ отрасли ИКТ

Для осуществления методической и надзорной деятельности за выполнением задач по обеспечению безопасности объектов КИИ в соответствии с Указом Президента Российской Федерации от 15 января 2013 года № 31с создана Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, которая представляет собой систему, включающую в себя силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты[8]. К силам ГосСОПКА относятся структуры Федеральной службы безопасности России, Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ) и субъекты КИИ. В задачи ФСБ РФ входит выполнение работ по организации ГосСОПКА, создание методических рекомендаций по обнаружению атак, по формированию защиты и разработка алгоритма обмена информацией об инцидентах между участниками процессов обеспечения безопасности объектов КИИ.

За невыполнение требований по предоставлению необходимой информации и обеспечению безопасности объектов КИИ предусмотрены меры административной ответственности в соответствии с Федеральным законом от 26 мая 2021 года № 141-ФЗ в размере до 500 000 рублей[9].

Административная ответственность также налагается на юридические и физические лица, владеющие значимыми объектами КИИ, в случае нарушения алгоритма извещения о случаях компьютерных атак или инцидентов. Степень значимости определяется присвоением одной из четырех категорий и включением в реестр значимых объектов КИИ в соответствии с приказом Федеральной службы по техническому и экспортному контролю от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ Российской Федерации». Категорирование объектов КИИ осуществляется на основании пяти аспектов: социальной, экономической, политической, экологической значимости и критериев безопасности. Всего устанавливаются три категории значимости:

[8] Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» – URL: https://base.garant.ru/70299068/ (дата обращения: 18.06.2024).

[9] «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ – URL: https://base.garant.ru/12125267/ (дата обращения: 01.07.2024).

первая, вторая и третья, но объекты, которые в соответствии с критериями значимости не попадают ни в одну из перечисленных категорий значимости, образуют четвертую группу «без категории». Отнесение объекта КИИ к той или иной категории определяется на основании перечня критериев по каждому из пяти блоков значимости [13].

За нарушения в сфере обеспечения безопасности объектов КИИ помимо административной предусмотрена уголовная ответственность. Так, в Уголовный кодекс Российской Федерации введена статья 274.1 Федеральным законом «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 194-ФЗ. Статья 274.1 Уголовного кодекса устанавливает ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Неправомерность действий может быть выражена в следующем:

- нарушении правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации объектов КИИ;
- нарушение правил доступа к информации объектов КИИ.

По вышеуказанной статье предусмотрено максимальное наказание в виде лишения свободы на срок до десяти лет.

В настоящее время в российской практике имеются примеры применения норм уголовного права за невыполнение требований по предоставлению необходимой информации и обеспечению безопасности объектов КИИ [14]. В апреле 2024 г. был задержан заместитель генерального директора по информационным технологиям и производству ООО «Сирена-Трэвел» по статье 274.1 УК в связи со взломом в сентябре 2023 г. базы данных компании в результате масштабной *DDoS*-атаки хакерской группировки, в результате чего у авиакомпаний «Аэрофлот», «Уральских авиалиний» и *Red Wings* возникли перебои с регистрацией пассажиров, так как компания «Сирена-Трэвел» является разработчиком российской системы бронирования авиабилетов «Леонардо», на которую в 2022 г. перешли значимые отечественные авиаперевозчики, такие как группы компаний «Аэрофлот» и *S*7, с целью замещения иностранного программного обеспечения американских систем *Sabre* и *Navitaire*, а также испанской *Amadeus* в сфере бронирования авиабилетов для исключения рисков утечки персональных данных клиентов авиакомпаний и минимизации прочих рисков отрасли авиаперевозок. По информации ООО «Сирена-Трэвел» компания исполнила свои обязательства по своевременному уведомлению органов ГосСОПКИ о произошедшем инциденте в сфере информационной безопасности.

С целью исключения возможности попадания под вышеуказанные меры административной и уголовной ответственности владельцам и менеджменту платформенного бизнеса и экосистемных моделей следует:

- соблюдать сроки извещения Национального координационного центра по компьютерным инцидентам о компьютерных инцидентах не позднее 3 часов с момента обнаружения для значимых объектов КИИ и не позднее 24 часов для иных объектов КИИ;
- при включении объекта КИИ в реестр значимых объектов КИИ подготовить и утвердить план ответных мер на компьютерные атаки и инциденты с направлением копии в Национальный координационный центр по компьютерным инцидентам не позднее 7 календарных дней;
- ежегодно подготавливать и осуществлять тренировки по применению мероприятий плана ответных мер.

Необходимо отметить, если для обеспечения безопасности объектов КИИ необходимо оказывать защиту другим информационным ресурсам, которые не являются субъектами КИИ, то компании-владельцы вышеуказанных ресурсов также могут быть отнесены к системе ГосСОПКА и обязаны будут обеспечивать выполнение выше обозначенного комплекса мер и обязанностей [15].

Заключение

Проведение комплекса вышеизложенных действий и мероприятий, направленных на выполнение положений федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» по обеспечению безопасности объектов КИИ, отвлекает у компаний отрасли ИКТ значительные объемы трудовых и финансовых ресурсов.

Выделить средства, достаточные для закупки априорных мер защиты (защитные меры, эксплуатация которых сокращает качественно или количественно существующие уязвимости объектов защиты информационных активов, тем самым снижая вероятность реализации соответствующих угроз информационной безопасности, например, средства защиты от несанкционированного доступа) и апостериорных защитных мер (защитные меры, эксплуатация которых сокращает степень тяжести последствий нарушения свойств информационной безопасности информационных активов, например, средства резервного копирования и восстановления информации) могут себе позволить только собственники крупных цифровых платформ и бизнес-экосистем отрасли ИКТ, при этом малый и средний бизнес становятся невалидными на конкурентном рынке ИКТ.

Таким образом, невозможность проведения мероприятий по обеспечению безопасности объектов КИИ имеет негативное влияние на предложение услуг со стороны цифровых платформ малого и среднего бизнеса отрасли ИКТ, а также выражается в повышении себестоимости и, как следствие, ценового предложения со стороны крупных участников цифрового экосистемного рынка.

Следствием этих тенденций будет существенное удорожание стоимости услуг предприятий экосистемной направленности отрасли ИКТ для конечного потребителя, монополизация рынка ИКТ и сокращение объемов спроса со стороны цифрового клиентского рынка ИКТ.

Литература

1. Павлова Е.В., Свистунов Л.О. Цифровизация экономики как часть процесса индустрии 4.0 // В сборнике: Современный менеджмент: проблемы и перспективы // Сборник статей по итогам XVIII национальной научно-практической конференции с международным участием. Санкт-Петербург, 2023. – С. 22-25.
2. Шитиков И.Е., Кваша Н.В. Актуальные направления устойчивого развития экономики России // В сборнике: Интеллектуальная инженерная экономика и Индустрия 5.0 (ИНПРОМ-2024). Сборник трудов X Международной научно-практической конференции. В 2-х томах. Санкт-Петербург, 2024. – С. 367-369.
3. Павлова Е.В., Куганов В.Г. Экономические проблемы цифровизации отдельных отраслей и сфер деятельности // Национальные концепции качества: роль качества в научно-технологическом развитии страны: сб. материалов Национал. науч.-практ. конф. с междунар. участием. СПб., 2023. – С. 263-266.
4. Павлова Е.В., Кулакова Ю.В. Перспективы развития нейросетевых технологий в условиях цифровизации экономики // Экономика и качество систем связи, 2024. – № 1 (31). – С. 10-17.
5. Александров М.А., Макаров В.В., Слуцкий М.Г. Инновационные услуги телекоммуникационного предприятия, обусловленные процессами цифровой

трансформации // Журнал правовых и экономических исследований, 2021. – № 2. – С. 139-144.
6. Жолобова А.И., Макаров В.В., Павлова Е.В. Проблемы развития рынка информационных технологий в условиях пандемии // Евразийское Научное Объединение, 2021. – № 10-3 (80). – С. 181-184.
7. Жолобова А.И., Макаров В.В., Павлова Е.В. Информационные технологии в цифровой экономике // Экономика и бизнес: теория и практика, 2021. – № 7 (77). – С. 59-62.
8. Макаров В.В., Павлова Е.В. Влияние экосистем на цифровую трансформацию экономики // Журнал правовых и экономических исследований, 2024. – № 2. – С. 209-214.
9. Куганов В.Г., Лобанов М.А. Обеспечение конкурентоспособности малого бизнеса в условиях цифровизации экономики // В сборнике: Современный менеджмент: проблемы и перспективы. Сборник статей по итогам XVI международной научно-практической конференции. Санкт-Петербург, 2021. – С. 523-527.
10. Макаров В.В., Гусев В.И., Воронин А.Г. Методологическая парадигма исследования интеллектуального капитала в условиях информационного общества // Российский гуманитарный журнал, 2012. – Т. 1. – № 1. – С. 78-83.
11. Исаков А.В., Свиридов И.В., Фёдорова М.Ю. Спрос и структура рынка инфокоммуникационных услуг в России // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). Сборник научных статей: в 4-х томах. Санкт-Петербург, 2021. – С. 439-442.
12. Макаров В.В., Слуцкий М.Г., Устриков Н.К. Проблемы и задачи цифровой трансформации экономики России // Международный журнал гуманитарных и естественных наук, 2020. – № 4-1 (43). – С. 174-177.
13. Куганов В.Г., Лобанов М.А. Особенности функционирования предприятий в условиях цифровизации // В сборнике: Современный менеджмент: проблемы и перспективы // Сборник статей по итогам XVIII национальной научно-практической конференции с международным участием. Санкт-Петербург, 2023. – С. 17-21.
14. К разработчику системы бронирования «Леонардо» пришли силовики. – URL: https://www.rbc.ru/politics/03/04/2024/660d55bb9a79473dc22a5041/ (дата обращения: 04.04.2024).
15. Как и кому необходимо подключаться к ГосСОПКА – URL: https://gossopka.ru/pub/kak-i-komu-neobkhodimo-podklyuchatsya-k-gossopka/ (дата обращения: 03.05.2024).

ОСОБЕННОСТИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ЦИФРОВЫХ УСЛУГ И СЕРВИСОВ ИНФОКОММУНИКАЦИОННЫХ КОМПАНИЙ

Т.А. Кузовкова, *д.э.н., профессор, Московский технический университет связи и информатики, t.a.kuzovkova@mtuci.ru;*
И.М. Шаравов, *Московский технический университет связи и информатики, ivansharavov@yandex.ru;*
Н.С. Курицын, *Московский технический университет связи и информатики, kuritsin.nikita@gmail.com.*

УДК 33+65 (075.8)

Аннотация. В статье приводятся результаты анализа развития телекоммуникационного рынка по видам основных услуг связи за пять лет. На основе статистических данных инфокоммуникационных компаний раскрываются особенности структуры и перспективы развития рынка цифровых услуг и сервисов. На основе выявления характера развития основных цифровых услуг и сервисов определены факторы роста российского рынка облачных сервисов и кибербезопасности. С учетом процессов цифрового преобразования экономики доказана необходимость трансформации методов и принципов завоевания рынка цифровых услуг и сервисов посредством совершенствования структурных элементов стратегической карты цифровизации компаний и персонализации спроса и предложения на данном сегменте рынка.

Ключевые слова: телекоммуникационный рынок; инфокоммуникационные компании; цифровые услуги и сервисы; анализ рынка и перспективы развития; методы и принципы завоевания рынка.

FEATURES AND PROSPECTS OF DEVELOPMENT OF DIGITAL SERVICES AND SERVICES OF INFORMATION AND COMMUNICATION COMPANIES

T.A. Kuzovkova*, Doctor of Economics, Professor, Moscow Technical University of Communications and Informatics;*
I.M. Sharavov, *Moscow Technical University of Communications and Informatics;*
N.S. Kuritsyn, *Moscow Technical University of Communications and Informatics.*

Annotation. The article presents the results of an analysis of the development of the telecommunications market by types of basic communication services over five years. Based on the statistical data of information and communication companies, the features of the structure and prospects for the development of the digital services market are revealed. Based on the identification of the nature of the development of the main digital services and services, the growth factors of the Russian market of cloud services and cybersecurity are determined. Taking into account the processes of digital transformation of the economy, the necessity of transforming the methods and principles of conquering the market of digital services and services by improving the structural elements of the strategic map of digitalization of companies and personalization of supply and demand in this market segment is proved.

Keywords: telecommunication market; infocommunication companies; digital services and services; market analysis and development prospects; methods and principles of market conquest.

Введение

При высоких темпах скорости и масштабов развития рынка цифровых услуг и сервисов он еще недостаточно исследован по характеру спроса и изменчивости потребительского поведения, не выявлены его отраслевые особенности и перспективы. Это определяет актуальность систематизации практического опыта внедрения цифровых услуг и сервисов инфокоммуникационными компаниями.

Слияние технологий в области информационно-коммуникационных технологий приводит к размыванию границ между отраслями, создавая в цифровой среде единый сектор с повышенной синергией, который также изменяет позицию потребителя в его интеракциях с производителями и другими факторами рыночной экономики. Интегрирование компонентов сетевой структуры, объединение разнообразных форм бизнес-деятельности, переход к цифровой экономике и

обществу требуют глубокой переориентации бизнес-моделей, а также стратегий и основ занятия лидирующих позиций на рынке цифровых продуктов и услуг [1-3].

Целью исследования является разработка системных решений по персонификации потребностей клиентов, интеграции офлайн-, онлайн- и мобильных процессов, оптимизации цен на пакетные цифровые сервисы с учетом персональных предложений, бонусов, скидок. Это приведет к росту спроса, популярности пакетных услуг, успешности бизнеса операторов связи и развитию рынка цифровых сервисов.

Анализ динамики развития рынка услуг связи

Для последнего пятилетия характерно уверенное развитие российского рынка связи (рис. 1).

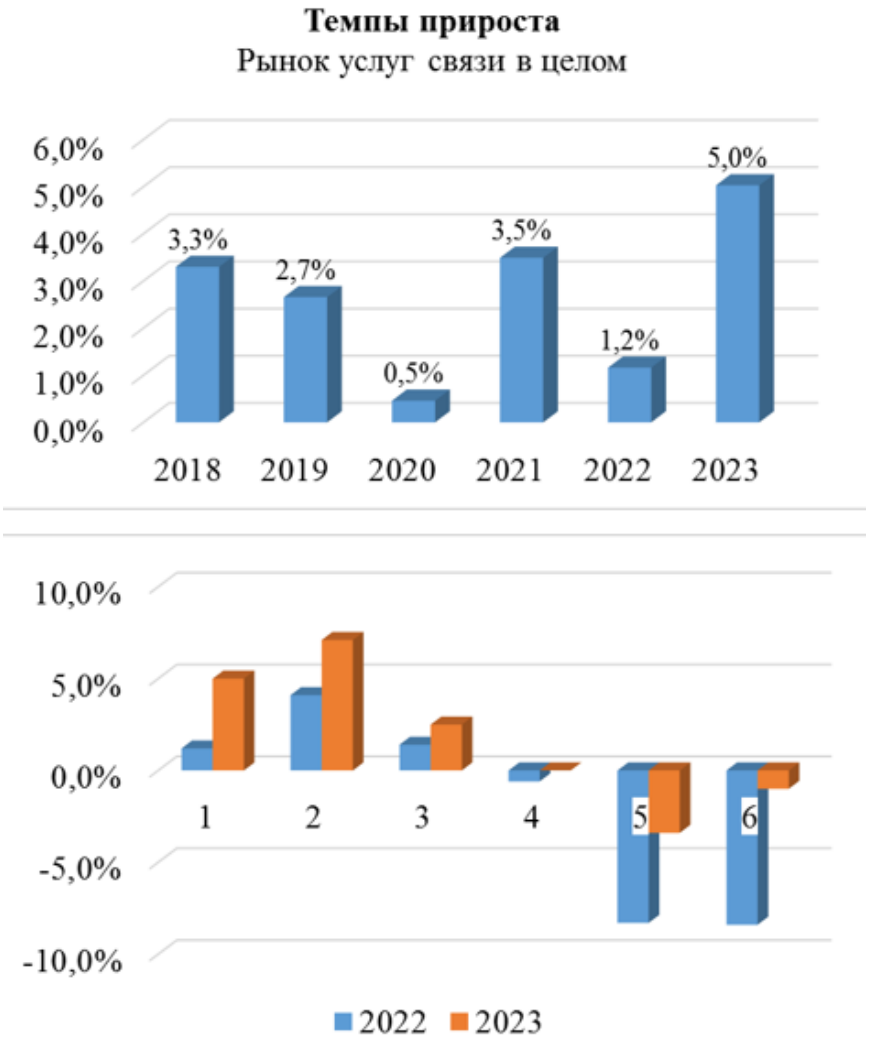
Рисунок 1

Источник: составлено авторами

Динамика развития рынка услуг связи в абсолютном выражении и темпах прироста по видам услуг связи, представленная на рис. 2, подтверждает положительный характер динамики за 2018-2023 гг. [4, 5].

В целом за год рынок услуг связи превысил объем в 1,9 млрд руб. и вырос на 5,1%. Это самая высокая динамика за последние 10 лет. Драйвером роста выступает рынок мобильной связи, доходы которой выросли на 7,1% и на который приходится 61% отраслевых доходов [4].

Количество пользователей, активно использующих *SIM*-карты для доступа к услугам мобильных операторов, увеличилось на 1,3% и достигло числа свыше 258 млн, при этом коэффициент распространенности мобильных устройств на душу населения превысил отметку в 176 устройств на каждые 100 жителей. Динамика роста доходов в сфере мобильной связи обусловлена не только повышением цен на телекоммуникационные услуги, но и увеличением объема потребления данных услуг. Особенно заметно увеличение интереса к мобильной связи со стороны корпоративных клиентов, а также восстановление активности в сегменте международного роуминга.



1 – Рынок услуг связи в целом; 2 – Мобильная связь; 3 – Интернет-доступ; 4 – Платное ТВ; 5 – Фиксированная телефония; 6 – Межоператорские услуги

Рисунок 2

Источник: составлено авторами

В сфере телекоммуникаций развиваются такие сегменты рынка, как широкополосный доступ в сеть (ШПД), фиксированная телефония, межоператорские услуги [4, 5]. Уровень проникновения ШПД на 2023 г. достиг 54%, при этом база абонентов увеличилась на 1,4%, а выручка выросла на 2,5%. Динамика роста числа абонентов достигается благодаря стратегии операторов по расширению сети в пригородные и загородные зоны городов, а также интеграции услуг в комплексные тарифные планы.

Из-за насыщения секторального рынка традиционными предложениями, рынок платного телевидения показал спад, отмеченный снижением количества абонентов на 0,1%, доходов – на 0,6%. Это происходит вследствие двух разнонаправленных факторов: с одной стороны, успешного развития платного сервиса видео-по-запросу и распространения партнерства с онлайн-кинотеатрами, с другой стороны - увеличение доли пользователей пакетов услуг. Доходы от фиксированной телефонной связи также сократились на 3,4% при снижении числа абонентов на 8,5% или на 1,5 млн.

На наш взгляд, в перспективе положительную динамику развития отраслевого рынка будет определять крупнейший сегмент мобильной связи с относительно высоким ростом выручки, а также развитие цифровых сервисов и

услуг со смещением в не телекоммуникационный сектор: медийные сервисы, ИТ-продукты и решения (облачные и *OTT*-сервисы, ЦОД, информационная безопасность, интернет вещей (*IoT*), видеонаблюдение и другие).

В аналитике важным инструментарием является структурный динамический анализ, позволяющий системно оценить сдвиги в рыночном пространстве в условиях динамичного изменения рыночной структуры [6].

Анализ структуры и перспектив развития рынка цифровых услуг и сервисов

В аналитике важным инструментарием является структурный динамический анализ, позволяющий системно оценить сдвиги в рыночном пространстве в условиях динамичного изменения рыночной структуры [6]. Поэтому нами систематизированы фактические и прогнозные данные о рынке услуг связи в разных сегментах: для физических лиц (*B*2*C*), корпоративных и государственных организациях (*B*2*B*/*G*) в 2022 г. (табл. 1 и 2).

Таблица 1.

Наименование компании	Мобильная связь	Фиксированный ШПД	Платное ТВ	*OTA*	*VoD*/*OTT*
ВымпелКом	10	6	3	-	10**
МегаФон	26	10	11+14= =25*	-	17***
МТС	34	10	10	23	23****
Ростелеком	10	39	38	69	11
Прочие	20	35	24	8	39

* Эр-Телеком, Триколор; ** *Okko*; ***-*IVI*; **** Кино-поиск

Источник: составлено авторами

Таблица 2.

Наименование компании	Мобильная связь	Фиксиро-ванный ШПД	*VNP*	*OTA*	Аренда каналов	Новая теле-фония
ВымпелКом	26	6	11	10	4	7
МегаФон	28	7*	7	-	7	6
МТС	31	10	4	12	7	22
Ростелеком	14	43	61	46	46	13
Прочие	1	34	17	32	36**	26= =8***+ +18****

* Эр-Телеком; ** ТТК; ***Манго-телеком; ****UISCom*.

Источник: составлено авторами

Прогнозируется, что к 2027 г. российский телеком рынок для абонентов – физических лиц продемонстрирует устойчивый рост с годовым приростом от 1 до 2%. Ведущие факторы развития включают мобильные сети, услуги платного телевидения и стриминговые сервисы фильмов и сериалов [7, 8].

Повышение доходов было достигнуто благодаря оптимизации состава абонентов и предложению тарифных планов с расширенным содержимым, а также интеграцией дополнительных цифровых сервисов. В свете устойчивого роста численности пользователей мобильного интернета, их возрастающие запросы на скорость подключения и способность обрабатывать значительные объемы данных

стимулируют операторов связи к техническому прогрессу и обеспечению превосходного качества обслуживания.

Не смотря на рост совокупного показателя *ARPU* (средней выручки на пользователя) происходит снижение числа абонентов из-за экспансии конвергентных услуг, объединяющих мобильную и фиксированную сети (*Fixed Mobile Convergence, FMC),* включая доступ в интернет по высокоскоростным каналам (ШПД), подписку на платное телевидение и использование стационарной телефонии. В сфере высокоскоростного интернета доминирующим фактором, стимулирующим рост, является строительство новых жилых комплексов. Что касается рынка платного телевидения, то рост предвидится исключительно в сегменте *IPTV*, так как его развитие напрямую связано с конкуренцией со стороны *OTT*-сервисов (*Over the Top* – технологии доставки контента через интернет без участия традиционных операторов связи) [7, 8].

Сектор онлайн-кинотеатров, демонстрирующий ежегодный рост на уровне 13% и представленный игроками вроде *Okko, IVI*, «КиноПоиск» и *Wink* от Ростелекома, является одним из наиболее динамично развивающихся направлений. Прогнозируется, что коэффициент проникновения услуг по подписке на *OTT*-контент достигнет отметки в 45% к 2030 г. благодаря ускоренному росту сегмента онлайн-кинотеатров в сочетании с распространением *Smart TV*. Такое развитие событий будет поддерживаться и трендом на интеграцию онлайн-платформ для просмотра фильмов в большие цифровые экосистемы, включая банковские услуги, операторов связи и другие цифровые службы.

Ожидается, что к 2027 г. объем рынка как традиционных, так и инновационных телекоммуникационных услуг, предоставляемых корпоративным клиентам и государственным учреждениям (*B2B* и государственный сегменты), достигнет 350 млрд рублей, демонстрируя ежегодный рост на уровне 4-5% (табл. 2). Уменьшение доли классических телекоммуникационных услуг будет взвешено за счет внедрения инновационных продуктов в области телекоммуникаций, включая обновленные телефонные услуги, номера 8-800, беспроводные *Wi-Fi* соединения и системы видеонаблюдения. Дополнительный положительный эффект для рынка создадут доходы от развивающихся сегментов добавленных услуг, таких как Интернет вещей (*IoT*), *SMS*-рассылки для корпоративных клиентов (*A2P SMS*) и прочие технологические инновации.

В домене классических коммуникационных сервисов завершена третья фаза государственной инициативы, направленной на интеграцию объектов социальной значимости в интернет-пространство. Реализация этого проекта способствует устойчивому прогрессу этого сектора через увеличение объема предложений виртуальных частных сетей (*VPN*), появление новых аспектов ценовой конкуренции, а также через рационализацию государственных и корпоративных расходов в рамках взаимодействия бизнеса с госсектором.

Экспансия новых рыночных сегментов, таких как виртуальные *ATC* (*BATC*) и *cloud-based* системы видеонаблюдения, будет стимулироваться активной региональной политикой и внедрением инновационных *BATC*-решений для масштабных и крупных предприятий, в том числе использованием речевой аналитики, систем отслеживания вызовов, голосовых ассистентов и прочих функциональных возможностей, прогнозируется увеличение на 11% ежегодно. Параллельно, рынок систем облачного видеонаблюдения ожидает рост на уровне 10% в год, благодаря реализации федеральной программы развития цифровой экономики, а также проектов «Умный город» и «Безопасный город», способствующих модернизации инфраструктуры с помощью передовых технологических решений в области умного видеонаблюдения и интеллектуальных транспортных систем на региональном уровне.

Основные факторы роста российского рынка облачных сервисов представлены на рис. 3.

Сектор облачных вычислений пребывает в стадии активного развития, при этом механизмы формирования спроса и предложения еще окончательно не сформированы. В частности, в области программного обеспечения как услуги (*Software as a Service – SaaS*) наблюдается значительная популярность и внедрение облачных решений. Предприятия стремятся минимизировать расходы на поддержку ИТ-инфраструктуры с помощью персонала и большие капиталовложения в покупку выделенного оборудования и лицензий на программное обеспечение.

Развитию этого сектора рынка способствует интенсивная работа над расширением государственных сервисов через облачные технологии и интеграцию федеральных и местных ведомств в общую облачную инфраструктуру, что подкрепляется планами по цифровизации функций этих организаций без необходимости создания их собственных ИТ-ресурсов. Это внедрение облаков в сфере *B2G* стимулирует их популярность также в секторе *B2B*, обеспечивая тем самым ускоренное развитие всего облачного рынка.

Рисунок 3

В современной индустрии цифровых технологий отрасль кибербезопасности занимает ключевую позицию. Доходы в этой сфере достигли порядка 103,4 млрд руб., где основные доли распределяются между разными сегментами рынка: корпоративный сектор заимствует 45%, государственные заказы – 27%, бизнес-клиенты – 23%, а раздел *B2C/SOHO* занимает 6%. В сегменте обращений от государства наблюдается устойчивое увеличение объемов на 10% ежегодно, при этом значительный вклад в этот рост вносят инвестиции федеральных органов власти в укрепление своей защищенности, которые составляют около 43%. Прогресс в развитии рынка кибербезопасности обусловлен активным поощрением со стороны государственных структур начиная с 2022 г., направленным на повышение уровня защиты информационных систем как в бизнесе, так и в правительственных организациях.

Драйверы роста рынка кибербезопасности представлены на рис. 4.

К факторам, способствующим развитию сектора кибербезопасности, можно отнести регуляторные инициативы на государственном уровне, например, принятие законодательных актов, направленных на укрепление защиты информационных систем в коммерческом секторе и государственных структурах, в частности указы Президента РФ № 250 от 1 мая и № 166 от 30 марта 2022 г. С другой стороны, к проблемам относится уменьшение инвестиций в область кибербезопасности со стороны малого и среднего бизнеса по причине предыдущих вложений в иностранные технологии и из-за доступности более дешевых отечественных продуктов, которые, однако, не всегда доступны по всему спектру требуемых услуг и часто уступают зарубежным по цене и качеству.

Рисунок 4

Источник: составлено авторами

Трансформация методов и принципов завоевания рынка цифровых услуг и сервисов

В последние десять лет развитие и всестороннее проникновение цифровых технологий оказались в авангарде прогресса, способствуя не только трансформации отдельных предприятий, но и целого рыночного пространства, увеличению аудитории цифровых платформ и модификации поведенческих моделей потребителей. Активная интеграция информационно-коммуникационных технологий (ИКТ), новаторские разработки в области цифровизации, повышение квалификации и переосмысление бизнес-моделей выступают в качестве драйвера и катализатора обширных изменений в операционной деятельности предприятий, их бизнес-процедурах и механизмах рынка с целью обеспечения их конкурентного преимущества, устойчивости в условиях меняющейся экономической среды и способствует формированию основ цифрового экономического порядка [9-22].

Развитие информационно-коммуникационных технологий (ИКТ) способствует созданию бизнес-интеграций и стратегических альянсов между организациями, включая те, что работают в телекоммуникационной отрасли и в областях, предоставляющих различные услуги. Это создание конвергентной бизнес-экосистемы дает возможность инкорпорировать предложения из других экономических секторов в комплекс инфокоммуникационных услуг, например, электронные платежные системы, дистанционные банковские услуги, удаленные

медицинские консультации, а также привлечь на рынок новых игроков, таких как поставщики контента, сервисные и системные интеграторы [3]. В то же время, определенные сектора экономики не только внедряют ИКТ для собственных производственных нужд, но и развивают собственные инфокоммуникационные сети, предлагая услуги связи напрямую своим потребителям [1-3].

Текущие динамики активно затрагивают сектор инфокоммуникаций, особенно компании, достигшие пика развития в предложении базовых услуг проводной и мобильной связи. Это создает необходимость в исследовании инновационных методов для повышения прибыльности и реформировании бизнес-стратегий. Данный процесс соответствует анализу Организации экономического сотрудничества и развития (ОЭСР) относительно ключевых направлений для развития цифровой экономики. Среди 20 основных целей, выделяются следующие приоритеты: улучшение предоставления государственных услуг через интернет, развитие инфраструктуры и компетенций в сфере информационно-коммуникационных технологий, повышение уровня кибербезопасности, а также разработка стратегий для адаптации предприятий к быстро меняющимся рыночным условиям через изменение форм и объемов деятельности [23-25].

Сегодня акцентируется внимание на технологии, играющие ключевую роль в цифровизации бизнес-процессов и рыночных условий:

- платформы и приложения для аналитики, функционирующие на основе технологий обработки больших данных (*Big Data*);
- приложения для мобильных устройств;
- платформы для разработки публичных сервисов, таких как *cloud computing*;
- инструментарий и приложения для работы с социальными медиа;
- интернет вещей (*IoT*), интеллектуальные сетевые и «умные» технологии [26, 27].

Эти инновационные цифровые инструменты глубоко трансформируют бизнес-модели телекоммуникационных компаний через внедрение новаторских цифровых услуг и сервисов, которые изменяют компоненты производственной деятельности (основные и вспомогательные процессы) в рамках цепи создания ценности. Это преобразует ключевые аспекты карты стратегического управления, включая финансовую стратегию, клиентоориентированность, оптимизацию бизнес-процессов, управление персоналом и интеграцию передовых технологий (рис. 5).

В эпоху цифровизации каждая часть организационной структуры подвергается изменениям, что приводит к необходимости трансформации каждого аспекта стратегии компании для повышения ее производительности [3]. Корректное переосмысление и обновление стратегической карты может привести к оптимизации расходов и повышению финансовой стабильности благодаря разработке новых методов увеличения дохода и прибыли через улучшение ключевой связи между производителем и потребителем в секторе информационных и коммуникационных технологий.

Функционирование в диджитал экосистеме и использование передовых технических решений для анализа *Big Data* и трендов на рынках, регулирующих спрос и предложение, акцентирует важность детального изучения предпочтений целевой аудитории и эффективного менеджмента. В этом контексте адаптация цифровых инноваций, превратившаяся из уникального конкурентного преимущества в основной фактор выживаемости и доминирования на рынке цифровых продуктов и услуг, становится императивом.

Основой для такого процесса трансформации служат все аспекты деятельности организации – от внутренних до внешних операций. Это включает в

себя развитие умений и цифровой грамотности персонала, формирование корпоративной идентичности, оптимизацию управленческой структуры и стимулирование инновационной активности.

Рисунок 5

Решение о выборе и адаптации новейших технологий должно основываться на всестороннем анализе их соответствия долгосрочной стратегии и текущим задачам бизнеса, а также включать оценку возможных рисков.

В нынешней динамичной экономической среде выделяются две ведущие стратегии цифровизации предприятий, которые радикально трансформируют организационные структуры и формируют основу для устойчивого конкурентного преимущества: подход, исходящий от инновационных технологических решений к определению бизнес-нужд, и стратегия, начинающаяся с выявления потребностей бизнеса для последующего поиска соответствующих технологических решений.

В начальной стадии цифровой трансформации, ключевую роль играет инновационное основание. Часто, в погоне за передовыми технологиями, игнорируются процессы сбора и анализа данных, при этом оценка эффективности внедряемых нововведений отстраняется на задний план. Тем не менее, достижение конкурентного преимущества через внедрение новаторских решений, которые способны повысить воспринимаемую ценность продукта или услуги для конечного пользователя, может обеспечить только временные успехи. Это связано с тем, что такой подход к стратегическому планированию не опирается на долгосрочную оценку результативности бизнеса.

Большинство компаний в секторе информационно-коммуникационных технологий отдает предпочтение стратегии, которая основывается на переходе от бизнес-потребностей к выбору соответствующих технологических решений. Этот подход начинается с тщательного изучения текущего состояния рынка, проведения оценки доступных ресурсов и формулировки целей, которых предприятие

стремится достичь. Выбор конкретных инновационных технологий обуславливается не столько внутренней организацией и существующей бизнес-моделью компании, сколько ориентацией на эффективное взаимодействие с клиентами и стремлением удовлетворить их потребности наилучшим образом.

Отсутствие общего подхода к формированию цифровой стратегии делается еще более сложным из-за динамически изменяющейся рыночной ситуации, уникальности бизнес-процессов в каждой организации и влияния корпоративной культуры. Это требует создания упорядоченной системы и регулярного обновления уже разработанных стратегических планов компании.

Применение передовых технологий в бизнес-процессы оказывает существенное влияние на всю отрасль, а также на операционную деятельность каждой компании в данном секторе. Аналитики из *BDG* убеждены, что внедрение таких технологий, как *IoT* (интернет вещей), *AI* (искусственный интеллект), трехмерное моделирование, робототехника и *AR* (технологии дополненной реальности), способствуют радикальному переосмыслению и оптимизации бизнес-моделей в различных секторах экономики (финансы, телекоммуникации, транспорт), путем автоматизации взаимодействий с клиентами, глубокого анализа их потребностей и разработки индивидуализированных предложений.

В эпоху цифровизации, где формируются инновационные рынки, продукция и сервисы, наблюдается значительное воздействие на определение потребительской стоимости. Важно, чтобы фирмы стратегически подходили к анализу возникающих цифровых потребностей, осознавали критические элементы как внешней, так и внутренней сферы цифрового производства и потребления. Это включает в себя интеграцию существующих компетенций в новые модели генерации прибыли через адаптацию к изменениям в спросе на цифровые продукты, сервисы и модели ценообразования.

В целях повышения спроса пользователей компании должны системно использовать следующие подходы:

- персонализированный подход к клиенту, который позволяет предложить ему персонифицированный набор сервисов, и тем самым повысить его удовлетворенность;
- омниканальный подход, который направлен на интеграцию офлайн-, онлайн- и мобильных процессов и обеспечивает сквозную идентификацию клиента и улучшает взаимодействие с ним;
- оптимизации цен, который учитывает внимание потребителя к ценообразованию и возможностям оптимизации цен за счет персональных предложений, бонусов, скидок;
- сокращения затрат, который отражает стремление потребителей к снижению расходов и приводит к росту популярности «пакетных» цифровых сервисов, включающих, например, наряду с телеком-услугами прокат электросамокатов и велосипедов.

Рост потребительского спроса на цифровые услуги и сервисы способствует развитию и повышению доходов компаний. Уровень платежеспособного спроса позволяет судить о степени удовлетворения потребностей пользователей в цифровых услугах и сервисах.

Заключение

На основе проведенного анализа развития рынка услуг связи по основным операторам и выявления структуры и перспектив развития рынка цифровых услуг и сервисов получены научно-практические выводы для совершенствования

методов и принципов завоевания рынка с учетом современной обстановки в России.

Анализ факторов роста российского рынка облачных сервисов и кибербезопасности подтвердил специфику принимаемых национальных и корпоративных решений по развитию рынка новых цифровых услуг и сервисов, обеспечивающих технологическую независимость страны и высокий уровень удовлетворения пользователей за счет учета их индивидуальных потребностей.

Литература

1. Кузовкова Т.А., Шаравова М.М., Алмаева О.П. Конвергентный характер стратегии цифровой трансформации инфокоммуникационных компаний // Экономика и качество систем связи, 2021. – № 3 (21). – С. 3-19.
2. Шаравова М.М. Выявление характера цифровой трансформации моделей инфокоммуникационного бизнеса // Экономика и качество систем связи, 2021. – № 1 (19). – С. 3-12.
3. Кузовкова Т.А., Алмаева О.П., Вольнов А.А., Шаравов И.М. Реализация сценариев использования технологий на базе сетей пятого поколения // В книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 47-й Международной конференции. Москва, 2021. – С. 30-33.
4. Итоги развития отрасли связи в 2033 г. / TMT Консалдинг. URL: https://www.content-review.com/articles/62934/ (дата обращения: 25.08.2024).
5. Как российские телеком-компании отчитались за 2023 год. URL: https://journal.tinkoff.ru/news/review-telecom-2023/ (дата обращения: 25.08.2024).
6. Кузовкова Т.А. Статистика цифрового развития и инфокоммуникаций: Учебник / Т. А. Кузовкова, Т. Ю. Салютина, О. И. Шаравова. – Москва: Ай Пи Ар Медиа, 2023. – 413 с.
7. J’son & Partners: интернет-доступ должен подешеветь в разы. URL: https://telecomdaily.ru/news/2021/01/25/j-son-partners-internet-dostup-dolzhen-podeshevet-v-razy (дата обращения: 25.08.2024).
8. Кузовкова Т.А., Салютина Т.Ю. Интегральная оценка состояния и потенциала развития инфокоммуникационной инфраструктуры в условиях цифровой экономики: Монография. – М.: ООО «ИД Медиа Паблишер», 2020. – 160 с.
9. Кузовкова Т.А., Кузовков Д.В., Шаравова О.И. Задачи и требования цифровой экономики к развитию инфокоммуникаций // Экономика и качество систем связи, 2019. – № 4 (14). – С. 20-28.
10. Кузовкова Т.А., Шаравова О.И., Кузовков Д.В. Закономерности развития цифровой экономики и базовые признаки нового технологического уклада // В книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) XLIII международной конференции РАЕН, 2019. – С. 33-37.
11. Кузовкова Т.А., Ву Д.Ф., Шаравова М.М., Шаравов И.М. Перспективы развития инфокоммуникаций в условиях реализации национальных проектов цифровой экономики // Технологии информационного общества. Сборник трудов XV Международной отраслевой научно-технической конференции «Технологии информационного общества», 2021. – С. 261-263.
12. Зайченко И.М., Горшечникова П.Д. Цифровая трансформация бизнеса: подходы и определение // Экономика и экологический менеджмент, 2020. – № 2. – С. 205-212.
13. Кузовкова Т.А., Иванов П.В., Смирнов А.А. Цифровая трансформация бизнеса на основе партнерских платформ и сервисных экосистем // Труды международной

НТК «Телекоммуникационные и вычислительные системы-2020». – М.: Горячая линия-Телеком, 2020. – С. 410-413.
14. Кузовкова Т.А., Кокленков М.А., Ткаченко Д.Н. Обоснование характера цифровой трансформации бизнеса и инфраструктуры инфокоммуникационных компаний // Телекоммуникации и информационные технологии, 2020. – № 2. – С. 145-151.
15. Кузовкова Т.А., Шаравова О.И., Шаравова М.М. Интегральный платформенный характер бизнес-моделей цифровых компаний // РИСК: Ресурсы, Информация, Снабжение, Конкуренция, 2021. – № 2. – С. 106-113.
16. Ценжарик М.К., Крылова Ю.В., Стешенко В.И. Цифровая трансформация компаний: стратегический анализ, факторы влияния и модели // Вестник Санкт-Петербургского университета. Экономика, 2020. – Т. 36. – В. 3. – С. 390-420.
17. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Статистическая информация РФ [Электронный ресурс]. URL: https://digital.gov.ru/ru/pages/statistika-otrasli/#section-720 (дата обращения: 25.08.2024).
18. Стратегия развития отрасли связи Российской Федерации на период до 2035 года. Утверждена распоряжением Правительства Российской Федерации от 24 ноября 2023 года № 3339-р. 2023. – 93 с.
19. Кузовкова Т.А., Шаравова О.И. Цифровая трансформация экономики: учебное пособие. – Москва: Ай Пи Ар Медиа, 2023. – 140 с.
20. Зараменских Е.П. Цифровые сервисы: их атрибуты и взаимосвязь с архитектурой предприятия // Вестник ГУУ. – 2018. – №10. URL: https://cyberleninka.ru/article/n/tsifrovye-servisy-ih-atributy-i-vzaimosvyaz-s-arhitekturoy-predpriyatiya (дата обращения: 25.08.2024).
21. Егина Н.А. Трансформация модели поведения потребителя в условиях цифровой экономики // Финансы и кредит, 2019. – Т. 25. – В. 9. – С. 1971-1986.
22. Вайл П. Цифровая трансформация бизнеса: Изменение бизнес-модели для организации нового поколения / Питер Вайл, Стефани Ворнер; перевод И. Окунькова. — Москва: Альпина Паблишер, 2019. – 264 с.
23. Годовой отчет ПАО «Ростелеком» за 2022 год. URL: https://www.company.rt.ru/ir/agm/files/2022/Annual_report_2022_rus.pdf (дата обращения: 25.08.2024).
24. Цифровая трансформация бизнеса на базе компании «ПАО Ростелеком» // Научный лидер, 2023. –№ 12 (110).
25. The 17 GOALS. Sustainable Development. United Nations. Department of Economic and Social Affairs Sustainable Development. URL: https://sdgs.un.org/goals (дата обращения: 25.08.2024).
26. Кузовкова Т.А., Шаравова О.И., Шаравова М.М. Интегральный платформенный характер бизнес-моделей цифровых компаний // РИСК: Ресурсы, Информация, Снабжение, Конкуренция, 2021. – № 2. – С. 106-113.
27. Кузовкова Т.А., Кузовков А.Д., Шаравов И.М. Понятие ценности цифровых платформ и методы оценки синергии их эффективности // Электронный научный журнал «Век качества», 2022. – № 3. – С.73-96.

СИСТЕМЫ, СЕТИ И УСТРОЙСТВА СВЯЗИ. РАДИОТЕХНИКА. АНТЕННЫ. ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА. ПРИБОРЫ И МЕТОДЫ ИЗМЕРЕНИЯ. МЕТРОЛОГИЯ

АНАЛИЗ ПРИМЕНИМОСТИ И СРАВНЕНИЕ ИЗВЕСТНЫХ МОДЕЛЕЙ РАСПРОСТРАНЕНИЯ РАДИОВОЛН С РЕЗУЛЬТАТАМИ РАДИОИЗМЕРЕНИЙ ТЕХНОЛОГИИ LoRa

А.А. Прасолов, *к.т.н., Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, prasolov.alex@gmail.com;*
А.С. Федоров, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, as.fdrv@bk.ru.*

УДК 621.391.81

Аннотация. Работа посвящена сравнению результатов радиоизмерений технологии *LoRa* с известными моделями распространения радиоволн. Измерения проводились в Санкт-Петербурге в различных диапазонах частот с учетом действующей на территории России нормативной базы. Приведены результаты радиоизмерений и их сравнение с расчетами, полученными с помощью моделей распространения радиоволн. Для каждой из рассматриваемых моделей приведено описание, их ограничения и математические выражения для расчета потерь в городской среде.

Ключевые слова: *LoRa;* радиоизмерения; покрытие; уровень принимаемого сигнала; отношение сигнал-шум; показатель потери пакетов; дальность связи; модели распространения радиоволн.

APPLICABILITY ANALYSIS AND COMPARISON OF KNOWN RADIO PROPAGATION MODELS WITH LoRa TECHNOLOGY RADIO MEASUREMENTS RESULTS

A.A. Prasolov, *Ph.D. of Engineering Sciences, St. Petersburg State University of Telecommunications n/a prof. M.A. Bonch-Bruevich;*
A.S. Fedorov, *St. Petersburg State University of Telecommunications n/a prof. M.A. Bonch-Bruevich.*

Annotation. The work is devoted to comparing the results of radio measurements of *LoRa* technology with known radio propagation models. Measurements were carried out in St. Petersburg in various frequency bands taking into account the Russian regulatory framework. The results of measurements are given and compared with calculations by radio propagation models. For each of the models under consideration, a description is given, their limitations and mathematical expressions for calculating losses in an urban environment.

Keywords: *LoRa*; radio measurements; coverage; received signal strength indicator; signal-to-noise ratio; packet loss ratio; communication range; radio propagation models.

Введение

Технология *LoRa* является одной из рекомендуемых технологий для построения узкополосных беспроводных сетей связи Интернета вещей на

территории Российской Федерации[1]. Для работы данная технология использует нелицензируемые участки спектра, определяемые и регулирующиеся на основе региональных ограничений (для стран Европы, как правило, это диапазоны 433 и 868 МГц). В России технология *LoRa* может эксплуатироваться в частотных диапазонах 864-865, 866-868, 868,7-869,2 МГц[2]. *LoRa Alliance* также выпустила документ с указанием региональных параметров, в том числе отдельный раздел «*RU*864-870», описывающий ограничения, действующие на территории России, в котором ширина канала технологии *LoRa* ограничена 125 кГц, а мощность излучения в восходящей и нисходящей линии не должна превышать 14 дБм [1].

Целью данной работы является проведение радиоизмерений технологии *LoRa* в условиях одного из районов города Санкт-Петербурга с учетом региональных ограничений, а также сравнение полученных результатов с теоретически рассчитанными показателями потерь и дальности связи по известным моделям распространения радиоволн (далее – *PPB*) с последующим анализом их применимости. Измерения и расчеты проводились как для диапазона 868 МГц, так и для диапазона 433 МГц.

Вопросы, связанные с радиоизмерениями технологии *LoRa,* на сегодняшний день являются актуальными и встречаются в отечественной и зарубежной научно-технической литературе. К примеру, в работах [2-13] представлены результаты радиоизмерений параметров технологии *LoRa*, проведенных как в России (Санкт-Петербург, Ленинградская область, Омск, Ижевск), так и в странах Европы (Финляндия, Италия, Франция, Германия), Южной Америки (Бразилия), Азии (Индонезия). В некоторых из указанных работ также рассматривается вопрос анализа применимости известных моделей распространения радиоволн и сравнение теоретических результатов расчетов дальности связи с полученными результатами радиоизмерений. На основании приведенных работ выделяется следующий набор параметров, необходимых для проведения измерений: уровень принимаемого сигнала (англ. *Received Signal Strength Indicator, RSSI*), отношение сигнал-шум (англ. *Signal-to-Noise Ratio, SNR*), а также показатель потери пакетов (англ. *Packet Loss Ratio, PLR*), либо показатель доставленных пакетов (англ. *Packet Delivery Ratio, PDR*). Также стоит отметить, что разработчик технологии *LoRa* (*Semtech Corporation*) предлагает использовать такой же набор параметров при проведении радиоизмерений, проводимых на базе специальных комплектов [14].

Модели распространения радиоволн, их применение и особенности

Модели распространения радиоволн (*PPB*) применяются при решении разнообразных задач, среди примеров которых можно назвать планирование сетей радиосвязи в системах автоматизированного проектирования (САПР) [15-16] и с помощью алгоритмов автоматического планирования [17], разработки методик модернизации сетей для повышения качества покрытия [18], оценки электромагнитной совместимости (ЭМС) [19] и электромагнитной безопасности [20].

Модели *PPB* позволяют оценить потери мощности сигнала в зависимости от расстояния между базовой и абонентской станциями (далее – БС и АС соответственно), типа среды распространения (в данной работе рассматривается только городская среда), рабочей частоты, высот расположения антенн БС и АС. Также, обладая информацией о параметрах передатчика (мощность излучения,

[1] Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 29 марта 2019 года № 113 «Об утверждении Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации».

[2] Решение Государственной комиссии по радиочастотам (ГКРЧ) от 7 мая 2007 года № 07-20.

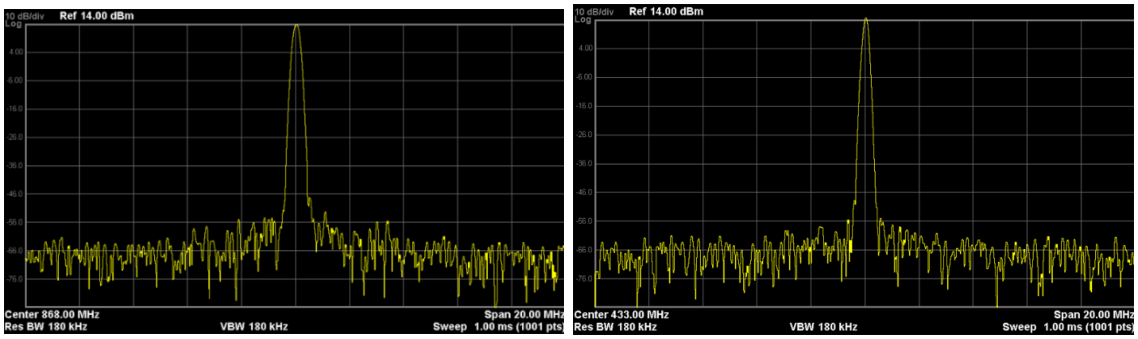
потери в АФТ, коэффициент усиления антенны) и приемника (коэффициент усиления антенны, потери в АФТ, чувствительность) и используя модели РРВ можно рассчитать, в том числе, теоретическую дальность связи и зону покрытия БС, исходя из соотношения (1):

$$P_{Tx} - L_{\text{АФТ}_{Tx}} + G_{Tx} - PL + G_{Rx} - L_{\text{АФТ}_{Rx}} = P_{Rx} \quad (1)$$

Выражение (1) включает в себя следующие параметры: мощность передатчика P_{Tx}, дБм; потери в антенно-фидерном тракте (далее – АФТ) передатчика $L_{\text{АФТ\_}Tx}$ и приемника $L_{\text{АФТ\_}Tx}$, дБ; коэффициенты усиления (далее – КУ) антенн передатчика G_{Tx} и приемника G_{Rx}, дБ; потери при распространении PL (от англ. *Path Loss*), дБ; уровень принимаемого сигнала P_{Rx}. Теоретическая дальность связи определяется расстоянием, при котором величина P_{Rx} становится равна чувствительности приемника.

Основными входными параметрами для расчета потерь при *PPB* служат рабочая частота f, расстояние между БС и АС R, высоты подвеса антенн БС и АС $h_{\text{БС}}$ и $h_{\text{АС}}$ соответственно. Далее при описании рассматриваемых моделей РРВ в математических выражениях будем пользоваться введенными обозначениями. Размерности входных параметров в моделях могут различаться, поэтому укажем их в квадратных скобках в качестве нижнего индекса у соответствующего коэффициента. Значения и размерности прочих коэффициентов, использующихся в рассматриваемых моделях, будут указаны после соответствующих математических выражений. Кроме того, каждая из моделей имеет ограничения по использованию, связанные с упомянутыми выше входными параметрами, что объясняется происхождением и разработкой данных моделей на основе множества проведенных измерений при различных условиях и статистической обработке их результатов.

В данной работе расчеты проводились в нисходящей линии связи (англ. *Downlink, DL*), соответственно, передатчиком выступала БС, антенна которого располагалась на высоте 30 м, приемником – АС, антенна которого располагалась на высоте 1,5 м. Мощность излучения БС для расчетов примем равной 14 дБм, чувствительность приемника – минус 136 дБм. КУ антенн передатчика и приемника примем равными 0 дБи, что соответствует случаю использования всенаправленных антенн.



а) б)

Рисунок 1

Параметры подобраны таким образом, чтобы результаты расчетов можно было сравнить с результатами радиоизмерений, процесс и результаты которых будут описаны и приведены в данной статье. Стоит отметить, что потерями в АФТ в рассматриваемом случае можно пренебречь, поскольку при проведении измерений мощность, подводимая к антенне передатчика, составляла 14 дБм, что

соответствовало выбранной мощности передатчика. Спектры сигналов передатчика в диапазонах 868 МГц и 433 МГц, полученные с помощью спектроанализатора, представлены на рисунках 1а и 1б соответственно.

Далее будут приведены описания известных моделей *PPB*, их ограничения по использованию и математические выражения, описывающие потери при распространении.

Модель Окамура

Модель Окамура основана на серии проведенных в городе Токио (Япония) измерений [21] и справедлива для диапазона частот от 150 до 1920 МГц, расстояния между БС и АС от 1 до 100 км, высот подвеса антенн БС и АС от 30 до 100 м и от 1 до 3 м соответственно. Потери при распространении определяются согласно выражению (2):

$$PL_{\text{Окамура}} = FSPL + A(f,R) - X_{\text{БС}} - X_{\text{АС}} - C \quad (2)$$

В выражении (2): *FSPL* – потери при распространении в свободном пространстве (англ. *Free-Space Path Loss*), определяется согласно выражению (3) [22], дБ:

$$FSPL = 10 \cdot lg\left(\frac{4 \cdot \pi \cdot R_{[\text{м}]}}{\lambda}\right)^2 = 20 \cdot lg\left(\frac{4 \cdot \pi \cdot R_{[\text{м}]} \cdot f_{[\text{Гц}]}}{c}\right) \quad (3)$$

В выражении (3): λ – длина волны, м; c – скорость света, равная $3 \cdot 10^8$ м/с.

Медианное затухание $A(f, R)$ и поправочный коэффициент местности C в выражении (2) определяются в соответствии с графическими зависимостями, представленными в первоисточнике модели [21]. Поправочные коэффициенты, учитывающие высоты расположения антенн БС и АС (в случае, если антенна АС расположена ниже высоты в 3 м), определяются согласно выражениям (4) и (5) соответственно:

$$X_{\text{БС}} = 20 \cdot lg\left(\frac{h_{\text{БС}_{[\text{м}]}}}{200}\right) \quad (4)$$

$$X_{\text{АС}} = 10 \cdot lg\left(\frac{h_{\text{АС}_{[\text{м}]}}}{3}\right) \quad (5)$$

Модель Окамура-Хата

Модель Окамура-Хата (она же модель Хата в ряде источников [23]) основана на модели Окамуры, являясь ее адаптацией, представляющей графические зависимости поправочных коэффициентов в виде эмпирических выражений [24], и справедлива для диапазона частот от 150 МГц до 1,5 ГГц, расстояния между БС и АС от 1 до 100 км, высот подвеса антенн БС и АС от 30 до 200 м и от 1 до 10 м соответственно. Потери при распространении в городской среде определяются согласно выражению (6):

$$\begin{aligned} PL_{\text{Окамура}-\text{Хата}} = {} & 69{,}55 + 26{,}16 \cdot lg\left(f_{[\text{МГц}]}\right) - 13{,}82 \cdot lg\left(h_{\text{БС}_{[\text{м}]}}\right) - a_{\text{АС}} + \\ & + \left(44{,}9 - 6{,}55 \cdot lg\left(h_{\text{БС}_{[\text{м}]}}\right)\right) \cdot lg\left(R_{[\text{км}]}\right) \end{aligned} \quad (6)$$

В выражении (2): $\alpha_{\text{АС}}$ – поправочный коэффициент, учитывающий высоту расположения антенны АС, для городской среды и диапазона частот свыше 400 МГц определяется согласно выражению (7):

$$a_{\text{АС}} = 3{,}2 \cdot \left(lg\left(11{,}75 \cdot h_{\text{АС}_{[\text{м}]}}\right)\right)^2 - 4{,}97 \quad (7)$$

Модель *COST*-231-Хата

Модель *COST*-231-Хата (англ. *Cooperation for Scientific and Technical Research*) основана на модели Окамура-Хата, являясь ее расширением для частотного диапазона от 1,5 ГГц до 2 ГГц [25], однако в научно-технической литературе (например, в работе [26]) под расширением частотного диапазона иногда понимается расширение верхней границы и, соответственно, применение модели для частотного диапазона от 150 МГц до 2 ГГц. Модель справедлива для расстояния между БС и АС от 1 до 20 км, высот подвеса антенн БС и АС от 30 до 200 м и от 1 до 10 м соответственно. Потери при распространении определяются согласно выражению (8):

$$\begin{gathered} PL_{COST-231-\text{Хата}} = 46{,}3 + 33{,}9 \cdot lg\left(f_{[\text{МГц}]}\right) - 13{,}82 \cdot \lg\left(h_{\text{БС}_{[\text{м}]}}\right) - a_{\text{АС}} + \\ + \left(44{,}9 - 6{,}55 \cdot \lg\left(h_{\text{БС}_{[\text{м}]}}\right)\right) \cdot \lg\left(R_{[\text{км}]}\right) + C \end{gathered} \quad (8)$$

В выражении (8): $\alpha_{\text{АС}}$ – поправочный коэффициент, определяемый согласно выражению (7); C – поправочный коэффициент, учитывающий застройку местности (для города принимается равным 3), дБ.

Модель Ирбид

Модель Ирбид основана на модели *COST*-231-Хата и является ее адаптацией, основанной на измерениях, проведенных в г. Ирбид (Иордания) [27]. Измерения проводились вблизи частоты 1800 МГц. В первоисточнике не приведены ограничения, противоречащие ограничениям оригинальной модели COST-231-Хата, поэтому их можно считать теми же. Потери при распространении определяются согласно выражению (9):

$$\begin{gathered} PL_{\text{Ирбид}} = 54{,}27 + 33{,}9 \cdot lg\left(f_{[\text{МГц}]}\right) - 13{,}82 \cdot lg\left(h_{\text{БС}_{[\text{м}]}}\right) - a_{\text{АС}} \\ + \left(44{,}9 - 6{,}55 \cdot lg\left(h_{\text{БС}_{[\text{м}]}}\right)\right) \cdot lg\left(R_{[\text{км}]}\right) \end{gathered} \quad (9)$$

В выражении (9): $\alpha_{\text{АС}}$ – поправочный коэффициент, определяется согласно выражению (7).

Также стоит отметить, что в научно-технической литературе описан ряд других вариантов адаптации модели *COST*-231-Хата (например, в работах [28] и [29]), однако в данной работе они не рассматриваются по причине несоответствия условиям их применимости, а именно по частотному диапазону.

Модель *CCIR*

Модель *CCIR* (англ. *Consultative Committee of International Radio*) основана на модели Окамура-Хата, однако ее отличительной особенностью является наличие поправочного коэффициента учета застройки местности [30]. Модель справедлива для диапазона частот от 150 МГц до 1 ГГц, расстояния между БС и АС от 1 до 20 км, высот подвеса антенн БС и АС от 30 до 200 м и от 1 до 10 м

соответственно. Потери при распространении определяются согласно выражению (10):

$$PL_{CCIR} = PL_{\text{Окамура–Хата}} - 30 + 25 \cdot lg\ (B) \quad (10)$$

В выражении (10): $PL_{\text{Окамура-Хата}}$ – потери при *PPB*, рассчитанные в соответствии с выражением (6), дБ; B – коэффициент, представляющий собой отношение площади местности, застроенной зданиями, к общей площади рассматриваемой местности (для расчетов было выбрано усредненное значение коэффициента, равное 50), %.

Модель *Ericsson* 9999

Модель *Ericsson* 9999 основана на модели Окамура-Хата, являясь ее расширением для частотного диапазона от 150 МГц до 3 ГГц [31] и справедлива для расстояния между БС и АС от 1 до 100 км, высот подвеса антенн БС и АС от 30 до 200 м и от 1 до 10 м соответственно. Потери при распространении в городской среде определяются согласно выражению (11):

$$\begin{aligned} PL_{Ericsson\ 9999} = {} & a_0 + a_1 \cdot lg\left(R_{[\text{км}]}\right) + a_2 \cdot lg\left(h_{\text{БС}_{[\text{м}]}}\right) + a_3 \\ & \cdot lg\left(h_{\text{БС}_{[\text{м}]}}\right) \cdot lg\left(R_{[\text{км}]}\right) - 3{,}2 \cdot \lg\left(11{,}75 \cdot h_{\text{АС}_{[\text{м}]}}\right)^2 + 44{,}49 \\ & \cdot lg\left(f_{[\text{МГц}]}\right) - 4{,}78 \cdot lg\ (f_{[\text{МГц}]})^2 \end{aligned} \quad (11)$$

В выражении (11): a_0, a_1, a_2, a_3 – набор поправочных коэффициентов, зависящих от типа местности (для городской среды принимаются равными 36,2; 30,2; 12; 0,1 соответственно [32]).

Модель Хата-Дэвидсон

Модель Хата-Дэвидсон [33] основана на модели Окамура-Хата и справедлива для частотного диапазона от 30 МГц до 1,5 ГГц, расстояния между БС и АС от 1 до 300 км, высот подвеса антенн БС и АС от 20 до 2500 м и от 1 до 10 м соответственно. Потери при распространении в городской среде определяются согласно выражению (12) [34]:

$$PL_{\text{Хата–Дэвидсон}} = PL_{\text{Окамура–Хата}} + A - S_1 - S_2 - S_3 - S_4 \quad (12)$$

В выражении (11): $PL_{\text{Окамура-Хата}}$ – потери при PPB, рассчитанные в соответствии с выражением (6), дБ; A – поправочный коэффициент, учитывающий расстояние между БС и АС, а также высоту подвеса антенны БС (при расстоянии менее 20 км принимается равным нулю); S_1 – поправочный коэффициент, учитывающий расстояние между БС и АС (при расстоянии менее 20 км принимается равным нулю); S_2 – поправочный коэффициент, учитывающий расстояние между БС и АС, а также высоту подвеса антенны БС (при высоте подвеса антенны БС менее 300 м принимается равным нулю); S_3 – поправочный коэффициент, учитывающий частоту, определяется в соответствии с выражением (13); S_4 – поправочный коэффициент, учитывающий частоту и расстояние между БС и АС (при расстоянии менее 64,38 км принимается равным нулю) [35].

$$S_3 = \frac{f}{250} \cdot lg\ \left(\frac{1500}{f}\right) \quad (13)$$

Модель Илорин

Модель Илорин основана на модели Хата-Дэвидсон и является ее адаптацией, основанной на измерениях, проведенных в г. Илорин (Нигерия) [36]. В первоисточнике не приведены ограничения, противоречащие ограничениям оригинальной модели Хата-Дэвидсон, поэтому их можно считать теми же. Потери при распространении определяются согласно выражению (14) [37]:

$$PL_{\text{Илорин}} = 73{,}56 + 26{,}16 \cdot lg\left(f_{[\text{МГц}]}\right) - 13{,}82 \cdot lg\left(h_{\text{БС}_{[\text{м}]}}\right) - a_{\text{АС}} + \\ +30{,}5 \cdot lg\left(R_{[\text{км}]}\right) + A - S_1 - S_2 - S_3 - S_4 \quad (14)$$

В выражении (14): $\alpha_{\text{АС}}$ – поправочный коэффициент, определяется согласно выражению (6); A, S_1, S_2, S_3, S_4 – набор поправочных коэффициентов, определяемых согласно модели Хата-Дэвидсон, в том числе и выражением (12).

Модель *ECC*-33

Модель *ECC*-33 (англ. *Electronic Communications Committee*) (она же расширенная или модифицированная модель Окамура-Хата в ряде источников [38]) является адаптацией модели Окамура-Хата для Европы и справедлива для частотного диапазона от 30 МГц до 3 ГГц, расстояния между БС и АС от 40 м до 100 км, высот подвеса антенн БС и АС от 30 до 200 м и от 1 до 3 м соответственно. Потери при распространении в городской среде определяются согласно выражению (15) [39]:

$$PL_{ECC-33} = FSPL + 20{,}41 + 9{,}83 \cdot lg\left(R_{[\text{км}]}\right) + 7{,}89 \cdot lg\left(f_{[\text{ГГц}]}\right) + 9{,}56 \\ \cdot \left(lg\left(f_{[\text{ГГц}]}\right)\right)^2 - X_{\text{БС}} - X_{\text{АС}} \quad (15)$$

В выражении (16): *FSPL* – потери при распространении в свободном пространстве, определяются согласно выражению (2), дБ; $X_{\text{БС}}$ – поправочный коэффициент, учитывающий высоту подвеса антенны БС и расстояние между БС и АС, определяется согласно выражению (16), дБ; $X_{\text{АС}}$ – поправочный коэффициент, учитывающий высоту подвеса антенны АС и для городской среды, определяется согласно выражению (17), дБ.

$$X_{\text{БС}} = lg\left(\frac{h_{\text{БС}_{[\text{м}]}}}{200}\right) \cdot \left(13{,}958 + 5{,}8 \cdot lg\left(R_{[\text{км}]}\right)^2\right) \quad (16)$$

$$X_{\text{АС}} = 0{,}759 \cdot h_{\text{АС}_{[\text{м}]}} - 1{,}862 \quad (17)$$

Модель *SUI*

Модель *SUI* (англ. *Stanford University Interim*) основана на серии измерений, проведенных на частоте 1,9 ГГц [40], и справедлива для частотного диапазона вплоть до 3,5 ГГц и расстояния между БС и АС от 100 м до 8 км, высот подвеса антенн БС и АС от 10 до 80 м и от 2 до 10 м соответственно [41]. Потери при распространении в городской среде определяются согласно выражению (18) [33]:

$$PL_{SUI} = FSPL + 10 \cdot \gamma \cdot lg\left(\frac{R_{[\text{м}]}}{d_0}\right) + X_f + X_{\text{АС}} + X_\sigma \quad (18)$$

В выражении (18): *FSPL* – потери при распространении в свободном пространстве, определяются согласно выражению (3), с той разницей, что определяются на расстоянии d_0, дБ; d_0 – нормирующее расстояние, равное 100

метров; γ – поправочный коэффициент, учитывающий тип местности и высоту подвеса антенны БС, определяется согласно выражению (19); X_f – поправочный коэффициент, учитывающий частоту, определяется в соответствии с выражением (20); $X_{\text{АС}}$ – поправочный коэффициент, учитывающий высоту подвеса антенны АС, определяется в соответствии с выражением (21); X_σ – поправочный коэффициент, учитывающий тип местности (для городской среды, указанной в модели как местность типа А, принимается равным 10,6 дБ [33]).

$$\gamma = a - b \cdot h_{\text{БС}_{[\text{м}]}} + \frac{c}{h_{\text{БС}_{[\text{м}]}}} \tag{19}$$

В выражении (19): a, b, c – набор поправочных коэффициентов, зависящих от типа местности (для городской среды принимаются равными 4,6; 0,0065; 12,6 соответственно [33]).

$$X_f = 6 \cdot lg\left(\frac{f_{[\text{ГГц}]}}{2000}\right) \tag{20}$$

$$X_{\text{АС}} = -10{,}8 \cdot lg\left(\frac{h_{\text{АС}_{[\text{м}]}}}{2}\right) \tag{21}$$

Модель Ли

Модель Ли основана на серии проведенных в США измерений на частоте 900 МГц [43]. Модель справедлива для диапазона частот от 30 МГц до 2 ГГц, расстояния между БС и АС от 2 до 30 км. Потери при распространении определяются согласно выражению (22) [44]:

$$PL_{\text{Ли}} = L_0 + \gamma \cdot lg\left(R_{[\text{км}]}\right) - 10 \cdot lg\,(F_0) \tag{22}$$

В выражении (23): L_0 и γ – экспериментально полученные на основе серии измерений эталонные потери и затухание на декаду (в данной работе для расчетов приняты равными 124 и 30,5, что соответствует г. Токио (Япония), застройка которого взята для примера [44]), дБ; F_0 – набор поправочных коэффициентов, определяется в соответствии с выражением (23):

$$F_0 = \prod_{i=1}^{5} F_i = \left(\frac{h_{\text{БС}_{[\text{м}]}}}{30{,}48}\right)^2 \cdot \left(\frac{G_{\text{БС}}}{4}\right) \cdot \left(\frac{h_{\text{АС}_{[\text{м}]}}}{3}\right)^{\upsilon} \cdot \left(\frac{f_{[\text{МГц}]}}{900}\right)^{-n} \cdot G_{\text{АС}} \tag{23}$$

В выражении (23): ν – показатель степени, учитывающий высоту подвеса антенны АС (для высоты антенны АС менее 3 м принимается равным 1); n – показатель степени, учитывающий частотный диапазон (принимается равным 2 или 3 при рабочей частоте ниже и выше 450 МГц соответственно); $G_{\text{БС}}$ и $G_{\text{АС}}$ – КУ антенн БС и АС соответственно (поскольку использовались ненаправленные антенны, то они имеют КУ, равные -2,15 дБд, что соответствует 0 дБи в логарифмическом масштабе и 0,61 в линейном).

Модель Эгли

Модель Эгли основана на серии проведенных в США измерений [45] и справедлива для частотного диапазона от 40 МГц до 1 ГГц [38]. Потери при распространении определяются согласно выражению (24) [45]:

$$PL_{\text{Эгли}} = -10 \cdot lg\left(0{,}345 \cdot \left(\frac{40 \cdot h_{\text{БС}_{[\text{м}]}} \cdot h_{\text{АС}_{[\text{м}]}}}{f_{[\text{МГц}]} \cdot {R_{[\text{м}]}}^2}\right)^2\right) \quad (24)$$

Модель Ибрагим-Парсонс

Модель Ибрагим-Парсонс основана на серии проведенных в г. Лондон (Великобритания) измерений [46] и справедлива для частотного диапазона от 150 МГц до 1 ГГц, расстояния между БС и АС до 10 км, высот подвеса антенн БС и АС от 30 до 300 м и до 3 м соответственно [47]. Потери при распространении представлены в двух вариантах и определяются согласно выражениям (25) и (26) [46]:

$$\begin{aligned} PL_{\text{Ибрагим}-\text{Парсонс (вариант 1)}} &= -20 \cdot lg\left(0{,}7 \cdot h_{\text{БС}_{[\text{м}]}}\right) - 8 \cdot lg\left(h_{\text{АС}_{[\text{м}]}}\right) + \frac{f_{[\text{МГц}]}}{40} + \\ &+ 26 \cdot lg\left(\frac{f_{[\text{МГц}]}}{40}\right) - 86 \cdot lg\left(\frac{f_{[\text{МГц}]} + 100}{156}\right) \\ &+ \left(40 + 14{,}15 \cdot lg\left(\frac{f_{[\text{МГц}]} + 100}{156}\right)\right) \cdot \\ &\cdot lg\left(R_{[\text{м}]}\right) + 0{,}265 \cdot L - 0{,}37 \cdot H + 0{,}087 \cdot U - 5{,}5 \end{aligned} \quad (25)$$

$$\begin{aligned} PL_{\text{Ибрагим}-\text{Парсонс (вариант 2)}} &= 40 \cdot lg\left(R_{[\text{м}]}\right) - 20 \cdot lg\left(h_{\text{БС}_{[\text{м}]}} \cdot h_{\text{АС}_{[\text{м}]}}\right) + 20 + \frac{f_{[\text{МГц}]}}{40} + \\ &+ 0{,}18 \cdot L - 0{,}34 \cdot H + 0{,}094 \cdot U - 5{,}9 \end{aligned} \quad (26)$$

В выражениях (25) и (26): L – коэффициент застройки местности (для типичной городской застройки принимается равным 50), %; U – коэффициент, учитывающий долю зданий этажностью выше 3 (для типичной городской застройки принимается равным 63,2 [48]), %; H – разница высот подвеса антенн БС и АС, м.

Радиоизмерения параметров технологии *LoRa*

Измерения проводились с помощью платформы *HelTec Automation LoRa* 32 *v*2, построенной на базе системы на кристалле *ESP*32 и приемопередатчиков стандарта *LoRa* семейства *SX*127*x* (*SX*1276 и *SX*1278 для диапазонов 868 МГц и 433 МГц соответственно) [49]. Данные приемопередатчики поддерживают рассматриваемые в данной работе частотные диапазоны (868 МГц и 433 МГц), SF от 7 до 12, мощность излучения до 20 дБм, ширину канала до 500 кГц, а также уровень чувствительности вплоть до минус 148 дБм [50]. Один модуль использовался в качестве передатчика, второй – в качестве приемника. Внешний вид описанных выше модулей с подключенной ненаправленной антенной представлен на рис. 2.

Рисунок 2

Измерения проводились в Санкт-Петербурге в окрестностях СПбГУТ им. проф. М.А. Бонч-Бруевича в точках, пронумерованных от «*Rx*1» до «*Rx*35» и отмеченных на рис. 3.

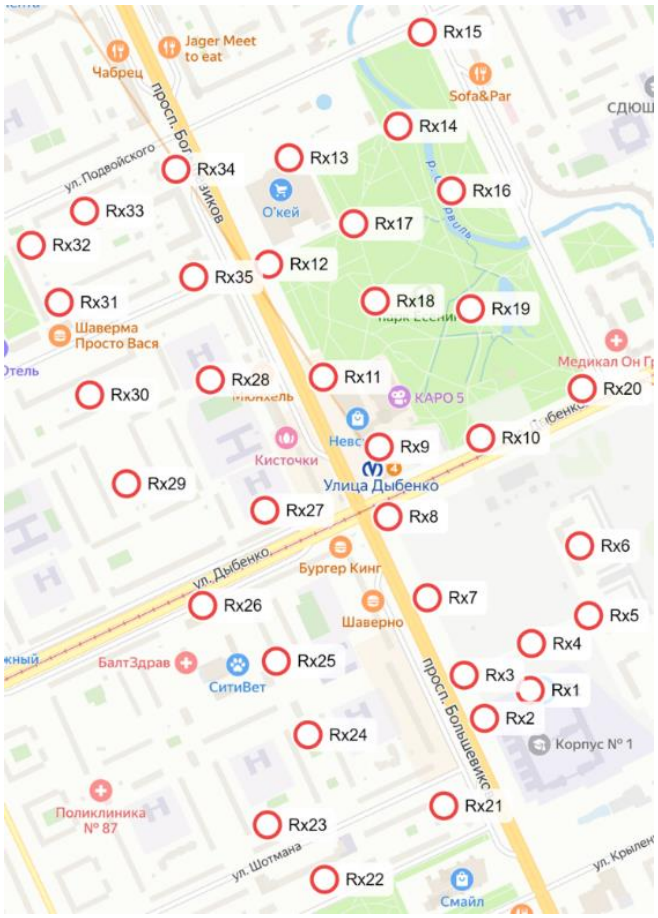


Рисунок 3

В данных точках располагался приемник, ненаправленная антенна которого располагалась на высоте 1,5 м. Ненаправленная антенна передатчика (отмечен на рисунке 3, как «*Tx*», практически совпадает с точкой «*Rx*1») была расположена на высоте 30 м. Мощность передатчика составляла 14 дБм, ширина канала – 125 кГц, что соответствует упомянутым выше региональным ограничениям. Скорость кода и *SF* были установлены равными 4/8 и 12 соответственно, и подобраны таким образом, чтобы обеспечить максимальную помехоустойчивость (в теории обеспечивается максимальная дальность связи и минимальная скорость передачи данных).

Измерения проводились следующим образом. Со стороны передатчика с указанными выше параметрами циклически передавались пакеты данных, полезной нагрузкой которых служили номера этих пакетов (от 1 до 100). Для

каждого пришедшего пакета оценивался уровень принимаемого сигнала (англ. *Received Signal Strength Indicator, RSSI*), дБм, и отношение сигнал-шум (англ. *Signal-to-Noise Ratio, SNR*), дБ. В каждой из точек маршрута данные показатели усреднялись по итогу приема переданных пакетов. Кроме того, оценивался показатель потери пакетов (англ. *Packet Loss Ratio, PLR*), %, представляющий из себя отношение числа потерянных пакетов к общему числу переданных пакетов. Оценивался данный показатель с помощью алгоритма, реализованного в программном обеспечении передатчика. При приеме очередного пакета данных алгоритм сравнивает его номер (заложенный в полезной нагрузке) с ожидаемым номером пакета. Ожидаемый номер пакета определяется исходя из предыдущего успешно принятого пакета. В случае, если номер принятого пакета не равен номеру ожидаемого пакета (что отражает случай, когда один или несколько пакетов не были доставлены), показатель потери пакетов инкрементируется до тех пор, пока ожидаемый номер пакета и номер принятого пакета не совпадут.

Результаты проведенных радиоизмерений в точках, отмеченных на рисунке 3, а также расстояния до этих точек приведены в таблице 1. Знаком «×» обозначены точки, в которых отсутствовал прием сигнала, и, соответственно, показатель потери пакетов в данных точках принимается равным 100 процентов.

Таблица 1.

Точка	Расстояние до точки, км	Диапазон 868 МГц			Диапазон 433 МГц		
		RSSI, дБм	*SNR*, дБ	*PLR*, %	*RSSI*, дБм	*SNR*, дБ	*PLR*, %
*Rx*1	0,023	-92	9	0	-86	11	0
*Rx*2	0,122	-110	7	2	-110	3	1
*Rx*3	0,150	-104	8	0	-106	6	1
*Rx*4	0,090	-108	9	0	-104	8	0
*Rx*5	0,166	-115	6	0	-100	9	0
*Rx*6	0,282	-125	-5	16	-115	-2	2
*Rx*7	0,280	-113	4	0	-106	7	1
*Rx*8	0,440	-118	0	0	-118	-6	6
*Rx*9	0,555	-120	0	0	-122	-9	2
*Rx*10	0,490	-113	7	3	-110	3	1
*Rx*11	0,720	-118	0	7	-126	-15	24
*Rx*12	0,956	-123	-4	7	-123	-10	0
*Rx*13	1,120	-130	-10	6	-126	-14	9
*Rx*14	1,100	-126	-6	0	-127	-19	86
*Rx*15	1,270	-135	-14	19	-129	-16	68
*Rx*16	0,960	-137	-15	52	-121	-8	0
*Rx*17	0,950	-125	-5	0	-128	-15	40
*Rx*18	0,800	-115	5	0	-120	-7	0
*Rx*19	0,730	-118	5	0	-126	-13	33
*Rx*20	0,573	-124	-4	0	-116	-4	0
*Rx*21	0,287	-132	-18	93	-129	-16	91
*Rx*22	0,546	×	×	100	×	×	100
*Rx*23	0,560	×	×	100	×	×	100
*Rx*24	0,450	-139	-17	98	-130	-17	94
*Rx*25	0,504	-128	-8	6	-129	-16	95
*Rx*26	0,660	-129	-8	17	-129	-16	87
*Rx*27	0,625	-125	-4	7	-125	-12	3
*Rx*28	0,860	×	×	100	-130	-16	70
*Rx*29	0,878	×	×	100	×	×	100
*Rx*30	1,020	-137	-13	16	-123	-18	99
*Rx*31	1,170	×	×	100	×	×	100
*Rx*32	1,280	×	×	100	×	×	100
*Rx*33	1,250	×	×	100	×	×	100
*Rx*34	1,200	-124	-5	0	-126	-13	1
*Rx*35	1,020	-119	-1	9	-125	-12	1

По итогу измерений в диапазоне 868 МГц сигнал отсутствовал в семи точках, в диапазоне 433 МГц – в шести точках. Максимальная дальность связи для обоих диапазонов составила приблизительно 1,3 км.

Сравнение результатов расчетов и результатов измерений

На рис. 4 представлены результаты расчетов по описанным выше моделям *PPB*, а также нанесенные в виде маркеров результаты радиоизмерений и чувствительность приемника, что позволяет сравнить теоретические и практические результаты.

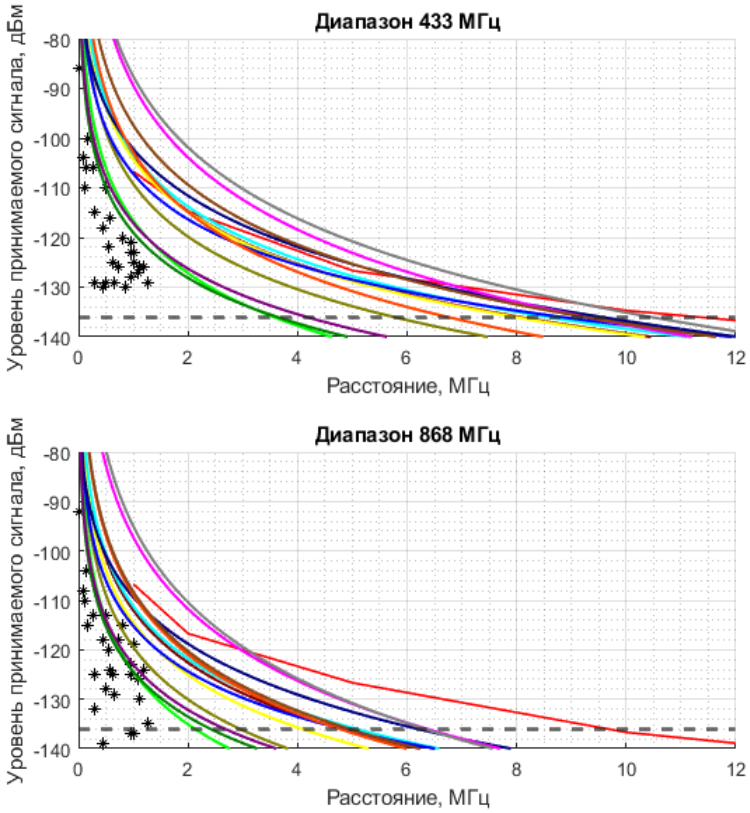


Рисунок 4

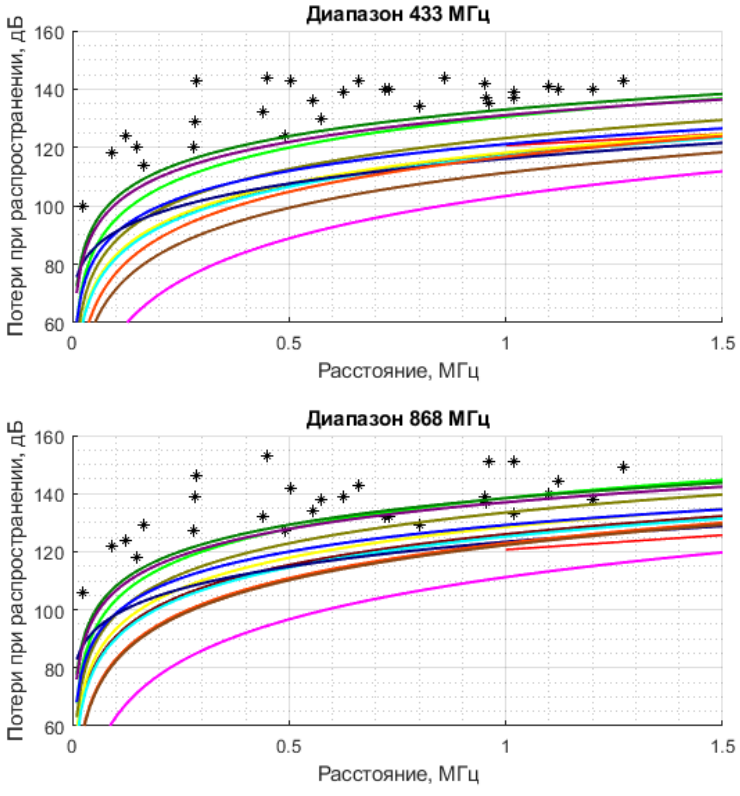


Рисунок 5

Используемая на рис. 4 и 5 легенда приведена на рис. 6.

Рисунок 6

Заключение

Таким образом, наиболее близкие результаты расчета дальности связи по сравнению с проведенными измерениями для диапазона 868 МГц показали модели *CCIR* (2,1 км), *Ericsson* 9999 (2,4 км), Ли (2,7 км). Данные модели, а также модель Ирбид в меньшей степени, частично совпали с результатами измерений на меньших расстояниях, что можно заметить на рис. 3. Для диапазона 433 МГц результаты расчета дальности связи значительно превысили практический результат (по наиболее близким моделям *CCIR* и *Ericsson* 9999 дальность связи составила 3,5 км), однако на меньших расстояниях наиболее близкими по характеру зависимостей можно назвать те же модели *CCIR, Ericsson* 9999 и Ли.

Расхождения рассмотренных моделей с результатами измерений могут быть вызваны разными типами застройки городов и ландшафтными условиями, в которых проводились измерения при разработке моделей, устаревшими поправочными коэффициентами, поскольку большая часть моделей была разработана во второй половине *XX* века и начале *XXI* века. Кроме того, рассмотренные модели не учитывают помеховую обстановку, что может влиять на зону покрытия, в особенности для систем связи, работающих при отрицательном отношении сигнал-шум, которой *LoRa* и является, а также многолучевое распространение сигнала.

Дальнейшим направлением исследований может стать разработка собственной модели *PPB*, которая может быть, как гибридной моделью (например, на базе моделей *CCIR, Ericsson* 9999 и Ли, подобная модель описана в работе [51]), так и моделью, учитывающей больше количество параметров конкретной системы связи (в случае с технологией *LoRa* можно также учитывать такие параметры, как SF, скорость кода, ширина канала).

Научная статья подготовлена в рамках прикладных научных исследований СПбГУТ, регистрационный номер 1023031600087-9-2.2.4;2.2.5;2.2.6;1.2.1;2.2.3 в ЕГИСУ НИОКТР.

Литература

1. RP002-1.0.3 LoRaWAN Regional Parameters // LoRa Alliance. URL: https://lora-alliance.org/resourcehub/rp2-1-0-3-lorawan-regional-parameters/ (дата обращения: 26.03.2024).
2. Андреев Р.А., Прасолов А.А., Федоров А.С. Исследование дальности связи технологии LoRa в условиях мегаполиса // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т, 2021. – Т. 3. – С. 21-27.
3. Андреев Р.А., Прасолов А.А., Федоров А.С. Анализ применимости известных моделей распространения радиоволн для технологии LoRa // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т, 2022. – Т. 3. – С. 13-17.
4. Седунов Д.П., Жунусова А.С., Зырянова Ю.О. Расчет параметров системы беспроводного сбора данных сети LoRaWAN // Техника радиосвязи, 2021. – № 2. – С. 31-41.
5. Суслов К.Н., Варнаков С.А. Исследование применимости технологии LoRa с учетом особенностей помеховой обстановки // Нанотехнологии. Информация. Радиотехника (НИР-22), 2022. – С. 45-49.
6. Сенаторов Л.А., Зиятдинов С.Ф. Исследование максимального расстояния передачи модуля LoRa SX1278 // Информационные технологии в науке, промышленности и образовании, 2021. – С. 255-260.
7. Augustin A., Yi J., Clausen T., Townsley W. M. A study of LoRa: Long range & low power networks for the internet of things // Sensors, 2016. – Т. 16. – № 9. – С. 1466.
8. Petajajarvi J., Mikhaylov K., Roivainen A., Hanninen T., Pettissalo M. On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology // 2015 14th international conference on its telecommunications (itst). – IEEE, 2015. – С. 55-59.
9. Centenaro M., Vangelista L., Zanella A., Zorzi M. Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios // IEEE Wireless Communications, 2016. – Т. 23. – № 5. – С. 60-67.
10. Dieng O., Pham C., Thiare O. Comparing and Adapting Propagation Models for LoRa Networks // 2020 16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). – IEEE, 2020. – С. 1-7.
11. Lima W. G., Lopes A. V. R., Cardoso C. M. M., Araujo J. P. L., Neto M. C. A., Tostes M. E. L., Nascimento A. A., Rodriguez M., Barros F. J. B. LoRa Technology Propagation Models for IoT Network Planning in the Amazon Regions // Sensors, 2024. – Т. 24. – № 5.
12. Suharjono A., Mukhlisin M., Wardihani E. D., Novitasari M., Khusna E., Feryando D.A., Adi W.T, Pramono S., Apriantoro R., Mujahidin I. Performance Evaluation of LoRa 915 MHz for IoT Communication System on Indonesian Railway Tracks with Environmental Factor Propagation Analysis // 2023 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT). – IEEE, 2023. – С. 264-270.
13. Aref M., Sikora A. Free space range measurements with Semtech Lora™ technology // 2014 2nd international symposium on wireless systems within the conferences on intelligent data acquisition and advanced computing systems. – IEEE, 2014. – С. 19-23.
14. SX1276 Development Kit User Guide // Semtech. URL: https://www.semtech.com/products/wireless-rf/lora-connect/sx1276dvk1jas (дата обращения: 26.03.2024).

15. ОНЕПЛАН РПЛС // ИнфоТел. URL: https://www.rpls.ru/ru/oneplan-rpls/ (дата обращения: 26.03.2024).
16. RadioPlanner 3.0 // Центр телекоммуникационных технологий. URL: https://www.ctt-group.ru/radioplanner (дата обращения: 26.03.2024).
17. Иванов В.С., Увайсов С.У., Иванов И.А. Алгоритм автоматического размещения базовых станций транкинговых систем связи // Труды учебных заведений связи, 2023. – Т. 9. – № 5. – С. 25-34.
18. Бабаев Н.В., Симонина О.А. Методика модернизации сети транкинговой связи стандарта TETRA // Труды учебных заведений связи, 2018. – Т. 4. – № 2. – С. 36-43.
19. Методика расчетов электромагнитной совместимости радиоэлектронных средств сухопутной подвижной службы с радиоэлектронными средствами гражданского назначения за исключением радиовещательной службы (решение ГКРЧ № 20-57-05 от 28 декабря 2020 г.).
20. Мордачев В.И. Электромагнитная безопасность широкополосных систем мобильной связи новых поколений // Доклады Белорусского государственного университета информатики и радиоэлектроники, 2018. – № 3 (113). – С. 39-46.
21. Okumura Y. Field strength and its variability in VHF and UHF land-mobile radio service // Review of the Electrical communication Laboratory, 1968. – Т. 16. – № 9. – С. 825-873.
22. Recommendation ITU-R P.525-2 «Calculation of free-space attenuation» // The International Telecommunication Union (ITU). URL: https://www.itu.int/md/R15-SG03-C-0009 (дата обращения: 24.04.2024).
23. Весоловский К. Системы подвижной радиосвязи. – М.: Горячая линия-Телеком, 2006.
24. Hata M. Empirical formula for propagation loss in land mobile radio services // IEEE transactions on Vehicular Technology, 1980. – Т. 29. – № 3. – С. 317-325.
25. Mogensen P.E., Eggers P., Jensen C., Andersen J. B. Urban area radio propagation measurements at 955 and 1845 MHz for small and micro cells // IEEE Global Telecommunications Conference GLOBECOM'91: Countdown to the New Millennium. Conference Record. – IEEE, 1991. – С. 1297-1302.
26. Попов В. И., Скуднов В. А., Васильев А. С. Математические модели и алгоритмы распространения радиоволн в сотовых сетях мобильной связи // Евразийский Союз Ученых, 2016. – № 3-3 (24). – С. 68-80.
27. Banimelhem O., Al-Zubi M., Al Salameh M.S. Hata Path Loss Model Tuning for Cellular Networks in Irbid City // 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing. – IEEE, 2015. – С. 1646-1650.
28. Jaghav A.N., Kale S.S. Suburban Area Path loss Propagation Prediction and Optimisation Using Hata Model at 2375MHz // International Journal of Advanced Research in Computer and Communication Engineering, 2014. – Т. 3. – № 1. – С. 5004-5008.
29. Chen Y.H., Hsieh K.L. A Dual Least-Square Approach of Tuning Optimal Propagation Model for Existing 3G Radio Network // 2006 IEEE 63rd Vehicular Technology Conference, 2006. – С. 2942-2946.
30. Recommendations and Reports of the CCIR, XVIth Plenary Assembly (Dubrovnik, 1986), Vol. V «Propagation in non-ionized media» // The International Telecommunication Union (ITU). URL: https://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.282.43.en.1006.pdf (дата обращения: 25.04.2023).

31. Zreikat A., Djordjevic M. Performance analysis of path loss prediction models in wireless mobile networks in different propagation environments // Proceedings of the 3rd World Congress on Electrical Engineering and Computer Systems and Science (EECSS'17), Rome, Italy, 2017.
32. Milanovic J., Rimac-Drlje S., Bejuk K. Comparison of propagation models accuracy for WiMAX on 3.5 GHz // 2007 14th IEEE international conference on electronics, circuits and systems, 2007. – С. 111-114.
33. Hata/Davidson. A Report on Technology Independent Methodology for the Modeling, Simulation and Empirical Verification of Wireless Communications System Performance in Noise and Interference Limited Systems Operating on Frequencies between 30 and 1500MHz // TIA TR8 Working Group, IEEE Vehicular Technology Society Propagation Committee, 1997.
34. Kasampalis S., Lazaridis P. I., Zaharis Z. D., Bizopoulos A., Zettas S., Cosmas, J. Comparison of Longley-Rice, ITU-R P. 1546 and Hata-Davidson propagation models for DVB-T coverage prediction // BMSB, 2014. – С. 1-4.
35. Kasampalis S. Modelling and coverage improvement of DVB-T networks: дис. // Brunel University London. – 2018.
36. Faruk N., Adediran Y. A., Ayeni A. A. Error Bounds of Empirical Path Loss Models at VHF/UHF Bands in Kwara State, Nigeria // Eurocon 2013, 2013. – С. 602-607.
37. Faruk, N., Bello, O. W., Ayeni, A. A., Surajudeen-Bakinde, N. T. Profiling of Radio Propagation in VHF Band // Ilorin Journal of Science, 2015. – Т. 2. – № 1. – С. 80-94.
38. Антипин Б. М., Виноградов Е. М. Анализ моделей для оценки потерь распространения сигналов при расчетах электромагнитной совместимости радиоэлектронных средств // СПбНТОРЭС: труды ежегодной НТК, 2021. – № 1. – С. 233-235.
39. Shahajahan M. Analysis of propagation models for WiMAX at 3.5 GHz // Blekinge Institute of Technology, 2009.
40. Channel Models for Fixed Wireless Applications // IEEE 802.16 Broadband Wireless Access Working Group, 2001.
41. Khan I., Eng T. C., Kamboh S. A. Performance analysis of various path loss models for wireless network in different environments // International Journal of Engineering and Advanced Technology (IJEAT), 2012. – Т. 2. – № 1. – С. 161-165.
42. Erceg, V., Greenstein, L. J., Tjandra, S. Y., Parkoff, S. R., Gupta, A., Kulic, B., Julius A. A., Bianchi R. Erceg V. An empirically based path loss model for wireless channels in suburban environments // IEEE Journal on selected areas in communications, 1999. – Т. 17. – № 7. – С. 1205-1211.
43. Lee W.C.Y. Mobile Communications Design Fundamentals, 2nd Edition // John Wiley & Sons, 1993.
44. Dobrilovic, D., Malic, M., Malic, D., Sladojevic, S. Analyses and optimization of Lee propagation model for LoRa 868 MHz network deployments in urban areas // Journal of Engineering Management and Competitiveness (JEMC), 2017. – Т. 7. – № 1. – С. 55-62.
45. Egli J. J. Radio propagation above 40 MC over irregular terrain // Proceedings of the IRE, 1957. – Т. 45. – № 10. – С. 1383-1391.
46. Ibrahim M. F., Parsons J. D. Signal strength prediction in built-up areas. Part 1: Median signal strength // IEE Proceedings F (Communications, Radar and Signal Processing). – IET Digital Library, 1983. – Т. 130. – № 5. – С. 377-384.
47. Свистунов А. С. Эмпирические модели распространения радиоволн для анализа внутрисистемной электромагнитной совместимости и безопасности сетей сотовой связи с микросотовой структурой // Журнал Белорусского государственного университета. Физика, 2018. – № 2. – С. 107-116.
48. Siwiak K., Bahreini Y. Radiowave Propagation and Antennas for Personal Communications. Third Edition // Artech House, 2007.

49. WiFi LoRa 32 (V2.1) Datasheet // HelTec Automation. URL: https://heltec.org/project/wifi-lora-32 (дата обращения: 26.03.2024).
50. Semtech SX1276-7-8-9 Datasheet // Semtech. URL: https://www.semtech.com/products/wireless-rf/lora-connect/sx1276 (дата обращения: 26.03.2024).
51. Мамченко М. В., Зорин В. А., Романова М. А. Эмпирическая модель расчета затухания сигнала с учетом коэффициента застройки местности для беспилотных транспортных средств // Известия Кабардино-Балкарского научного центра РАН, 2022. – № 1 (105). – С. 59-73.

ПОДХОДЫ К ИНТЕГРАЦИИ ТЕХНОЛОГИИ NB-IoT С СЕТЬЮ 5G

О.А. Шорин, *д.т.н., профессор, Московский технический университет связи и информатики, o.a.shorin@mtuci.ru;*
В.А. Асланян, *Московский технический университет связи и информатики, varazdataslanian@gmail.com.*

УДК 621

Аннотация. Новая узкополосная радиотехнология *NB-IoT* (Интернета Вещей), разработанная консорциумом 3*GPP*, нацелена на сверхнизкое энергопотребление, низкую стоимость устройств и максимальное покрытие. *NB-IoT* работает с минимальной пропускной способностью, что позволяет связывать огромное количество устройств с низкой скоростью передачи данных в будущем. В данной статье раскрыты результаты исследования по объединению узкополосной технологии *NB-IoT* с сетью пятого поколения. Основное внимание уделяется развертыванию пограничных облачных систем для приложений, работающих с минимальной задержкой.

Ключевые слова: *NB-IoT*; Интернет вещей; *MEC* (*Mobile Edge Computing*; 5*G;* архитектура.

APPROACHES TO INTEGRATING NB-IOT TECHNOLOGY INTO 5G NETWORKS

O.A. Shorin*, Doctor of Technical Sciences, Professor, Moscow Technical University of Communications and Informatics;*
V.A. Aslanian *Moscow Technical University of Communications and Informatics, Russia.*

Annotation. The new narrowband radio technology developed by the 3*GPP* consortium is called *NB-IoT* (narrowband radio technology of the Internet of Things). The main goals of creating this technology are ultra-low power consumption, low cost of devices and maximum coverage. *NB-IoT* works with minimal bandwidth, which allows you to connect a huge number of devices with low data transfer rates in the future. In this work, the narrowband *NB-IoT* technology is combined with the fifth generation network. The focus is on deploying edge cloud systems for applications running with minimal latency.

Keywords: *NB-IoT*; Internet of Things; *MEC*; 5*G*; architecture.

Введение

Развитие мобильных сетей связи пятого поколения 5*G*, включая обеспечение связи и оптимального уровня трафика, сталкивается с трудностями из-за резкого увеличения числа беспроводных устройств, таких как смартфоны [1, 2]. Прогнозируется, что к 2030 г. мировой трафик увеличится в 1000 раз по сравнению с 2020 г. Одной из основных целей развития сетей 5*G* является достижение скорости передачи данных около 10 Гбит/с. Кроме того, сети пятого поколения обещают высокую пропускную способность, низкие задержки, надежность, связность и мобильность.

Для решения проблем загрузки трафика, проблем подключения и достижения высокой скорости передачи данных с минимальной задержкой, новая сотовая система 5*G* должна использовать новые технологии в различных точках сети. Некоторые из этих технологий, такие как программно-определяемая сеть (*SDN*) и виртуализация сетевых функций (*NFV*), должны быть внедрены в основной сети [3].

Глобальное медиа агентство *MEC* проводит облачные вычисления непосредственно рядом с пользователем – буквально на расстоянии шага от него [4]. Использование *MEC* означает переход от централизованных крупных центров обработки данных к небольшим распределенным центрам обработки данных с ограниченными возможностями по сравнению с централизованными единицами. Это позволяет достичь больших успехов и преимуществ. Мобильное облачное вычисление – это, безусловно, тренд в области облачных вычислений, поскольку все вычисления переносятся на мобильное портативное устройство. С точки зрения лицензирования частотного спектра технологии Интернета вещей [5, 6] можно разделить на две категории: работающие в разрешенном и неразрешенном спектре. Первую категорию представляют *Lora, Sigfox* и др. Большинство из них являются нестандартными. Вторую категорию составляют уже известные всем сотовые коммуникационные технологии 2*G*/3*G* (такие как *GSM, CDMA, WCDMA* и др.), а также *LTE* – технология, поддерживающая различные виды терминалов. Стандарты для этих коммуникационных технологий, работающих в разрешенном спектре, разработаны международными организациями стандартов, такими как 3*GPP* (*GSM, WCDMA, LTE* и др.) и 3*GPP2* (*CDMA* и др.).

Технология узкополосного Интернета вещей (*NB-IoT*) является доступной и энергоэффективной технологией, разработанной 3*GPP* для передачи данных с низкой скоростью. Она предназначена для использования в интеллектуальных приложениях, таких как системы измерения данных и мониторинг окружающей среды. *NB-IoT* поддерживает массовое подключение, потребляет очень мало энергии, имеет широкий радиус действия и обеспечивает двунаправленную связь между сигнализацией и данными. Кроме того, она обладает эффективной сотовой коммуникационной сетью. Технология способна работать от одной батареи до 10 лет, что делает ее идеальным решением для проектов, где требуется продолжительное автономное функционирование, например, для интеллектуальных счетчиков, агротехнических датчиков и носимых устройств.

Основной целью исследования является нахождение подхода к интеграции *NB-IoT* с сетями 5*G*.

Задачей исследования является поиск и разработка решений для развертывания экономически выгодной упрощенной системы интеграции технологии *NB-IoT* сетям 5*G*, которая может быть реализована на универсальной вычислительной платформе.

Характеристики *NB-IoT*

В данном разделе рассмотрены некоторые характеристики *Narrrowband IoT*.

Низкое энергопотребление. NB-IoT может обеспечить длительное время работы в режиме ожидания, благодаря использованию режима энергосбережения *PSM* (*power saving mode*) и расширенного прерывистого восприятия *eDRX* (*expanded discontinuous reception*). Для достижения требуемого срока службы батареи в 10 лет для типичного низкоскоростного низкочастотного обслуживания потеря связи должна составлять 164 дБ. При использовании *PSM* и *eDRX* батарея мощностью 5 Вт может проработать 12,8 лет, если терминал отправляет 200 байт один раз в день. Сроки службы батареи в годах в зависимости от потери связи показаны в табл. 1.

Таблица 1.

	Сроки службы батареи/год		
Размер сообщения / интервал	Потеря связи в 144 дБ	Потеря связи в 154 дБ	Потеря связи в 164 дБ
50 байтов / 7200 с	22,4	11	2,5
200 байтов / 7200 с	18,2	5,9	1,5
50 байтов / 86400 с	36	31,6	17,5
200 байтов / 86400 с	34,9	26,2	12,8

Такой охват и низкая чувствительность к задержке достигаются за счет применения механизмов, в частности, повторной передачи (200 раз) и низкочастотной модуляции. В настоящее время допустимая задержка в стандарте 3*GPP IoT* составляет 10 с. Также фактически может быть обеспечена более низкая задержка около 6 с для максимальных потерь связи.

Режим передачи. Ширина полосы пропускания физического уровня составляет 200 кГц. В нисходящей линии связи используется модем *QPSK* и технология *OFDMA* с интервалом между несущими 15K. В восходящей линии связи применяются модемы *BPSK* или *QPSK* и технология *SC-FDMA*, включающая одну или несколько поднесущих. Кроме того, с точки зрения производительности, *NB-IoT* обеспечивает покрытие сигналом на уровне +20 дБ, поддерживает до 1000 соединений и имеет ресурсоемкость, позволяющую работать до 10 лет, используя только полосу частот шириной 200 кГц.

Ресурс спектра. Использование *NB-IoT* в диапазонах частот 700 МГц, 800 МГц и 900 МГц является оптимальным выбором из-за широкой экосистемы и поддержки мировыми операторами. Например, в Китае *NB-IoT* активно поддерживается четырьмя крупнейшими телекоммуникационными операторами.

Режим работы NB-IoT. В настоящее время поддерживает только *FDD* режим передачи с полосой пропускания 180 кГц и три типа развертывания:

- независимое развертывание (автономный режим);
- разделение защитных полос (защитный режим);
- внутриполосное развертывание (внутриполосный режим).

Уровни покрытия. Существуют три типа классов покрытия: нормальный охват, надежный охват и экстремальный охват. Они соответствуют минимальным потерям связи в 144, 154 и 164 дБ соответственно. Выбор модуляции, режима кодирования и повторного времени передачи данных зависит от класса покрытия терминалов.

Повторная передача данных. Для улучшения производительности демодуляции и покрытия, *NB-IoT* использует механизм повторной передачи данных, который позволяет получить коэффициент разнесения во времени и модуляцию низкого порядка. Все каналы поддерживают этот механизм.

Сеть *NB-IoT* состоит из пяти компонентов:

1) Вертикальный технический центр, который получает данные от службы *NB-IoT* и хранит их в своем центре. Он также контролирует терминалы *NB-IoT*.

2) Облачная платформа *NB-IoT*, которая обрабатывает различные услуги и перенаправляет результаты в вертикальный технический центр или терминалы *NB-IoT*.

3) Ядро сети *NB-IoT*, которое позволяет базовой станции *NB-IoT* подключаться к облачной платформе *NB-IoT*.

4) Базовая станция *NB-IoT*, которая уже развернута операторами связи и поддерживает все три типа режимов развертывания.

5) Терминалы *NB-IoT*, которые позволяют устройствам *IoT* в различных отраслях промышленности подключаться к сети *NB-IoT* при наличии соответствующей *SIM*-карты.

Наглядное изображение структуры сети *NB-IoT* представлено на рис. 1

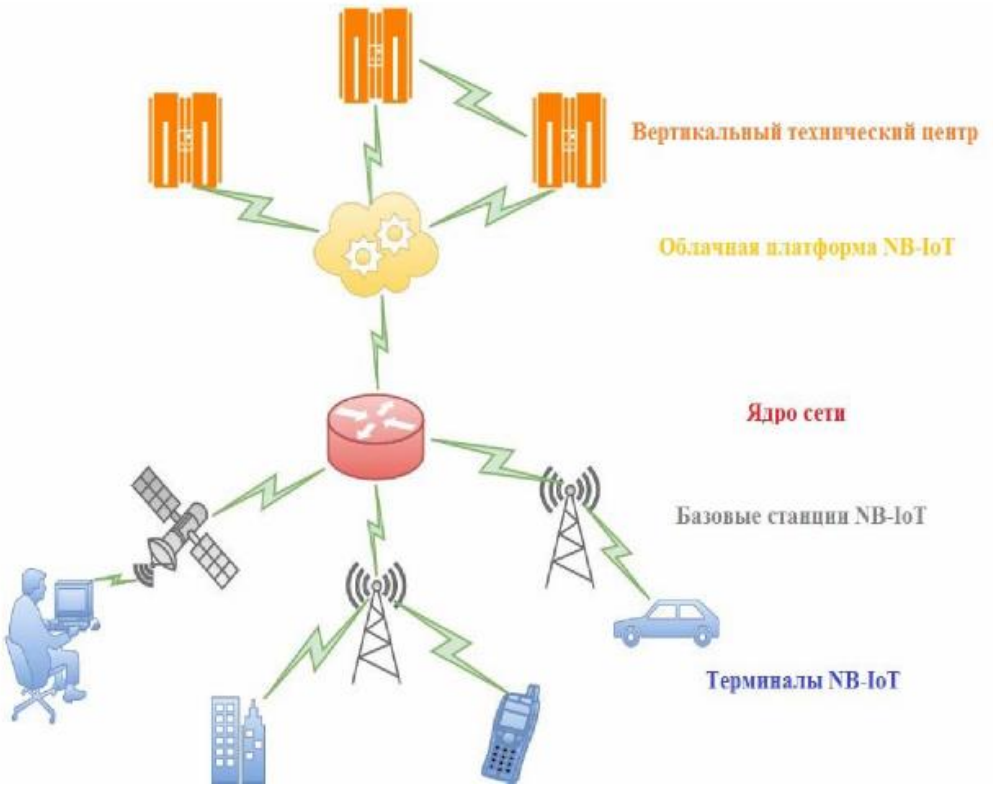


Рисунок 1

Система интеграции *NB-IoT* с сетями 5*G*

Основная цель мобильного облачного вычисления – предоставить пользовательский интерфейс для использования этих приложений. Облачные вычисления в мобильных устройствах можно классифицировать по модели обслуживания на четыре типа [9]: как потребитель (*MaaSC*), как поставщик услуг (*MaaSP*), как брокер-сервис (*MaaSB*) и как представитель службы (*MaaSR*).

Каждый пользователь в сотовой ячейке может быть одним из этих типов. Как потребитель, мобильное устройство не выполняет задачи, а все вычисления происходят в облаке или на других устройствах. Этот тип является наиболее распространенным. Если устройство может разделить процесс обработки и хранения данных, оно относится к поставщикам. В данном примере устройство собирает информацию с встроенных датчиков (камера или *GPS*) и передает данные другим пользователям. Брокер-сервис работает аналогично поставщику, но с возможностью организации сетей и переадресации. Это означает, что мобильные устройства в роли сервис-брокера могут быть шлюзом для других устройств.

Система состоит из ядра сети и распределенных ячеек. На рис. 2 показана структура системы, которая включает в себя пользовательские устройства, базовые станции (*RAN*), облачные блоки, коммутаторы доступа, коммутаторы на основе *OpenFlow*, *Middleboxes* и контроллер *SDN*. Каждая базовая станция подключается к сети через коммутаторы доступа, которые выполняют классификацию пакетов от пользовательских устройств. Коммутаторы доступа представляют собой программные коммутаторы, такие как *Open vSwitch*.

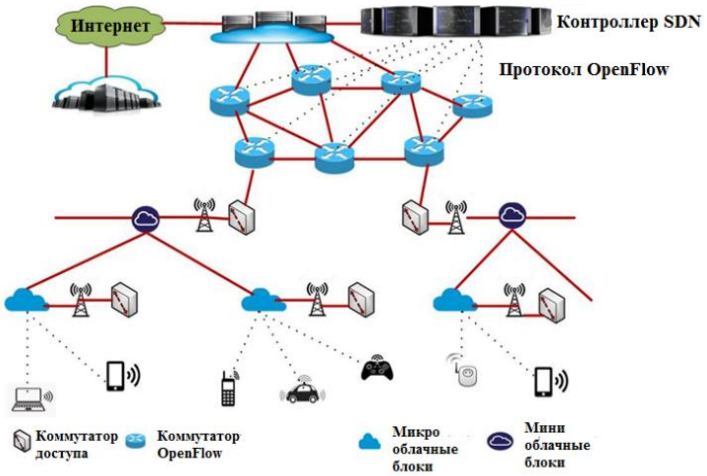


Рисунок 2

Вся сеть использует коммутаторы *OpenFlow* для управления пакетами данных и пересылки трафика на основе таблиц потоков. *Middleboxes* – это оборудование, которое позволяет сетевым операторам добавлять дополнительные функции, такие как межсетевой экран и трансляция сетевых адресов. Основные требования к функциям и сервисам, предоставляемым этими *Middleboxes*, включают эффективное использование ресурсов и защиту системы от атак. Все эти элементы составляют плоскость данных сети.

Для уменьшения количества промежуточных узлов и разгрузки системы используется облачный модуль. Разгрузка состоит из трех частей, как показано на рис. 3. Первая часть – разгрузка базовой станции, где облачный модуль помогает в выделении ресурсов. Вторая часть – разгрузка *IoT*, представляющая собой передаваемую рабочую нагрузку от узлов датчиков. Третья часть – разгрузка сотовых данных.

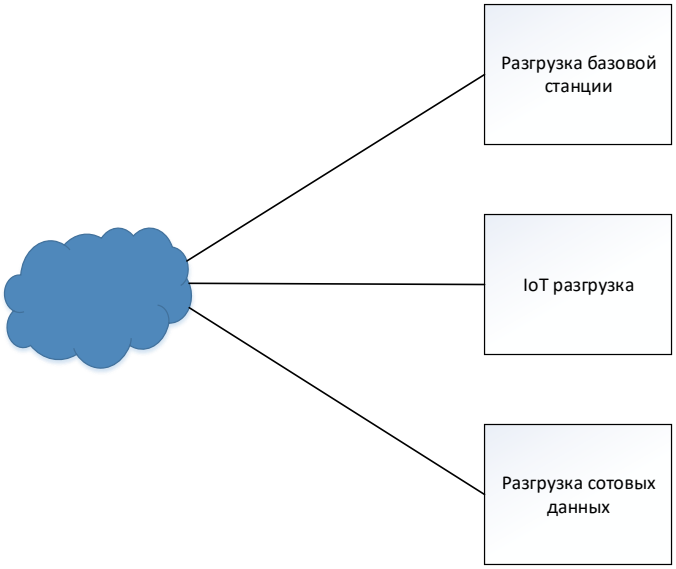


Рисунок 3

Заключение

Предлагаемая система способна эффективно управлять и устанавливать гибкий маршрут между любыми двумя конечными точками, что позволяет сократить количество промежуточных узлов в процессе коммуникации. Она основана на использовании *SDN* в ядре сети, что делает ее актуальной и эффективной для интеграции *NB-IoT* с системой 5*G*.

Литература

1. Бородин А. С., Кучерявый А. Е. Сети связи пятого поколения как основа цифровой экономики // Электросвязь, 2017. – № 5. – С. 45-49.
2. Muthanna A., Masek P., Hosek J., Fujdiak R., Hussein O., Paramonov A., Koucheryavy A. Analytical Evaluation of D2D Connectivity Potential in 5G Wireless System // Lecture Notes in Computer Science, 2016. – Vol. 9870. – pp. 395-403.
3. Курбанова Ф. Ф., Залкеприева А. А., Рамазанова П. М. [и др.] NFV Виртуализация сетевых функций // Научное сообщество студентов XXI столетия. Технические науки: сб. ст. по мат. XLIII междунар. студ. науч.-практ. конф. № 6 (42). URL: https://sibac.info/archive/technic/6(42).pdf
4. Мутханна А. С. А., Атея А. А., Филимонова М. И. Исследование облачных вычислений в сотовых сетях // Информационные технологии и телекоммуникации, 2017. – Т. 5. – № 3. – С. 45-59.
5. Vladyko A., Muthanna A., Kirichek R. Comprehensive SDN Testing Based on Model Network // Lecture Notes in Computer Science, 2016. – Vol. 9870. – pp. 539-549.
6. Кучерявый А. Е. Интернет Вещей // Электросвязь, 2013. – № 1. – С. 21-24.
7. Шорин О.А. Улучшенные сигнальные структуры FBMC (5G) для систем критических коммуникаций: повышение помехоустойчивости в условиях многолучевого распространения // Экономика и качество систем связи, 2022 – № 3 (25). – С. 22-37.
8. Шорин О.А., Бокк Г.О. Снижение негативного влияния высоких значений пик-фактора сигналов в системе McWILL // Экономика и качество систем связи, 2019. – № 1 (11). – С. 9-13.
9. Ateya A., Muthanna A., Gudkova I., Vybornova A., Koucheryavy A. Intelligent core network for Tactile Internet system // International Conference on Future Networks and Distributed Systems, 2017.

10. Гребенщикова А. А., Атея А. А., Мутханна А. С. А., Киричек Р. В. Подходы к интеграции технологии NB-IoT сетям 5G/IMT-2020/IMT-2020 // Информационные технологии и телекоммуникации, 2017. – Т. 5. – № 4. – С. 8-16.
11. URL https://www.researchgate.net/publication/350857731_Application_and_Research_of_New_Power_Supply_in_the_Construction_of_Internet_of_Things_Plus_Smart_City (дата обращения - июнь 2024 г.).
12. URL https://www.researchgate.net/publication/354839523_A_Review_of_Interference_Challenges_on_Integrated_5GNR_and_NB-IoT_Networks (дата обращения - июнь 2024 г.)
13. URL https://www.researchgate.net/publication/344930200_Building_upon_NB-IoT_networks_A_roadmap_towards_5G_new_radio_networks (дата обращения - июнь 2024 г.)
14. URL https://www.researchgate.net/publication/260204418_5G_wireless_communication_systems_Prospects_and_challenges_Guest_Editorial (дата обращения - июнь 2024 г.)
15. Devaki Chandramouli, Rainer Liebhart, Juho Pirskanen. 5G for the Connected World – М.: Изд-во Wiley, 2019. – 505 с.
16. Klas G. I. Fog Computing and Mobile Edge Cloud Gain Momentum Open Fog Consortium // The Eleventh International Conference on Systems and Networks Communications (ICSNC), 2016. – 122 p.
17. Рыжков А. Е. Развитие технологии NB-IoT // Труды учебных заведений связи, 2017. – Т. 3. – № 4. – С. 94-101.

КАЧЕСТВО АЛГОРИТМОВ ОЦЕНКИ ПАРАМЕТРОВ СИГНАЛА В СИСТЕМЕ МАКВИЛ

Е.М. Лобов, *к.т.н., доцент, Московский технический университет связи и информатики, e.m.lobov@mtuci.ru;*
В.О. Шорин, *Московский технический университет связи и информатики, shorinvasily23@gmail.com.*

УДК 621.396.969

Аннотация. Цель данной статьи – анализ методов улучшения качества систем связи. Методология исследования включала использование аналитических методов и моделирования. Результаты показывают значительное улучшение параметров качества при применении предложенных подходов. Выводы подтверждают эффективность предложенных методов.

Ключевые слова: качество связи; системы связи; улучшение качества.

QUALITY OF ALGORITHMS FOR ESTIMATING SIGNAL PARAMETERS IN THE MCWILL SYSTEM

Evgeniy Lobov, *Ph.D. of Engineering Sciences, assistant professor, Moscow Technical University of Communication and Informatics;*
Vasiliy Shorin, *Moscow Technical University of Communication and Informatics.*

Annotation. The aim of this article is to analyze methods for improving the quality of communication systems. The research methodology included the use of analytical methods and modeling. The results show a significant improvement in quality parameters when the proposed approaches are applied. The conclusions confirm the effectiveness of the proposed methods.

Keywords: communication quality; communication systems; quality improvement.

Введение

Главным инструментом, формирующим показатели помехоустойчивости систем и линий связи, являются алгоритмы обработки сигнала, реализующие на приеме заданное качество выделения информации в условиях предельно низких значений сигнал/(помеха+шум) в радиоканале. Для идеализированных ситуаций, характеризующихся отсутствием искажений сигнала, в условиях справедливости модели аддитивных гауссовских шумов, потенциально достижимые показатели режима безошибочного информационного обмена известны специалистам в виде второй теоремы Шеннона [1]. Однако в реальных приложениях, связанных с сетями связи подвижных абонентов, исключить искажения радиоканала невозможно. Распространение практически всегда осуществляется по ряду лучей с переотражениями. В месте приема сигналы лучей интерферируют, что приводит к трудно прогнозируемым частотно-селективным замираниям, демонстрирующим быстрые изменения. Дополнительную сложность привносит нестабильность показателей амплитудно-частотных (АЧХ) и фазо-частотных (ФЧХ) характеристик устройств, возникающая вследствие зависимости от изменяющейся температуры, нестабильности генераторов, допусков реализации, старением оборудования и даже из-за нелинейных искажений, порождаемых высоким показателем пик-фактора (*PAPR*), характерным для широко применяемых в современных системах радиосвязи *OFDM*-сигналов [2]. Из-за движения абонентов в каждом луче возникает индивидуальный доплеровский сдвиг.

Отдельную значимость приобретают задачи высокоточной синхронизации по частоте и задержке на приеме. Без их решения невозможно добиться согласования алгоритмов сигнальной обработки с наблюдаемыми параметрами радиоканала, что резко снижает показатели пропускной способности. Возникает взаимная увязка между структурой алгоритмов высокоточной синхронизации со структурой применяемых радиосигналов, режимом доступа, условиями распространения и уровнем сигнал/(помеха+шум) в канале. Особенно выраженно отмеченная связь проявляется в системах с доступом на основе временного разделения (*TDD*), как например в технологии МАКВИЛ. Это объясняется тем, что при обработке на интервалах больше кадра возникают отрезки времени, используемые обратным каналом, и динамическая природа флуктуаций проявляется сильнее. В [3, 4] были сформулированы задачи синтеза алгоритмов синхронизации и оценки/компенсации искажений АЧХ/ФЧХ на сверхкоротких выборках наблюдений для условий, отвечающих моделям многолучевого распространения, установленным рекомендациями 3*GPP* [5, 6], и при предельно общей модели динамического поведения. В качестве дополнительного условия выдвигалось требование учета кадровой организации информационного обмена, применяемой в современных системах.

Одним из требований синтеза являлось получение субоптимального алгоритма с предельно простыми вариантами агрегирования статистических данных, который бы уже на малых выборках гарантировал рабочие характеристики, незначительно уступающие потенциальным. В качестве

допустимых для МАКВИЛ были использованы эквивалентные энергетические потери, составляющие не более 1,5 дБ.

Для *LTE* вопросы поиска сигналов/синхронизации/коррекции АЧХ-ФЧХ хорошо проработаны в теоретическом плане. Они прошли широкую проверку на практике. Соответствующие результаты можно найти в документах международного союза электросвязи, рекомендациях 3*GPP*, а также в широкодоступной технической литературе по профилю (например, [7]).

Для системы МАКВИЛ данные вопросы пока не получили своего детального исследования и не нашли широкого освещения. При этом следует отметить, что МАКВИЛ использует режим *TDD*, имеет ряд отмеченных выше отличий в структурах служебных каналов и условиях функционирования. Прямое заимствование результатов *LTE* невозможно.

Как в сетях *LTE*, так и в сети МАКВИЛ базовым элементом сигнальных структур синхронизации и контроля выступают расположенные на выделенных частотных позициях поднесущих «пары» одинаковых символов (*RS* или *Pilot*). Из-за ошибок синхронизации по частоте символы в таких «парах» могут приобретать некоторый фазовый сдвиг. Если же рассматривать символы на разных поднесущих, то от позиции к позиции символы могут демонстрировать произвольные амплитудно-частотные искажения. На начальном этапе, связанном с режимом вхождения в синхронизацию, справедливо полагать, что априорная информация о характеристиках распределения амплитуд и фаз символов на поднесущих отсутствует. В [3, 4] приведены алгоритмы оценок необходимых параметров сигнала по векторам квадратурных компонент спектральных составляющих, наблюдаемые в позициях квадратурных уровней (синфазных и ортогональных, соответственно) поднесущих принимаемой базовой сигнальной структуры. Для систем связи МАКВИЛ значение числа поднесущих K составляет 64 для сигнала Преамбулы и 16 – для широковещательного канала управления (*BCH – broadcast channel)* или выделенного речевого абонентского соединения. На основе выборки квадратурных составляющих сигнала формируется оценка максимального правдоподобия (ОМП) в начальный момент установления сеанса связи или оценка апостериорного максимума при установлении соединения.

Для синтезированных в [3, 4] оптимальных и субоптимальных алгоритмов были реализована программа, интерфейс которой показан на рис. 1, позволяющая устанавливать модели многолучевого распространения, в том числе и согласно [5, 6]. Поскольку предлагаемый подход изначально не обладает общностью универсальной теории, то необходимо конкретизировать сигнально-кадровую структуру исследуемой системы. На рис. 2 показана сигнально-кадровая структура радиоканала системы МАКВИЛ, на которой выделена Преамбула, используемая для первоначального входа абонентской станции (АС) в синхронизацию с сетью и обнаружения работающих БС. Обработка Преамбул осуществляется согласно (2.2) - (2.5) в источнике [8]. Из-за того, что на интервале Преамбул работают сразу все БС, то помеховая обстановка является сложной и высокую точность синхронизации гарантировать нельзя. Поэтому данная обработка обеспечивает только грубую предварительную синхронизацию, составляющую «шаг 1» вхождения в синхронизацию.

На рис. 3 показана сигнально-кадровая структура радиоканала системы МАКВИЛ, на которой выделен тайм-слот (*TS*), содержащий широковещательный канал управления (*BCH*). *Pilot*-врезки канала *BCH* (помечены на рис. 3 красным цветом) используются для начала входа АС в режим точной синхронизации с сервирующей БС МАКВИЛ, а также для начальной оценки и коррекции искажений спектральных характеристик радиоканала.

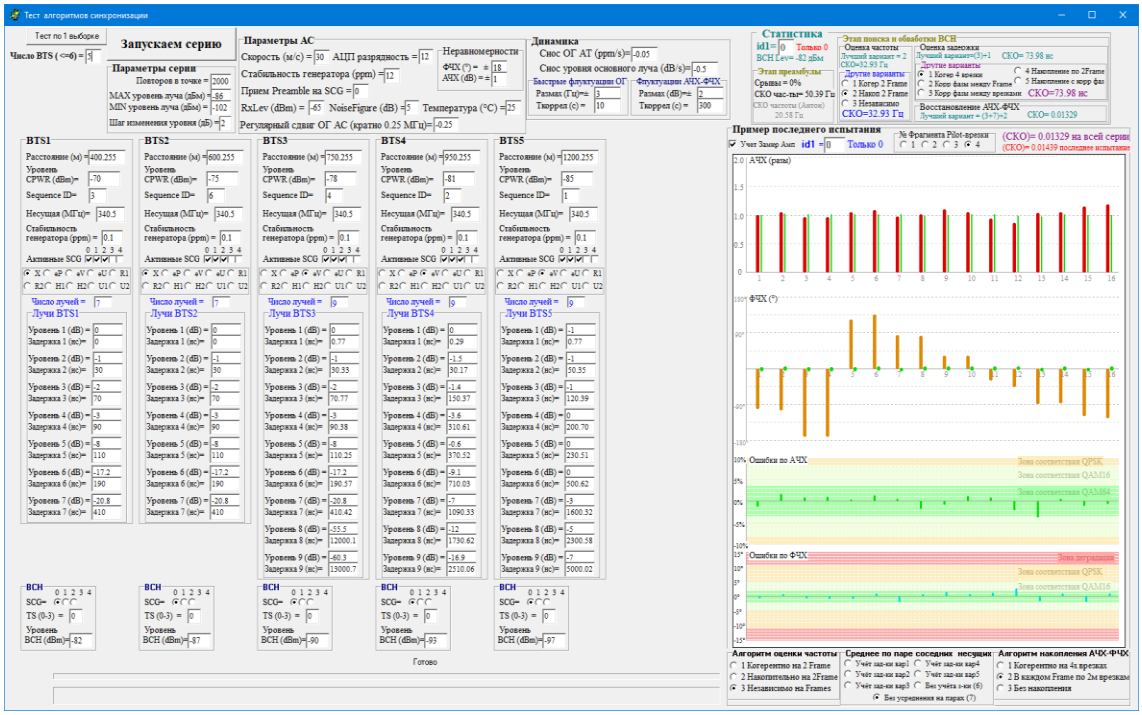


Рисунок 1

Врезки Pilot на символах OFDM

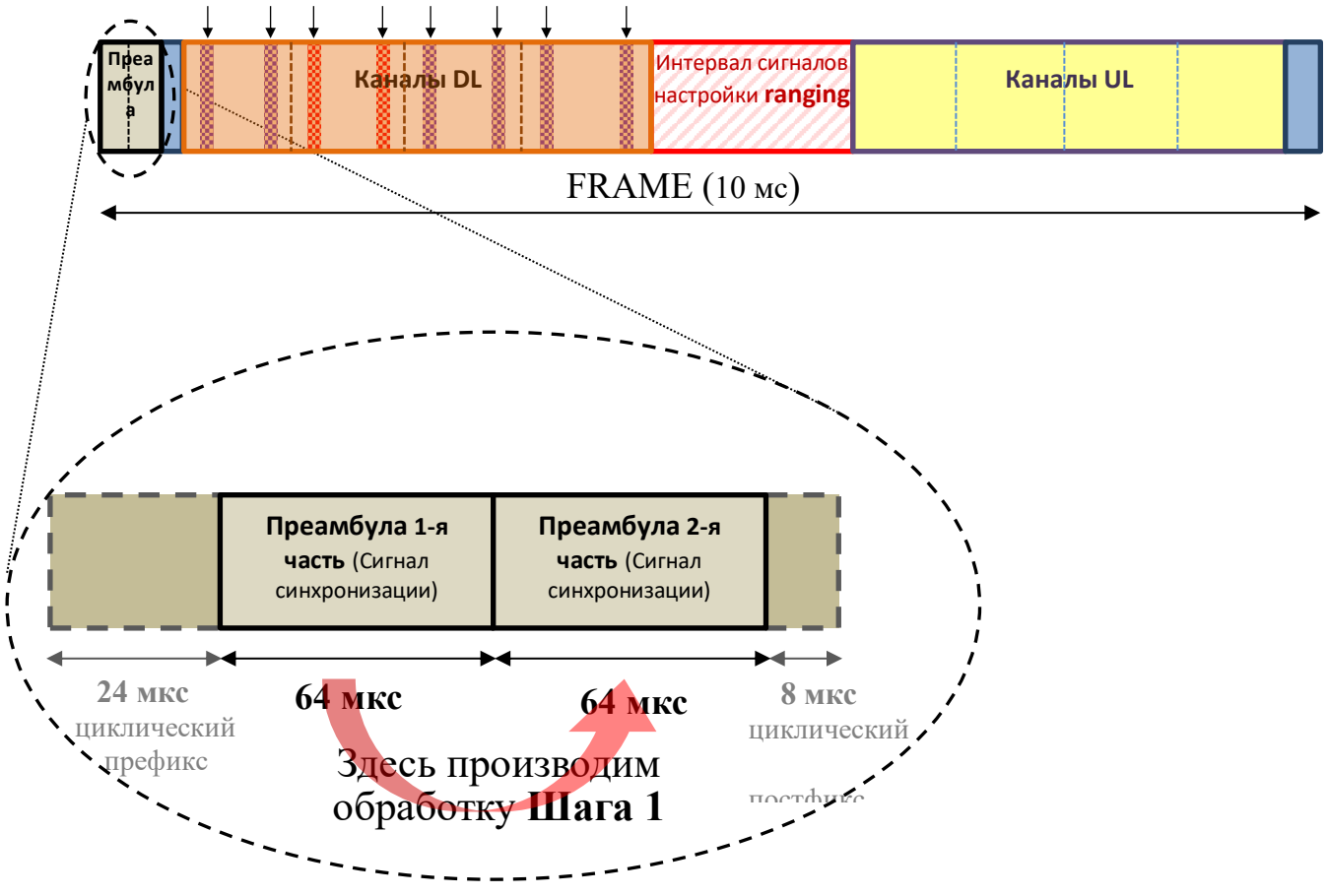


Рисунок 2

Обработка *Pilot*-врезок первого принимаемого кадра с *BCH*, составляющая «шаг 2», не предполагает накопления. Она основывается на простом применении соотношений (2.2) - (2.5), приведенных в [8] при синхронизации и контроле спектральных искажений.

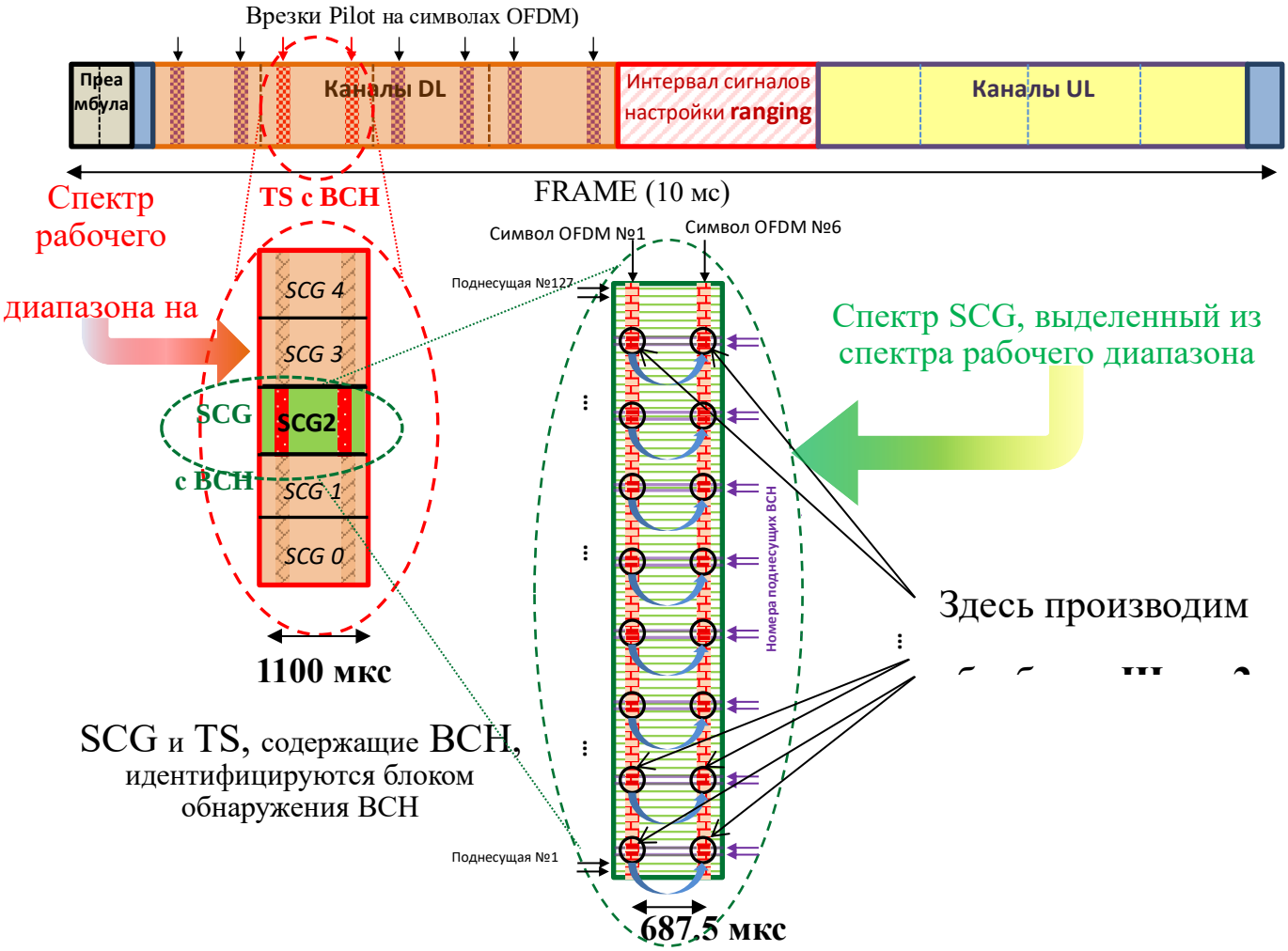


Рисунок 3

На рис. 4 показывает следующий (возможный) «шаг 3» обработки, состоящий в накоплении (когерентном, статистическом, статистическом с дополнительными преобразованиями и т.д.) данных на двух кадрах радиоканала МАКВИЛ. Значительное увеличение измерительной базы на «шаге 3» открывает большие возможности для получения высокоточной оценки сдвига частоты при когерентной обработке. Для оценок задержки и спектральных искажений потенциальные возможности данного шага не столь значительны. Они состоят исключительно в доступности двукратного статистического накопления замеров. Но для всех случаев существенным остается вопрос устойчивости параметров на интервале двух кадров (2*10мс) в условиях многолучевого распространения. При ее частичном нарушении вполне возможно получить ухудшение результатов после введения в алгоритм обработки «шага 3».

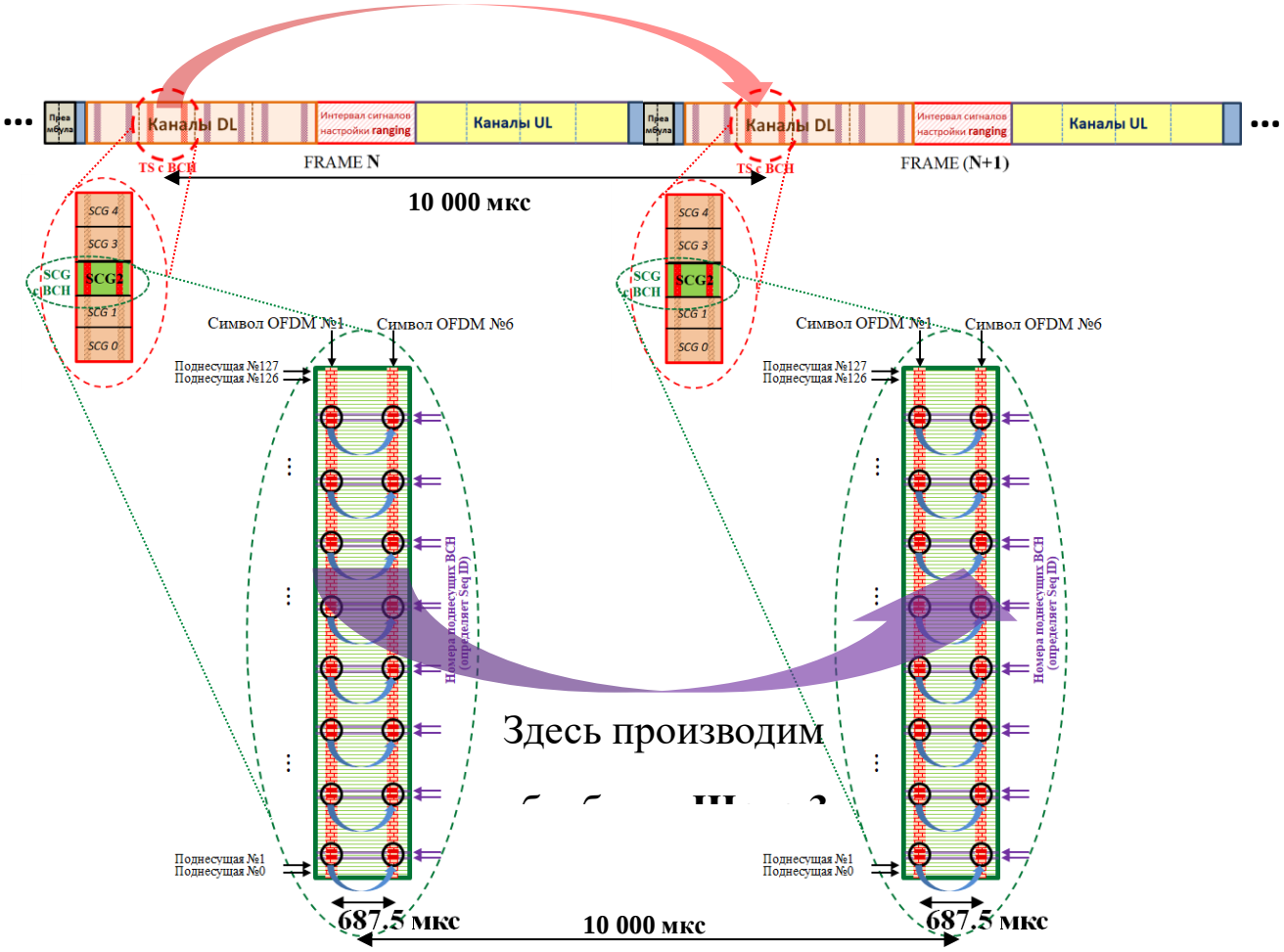


Рисунок 4

Для поиска наиболее эффективных вариантов алгоритмов синхронизации и коррекции искажений радиоканала на коротких выборках предлагается эмпирический подход, состоящий в экспериментальной проверке (сопоставлении) того, на сколько значимым будет результат статистического накопления («Шаг 1» + «Шаг 2» или («Шаг 1» + «Шаг 2» + «Шаг 3») в различных условиях многолучевого распространения и при разных скоростях движения абонентов.

Алгоритмы накопления для оценки сдвига частоты

F.1. Когерентное накопление на двух соседних кадрах (фреймах)

Этот вариант предполагает высокую стабильность спектральных характеристик радиоканала и малые девиации частоты ОГ на интервале между кадрами. В таком случае предлагается применять алгоритм (ниже обозначаемый как № *f*1), включающий обработку «шага 2» и «шага 3». На «шаге 2» формируются оценки спектральных компонент оценки частотных сдвигов для соседних кадров *N* и *N*+1, показанных на рис. 5. На «шаге 3» формируется усредненная оценка частотного сдвига и устраняется фазовый набег. Далее оценки используются в качестве измерений на следующем шаге, который формирует окончательную коррекцию сдвига частоты для задержки *TFRAME*=10 мс. Рис. 5 поясняет способ формирования замеров и их группировку в пары.

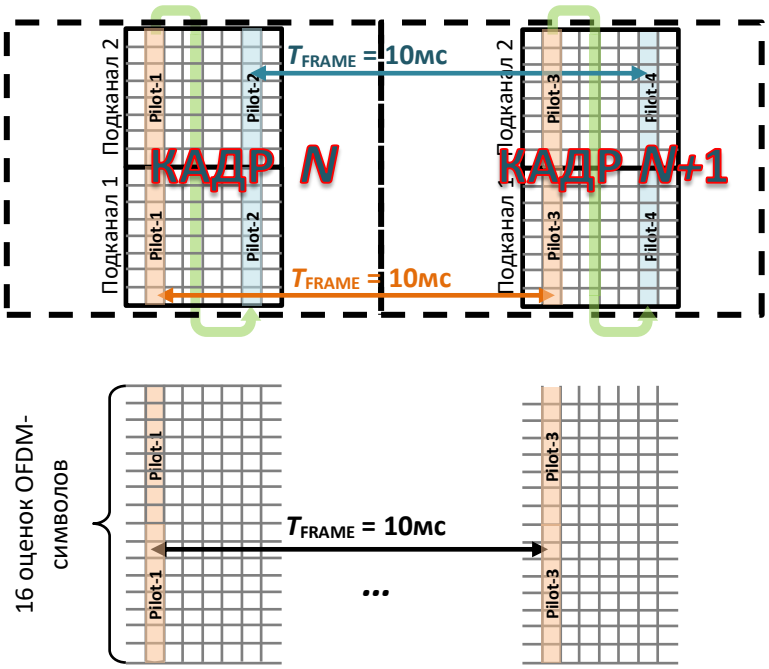


Рисунок 5

Оптимальный по критерию МП алгоритм в данном случае, конечно, требует учета имеющейся функциональной связи между корректирующими параметрами, относящимися как к *Pilot*-врезкам соседних кадров, так и связанными с обработкой «шага 3» на интервале между кадрами. Такую связь можно учесть путем введения рекуррентной процедуры коррекций. Но это заметно повысит вычислительную сложность. А так как длительность кадра в МАКВИЛ примерно в 14,55 раз превосходит задержку между *Pilot*-врезками внутри *TS*, то точность оценки набега фазы не может быть заметно улучшена за счет указанных коррекций (эффективный энергетический выигрыш от коррекций принципиально ограничен уровнем $10lg(1+1/14{,}55)2 = 0{,}58$ дБ). Поэтому на данном этапе рекуррентные коррекции не использовались.

Описанный алгоритм оценки частотного сдвига потенциально имеет значительные преимущества над алгоритмами, работающими в отдельных ресурсных блоках. Но это будет действительно так, если только динамические эффекты и частотно-селективные замирания не будут проявляться слишком сильно на интервалах порядка *TFRAME*=10 мс.

F.2. Статистическое накопление на двух соседних кадрах

Данный вариант алгоритма предполагает, что на интервале задержки между соседними кадрами происходят заметные частотно-селективные замирания, но сдвиг частоты ОГ АС остается стабильным. Поэтому оценку сдвига частоты ОГ можно сформировать как результат усреднения двух значений для *Pilot*-врезок канала *BCH* на двух соседних кадрах.

Указанный вариант алгоритма в представленных ниже экспериментальных результатах обозначается как № *f*2.

F.3. Алгоритм независимой оценки (без накопления)

Данный вариант алгоритма предполагает, что на интервале задержки между кадрами происходят заметные частотно-селективные замирания, и сдвиг частоты ОГ АС не обладает стабильностью. В этом случае сдвиг частоты формируется для каждого кадра отдельно, т.е. «шаг 3» не используется.

Указанный вариант алгоритма в представленных ниже экспериментальных результатах обозначается как № *f*3.

Алгоритмы оценки задержки:

T.1. Когерентное сложение откликов *IFFT* (обратное преобразование Фурье) от спектров *Pilot*-врезок соседних кадров

Такой вариант ориентирован на устойчивое поведение частотно-селективных замираний и ОГ на интервале двух кадров.

Указанный вариант алгоритма в представленных ниже экспериментальных результатах обозначается как № *t*1.

T.2. Когерентное сложение откликов *IFFT* от *Pilot*-врезок внутри кадра и последующее сложение модулей результатов соседних кадров

Обработка ориентирована на ситуации с устойчивым поведением частотно-селективных замираний на интервале двух кадров, но в условиях, когда синхронизация по частоте не обеспечивает когерентность измерений на соседних кадрах.

Указанный вариант алгоритма в представленных ниже экспериментальных результатах обозначается как № *t*2.

T.3. Сложение модулей откликов *IFFT* для четырех *Pilot*-врезок соседних кадров

Обработка, ориентированная на ситуации, когда частотно-селективные замирания нельзя считать устойчивыми уже на интервале кадра, но параметр задержки остается стабильным (практически не изменяется).

Указанный вариант алгоритма в представленных ниже экспериментальных результатах обозначается как № *t*3.

T.4. Статистическое усреднение оценок задержки, полученных в соседних кадрах по критерию максимума отклика, формируемого методом когерентного сложения

Обработка, ориентированная на ситуации, когда на интервале между кадрами могут происходить одновременно заметные замирания как сигнала, так и помех, доминирующих над шумами, но при этом в пределах каждого *TS* спектральные характеристики канала стабильны, а параметр задержки сигнала (в трактах передачи и приема) сохраняется на интервале двух кадров.

Указанный вариант алгоритма в представленных ниже экспериментальных результатах обозначается как № *t*4.

T.5. Статистическое усреднение оценок задержки, полученных в соседних кадрах по критерию максимума отклика, формируемого методом сложения модулей

Обработка предполагает ситуации, в которых имеют место условия, отмеченные для предыдущего варианта, кроме стабильности спектральных характеристик в пределах каждого *TS*. Указанный вариант алгоритма в представленных ниже экспериментальных результатах обозначается как № *t*5. Интерполяционные расчеты позиций и значений максимумов во всех вышеперечисленных вариантах оценок задержки должны выполняться с использованием коррекции.

Алгоритмы коррекции искажений спектральной характеристики канала

Q.1. Когерентное накопление замеров четырех *Pilot*-символов, расположенных в одинаковых позициях поднесущих в двух соседних кадрах

В данной ситуации могут использоваться оценки сдвига частоты, полученные по описанным выше алгоритмам *f*1 или *f*2. Для полноты эксперимента были проведены тесты и для комбинации данного алгоритма с оценкой сдвига *f*3. В этом случае набеги фазы внутри *TS* действительно рассчитывались с использованием оценок сдвига частоты *f*3, а между кадрами с использованием *f*2.

Данный вариант алгоритма оценки/коррекции спектральных искажений в представленных ниже экспериментальных результатах обозначается как № *q*1.

Q.2. Накопление замеров двух *Pilot*-символов в одинаковых позициях поднесущих текущего кадра для момента первой *Pilot*-врезки текущего кадра (т.е. для позиции символа *OFDM* №1 линии *Down*). А для других символов *OFDM* линии *Down*, имеющих номер *m* (*m*=0, …, 7) используется интерполяционная формула:

где Δf вычисляется согласно (2.3) в [8], $T = 5TOFDM = 687{,}5$ мкс – интервал между *Pilot*-врезками в *TS*, *m* – номер символа *OFDM* в линии *Down* текущего кадра, $D(m) = \left((6-m) + (m-1)\sqrt{\hat{R}^2 + \hat{P}^2}\right)/5$ – интерполяционная оценка относительной амплитуды символа *OFDM* с номером *m*, вычисляются согласно (2.2) в [8].

Данный вариант алгоритма оценки/коррекции спектральных искажений в представленных ниже экспериментальных результатах обозначается как № *q*2.

Q.3. Без накопления замеров для момента первой *Pilot*-врезки текущего кадра (т.е. для позиции символа *OFDM* №1 линии *Down*). А для других символов *OFDM* линии *Down*, имеющих номер *m* (*m*=0, …, 7) используются интерполяционные формулы.

Данный вариант алгоритма оценки/коррекции спектральных искажений в представленных ниже экспериментальных результатах обозначается как № *q*3.

T.*+*Q*.*. Частотно-временное накопление замеров

В технической документации *Xinwei* [8, п.14.3.2] предлагается применять для оценки искажений спектральной характеристики канала алгоритм, использующий операцию усреднения замеров на двух соседних поднесущих. Такой вариант появился потому, что при распределении ресурсов радиоканала в МАКВИЛ минимальная порция (квант) составляет два подканала, первый из которых имеет четный номер 2*k*, а второй нечетный номер 2*k*+1. В результате спектр выделенного ресурса, как и минимальной порции, всегда представляет собой пары соседних поднесущих, следующих периодически с некоторым шагом в рабочей частотной области. Это можно видеть на примере канала *BCH* в нижней части рис. 4.

Сразу нужно отметить, что вариант (2.21), предложенный в [8], содержит определенный изъян. Он с целью упрощения вычислений предлагает игнорировать фазовые набеги, возникающие из-за ненулевого параметра задержки в замерах на соседних поднесущих.

Можно видеть, что уточнение предварительного усреднения зависит от способа оценки параметра задержки. Поэтому ниже в экспериментальных результатах варианты с предварительным усреднением по соседним поднесущим обозначается как (*t**) + *q**, где вместо звездочек стоят цифры. Например, (*t*1) + *q*1 обозначает, что предварительное усреднение выполнено с учетом фазовых набегов и с использованием оценки задержки, полученной алгоритмом *t*1, после чего применялся алгоритм когерентного накопления *q*1 для оценки спектральных искажений. Варианты (*t*6) + *q** обозначают случаи с предварительным усреднением замеров на двух соседних поднесущих. Это точно соответствует варианту, прописанному в [8]. А варианты (*t*7) + *q** обозначают случаи, когда предварительное усреднение на соседних поднесущих не применяется.

Также в обозначающих сочетаниях на первых позициях присутствуют символы *f**. Они раскрывают вариант примененного вспомогательного алгоритма синхронизации по частоте, который нужен для устранения набега фаз и устранения возможных неоднозначностей в формируемых оценках.

Таким образом, полное обозначение тестируемого алгоритма коррекции искажений спектральной характеристики канала имеет формат (*f**+*t**)+*q**, где в позициях первой и последней звездочек могут стоять цифры от 1 до 3, а в позиции второй звездочки – от 1 до 7.

Алгоритмы с наилучшими показателями обеспечивают наилучшие рабочие характеристики (или отличающиеся от наилучших не более чем на 1 дБ по эффективному показателю сигнал/шум) для всех сочетаний (мощность сигнала) + (скорость движения абонента). Общий объем обучающей выборки составил 240 тыс. независимых испытаний.

На рис. 6 показана мощностно-скоростная плоскость с полученной разбивкой на кластеры для режима синхронизации по частоте. В каждом кластере показан тип алгоритма, обеспечивающий в нем наилучшие показатели по точности (минимум СКО) синхронизации.

Нумерация наилучших алгоритмов соответствует вышеприведенному описанию.

На рис. 7а-г для ряда скоростей показаны зависимости СКО оценок сдвига частоты от уровня сигнала, формируемых разными алгоритмами. Результаты получены при тестировании работы системы МАКВИЛ в диапазоне 340 МГц.

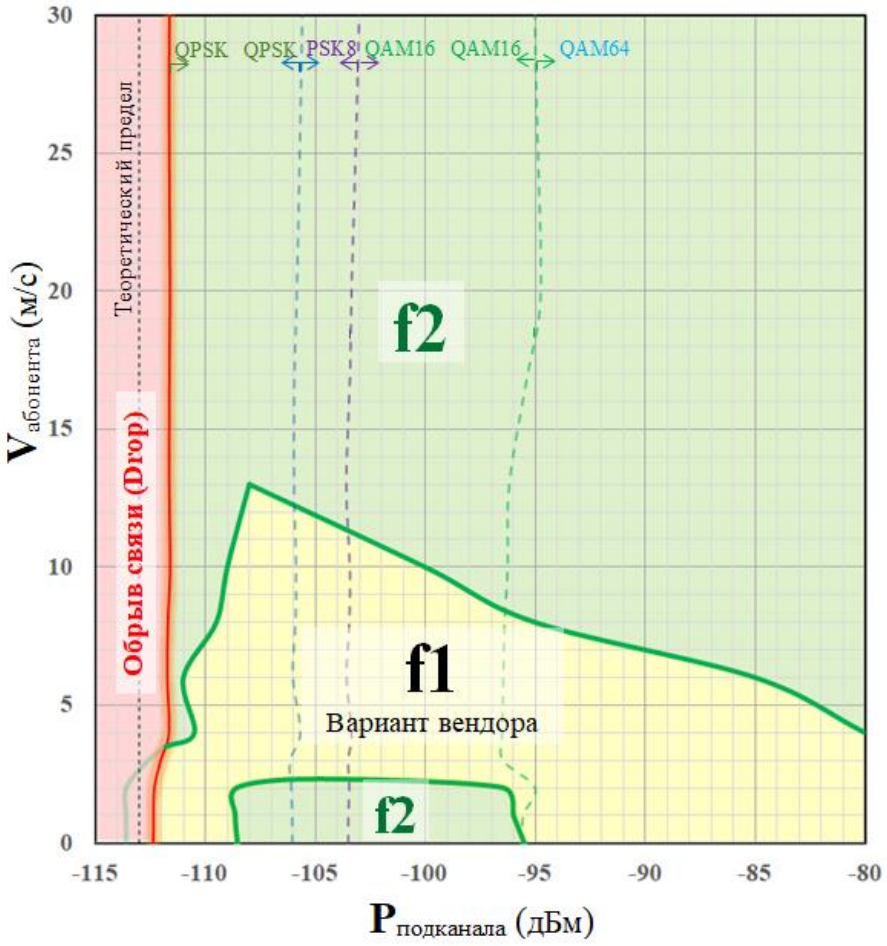


Рисунок 6

Толстыми линиями соответствующего цвета показаны характеристики алгоритма, выбираемого по расширенной таблице *CQI* (*Channel Quality Indicator*) (отвечающего кластеру рис. 6), обладающего либо наилучшими, либо близкими к наилучшим показателям.

Теоретический предел уровня приема, соответствующий мощности сигнала в подканале МАКВИЛ, рассчитывался исходя из паспортных данных производителя, в котором установлен минимально допустимый показатель сигнал/шум = 8 дБ для работы с модуляцией *QPSK* [8].

На рис. 8 показана мощностно-скоростная плоскость с полученной разбивкой на кластеры для режима синхронизации по задержке. В каждом кластере показан тип алгоритма, обеспечивающий в нем наилучшие показатели по точности (минимум СКО) синхронизации.

Выяснилось, что показатели синхронизации по задержке связаны с тем, какую точность обеспечивает алгоритм оценки частоты при компенсации набегов фазы. Поэтому тестировались сочетания алгоритмов оценки частоты (на рис.8 тип проставлен в скобках) и оценки задержки.

На рис. 9а-г для ряда скоростей показаны зависимости СКО оценок задержки от уровня сигнала, формируемых разными алгоритмами.

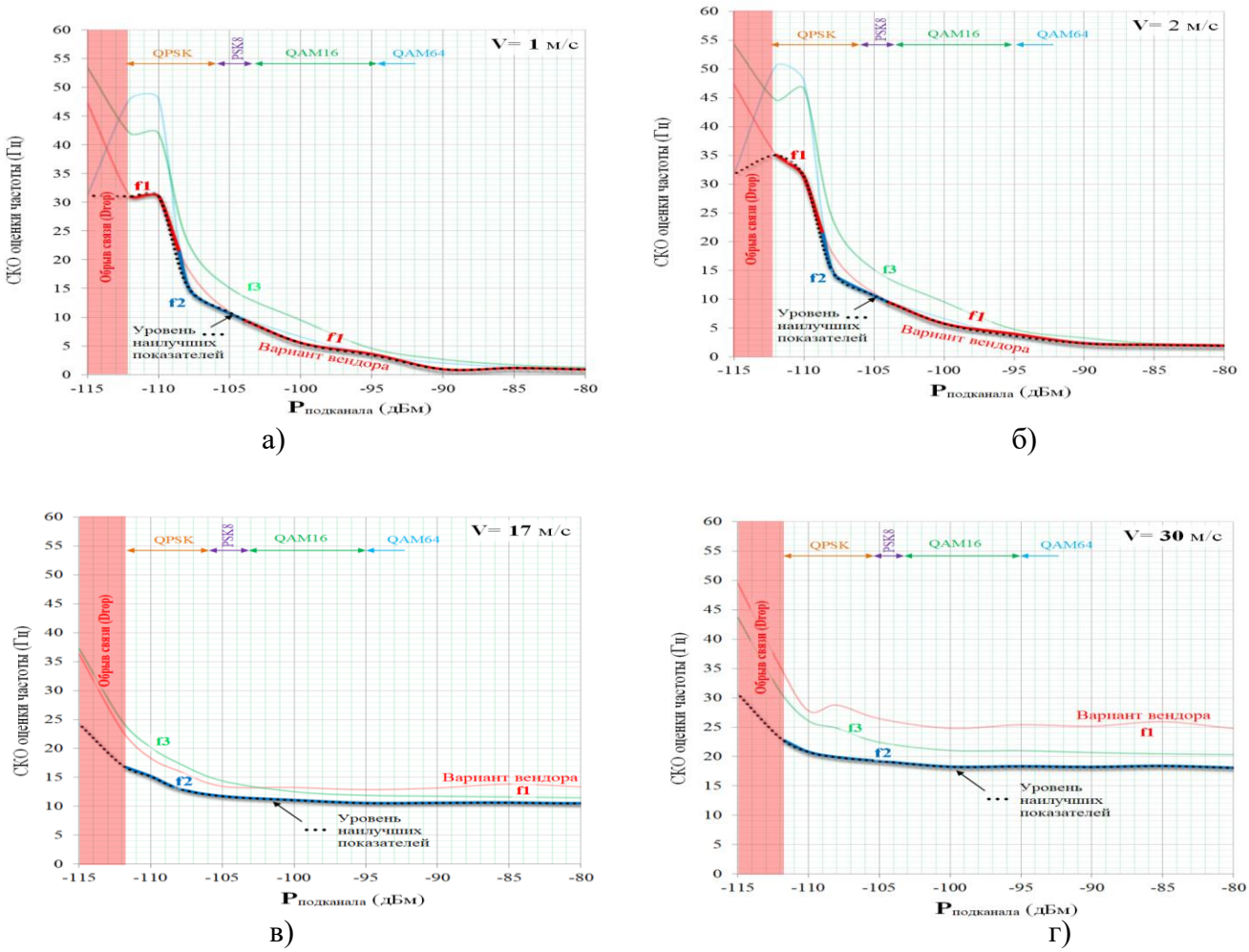


Рисунок 7

Выяснилось, что показатели синхронизации по задержке связаны с тем, какую точность обеспечивает алгоритм оценки частоты при компенсации набегов фазы. Поэтому тестировались сочетания алгоритмов оценки частоты (на рис. 8 тип проставлен в скобках) и оценки задержки.

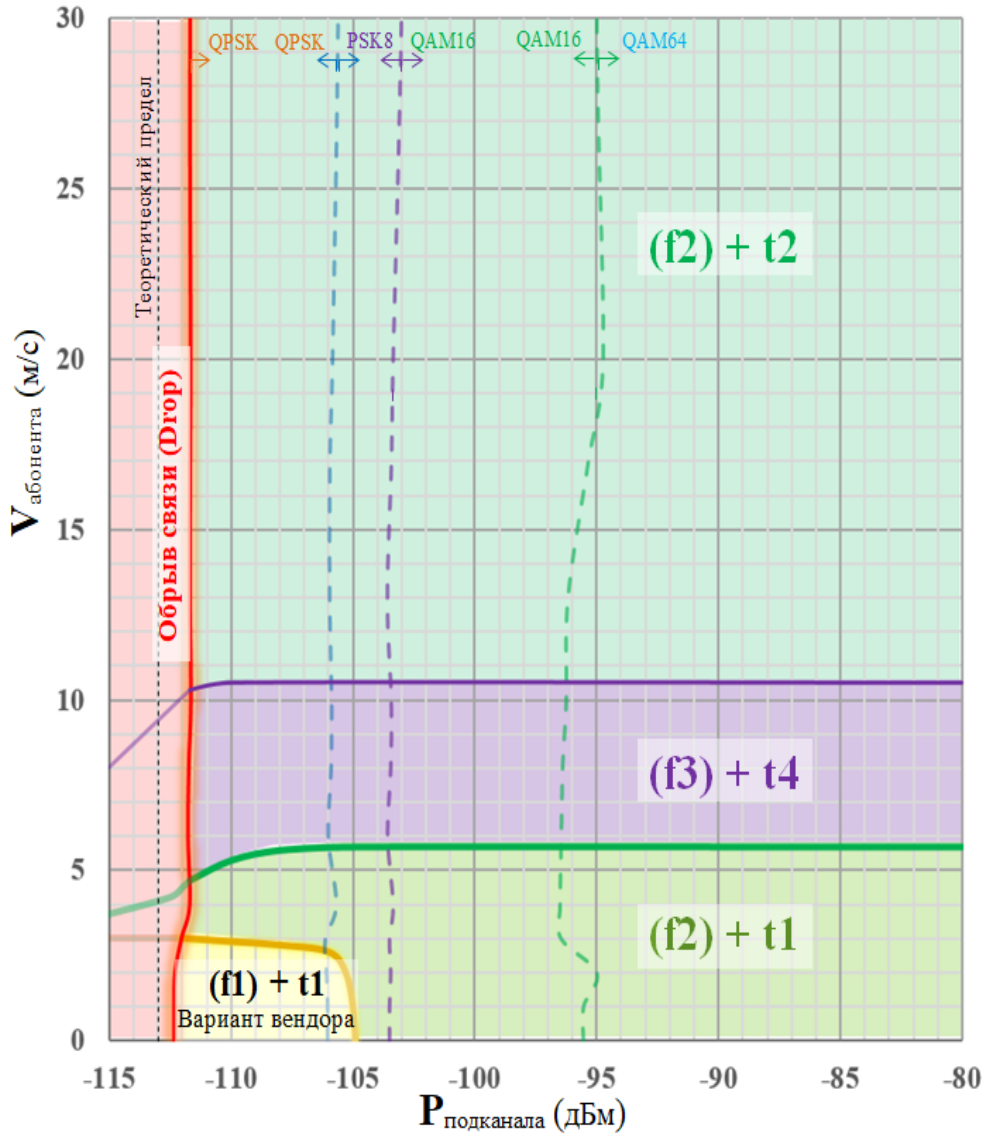


Рисунок 8

Результаты получены при тестировании работы системы МАКВИЛ в диапазоне 340 МГц.

Можно видеть, что точность оценки параметра задержки в условиях многолучевого распространения не улучшаются с ростом уровня сигнала. На рис. 9, аналогично рис. 7, толстыми линиями показаны характеристики алгоритма, выбираемого по расширенной таблице *CQI* (отвечающего кластеру рис. 8), обладающего наилучшими показателями.

На рис. 10 показана мощностно-скоростная плоскость с полученной разбивкой на кластеры для режима оценки-коррекции частотно-селективных искажений радиоканала. В каждом кластере показан тип алгоритма, обеспечивающий в нем наилучшие показатели по точности (минимум относительного уровня остаточных ошибок).

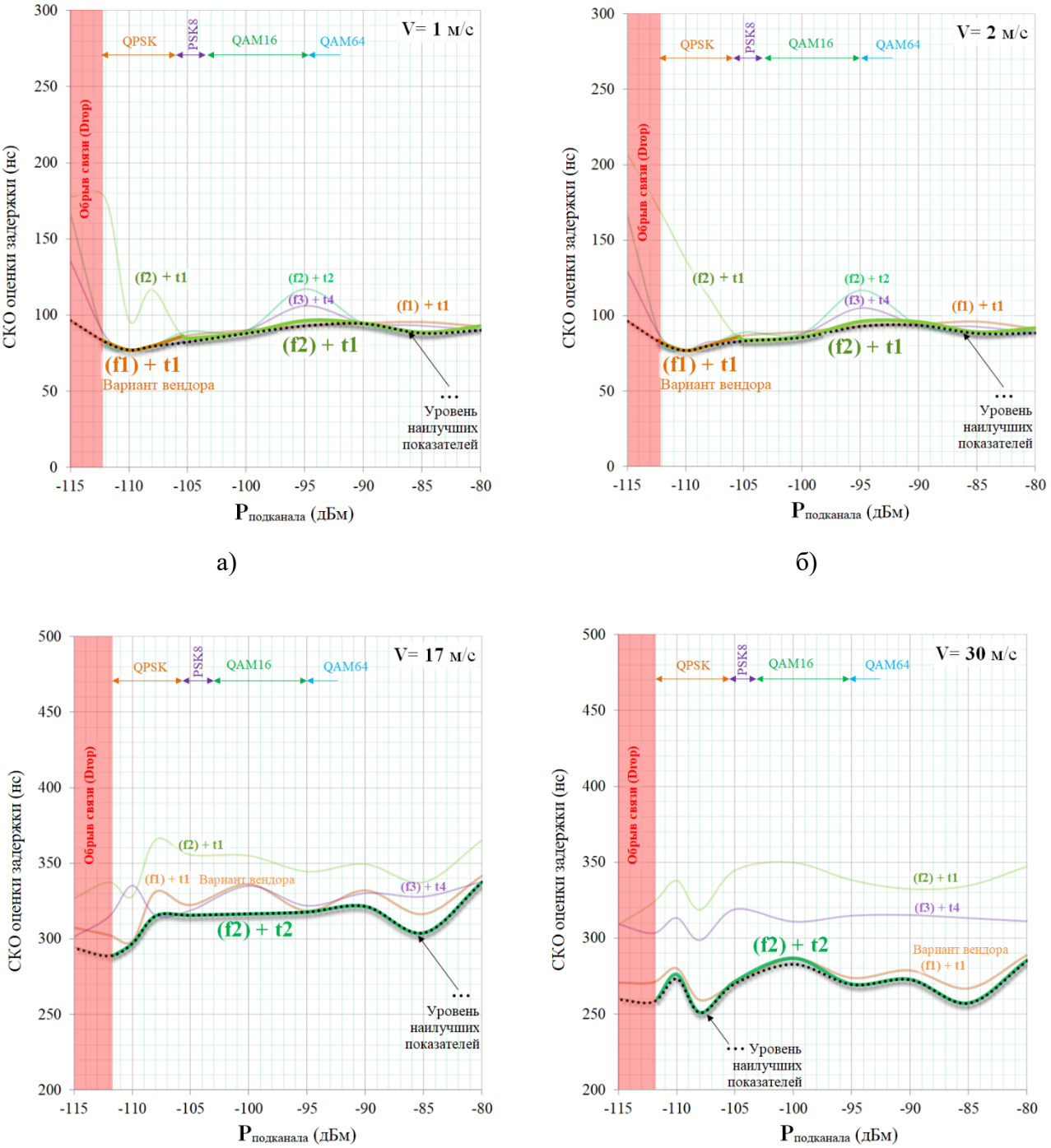


Рисунок 9

Так как показатели точности оценок частотно-селективных искажений демонстрировали зависимость от алгоритмов синхронизации (по задержке и частоте), то тестирование проводилось для всевозможных сочетаний указанных алгоритмов. Используемые алгоритмы оценки частоты и задержки на рис. 10 проставлены в скобках. Нумерация соответствует вышеприведенному описанию. Случаи, помеченные звездочками, показывают то, что без заметной потери качества можно использовать любой вариант алгоритма с цифрой меньше указанной.

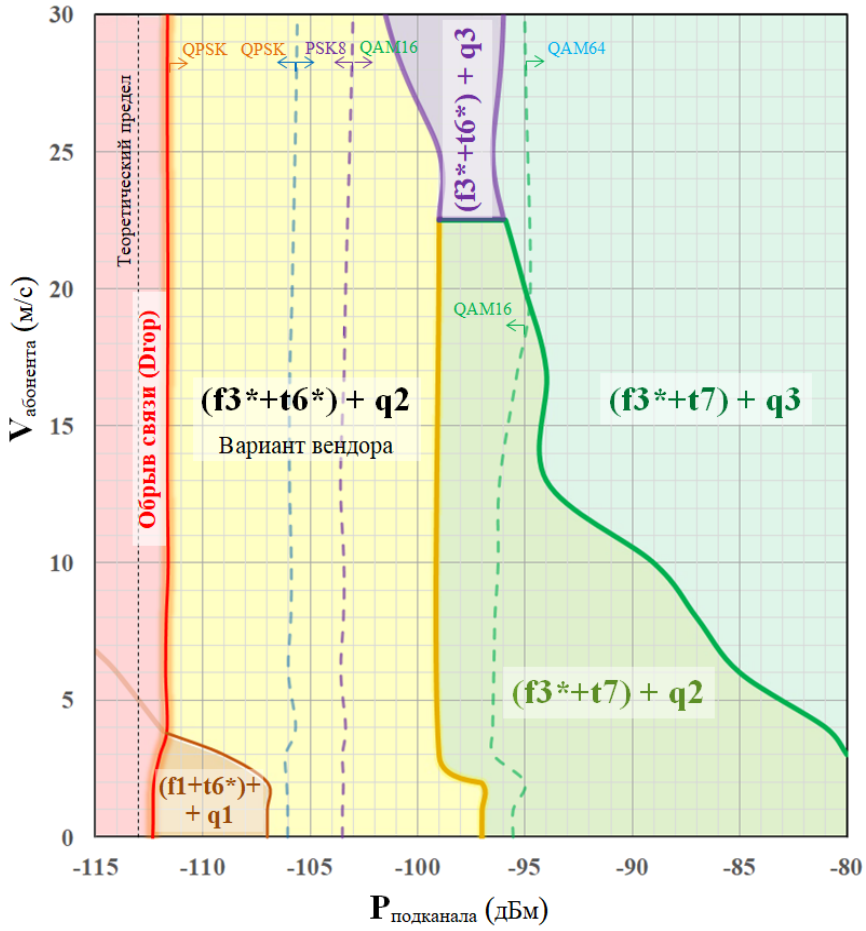
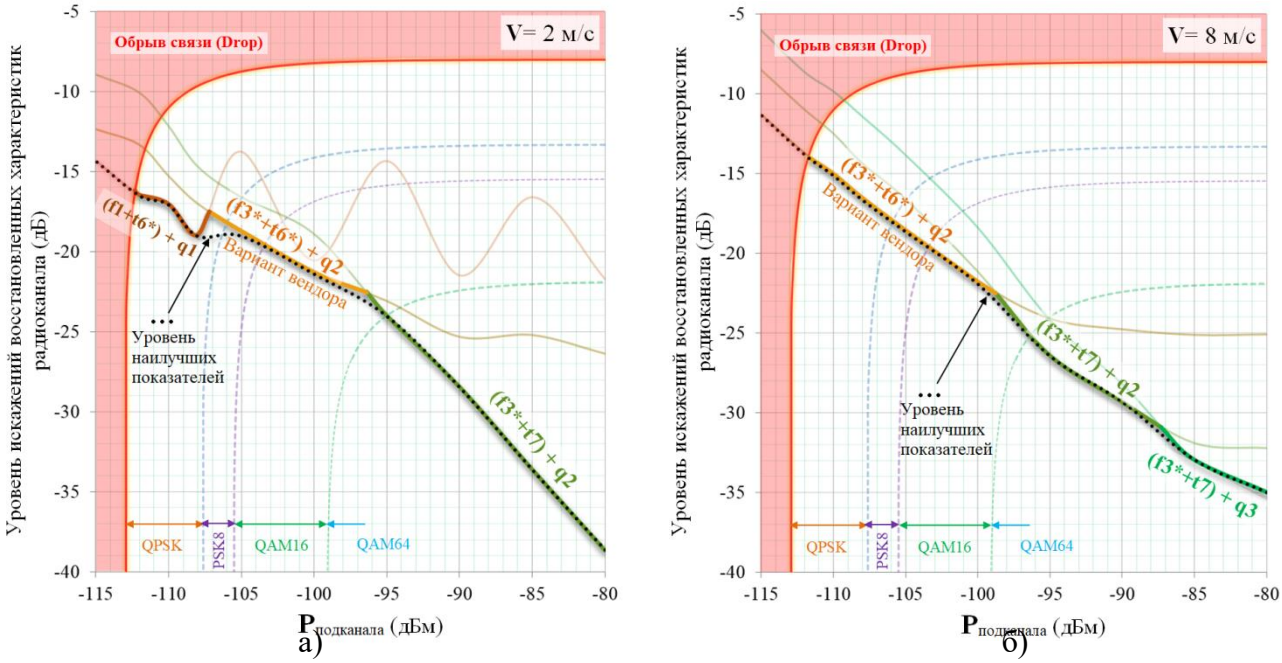


Рисунок 10

При этом отметим, что записанная цифра соответствует варианту алгоритма наименьшей сложности.



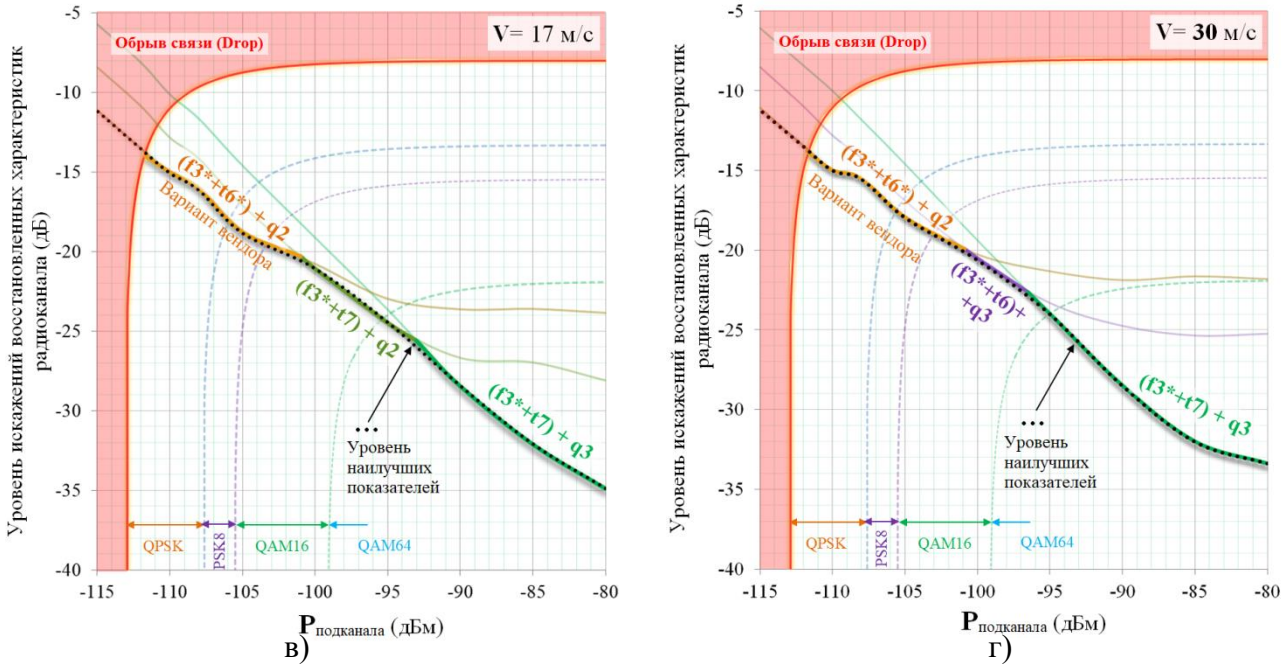


Рисунок 11

На рис. 11а-г для ряда скоростей показаны зависимости относительных ошибок оценок частотно-селективных искажений от уровня сигнала, для наилучших сочетаний алгоритмов. Штриховыми линиями показаны границы применимости различных схем модуляции (*QPSK*, *PSK*8, *QAM*16 и *QAM*64) с учетом остаточных ошибок восстановления радиоканала.

Потенциальные возможности выигрыша от алгоритмов с накоплением более чем на четырех врезках могут составить порядка 0,7 дБ (как видно из данных рис. 11а) и только в случае стационарных абонентов. Для мобильных абонентов усреднение уже на четырех *Pilot*-врезках приносит отрицательный результат.

Алгоритм (*f*3+*t*6) + *q*2, прописанный изначально в документации вендора, демонстрирует наилучшие или близкие к наилучшим показатели только при низких уровнях сигнала (≤-100 дБм). При высоких уровнях приема он значительно уступает вариантам (*f*3+*t*7) +*q*2,3, которые способны обеспечить качество восстановления радиоканала, пригодное даже для использования модуляции *QAM*256.

Алгоритм контроля мобильности

Предложенная методика расширенной таблицы *CQI* предполагает дополнительное использование информации о скорости движения абонента. Нужно отметить, что прямое измерение скорости мобильных абонентов через радиоканал в системах поколения 4*G* не предусматривается. Не составляет исключения и система МАКВИЛ. Поэтому для использования предложенной методики расширенного *CQI* потребовалось найти решение задачи оценки скорости абонента на основе параметров радиоканала, доступных прямым измерениям.

При помощи методов машинного обучения удалось установить, что наиболее значимой корреляционной связью со скоростью движения абонента обладает показатель статистики, формируемой как квадратный корень значения минимума трех оценок дисперсий замеров сдвига частоты, получаемых с помощью алгоритмов *f*1, *f*2 и *f*3, соответственно.

$$\hat{\sigma}_{f\,\min} = \sqrt{\min\left(\hat{\sigma}_{f1}^2, \hat{\sigma}_{f2}^2, \hat{\sigma}_{f3}^2\right)} \ . \qquad (1)$$

Для согласования по абсолютным значениям, при этом, требуется для каждой системы и каждого диапазона подбирать соответствующий масштабный коэффициент длины. Для системы МАКВИЛ, работающей в диапазоне 340МГц, он оказался равным 1,6 м.

На рис. 12 показаны установленные при тестировании зависимости между скоростью движения абонента и умноженным на масштабный коэффициент 1,6 показателем (1) для случаев различных уровней принимаемых сигналов. Интервал формирования выборок в алгоритме вынесения решения, основанном на (1), составлял 12 с (что для МАКВИЛ соответствует 1200 отсчетам). Можно видеть, что начиная со скоростей 10м/с и выше, алгоритм оценки скорости на основе (1) дает точность в пределах 5%. Это вполне пригодно для управления переключениями через расширенные таблицы *CQI* и в полном масштабе поддерживает корректное управление алгоритмом коррекции частотно-селективных замираний на трех границах переключений:

(*f*3*+*t*7)+*q*2 ↔ (*f*3*+*t*7)+*q*3, (*f*3*+*t*6)+*q*3 ↔ (*f*3*+*t*7)+*q*3 и (*f*3*+*t*6*)+*q*2 ↔ (*f*3*+*t*6)+*q*3, показанных зеленой и фиолетовыми линиями на рис. 10.

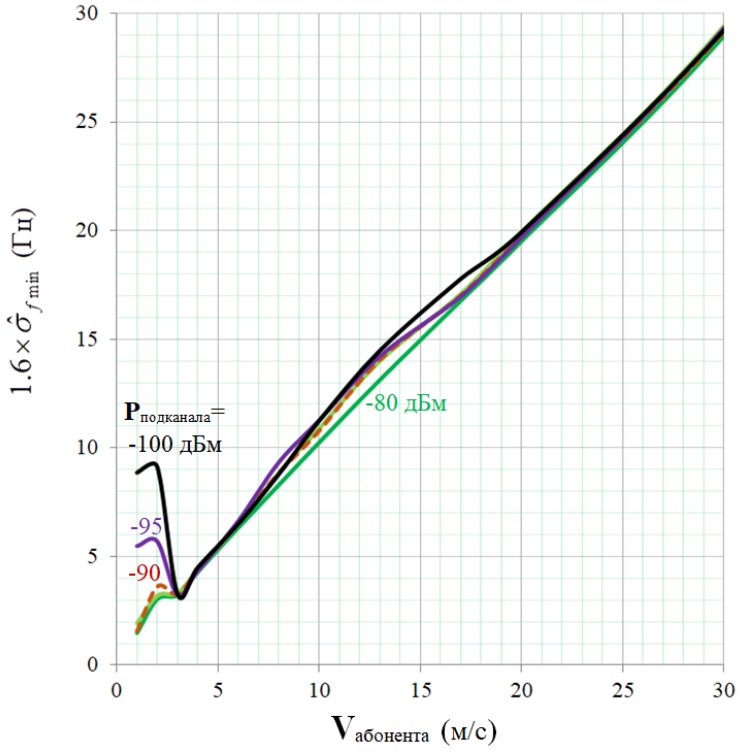


Рисунок 12

Переключение на границе (*f*3*+ *t*6*)+*q*2 ↔ (*f*3*+ *t*7)+*q*2 при скоростях от 3 м/с и выше, также не вызывает вопросов, т.к. указанная граница, показанная светло-коричневым цветом на рис. 10, в указанном диапазоне практически не зависит от скорости. Но при движениях со скоростями до 3 м/с на границах между режимами (*f*1+ *t*6*)+*q*1 ↔ (*f*3*+ *t*6*)+*q*2 и (*f*3*+ *t*6*)+*q*2 ↔ (*f*3*+ *t*7)+*q*2, показанных коричневым и светло-коричневым цветами на рис. 10, могут возникать ошибки, приводящие к заметным потерям. Причиной тому является неоднозначность

оценки скорости, формируемой по показателю мобильности (1). Это можно видеть из рис. 10 по заметному изменению монотонного характера поведения кривых при уровнях ниже -90 дБм. Поэтому для таких случаев пока остается единственная возможность: организация управления переключением с использованием априорных сведений о стационарном типе абонента.

Заключение

Проведенный анализ рабочих субоптимальных алгоритмов оценки параметров сигнала в системе МАКВИЛ показал, что потери по сравнению с оптимальными алгоритмами не превышают 1,5 Дб, т.е. являются весьма приемлемыми. При этом использование алгоритма «(*f*3+*t*6) + *q*2», прописанного изначально в документации вендора, демонстрирует наилучшие или близкие к наилучшим показатели только при уровнях сигнала (≤-100 дБм), а выбранный лучший алгоритм (*f*3+*t*7) +*q*2,3, позволяет даже в самых сложных помеховых условиях вплоть до -112 дБм работать с модуляцией *QAM*64. Из проведенных результатов теста также видно, что движение абонентов со скоростями до 6 м/с в диапазоне 340 МГц практически не оказывает влияние на рабочие характеристики и след таких абонентов можно считать стационарными.

Потенциальные возможности выигрыша от алгоритмов с накоплением более чем на четырех врезках могут составить порядка 0,7 дБ (как видно из данных рис. 11а) и только в случае стационарных абонентов. Для мобильных абонентов усреднение уже на четырех *Pilot*-врезках приносит отрицательный результат.

Литература

1. Стратонович Р.Л. Теория информации. М., «Сов. радио», 1975. – 424 с.
2. Шорин О.А., Бокк Г.О. Снижение негативного влияния высоких значений пик-фактора сигналов в системе McWILL // Экономика и качество систем связи, 2019. – № 1 (11). – С. 9-13.
3. Шорин О.А., Бокк Г.О., Помехоустойчивость системы МАКВИЛ // Электросвязь, 2021. – № 6. – С. 47-54.
4. Бокк Г.О., Аверьянов Р.С., Синхронизация в системах радиосвязи с временным дуплексом // Электросвязь, 2021. – № 6. – С. 32-39.
5. Digital cellular telecommunications system (Phase 2+); Radio transmission and reception// GSM 05.05 version 8.5.1 Release 1999. – 95 p.
6. LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception // 3GPP TS 36.104 version 9.4.0 Release 9 (2010-07). – 98 p.
7. Stefania Sesia, Issam Toufik, Matthew Baker. LTE – The UMTS Long Term Evolution. A John Wiley & Sons, 2011. – p. 752.
8. McWiLL V6 Air Interface Physical Layer Specification (Version 3.0)// Enterprise Standard McWiLL 41.01-v3.0. R&D center released 2012-06-15 implementation. – 123 p.

МЕТОДИКА ИСПОЛЬЗОВАНИЯ МЕЖДУНАРОДНОЙ СТАНДАРТНОЙ МОДЕЛИ ИОНОСФЕРЫ ПРИ ПРОГНОЗИРОВАНИИ ЭНЕРГЕТИЧЕСКИХ ПАРАМЕТРОВ РАДИОЛИНИЙ ДИАПАЗОНА ОЧЕНЬ НИЗКИХ ЧАСТОТ

А.А. Типикин*, к.т.н., НИИ ОСИС ВМФ ВУНЦ ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н.Г. Кузнецова», alextip@mail.ru.*

УДК 621.371.3

Аннотация. Проведено исследование возможности внедрения современных геофизических моделей в методику расчета энергетических параметров радиотрасс. Разработана методика использования вертикальных профилей электронной концентрации, полученных с помощью стандартной модели ионосферы, в волновом методе расчета напряженности поля диапазона очень низких частот. Проведено сравнение результатов расчетов, выполненных с помощью экспоненциальной и стандартной моделей ионосферы, получена количественная оценка различий прогнозов.

Ключевые слова: стандартная модель ионосферы; экспоненциальная ионосфера; электронная концентрация; прогнозирование энергетических параметров; диапазон очень низких частот.

THE METHOD OF THE INTERNATIONAL STANDARD IONOSPHERIC MODEL USAGE FOR THE RADIO LINES ENERGY PARAMETERS FORECASTING IN THE VERY LOW FREQUENCY BAND

Aleksey Tipikin*, candidate of engineering sciences, Research Institute for Operational and Strategic Research of the Navy Development, Military Research and Educational Center of the Navy «Naval Academy named after Admiral of the Fleet of the Soviet Union N.G. Kuznetsov».*

Annotation. In the article, we studied the possibility of introducing modern geophysical models into the methodology for calculating the energy parameters of radio lines. We developed a method for using vertical electron density profiles obtained with the standard ionospheric model in a wave method calculation of the field strength in a very low frequency band. We compared calculation results performed with exponential and standard ionospheric models and estimated quantitative differences in forecasts.

Keywords: international standard ionosphere model; exponential ionosphere; electron density; energy parameters forecasting; very low frequency band.

Введение

Прогнозирование энергетических параметров радиолиний является необходимым этапом при планировании применения систем связи [1, 2]. Точность данных прогнозов напрямую влияет на эффективность применения систем общего и специального назначения [3] и зависит от точности самого метода прогнозирования и качества исходных данных, включающих состояние подстилающей поверхности, состояние ионосферы и геомагнитного поля Земли. В работе [4] оценена степень влияния различных моделей геомагнитного поля Земли на результаты прогнозирования напряженности электрического поля в точке приема. В работах [5, 6] обосновано использование цифровых карт электрических характеристик подстилающей поверхности при прогнозировании энергетических параметров радиотрасс и современных ионосферных моделей. В работах [7, 8] описано использование стандартной модели ионосферы при прогнозировании энергетических параметров радиотрасс диапазона очень низких частот (ОНЧ) скачковым методом.

В настоящее время одним из наиболее распространенных инструментов прогнозирования работы радиолиний ОНЧ диапазона является пакет программ *LWPC*, разработанный в 1980-х гг. [9, 10], который по настоящее время остается одним из наиболее удобных для использования программных пакетов, реализующих волновой метод прогнозирования (метод нормальных волн) [11]. Адекватность прогнозов, полученных с помощью *LWPC,* по-прежнему остается на

высоком уровне и не вызывает сомнения у исследователей, несмотря на использование экспоненциальной модели ионосферы, считающейся устаревшей [12]. В то же время, представляется актуальным вопрос внедрения современных ионосферных моделей в процесс расчета энергетических параметров радиотрасс ОНЧ диапазона и оценка влияния указанных изменений на конечный результат. В этих целях может быть использована стандартная модель ионосферы (*IRI*) [13-15]. Например, на рис. 1 показаны графики зависимости электронной концентрации, полученные с помощью экспоненциальной модели и стандартной модели ионосферы. Из рисунка видны существенные отличия в характере изменения электронной концентрации с высотой по данным разных моделей, что дает основание предполагать об изменении точности прогнозирования при замене ионосферной модели.

Одним из недостатков использования экспоненциальной модели ионосферы является необходимость в априорных знаниях относительно эталонной высоты отражения h' и масштабного коэффициента β. Поэтому в некоторых работах параметры h' и β выбираются таким образом, чтобы вертикальный профиль электронной концентрации над поверхностью Земли согласовывался с оперативными данными ионосферного зондирования [16].

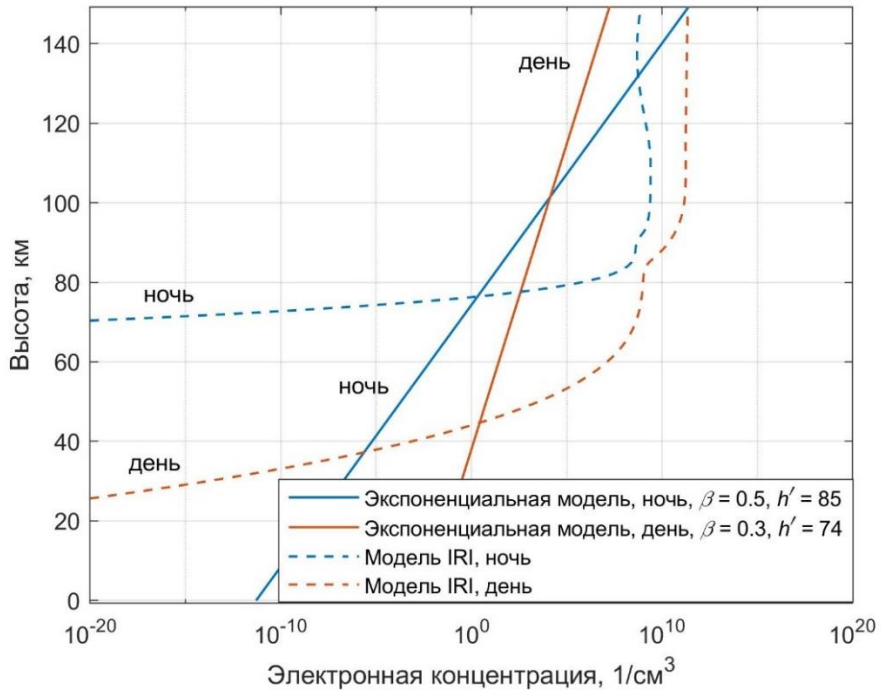


Рисунок 1

IRI является статистической моделью, которая базируется на различных коэффициентах солнечной и геомагнитной активности, а также непосредственно ионосферных индексах. Одним из основных коэффициентов является количество солнечных пятен R, который использовался в начальных версиях *IRI*. В настоящее время применяется годовое скользящее среднее количества солнечных пятен R_{12}. Исследования показали высокую корреляцию между значениями плазменной частоты слоя $foF2$, измеренными с помощью зондов, и R_{12}. Индекс $F10.7$ является измеренным значением потока солнечного излучения на длине волны 10,7 см. В настоящее время используется 81-дневное скользящее среднее и 365-дневное скользящее среднее $F10.7$. Глобальный индекс ионосферного зондирования IG получается путем месячного усреднения результатов сравнения прогнозных значений $foF2$ с измеренными значениями $foF2$. Как и в случае с количеством

солнечных пятен, в *IRI* используется годовое скользящее среднее IG_{12}. Кроме указанных коэффициентов, в модели *IRI* существует возможность корректуры данных по результатам текущих ионосферных измерений [13].

Тем не менее, формирование и внедрение в *LWPC* исходных данных, полученных из *IRI,* осложняется различием в представлении выходных и входных данных *IRI* и *LWPC* соответственно. Таким образом, целью данной статьи является разработка частной методики, обеспечивающей использование данных о состоянии ионосферы, полученных с помощью модели *IRI,* в процессе расчета энергетических параметров радиолиний.

Методика использования модели *IRI* для формирования входных данных при выполнении расчетов напряженности поля ОНЧ диапазона

Для замены ионосферной модели предлагается использовать ввод табличной ионосферы во входных файлах программы *LWPM* с помощью команды управления *range table*. Операция ввода требует создания дополнительных текстовых файлов с расширениями «*ndx*» и «*prf*». Файл типа «*ndx*» является файлом ионосферных индексов, в котором указаны два столбца чисел. В первом столбце вводятся расстояния от передатчика до начала каждого сегмента радиотрассы в км, а во втором – индексы ионосферных профилей NNN, соответствующих данным сегментам, где *NNN* – трехзначный номер индекса. Файл типа «*prf*» является файлом ионосферных профилей, в котором вводится таблица минимум из двух столбцов чисел. В первом столбце указываются высоты в обратном порядке, причем конец таблицы обозначается отрицательной высотой. Во втором столбце указываются данные электронной концентрации или частоты столкновений электронов. Тип вводимых данных во втором столбце таблицы определяется командами *Collision-Frequency-Table* и *Density-table*. С помощью команды *Species* может устанавливаться дополнительное количество заряженных частиц, для которых указываются входные данные. Максимальный аргумент команды равен трем, т.е. вводятся данные для электронов, отрицательных и положительных ионов. В результате должны быть созданы файлы «*fName.ndx*» и «*fNameNNN.prf*», где имя *fName* должно совпадать с именем файла, введенном во входном файле «*inp*» с помощью команды *tx*. Также могут вводиться и другие команды в соответствии с руководством пользователя [17].

Для реализации методики создан скрипт на языке *Matlab*. Блок-схема методики показана на рис. 2.

В соответствии с разработанной методикой входные данные вводятся в структуры *LWPCinput*, *LWPCinput01* и переменную *LWPCpath* (блок 1). В структурах LWPCinput и LWPCinput01 хранятся сведения о рабочей частоте, координатах передатчика, азимутах радиотрасс (или координатах приемников), дата и время выполнения прогноза. В переменную *LWPCpath* вводится путь к программе *LWPM*. Из структуры входных данных *LWPCinput* с помощью вспомогательной функции *MakeLWPCinput* (блок 2) создается входной файл *fileName.inp*, содержащий команды управления программой *LWPM*, а также скрипт операционной системы *fileName.cmd*. Скрипт операционной системы используется для предварительной очистки выходных директорий и запуска *LWPM* с заданным входным файлом (блоки 3 и 4). Результаты расчетов записываются в *SWG*- и *LWF*-файлы в выходных директориях, а также в лог-файл *fileName.log*, причем реальное имя лог-файла определяется командой *tx* в файле *fileName.inp*.

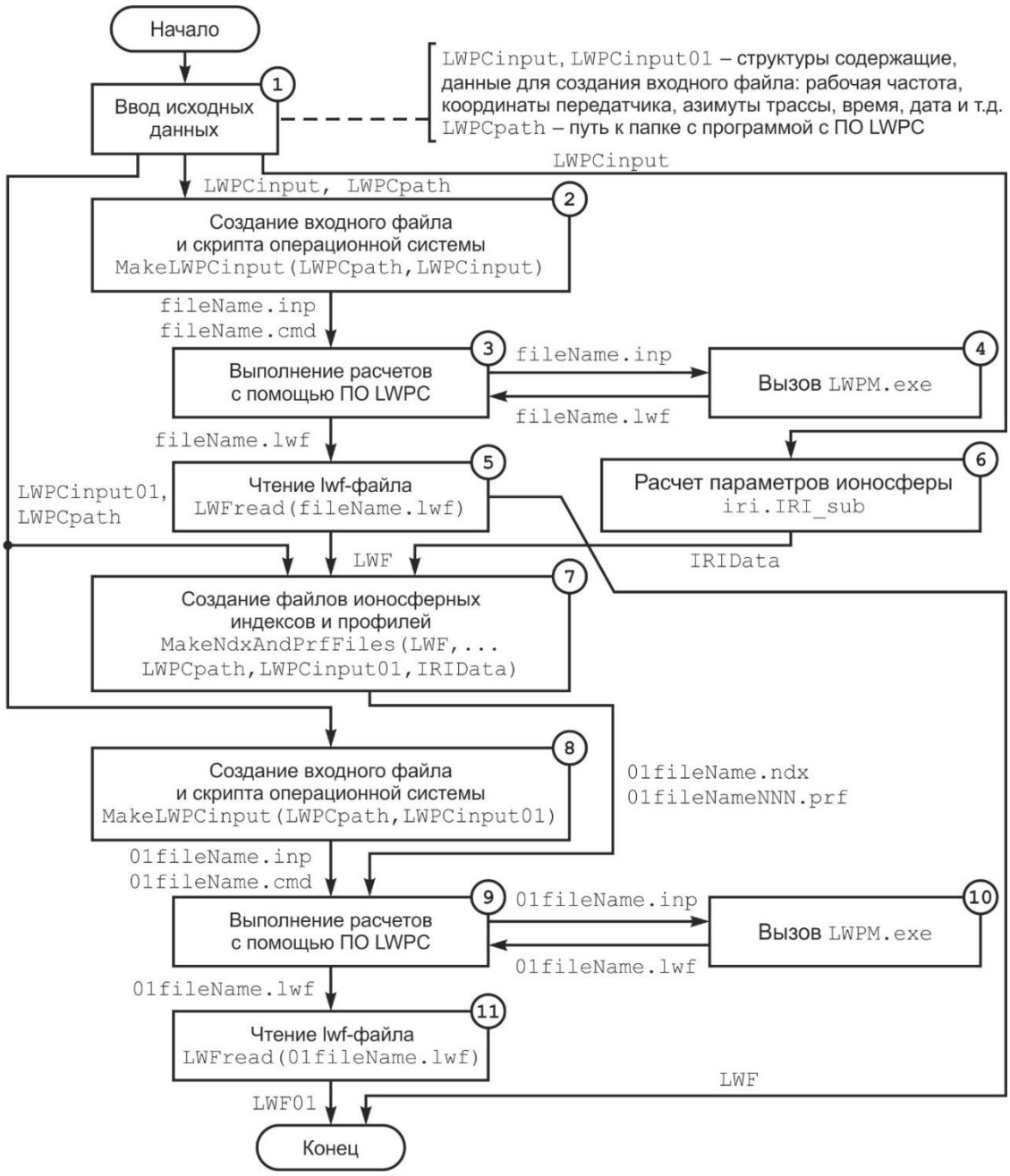


Рисунок 2

С помощью вспомогательной функции *LWFread* из *LWF*-файла извлекаются данные расчетов (блоки 5), которые записываются в структуру *LWF* и используются в блоке 7 для формирования файлов ионосферных индексов типа «*ndx*» и профилей типа «*prf*» с помощью вспомогательной функции *MakeNdxAndPrfFiles*. Также в блок 7 поступает структура *IRIData*, в которой хранятся данные концентрации заряженных частиц в зависимости от высоты, рассчитанные на основе модели *IRI* в блоке 6. Полученные файлы 01*fileName.ndx* и 01*fileNameNNN.prf* поступают в блок 9, куда также вводятся новый входной файл 01*fileName.inp* и скрипт операционной системы 01*fileName.cmd* из блока 8. На основе указанных файлов выполняются новые расчеты путем повторного вызова программы *LWPM* (блоки 9 и 10). После этого в блоке 11 считывается новый *LWF*-файл, данные которого записываются в структуру *LWF*01. Таким образом, в результате работы скрипта формируются две

структуры *LWF* и *LWF*01. В первой структуре данные расчетов базируются на экспоненциальной модели ионосферы, а во второй – на модели *IRI*.

Результаты прогнозирования напряженности электрического поля ОНЧ диапазона

Визуально сравнить эффект от использования разных моделей ионосферы можно на рис. 3, где изображены графики напряженности вертикальной составляющей электрической составляющей поля на частоте 10,2 кГц. Передатчик мощностью 10 кВт расположен в точке с координатами 46.366° с.ш., 98.336° з.д., азимут радиотрассы 240° (рис. 4). Данные для расчетов средствами *LWPC* взяты на 22:00 15 апреля. Данные для расчетов с помощью модели *IRI* взяты на такое же время и дату 2015 г.

Как видно из рис. 3, разница в прогнозируемых значениях напряженности поля может быть существенной и на отдельных участках превышает 10 дБ.

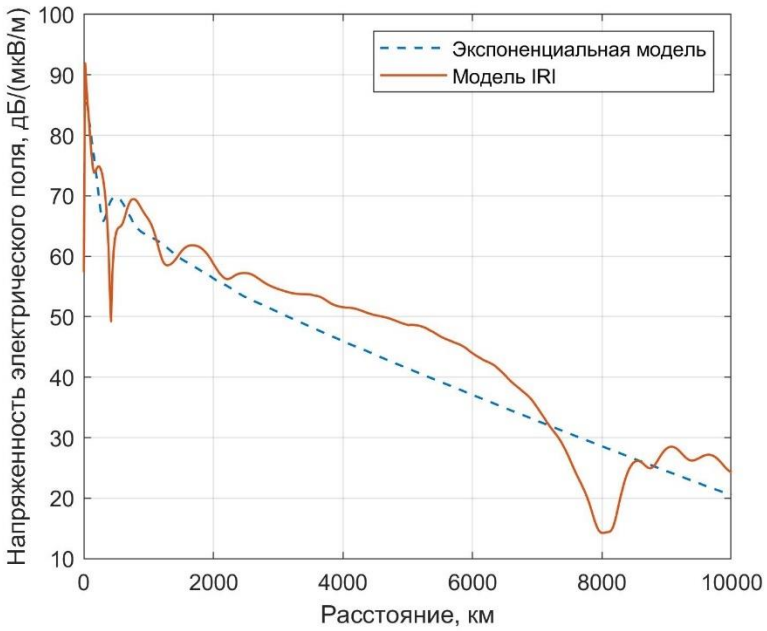


Рисунок 3

Рисунок 4

Для выполнения количественной оценки различий прогнозирования рассчитана разница прогнозов, которая для каждого i-го прогноза, характеризующегося своей совокупностью исходных данных (длина трассы, частота, время и т.д.), вычисляется по формуле [18; 19]:

$$e_i = x_i - y_i, \tag{1}$$

где: $x_i = (x_1, x_2, \ldots, x_N)$ – результаты прогнозирования (вариант 1), а $y_i = (y_1, y_2, \ldots, y_N)$ – результаты прогнозирования (вариант 2).

На рис. 5 показаны разницы прогнозных значений, где абсолютная средняя разница прогнозирования рассчитывается по формуле [20]:

$$MAE = \frac{1}{N}\sum_{i=1}^{N}|e_i|. \tag{2}$$

Здесь N – количество серий расчетов для каждого значения расстояния от передатчика до точки приема. Каждая серия прогнозов получена для тех же исходных данных и азимутов радиотрассы от 0° до 336° с шагом 24°. Графики сглажены путем вычисления скользящего среднего по 50 элементам выборки.

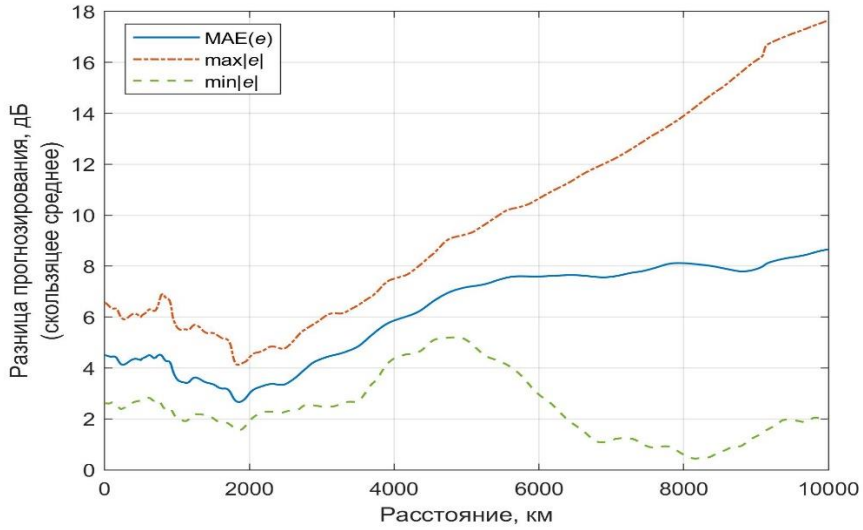


Рисунок 5

Как видно из рисунка, начиная с длины радиотрассы 2000 км, средняя абсолютная разница возрастает и достигает величины приблизительно 8 дБ на расстоянии 10000 км. На достаточно большой выборке результаты, полученные с помощью различных методик расчета, можно рассматривать как две случайные величины. Если основной вклад в результат расчетов при изменении системы входных данных вносит погрешность модели, то обе случайные величины должны иметь одинаковый закон распределения, возможно, с отличающимися математическим ожиданием (МО) и среднеквадратичным отклонением (СКО). Поэтому стандартизированные выборки (нормированные с учетом МО и СКО) должны быть однородными [18; 21]. В противном случае – при наличии существенных различий в результатах, обусловленных изменением системы входных данных, – однородность выборок должна отклоняться статистическими критериями, например, критерием Колмогорова-Смирнова. На рисунке 6 показаны гистограммы стандартизированных выборок, полученных с помощью методик расчета с использованием экспоненциальной модели ионосферы и модели *IRI*.

Однородность выборок отклонена критерием Колмогорова-Смирнова на уровне значимости 5%.

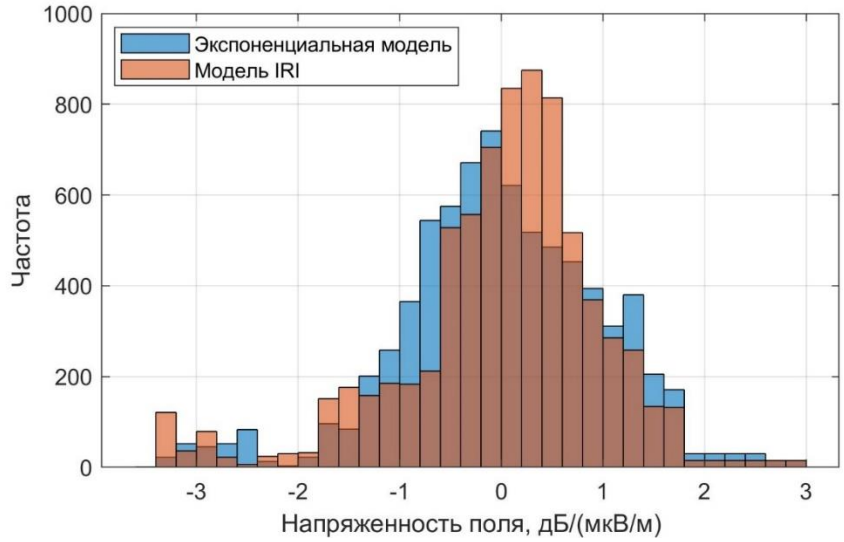


Рисунок 6

Заключение

Таким образом, средняя абсолютная разница прогнозирования возрастает с расстоянием и по всей длине трассы принимает существенные значения приблизительно от 3 до 8 дБ, а также не является следствием случайного различия входных данных. Это означает, что разница прогнозирования действительно обусловлена значимыми различиями в применяемых моделях. Следовательно, применение *IRI* при прогнозировании заметно отразится в точности прогнозов энергетических параметров радиотрасс ОНЧ диапазона, однако данный факт нуждается в дополнительной проверке и сравнении с результатами измерений на реальных радиотрассах.

Литература

1. Cohen M.B., Inan U.S., Paschal E.W. Sensitive Broadband ELF/VLF Radio Reception with AWESOME instrument // IEEE Transactions on Geoscience and Remote Sensing, 2010. – Vol. 48. – № 1. – P. 3-17. DOI:10.1109/TGRS.2009.2028334.
2. Bradley P.A. IRI and VLF/LF radio service planning. // Advances in Space Research, 2001. – № 27. – P. 145-152. DOI:10.1016/S0273-1177(00)00150-2.
3. Шпак В.Ф. Информационные технологии в системе управления силами ВМФ (теория и практика, состояние и перспективы развития). – СПб.: Элмор, 2005. – 832 с.
4. Типикин А.А. Методика использования моделей геомагнитного поля Земли при прогнозировании энергетических параметров радиотрасс диапазона очень низких частот. Сер.: Радиотехнические и инфокоммуникационные системы // Вестник Поволжского государственного технологического университета, 2024. – № 1 (61). – С. 23-34. DOI: 10.25686/2306-2819.2024.1.23, EDN: ELLSQJ.
5. Типикин А.А. Методика формирования глобальных цифровых карт электрических характеристик подстилающей поверхности в диапазоне очень низких частот // Информатика, телекоммуникации и управление, 2022. – Т. 15. – № 1. – С. 7-18. DOI:10.18721/JCSTCS.15101.
6. Типикин А.А., Потапов Д.С., Парафейник Д.В. Результаты исследований по формированию цифровых картографических данных электрических характеристик подстилающей поверхности в диапазоне СДВ // Морской вестник, 2023. – № S1 (16). – С. 27-29.

7. Типикин А.А., Пыков Е.В. Уточненная модель высоты точки отражения для методики прогнозирования энергетических параметров радиотрасс в диапазоне очень низких частот // В книге: Труды всеармейской научно-практической конференции «Инновационная деятельность в ВС РФ», 2023. – С. 15-23.
8. Типикин А.А., Пыков Е.В. Методика определения траекторных параметров радиотрассы ОНЧ диапазона на основе уточненной модели высоты точки отражения // Сборник научных трудов ВУНЦ ВМФ «Военно-морская академия», 2022. – С. 73-81.
9. Ferguson J.A. Longwave Propagation Capability; Full FORTRAN Release: Version 1.0. TD 1847 – San Diego: Naval Ocean Systems Center, 1990.
10. Ferguson J.A. Computer Programs for Assesment of Long Wavelength Radio Communications; Version 1.1: User's Guide and Source Files. TD 2394 – San Diego: Naval Command, Control and Ocean Surveillance Center. RDT&E Division, 1993.
11. Макаров Г.И., Новиков В.В., Рыбачек С.Т. Распространение радиоволн в волноводном канале Земля-ионосфера и в ионосфере. – М.: Наука, 1994. – 152 с.
12. Gasdia F., Marshall R.A. A new longwave mode propagator for the Earth-ionosphere waveguide // IEEE Transactions on Antennas and Propagation, 2021. DOI:10.1109/TAP.2021.3083753.
13. Bilitza D. IRI the international standard for the ionosphere // Adv. Radio Sci., 2018. – № 16. – P. 1-11. DOI:10.5194/ars-16-1-2018.
14. Fron A., Galkin I., Krankowski A., Bilitza D., Hernandez-Pajares M., Reinisch B., Li Z., Kotulak K., Zakharenkova I., Cherniak Iu., Dollase D. R., Wang N., Flisek P., Garcia-Rigo A. Towards cooperative global mapping of the ionosphere: fusion feasibility for IGS and IRI with global climate VTEC maps // MDIP Remote Sens, 2020. – № 12 (21). – P. 3531. DOI:10.3390/rs12213531.
15. Galkin I., Fron A., Reinisch B., Hernandez-Pajares M., Krankowski A., Nava B., Bilitza D., Kotulak K., Flisek P., Li Z., Wang N., Dollase D. R., Garcia-Rigo A., Batista I. Global monitoring of ionospheric weather by GIRO and GNSS data fusion // Atmosphere, 2022. – № 13. – P. 371. DOI:10.3390/atmos13030371.
16. Ахметов О.И., Мингалев И.В., Мингалев О.В., Белаховский В.Б., Суворова З.В. Распространение электромагнитных волн в области высоких широт при различном состоянии ионосферы на частотах системы точного времени «Бета» // Известия РАН. Серия физическая, 2021. – Т. 85. – С. 315-320. DOI: 10.31857/S0367676521020034.
17. Ferguson J.A. Computer Programs for Assessment of Long-Wavelength Radio Communications, Version 2.0. User's Guide and Source Files. Technical Document 3030. TD 3030 – San Diego: Space Naval and Systems Center, 1998.
18. Гнатюк В.И. Закон оптимального построения техноценозов: Монография. – Калининград: Издательство КИЦ «Техноценоз», 2019. – 940 с.
19. Дорофеев С.А., Кивчун О.Р., Прохода А.Н. Оценка реализации потенциала энергосбережения при эксплуатации объектов военной инфраструктуры // Известия Тульского государственного университета. Технические науки, 2018. – № 1. – С. 267-274.
20. Hora J., Campos P. A review of performance criteria to validate simulation models // Expert Systems, 2015. – Vol. 32. – № 5. – P. 598-595. DOI:10.1111/exsy.12111.
21. Лапшов Д.Я., Когновицкий О.С. Статистические особенности канала связи с морским подвижным объектом // В книге: Актуальные проблемы инфотелекоммуникаций в науке и образовании. III Международная научно-техническая и научно-методическая конференция: сборник научных статей, 2014. – С. 264-268.

ИНФОРМАЦИОННЫЕ СИСТЕМЫ, СЕТИ И ТЕХНОЛОГИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ

ОЦЕНКА И КОМПЕНСАЦИЯ ПОГРЕШНОСТИ СИНХРОНИЗАЦИИ БАЗОВЫХ СТАНЦИЙ ПРИ ПОЗИЦИОНИРОВАНИИ ПОЛЬЗОВАТЕЛЬСКИХ УСТРОЙСТВ

Г.А. Фокин, *д.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, grihafokin@gmail.com;*
К.Е. Рютин, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, ryutin.sut@gmail.com.*

УДК 621.396.969

Аннотация. Разностно-дальномерный метод позиционирования пользовательских устройств требует жесткой временной и частотной синхронизации источников навигационных сигналов. В данном исследовании описан лабораторный эксперимент по оценке и компенсации погрешности синхронизации базовых станций при позиционировании пользовательских устройств.

Ключевые слова: *4G; LTE; SDR;* синхронизация; позиционирование.

ESTIMATION AND COMPENSATION OF BASE STATION SYNCHRONIZATION ERROR DURING POSITIONING OF USER DEVICES

Grigoriy Fokin, *Doctor of Science, assistant professor, St. Petersburg State University of Telecommunications n/a prof. M.A. Bonch-Bruevich;*
Konstantin Ryutin, *St. Petersburg State University of Telecommunications n/a prof. M.A. Bonch-Bruevich.*

Annotation. The range-difference method of positioning user equipment requires strict time and frequency synchronization of navigation signal sources. This study describes a laboratory experiment on estimation and compensation of base station synchronization error during positioning of user equipment.

Keywords: *4G; LTE; SDR;* synchronization; positioning.

Введение

Актуальность задачи позиционирования пользовательских устройств (*UE – User Equipment*) в инфраструктуре сетей беспроводной связи [1-3] обусловлена проблемой стабильного приема сигналов глобальных навигационных спутниковых систем (ГНСС) в условиях плотной городской застройки и внутри помещений. Использование сигналов базовых станций стандартов *LTE* (*Long Term Evolution*) *eNodeB* (*eNB*) [4] и 5*G NR* (*New Radio*) *gNodeB* (*gNB*) [5] может помочь преодолеть эту проблему и повысить точность определения местоположения *UE*.

Целью исследования, результаты которого отражены в статье, является разработка подсистемы синхронизации базовых станций (*eNB – eNodeB*) для задачи повышения точности определения местоположения (ОМП) пользовательских устройств (*UE – User Equipment*) в сети стандарта *LTE* (*Long-Term Evolution*).

В стандартах *LTE* [6] и 5*G* [7] специфицирован метод позиционирования по разности времен приема (*OTDOA – Observed Time Difference Of Arrival*) опорных

сигналов позиционирования (*PRS – Positioning Reference Signal*) [8]. Предыдущие разработки технологии сетевого позиционирования на основе программно-определяемого радио (*SDR – Software-Defined Radio*) показали, что передача [9] и прием [10] опорных сигналов сот (*CRS – Cell-Specific Reference Signal*) позволяют достичь дециметровой точности определения местоположения *UE*. Однако, лабораторные [11] и полевые [12] испытания показали, что достигнутая точность сильно зависит от идеальной временной и частотной синхронизации источников навигационных сигналов *eNB*. Если для задач связи восстановление *MIB* (*Master Information Block*) [13] требует синхронизации до одного субкадра длительностью 1 мс, то для задач навигации ошибка синхронизации, равная 1 нс, приводит к ошибке определения местоположения *UE*, равной 0,3 м. Проблема высокоточной временной синхронизации беспроводных устройств связи и навигации также была тщательно исследована в работах [14-20].

Материал данной статьи сформирован следующим образом: во втором разделе приводится описание идеальной подсистемы синхронизации, используемой при проведении полевых испытаний; в третьем – приводится описание подсистемы синхронизации, работающей по протоколу *PTP*; в четвертом – приводится описание метода компенсации погрешности синхронизации опорным приемником сигналов стандарта *LTE*; в последнем разделе приводится экспериментальная апробация описанного метода компенсации погрешности синхронизации в лабораторных условиях.

Описание идеальной подсистемы синхронизации

В ходе проведения полевых испытаний использовалась подсистема синхронизации *eNB*, состоящая из сервера точного времени «Метроном-*PTP*-1*U*-*V*2» [21] и транслятора [22] «Метроном-Т» производства компании Метротек. При данном подходе выходы сигналов временной и частотной синхронизации 1 *PPS* и 10 МГц сервера точного времени подключаются коаксиальными кабелями [23] к соответствующим входам транслятора, а уже с него раздаются на четыре макета *eNB* [12]. То есть, *eNB* синхронизированы от одного источника.

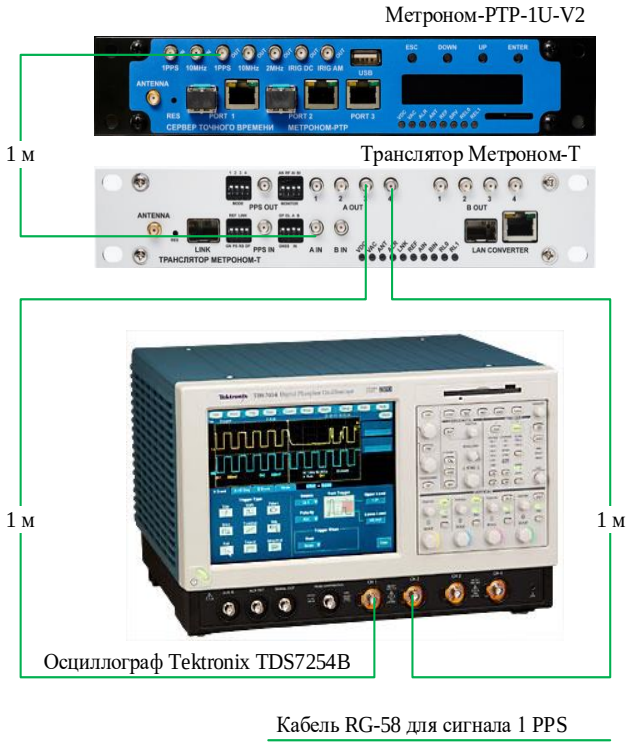


Рисунок 1

При анализе на осциллографе [24] двух каналов сигнала 1 *PPS* транслятора, фронты импульсов синхронизации отстоят друг от друга меньше, чем на 100 пс, что позволяет использовать данную подсистему синхронизации в качестве эталонной, с которой можно сравнивать все последующие решения в данном направлении работ. На рис. 1-3 приводятся схема, фотография и осциллограмма измерения относительного сдвига фронтов двух сигналов 1 *PPS* транслятора Метроном-Т, соответственно. На рис. 3 цена деления шкалы времени равна 500 пс/дел (крупные клетки).

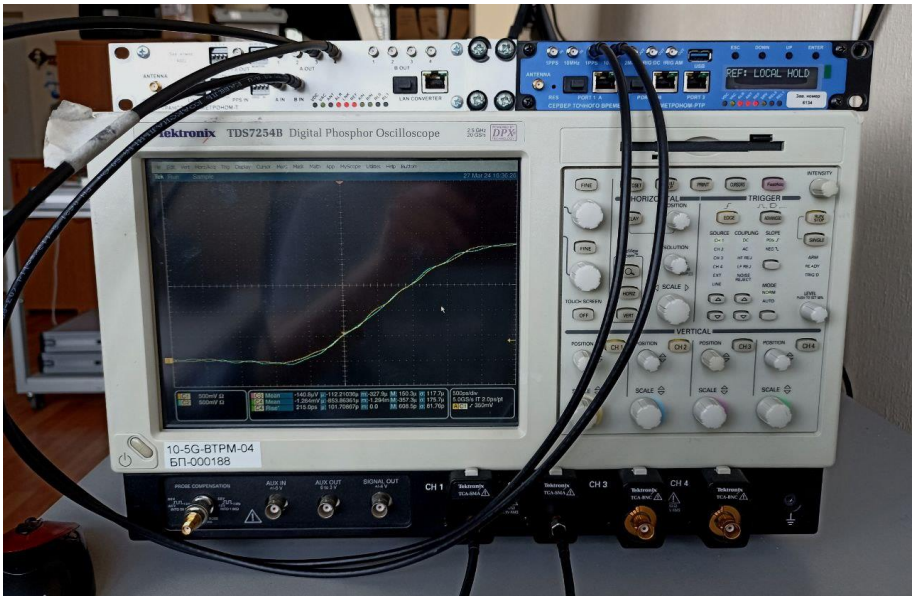


Рисунок 2

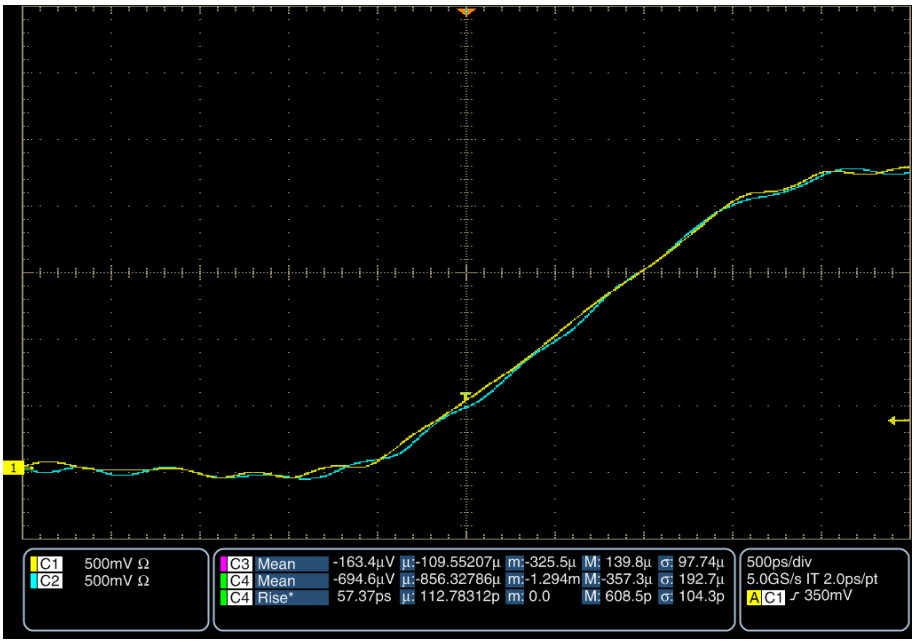


Рисунок 3

Для оценки влияния погрешности синхронизации на точность ОМП при использовании эталонной подсистемы синхронизации выходы сигналов 1 *PPS* и 10 МГц транслятора подключались к соответствующим входам двух макетов *eNB*, далее происходили синхронизация и запуск *eNB* на передачу сигнала стандарта *LTE*. Сигналы с двух макетов *eNB* объединялись в сумматоре [25], выход которого был подключен ко входу приемного канала макета *UE*. Для конфигурации и

запуска макетов *eNB* и *UE* они были подключены в общую локальную сеть через сетевой коммутатор [26]. После приема сигнала стандарта *LTE* макетом *UE* выполнялась оценка разности расстояний между макетами *eNB* и данным местоположением макета *UE*. Эквивалентом расстояний между каждой *eNB* и *UE* в данном эксперименте являются коаксиальные кабели разной длины (5 и 2 метра), по которым сигнал *LTE* передается от *eNB* к *UE*. Следовательно, ожидаемая разность расстояний Δd, измеренная на стороне *UE*, равна $\Delta d = d_{eNB2} - d_{eNB1} = 5\text{ м} - 2\text{ м} = 3\text{ м}$. На рис. 4 изображена схема тестирования эталонной подсистемы синхронизации.

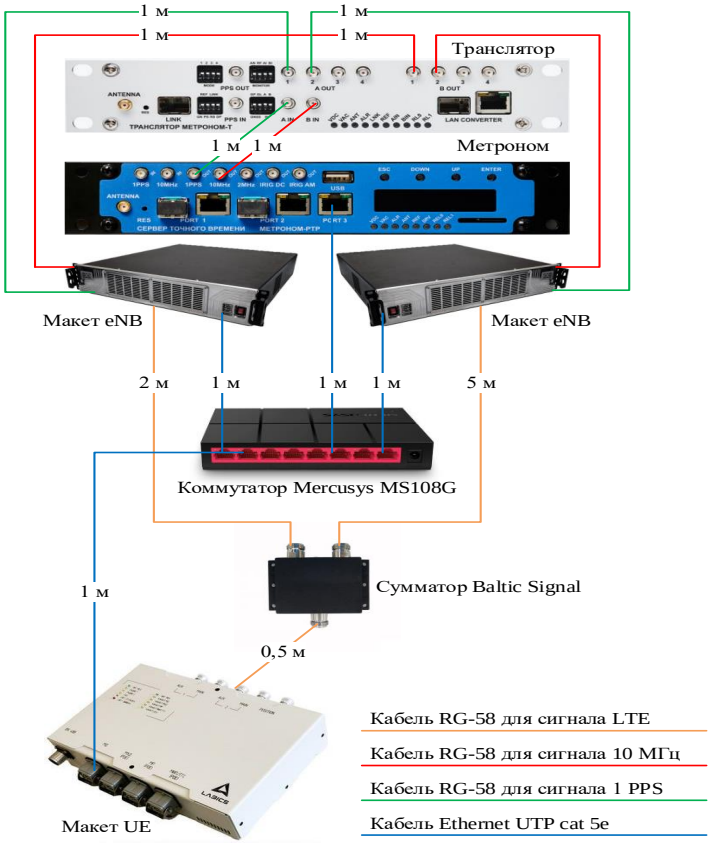


Рисунок 4

Вследствие выполнения описанных процедур был получен ожидаемый результат на графике разностей расстояний для двух макетов *eNB* (рис. 5).

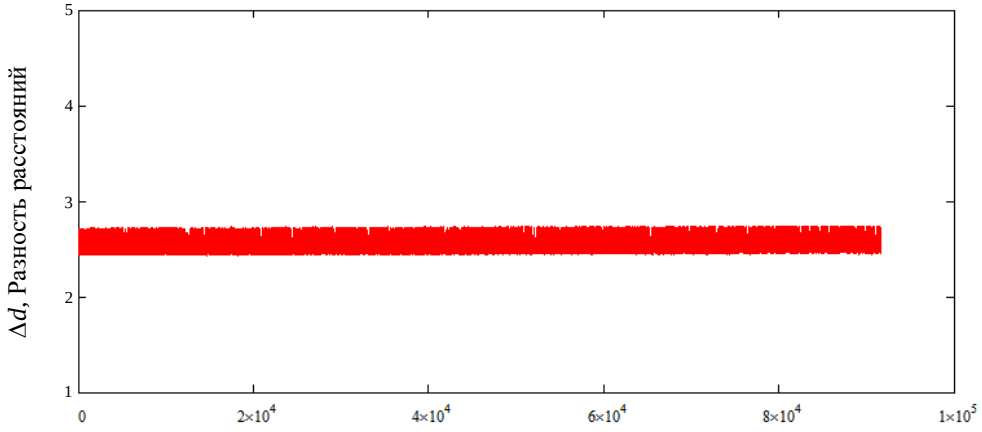


Рисунок 5

Анализ приведенного выше графика показывает, что вычислительная погрешность метода измерений [10] в сумме с приборной погрешностью трансивера (толщина линии) при использовании эталонной подсистемы синхронизации постоянна и составляет примерно ±15 см, а погрешность синхронизации на продолжительном интервале времени отсутствует, что очевидно следует из постоянства среднего значения оценок разностей расстояний (рис. 5).

Однако, затухание в радиоканале делает невозможным стабильный прием сигналов синхронизации в контексте использования данной подсистемы на реальной сети мобильной связи, где *eNB* отстоят друг от друга на сотни метров. Следовательно, о доступности и точности услуги позиционирования при использовании такого подхода говорить не приходится.

Описание подсистемы синхронизации по протоколу *PTP*

Далее была выполнена проверка возможности синхронизации нескольких метрономов (по числу *eNB*) по сетевому протоколу синхронизации *PTP* (*Precision Time Protocol*) с точностью до единиц наносекунд. В такой подсистеме один метроном, установленный на опорной *eNB*, выступает ведущим (*Master*), а все остальные метрономы, установленные на соответствующих *eNB*, выступают в роли ведомых (*Slave*). Ведущий и ведомый метрономы соединялись между собой *Ethernet* патчкордом, а также для контроля и настройки подключались в локальную сеть через сетевой коммутатор. В ходе измерения на осциллографе сдвига фронтов двух сигналов 1 *PPS* с ведущего и ведомого метрономов, синхронизированных по протоколу *PTP*, удалось получить синхронизацию с точностью примерно 2,5 нс [27]. На рис. 6 и рис. 7 приводятся схема и осциллограмма измерения относительного сдвига фронтов двух сигналов 1 *PPS* с ведущего и ведомого метрономов. На рис. 7 цена деления шкалы времени равна 1,25 нс/дел. (крупные клетки).

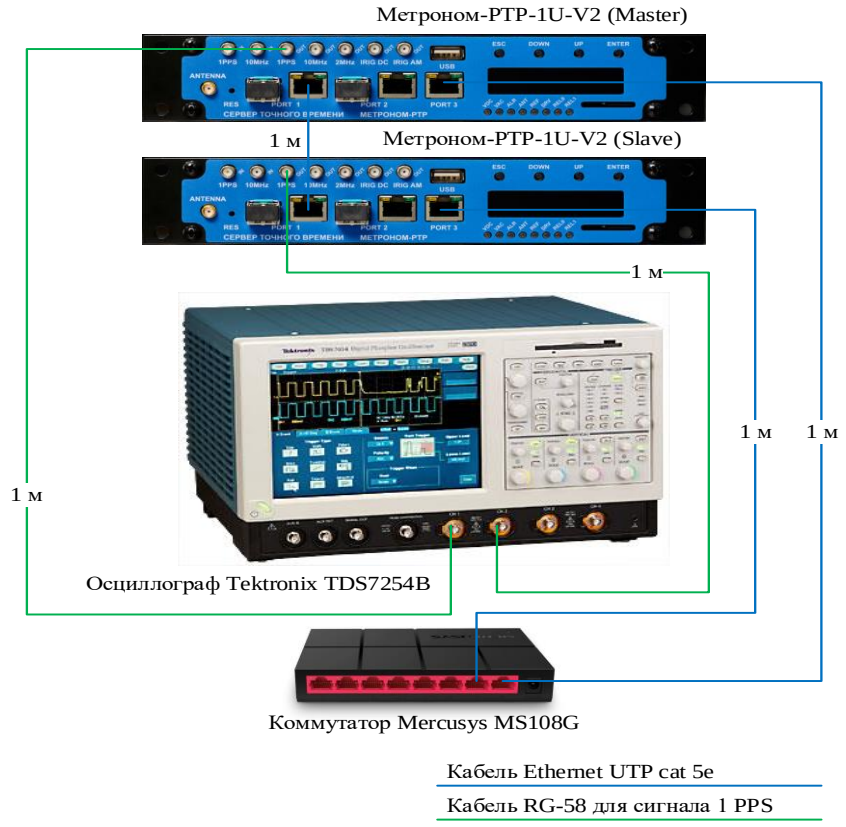


Рисунок 6

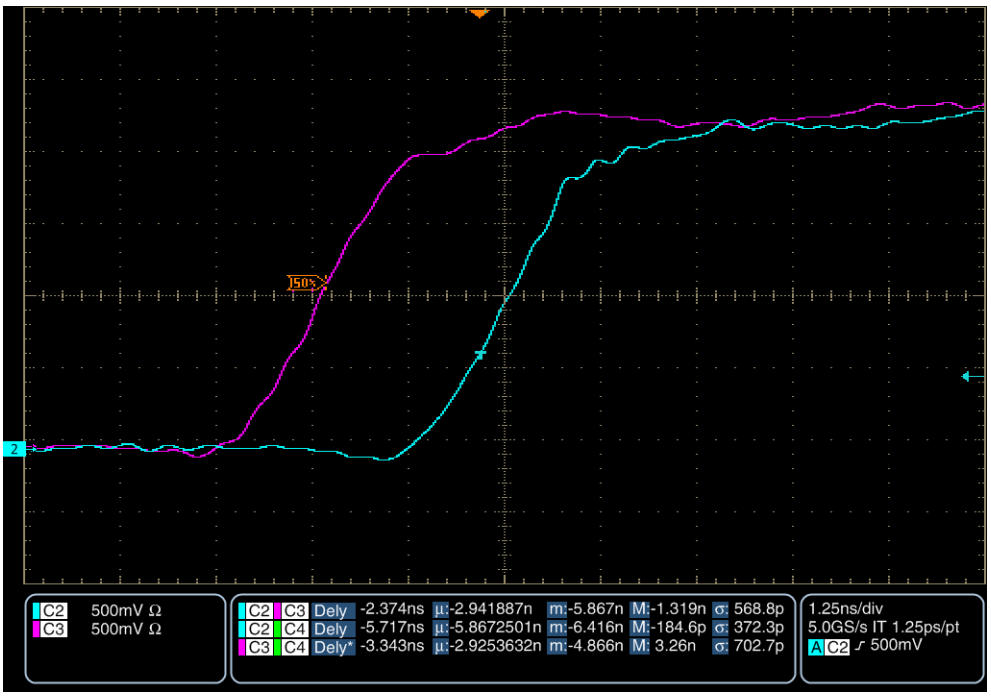


Рисунок 7

Однако в ходе длительного (12,5 час) наблюдения осциллограф зафиксировал плавный сдвиг фронта сигнала 1 *PPS* ведомого метронома относительно фронта соответствующего сигнала ведущего метронома в пределах 10 нс (рис. 8). Данное свойство уменьшает точность оценки координат *UE*.

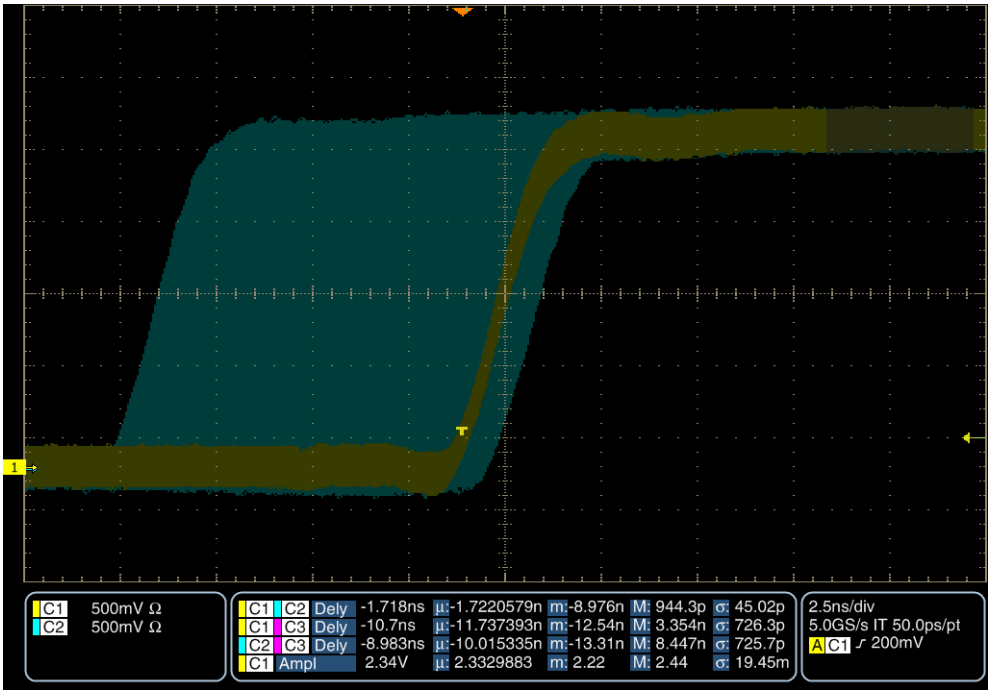


Рисунок 8

Для оценки влияния погрешности синхронизации на точность ОМП при использовании системы синхронизации метрономов по протоколу *PTP* была собрана схема, изображенная на рис. 9. Она отличается от схемы на рис. 4 заменой транслятора ведомым метрономом и конфигурацией обоих метрономов на работу в режиме *PTP* (для этого первые *Ethernet*-порты коммутируются патчкордом). На

рис. 10 представлен график разностей расстояний для двух макетов *eNB* при использовании подсистемы синхронизации по протоколу *PTP*.

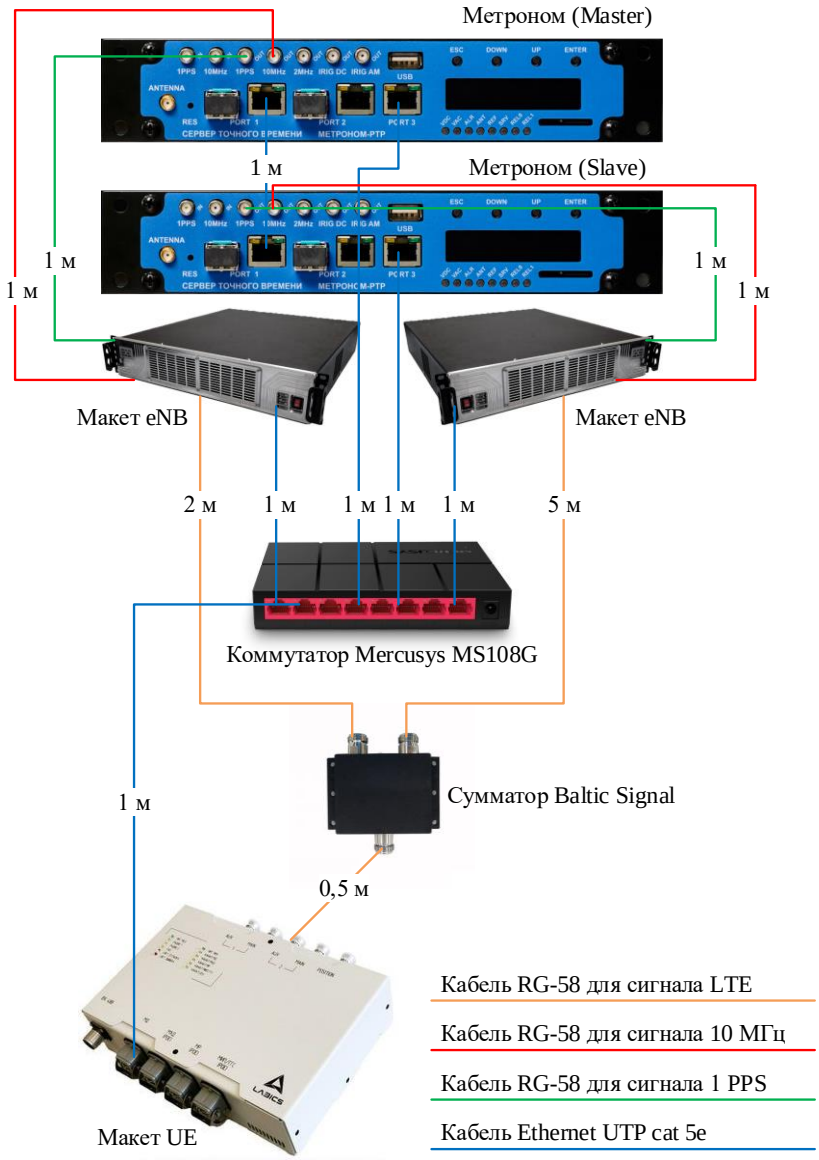


Рисунок 9

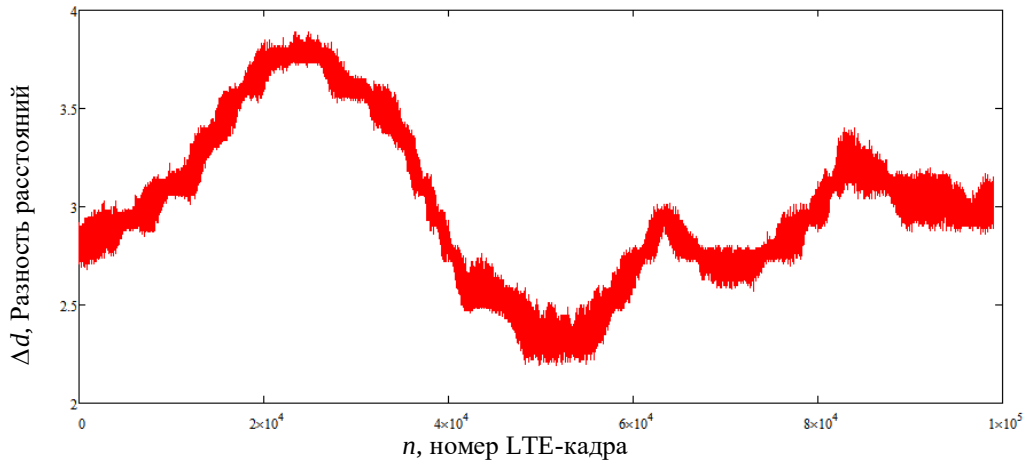


Рисунок 10

Анализ приведенного выше графика показывает, что вычислительная погрешность метода измерений [10] в сумме с приборной погрешностью трансивера (толщина линии) при использовании системы синхронизации метрономов по протоколу *PTP* равна погрешности при использовании эталонной системы синхронизации (рис. 5). Однако, если применить к данной последовательности отсчетов алгоритм скользящего среднего (или фильтр нижних частот), то можно заметить, что разности расстояний изменяются согласно некоторому неизвестному закону. Это изменение является погрешностью синхронизации, которая составляет в данном случае примерно ±0,75 м.

Компенсация погрешности синхронизации опорным приемником

В целях компенсации погрешности синхронизации в описанную [12] систему позиционирования вводится опорный приемник. Он является фиксированным элементом инфраструктуры системы позиционирования, следовательно, разности расстояний от пар *eNB* в данном местоположении опорного приемника должны быть детерминированными и постоянными. На стороне драйвера трансиверов *eNB* реализована возможность сдвига сигнала во времени с шагом 1 пс, при этом величина необходимого временного сдвига передается от опорного приемника к соответствующей *eNB* по *TCP*-сокету. Эта величина вычисляется таким образом, чтобы скомпенсировать отличие оценок разностей расстояний от детерминированного значения в данном местоположении опорного приемника. Схема работы алгоритма учета временных поправок приведена на рис. 11.

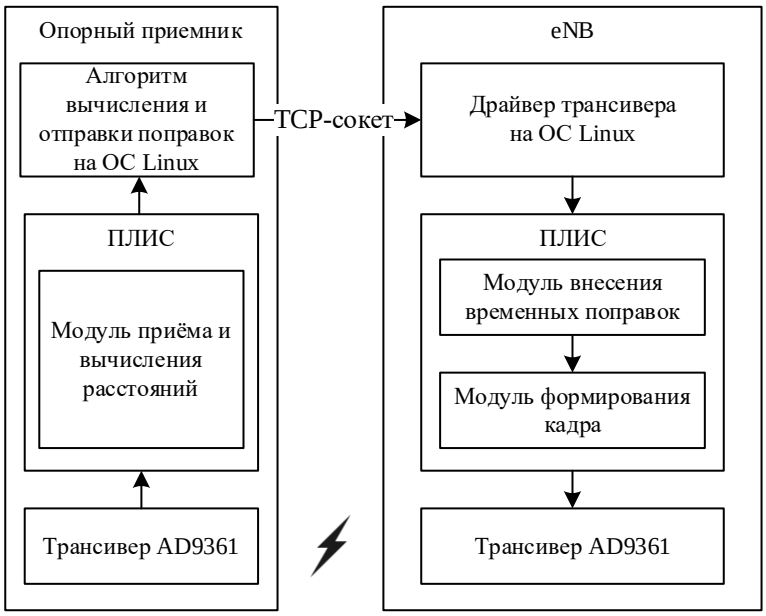


Рисунок 11

Экспериментальная апробация алгоритма компенсации

Экспериментальная апробация алгоритма компенсации погрешности синхронизации передатчиков *eNB* заключалась в задании ожидаемой разности расстояний на стороне опорного приемника (в данном эксперименте им выступает макет *UE* на рис. 9), отправки соответствующей этой разности расстояний временной поправки на *eNB* по *TCP*-сокету и наблюдении изменения величины разности расстояний на стороне опорного приемника. Схема эксперимента аналогична схеме на рис. 9. В данном эксперименте в алгоритме компенсации погрешности синхронизации была задана ожидаемая разность расстояний $\Delta d = 3$ м.

На рис. 12 приведены графики разностей расстояний до и после применения алгоритма компенсации погрешности синхронизации.

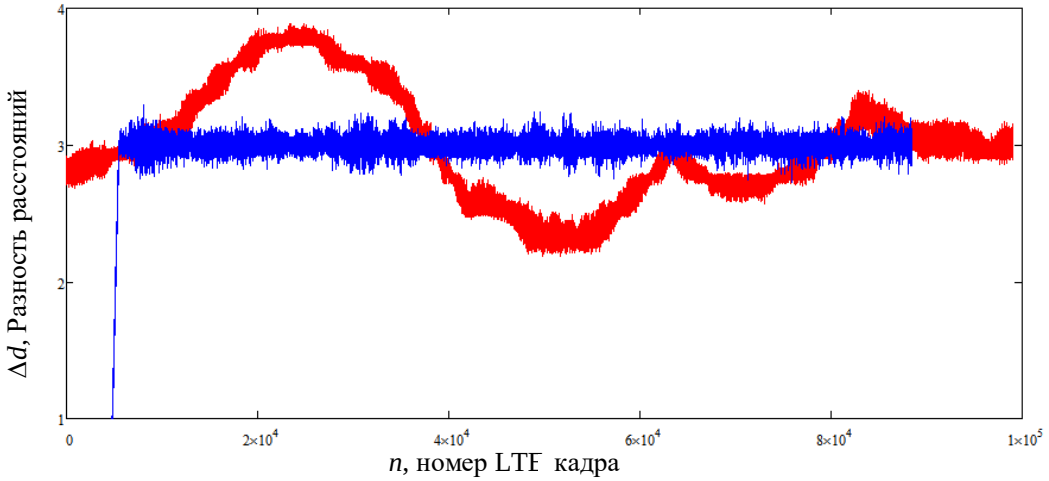


Рисунок 12

Из анализа рис. 12 очевидно следует, что применение алгоритма компенсации позволяет добиться точности синхронизации передатчиков *eNB*, которая сопоставима с синхронизацией от одного источника (рис. 5).

Заключение

В ходе проведения данного исследования была произведена оценка погрешности синхронизации, которую вносят серверы точного времени Метроном-*PTP*-1*U*-*V*2 в алгоритм приема и первичной обработки системы сетевого позиционирования *LTE*. Также был описан и экспериментально апробирован метод компенсации данной погрешности с использованием алгоритма автоматической временной подстройки передатчиков *eNB* опорным приемником путем отправки временного сдвига по *TCP*-сокету.

Литература

1. Zekavat R., Buehrer R.M. Handbook of position location: Theory, practice and advances, 2nd Edition. John Wiley & Sons, 2019.
2. Campos R.S., Lovisolo L. RF Positioning: Fundamentals, Applications, and Tools. Artech House, 2015.
3. Sand S., Dammann A., Mensing C. Positioning in Wireless Communications Systems. John Wiley & Sons, 2014.
4. Fischer S. Observed time difference of arrival (OTDOA) positioning in 3GPP LTE, Qualcomm White Paper, San Diego, CA, USA, Jul. 2014.
5. Fischer S. «5G NR positioning» in 5G and Beyond. Springer International Publishing, Mar. 2021, ch. 15.
6. 3GPP TS 36.214 V17.0.0 (2022-03) Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer; Measurements (Release 17).
7. 3GPP TS 38.215 V18.1.0 (2023-12) NR; Physical layer measurements (Release 18).
8. Рютин К.Е., Фокин Г.А. Особенности реализации приёмника системы позиционирования в сети LTE с помощью сигналов PRS методом OTDOA // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022): Сборник научных трудов XI Международной научно-технической и научно-методической конференции, 2022. – С. 339-344.
9. Рютин К.Е. Разработка демонстратора формирователя опорных сигналов стандарта LTE // Студенческая весна, 2022: 76-я Региональная научно-техническая

конференция студентов, аспирантов и молодых ученых, Санкт-Петербург, 24-25 мая 2022 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2022. – С. 29-34.
10. Фокин Г.А., Волгушев Д.Б. Использование SDR-технологии для задач сетевого позиционирования. Процедуры приема и обработки опорных сигналов LTE // Вестник СибГУТИ, 2023. – Т. 17. – № 1. – С. 52-65.
11. Фокин Г.А., Григорьев В.А., Рютин К.Е. Технология сетевого позиционирования LTE. Часть 3. SDR-демонстратор в лабораторных условиях // Первая миля, 2023. – № 3 (111). – С. 72-80.
12. Фокин Г.А., Григорьев В.А., Рютин К.Е. [и др.] Технология сетевого позиционирования LTE часть 4. SDR-демонстратор в полевых условиях // Первая миля, 2023. – № 4 (112). – С. 34-41.
13. Фокин Г.А., Рютин К.Е. Использование SDR-технологии для задач сетевого позиционирования: формирование информационного блока MIB // Экономика и качество систем связи, 2023. – № 2 (28). – С. 30-42.
14. Koelemeij J.C.J., Dun H., Diouf et al. C.E.V. «A hybrid optical–wireless network for decimetre-level terrestrial positioning» Nature, 2022. – V. 611. – № 7936. – pp. 473-478.
15. Dun H., Tiberius C.C., Diouf C., Janssen G.J. «Terrestrial precise positioning system using carrier phase from burst signals and optically distributed time and frequency reference», 2021 International Technical Meeting of The Institute of Navigation, 2021. – pp. 510-524.
16. Diouf C., Janssen G.J.M., Kazaz T., Dun H., Chamanzadeh F. and Tiberius C.C. J. M. «A 400 Msps SDR platform for prototyping accurate wideband ranging techniques», 2019 16th Workshop on Positioning, Navigation and Communications (WPNC), Bremen, Germany, 2019. – pp. 1-6.
17. Diouf C. Janssen G.J.M., Dun H., Kazaz T. and Tiberius C.C.J.M. «A USRP-Based Testbed for Wideband Ranging and Positioning Signal Acquisition», in IEEE Transactions on Instrumentation and Measurement, 2021. – V. 70. – pp. 1-15.
18. Prager S., Thrivikraman T., Haynes M., Stang J., Hawkins D. and Moghaddam M. «Ultra-wideband synthesis for high-range resolution software defined radar», 2018 IEEE Radar Conference (RadarConf18), Oklahoma City, OK, USA, 2018. – pp. 1089-1094.
19. Prager S., Haynes M.S. and Moghaddam M. «Wireless Subnanosecond RF Synchronization for Distributed Ultrawideband Software-Defined Radar Networks» in IEEE Transactions on Microwave Theory and Techniques, 2020. – V. 68. – № 11. – pp. 4787-4804.
20. Yan H., Hanna S., Balke K., Gupta R. and Cabric D. «Software Defined Radio Implementation of Carrier and Timing Synchronization for Distributed Arrays», 2019 IEEE Aerospace Conference, Big Sky, MT, USA, 2019. – pp. 1-12.
21. URL https://kbmetrotek.ru/ptp-1u-v2/ (дата обращения – июнь 2024 г.).
22. URL https://kbmetrotek.ru/metronom-t/ (дата обращения – июнь 2024 г.).
23. URL https://gsm-repiteri.ru/prodazha/cable/kabel-5d-fb-pvc-chernyy (дата обращения – июнь 2024 г.).
24. URL https://www.tek.com/en/oscilloscope/csa7404b-manual/csa7404b-tds7704b-tds7404b-tds7254b-tds7154b-user-manual (дата обращения – июнь 2024 г.).
25. URL https://gsm-repiteri.ru/prodazha/deliteli/delitel-moshhnosti-bs-700-2700-1-2 (дата обращения – июнь 2024 г.).
26. URL https://www.mercusys.com/en/product/details/ms108g (дата обращения – июнь 2024 г.).
27. Fokin G., Ryutin K., Grigoriev V. and Bobrovskiy V. «Software-Defined Radio Network Positioning Technology Design. Synchronization Subsystem» 2023 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO, Pskov, Russian Federation, 2023. – pp. 1-6.

СИНТЕЗ ПРОГРАММНОГО АЛГОРИТМА И АРХИТЕКТУРЫ ПРИЛОЖЕНИЯ ПО АВТОМАТИЗИРОВАННОМУ СБОРУ ИНФОРМАЦИИ В СЕТЕВЫХ АГРЕГАТОРАХ

К.В. Портнов, *к.т.н., доцент, Самарский государственный технический университет, sk7@mail.ru;*
М.А. Фошин, *Самарский государственный технический университет, valp@mail.ru.*

УДК 004.9

Аннотация. Настоящая статья посвящена техническим вопросам, связанным с автоматизированным поиском данных на страницах *web*-браузеров и трансформацией этих данных в необходимые формы. Данная проблема актуальна для множества сфер, где необходимо собирать данные для их последующей обработки. В качестве прикладной сферы для разработки прототипа алгоритма и программы сбора данных выбрана оценочная деятельность. Авторами проведен системный анализ предметной области, описаны процессы проведения оценки, выделены наиболее трудоемкие процессы, которые связаны со сбором данных с веб-страниц и требуют первичной автоматизации. Разработано приложение для сбора данных для целей оценки недвижимости.

Ключевые слова: интерфейс браузера; сбор данных с веб-страниц; парсинг данных; автоматизация оценочной деятельности; алгоритм сбора данных; системный анализ процессов оценки недвижимости; оценка квартир.

SYNTHESIS OF SOFTWARE ALGORITHM AND ARCHITECTURE OF APPLICATION FOR AUTOMATED COLLECTION OF INFORMATION IN NETWORK AGGREGATORS

K.V. Portnov, *candidate of technical science, associate professor, Samara State Technical University;*
M.A. Foshin, *Samara State Technical University.*

***Annotation*.** This article is devoted to technical issues related to automated data search on web browser pages and transformation of this data into the necessary forms. This problem is relevant for many areas where it is necessary to collect data for subsequent processing. Assessment activities were chosen as the applied area for developing a prototype algorithm and data collection program. The authors conducted a systematic analysis of the subject area, described the assessment processes, identified the most labor-intensive processes that are associated with collecting data from web pages and require primary automation. An application has been developed to collect data for real estate valuation purposes.

Keywords: browser interface; data collection from web pages; data parsing; automation of valuation activities; data collection algorithm; system analysis of real estate valuation processes; apartment valuation.

Введение

Интернет становится местом концентрации большого количества информации, которая может быть использована в различных отраслях. Несмотря на открытость некоторых источников, отсутствие *API*-интерфейса для получения к ним доступа составляет проблему для их автоматизированной обработки. На большинстве открытых ресурсов данные в них представлены в форме, мало пригодной для программной обработки, а некоторые ресурсы специально

ограничивают даже ручное копирование открытых данных (объявлений, отчетов, статистики). В подобных случаях становится актуальной задача сбора данных посредством преобразования «аналоговых» данных – растровых картинок, защищенного текста – в данные, необходимые для обработки или решения практических задач.

Задачи автоматизированного сбора данных актуальны для составления экономических, статистических, социологических отчетов, проведения различного рода исследований, накопления статистических данных и т.п.

Одной из таких задач является задача по сбору данных на агрегаторах недвижимости для формирования перечня аналогичных объектов при проведении оценки объектов недвижимости. Оценка объектов недвижимости играет ключевую роль в различных аспектах бизнеса и инвестиций, таких как сделки купли-продажи, ипотечное кредитование, управление активами, финансовая отчетность и другие. Время, необходимое для изготовления одного отчета об оценке объекта недвижимости, может значительно варьироваться в зависимости от различных факторов, таких как тип недвижимости, объем работы, сложность объекта, доступность информации, методы оценки, требования заказчика и другие. В среднем, оценка недвижимости может занять от нескольких дней до нескольких недель.

Цель работы – разработка математического, алгоритмического и программного обеспечения для парсинга сетевых страниц на примере оценочной деятельности, способного к адаптации под другие задачи сбора однотипных данных с *html*-страниц.

Анализ процессов в оценочной деятельности

Процесс оценки объекта недвижимости представляет собой однообразный процесс по изготовлению типовых отчетов об оценке объекта со стандартными разделами.

Первым делом для автоматизации оценочной деятельности необходимо провести системный анализ процессов для построения модели действия оценщика, для понимания возможности программной автоматизации данной процедуры.

В общем виде процесс подготовки отчета об оценке выглядит как однообразный процесс составления отчета об оценке на основании документов, полученных от заказчика, результатов осмотра и других данных. Контекстная диаграмма процесса оценки недвижимости в общем виде представлена на рис. 1.

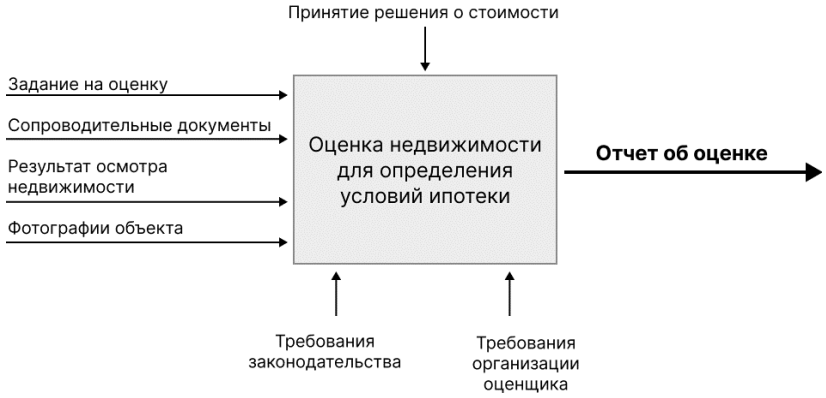


Рисунок 1

Тем не менее, несмотря на шаблонность большинства процедур процесса оценки, эта деятельность в настоящее время осуществляется с помощью ручного труда оценщика, заполняющего *DOC*-шаблон.

Информацию, содержащуюся в отчете об оценке, можно свести к следующим классам:

- типовые формы (титульный лист и т.п.);
- типовая стандартная информация (сведения об оценщике, сведения об организации, в которой работает оценщик, принятые при проведении оценки объекта допущения, применяемые стандарты при проведении оценки, обоснование выбора подходов к оценке объектов, описание подходов к оценке объектов, социально-экономическое развитие региона и т.п.);
- индивидуальная информация (информация о заказчике, информация об объекте недвижимости и т.п);
- динамическая информация – информация, которая меняется (анализ рынка недвижимости, таблица аналогичных объектов).

Анализ информации, содержащейся в отчете об оценке объекта недвижимости, позволил произвести ее классификацию. Классификация информации представлена на рис. 2.

Рисунок 2

Как видим, большинство информации остается достаточно однообразной и из 100 страниц, содержащихся в отчете, 80% информации является типовой информацией, которая не сильно меняется из-за отчета в отчет. Однако копирование данной информации не составляет высоких трудозатрат, поэтому автоматизация заполнения шаблонных документов может быть одним из будущих направлений развития данной работы.

Анализ процесса составления отчета позволил выделить следующие процедуры:

1. Прием документов.
2. Выездной осмотр объекта недвижимости.
3. Формирование *DOC*-шаблона отчета об оценке объекта недвижимости.
4. Заполнение типовых разделов отчета об оценке (класс общей информации).
5. Заполнение раздела с индивидуальными характеристиками объекта (класс специальной информации).
6. Поиск объектов-аналогов и сравнительный анализ объектов (класс анализа рынка).
7. Принятие решения об окончательной стоимости.
8. Компиляция (сборка) отчета как документа.

Наиболее трудоемкой и долговременной процедурой является поиск оценщиком на разных интернет-агрегаторах недвижимости аналогичных объектов и ручное копирование характеристик найденных объектов с последующим переносом информации в отчет об оценке (информация в данном случае представлена таблицей аналогов с основными характеристиками и *url*-ссылкой на источник).

После того как найден аналогичный объект, необходимо произвести поочередно копирование следующих его характеристик:

- наименование объекта недвижимости;
- адрес объекта недвижимости;
- цена объекта недвижимости;
- общая площадь объекта недвижимости;
- этаж;
- материалы стен;
- краткое описание;
- *URL*-ссылка;
- и прочие характеристики.

Перечисленные данные в типовом объявлении (например, с сайта *Avito*) размещены в разных местах, их необходимо поочередно выделить, скопировать и поместить в таблицу. Данная процедура на копирование характеристик одного объекта-аналога может занимать от 1 до 5 мин. А количество аналогов для высокой адекватности оценки должно быть достаточно большим (20-30). Указанный процесс настолько однообразен, что при правильной постановке задачи может быть частично автоматизирован программно. Таким образом, задача сводится к возможности на нужной *HTML*-странице объекта-аналога указать программе расположение требуемых характеристик (создание шаблона) и на последующих страницах-аналогах произвести автоматизированное копирование необходимой информации и дальнейший перенос этих данных в таблицу аналогичных объектов недвижимости.

Авторами предлагается программный алгоритм автоматизации поиска и переноса из агрегаторов данных об объектах-аналогах. Процедура не может быть полностью автоматической, так как критерий схожести объектов очень субъективен и опирается на множество факторов, а решение, какой объект считать аналогом, принимается самим экспертом-оценщиком.

Частичная автоматизация будет заключаться в создании программы и алгоритма, которые позволяют для конкретного агрегатора создавать шаблон расположения необходимой информации в объявлении-аналоге, с дальнейшим ее перемещением в конечную таблицу-аналогов, являющуюся результатом работы проектируемого программного продукта.

Подобная организация процесса позволит существенно сократить временные затраты оценщика, что обеспечивает увеличение производительности труда.

Синтез алгоритма и архитектуры приложения

Характеристики об объекте-аналоге находятся на сайте-агрегаторе и представляют из себя элементы *HTML*-разметки страницы. В большинстве популярных браузеров существуют специальные инструменты, предназначенные для веб-разработчиков. Среди функционала данных инструментов присутствует возможность посмотреть разметку страницы и все расположенные на ней элементы в формате *HTML*.

Получив полную разметку страницы и зная некоторую информацию о элементе с интересующей характеристикой объекта (например, текст, сопровождающий значение характеристики), можно определить «маркеры», чтобы программно-алгоритмически получить эти значения для последующего переноса в таблицу аналогов.

Получив значения характеристик с выбранной страницы, необходимо каким-либо образом отправить в файл с электронной таблицей. Проблема заключается в том, что возможности браузерных расширений ограничены в целях безопасности. Для этого создана дополнительная программа для переноса скопированных характеристик объектов в *xlsx* файл. Для пересылки данных можно воспользоваться технологией *WebSocket*, что позволит наладить связь между браузерным расширением и десктоп-приложением.

Таким образом, конечный программный продукт будет состоять из двух частей:

1) Браузерное расширение (сбор данных со страницы объявления о продаже объекта недвижимости и переправка их через веб-сокет в десктоп-приложение);
2) Десктоп-приложение (принятие отправленных данных и запись их в *xlsx*-таблицу объектов-аналогов).

Полученный процесс взаимодействия разных частей приложения изображен на рис. 3:

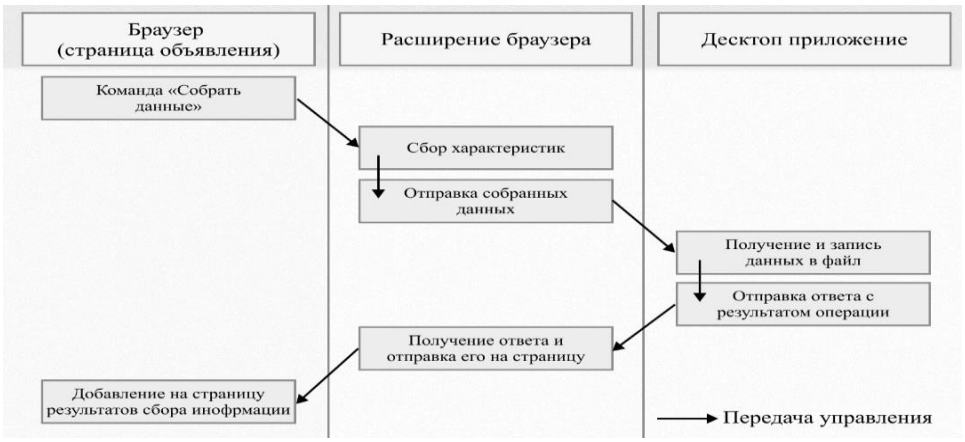


Рисунок 3

Моделируя процесс выгрузки информации с разных сайтов агрегаторов недвижимости, нельзя не отметить важную проблему: разные сайты имеют разную разметку и оформление информации о объектах. Следовательно, нельзя заранее определить, где на разметке страницы будут располагаться необходимые данные, так как на разных сайтах разметка будет отличаться. Тем не менее, определив расположение элемента однажды, не составит труда сохранить путь к нему для последующего использования при повторных посещениях текущей страницы и аналогичных страниц сайта.

Для реализации подобного подхода введем понятие «Шаблон». Шаблоном будет являться объект, указывающий какие данные необходимо выгрузить в таблицу, где эта информация располагается на разметке страницы и для какого сайта актуален сам шаблон. Шаблон будет создаваться самим оценщиком.

Возможность создания шаблона лучше всего реализовать непосредственно в браузере с помощью создания браузерного расширения, интегрировав необходимый интерфейс на страницу с объявлением, чтобы оценщик мог выбрать все интересующие его элементы, не прибегая без необходимости к непосредственному анализу разметки страницы. Созданные шаблоны можно

сохранять для последующего использования прямо в браузере. Это возможно благодаря доступу к *API* хранилища, предоставляемом браузером всем расширениям.

В результате общий процесс выгрузки информации для конечного пользователя будет состоять из этапов, отраженных на рис. 4.

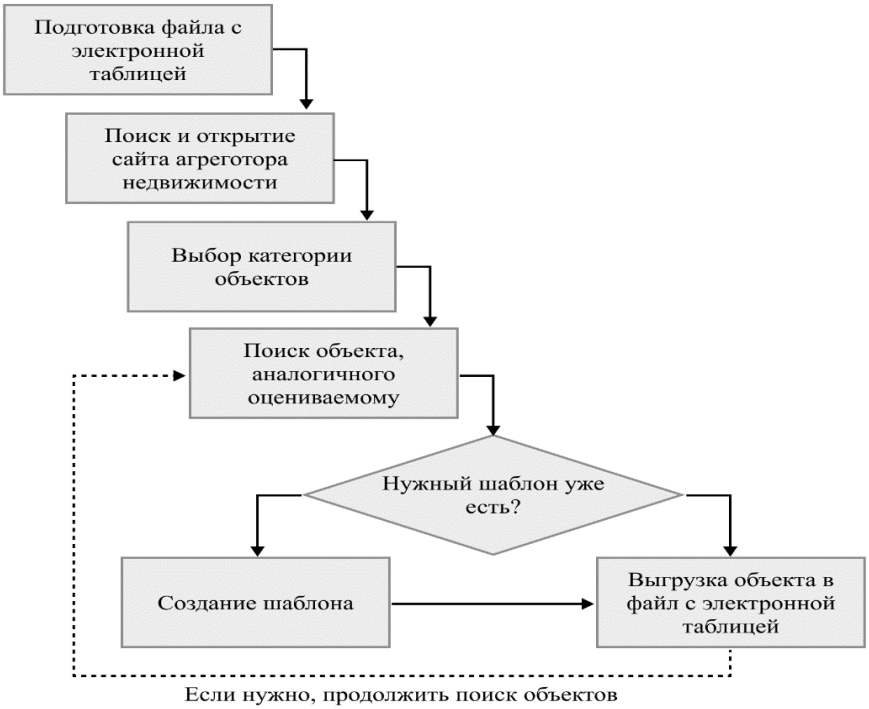


Рисунок 4

Браузерное расширение должно реализовывать следующий функционал:

- возможность создавать шаблоны сбора информации;
- возможность просматривать, редактировать и удалять созданные шаблоны;
- возможность использовать созданные шаблоны для сбора информации со страниц сайтов;
- отправка собранной со страницы информации через веб-сокет в десктоп-приложение;

Ориентируясь на требования к функционалу расширения, введем необходимые интерфейсы. В качестве отправной точки, из которой можно будет получить доступ ко всем функциональным возможностям, станет *Popup*-окно. Находясь на какой-либо интернет странице, из него можно вызывать окно создания и редактирования шаблонов или непосредственного сбора данных. Созданные шаблоны можно просмотреть на отдельной странице «*allTemplatesPage*», перейти на которую можно все из того же поп-ап окна.

Каждый из фронта энд-скриптов ответственен исключительно за свои функциональные возможности и лишь отражает текущее состояние браузерного расширения, информацию о котором он получает из бэкграунд-контекста. При возникновении необходимости изменения этого состояния (например, команда создания или изменения шаблона), фронт энд скрипты лишь оповещают об этом бэкграунд скрипт, который уже взаимодействует с хранилищем браузера и десктоп-приложением посредством веб-сокета.

Структура браузерного расширения представлена на рис. 5.

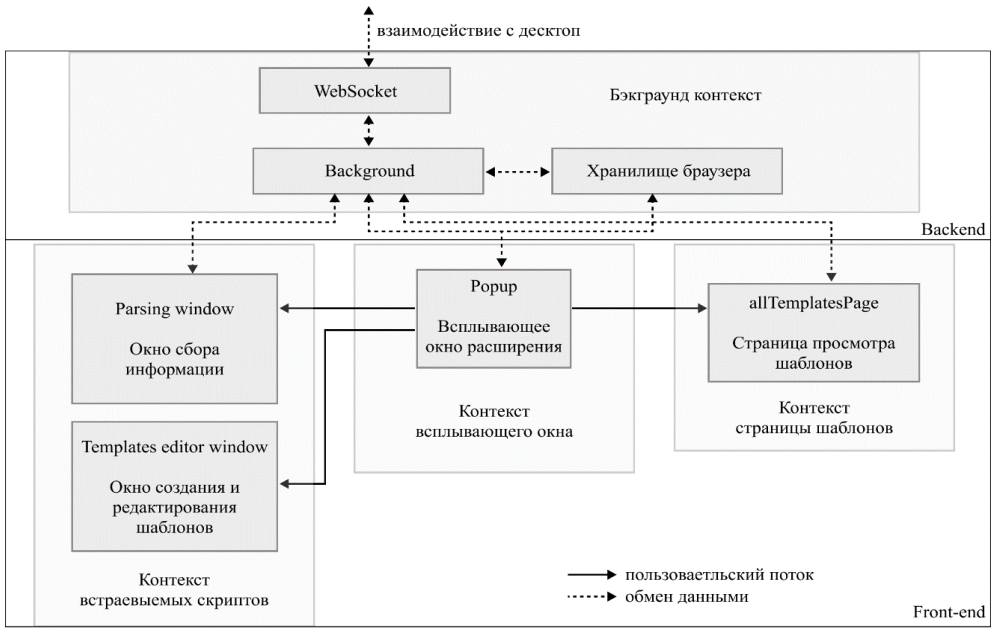


Рисунок 5

Созданные шаблоны используются при сборе информации. Сценарий пользовательского опыта парсинга характеристик объекта изображен на рис. 6.

Доступ к окну сбора информации осуществляется через всплывающее окно расширения или через специальную команду. Как и в случае с окном редактирования шаблонов, на команду реагирует бэкграунд-контекст. Он имеет доступ к доменному имени активной вкладки, что позволяет ему собрать все ассоциированные с ним шаблоны. Собранные шаблоны и команда перенаправляются в контекст контент-скрипта.

Получив запрос на сбор информации, контент-скрипт начнет проверку полученных шаблонов на актуальность. Для этого он попытается собрать все элементы, селекторы которых содержатся в шаблонах. В случае, если элемент не удается найти, шаблон отбраковывается как неактуальный. Таким образом, пользователю будут предоставлены только те шаблоны, которые подходят для текущей страницы. Псевдокод алгоритма проверки шаблонов можно представить следующим образом:

```
Шаблоны = аргумент функции

КорректныеШаблоны = новый пустой массив

Для каждого Шаблон внутри Шаблоны:
        Корректный: = True
        Для каждого Поле внутри Шаблон.Поля:
            Элемент: = Найти в разметке HTML элемент по Поле.Селектор
            Если Элемент == Null:
                Корректный: = False
        Если Корректный == True
            Добавить Шаблон в КорректныеШаблоны
Вернуть КорректныеШаблоны
```

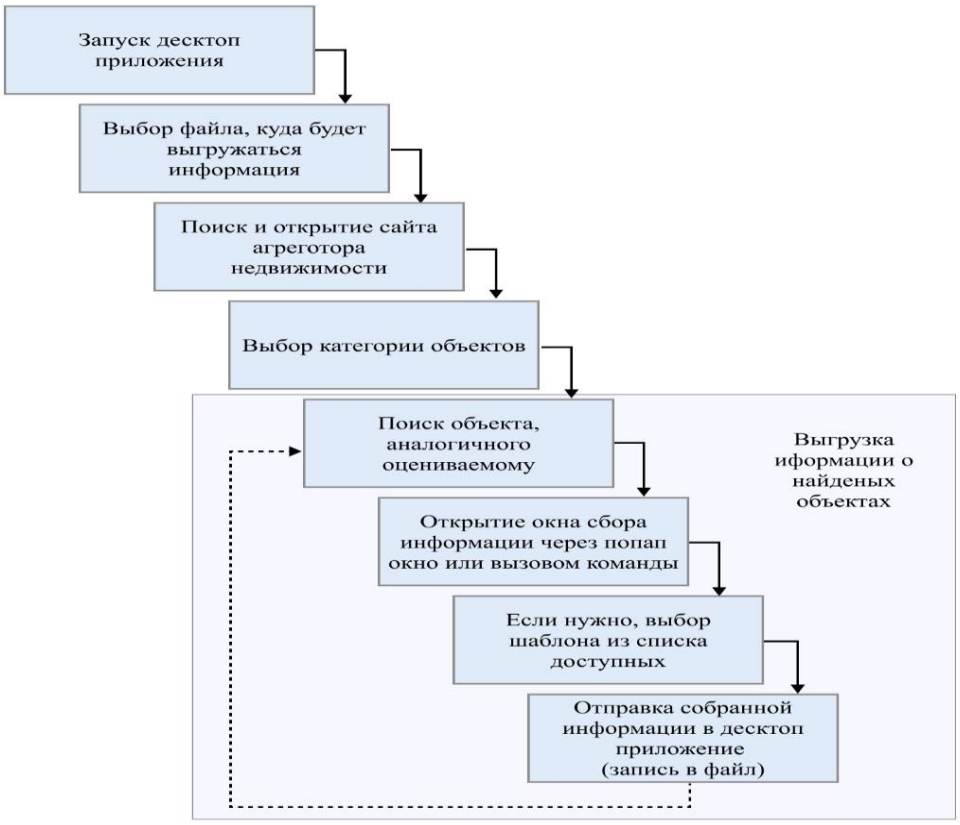


Рисунок 6

После процесса проверки контент-скрипт интегрирует на страницу окно сбора информации. Внутри него присутствуют все актуальные шаблоны. Выбор какого-либо из доступных шаблонов приведет к сбору информации на странице согласно полям шаблона и отображению результатов сбора в интерфейсе. Отображается как сырая (необрезанная по маркерам) информация, так и обработанная (та, которая будет отправлена в десктоп-приложение). Пример отображения собранных данных приведен на рис. 7.

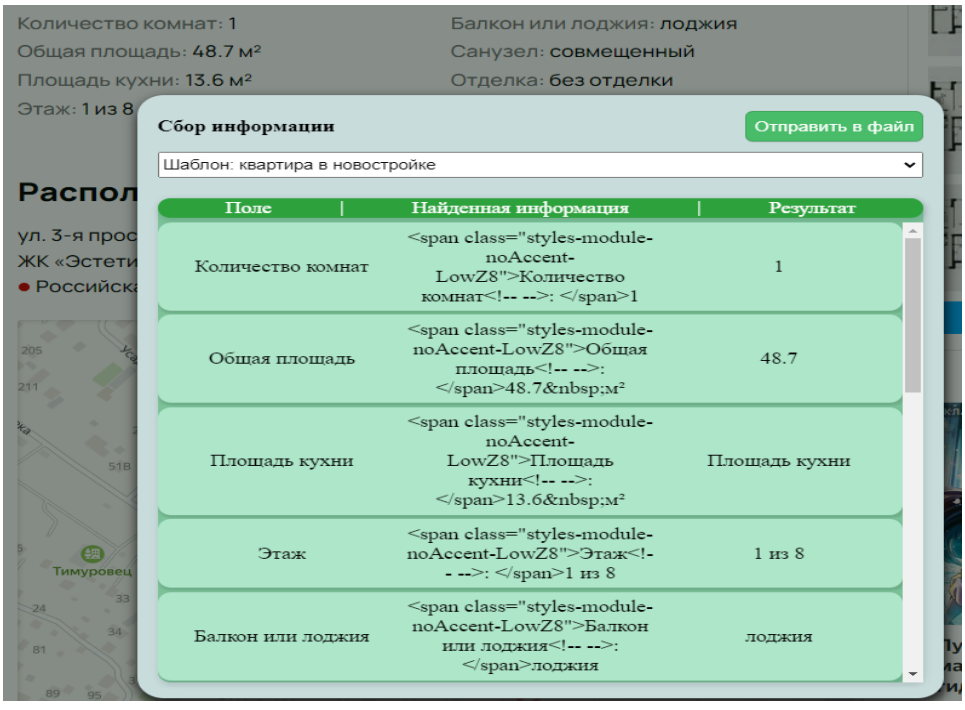


Рисунок 7

Получив запрос на пересылку данных в десктоп приложение, бэкграунд-скрипт попытается установить с ним связь через *WebSocket*. Как только связь будет установлена, он отправит данные по открывшемуся каналу и станет ожидать ответа от приложения. При получении ответа бэкграунд-скрипт закроет соединение и оповестит о результате контент-скрипт активной вкладки. В случае возникновения ошибки сформируется сообщение о провале операции, которое также будет переслано контент-скрипту.

Среди списка ошибок может быть неуспешность установления соединения (когда десктоп-приложение не запущено или не выбран выходной файл, где должна формироваться таблица аналогов), провал записи (когда неверно указано смещение внутри электронной таблицы или номер объекта) или провал открытия файла для записи (когда файл не существует или занят другой программой).

В любом случае в окне сбора информации отобразится результат операции, оповещающий пользователя о успешности процедуры или о возникших ошибках. Полный процесс сбора и отправки данных приведен на рис. 8.

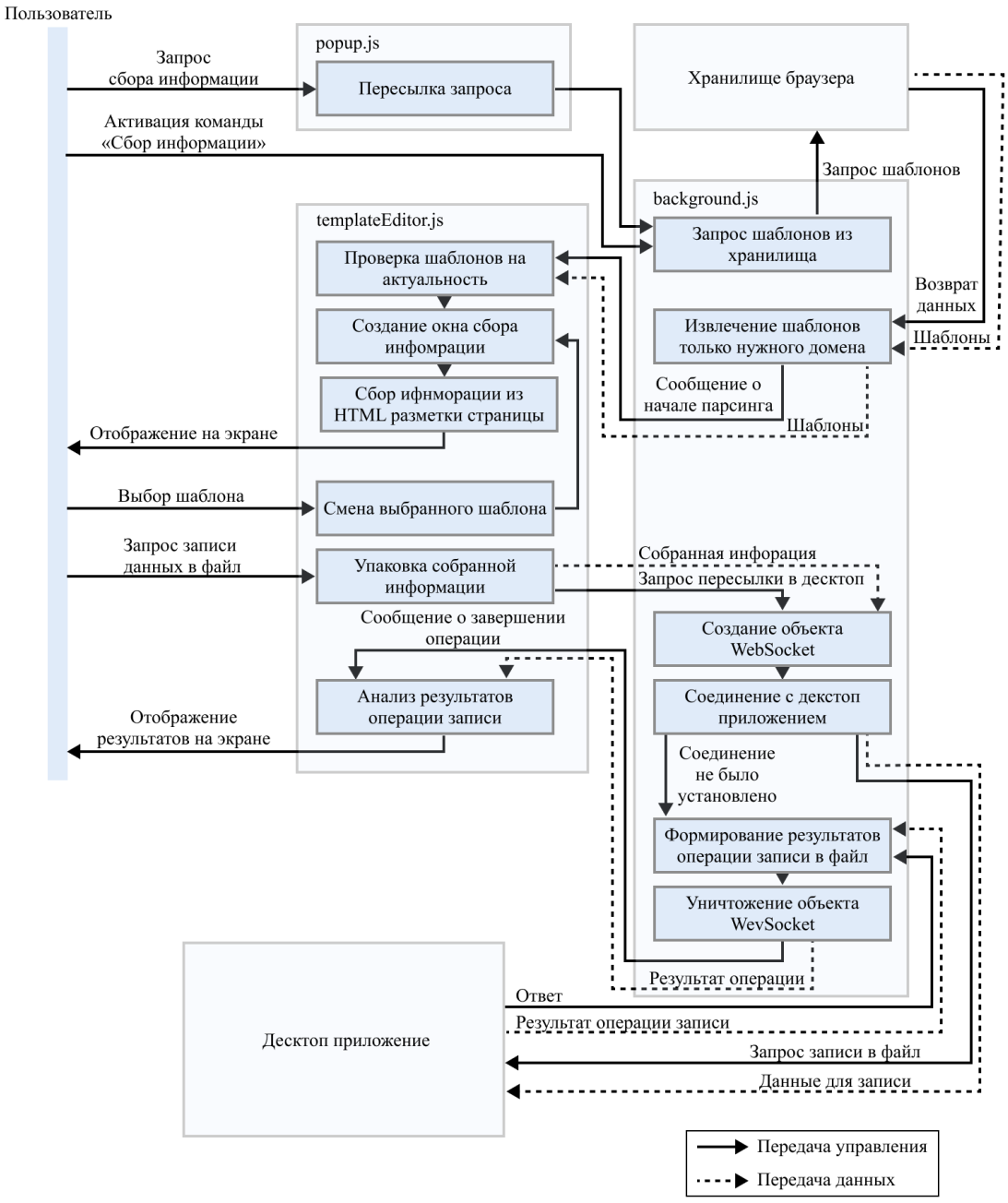


Рисунок 8

После сбора информации, используемый шаблон должен быть помечен как последний используемый для данного доменного имени. При открытии окна сбора информации именно он должен выбираться в первую очередь, если это возможно.

Результаты разработки приложения

Программа автоматизации сбора информации реализована в виде двух компонентов: браузерное расширение и десктоп-приложение. Расширение рассчитано на установку в интернет-браузеры, основанные на движке *Chrome* («Яндекс.Браузер» «*Google Chrome*»). Десктоп-приложение скомпилировано в исполняемый файл (*exe*) и рассчитано на использование в рамках персональных компьютеров на базе ОС *Windows* 10 и выше, обладающих шестидесяти четырехразрядной архитектурой процессора.

Пример шаблона, созданного посредством окна редактирования, приведен на рис. 9.

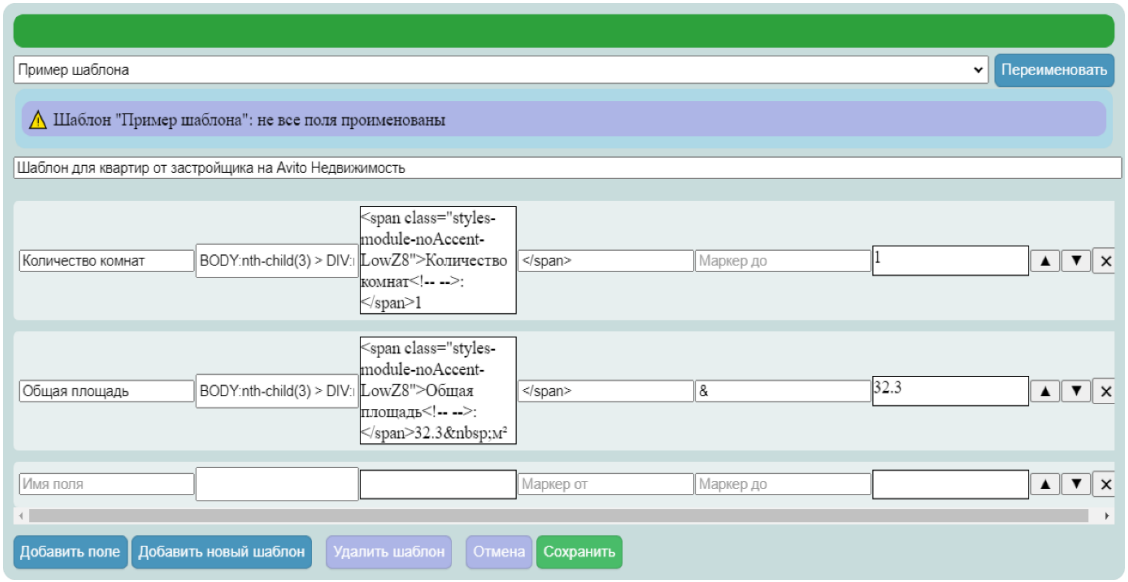


Рисунок 9

На рис. 10 продемонстрирован результат записи собранных данных, произведенных десктоп-приложением, в файл *Microsoft Office Excel*. Данные собраны посредством ранее сформированного шаблона.

	A	B	C	D	E	F	G
1	Номер объекта	Расположение	Общая площадь	Количество комнат	Этаж	Отделка	Цена
2	Объект №1	пос. Мехзавод, 1 кв-л/Московское ш./ул. Николая Баженова, жилые дома	62.8	2	7 из 10	предчистовая	6200000
3	Объект №2	Самарская обл., Самара, посёлок Прибрежный, ул. Труда, 22	60.4	3	2 из 2	кухня, хранение одежды	3150000
4	Объект №3	тер. 18 км Московского шоссе, д. 7А	69.3	2	2 из 17	без отделки	4800000

Рисунок 10

Заключение

Авторами решена актуальная проблема сбора данных с веб-страниц в случаях, когда требуется производить сбор однотипных данных с разных сайтов. Программно-алгоритмическое решение позволяет адаптировать программу к сбору разных наборов данных по созданным шаблонам.

Авторами достигнуты следующие результаты:

1) Проведен анализ деятельности по оценке недвижимости.

2) Определены наиболее трудоемкие и шаблонные процедуры в процессе оценки, подлежащие первичной автоматизации.

3) Проведен анализ технической возможности автоматизации процесса сбора информации со страниц агрегаторов недвижимости.

4) Разработана архитектура приложения, состоящая из двух взаимосвязанных частей.

5) Разработан алгоритм поиска информации на страницах агрегаторов недвижимости.

6) Разработан алгоритм переноса информации в конечную форму документа.

7) Реализован программный комплекс сбора информации с сайтов агрегаторов недвижимости.

8) Определены перспективы развития разработанного приложения.

Программно-алгоритмические решения позволяют адаптировать данную программу для любых предметных областей, связанных со сбором данных с веб-страниц.

Литература

1. Портнов К.В. Анализ цифровой трансформации бизнес-процессов. Актуальные проблемы общества, экономики и права в контексте глобальных вызовов: Сборник материалов X Международной научно-практической конференции, Москва, 17 мая 2022 года. Редколлегия: Л.К. Гуриева [и др.]. – Москва: Общество с ограниченной ответственностью «ИРОК», ИП Овчинников Михаил Артурович (Типография Алеф), 2022. – С. 49-58. – DOI 10.34755/IROK.2022.92.13.091. – EDN EJPTQW.

2. Портнов К.В. Генетические алгоритмы и поиск эффективных порядков индикаторов в биржевой торговой стратегии на основе пересечения трех скользящих средних // Вестник Самарского государственного технического университета. Серия: Технические науки, 2005. – № 32. – С. 72-76. – EDN JWUXKZ.

3. Портнов К.В. Информационные технологии в оценке показателя лояльности клиентов // В мире научных открытий, 2011. – № 3 (15). – С. 254-258. – EDN OCSJNX.

4. Смагина З.А. Технология интернет вещей и ее влияние на современную экономику // Теоретические и прикладные вопросы экономики, управления и образования: Сборник статей II Международной научно-практической конференции. В 2-х томах, Пенза, 15-16 июня 2021 года. Том II. – Пенза: Пензенский государственный аграрный университет, 2021. – С. 182-186. – EDN AJTHBC.

5. Портнов К.В. Анализ задачи оценки лояльности в деятельности компаний в сфере профессиональных услуг // Проблемы развития предприятий: теория и практика, 2020. – № 1-2. – С. 241-244. – EDN HDSWOD.

6. Свидетельство о государственной регистрации программы для ЭВМ № 2023664735 Российская Федерация. Система учета товаров на складе интернет-магазина: № 2023660391: заявл. 24.05.2023: опубл. 06.07.2023 / К.В. Портнов; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный технический университет». – EDN VFHCBC.

7. Латушкина Т.С. Исследование возможностей интернет-продвижения и настройка рекламной компании // Московский экономический журнал, 2023. – Т. 8. – № 5. – DOI 10.55186/2413046X_2023_8_5_280. – EDN RFPBDO.

8. Сахбиева А.И., Калякина И.М., Косников С.Н., Латушкина Т.С., Майорова И.А. Цифровизация экономики и обеспечение безопасности данных // Московский экономический журнал, 2021. – № 8. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-8-2021-28.

9. Иноземцев В.Л. На рубеже эпох. Экономические тенденции и их неэкономические следствия [Текст]. – М.: Экономика, 2003. – 730 с.
10. Латушкина Т.С., Харитонова Е.А., Майорова И.А. Анализ подходов к ESG на примере металлообрабатывающего предприятия // Экономика и предпринимательство, 2022. – № 7 (144). – С. 1059-1064.
11. Латушкина Т.С., Майорова И.А. Использование и применение JAVASCRIPT-фреймворков (REACT, ANGULAR, VUE.JS) для разработки WEB-приложений // Экономика и предпринимательство, 2023. – № 9 (158). – С. 1374-1376.
12. Портнов К.В. Актуальные проблемы и задачи автоматизированных систем в сфере ЖКХ // Журнал монетарной экономики и менеджмента, 2024. – № 2. – С. 230-236. – DOI 10.26118/2782-4586.2024.35.72.033. – EDN AEQRFJ.
13. Портнов К.В. Разработка информационной системы на основе многофакторной логистической регрессии // Информационные технологии. Радиоэлектроника. Телекоммуникации, 2012. – № 2-3. – С. 129-133. – EDN PEDEUX.
14. Портнов К.В. Анализ оценки неопределенности инвестиционного портфеля. Математическое моделирование и краевые задачи: Труды Третьей Всероссийской научной конференции, Самара, 29-31 мая 2006 года. Редколлегия: В.П. Радченко (ответственный редактор), Э.Я. Рапопорт, Е.Н. Огородников, М.Н. Саушкин (ответственный секретарь). Том Часть 4. – Самара: Самарский государственный технический университет, 2006. – С. 80-82. – EDN TGOHNF.

ИЕРАРХИЧЕСКАЯ МОДЕЛЬ ИЗМЕНЕНИЯ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ КОМПЬЮТЕРНЫХ АТАК НА КОРПОРАТИВНУЮ СЕТЬ СВЯЗИ

М.М. Добрышин, *к.т.н., Академия ФСО России, dobrithin@ya.ru.*

УДК 004.942

Аннотация. Совершенствование средств и информационных технологий, а вместе с ними предоставляемых услуг связи, требуют расширения понятия «информационная безопасность». Принятые подходы по оценке целостности, доступности и конфиденциальности защищаемой информации недостаточно информативны при проведении оценок в информационных системах, предоставляющих своим абонентам различные услуги связи и информационного обеспечения. Для чего представлена иерархическая блочная модель, позволяющая осуществить оценку уровня информационной безопасности единичного средства обработки, хранения и передачи информации, защищенности применяемой информационной технологии, на основании которых провести оценку уровня информационной безопасности элемента сети и сети связи в целом, что и позволит оценить безопасность услуги связи. В статье представлены функциональные и аналитические взаимосвязи между изменениями значений параметров свойств защищаемых объектов в условиях различных компьютерных атак. Представление взаимосвязей в виде функциональных зависимостей является упрощенной постановкой задачи и направлением дальнейших исследований.

Ключевые слова: корпоративная сеть; компьютерные атаки; уровень информационной безопасности; иерархическая модель.

A HIERARCHICAL MODEL OF CHANGING THE LEVEL OF INFORMATION SECURITY IN THE CONTEXT OF COMPUTER ATTACKS ON THE CORPORATE COMMUNICATIONS NETWORK

M.M. Dobryshin, *Candidate of Technical Science, Academy of the FSO of Russia, employee.*

Annotation. The improvement of tools and information technologies require, and together with them, the provided communication services require the expansion of the concept of information security. The accepted approaches to assessing the integrity, accessibility and confidentiality of protected information are not informative enough when conducting assessments in information systems that provide their subscribers with various communication and information support services. For this purpose, a hierarchical block model is presented, which allows to assess the level of information security of a single means of processing, storing and transmitting information, the security of the information technology used, on the basis of which to assess the level of information security of the network element and the communication network as a whole, which will allow to assess the security of the communication service. The article presents functional and analytical relationships between changes in the values of the parameters of the properties of protected objects in the conditions of various computer attacks. The representation of relationships in the form of functional dependencies is a simplified statement of the problem and a direction for further research.

Keywords: corporate network; computer attacks; information security level; hierarchical model.

Введение

Основной полезной функцией корпоративной сети (КС) является предоставление абонентам КС услуг связи и информационного обеспечения (УС). Концепция качества обслуживания абонентов подразумевает, что услуги должны предоставляться, в том числе в условиях реализации злоумышленником различных компьютерных атак (КА).

Развитие и совершенствование средств и способов реализации КА для злоумышленника направлено на достижение цели воздействия – реализации угрозы информационной безопасности (ИБ), а для абонента и КС – на изменение в системе свойств КС, применяемых информационных технологий (ИТ), средств обработки, хранения и передачи информации (с учетом установленного комплекта программного обеспечения), а также свойств защищаемой информации [1].

Существующие подходы защиты от КА, основанные на «предположении» о цели применения КА (предполагаемые угрозы ИБ), не всегда отражают замысел деструктивных действий злоумышленника, а в некоторых случаях способствуют достижению цели воздействия.

С целью повышения обоснованности применяемых механизмов и средств обеспечения ИБ (СрОИБ) в ряде актуальных регламентирующих документах [2-5] предлагается оценивать фактическое изменение значений контролируемых параметров, на основе которых и принимать решение о формировании и реализации мероприятий по противодействию выявленной КА, например [5]:

- замедление, временный сбой или прекращение работы АРМ, сервисов и иных компонентов объектов инфраструктуры;
- превышение допустимой нагрузки на вычислительные ресурсы элементов объектов инфраструктуры;
- иные нарушения в работе элементов объекта инфраструктуры, вызывающих прекращение выполнения его целевых функций.

Однако в указанных подходах оцениваются изменения значений единичных параметров (эксплуатационных характеристик), что не позволяет в полной мере оценить влияние КА на свойства защищаемого ресурса: ЭВМ, узла КС, информации, циркулирующей между узлами КС, и сеть в целом (низкая достоверность оценки), и, как следствие, снижает обоснованность реагирования на выявленный факт реализации КА (например, применение механизмов или СрОИБ, определение режимов их функционирования).

Следует также отметить, что для повышения своевременности применяемых средств и изменения режимов работы (настроек) указанных средств применяют не фактическое отклонение измеренных параметров, а прогнозные модели оценки изменения параметров, однако эти модели также обладают низкой достоверностью результатов прогнозирования влияния конкретной КА на изменение уровня ИБ КС.

Таким образом, возникает научная задача, заключающаяся в повышении достоверности результатов оценки уровня ИБ в условиях КА на элементы (узлы) КС за счет учета влияния КА на группу свойств защищаемых ресурсов.

Иерархическая модель изменения уровня информационной безопасности в условиях компьютерных атак на корпоративную сеть связи

С целью разрешения сформулированной научной задачи разработана иерархическая модель, объединяющая (рис. 1): модель изменения уровня ИБ *i*-го СОИ, вызванного КА; модель изменения уровня защищенности *k*-й ИТ, вызванного КА; модель изменения уровня ИБ *y*-го элемента и КС, вызванного КА, и модель изменения безопасности предоставляемой *u*-й услуги связи, вызванного КА.

Выбор в качестве способа построения модели – блочный подход [6, 7], обусловлен необходимостью объединения разнородных объектов моделирования и дестабилизирующих воздействий, влияющих на эти объекты, а также структурой протекающих процессов и, в частности, тем, что безопасность предоставляемой услуги связи зависит от безопасности КС, которое, в свою очередь, определяется с организационной стороны особенностями ее построения, а с технической стороны – безопасностью применяемых СОИ и ИТ.

Модель изменения уровня ИБ *i*-го СОИ, вызванного КА, описывает изменение значений группы *j*-х параметров, характеризующих функциональные свойства *i*-го СОИ, обеспечивающих реализацию *b*-го контекста (услуги, функции) (блок 3.1, $p_a^{ibjw}(t)$) с учетом выявленных уязвимостей ИБ *i*-го СОИ $\left(\left\langle u_i^{\text{факт}} \right\rangle\right)$, в условиях влияния *a*-го вида КА с *w*-ми характеристиками на изменение значений *j*-го параметра СОИ (блок 4.1, $p_a^{ijw}(t)$), с учетом возможностей *g*-го средства обеспечения ИБ (СрОИБ) по минимизации или недопущения воздействия *a*-й КА с *w*-ми значениями параметров (блок 5.1, $z_j^{iwg}(t)$). Уровень защищенности *i*-го СОИ к *a*-й КА $\left(z_a^i(t)\right)$ и уровень защищенности *i*-го СОИ $\left(Z^{iA}(t)\right)$ к известному множеству КА (А) определяется в блоке 2.1.

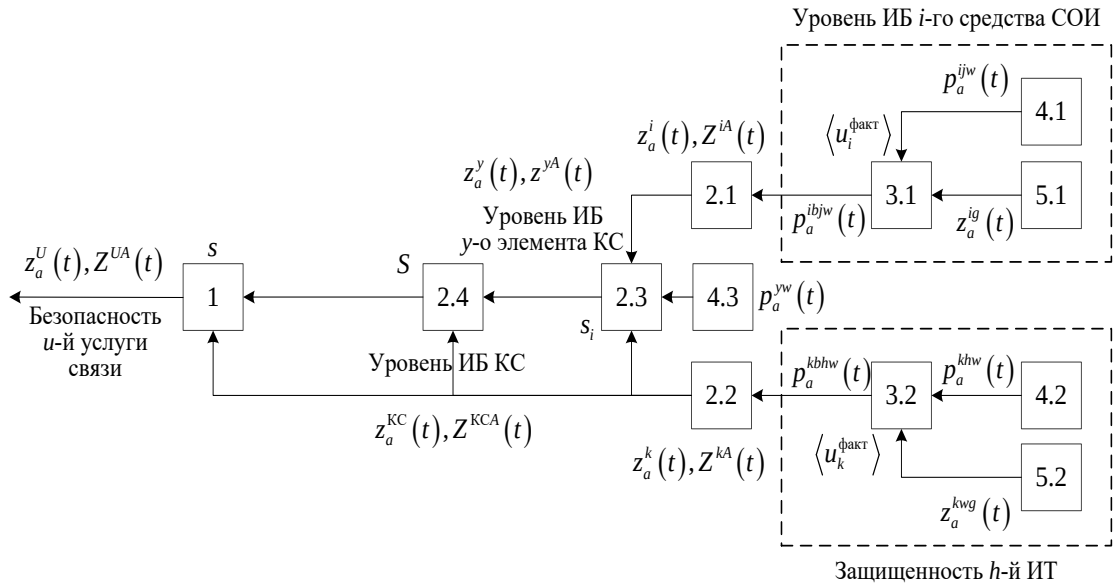


Рисунок 1

Модель изменения уровня защищенности *k*-й ИТ, вызванного КА, описывает изменение значений группы *k*-х параметров, характеризующих функциональные свойства *h*-й ИТ, обеспечивающих реализацию *b*-го контекста (услуга, функция) (блок 3.2, $p_a^{kbhw}(t)$) с учетом выявленных уязвимостей ИБ *k*-й ИТ $\left(\langle u_k^{факт} \rangle\right)$, в условиях влияния *a*-го вида КА с *w*-и характеристиками на изменение значений (блок 4.2, $P_a^{khw}(t)$), с учетом возможностей *g*-го средства обеспечения ИБ (СрОИБ) по минимизации или недопущения воздействия *a*-й КА (блок 5.2, $z_a^{kwg}(t)$). Уровень защищенности *k*-й ИТ от *a*-й КА $\left(z_a^k(t)\right)$ и уровень защищенности *k*-й ИТ $\left(Z^{kA}(t)\right)$ к известному множеству КА (*A*) определяется в блоке 2.2.

Модель изменения уровня ИБ *y*-го элемента и КС, вызванного КА**,** описывает изменение значений параметров, характеризующих функциональные свойства *y*-го элемента (узла) КС (блок 2.3, $z^{yA}(t)$), учитывающие изменения значений параметров *i*-х СОИ $\left(Z^{iA}(t)\right)$, входящих в состав элемента, изменения значений параметров *k*-х ИТ $\left(Z^{kA}(t)\right)$, используемых в *y*-м элементе, значений *w*-го параметра, характеризующего *a*-ю КА (блок 4.3, $p_a^{yw}(t)$) на *y*-й элемент КС, а также топологию построения *y*-го элемента КС $\left(s_i\right)$. В блоке 2.4 определяется изменение уровня ИБ КС $\left(Z^{KCA}(t)\right)$ из-за КА на КС, включая изменения уровня ИБ элементов КС $\left(z^{yA}(t)\right)$, входящих в ее состав, изменение уровня защищенности применяемых для взаимодействия ИТ (блок 2.2, $Z^{kA}(t)$) и топологию КС (*S*).

Модель изменения безопасности предоставляемой *u*-й услуги связи, вызванное *КА,* описывает изменение значений параметров, характеризующих *u*-ю УС и все предоставляемые УС (*U*) (блок 1, $z_a^u(t), Z^{UKA}(t)$), вызванные КА на КС, учитывающие изменение уровня ИБ КС (блок 2.4, $Z^{KCA}(t)$), изменение уровня

защищенности применяемых для взаимодействия ИТ (блок 2.2, $Z^{kA}(t)$) и топологию КС (*S*).

Исходными данными для модели являются вид (a) и значения параметров (w) КА (диапазон изменения параметров), изменение значений *j*-х или *k*-х параметров СОИ и ИТ соответственно в условиях *a*-*q* КА с *w*-*u* параметрами (значения получают на основании результатов моделирования), значения ослабляющей способности СрОИБ, топология и структура КС, схемы, описывающие взаимодействия элементов для организации и предоставления УС.

Промежуточными результатами являются изменение значений параметров, описывающих следующие свойства [8-15]:

<u>для СОИ и применяемых ИТ</u>:

– результативность – доля задач, которые выполняются правильно в условиях КА $\left(X_a^{Ri}(t)\right)$:

$$X_a^{Ri}(t) = \frac{A_a^{Ri}(t)}{B^{Ri}}, \tag{1}$$

где: $A_a^{Ri}(t)$ – количество выполненных уникальных задач при *a*-й КА на *i*-м СОИ, B^{Ri} – общее количество выполненных уникальных задач *i*-м СОИ $\left(B^{Ri} \supseteq A_a^{Ri}, A_a^R = \left(a_b^{Ria}\right),\ b = 1,2,...B\right)$, *t* – время реализации КА.

$$A_a^{Ri}(t) = \sum_{b=1}^{B} a_b^{Ria}(t), \tag{2}$$

$$a_b^{Ria}(t) = \begin{cases} 0, \text{ если } p_a^{ibjw}(t) \geq p_a^{b\ \text{доп}} \\ 1, \text{ если } p_a^{ibjw}(t) < p_a^{b\ \text{доп}} \end{cases}, \tag{3}$$

где: $a_b^{Ria}(t)$ – *b*-я уникальная задача, выполняемая *i*-м СОИ в условиях *a*-й КА, $p_a^{ibjw}(t)$ – вероятность успешной реализации *a*-й КА с *w*-и характеристиками, повлекшее ухудшение значения *j*-го параметра, характеризующего *b*-ю задачу, выполняемую *i*-м СОИ, $p_a^{b\ \text{доп}}$ – значение вероятности реализации *a*-й КА, при которой *b*-я уникальная задача выполняется.

$$\begin{aligned} P_a^{ibjw}(t) &= f\left(P_a^{iw}(t), h_a^{ijwb}(t), \left\langle u_a^{i\ \text{факт}}\right\rangle, z_a^{ig}(t)\right) \\ P_a^{khwb}(t) &= f\left(P_a^{kw}(t), h_a^{khwb}(t), \left\langle u_a^{i\ \text{факт}}\right\rangle, z_a^{kg}(t)\right) \end{aligned}, \tag{4}$$

где: $P_a^{iw}(t)$ – функция, описывающая изменение значений *w*-го параметра *a*-й КА, $h_a^{ijwb}(t)$ – функция, описывающая изменение значений *j*-го параметра *b*-й уникальной задачи *i*-го СОИ или *k*-й параметр *h*-й ИТ при *a*-й КА с *w*-и характеристиками КА; $\left\langle u_a^{i\ \text{факт}}\right\rangle$ – набор выявленных уязвимостей *i*-м СОИ на

момент начала *a*-й КА; $z_j^{ig}(t)$ – функция, описывающая изменение значений *w*-го параметра *a*-й КА при применении *i*-м СОИ *g*-го СрОИБ;

– эффективность / производительность – время, затраченное на успешное выполнение задачи в условиях КА $\left(X_a^{Oi}\right)$ и коэффициент затруднения работы СОИ в условиях КА $\left(x_a^{Oib}\right)$:

$$X_a^{Oi} = \frac{A_a^{Oi}}{T^{Oi}}, \tag{5}$$

где: A_{ia}^{O} – количество выполненных уникальных задач *i*-м СОИ при *a*-й КА на *i*-е СОИ, T^{Oi} – время на выполнение заданного количества задач *i*-м СОИ (задается для нормальных условий – без КА);

$$x_a^{Oib} = \frac{t_a^{Oib}}{\bar{t}^{Oi}}, \tag{6}$$

где: t_a^{Oib} – время выполнения *b*-й уникальной задачи при *a*-й КА на *i*-м СОИ, $\bar{t}^{Oi}$ – среднее время выполнения *b*-й уникальной задачи *i*-м СОИ в нормальных условиях – без КА.

– покрытие контекста – доля предполагаемых контекстов использования (УС и выполняемых функций), в которых СОИ или ИТ могут использоваться с приемлемым удобством использования и риском $\left(X_a^{Ki}(t), X_a^{Kk}(t)\right)$:

$$\begin{gathered} X_a^{Ki}(t) = 1 - \frac{\left(B^{Ki}\right)^2 - \left(B^{Ki} - A_a^{Ki*}(t)\right)\left(B^{Ki} - A_a^{Ki**}(t)\right)}{\left(B^{Ki}\right)^2} \\ X_a^{Kk}(t) = 1 - \frac{\left(B^{Kk}\right)^2 - \left(B^{Kk} - A_a^{Kk*}(t)\right)\left(B^{Kk} - A_a^{Kk**}(t)\right)}{\left(B^{Kk}\right)^2}, \end{gathered} \tag{7}$$

где: $A_a^{Ki*}(t)$, $A_a^{Kk*}(t)$– количество контекстов с приемлемым удобством использования при *a*-й КА на *i*-е СОИ или *k*-ю ИТ, $A_a^{Ki**}(t)$, $A_a^{Kk**}(t)$ – количество контекстов с приемлемым риском использования при *a*-й КА на *i*-е СОИ или *k*-ю ИТ, B^{Ki}, B^{Kk} – общее количество требуемых различных контекстов использования *i*-го СОИ или *k*-й ИТ.

$$\begin{aligned} A_a^{Ki*}(t) &= f\left(n_a^{ui}(t), X_a^{Oi}(t)\right) \\ A_a^{Kk*}(t) &= f\left(n_a^{uk}(t), X_a^{Ok}(t)\right) \end{aligned} \tag{8}$$

где: $n_a^{ui}(t)$, $n_a^{uk}(t)$ – количество операций, выполняемых для использования *u*-й УС при реализации *a*-й КА на *i*-й СОИ или *k*-й ИТ;

$$A_a^{Ki**}(t) = f\left(p_a^{ijw}(t)\right)$$

$$A_a^{Kk**}(t) = f\left(p_a^{khw}(t)\right) \tag{9}$$

где: $p_a^{ijw}(t)$, $p_a^{khw}(t)$ – вероятность реализации *a*-й КА с *w*-й характеристикой на *j*-й параметр *i*-й СОИ или *h*-й параметр, характеризующий *k*-ю ИТ.

<u>для элемента сети и сети связи (КС)</u>:

– уровень укомплектованности КС $(Y(t))$:

$$Y(t) = \frac{N^{\text{факт}}(t)}{N^0}, \tag{10}$$

где: $N^{\text{факт}}(t)$ – количество элементов КС, выполняющих функциональные задачи; N^0 – количество элементов КС в начальный момент времени;

$$N^{\text{факт}}(t) = \sum_{y=1}^{Y} n_y p_y^{\text{фз}}(t), \tag{11}$$

где: n_y – *y*-й элемент КС ($y = 1, 2, ...Y^{\text{кс}}$ – порядковый номер элемента КС), $P_y^{\text{фз}}(t)$ – вероятность выполнения функциональных задач *y*-м элементом КС.

$$p_y^{\text{фз}}(t) = f\left(X_a^{Ri}(t), n_y^u, s_y\right), \tag{12}$$

где: n_y^u – количество УС, предоставляемых абонентам *y*-го элемента КС, s_y – топология (связность) *y*-го элемента КС;

– устойчивость (живучесть) – коэффициент оперативной готовности:

$$K^{\text{or}}(t) = f\left(k_i^{\text{or}}, Y(t), s\right), \tag{13}$$

где: k_i^{or} – коэффициент оперативной готовности *y*-го элемента КС (узла), s – топология (связность) элемента КС.

$$k_y^{\text{or}}(t) = f\left(X_a^{Ki}(t), s_y\right), \tag{14}$$

где: s_y – связность *y*-го элемента КС;

– пропускная способность – вероятность выполнения функциональных задач в условиях изменения пропускной способности, вызванных *a*-м КА на *y*-й элемент $\left(P_a^{\text{пс}}(t)\right)$:

$$p_a^{ywg}(t) = f\left(v_a^y(t), v^{\text{тр}\,y}(t), H_a^{yw}(t), z_a^{yg}(t)\right), \tag{15}$$

где: $v_a^y(t)$ – фактическая пропускная способность *y*-й линии (информационного потока) в условиях *a*-й КА; $v^{\text{тр}\,y}(t)$ – пропускная способность, необходимая для

предоставления требуемого количества УС в заданный момент времени (t); $H_a^{yw}(t)$ – функция, описывающая a-ю КА с w-и параметрами на y-й элемент КС; $z_a^{yg}(t)$ – функция, описывающая ослабляющие способности g-о СрОИБ, применяемого для защиты y-о элемента КС;

$$v^{\text{тр}\,y}(t) \sum_{u=1}^{U_y} v_u^y , \tag{16}$$

где: v_u^y – требуемая скорость передачи данных для предоставления u-й услуги связи абонентам y-го элемента КС;

– вероятность выполнения функциональных задач в условиях изменения пропускной способности, вызванных a-м на группу элементов КА $\left(P_a^{\text{пс}}(t)\right)$:

$$P_a^{\text{пс}}(t) = f\left(v_a^{\Sigma}(t), V^{\text{КС}}(t), p_a^{yg}(t), s,\right), \tag{17}$$

где: $v_a^{\Sigma}(t)$ – фактическая пропускная способность группы линий связи (информационных потоков) в условиях a-й КА на КС; $V^{\text{КС}}(t)$ – пропускная способность, необходимая для предоставления требуемого количества УС в заданный момент времени (t); $p_a^{yg}(t)$ – функция, описывающая ослабляющие способности g-го механизма защиты или СрОИБ применяемого для защиты КС.

– разведзащищенность – вероятность вскрытия структуры КС $\left(P^{\text{вскр}}(t)\right)$ и идентификации информационных потоков $\left(p_y^{\text{ид}}(t), P^{\text{ид}}(t)\right)$ средствами сетевой и потоковой компьютерных разведок (КР):

$$P^{\text{вскр}}(t) = f\left(D_y^{\text{КС}}(t), s, H^{\text{СКР}}(t)\right), \tag{18}$$

где: $D_y^{\text{КС}}(t)$ – демаскирующие признаки y-го элемента КС, $H^{\text{СКР}}(t)$ – функция, описывающая возможности средств сетевой КР;

$$p_y^{\text{ид}}(t) = f\left(D_y^{\text{п}}(t), H_y^{\text{ПКР}}(t)\right), \tag{19}$$

где: $D_y^{\text{п}}(t)$ – демаскирующие признаки y-го информационного потока ($y \supseteq h$, h-я ИТ), $H_y^{\text{ПКР}}(t)$ – функция, описывающая возможности средств потоковой КР, выделяемых для идентификации y-го информационного потока КС;

$$P^{\text{ид}}(t) = f\left(p_y^{\text{ид}}(t), s, H^{\text{ПКР}}(t)\right), \tag{20}$$

где: $H^{\text{ПКР}}(t)$ – функция, описывающая возможности средств потоковой КР;

– имитостойкость – вероятность защиты от a-й КА, направленной на навязывание ложной информации или ложных режимов работы $\left(P_a^{\text{ис}}(t)\right)$:

$$P_a^{\text{ис}}(t) = f\left(a_{kh}^{\text{КС}}, H_a^{\text{ис}}(t)\right), \quad (21)$$

где: $a_h^{\text{КС}\,k}$ – *h*-я характеристика применяемого алгоритма идентификации (группы алгоритмов) (*k*-й ИТ), $H_a^{\text{ИС}}(t)$ – функция, описывающая *a*-ю КА, направленную на навязывание ложной информации или навязывания ложных режимов работы.

– мобильность – время (вероятность) реконфигурации КС рассматривается как механизм защиты от КА;

– криптостойкость КС не рассматривается, и предполагается, что средства криптографической защиты информации обеспечивают скрытие смыслового содержания передаваемой информации.

<u>для предоставляемых услуг связи</u>:

– действенность – вероятность установления соединения между элементами КС в условиях *j*-й КА $\left(P_a^{\text{соед}}(t)\right)$, вероятность предоставления УС в условиях КА на КС (элемент КС) $\left(P_a^U(t), p_a^u(t)\right)$, вероятность сохранения предоставляемой услуги связи в условиях КА на КС (элемент КС) $\left(P_a^{zU}(t), p_a^{zu}(t)\right)$.

<u>для восприятия услуг связи</u>:

– удовлетворенность абонентов провайдером связи – доля инцидентов ИБ, повлекших ухудшение качества предоставляемой УС, к количеству событий ИБ, зафиксированных СОИБ.

Выходными результатами моделей являются:

– для модели изменения уровня ИБ *i*-го СОИ, вызванного КА, – обобщенный показатель, характеризующий способность *i*-го СОИ выполнять функциональные задачи в условиях *a*-й КА $\left(z_a^i(t)\right)$ и заданного множества КА (*A*) $\left(Z^{iA}(t)\right)$:

$$z_a^i(t) = 1 - \left(1 - X_a^{Ri}(t)\right)\left(1 - X_a^{Oi}(t)\right)\left(1 - X_a^{Ki}(t)\right) \quad (22)$$

$$Z^{iA}(t) = \prod_{a=1}^{A} z_a^i(t). \quad (23)$$

– для модели изменения уровня защищенности *k*-й ИТ, вызванного КА – обобщенный показатель, характеризующий способность *h*-й ИТ выполнять функциональные задачи в условиях *a*-й КА $\left(z_a^k(t)\right)$ и заданного множества КА (*A*) $\left(Z^{kA}(t)\right)$:

$$z_a^k(t) = 1 - \left(1 - X_a^{Rk}(t)\right)\left(1 - X_a^{Kk}(t)\right) \quad (24)$$

$$Z^{kA}(t) = \prod_{a=1}^{A} z_a^k(t). \quad (25)$$

– для модели изменения уровня ИБ *y*-го элемента КС, вызванного КА:

– обобщенный показатель, характеризующий способность *y*-го элемента КС выполнять функциональные задачи в условиях *a*-й КА $\left(z_a^y(t)\right)$ и в условиях заданного множества КА (*A*) $\left(z^{yA}(t)\right)$:

$$z_a^y(t)=1-\left(1-k_a^{\text{ог}\,y}(t)\right)\left(1-p_a^{\text{пс}\,y}(t)\right)\left(1-p_a^{\text{ид}\,y}(t)\right)\left(1-p_a^{\text{ис}\,y}(t)\right) \tag{26}$$

$$z^{yA}(t)=\prod_{a=1}^{A} z_y^a(t). \tag{27}$$

– обобщенный показатель, характеризующий способность КС выполнять функциональные задачи в условиях *a*-й КА $\left(z_a^{\text{КС}}(t)\right)$ и в условиях заданного множества КА (*A*) $\left(z^{yA}(t)\right)$:

$$z_{\text{а}}^{\text{КС}}(t)=1-\left(1-K^{\text{ог}}(t)\right)\left(1-P_a^{\text{пс}}(t)\right)\left(1-P_a^{\text{вскр}}(t)\right)\left(1-P_a^{\text{ис}}(t)\right) \tag{28}$$

$$z^{\text{КС}\,A}(t)=\prod_{a=1}^{A} z_{\text{а}}^{\text{КС}}(t). \tag{29}$$

– для модели изменения безопасности предоставляемой *u*-й услуги связи вызванного КА – обобщенный показатель, характеризующий способность КС выполнять функциональные задачи:

$$z_{\text{а}}^{U}(t)=1-\left(1-P_a^{\text{соед}}(t)\right)\left(1-P_a^{U}(t)\right)\left(1-P_a^{zU}(t)\right) \tag{30}$$

$$Z^{UA}(t)=\prod_{a=1}^{A} z_{\text{а}}^{U}(t). \tag{31}$$

Заключение

Иерархическое представление рассматриваемого процесса позволило осуществить переход от оценок влияния различных видов КА на изменение свойств, характеризующих СОИ и ИТ, влияющих на качество предоставляемых услуг связи, к изменению свойств элементов КС, влияющих на качество сети.

Представленная модель (22-31) позволяет за счет комплексной оценки разнонаправленных факторов, выводящих систему из равновесного состояния, повысить достоверность оценки уровня ИБ КС и создает основу для адаптивного управления системы обеспечения ИБ, позволяющей предоставить требуемое количество услуг связи с заданным качеством в условиях различных компьютерных атак.

Сформулированные функциональные зависимости, не описанные аналитически, представляют собой постановку задачи для дальнейшего исследования.

Литература

1. Белов А. С., Добрышин М. М., Шугуров Д. Е. Функциональный подход к комплексной оценке уровня информационной безопасности элемента

корпоративной сети связи // Приборы и системы. Управление, контроль, диагностика, 2023. – № 3. – С. 30-39.
2. Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения».
3. Приказ ФСБ России от 19.06.2019 № 282 (ред. от 07.07.2022) «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации».
4. Методические рекомендации НКЦКИ по разработке Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации.
5. НКЦКИ Проект. Методические рекомендации по разработке плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации. 2023 г.
6. Советов Б. Я., Яковлев С. А. Моделирование систем: Учеб. для вузов – 3-е юд., перераб. и доп. – М.: Высш. шк., 2001. – 343 с: ил.
7. Добрушин М. М. Концептуальная модель оценки качества предоставления услуг связи в условиях компьютерных атак // Известия Тульского государственного университета. Технические науки, 2024. – № 2. – С. 263-269.
8. Добрышин М. М., Горбуля Д. С. Подходы оценки качества связи и предоставления услуг связи и задачи по их совершенствованию в рамках обеспечения информационной безопасности // Экономика и качество систем связи, 2023. – № 3 (29). – С. 60-71.
9. МСЭ-Т Е.802 (02/2007) Серия Е: Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы. Принципы и методики определения и применения параметров QoS.
10. Приказ Министерства информационных технологий и связи Российской Федерации от 27.09.2007 № 113 «Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования».
11. Давлятова М. А., Курочкина А. А., Стародубцева В. В. Оценка нормативных документов в области качества услуг, предоставляемых на базе инфотелекоммуникационной сети // Перспективы науки, 2016. – № 12 (87). – С. 107-110.
12. Квятковская И. Ю., Фам Куанг Хиеп. Система показателей оценки качества телекоммуникационных услуг и метод их оценки // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика, 2013. – № 2. – С. 98-103.
13. Давлятова М. А., Стародубцев Г. Ю., Хныкина Т. С. Эволюция развития теории и практики управления качества // Международный технико-экономический журнал, 2017. – № 2. – С. 82-85.

14. Белов А. С., Добрышин М. М., Шугуров Д. Е. Научно-методический подход к оцениванию качества систем обеспечения информационной безопасности // Приборы и системы. Управление, контроль, диагностика, 2022. – № 11. – С. 34-40.
15. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. Под редакцией профессора РАН, доктора технических наук Д. П. Зегжды. – М.: Горячая линия – Телеком, 2020. – 560 с.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЫНКА ЭКОСИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К.А. Ахрамеева, *к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», ksenya_2002@mail.ru;*
С.С. Вистунов, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», solekvis@yandex.ru.*

УДК 004.056

Аннотация. В данной статье представлен результат сравнительного анализа рынка готовых решений для внедрения экосистем информационной безопасности в разрезе крупного и среднего бизнеса. Определены преимущества и недостатки сравниваемых компаний, предоставляющих услуги развертывания экосистем информационной безопасности.

Ключевые слова: экосистема ИБ; защита; информация; информационная безопасность; технологии.

COMPARATIVE ANALYSIS OF THE INFORMATION SECURITY ECOSYSTEM MARKET

Kseniia Akhrameeva, *Ph.D. of Engineering Sciences, Associate Professor, The Bonch-Bruevich Saint Petersburg State University of telecommunications;*
Stepan Vistunov, *The Bonch-Bruevich Saint Petersburg State University of telecommunications.*

Annotation. This article presents the results of a comparative analysis of the market of ready-made solutions for the implementing for the information security ecosystems in large and medium-sized businesses. The advantages and disadvantages of the compared companies providing information security ecosystem deployment services are identified.

Keywords**:** information security ecosystem; protection; information; information security; technology.

Введение

В связи с активным развитием технологий информационной безопасности (ИБ) в современном мире, а также методов кибератак, для каждой компании немаловажным является правильный выбор поставщика защитного программного обеспечения, которое сформирует экосистему ИБ предприятия. Целью данной статьи является изучение рынка готовых решений для создания экосистем информационной безопасности, а также проведение сравнительного анализа компаний, предоставляющих такие решения.

Сравнительный анализ экосистем

Как правило, на рынке экосистемы информационные технологии представлены в виде продукта или наборов продуктов, которые поставляет некая компания-поставщик *(vendor)*. Такие фирмы могут иметь готовые решения для потребности компании в данный момент или же создавать конкретные решения по запросу компании-потребителя, которые будут предоставлены в виде локальной, облачной или гибридной модели экосистемы [1].

Большая часть компаний, которые предоставляют подобные услуги, реализуют свои решения с помощью облачной или гибридной модели экосистемы ИБ. Это связано с тем, что готовые решения уже развернуты на их серверах, а все, что остается сделать, это подключить к своей сети компанию-потребителя, однако такие фирмы могут предоставить для компании решение, которое ей необходимо, с реализацией локальной экосистемы. Основная проблема такого подхода заключается в том, что в случае, если компания-потребитель будет подвержена кибератаке, компания с локальной экосистемой будет в одиночку решать проблемы, последующие за атакой. А компания-поставщик отвечает только за установку оборудования и предоставление решения по безопасности. Также на компанию-потребителя возлагаются большие разовые затраты, которые будут включать в себя оплату оборудования и наем специалистов для работы в собственной инфраструктуре [6].

В случае если компания-поставщик предоставляет услуги типа *MSSP* (*Managed Security Service Providers*) или же *SECaaS* (*Security-as-a-Service*), означающие, что фирма предоставляет услуги безопасности как сервиса, то чаще придерживаются облачной или гибридной модели экосистем [1].

Разберем примеры предоставляемых услуг некоторых компаний, которые занимаются развертыванием экосистем информационной безопасности.

Компания «*BI.ZONE*». Сама компания имеет слоган *BI.ZONE*: «Комплексная кибербезопасность для вашего бизнеса». В основе концепции *BI.ZONE* лежит комплексный подход к обеспечению кибербезопасности и непрерывности бизнеса [2].

Компания предлагает набор практик и инструментов, позволяющих:

- повысить киберустойчивость компании в условиях постоянно меняющихся угроз;
- создать собственный центр кибербезопасности (*SOC*);
- использовать центр мониторинга по модели *SecaaS*;
- оснастить центр кибербезопасности компании.

BI.ZONE предлагает широкий спектр продуктов и услуг:

- средства для пентестинга (*BI.ZONE CPT*);
- платформа *BI.ZONE Bug Bounty* для запуска программ вознаграждения за найденные уязвимости;
- *BI.ZONE Secure DNS* для защиты бизнеса от атак с использованием *DNS*;
- *BI.ZONE Brand Protection* для защиты бренда;
- *BI.ZONE TDR Threat Detection and Response* – решение для непрерывного мониторинга безопасности;
- платформа для сбора, верификации и распространения потоков данных *Threat Intelligence*;
- служба получения сведений об актуальных киберугрозах *BI.ZONE ThreatVision*;
- *BI.ZONE Secure SD-WAN* – сервис для безопасной трансформации сети;
- *BI.ZONE AntiFraud* (*BI.ZONE BFP*) – средство противодействия мошенничеству;

- услуги по реагированию на инциденты;
- *BI.ZONE Compromise Assessment* – проверка всей инфраструктуры на предмет компрометации;
- приватное облако *BI.ZONE* для безопасного взаимодействия с внешним миром;
- *WAF* и защита электронной почты.

BI.ZONE работает по сервисной модели и специализируется на аутсорсинге.

Компания предлагает следующие услуги:

- функции сервис-провайдера;
- экспертные услуги и консалтинг;
- широкую линейку инструментов кибербезопасности;
- *BI.ZONE Compliance Platform* – решение для построения зрелых процессов, необходимых для соответствия требованиям федерального закона № 152-ФЗ;
- сервис «Виртуальный директор по кибербезопасности» (*BI.ZONE vCISO*).

Преимуществом компании является комплексный подход к индивидуальным стратегическим проектам в области кибербезопасности. Этот подход включает в себя несколько последовательных этапов, таких как аудит защиты, разработка архитектуры кибербезопасности, тестирование сервисов, аудит технической инфраструктуры, внедрение сервисов кибербезопасности, а также их сопровождение и поддержка. Заказчики, уже имеющие сформированные собственные команды по кибербезопасности, особенно заинтересованы в блоке решений по управлению уязвимостями, вознаграждениям за нахождение уязвимостей (баг-баунти) и использовании киберполигона.

Недостатками компании является то, что *BI.ZONE,* в основном, фокусируется на собственных продуктах и решениях, что может ограничить возможности интеграции с другими экосистемами ИБ, а также предоставляет неполный набор функций для управления экосистемой ИБ, что может потребовать использования дополнительных решений от других поставщиков.

Компания *R-Vision EVO* [4]. *R-Vision EVO* представляет собой экосистему взаимосвязанных технологий, компонентов и процессов, предназначенных для построения и развития *SOC* (*Security Operations Center*).

Создание экосистемы *R-Vision EVO* стало логичным продолжением многолетней работы компании по разработке продуктов для *SOC* [4].

Основная задача *R-Vision EVO*:

- предоставить компаниям возможность поэтапного развития *SOC*, его технологий и процессов;
- обеспечить комплексную кибербезопасность организации.

R-Vision использует лучшие практики риск-ориентированного подхода:

- инвентаризация активов;
- оценка рисков;
- мониторинг инфраструктуры;
- выявление инцидентов;
- реагирование на инциденты.

Все эти процессы непрерывны и позволяют эволюционно развивать *SOC*.

Внедрение технологий *R-Vision EVO*:

- расширяет возможности детектирования;
- обеспечивает дополнительный контекст при расследовании инцидентов;
- помогает избежать финансовых и репутационных потерь;

Построение эффективного *SOC* на базе *R-Vision EVO:*

- *Security Asset Management*: Формирование полной видимости инфраструктуры, оценка активов и их критической значимости.
- *Governance, Risk Management, Compliance*: Работа с рисками, оценка состояния защиты, определение вероятности реализации угроз и возможного ущерба.
- *Vulnerability Management*: Автоматизация работы с уязвимостями, их выявление, приоритизация и устранение.
- *Security Information and Event Management*: Мониторинг инфраструктуры, сбор событий со всех активов, их нормализация, хранение и анализ.
- *Security Orchestration, Automation and Response*: Автоматизация управления инцидентами в ИБ за счет преднастроенных сценариев.
- *User and Entity Behavior Analytics*: Детальное расследование инцидентов, обнаружение отклонений от нормального поведения пользователей и объектов;
- *Deception*: Имитация элементов инфраструктуры для обнаружения злоумышленников и замедления их передвижения в сети.
- *Threat Intelligence*: Всестороннее управление данными о киберугрозах.

Использование экосистемы кибербезопасности *R-Vision EVO* при создании *Security Operations Center* (*SOC*) предоставляет ряд преимуществ. Эта экосистема позволяет поэтапно расширять функциональность *SOC* в соответствии с потребностями организации, обеспечивая адаптацию к изменяющимся угрозам. Встроенные интеграционные механизмы, конфигурации и ролевые модели экосистемы упрощают процесс интеграции компонентов и обеспечивают единое управление и контроль над всеми технологиями *SOC*. [8] Компания *R-Vision* предлагает экосистемный подход, который помогает разрабатывать долгосрочные планы развития *SOC* и эффективно защищать организацию, предоставляя инструменты и ресурсы для планирования и управления развитием *SOC* с учетом специфических задач заказчика. Кроме того, вендор обеспечивает экспертную поддержку внедрения технологий *R-Vision EVO*, включая консультации, обучение персонала, настройку системы и постоянное сопровождение в процессе эксплуатации *SOC*. Цель развития экосистемы *R-Vision EVO* заключается в предоставлении заказчику уникального набора технологий, которые помогут создать долгосрочные планы развития *SOC* и будут полезны на всех этапах его развития.

Компания «Лаборатории Касперского» [3]. Экосистема информационной безопасности «Лаборатории Касперского» разработана компанией для активной борьбы за рынок экосистем ИБ. Она начала свое развитие с отдельных продуктов и постепенно перешла к комплексным решениям, объединяющим несколько систем информационной безопасности (ИБ-систем). В конце 2021 г. компания представила решение под названием *Kaspersky Symphony XDR*, которое является ключевым элементом экосистемы. *Symphony XDR* обладает технологиями автоматического предотвращения, мониторинга, обнаружения, расследования, проактивного поиска, анализа первопричин и предотвращения атак. Оно предназначено для компаний всех размеров и отраслей, но особенно актуально для крупных организаций, где высокие требования к безопасности и есть специалисты, работающие с передовыми решениями.

«Лаборатория Касперского» считает, что комплексный подход и экосистема информационной безопасности не являются одним и тем же. Экосистема должна включать все необходимое для борьбы с современными атаками и, в первую

очередь, предназначена для крупных компаний, таких как промышленные организации и финансовые учреждения. Вендор предлагает экосистемы, учитывающие специфику различных отраслей, и в 2022 г. представил *Kaspersky OT CyberSecurity*, которая ориентирована на промышленные предприятия [3]. Она включает в себя специализированную промышленную *XDR*-платформу *Kaspersky Industrial CyberSecurity* и интегрируется с экосистемой для корпоративного сегмента.

Экосистема «Лаборатории Касперского» предоставляет ряд преимуществ. Она позволяет заказчику сократить издержки, благодаря единому лицензированию, поддержке и управлению компонентами, а также обеспечивает доступ к передовой аналитике по угрозам. Технологически экосистема строится на централизации и автоматизации. Автоматизация сокращает трудозатраты аналитиков на типичные операции, снижает выгорание специалистов и устраняет человеческие ошибки. Централизация позволяет собирать и анализировать инциденты со всех интегрированных продуктов, обеспечивая фокусировку на значимых угрозах.

«Лаборатория Касперского» утверждает, что их экосистема информационной безопасности является не просто концепцией, а реальной потребностью, которая делает процессы обеспечения безопасности более стабильными, эффективными и прозрачными. Она предоставляет ИБ-командам продвинутые инструменты и технологии для борьбы с угрозами любого масштаба и сложности, не перегружая специалистов. В результате система безопасности становится целостной, гибкой и адаптивной к изменяющейся угрозой среде. Экосистема информационной безопасности «Лаборатории Касперского» стремится обеспечить комплексную защиту организаций, улучшить проективное обнаружение и реагирование на инциденты, а также повысить эффективность работы ИБ-специалистов.

Компания «Газинформсервис» [5]. «Газинформсервис» (ГИС) – это компания, предоставляющая комплексные решения в сфере ИБ. ГИС предлагает клиенту широкий спектр продуктов и услуг, в которые входят: средства защиты информации, услуги по аудиту и консалтингу, а также предлагает интеграцию готовых решений для экосистем ИБ. Это позволяет заказчику обеспечить комплексную защиту *IT*-инфраструктуры, при этом не обязательно переходить только на продукты компании ГИС, а возможно объединить в единый защитный комплекс применяемые программные продукты других компаний и продукты ГИС.

Продукты компании ГИС закрывают такие области, как:

- защита *ИТ*-инфраструктуры – линейка продуктов *Efros* (комплекс программных и программно-аппаратных средств, предназначенный для защиты информации от несанкционированного доступа, модификации, уничтожения, кражи и других угроз) [7];
- защита рабочих станций и серверов – *SafeNode* (программно-техническое средство, встраиваемое в *UEFI BIOS*, обеспечивающее защиту от несанкционированного доступа к рабочим станциям и серверам с момента их включения до момента старта операционной системы) [7] и Блокхост-сеть (средство контроля съемных машинных носителей информации, управления двухфакторной аутентификацией и защиты от несанкционированного доступа ресурсов рабочих станций и серверов);
- электронный документооборот – *Litoria* (создание внешнего и внутреннего юридически значимого электронного документооборота);
- защита *SAP* – *SafeERP* (многофункциональный модульный комплекс по защите бизнес-приложений *SafeERP* обеспечивает контроль безопасности *ERP* систем, размещенных на платформах *1С* и *SAP*);

- информационные системы – *СУБД Jatoba* (ПО общего назначения, предназначенное для создания и управления реляционными базами данных. *СУБД Jatoba* обеспечивает многопользовательский доступ к расположенным в ней данным с разным уровнем конфиденциальности) [10];
- управление *ИБ* – *Ankey ASAP* (Платформа расширенной аналитики безопасности с функциями поведенческого анализа на базе *ИИ*), *Ankey IDM* (Программный продукт для централизованного управления учетными записями пользователей и их полномочиями в корпоративных информационных системах, включающий лучшие решения *IGA* (*Identity Governance and Administration*)), *Ankey SIEM* (Система мониторинга событий информационной безопасности и выявления инцидентов в реальном времени) [9]. Обеспечивает комплексный мониторинг информационной безопасности как всей инфраструктуры организаций, так и отдельных подразделений, узлов и приложений. Система адаптируется практически к любой инфраструктуре и работает для всех уровней управления – от рядового администратора до руководителя предприятия).

Система управления информационной безопасностью «Газинформсервис» – это комплекс мер, направленных на обеспечение информационной безопасности организации. *СУИБ* «Газинформсервис» включает в себя разработку политик и процедур *ИБ*, аудит *ИБ*, обучение сотрудников по вопросам *ИБ* и другие мероприятия.

Материал выше предоставляет общее понимание, на каких задачах концентрируется та или иная фирма, с выводом об их преимуществах, что позволяет провести сравнительный анализ деятельности этих компаний (табл. 1).

Таблица 1.

Критерий	*BI.ZONE*	*R-VISION*	*Kaspersky*	ГИС
Фокус	Экспертиза, сервисная модель	Экосистемный подход, риск-ориентированный подход	Глобальный лидер, инновации	Готовые решения, интеграция экосистем
Продукты и услуги	Пентестинг, *Bug Bounty*, *SecaaS*, консалтинг	*EVO, SAM, EDR, Threat Intelligence*	Защита домашних пользователей, защита предприятий, *Threat Intelligence*	*Litoria, СЗИ “ Efros ”, SafeNode , Ankey ASAP, Ankey SIEM, Ankey IDM , СУБД Jatoba, SafeERP*
Подход к развитию *SOC*	Индивидуальный подход	Планомерное развитие	Разнообразные решения	Многоуровневая защита
Преимущества	Глубокая экспертиза, гибкость	Экосистемный подход, адаптивность	Глобальный охват, инновации	Широкий спектр продуктов и услуг, использование ИИ, интегрируемость
Недостатки	Относительно высокая стоимость	Требует квалифицированного персонала	Может быть сложно для небольших организаций	Относительно высокая стоимость услуг и продуктов

Каждая компания имеет свои особенности:

BI.ZONE:

- фокус на экспертизе: пентестинг, *Bug Bounty*, защита бренда;

- сервисная модель: *SecaaS*, экспертные услуги, консалтинг;
- индивидуальный подход: стратегические проекты, аудит, развертывание сервисов.

R-VISION:
- экосистемный подход: *EVO*, планомерное развитие *SOC*;
- риск-ориентированный подход: управление активами, оценка рисков;
- широкий спектр технологий: от *SAM* до *Threat Intelligence*.

Kaspersky:
- глобальный лидер: многолетний опыт, широкий охват рынка;
- широкий спектр продуктов: для всех типов организаций, от домашних пользователей до крупных предприятий;
- фокус на инновациях: машинное обучение, искусственный интеллект.

Газинформсервис
- комплексный подход к защите информации;
- интеграция рисков *ИБ* в существующую систему управления рисками;
- не требует строгого соответствия средств защиты информации одной экосистеме и работает с различными источниками.

Заключение

В данной статье проведен сравнительный анализ некоторых компаний, занимающихся предложением готовых решений или же создания необходимой экосистемы с учетом *IT*-инфраструктуры компании заказчика. Важно отметить, что не существует универсального решения для экосистемы по информационной безопасности и что лучшей экосистемой будет та, которая соответствует потребностям заказчика. При правильном подходе к выбору и реализации экосистемы можно значительно повысить уровень защиты организации от киберугроз. Важно учитывать, что не существует готового решения для каждой компании, а идеальной экосистемой информационной безопасности является экосистема, соответствующая всем требованиям компании заказчика.

Литература

1. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Cyber-Security-Ecosystems (дата обращениея апрель 2024 г.).
2. URL: https://bi.zone/ (дата обращениея апрель 2024 г.).
3. URL: https://www.kaspersky.ru (дата обращениея апрель 2024 г.).
4. URL: https://www.rvision.ru/ (дата обращениея апрель 2024 г.).
5. URL: https://www.gaz-is.ru/ (дата обращениея апрель 2024 г.).
6. Волкогонов В.Н., Гельфанд А.М., Деревянко В.С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019), 2019. – С. 262-266.
7. Волкогонов В.Н., Гельфанд А.М., Карамова М.Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019), 2019. – С. 266-270.
8. Виткова Л.А. и др. Конвергенция информационных технологий для повышения эффективности управления информационным пространством Санкт-Петербурга // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018), 2018. – С. 140-142.

9. Штеренберг С.И., Москальчук А.И., Красов А.В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Информационные технологии и телекоммуникации, 2021. – Т. 9. – С. 1-2.
10. Штеренберг С.И. Компьютерные вирусы. Часть 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. – 63 с. – EDN CMMEML.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ФОРМАТОВ SQL И NoSQL ДЛЯ ОПИСАНИЯ СОБЫТИЙ БЕЗОПАСНОСТИ

Э.В. Бирих, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, be1982@mail.ru;*
Н.С. Ершова, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Ershova.for.work@gmail.com.*

УДК 004.056

Аннотация. Проведено исследование форматов *SQL* и *NoSQL* в контексте использования их для описания событий безопасности. В результате представлен анализ особенностей, преимуществ и недостатков каждого из форматов, а также их применимость для описания событий безопасности. Рассмотрены различные сценарии использования и представлены примеры применения форматов для конкретных потребностей.

***Ключевые слова*:** события безопасности; *NoSQL*; *SQL*; базы данных; базы данных событий безопасности; описание событий безопасности.

COMPARATIVE ANALYSIS OF SQL AND NoSQL FORMATS FOR DESCRIBING SECURITY EVENTS

Ernest Birikh, *The Bonch-Bruevich Saint-Petersburg State University of Telecommunications;*
Natalya Ershova, *The Bonch-Bruevich Saint-Petersburg State University of Telecommunications.*

***Annotation*.** A study of the *SQL* and *NoSQL* formats has been conducted in order to use them to describe security events. As a result, an analysis of the features, advantages and disadvantages of each of the formats is presented, as well as their applicability to describe security events. Various usage scenarios are considered and examples of using formats for specific needs are presented.

***Keywords*:** security events; *NoSQL*; *SQL*; databases; databases of security events; description of security events.

Введение

Обработка событий безопасности играет критически важную роль в современной информационной безопасности. События безопасности могут включать в себя различные инциденты, такие как попытки взлома, вирусные атаки, утечки данных и другие потенциальные угрозы. Быстрое и эффективное реагирование на эти события может помочь предотвратить ущерб и минимизировать риски, а также выявить уязвимости в системе и принять меры по

их устранению и предотвращению возможных атак в будущем. Цель данной статьи – провести сравнительный анализ форматов *SQL* и *NoSQL* в контексте описания событий безопасности. Данная работа позволит обосновать выбор между этими форматами в зависимости от конкретных потребностей пользователя.

SQL (*Structured Query Language*) и *NoSQL* (*Not Only SQL*) – это два основных формата баз данных, которые могут быть использованы для описания событий безопасности. Они предоставляют средства для хранения, обработки и анализа данных о событиях безопасности, что позволяет специалистам по безопасности быстро выявлять угрозы и принимать меры. Важность эффективного описания и анализа событий безопасности не может быть недооценена. Выбор подходящего формата для хранения и обработки этих данных является критическим фактором.

Прежде чем приступить к анализу данных форматов, следует рассмотреть определения основных понятий, используемых в данной статье:

Событие безопасности – это некоторое происшествие в сети или системе, которое может иметь влияние на конфиденциальность, целостность или доступность данных [1]. Это может включать в себя широкий спектр инцидентов, от попыток несанкционированного доступа и вирусных атак до утечек данных и других нарушений безопасности [2]. События безопасности могут быть идентифицированы с помощью различных средств мониторинга и анализа, таких как системы обнаружения вторжений (*IDS*), системы предотвращения вторжений (*IPS*) и системы управления информацией и событиями безопасности (*SIEM*) [3].

Системы, поддерживающие эффективное программное обеспечение для автоматизированного анализа событий безопасности на основе технологий СУБД, позволяют регулярно вносить информацию о событиях в базу данных, а также выполнять сложные операции по хранению, фильтрации, отображению и поиску инцидентов безопасности [4].

Базы данных, хранящие информацию о событиях безопасности, имеют название базы данных событий безопасности (БДСБ). События в них добавляются специальным модулем, отвечающим за регистрацию событий безопасности. Информация о событиях направляется в модуль регистрации событий безопасности от модуля фильтрации событий аудита операционной системы и агентов дополнительной регистрации событий. Эти агенты отфильтровывают события аудита приложений и, при необходимости, регистрируют те события безопасности, которые не были зарегистрированы с помощью инструментов аудита операционной системы и приложений [1].

Периодическое пополнение базы данных может происходить, например, с помощью программы конвертера данных, который преобразует данные из журналов аудита операционной системы и приложений [5]. Непрерывное пополнение базы данных происходит с помощью модуля регистрации событий, который в режиме реального времени отслеживает состояние журналов аудита и пополняет БД при обнаружении новых записей.

Форматы *SQL* и *NoSQL* в контексте описания событий безопасности

SQL – это стандартный язык для управления данными в реляционных базах данных. *SQL* базы данных используют структурированный подход, где информация организована в таблицы, и каждая из них имеет определенную схему, определяющую структуру данных [6]. *SQL* поддерживает сложные запросы и обеспечивает мощные средства для анализа данных. В контексте описания событий безопасности *SQL* может быть использован для хранения, обработки и анализа данных о различных инцидентах безопасности, таких как попытки взлома, вирусные атаки, утечки данных и т.д.

К преимуществам использования *SQL* для описания событий безопасности можно отнести следующее:

- Структурированность. *SQL* базы данных применяют структурированный подход, что позволяет эффективно организовать данные о событиях безопасности. Это облегчает поиск и анализ данных.
- Сложные запросы. *SQL* предоставляет мощные средства для выполнения сложных запросов. Это может быть особенно полезно при анализе событий безопасности, когда необходимо выявить сложные взаимосвязи и корреляции.
- Транзакционность. *SQL* базы данных поддерживают транзакции, что обеспечивает целостность данных даже в случае сбоев или ошибок.
- Безопасность. Большинство *SQL* баз данных предлагают продвинутые функции безопасности, такие как управление доступом, шифрование данных и аудит.

Недостатки и ограничения *SQL* в этом контексте описания событий безопасности:

- Масштабируемость. *SQL* базы данных могут столкнуться с проблемами масштабируемости при обработке очень больших объемов данных о событиях безопасности.
- Гибкость схемы. *SQL* требует строгой схемы данных, что может быть неудобно при работе с неструктурированными данными, такими как логи событий безопасности.

Если говорить о примерах использования *SQL* для описания событий безопасности, то он может быть использован для создания таблицы *security_events.*

На рис. 1 показан пример создания таблицы, которая содержит данные о различных событиях безопасности.

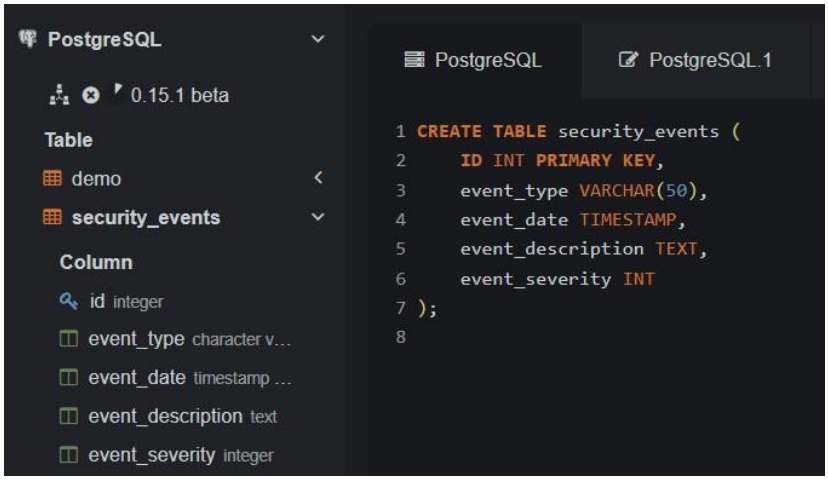


Рисунок 1

Затем можно использовать *SQL* – запросы для добавления, извлечения и анализа данных о событиях безопасности. Например, запрос на рис. 2 добавляет новое событие безопасности в таблицу.

```
INSERT INTO security_events (ID, event_type, event_date,
                             event_description, event_severity)
VALUES (1, 'Unauthorized Access Attempt', '2024-04-20 00:00:00',
        'An unauthorized access attempt was detected.', 5);
```

Рисунок 2

А запрос на рис. 3 извлекает все события безопасности с высокой степенью серьезности.

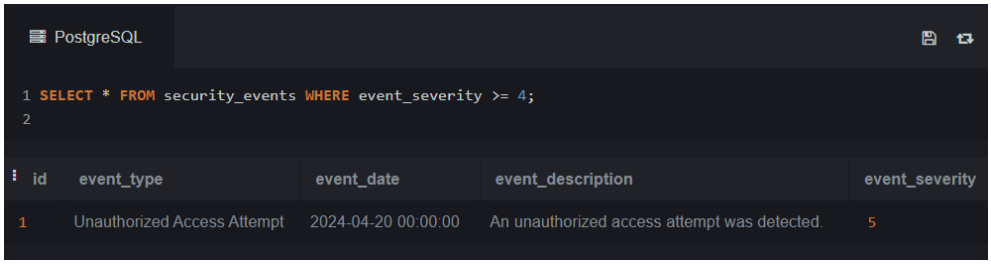


Рисунок 3

Это лишь некоторые из примеров того, как *SQL* может быть использован для описания и анализа событий безопасности. Однако возможности *SQL* в этом контексте значительно шире и могут включать в себя более сложные запросы и аналитические функции.

NoSQL – это альтернативный подход к управлению данными, который был разработан для обработки больших объемов данных, которые могут быть структурированы, полуструктурированы или неструктурированы. *NoSQL* базы данных не требуют фиксированной схемы, они могут масштабироваться горизонтально и гарантируют высокую эффективность при работе с большими объемами данных [7]. *NoSQL* включает в себя различные типы баз данных, такие как документо-ориентированные, ключ-значение, колоночные и графовые базы данных. В контексте описания событий безопасности, *NoSQL* может быть использован для хранения и обработки больших объемов данных о событиях безопасности, включая неструктурированные данные, такие как логи, сетевой трафик и т.д.

Так как информация о событиях безопасности приходит из разных мест, то зачастую рационален выбор баз данных семейства *NoSQL* для получения, хранения и обновления в режиме реального времени большого потока информации. С целью оптимизации запросов к данным о событиях безопасности в *NoSQL* базах данных можно использовать индексы, кэширования данных и партиционирования. Индексы позволяют быстро находить данные по определенным атрибутам, кэширование данных позволяет ускорить доступ к часто запрашиваемым данным, а партиционирование позволяет распределить данные по нескольким узлам для увеличения производительности.

Преимущества использования *NoSQL* для описания событий безопасности:

- Гибкость схемы. *NoSQL* базы данных не требуют фиксированной схемы, что позволяет легко и быстро адаптироваться к изменяющимся требованиям и структурам данных. Это может быть особенно полезно при работе с неструктурированными данными, такими как логи событий безопасности.

- Масштабируемость. *NoSQL* базы данных обеспечивают высокую горизонтальную масштабируемость, что позволяет эффективно обрабатывать большие объемы данных.
- Быстродействие. *NoSQL* базы данных имеют высокую производительность при работе с большими объемами данных, что может быть критически важно при обработке данных о событиях безопасности в реальном времени [8].

Недостатки и ограничения *NoSQL* в этом контексте:

- Сложность запросов. *NoSQL* базы данных могут не поддерживать такой широкий спектр сложных запросов, как *SQL*. Это может ограничить возможности анализа данных о событиях безопасности.
- Транзакционность. В отличие от *SQL*, многие *NoSQL* базы данных не поддерживают полную *ACID* транзакционность, что может быть проблемой в некоторых сценариях.

NoSQL может быть использован для хранения и обработки больших объемов данных о событиях безопасности. Например, документо-ориентированная *NoSQL* база данных, такая как *MongoDB*, может быть использована для хранения логов событий безопасности в формате *JSON*.

Также можно использовать *NoSQL* запросы для извлечения и анализа данных о событиях безопасности. Например, описанный на рис. 4 код создает коллекцию «*security_events*», вставляет новый документ в коллекцию «*security_events*». Документ, который добавляется, содержит информацию о событии безопасности, включая идентификатор события, тип события, дату события, описание события и уровень серьезности события. Далее выполняется поиск в коллекции «*security_events*» и извлекаются все документы, где значение поля «*event_severity*» больше или равно 4 (высокая степень серьезности).

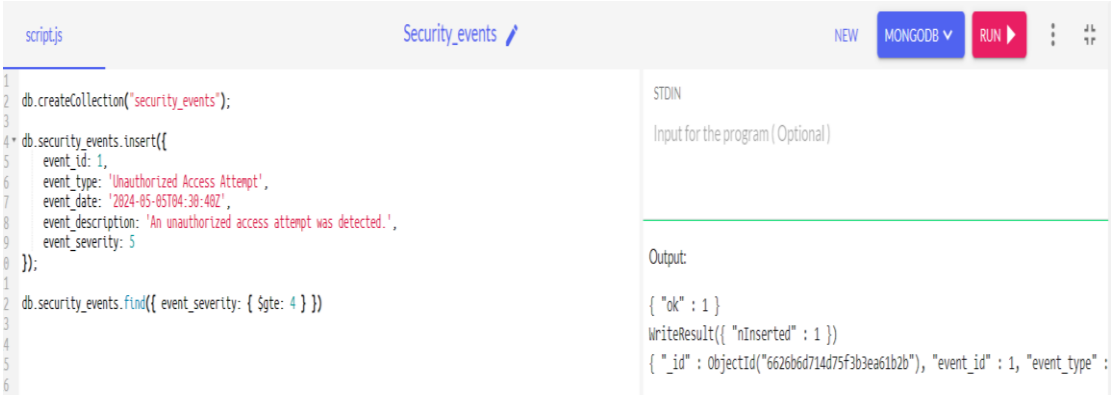


Рисунок 4

Это лишь некоторые из примеров того, как *NoSQL* может быть использован для описания и анализа событий безопасности. *NoSQL* следует выбирать для описания событий безопасности, когда необходимо обрабатывать большие объемы данных с высокой скоростью и гибкостью.

Сравнительный анализ *SQL* и *NoSQL*

Нереляционные *NoSQL* базы данных отличаются от реляционных *SQL* тем, что они не используют традиционную схему таблиц и связей между ними. Вместо этого они используют различные модели данных, такие как документы, ключ-

значение, столбцы и графы [9]. Эти модели данных позволяют гибко хранить и обрабатывать данные о событиях безопасности.

SQL и *NoSQL* базы данных могут предложить различные показатели, которые полезны в зависимости от конкретных требований системы и условий использования. Рассмотрим их более подробно на примере *MySQL* и *MongoDB*. Результаты представлены в табл. 1.

Таблица1.

	SQL	***NoSQL***
Тип	Реляционный	Нереляционный
Данные	Структурированные данные, хранящиеся в таблицах	Неструктурированные данные, хранятся в файлах *JSON*
Схема	Статический	Динамический
Масштабируемость	Вертикальный	Горизонтальный
Язык	Язык структурированных запросов	Язык неструктурированных запросов
Объединение элементов (*Joins*)	Присутствует для написания сложных запросов	Отсутствует
OLTP	Рекомендуется в *OLTP*-системах	С наименьшей вероятностью будет рассмотрен в системе *OLTP*
Поддержка	Активная поддержка	Расширяется
Интегрированное кэширование	Поддерживает встроенную память	Поддерживает интегрированное кэширование
Гибкость	Жесткая схема, привязанная к отношениям	Нежесткая схема и гибкость
Операции	*ACID*	Теоремы *CAP*
Эластичные запросы	В большинстве случаев требуется время простоя	Автоматические, не требующие отключения

Описанные выше характеристики *SQL* и *NoSQL* баз данных могут напрямую влиять на эффективность описания событий безопасности следующим образом:

Данные и схема. Тип данных, которые необходимо хранить, может определить, какой формат базы данных будет наиболее эффективным. *SQL* использует фиксированную схему, что обеспечивает структурированность и предсказуемость данных, в то время как *NoSQL* предлагает гибкую схему, что позволяет легко адаптироваться к изменяющимся требованиям и структурам данных, также он полезен для работы с данными, которые не имеют жесткой структуры, например, данные о поведении пользователей.

Масштабируемость. *SQL* базы данных обычно поддерживают вертикальное масштабирование, означающее, что можно увеличить производительность, добавив больше ресурсов (например, *CPU, RAM*) к серверу. Однако, они могут столкнуться с проблемами при горизонтальном масштабировании (т.е., добавлении большего количества серверов). *NoSQL* базы

данных предлагают высокую горизонтальную масштабируемость, подразумевающую, что можно увеличить производительность, добавив больше серверов в систему [10]. Это может быть особенно полезно при обработке больших объемов данных о событиях безопасности. Если данные сравнительно статичны и не ожидается значительного роста, то *SQL* может быть более подходящим.

Язык. SQL предлагает мощный язык запросов для сложного анализа данных, что может быть полезно при исследовании событий безопасности. *NoSQL* может быть менее мощным в этом отношении, но некоторые *NoSQL* базы данных предлагают гибкие языки запросов, в зависимости от типа базы данных (например, *MongoDB* использует *JavaScript*-подобный язык запросов), которые могут быть достаточно мощными для многих задач.

Объединение (*Joins*). Если присутствует необходимость связывать данные из разных таблиц или коллекций, *SQL* может быть более эффективным благодаря своей поддержке операций объединения. Большинство *NoSQL* баз данных не поддерживают операции объединения.

OLTP. Если нужно обрабатывать транзакции, *SQL* может быть более эффективным, благодаря своей поддержке *ACID* транзакций. *NoSQL* может поддерживать транзакции, но это зависит от конкретной базы данных.

Поддержка. SQL базы данных имеют долгую историю и большое сообщество поддержки, что может облегчить решение проблем и улучшение производительности. *NoSQL* базы данных также имеют активные сообщества, но они могут быть менее зрелыми.

Интегрированное кэширование. Некоторые *NoSQL* базы данных предлагают интегрированные возможности кэширования, что может улучшить производительность при обработке больших объемов данных. *SQL* базы данных, как правило, нуждаются в специализированном решении для кэширования, таком как *Memcached.*

Гибкость. *NoSQL* базы данных обычно более гибкие в отношении структуры данных и схемы, что может быть полезно при работе с неструктурированными данными, такими как логи событий безопасности [6]. *SQL* базы данных требуют более строгой структуры и схемы [11].

Операции. *SQL* поддерживает широкий спектр операций и функций, включая сложные запросы и аналитические функции. *NoSQL* базы данных могут поддерживать различные операции, в зависимости от типа базы данных, но они могут быть менее мощными для сложных запросов [12].

Эластичные запросы. Некоторые *NoSQL* базы данных, такие как *Elasticsearch,* поддерживают эластичные запросы, что позволяет выполнять гибкие и динамические запросы. *SQL* базы данных обычно требуют более строгих и статических запросов.

Пример использования

Рассмотрим пример события безопасности, которое включает в себя обнаружение несанкционированного доступа к системе.

Если используется *SQL* база данных для описания этого события, можно создать таблицу с полями для *IP*-адреса, времени доступа, местоположения и других связанных данных. *SQL* позволяет вам легко связывать эти данные с другими таблицами, например, с таблицей пользователей или таблицей серверов. Это может быть полезно для анализа паттернов поведения и выявления подозрительной активности. Однако, если объем данных очень большой или данные приходят в большом объеме и быстро меняются, *SQL* база данных может столкнуться с проблемами производительности и масштабируемости.

Если используется *NoSQL* база данных, например, документо-ориентированная база данных типа *MongoDB*, можно хранить данные о событии безопасности в формате *JSON*, что может включать в себя различные типы данных, и можно легко добавлять новые типы данных по мере необходимости. *NoSQL* база данных может легко масштабироваться для обработки больших объемов данных, что может быть полезно для обработки больших потоков данных о событиях безопасности в реальном времени. Однако, *NoSQL* может быть менее эффективным для сложного анализа данных, так как он не поддерживает сложные запросы и операции объединения, как *SQL*.

В обоих случаях выбор между *SQL* и *NoSQL* будет зависеть от конкретных требований к описанию событий безопасности, включая объем данных, скорость изменения данных, необходимость в сложном анализе данных и другие факторы.

Примеры использования *SQL* баз данных для хранения и анализа данных о событиях безопасности

В области обработки событий безопасности *SQL* базы данных могут быть использованы для хранения и анализа данных о событиях безопасности. Приведем несколько примеров:

Журналы аудита. *SQL* базы данных могут быть использованы для хранения журналов аудита, которые содержат информацию о действиях, произведенных пользователями или системами. Это может включать в себя действия, такие как вход в систему, изменение настроек безопасности или доступ к конфиденциальной информации.

События IDS/IPS. Системы обнаружения и предотвращения вторжений (*IDS/IPS*) часто используют *SQL* базы данных для хранения информации об обнаруженных угрозах. Это может включать в себя детали о типе угрозы, целевом устройстве и времени обнаружения.

Данные об угрозах. *SQL* базы данных могут быть использованы для хранения данных об угрозах, таких как *IP*-адреса, связанные с известными злонамеренными активностями, или хэши файлов, связанных с вредоносным ПО.

События журнала безопасности. *SQL* базы данных могут быть использованы для хранения событий из журналов безопасности, таких как журналы безопасности *Windows* или журналы событий *Linux.*

Важно отметить, что при использовании *SQL* баз данных для обработки событий безопасности необходимо учесть некоторые вопросы безопасности. Например, база данных должна быть защищена от несанкционированного доступа, а данные должны быть зашифрованы при хранении и передаче. Кроме того, может потребоваться регулярное резервное копирование данных для обеспечения их восстановления в случае сбоя или атаки.

Рекомендации по использованию *NoSQL* баз данных и их возможности для хранения и анализа данных о событиях безопасности

Различные типы *NoSQL* предоставляют множество возможностей, поэтому выбор конкретного типа зависит от требований к системе обработки событий безопасности. Для решения задач мониторинга кибербезопасности можно использовать различные базы данных *NoSQL* в зависимости от конкретных требований и объема данных, например:

1. Документно-ориентированные базы данных хранят данные в формате документов, что особенно полезно при хранении неструктурированных данных о событиях безопасности, таких как логи и сообщения. Эти базы данных обеспечивают гибкость и масштабируемость, а также возможность анализировать данные с помощью запросов на языке запросов к документам

(например, *MongoDB*). Например, системы мониторинга событий могут использовать их для хранения логов событий в виде документов, содержащих информацию о времени события, типе события и других атрибутах. Индексы могут быть использованы для быстрого поиска логов по определенным атрибутам.

2. Столбцовые базы данных предоставляют возможность хранить данные в виде столбцов, что особенно полезно при обработке больших объемов структурированных данных, таких как журналы событий безопасности. Эти базы данных обеспечивают быстрый доступ к данным и масштабируемость, а также возможность анализировать данные с помощью запросов на языке запросов к столбцам (например, *Apache Cassandra*) [13]. Системы управления доступом могут использовать эти базы данных для хранения информации о пользователях, ролях и правах доступа к определенным ресурсам [14].
3. Ключ-значение базы данных позволяют хранить данные в виде пар ключ-значение, что особенно полезно при хранении метаданных о событиях безопасности, таких как время и место события [15]. Также они могут быть использованы для отслеживания сессий пользователей и ассоциированных с ними событий безопасности. Ключ может представлять собой идентификатор сессии, а значение – детали сессии или связанные события безопасности. Эти базы данных обеспечивают высокую производительность и масштабируемость, а также возможность анализировать данные с помощью запросов на языке ключ-значение (например, *Redis*).
4. Графовые базы данных представляют данные и связи в виде графа, что особенно полезно при анализе связей между различными событиями безопасности. Эти базы данных обеспечивают гибкость и масштабируемость, а также возможность анализировать данные с помощью запросов на языке графовых запросов (например, *Neo4j*). Такие базы данных могут быть использованы системами обнаружения вторжений для хранения информации о событиях безопасности и их связях с узлами, представляющими пользователей, ресурсы и другие объекты в системе безопасности. Это позволяет быстро находить связанные события и анализировать их в контексте системы безопасности.

Заключение

В соответствии с проведенным исследованием, итоговым результатом данной статьи является таблица, в которой отображены характеристики исследуемых форматов. В результате исследования описаны преимущества и недостатки форматов *SQL* и *NoSQL* в контексте описания событий безопасности, а также даны рекомендации по использованию форматов. Этот сравнительный анализ позволяет выбрать оптимальный формат для системы в соответствии с её требованиями безопасности.

Помимо вышеперечисленного, дальнейшее развитие исследования в этой области может быть направлено не только на углубление понимания процессов, но и на моделирование надежной защиты информации, хранящейся в базах данных. Это подчеркивает важность выбора правильного формата базы данных для описания событий безопасности.

В целом, использование баз данных и средств автоматизированного анализа данных является важным шагом в обеспечении безопасности информационных систем и защите от кибератак. Описание событий безопасности с помощью верно подобранной БД позволяет выделять общие черты инцидентов, по ним составлять шаблоны, а также выводить необходимую информацию для их анализа и

ликвидирования, что во многом повышает эффективность анализа событий и быстрого реагирования на инциденты.

Литература

1. Макаревич О. Б., Шелудько И. А. Регистрация и анализ событий безопасности в информационных системах // Известия ТРТУ, 2003. – № 4 (33). – С. 211-216.
2. Бирих Э. В., Виткова Л. А., Гореленко В. В., Казаков Д. Б. Защита информации в базах данных // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Материалы конференции АПИНО 2017, 2017. – С. 89-92.
3. Ушаков И. А. Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных: Дис. канд. техн. наук: 05.13.19; [Место защиты: Санкт-Петербургский институт информатики и автоматизации Российской академии наук]. – Санкт-Петербург, 2020. – 32 с.
4. Шелудько И.А. Разработка и исследование системы оперативного сетевого мониторинга событий безопасности: Дис. канд. техн. наук: 05.13.19; [Место защиты: Таганрогский государственный радиотехнический университет]. – Таганрог, 2004. – 179 с.
5. Цифровые технологии и проблемы информационной безопасности / под ред. Е.В. Стельмашонок, И.Н. Васильевой. – СПб.: Изд-во СПбГЭУ, 2021. – 47 с.
6. URLhttps://cc.bingj.com/cache.aspx?q=1+таблица+1+sql+nosql+тип+реляционный+нереляционный+данные+структурированные&d=456867736448676&mkt=en-US&setlang=en-US&w=ut03PNqWZEwdmGPcoiZ_RsXI9-_-UIKr (дата обращения – апрель 2024 г.).
7. URL https://habr.com/ru/companies/otus/articles/760226/ (дата обращения – апрель 2024 г.).
8. URL https://cc.bingj.com/cache.aspx?q=данных+требуют+фиксированной+схемы+могут+масштабироваться+горизонтально+обеспечивают+высокую+производительность&d=4835038350961123&mkt=en-US&setlang=en-US&w=Zb11VPLBF02WuOhch2q4_y9CxOfCDF1F (дата обращения – апрель 2024 г.).
9. URL https://www.guru99.com/ru/nosql-tutorial.html (дата обращения – апрель 2024 г.).
10. URL https://veesp.com/ru/blog/sql-or-nosql/ (дата обращения – апрель 2024 г.).
11. URL https://kartaslov.ru/книги/Ponin_Fedor_Методика_эффективного_управления_данными_в_IT-проектах/3 (дата обращения – апрель 2024 г.).
12. URL https://bpium.ru/blog/chem-baza-dannyh-luchshe-elektronnoy-tablicy (дата обращения – апрель 2024 г.).
13. URL https://www.arsis.ru/blog/nosql (дата обращения – апрель 2024 г.).
14. URL https://www.astera.com/ru/knowledge-center/sql-vs-nosql/ (дата обращения – апрель 2024 г.).
15. URL https://habr.com/ru/companies/otus/articles/562852/ (дата обращения – апрель 2024 г.).

АТАКИ И МЕТОДЫ ЗАЩИТЫ ПРИ ИСПОЛЬЗОВАНИИ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ В КОНТЕКСТЕ СТЕГОАНАЛИЗА ЦИФРОВОГО КОНТЕНТА

Д.И. Сивков, *Национальный исследовательский университет ИТМО, sivkov@itmo.ru;*
М.Ю. Федосенко, *Национальный исследовательский университет ИТМО, аспирант, fedosenkomaksim98@gmail.com.*

УДК 004.056

Аннотация. Статья освещает роль методов машинного обучения в стегоанализе – выявлении скрытой информации в цифровых носителях. Описывается, как различные методы, в том числе глубокие нейронные сети и графовые сети, используются для улучшения процессов обнаружения стеганографии, обеспечивая более эффективную защиту данных. Рассматривается их применение, преимущества и ограничения, а также риски, связанные с атаками на машинное обучение и методы защиты.

Ключевые слова: стеганография; машинное обучение; нейронные сети; атаки отравления; атаки с уклонением; атаки на модель.

ATTACKS AND DEFENSE METHODS WHEN USING MACHINE LEARNING METHODS IN THE CONTEXT OF STEGOANALYSIS OF DIGITAL CONTENT

D. Sivkov, *National Research University ITMO;*
M. Fedosenko, *National Research University ITMO.*

Annotation. The article highlights the role of machine learning methods in steganalysis – identifying hidden information in digital media. Describes how various techniques, including deep neural networks and graph networks, are used to improve steganography detection processes, providing more effective data protection. Reviews their applications, advantages and limitations, and risks associated with machine learning attacks, and discusses defense methods.

Keywords*:* steganography; machine learning; neural networks; poisoning attacks; evasion attacks; attacks on the model.

Введение

В нашем быстро меняющемся цифровом мире стеганография и стегоанализ становятся все более важными понятиями в области информационной безопасности. В то время как стеганография предоставляет способы для скрытой передачи данных, стегоанализ стремится эти способы обнаружить и анализировать. С развитием машинного обучения возникают новые подходы к распознаванию и классификации скрытых сообщений, что позволяет раскрыть новые горизонты в обнаружении цифровых угроз и обеспечении конфиденциальной информации [1].

Целью данной работы является анализ методов машинного обучения на применимости в задачах стеганоанализа. Каждый из данных методов имеет свои особенности и сферы применения, что подчеркивает необходимость тщательного выбора инструментов в зависимости от конкретных задач и типов данных. Работа содержит в себе решение следующих задач:

1. Анализ особенностей методов машинного обучения с выделением их достоинств и недостатков для задач обработки стеганоконтейнеров.

2. Выявление подходов искусственного интеллекта (*AI*) и соответствующих им технологий под конкретные виды контейнеров: изображение, текст, файлы.
3. Разбор возможных атак на системы искусственного интеллекта применительно к интеллектуальным системам стеганоанализа.
4. Формулирование подходов защиты от атак на интеллектуальные системы стеганоанализа со стороны вредоносных изменений обрабатываемого информационного контента.

Таблицы, представленные в данной статье, демонстрируют сравнительный анализ разнообразных методов машинного обучения, каждый из которых привносит свой вклад в понимание применения методов машинного обучения в стеганографии, учитывая при этом свои уникальные особенности и области применения. Эти методы варьируются от глубоких нейронных сетей до графовых нейронных сетей, отражая многообразие подходов и спецификаций, необходимых для успешного стегоанализа. Однако не стоит забывать о присущих им ограничениях и сложностях, которые могут возникнуть при работе со сложными задачами обнаружения. Вместе с возможностями, методы машинного обучения приносят и угрозы, такие как атаки с уклонением, отравления данных и модельные атаки, которые могут подорвать эффективность стегоанализа в контексте разработки интеллектуальной модели анализа контента. В ответ на эти вызовы, применяются различные методы защиты, исследование которых также является целью данной работы.

Теоретические основы машинного обучения в стегоанализе

Стегоанализ, сложный процесс анализа скрытой информации в цифровых носителях, в последнее время активно развивается благодаря применению методов машинного обучения [2]. Важность теоретической базы в данной области сложно переоценить, так как она лежит в основе понимания, каким образом алгоритмы могут «учиться» распознавать и анализировать стеганографические вложения.

Применение различных методов машинного обучения в стегоанализе открывает новые перспективы для распознавания и классификации скрытых сообщений в цифровых средствах. Табл. 1 представляет собой сравнение нескольких подходов, каждый из которых имеет свои уникальные особенности и области применения.

Таблица 1.

Методы машинного обучения	**Подходит для**	**Особенности**
Глубокие нейронные сети [3]	Общего анализа	Многослойная обработка
Сверточные нейронные сети [4]	Изображений и видео	Специализирован на визуальных данных
Рекуррентные нейронные сети [5]	Последовательностей (текст, аудио)	Учитывает временную последовательность
Сети долгой краткосрочной памяти [6]	Длительных последовательностей	Эффективен для долгосрочных зависимостей

Методы машинного обучения	Подходит для	Особенности
Автокодировщики [7]	Реконструкции и обнаружения	Использует обучение без учителя
Ограниченные машины Больцмана [8]	Вероятностного моделирования	Эффективен для извлечения признаков
Глубокая сеть доверия [9]	Сложных вероятностных моделей	Мощный, но сложный в настройке
Графовые нейронные сети [10]	Анализа графов и сетей	Подходит для структурированных данных

Из представленного сравнения видно, что каждый метод машинного обучения имеет свои сильные стороны в зависимости от контекста применения. Выбор метода зависит от множества факторов, включая тип и структуру данных, требуемую точность и сложность моделирования. Сбалансированный выбор подхода к машинному обучению позволяет повысить эффективность процесса стегоанализа, одновременно оптимизируя ресурсы и время обработки.

Однако, как и любая технология, методы машинного обучения не лишены недостатков, особенно когда речь идет о сложных задачах стегоанализа. В табл. 2 приведены ключевые недостатки различных методов машинного обучения в стегоанализе.

Таблица 2.

Методы машинного обучения	Недостатки
Глубокие нейронные сети [3]	Требуют большого количества данных для обучения и сложны в настройке
Сверточные нейронные сети [4]	Не эффективны для обработки временных последовательностей и анализа неструктурированных данных
Рекуррентные нейронные сети [5]	Могут страдать от проблемы затухания градиента и сложны в работе с очень длинными последовательностями
Сети долгой краткосрочной памяти [6]	Сложны в настройке и тренировке, а также требовательны к вычислительным ресурсам
Автокодировщики [7]	Могут неэффективно работать с сильно зашумленными данными и риск переобучения
Ограниченные машины Больцмана [8]	Сложны в понимании и настройке, а также могут быть неэффективными для очень сложных задач

Методы машинного обучения	Недостатки
Глубокая сеть доверия [9]	Требуют значительных вычислительных ресурсов и сложны в настройке, а также интерпретации
Графовые нейронные сети [10]	Ограничены в обработке неструктурированных данных, а также сложность в интерпретации результатов

Анализ недостатков, представленных в табл. 2, подчеркивает значимость тщательного планирования и тестирования при внедрении методов машинного обучения в практику стегоанализа. Понимание и принятие во внимание ограничений каждого метода является критически важным для минимизации ошибок и увеличения надежности результатов. Это также подчеркивает важность постоянного развития и адаптации моделей машинного обучения в соответствии с постоянно меняющимися требованиями информационной безопасности.

Методы машинного обучения для стегоанализа цифрового контента

На основе анализа случаев использования технологий искусственного интеллекта в задачах стеганоанализа выделены технологии, применение которых целесообразно как для несбалансированного характера набора данных контента интернет-ресурсов, так и для специфики данной отрасли. Конкретные технологии для подходов *Artificial Intelligence* в задачах стеганоанализа [11] в зависимости от покрывающего объекта представлены в табл. 3.

Таблица 3.

Вид вложения	Подход *AI*	Технология
Изображение	Методы обработки изображений (компьютерное и машинное зрение)	Рендеринг Сопоставление шаблонов Бинаризация Сегментация Счетчик пикселей Обнаружение и измерение краев изображений Оптическое распознавание Анализ признаков (текстуры, гистограммы) Пространственная и фильтрация Фильтры Габора Фильтры *ICA* Детекторы *LoG*, *DoG*, Харриса Дескриптор *SIFT* частотная
Лингвистическая стеганография	Обработка естественного языка (*Natural language processing*)	*AlchemyAPI*, *Expert System S.p.A.*, *General Architecture for Text Engineering* (*GATE*), *Modular Audio Recognition Framework, MontyLingua*, *Natural Language Toolkit* (*NLTK*)

Вид вложения	Подход *AI*	Технология
Цифровая стеганография	Методы машинного обучения (с учителем, без учителя)	Наивный Байес, деревья решений, логистическая регрессия, *k*-ближайших соседей, метод опорных векторов, линейная регрессия, полиномиальная регрессия, Метод *k*-средних, *Mean-Shift, DBSCAN, SOM*
Новые виды сокрытия информации	Нейронные сети (свёрточные сети)	Нейронная сеть Хопфилда Самоорганизующаяся карта Кохонена Нейронная сеть Ворда Сеть Хэмминга Сеть Элмана Многослойный перцептрон Перцептрон Розенблатта Когнитрон *AlexNet,* *ResNets*, *VGGs*, *Inception*

Исходя из анализа технологий, можно определить следующие области применения искусственного интеллекта, которые особенно подходят для стеганоанализа:

- Классификация: этот процесс включает в себя отнесение объектов к определенным классам на основании их атрибутов, где классы известны заранее. Эта задача решается с использованием методов обучения с учителем.
- Кластеризация: задача заключается в выявлении групп объектов (кластеров) по их характеристикам, при этом количество и свойства кластеров не заданы заранее. Решается с помощью методов обучения без учителя и нейронных сетей.
- Регрессия: предполагает определение значений атрибутов объекта на основе его взаимосвязей с другими объектами. Методы как обучения с учителем, так и без учителя используются для выявления этих зависимостей.
- Прогнозирование: включает как классификацию объектов и регрессионный анализ их характеристик, так и определение конечных объектов и их свойств. Методы машинного обучения применяются для первой категории задач, а нейронные сети – для второй.
- Аппроксимация: ищет функцию, которая максимально точно описывает данные или упрощает их для анализа взаимосвязей и создания новых объектов. Применяются нейронные сети для моделирования процессов мышления и принятия решений на основе ограниченных данных.
- Сжатие данных: направлено на устранение избыточности данных для экономии ресурсов и улучшения точности прогнозов ИИ, используя алгоритмы минимизации ошибок. Задача решается через ассоциативную память и алгоритмы обратного распространения ошибки в нейронных сетях, а также через предварительную обработку данных.
- Оптимизация: заключается в выборе наилучших параметров для создания эффективной и экономичной модели ИИ. Решается через предварительную обработку данных и использование самоорганизующихся нейронных сетей для оптимизации конкретных моделей ИИ [11].

Безопасность методов машинного обучения применительно к стегоанализу

Модели машинного обучения, хотя и являются мощными инструментами для обнаружения стеганографических сообщений, также могут быть уязвимы для ряда атак. Угрозы безопасности могут подорвать целостность и надежность систем стегоанализа, делая защиту моделей критически важной задачей.

Типы угроз и атак на модели машинного обучения

1. Атаки с уклонением представляют собой методы, используемые для обмана систем обнаружения стеганографии, обычно реализуемых с помощью алгоритмов машинного обучения. Цель таких атак – модифицировать стеганографический контент таким образом, чтобы он не был обнаружен как подозрительный [12].

Виды атак с уклонением:

1) Модификация изображений, предположим, есть изображение, в которое встроено стеганографическое сообщение. Стеганоанализатор, обученный на определенном наборе признаков, может обнаружить такие изменения. Атакующий может добавить в изображение специальный шум или применить техники обработки изображений, чтобы изменить эти признаки и сделать их менее заметными для системы стегоанализа, сохраняя при этом встроенное сообщение.
2) Адаптивные методы стеганографии изменяют способ встраивания сообщения в зависимости от содержимого носителя. Например, сообщение может быть встроено в области изображения с высокой текстурой, где изменения менее заметны. Таким образом, даже если стеганоанализатор обучен распознавать изменения в низкотекстурных областях, атака с уклонением будет направлена на уклонение от этих областей, уменьшая вероятность обнаружения.
3) Генеративно-состязательные сети могут быть использованы для создания стеганографических изображений, которые выглядят естественно и не вызывают подозрений у систем машинного обучения. *GAN* обучается генерировать изображения, которые не только содержат стеганографическую информацию, но и успешно обходят обнаружение путем имитации нормального распределения признаков в немодифицированных изображениях.

2. Атаки отравления включают намеренное введение некорректных, манипулированных или вредоносных данных в обучающий набор данных, с которым работает система обнаружения стеганографии. Целью такой атаки является искажение процесса обучения модели машинного обучения, чтобы ослабить ее способность правильно классифицировать данные и обнаруживать стеганографические сообщения в будущем [13].

Разновидности атак с отравлением данных:

1) Атакующий может предоставить исследователям или системам безопасности стеганографические изображения, которые ошибочно помечены как чистые. Если эти изображения используются в обучающем наборе данных, то обученная на них модель может стать менее чувствительной к реальным стеганографическим вложениям.
2) Злоумышленник может внедрить в обучающий набор сложноструктурированные образцы, которые маскируются под безопасный контент, но при этом содержат стеганографические данные. Таким образом, модель обучается рассматривать подобные шаблоны как нормальные, что снижает точность будущего обнаружения.

3. Атаки на модель представляют собой вид атак на системы машинного обучения, где атакующий использует выходные данные модели для восстановления информации о входных данных или о самой модели. Эти атаки могут быть использованы для восстановления стеганографического сообщения, скрытого в носителе, или для получения информации о параметрах стеганографического алгоритма [14].

Разновидности атак на модели машинного обучения:

1) Если атакующий имеет доступ к стегоанализатору, который определяет наличие стеганографического сообщения в носителе, он может попытаться изменять входные данные и наблюдать за реакцией системы, чтобы восстановить скрытое сообщение. Например, изменяя пиксели изображения и изучая изменения в выходных данных модели, атакующий может вывести характеристики встроенного сообщения и даже восстановить его содержимое.
2) Атакующий может использовать доступ к модели стегоанализа, чтобы определить специфические характеристики стеганографического алгоритма, используемого для скрытия информации. Путем постепенного модифицирования входных данных и анализа выходных данных, можно выявить, какие параметры алгоритма были использованы для встраивания сообщения, что позволит эффективнее создавать стеганографический контент, который трудно обнаружить.
3) В ситуации, когда атакующий пытается обнаружить, как модель делает прогнозы относительно наличия или отсутствия стеганографии, он может использовать различные входные данные для создания «карты» решений модели. Это может включать в себя попытку определить границы решения или даже восстановить функцию потерь, используемую при обучении модели.

Способы защиты от атак

1. Состязательное обучение – это метод обучения машинного обучения, направленный на повышение устойчивости моделей к атакам с уклонением, в том числе к состязательным примерам. Этот метод включает в обучающий процесс примеры, специально разработанные для введения модели в заблуждение, тем самым заставляя ее «учиться» на своих ошибках и становиться более устойчивой к подобного рода атакам [15].

Способы применения состязательного обучения:

1) Исследователь может генерировать изображения, в которые встроены стеганографические сообщения с использованием различных алгоритмов и техник. Затем эти изображения могут быть искусственно модифицированы для создания состязательных примеров, которые затрудняют обнаружение встроенных сообщений существующими методами стегоанализа. Включая эти модифицированные изображения в набор данных для обучения, можно улучшить способность модели обнаруживать стеганографию, даже если она была специально адаптирована для уклонения от детекции.
2) Создается модель машинного обучения, которая обучается обнаруживать стеганографические сообщения в изображениях. В процессе обучения модели предъявляются не только обычные примеры стеганографии, но и адверсариальные примеры, созданные для обхода детекции. Это позволяет модели адаптироваться к разнообразным стратегиям скрытия информации и повышает ее эффективность в условиях реального использования.
3) После обучения модель стегоанализа может быть протестирована на новом наборе состязательных примеров, чтобы оценить ее устойчивость к атакам

с уклонением. Этот подход позволяет идентифицировать потенциальные слабости в модели и дополнительно улучшить ее защищенность.

2. Регуляризация в машинном обучении – это метод, направленный на предотвращение переобучения модели за счет добавления дополнительного ограничения (штрафа) на величину весов модели. Это помогает улучшить обобщающую способность модели на новых, невиданных данных, делая ее менее чувствительной к шуму в обучающем наборе данных. В контексте стеганографии и стегоанализа регуляризация может использоваться для улучшения устойчивости и точности моделей, обнаруживающих стеганографические вложения [16].

Способы применения регуляризации:

1) При разработке модели машинного обучения для обнаружения стеганографических сообщений в мультимедийных файлах, таких как изображения или аудио, использование регуляризации помогает предотвратить переобучение на особенности конкретного набора данных. Например, $L1$-регуляризация (*Lasso*) может быть использована для обеспечения разреженности весов модели, что полезно для выявления наиболее значимых признаков, указывающих на наличие стеганографии, в то время как $L2$-регуляризация (*Ridge*) помогает снизить общую величину весов, делая модель менее чувствительной к шуму в данных.
2) В сценариях, где генеративные модели, такие как генеративно-состязательные сети, используются для создания стеганографических вложений, регуляризация может способствовать генерации более естественно выглядящих изображений или аудиофайлов, в которые встроено скрытое сообщение. Это уменьшает вероятность обнаружения встроенной информации аналитическими инструментами.
3) Разработчики стеганографических алгоритмов могут применять регуляризацию для минимизации изменений, вносимых в контейнер (например, в изображение), тем самым снижая обнаружимость стеганографического сообщения. Например, методы, основанные на минимизации общего вариационного регуляризатора, могут использоваться для сохранения гладкости и структурных особенностей изображения при встраивании в него информации, делая модификации менее заметными для стегоанализа.

3. Ансамблевые методы в машинном обучении – это подходы, при которых для принятия окончательного решения используются несколько обучающих моделей. Основная идея состоит в том, что комбинация предсказаний от множества моделей приведет к лучшей производительности, чем использование любой отдельной модели. Это достигается за счет уменьшения дисперсии (*variance*), смещения (*bias*) и ошибок из-за случайных флуктуаций в обучающем наборе данных [17].

Кейсы применения ансамблевых методов:

1) В контексте стегоанализа ансамблевые методы могут использоваться для комбинирования различных детекторов стеганографии. Например, можно использовать ансамбль из разных типов нейронных сетей, таких как сверточные нейронные сети (*CNN*) для обработки изображений и рекуррентные нейронные сети (*RNN*) для обработки временных последовательностей аудиофайлов, чтобы повысить точность обнаружения стеганографических сообщений.
2) Иногда одна модель лучше работает с определенными типами стеганографии, в то время как другая модель лучше справляется с другими типами. Создание ансамбля, включающего различные методы стегоанализа,

такие как анализ наименьших значащих битов (*LSB analysis*) и частотный анализ, может обеспечить более всестороннее обнаружение.

3) Методы усиления, такие как *AdaBoost*, могут использоваться для комбинирования нескольких слабых классификаторов стеганографии в более мощный ансамбль. Например, несколько простых детекторов, каждый из которых способен обнаружить только определенные виды стеганографических вмешательств, могут быть объединены, чтобы создать систему, способную эффективно обнаруживать широкий спектр стеганографических методов.

Заключение

Стегоанализ представляет собой динамично развивающуюся область, в которой применение методов машинного обучения в будущем будет играть важную роль. В результате анализа интеллектуальных подходов, таблицы 1 и 2 показывают, что каждый из методов обучения обладает определенными преимуществами и недостатками, варьирующимися в зависимости от типа данных и специфики задачи. Важно осознавать, что ни один метод не является универсальным решением, и именно сочетание различных подходов часто приводит к наиболее эффективным системам стегоанализа.

С другой стороны, необходимо учитывать потенциальные угрозы и уязвимости, связанные с применением машинного обучения в области стеганографии. Учет этих угроз крайне важен при разработке комплексной программной системы интеллектуального стеганоанализа информационного контента, поскольку злоумышленник за счет изменения данных способен нарушить процесс работы данного компонента защиты [11]. Осведомленность об атаках с уклонением, отравления данных и атаках на модель позволяет разработать защитные механизмы, такие как состязательное обучение, регуляризация и ансамблевые методы, которые повышают устойчивость и надежность моделей. Эти методы позволяют не только улучшить точность обнаружения, но и обеспечить защиту от современных и сложных форм атак. Следует также отметить, что применение состязательного обучения, регуляризации и ансамблевых методов может существенно повысить способность моделей выявлять и противостоять новым видам и формам стеганографии, обеспечивая тем самым более надежную защиту информации.

В перспективе, сочетание продвинутых методов машинного обучения с глубоким пониманием специфики стегоанализа открывает новые возможности для создания более эффективных и устойчивых систем защиты информации, вносит вклад в такие научные отрасли, как криптографическая защита информации и искусственный интеллект, реализует приоритет стратегии научно-технологического развития РФ «Переход к передовым технологиям проектирования и создания высокотехнологичной продукции, основанным на применении интеллектуальных производственных решений, роботизированных и высокопроизводительных вычислительных систем, новых материалов и химических соединений, результатов обработки больших объемов данных, технологий машинного обучения и искусственного интеллекта» [18].

Литература

1. Юренский П.В. Методы статистического и нейросетевого стегоанализа скрытых каналов // Инновации в науке, 2019. – № 1. – С. 11-13.
2. Дрюченко М.А., Сирота А.А. Стегоанализ цифровых изображений с использованием глубоких нейронных сетей и гетероассоциативных интегральных преобразований // Прикладная дискретная математика, 2022. – № 55. – С. 36-56.

3. Созыкин А.В. Обзор методов обучения глубоких нейронных сетей // Вестник ЮУрГУ. Серия: Вычислительная математика и информатика, 2017. – № 3. – С. 28-59.
4. Скрипачев В. О., Гуйда М. В., Гуйда Н. В., Жуков А. О. Особенности работы сверточных нейронных сетей // International Journal of Open Information Technologies, 2022. – № 12. – С. 53-60.
5. Андросова Е.Е. Применение рекурсивных рекуррентных нейронных сетей // Новые информационные технологии в автоматизированных системах, 2016. – № 19. – С. 107-114.
6. Пустынный Я.Н. Решение проблемы исчезающего градиента с помощью нейронных сетей долгой краткосрочной памяти // Инновации и инвестиции, 2020. – № 2. – С. 130-132.
7. Ваняшкин Ю.Ю., Макаров Д.А., Попова И.А., Соболева Е.Д. Применение автокодировщиков для устранения шумов с изображений // StudNet, 2020. – № 10. – С. 27-38.
8. Абросимов М.А., Бровко А.В. Метод обучения слоев свертки в искусственной нейронной сети с помощью ограниченной машины Больцмана // Вестник СГТУ, 2015. – № 1. – С. 114-117.
9. Татьянкин В.М., Дюбко И.С. Нейронные сети глубокого доверия в сравнение с многослойным персептроном // Вестник ЮГУ, 2015. – № 2. – С. 87-89.
10. Циликов Н.С., Федосин С.А. Графовые нейронные сети // Вестник МГУ, 2012. – № 2. – С. 161-163.
11. Федосенко М.Ю., Беззатеев С.В. Анализ проблематики применения методов стеганографии при осуществлении противоправных действий и ее роли в цифровой криминалистике // Проблемы информационной безопасности. Компьютерные системы, 2023. – № 3. – С. 33-57.
12. Костюмов В.В. Обзор и систематизация атак уклонением на модели компьютерного зрения // International Journal of Open Information Technologies, 2022. – № 10. – С. 11-20
13. Намиот Д.Е. Введение в атаки отравлением на модели машинного обучения // International Journal of Open Information Technologies, 2023. – № 3. – С. 58-68.
14. Намиот Д.Е. Схемы атак на модели машинного обучения // International Journal of Open Information Technologies, 2023. – № 5. – С. 68-86.
15. Li H., Namiot D. A Survey of adversarial attacks and defenses for image data on deep learning // International Journal of Open Information Technologies, 2022. – № 5. – С. 9-16.
16. Тимофеева О.П., Неимущев С.А., Неимущева Л.И., Тихонов И.А. Распознавание эмоций по изображению лица на основе глубоких нейронных сетей // Труды НГТУ им. Р. Е. Алексеева, 2020. – № 1. – С. 16-24.
17. Фирюлина М.А., Каширина И.Л. Описание процесса прогнозирования проблемных состояний с применением ансамблевых методов машинного обучения // Инженерный вестник Дона, 2022. – № 4. – С. 34-46.
18. URL https://нтр.рф/challenges-priorities/ (дата обращения – июль 2024 г.).

АНАЛИЗ ПОТЕНЦИАЛЬНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ В РЕЗУЛЬТАТЕ ОСУЩЕСТВЛЕНИЯ СТЕГАНОГРАФИЧЕСКИХ АТАК

М.Ю. Федосенко, *Национальный исследовательский университет ИТМО, аспирант, fedosenkomaksim98@gmail.com.*

УДК 004.056

Аннотация. Данная работа представляет собой обзор и анализ угроз информационной безопасности, осуществление которых прямо или косвенно возможно в результате применения злоумышленниками методов стеганографии в корыстных целях. Данные угрозы были взяты из Банка данных угроз информационной безопасности ФСТЭК России. В работе представлено их описание, выделен потенциальный злоумышленник и объект его воздействия. В результате получены основные вектора атак злоумышленников, а также наиболее уязвимые компоненты информационной инфраструктуры предприятия для данного вида атак.

Ключевые слова: информационная безопасность; угрозы; стеганография; БДУ ИБ ФСТЭК; нарушение целостности информации; нарушение доступности информации; нарушение конфиденциальности информации.

ANALYSIS OF POTENTIAL THREATS TO INFORMATION SECURITY OF ENTERPRISE COMPUTER INFRASTRUCTURE AS A RESULT OF STEGANOGRAPHIC ATTACKS

M. Fedosenko, *National Research University.*

Annotation. This work is a review and analysis of information security threats, the implementation of which is directly or indirectly possible as a result of the use of steganography methods by attackers for personal gain. These threats were taken from the Data Bank of Information Security Threats of the FSTEC of Russia. The work presents their description, identifying a potential attacker and the object of his influence. As a result, the main attack vectors for attackers were obtained, as well as the most vulnerable components of an enterprise's information infrastructure to this type of attack.

Keywords: information security; threats; steganography; BDU IS FSTEC; information integrity; information availability; information confidentiality.

Введение

В настоящее время практически каждое предприятие имеет компьютерную инфраструктуру. Она же, в свою очередь, является одной из главных целей нарушителей при осуществлении атак, направленных на предприятие. Это обусловлено тем, что компьютерные инфраструктуры предприятий содержат большое количество цифровых данных и обеспечивают стабильность работы многих компонентов. Нарушение данной стабильности, а именно нарушение целостности, доступности и конфиденциальности процесса работы систем и хранящейся на них информации, способна привести к финансовым и репутационным потерям [1]. Поэтому немаловажной задачей достижения качества и стабильности бизнес –процессов предприятия является задача обеспечения качественного уровня информационной и компьютерной безопасности.

Задача защиты информации известна с давних времен. В разные эпохи развития общества ее решали разными способами. Одним из самых важных подходов является шифрование, в последствии чего появилась наука криптография [2]. Однако с процессом перехода общества от индустриального в постиндустриальное, который выражается в его цифровизации, объемы информации и способов ее обмена значительно увеличились, что привело к увеличению способов атак злоумышленников. В своих атаках хакеры применяют все более новые и изощренные способы, одним из которых является использование стеганографии – метода сокрытия злонамеренной информации внутри легитимной. В среде специалистов в области информационной безопасности уже известны случаи применения стеганографии при реализации компьютерных атак, а также для обмена преступными данными [3]. Одним из самых громких примеров является сокрытие информации в фотографиях, размещенных на сайте *Ebay* террористической группировкой «Аль-Каида» [4].

Целью данной работы является анализ угроз информационной безопасности, реализация которых возможна при применении злоумышленником методов стеганографии в процессе осуществления компьютерных атак. Для достижения поставленной цели необходимо решить следующие задачи:

1. Рассмотреть имеющиеся данные об угрозах информационной безопасности согласно открытому банку данных ФСТЭК,
2. Установить нарушителя и объект его атаки в рамках атакуемой информационной системы,
3. Определить потенциал злоумышленника и вектор атаки на основе объекта атаки и деструктурирующего воздействия,
4. Проанализировать действия злоумышленника и возможные деструктурирующие воздействия на информационную систему,
5. Сравнить полученные результаты, оценить перспективы реализации представленных угроз.

Угрозы информационной безопасности

Для сравнения потенциальных угроз информационной безопасности, возможных в результате стеганографических атак, обратимся к Банку данных угроз от ФСТЭК России [5]. Он представляет собой сборник сведений об основных угрозах и уязвимостях, которые характерны для автоматизированных систем управления, государственных информационных систем. Банк угроз ФСТЭК, помимо названия и кода угрозы, содержит ее краткое описание, вероятные источники, объекты воздействия и, конечно, последствия, которые повлечет за собой реализация угрозы. Первоначальной целью создания банка угроз ФСТЭК являлось повышение информированности специалистов ИБ о существующих угрозах безопасности информации в автоматизированных системах. В основном он использовался заказчиками, операторами, разработчиками информационных систем и систем защиты, применялся лабораториями и органами сертификации средств защиты информации [6].

Что касается проблемы скрытого обмена данных, то ФСТЭК России выделяет под нее конкретную угрозу – УБИ.111 «Угроза передачи данных по скрытым каналам» [7]. Суть ее заключается в возможности осуществления нарушителем неправомерного вывода защищаемой информации из системы, а также передачи управляющих команд путем ее нестандартного (незаметного, скрытого) размещения в легитимно передаваемых по сети (или сохраняемых на отчуждаемые носители) открытых данных путем ее маскирования под служебные протоколы, сокрытия в потоке других данных (стеганография), использования скрытых пикселей («пикселей отслеживания»). Данная угроза обусловлена

недостаточностью мер защиты информации от утечки, а также контроля потоков данных. Реализация возможна при:

1. Наличии у нарушителя прав в дискредитируемой системе на установку специализированного программного обеспечения, реализующего функции внедрения в пакеты данных, формируемых для передачи в системе, собственной информации;
2. Доступа к каналам передачи данных;
3. Посещении пользователем сайтов в сети интернет и открытия электронных писем, содержащих скрытые пиксели.

Однако, помимо явно выделенной в базе данных от ФСТЭК угрозы, связанной непосредственно с скрытым обменом данных, существуют также угрозы, имеющие к ней косвенное отношение. Это обусловлено тем, что наличие данных угроз может являться следствием осуществления атак с использованием скрытых каналов связи. Среди таких угроз можно выделить следующие:

- Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением (УБИ.068) [8]: Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на *API* в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава *API*). Данная угроза обусловлена наличием слабостей в механизме проверки входных данных и команд *API*, используемого программным обеспечением.

  Реализация данной угрозы возможна в условиях:

  – Наличия у нарушителя доступа к *API.*

  – Отсутствия у дискредитируемого приложения механизма проверки вводимых данных и команд.
- Угроза неправомерных действий в каналах связи (УБИ.069) [9]: Угроза заключается в возможности внесения нарушителем изменений в работу сетевых протоколов путем добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи. Данная угроза обусловлена слабостями сетевых протоколов, заключающимися в отсутствии проверки целостности и подлинности получаемых данных.

  Реализация данной угрозы возможна:

  − При условии осуществления нарушителем несанкционированного доступа к сетевому трафику.
- Угроза несанкционированного копирования защищаемой информации (УБИ.088) [10]: Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путем проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съемный носитель (или в другое место, доступное нарушителю вне системы). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне.

  Реализация данной угрозы возможна в случае:

  − Отсутствия криптографических мер защиты или снятия копии в момент обработки защищаемой информации в нешифрованном виде.
- Угроза подмены содержимого сетевых ресурсов (УБИ.130) [11]: Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемым данным пользователей сети

или проведения различных мошеннических действий путем скрытной подмены содержимого хранящихся (сайты, веб-страницы) или передаваемых (электронные письма, сетевые пакеты) по сети данных. Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности содержимого электронного сообщения.

Реализация данной угрозы возможна при условии:

– Наличия у нарушителя прав на доступ к сетевым ресурсам.

– Отсутствии у пользователя сети мер по обеспечению их целостности.

- Угроза пропуска проверки целостности программного обеспечения (УБИ.145) [12]: Угроза заключается в возможности внедрения нарушителем в дискредитируемую систему вредоносного программного обеспечения путем обманного перенаправления запросов пользователя или его программ на собственный сетевой ресурс, содержащий вредоносное программное обеспечение, для его «ручной» или «автоматической» загрузки с последующей установкой в дискредитируемую систему от имени пользователя или его программ. Данная угроза обусловлена слабостями механизмов проверки целостности файлов программного обеспечения и/или проверки подлинности источника их получения.

  Реализация данной угрозы возможна при условии успешного использования обманных техник одного из следующих методов:

  – «Ручного метода» – нарушитель, используя обманные механизмы, убеждает пользователя перейти по ссылке на сетевой ресурс нарушителя, что приводит к запуску вредоносного кода на компьютере пользователя, или убеждает пользователя самостоятельно загрузить и установить вредоносную программу (например, под видом игры или антивирусного средства).

  – «Автоматического метода» – нарушитель осуществляет деструктивное воздействие переадресацию функции автоматического обновления дискредитируемой программы на собственный вредоносный сервер.

- Угроза сбоя обработки специальным образом измененных файлов (УБИ.149) [13]: Угроза заключается в возможности осуществления нарушителем различных неправомерных действий от имени дискредитированных приложений путем вызова сбоя в их работе за счет внесения изменений в обрабатываемые дискредитируемыми программами файлы или их метаданные. Данная угроза обусловлена слабостями механизма проверки целостности обрабатываемых файлов и корректности содержащихся в них данных.

  Реализация данной угрозы возможна в условиях:

  – Наличия у нарушителя сведений о форматах и значениях файлов, вызывающих сбой функционирования дискредитированных приложений при их обработке.

  – Успешно созданном в дискредитируемой системе механизме перехвата управления над обработкой нарушителем программного сбоя.

- Угроза эксплуатации цифровой подписи программного кода (УБИ.162) [14]: Угроза заключается в возможности повышения нарушителем привилегий в системах, использующих цифровую подпись кода в качестве связующей информации между программой и ее привилегиями, путем дискредитации механизма подписывания программного кода. Данная угроза обусловлена слабостями в механизме подписывания программного кода.

Реализация данной угрозы возможна при следующих условиях:

− Дискредитируемый программный код написан с помощью фреймворка (*framework*), поддерживающего подписывание программного кода.

− Дискредитируемый программный код подписан вендором (поставщиком программного обеспечения).

− Нарушитель имеет возможность внедрить программный код в дискредитируемый компьютер.

- Угроза неправомерного шифрования информации (УБИ.170) [15]: Угроза заключается в возможности фактической потери доступности защищаемых данных из-за их несанкционированного криптографического преобразования нарушителем с помощью известного только ему секретного ключа.

  Данная угроза обусловлена наличием слабостей в антивирусной защите, а также в механизмах разграничения доступа.

  Реализация данной угрозы возможна при условии:

  − Успешной установки нарушителем на дискредитируемый компьютер средства криптографического преобразования информации.

  − Успешного обнаружения (идентификации) нарушителем защищаемых файлов.
- Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью (УБИ.177) [16]: Угроза заключается в возможности возникновения ошибок в работе системы вследствие отсутствия (или игнорирования) процедуры обнаружения и исправления ошибок в данных, вводимых во время работы самим оператором, до активизации управляемого оборудования. Кроме того, к реализации данной угрозы могут привести некорректно реализованные (или отсутствующие) средства реагирования на неправильные, самопроизвольные действия оператора, средства учета нижних/верхних пределов скорости и направления реакции оператора, схемы реагирования на двойное нажатие клавиш при вводе обычных и критических данных, процедуры формирования временных пауз с возможностью выбора разных ответов (да/нет и т.п.).

  Реализуемость данной угрозы зависит от:

  − Требований, предъявляемых к процедурам обнаружения и исправления ошибок во вводимых данных в систему, связанную с безопасностью.

  − Разницы между этими требованиями и фактическим уровнем обнаружения и исправления ошибок.
- Угроза несанкционированной модификации защищаемой информации (УБИ.179) [17]: Угроза заключается в возможности нарушения целостности защищаемой информации путем осуществления нарушителем деструктивного физического воздействия на машинный носитель информации или деструктивного программного воздействия (в т.ч. изменение отдельных бит или полное затирание информации) на данные, хранящиеся на нем.

  Реализация данной угрозы возможна в случае получения нарушителем системных прав на запись данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия
- Угроза подмены программного обеспечения (УБИ.188) [18]: Угроза заключается в возможности осуществления нарушителем внедрения в

систему вредоносного программного обеспечения за счет загрузки и установки вредоносного программного обеспечения, скрытого под видом легитимного свободно распространяемого программного обеспечения. Данная угроза обусловлена наличием у пользователя прав для установки программного обеспечения из сети интернет.

Реализация данной угрозы возможна:

– При скачивании программного обеспечения в сети интернет.

- Угроза маскирования действий вредоносного кода (УБИ.189) [19]: Угроза заключается в возможности сокрытия в системе действий вредоносного кода за счет применения специальных механизмов маскирования кода (архивирование, изменение формата данных и др.), которые препятствуют его дальнейшему анализу. Данная угроза обусловлена наличием способов маскирования программного кода, не учтенных сигнатурными базами средств защиты информации, а также механизмов операционной системы, позволяющих осуществить поиск модулей средств защиты информации.

  Реализация данной угрозы возможна при условии:

  – Использования в системе устаревших версий средств защиты информации.
- Угроза внедрения вредоносного кода в дистрибутив программного обеспечения (УБИ.191) [20]: Угроза заключается в возможности осуществления нарушителем заражения системы путем установки недоверенного дистрибутива, в который внедрен вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты.

  Реализация данной угрозы возможна при:

  – Применении пользователем сторонних дистрибутивов.

  – Отсутствии антивирусной проверки перед установкой дистрибутива.
- Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика (УБИ.193) [21]: Угроза заключается в возможности утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика, скрывающих сам факт передачи данных. Данная угроза обусловлена слабостями мер защиты информации при хранении, обработке и передаче информационных ресурсов.

  Реализация данной угрозы возможна:

  – При условии успешного внедрения в дискредитируемую систему указанного вредоносного программного обеспечения.

  – При отсутствии или недостаточной реализации мер межсетевого экранирования.

Помимо понимания сути угрозы, необходимо также установить потенциального злоумышленника для ее реализации, а также объект его воздействия – компонент информационной инфраструктуры предприятия. Соотношение источников и объектов воздействия для приведенных угроз представлено в табл. [6].

Код	Угроза	Источник	Объект
УБИ.111 [7]	Угроза передачи данных по скрытым каналам	Внешний нарушитель со средним потенциалом. Внутренний нарушитель со средним потенциалом.	Сетевой узел. Сетевое программное обеспечение. Сетевой трафик.
УБИ.068 [8]	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Внешний нарушитель со средним потенциалом. Внутренний нарушитель со средним потенциалом.	Системное программное обеспечение. Прикладное программное обеспечение. Сетевое программное обеспечение. Микропрограммное обеспечение. Реестр.
УБИ.069 [9]	Угроза неправомерных действий в каналах связи	Внешний нарушитель с низким потенциалом.	Сетевой трафик
УБИ.088 [10]	Угроза несанкционированного копирования защищаемой информации	Внешний нарушитель с низким потенциалом. Внутренний нарушитель с низким потенциалом.	Объекты файловой системы. Машинный носитель информации.
УБИ.130 [11]	Угроза подмены содержимого сетевых ресурсов	Внешний нарушитель с низким потенциалом.	Прикладное программное обеспечение. Сетевое программное обеспечение, сетевой трафик.
УБИ.145 [12]	Угроза пропуска проверки целостности программного обеспечения	Внешний нарушитель с низким потенциалом. Внутренний нарушитель с низким потенциалом.	Системное программное обеспечение. Прикладное программное обеспечение. Сетевое программное обеспечение.
УБИ.149 [13]	Угроза сбоя обработки специальным образом измененных файлов	Внешний нарушитель со средним потенциалом. Внутренний нарушитель со средним потенциалом.	Метаданные, объекты файловой системы. Системное программное обеспечение.

УБИ.162 [14]	Угроза эксплуатации цифровой подписи программного кода	Внешний нарушитель с низким потенциалом. Внутренний нарушитель с низким потенциалом.	Системное программное обеспечение. Прикладное программное обеспечение.
УБИ.170 [15]	Угроза неправомерного шифрования информации	Внешний нарушитель с низким потенциалом.	Объект файловой системы.
УБИ.177 [16]	Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	Внутренний нарушитель с низким потенциалом.	Системное программное обеспечение. Сетевое программное обеспечение. Прикладное программное обеспечение. Аппаратное обеспечение.
УБИ.179 [17]	Угроза несанкционированной модификации защищаемой информации	Внешний нарушитель с низким потенциалом. Внутренний нарушитель с низким потенциалом.	Объекты файловой системы.
УБИ.188 [18]	Угроза подмены программного обеспечения	Внутренний нарушитель со средним потенциалом.	Прикладное программное обеспечение. Сетевое программное обеспечение. Системное программное обеспечение.
УБИ.189 [19]	Угроза маскирования действий вредоносного кода	Внешний нарушитель со средним потенциалом.	Системное программное обеспечение. Сетевое программное обеспечение.
УБИ.191 [20]	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Внешний нарушитель с низким потенциалом. Внутренний нарушитель с низким потенциалом.	Прикладное программное обеспечение. Сетевое программное обеспечение. Системное программное обеспечение.

УБИ.193 [21]	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Внешний нарушитель со средним потенциалом.	Информационные ресурсы. Объекты файловой системы.

Реализация атак злоумышленников, происходящая вследствие успешной реализации угроз информационной безопасности, всегда направлена на нарушение одного или нескольких свойств информации: целостности, доступности, конфиденциальности. От результата нарушения данных принципов в случае успешной атаки зависят последствия действий злоумышленника на информацию и инфраструктуру предприятия.

- В результате нарушения целостности информация меняет свой вид, искажается или вовсе перестает существовать.
- В результате нарушения доступности использование информации затрудняется или становится невозможным.
- В результате нарушения конфиденциальности нарушается ее защита, что приводит к ее доступности нелегитимному кругу лиц.

Соотношение угроз в зависимости от влияния на конкретные свойства информации представлено на рис. 1.

Рисунок 1

Таким образом, каждая угроза или атака нарушает хотя бы один принцип информационной безопасности. Также имеются угрозы, затрагивающие все упомянутые принципы, что делает их наиболее опасными и сложными для предотвращения специалистами по информационной безопасности.

Заключение

Таким образом, для обеспечения необходимого и достаточного уровня защиты инфраструктуры от данного вида атак, стоит уделить особое внимание этапу управления рисками информационной безопасности, а именно их установлению, прогнозированию, расчету [22].

Что касается данной работы, то были выделены основные вектора атак злоумышленников, свойственные применению стеганографии:

1. Прямое применение стеганографии в корыстных целях.
2. Использование программных компонентов для сокрытия информации.
3. Использование сетевой стеганографии.
4. Утечки конфиденциальной/критической/корпоративной информацией по скрытым каналам связи.
5. Нарушение работы СЗИ за счет скрытого вложения.

Данные вектора атак были распределены в зависимости от воздействия на принципы информационной безопасности: нарушения целостности, доступности, конфиденциальности информации.

В данной работе были рассмотрены основные угрозы информационной безопасности, наличие которых прямо или косвенно возможно при использовании злоумышленником методов стеганографии при осуществлении атак на информационные инфраструктуры предприятий. Угрозы были выбраны согласно открытому банку данных ФСТЭК России. Для каждой из угроз представлена ее характеристика, выделен потенциальный злоумышленник и объект его воздействия, заключающийся в конкретном компоненте компьютерной инфраструктуры предприятия.

Таким образом, открытая база данных угроз информационной безопасности от ФСТЭК содержит достаточно информации для составления модели нарушителя. Однако этап установления злоумышленника требует более тщательного анализа, заключающегося в его целях, мотивах, инструментах. Данный анализ представлен в работах [3, 23, 24].

Литература

1. https://rt-solar.ru/products/solar_dozor/blog/3320/?ysclid=lm6parb5ug278920368 (дата обращения – июль 2024).
2. Коржик В.И., Яковлев В.А. Основы криптографии: учебное пособие – М.: Изд-во Интермедиа, 2017. – 312 с.
3. Федосенко М.Ю., Беззатеев С.В. Анализ проблематики применения методов стеганографии при осуществлении противоправных действий и её роли в цифровой криминалистике // Проблемы информационной безопасности. Компьютерные системы, 2023. – № 3. – С. 33-57.
4. Герлинг Е.Ю., Ахрамеева К.А. Обзор современного программного обеспечения, использующего методы стеганографии // Экономика и качество систем связи, 2019. – № 3. – С. 51-58.
5. URL https://rtmtech.ru/articles/fstek-threats-bank/?ysclid=lsepnzc8q4500547833#anchor2 (дата обращения – июль 2024).
6. URL https://bdu.fstec.ru/threat (дата обращения – июль 2024).
7. URL https://bdu.fstec.ru/threat/ubi.111 (дата обращения – июль 2024).
8. URL https://bdu.fstec.ru/threat/ubi.068 (дата обращения – июль 2024).
9. URL https://bdu.fstec.ru/threat/ubi.069 (дата обращения – июль 2024).
10. URL https://bdu.fstec.ru/threat/ubi.088 (дата обращения – июль 2024).
11. URL https://bdu.fstec.ru/threat/ubi.130 (дата обращения – июль 2024).
12. URL https://bdu.fstec.ru/threat/ubi.145 (дата обращения – июль 2024).

13. URL https://bdu.fstec.ru/threat/ubi.149 (дата обращения – июль 2024).
14. URL https://bdu.fstec.ru/threat/ubi.162 (дата обращения – июль 2024).
15. URL https://bdu.fstec.ru/threat/ubi.170 (дата обращения – июль 2024).
16. URL https://bdu.fstec.ru/threat/ubi.177 (дата обращения – июль 2024).
17. URL https://bdu.fstec.ru/threat/ubi.179 (дата обращения – июль 2024).
18. URL https://bdu.fstec.ru/threat/ubi.188 (дата обращения – июль 2024).
19. URL https://bdu.fstec.ru/threat/ubi.189 (дата обращения – июль 2024).
20. URL https://bdu.fstec.ru/threat/ubi.191 (дата обращения – июль 2024).
21. URL https://bdu.fstec.ru/threat/ubi.193 (Дата обращения – июль 2024).
22. URL https://www.intuit.ru/studies/courses/531/387/lecture/8996?page=1#sect (дата обращения – июль 2024).
23. Ахрамеева К.А., Федосенко М.Ю. Сравнительный анализ возможностей использования стеганографического программного обеспечения для скрытого обмена данными в сети интернет // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2022. – № 1. – С. 37-43.
24. Федосенко М.Ю. Особенности решения задачи управления рисками информационной безопасности при разработке методов защиты от скрытого (стеганографического) обмена информацией на публичных интернет-ресурсах // Проблемы информационной безопасности. Компьютерные системы, 2024. – № 1. – С. 80-95.