ЭКОНОМИКА И КАЧЕСТВО СИСТЕМ СВЯЗИ ***№ 2(28) / 2023***

ISSN 2500-1833

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

Учредители:
Региональное отделение Российской академии естественных наук,
АО «Национальный институт радио и инфокоммуникационных технологий»

Издатель:
АО «Национальный институт радио и инфокоммуникационных технологий»

Журнал публикует статьи, отражающие результаты исследований в соответствии со следующими разделами ГРНТИ:
06.00.00 – Экономика и экономические науки
10.00.00 – Государство и право. Юридические науки
14.00.00 – Народное образование. Педагогика
19.00.00 – Массовая коммуникация. Журналистика. СМИ
20.00.00 – Информатика
47.00.00 – Электроника. Радиотехника
49.00.00 – Связь
73.00.00 – Транспорт
82.00.00 – Организация и управление
84.00.00 – Стандартизация
90.00.00 – Метрология

Адрес редакции: *111024, Москва, ул. Авиамоторная, дом 8А, стр. 5.*
АО «НИРИТ»

Тел.: *8 (495) 643-11-86 (282)* ***сайт:*** *http://journal-ekss.ru/* ***e-mail:*** *ekss@nirit.org*

СОДЕРЖАНИЕ

ЭКОНОМИКА И УПРАВЛЕНИЕ

СЕТИ СВЯЗИ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СЕТИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЭКОНОМИКА И УПРАВЛЕНИЕ

ЭКОНОМИКА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЦИФРОВИЗАЦИИ: ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ ВОПРОСЫ ДЛЯ ИССЛЕДОВАНИЯ

М.А. Дмитриева, *Нижегородский государственный университет им. Н.И. Лобачевского, 050801mad@mail.ru.*

УДК 338:004.04:004.05

Аннотация. За последние 30 лет ИТ-технологии и цифровизация коренным образом изменили экономику. Развитие этих технологий не только выявило сложные исследовательские вопросы, но и предоставило новые инструменты для ответа на них. Исследователи теперь используют ИТ-технологии и повсеместную цифровизацию, чтобы активно вносить свой вклад в другие области. В данной статье проведен анализ основных перспективных направлений исследований в области цифровой экономики, а также собраны основные вопросы, на которые необходимо дать ответ.

Ключевые слова: экономика; исследование; вопрос; метод; область; рынок; ИТ-технологии; ИИ.

ECONOMICS OF INFORMATION TECHNOLOGY AND DIGITALIZATION: THE MAIN THEORETICAL AND PRACTICAL ISSUES FOR RESEARCH

Maria Dmitryeva, *Nizhny Novgorod State University N.I. Lobachevsky.*

Annotation. Over the past 30 years, *IT*-technology and digitalization have fundamentally changed the economy. The development of these technologies has not only generated complex research questions, but also provided new tools to answer them. Researchers are now using information technology and ubiquitous digitalization to actively contribute to other fields. This article analyzes the main promising areas of research in the field of digital economy, as well as collects the main questions that need to be answered.

Keywords: economics; research; question; method; area; market; *IT*-technologies; *AI*.

Введение

Теоретики, изучающие экономику информационных технологий (ИТ) и цифровизации, воспользовались возможностями для инновационных исследований экономики. Исследования в области ИТ-технологий теперь стимулируют передовые разработки в области финансов, маркетинга, управления операциями и даже управления человеческими ресурсами [1-4].

Новые и новаторские исследовательские проекты должны выходить за рамки, ограничивающие вопросы и методы. Следует сосредоточиться на новых и актуальных исследовательских вопросах, применять правильные и полезные методы и добиваться важных и репрезентативных результатов исследований [5-7].

В табл. 1 представлены шесть критериев для оценки и продвижения новой экономики исследований в области ИТ-технологий и оцифровки. Они помогают расширить исследовательские вопросы, методы и результаты [8].

Возможности для ведущих экономических исследований в области ИТ-технологий

ИТ-технологии имеют глубокие и многогранные последствия для экономического развития. Наноданные, полученные в результате оцифровки производства, рыночных транзакций и человеческого поведения, позволяют быстро принимать решения. Технологии искусственного интеллекта (ИИ) и автоматизации повышают производительность во всех видах бизнеса, но в то же время коренным образом изменяют экономику труда. Продукты и услуги объединяют онлайн и оффлайн опыт, а потребление становится все более социальным. Потребители делают лучший выбор, используя поисковые системы и инструменты поддержки принятия решений на базе ИИ для извлечения и обработки информации [9].

Таблица 1.

Вопросы: релевантные и актуальные	Имеет ли исследовательский вопрос отношение к сбоям и непредвиденным ситуациям, вызванным новыми ИТ-технологиями? Затрагивает ли исследовательский вопрос общие, новые проблемы на практике? Предложит ли исследовательский вопрос экономистам и менеджерам новое понимание таких тем, как выбор, координация, дефицит (избыток), рациональность человека и машины?
Методы: правильные и полезные	Подтверждены ли выводы строго? Являются ли методы полезными для практики? Можно ли обобщить полученные результаты?
Результаты: важные и существенные	Важны ли полученные результаты для ключевых заинтересованных сторон экономики? Предлагает ли исследование четкие рекомендации для разработки стратегии и политики? Оспаривает ли исследование статус-кво в отношении существующих убеждений?

Рынки также меняются. Цифровые рынки снижают цены, повышают разнообразие и прозрачность, а также позволяют потребителям и предприятиям осуществлять более эффективный поиск товаров и услуг [10]. Новые ИТ-технологии, такие как чат-боты, блокчейн, виртуальная реальность и прямая трансляция, в дальнейшем приведут к более открытой, эффективной цифровой экономике [11].

Исследователи, изучающие экономику ИТ-технологий и цифровизации, должны выйти за рамки узких исследовательских блоков и изучать сложные теории принятия решений, организации производства, экономики труда, социального обеспечения и равенства, а также других подразделов экономики. В конечном итоге, экономика должна стать эталонной дисциплиной для исследований в таких областях, как маркетинг, финансы и операционный менеджмент, в частности, отвечая на перспективные вопросы и переключая внимание на широко определенные темы [12].

На рис. 1 показан эффект цифровизации экономики Российской Федерации.

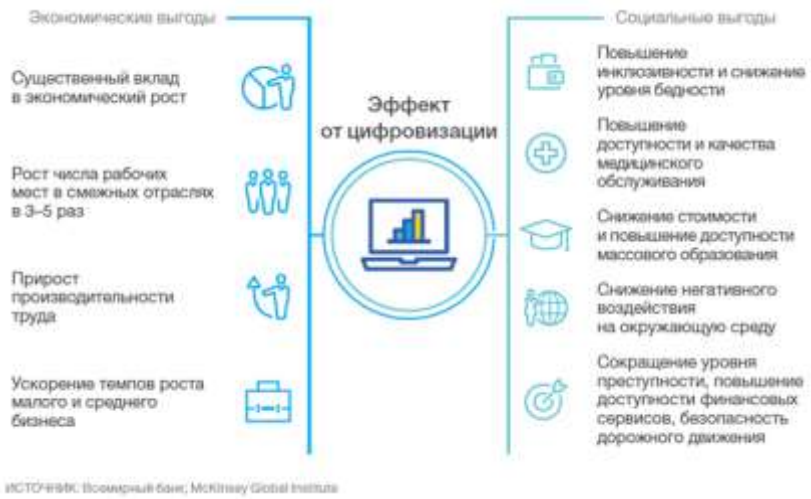

Рисунок 1

Смена исследовательской парадигмы вместе с ИТ-технологиями

Исследования в области экономики ИТ-технологий и цифровизации должны полностью охватывать новые методологии исследований, основанные на ИТ-технологиях. Цифровые и вычислительные технологии глубоко изменили исследования в области социальных и гуманитарных наук, особенно экономики, и предоставили новые инструменты для качественного и количественного понимания экономических процессов. Машинное обучение и цифровая инфраструктура способствуют смене парадигмы, которая включает открытие новых теорий, а также исследования, ориентированные на прогнозирование, и массовые полевые эксперименты [13].

Наноданные из поисковых систем, потоков кликов, сообщений в социальных сетях и интернета вещей открывают новые возможности для точных прогнозов. Данные дистанционного зондирования и мобильных устройств предоставляют всеобъемлющую пространственную информацию, получение которой ранее было невозможным. Более быстрые мобильные широкополосные соединения, камеры с более высоким разрешением и более интеллектуальное цифровое оборудование продолжают расширять полный спектр наблюдений за социально-экономической деятельностью в режиме реального времени. Цифровые платформы предоставляют количественные данные в режиме реального времени. Массовые онлайн-полевые эксперименты, проводимые на интернет-платформах, открывают неоценимые возможности для развития теории экономических наук [14].

Продвинутые алгоритмы машинного обучения могут улучшить методы проверки теорий, предоставляя множество удивительно эффективных инструментов для анализа разных данных. Исследования в области экономики ИТ-технологий только начали охватывать применение алгоритмов машинного обучения для генерации новых задач, постановки инновационных вопросов, предложения новых теорий, эмпирического определения причинно-следственных связей, прогнозирования противоречащих фактов и моделирования результатов политики компаний и организаций [15].

Исследователи теперь могут проводить обширные полевые эксперименты, выходящие за рамки прежних возможностей. Они могут анализировать неструктурированные данные в режиме реального времени для получения новых идей, инновационных моделей и точных прогнозов, основанных на теории и

данных. Такие изменения продолжат бросать вызов нынешней парадигме экономики ИТ-технологий и исследований в области цифровизации.

В табл. 2 выделяются восемь важных, но недостаточно изученных вопросов для следующего поколения теорий экономики ИТ-технологий. Эти сложные вопросы предполагают многообещающие исследовательские возможности. Для каждого вопроса предлагаются несколько примеров тем исследования в соответствии с критериями оценки. В табл. 2 представлены релевантные вопросы для исследования экономики цифровизации и ИТ-технологий.

Таблица 2.

Вопросы	Критерии и примеры	
Как ИТ-технологии меняют организации?	Новизна	Как децентрализованное принятие решений с поддержкой ИТ-технологий изменит работу организаций и методы управления?
	Корректность	Каким образом собирать данные и проводить эксперименты в новых организациях?
	Важность	Как новые формы организаций и бизнес-модели меняют общество? Как удаленная работа влияет на вовлеченность рабочей силы и гендерные различия в заработной плате?
Как ИТ-технологии создает новые рынки?	Новизна	Как следует проектировать рынки для размещения прорывных технологий? Как должны быть организованы транзакции с данными?
	Корректность	Следует ли пересмотреть экономическую теорию, чтобы охватить экономику совместного использования и рынки, основанные на технологии блокчейн? Если да, то как?
	Важность	Какие новые меры политики необходимы для регулирования участников рынка?
Как ИИ и большие данные преобразуют процесс принятия решений?	Новизна	ИИ и принятие решений на основе данных (*Data-driven decision, DDD*) усиливают всестороннюю обработку информации. Как эти изменения соотносятся со сбоями, произошедшими во время последней промышленной революции? Как ИИ и *DDD* изменят мышление и действия менеджеров? Как ИИ и *DDD* изменяют уровни рациональности среди экономических агентов?
	Корректность	Как ИИ и *DDD* изменяют предыдущие рациональные модели и модели поведения?
	Важность	Повысят ли ИИ и *DDD* эффективность рынка? Какие этические и юридические проблемы связаны с использованием ИИ и *DDD* на рынках и в организациях?

Вопросы	Критерии и примеры	
Как ИТ-технологии влияют на неравенство социальное?	Новизна	Какую роль играет *ESG*-управление (*Environmental, social, and corporate governance*) в новой экономике? Компьютеры какой вычислительной мощности порождают решения, превосходящие по эффективности решения, принятых людьми?
	Корректность	Какие методы наилучшим образом позволят ИТ-технологиям сократить социальное, экономическое и информационное неравенство? Следует ли директивным органам устранять неравенство, созданное преимуществами первопроходцев в инвестициях в ИИ?
	Важность	Как можно ограничить рыночную власть, но при этом продвигать инновации в крупных ИТ-компаниях? Как можно обеспечить равный доступ к информации и социальным ресурсам?
Какие принципы должны быть установлены в отношении владения данными и конфиденциальности?	Новизна	Кому принадлежат права на личные данные? Аналогичны ли операции с данными экономики товаров и ресурсов?
	Корректность	Как экономические исследования должны эмпирически учитывать конфиденциальность данных? Может ли быть достигнута ценовая дискриминация первой степени? Каковы экономические последствия? Когда и как люди выбирают между конфиденциальностью и удобством?
	Важность	Следует ли поощрять цифровые платформы за обеспечение конфиденциальности? Поскольку с помощью различных устройств, собирается все больше данных, следует ли регулировать владение данными? Если да, то как?
Какие глобальные проблемы могут быть вызваны передовыми технологиями?	Новизна	Должны ли разработчики ИТ-систем внедрять ограниченные рациональные ИТ-технологии, чтобы предотвратить чрезвычайные ситуации? Как алгоритмы совместной фильтрации создают социальную пропасть?
	Корректность	Является ли оптимальный выбор иллюзией, несмотря на точные прогнозы рекомендательных систем и алгоритмов выявления предпочтений?
	Важность	Кто должен определять оптимальные уровни социальных взаимодействий?

Вопросы	Критерии и примеры	
Как следует верно оценивать возможности цифровой экономики?	Новизна	Как цифровые бизнес-модели генерируют ранее не учитываемые параметры в уже существующих моделях?
	Корректность	Как правильно измерить нематериальную социальную ценность чего-либо? Как учет национального дохода должен измерять неденежные операции с цифровыми товарами и услугами?
	Важность	Как государственные нормативные акты могут способствовать или препятствовать цифровизации экономики?
Как можно переосмыслить экономику области исследований ИТ-технологий?	Новизна	Какие альтернативные методы исследования можно было бы использовать помимо аналитического моделирования и эмпирических исследований данных наблюдений и экспериментов? Возможно ли генерировать теории, основанные на доступе к экономическим данным на наноуровне?
	Корректность	Следует ли расширить область анализа за пределы отдельных лиц, групп и организаций, включив в нее идеи, задачи и алгоритмы?
	Важность	Следует ли обобщить экономику ИТ-исследований?

Заключение

Инновации следующего поколения требуют, чтобы все члены научного сообщества признавали ценность междисциплинарных исследований, задавали правильные вопросы, принимали новые методологии и вносили свой вклад в другие дисциплины.

Исследования могут и должны привнести новые знания или методы в управленческие дисциплины за пределами экономической области. Должны быть рассмотрены вопросы, которые являются более актуальными для маркетинга или финансов, если эти вопросы касаются новых и важных проблем в цифровой экономике. Помимо владения теорией и эконометрикой, специалисты должны уметь работать с большими данными, передовыми методами интеллектуального анализа данных и методами глубокого обучения, придерживаясь бизнес-операций, работая на месте и сотрудничая с практиками в создании ИТ-систем с разумным экономическим обоснованием.

Литература

1. Brynjolfsson E. and Smith M.D. Frictionless commerce? A comparison of internet and conventional retailers // Management science (46:4), 2000. – pp. 563-585.
2. Brynjolfsson E. and Mc Elheran K. The rapid aAdoption of data-driven decision-making // American economic review (106:5), 2016. – pp. 133-139.

3. Gupta A., Kannan K. and Sanyal P. Economic experiments in information systems // MIS Quarterly (42:2), 2018. – pp. 595-606.
4. Анискин С.С. Кибербезопасность как один из трендов цифровой экономики России // Образование и наука без границ: социально-гуманитарные науки, 2019. – № 12. – С. 28-31.
5. Белокрылова О.С. Блокчейн как эффективный инструмент согласования экономических интересов авторов цифровой экономики России // Journal of Economic Regulation, 2019. – Т. 10. – № 1. – С. 50-63.
6. Гэд Т. 4D брэндинг: Взламывая корпоративный код экономики. – М.: СПб: Стокгольмская школа экономики в Санкт-Петербурге; Издание 3-е, 2013. – 230 с.
7. Духовных Д.А. Проблемы и риски формирования и развития цифровой экономики в России // European journal of natural history, 2020. – № 1. – С. 110-114.
8. Еремейчук К.Ю. Цифровая экономика – будущее России // Аллея науки, 2017. – Т. 2. – № 14. – С. 419-422.
9. Львов Д.С. Институциональная экономика. Под ред. Д.С. Львов. – М.: ИНФРА-М, 2016. – 318 с.
10. Климова Ю.О. Теоретические аспекты и институциональная среда развития цифровой экономики России // Вестник Челябинского государственного университета, 2020. – № 2 (436). – С. 43-51.
11. Ковальчук Ю.А. Высокотехнологичное производство как «новое окно возможностей» в посткризисной экономике // Корпоративное управление и инновационное развитие экономики Севера: Вестник Научно-исследовательского центра корпоративного права, управления и венчурного инвестирования Сыктывкарского государственного университета, 2016. – № 3. – С. 25-33.
12. Конюховский П. Математические методы исследования операций в экономике. – М.: [не указано], 2016. – 439 с.
13. Крохичева Г.Е. Электронная коммерция, как структурный элемент цифровой экономики // Матрица науч. познания, 2017. – № 12. – С. 51-55.
14. Маймина Э.В. Особенности и тенденции развития цифровой экономики // Вестн. Белгородского ун-та кооперации, экономики и права, 2017. – № 6. – С. 37-45.
15. Морозов М.А., Морозова Н.С. Новая парадигма развития туризма и индустрии гостеприимства в условиях цифровой экономики // Вестник Российского нового университета. Серия: «Человек и общество», 2018. – № 1. – С. 135-141.

ИННОВАЦИОННАЯ ИНФРАСТРУКТУРА КАК ИНСТРУМЕНТ ГОСУДАРСТВЕННОЙ ПОДДЕРЖКИ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

С.А. Сидоров, *Оренбургский государственный университет, sidorov.s13@mail.ru.*

УДК 336.027

Аннотация. Без создания и развития основных составляющих элементов невозможно эффективно развивать функционирующую и результативную инновационную деятельность. При решении задачи дальнейшего развития инновационной деятельности с позиции администрирования существует объективная необходимость реализации обоснованной и долгосрочной инновационной политики, базой которой является создание системы

регулирования инновационной деятельности в экономическом и правовом аспектах. При этом основными целями и задачами государства в отношении инновационной деятельности является соблюдение приоритета интересов государства и общества при использовании инноваций и частных интересов бизнеса. В статье проведен обзор основных методов государственной поддержки инновационной деятельности как на региональном, так и на федеральном уровнях.

Ключевые слова: инновационное развитие; государственная поддержка; инновация; технологии; регулирование; государственные программы.

STATE PROGRAMS AS A TOOL OF STATE SUPPORT OF INNOVATION ACTIVITIES

S.A. Sidorov, *Orenburg State University.*

Annotation. Without the creation and development of the main constituent elements, it is impossible to develop an effectively functioning and productive innovation activity. Solving the problem of further development of innovation activity, there is an objective need from the standpoint of administration to implement a sound and long-term innovation policy, the basis of which is the creation of a system for regulating innovation activity in economic and legal aspects with the goals and objectives of the state in relation to innovation activity in order to comply with the priority of the interests of the state and society when using innovations and private business interests. The article provides an overview of the main methods of state support for innovation activities both at the regional and federal levels.

Keywords: innovative development; government support; innovation; technology; regulation; government programs.

Введение

В настоящее время инновации и результаты НИОКР являются фундаментом для диверсификации национальной экономики Российской Федерации, основанной на экономике знаний. Инновационный и научно-технический потенциал страны зачастую определяет уровень ее конкурентоспособности и инвестиционной привлекательности для внешних инвесторов на глобальном рынке. Необходимость государственной поддержки инновационной деятельности объясняется как общенациональным значением, так и экономическим содержанием инноваций. В настоящее время инновации становятся основным средством хозяйствующих субъектов по увеличению прибыли. Однако при отсутствии государственного регулирования многие нововведения не могли бы быстро внедряться в практику.

В связи с этим, актуальной задачей является постоянная оценка проводимой государственной политики в сферах инновационного и научно-технического развития, основанной на анализе показателей статистики науки и инноваций, а также выявление положительных и отрицательных факторов, оказывающих влияние на формирование экономики знаний.

Несмотря на все трудности (пандемия, санкции), в прошлом 2022 г. в России создали и внедрили десятки технологических решений. Всего в 2021 г. премией отметили несколько десятков проектов и разработок. Список победителей позволяет оценить основные тренды в разных технологических направлениях.

Динамика объема инновационных товаров характеризуется его стабильным ростом на протяжении 2000-2021 гг., что обусловлено расширением потребительской активности населения и спроса на продукцию производственного

назначения. В целом фиксировался устойчивый рост объема инновационных товаров, работ, услуг несмотря на то, что в 2021 г. по сравнению с 2020 г. объем инновационной продукции снизился относительно общего объема отгруженных товаров в процентном соотношении, что отчасти объясняется снижением инновационной активности товаров в России [1]. Динамика объема инновационных товаров за период 2000-2021 гг. представлена в табл. 1.

Таблица 1.

Годы	В абсолютном выражении, млрд руб.	В процентах от общего объема отгруженных товаров, выполненных работ, услуг
2000	154,7	4,4
2010	1243,7	4,8
2018	4516,2	5,7
2019	4863,3	5,3
2020	5189,0	5,7
2021	6003,3	5,0

Исходя из статистической информации, разрабатываемой Росстатом, следует отметить, что с 2000 г. количество научно-исследовательских, проектных и экспериментальных организаций в России увеличилось почти вдвое. В табл. 2 представлена динамика количества организаций, выполнявших исследования и разработки за 2000-2021 гг. [2].

Таблица 2.

Показатели	Годы						Темп роста/спада 2021 г. к 2000 г., %
	2000	2010	2018	2019	2020	2021	
Всего, в том числе:	4 099	3 492	3 950	4 051	4 175	4 175	101,8
- научно-исследовательские организации	2 686	1 840	1 574	1 618	1 633	1 627	60,6
- конструкторские организации	318	362	254	255	239	233	73,3
- проектные и проектно-изыскательские организации	85	36	20	11	12	13	15,3
- опытные заводы	33	47	49	44	35	33	100,00
- образовательные организации высшего образования	390	517	917	951	969	990	253,8
- организации промышленности, имевшие научно-исследовательские, проектно-конструкторские подразделения	284	238	419	450	441	446	157,0
- прочие	303	452	717	722	846	833	274,9

Количество научно-исследовательских организаций за 2000-2021 гг. снизилось на 39,4 %. За последние 10-15 лет развалились почти все крупные проектно-изыскательские институты России времен СССР, и произошло это в основном не в самые трудные 90-е, но и уже в новом столетии. В 2021 г. численность всего персонала с учетом техников, вспомогательного персонала и прочих лиц в отечественной сфере исследований и разработок трудится 662,7 тыс. человек – в 0,7 раза меньше, чем в 2000 г. (887,7 тыс.). При этом сохраняется тенденция снижения численности исследователей на 20,1 % по сравнению с 2000 г. [1].

Важную роль в анализе показателей инновационного развития и функционировании инновационных организаций в России занимают затраты на инновационную деятельность в РФ за 2019-2021 гг. (рис. 1).

Как видно из данных рис. 1, тенденция повышения затрат на инновационную деятельность в Российской Федерации является достаточно положительным фактом, поскольку инновации являются двигателем прогресса и экономики. Снижение доли инновационных товаров, работ и услуг в общем объеме отгруженных товаров, выполненных работ и услуг свидетельствует о неэффективности направленных средств в инновационную сферу в Российской Федерации.

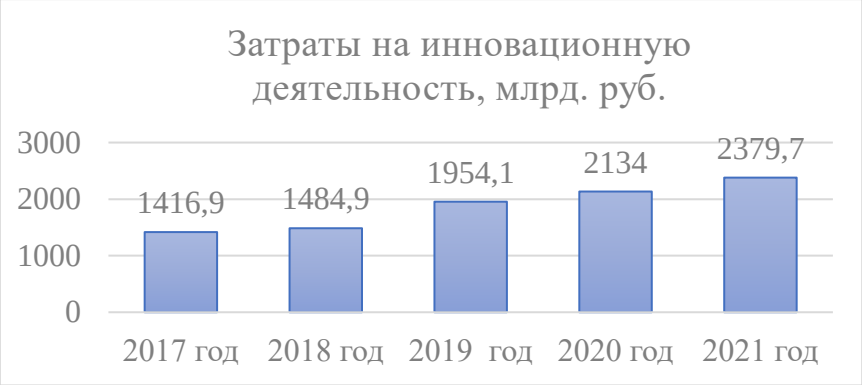

Рисунок 1

Как видим, доля высокотехнологичных товаров в объеме импорта на протяжении всего анализируемого периода в России превышает долю экспорта. Доля высокотехнологичных товаров в объеме импорта составляет около 60-70 %. Это означает, что Российская Федерация в основном закупает высокотехнологичные товары за рубежом. Доля высокотехнологичных товаров в объеме экспорта составляет около 11-14 %, что достаточно мало [3].

Таким образом, затраты компаний на развитие инноваций составили 2,4 трлн руб., что на 11,5 % (в действующих ценах) выше значения 2020 г. и на 21,7 % выше по сравнению с доковидным (предкризисным) 2019 г. Результативность инновационной деятельности практически не изменилась: объем произведенных инновационных товаров, работ, услуг в 2021 г. превысил 6 трлн руб. (-0,7 % в постоянных ценах относительно 2020 г., но +5,2 % к 2019 г.). В общем объеме продаж их доля по-прежнему остается невысокой (в 2021 г. – 5 %; в 2020 г. – 5,7 %).

Исходя из источника финансирования инструменты государственного стимулирования инновационной деятельности можно разделить на следующие:

- бюджетные, финансируемые непосредственно из бюджетов различных уровней (субсидии на поддержку научных мероприятий, гранты, федеральные целевые программы в области инноваций и т.д.);
- внебюджетные, финансируемые из внебюджетных страховых фондов (страховые взносы);
- финансируемые из средств предприятий и организаций (коэффициенты амортизации, налоговые льготы и пр.), но, по существу, оплачиваемые государством и выступающие следствием установления государством норм, означающих сознательное недополучение им финансовых ресурсов, расходуемых предприятиями на осуществление затрат инновационного характера [4].

Для рассмотрения регионального аспекта государственной поддержки инновационной деятельности выбрана практика создания и развития инновационной инфраструктуры в Оренбургской области.

В Оренбургской области действует Закон Оренбургской области от 16.11.2009 № 3222/739-IV-ОЗ «О государственной поддержке инновационной деятельности в Оренбургской области»[1]. Также согласно Информации о ходе реализации этого закона [5] на построение инновационной региональной экономики ориентирована «Стратегия развития Оренбургской области до 2020 г. и на период до 2030 г.»[2], Государственная программа «Экономическое развитие Оренбургской области»[3].

В рамках реализации Закона в Оренбуржье создана и продуктивно работает расширенная система поддержки научной и научно-технической деятельности, а также основные механизмы отраслевой поддержки инновационной деятельности предприятий и организаций (в малом и среднем бизнесе; машиностроении и легкой промышленности; строительном и агропромышленном секторе). Ежегодная поддержка научно-технической и инновационной деятельности производится на территории области в рамках исполнения бюджетных обязательств Министерства образования и Министерства экономического развития, промышленной политики и торговли Оренбургской области.

Так, например, в городе Оренбурге с 2013 г. осуществляет свою деятельность региональное представительство Фонда содействия развитию малых форм предприятий в научно-технической сфере (далее – представительство Фонда).

Целью открытия представительства Фонда является организация совместной работы по ускорению темпов развития малого инновационного предпринимательства в области реализации научно-технических проектов молодых ученых вузов, НИИ, промышленных предприятий, а также ежегодное проведение конкурсного отбора проектов для их финансирования Фондом [5].

Фонд реализует программы инновационного развития, направленные на создание новых и развитие действующих высокотехнологичных компаний, коммерциализацию результатов научно-технической деятельности, привлечение инвестиций в сферу малого инновационного предпринимательства, создание новых рабочих мест. Объем привлеченного финансирования на инновационные

[1] Закон Оренбургской области от 16.11.2009 № 3222/739-IV-ОЗ «О государственной поддержке инновационной деятельности в Оренбургской области» // КонсультантПлюс.
[2] Стратегия развития Оренбургской области до 2020 года и на период до 2030 г. // КонсультантПлюс.
[3] Постановление от 25 декабря 2018 г. № 888-пп «Об утверждении государственной программы «Экономическое развитие Оренбургской области» // КонсультантПлюс.

проекты физических и юридических лиц Оренбургской области по конкурсным программам Фонда с 2014 г. составляет более 70 млн руб.

Целью функционирования платформы «АгроБиоТех» является создание в Оренбургской области центра коммерциализации инновационных агро- и биотехнологических бизнес-проектов, развитие научно-технологического потенциала производства отечественной агро- и биотехнологической продукции. Платформа объединяет на одной площадке предпринимателей, бизнес-экспертов, ученых и общественных деятелей из Оренбургской области, регионов РФ, Москвы и стран ЕАЭС.

Кроме того, при поддержке Министерства экономического развития, промышленной политики и торговли Оренбургской области на территории региона были открыты два центра молодежного инновационного творчества (далее – ЦМИТ). Целью создания ЦМИТ явилась необходимость обеспечения доступа детей и молодежи к современному оборудованию прямого цифрового производства для реализации, проверки и коммерциализации их инновационных идей, поддержки инновационного творчества детей и молодежи, в том числе в целях профессиональной реализации и обеспечения вовлечения молодежи в предпринимательскую деятельность.

Первый опыт успешного создания ЦМИТ состоялся в 2016 г. на базе ООО «Пластик» в Оренбурге, где ребята проходят практику, занимаются научными разработками, осваивают новые профессии. За время существования центра прошли обучение более 700 молодых людей. В 2018 г. состоялось открытие ЦМИТ в Ясненском городском округе Оренбургской области. Всего в прошедшем 2022 г. было вовлечено в реализацию мероприятий ЦМИТа более 680 человек, а также завершили обучение 76 человек. В процессе деятельности центра создано три новых рабочих места.

Успешно осуществляет свою деятельность АО «Корпорация развития Оренбургской области». Основным направлением деятельности Корпорации является создание благоприятных условий для развития инфраструктуры области с использованием механизмов государственно-частного партнерства. Выступает в качестве оператора системы «одного окна» для инвесторов [5].

Таким образом, имеющиеся социально-экономические и социально-демографические ресурсы, усиление значимости развития регионов являются базой прогресса инновационного потенциала РФ, причем качество инновационной среды в итоге может ускорять либо затормаживать возникновение и распространение инноваций на территории России.

Для развития инновационной деятельности в РФ и повышения уровня инновационной активности организаций необходимо разработать мобильную и соответствующую мировым стандартам инфраструктуру, которая будет оказывать всестороннюю поддержку бизнесу; создавать благоприятные условия для развития и возможности выхода на мировой рынок российских производителей; упростит и сделает более доступной систему патентования интеллектуальной собственности; позволит разработать мотивационные рычаги, стимулирующие руководителей предприятий финансировать собственную деятельность по разработке и внедрению инноваций, а также обеспечит достойные рабочие места молодым специалистам в перспективные для страны отрасли.

Так, например, с учетом разработанной Правительством РФ стратегии по развитию инновационных предприятий, повышению инновационной активности, поддержки науки и изменению ситуации по развитию инновационной

деятельности в регионах страны планируется реализация следующих мероприятий в соответствии с государственными программами России (рис. 2).

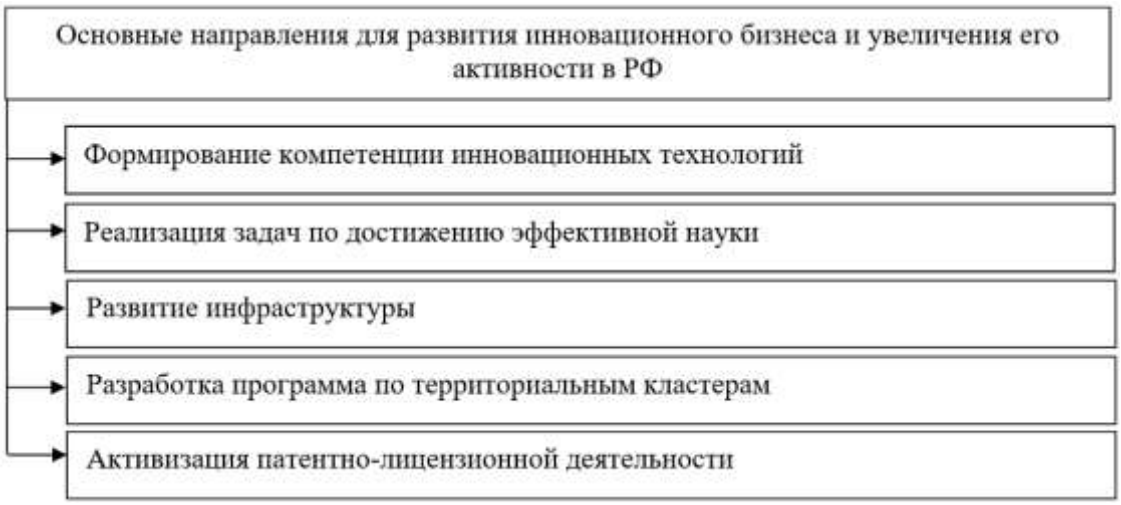

Рисунок 2

Представленные направления повлияют на совершенствование экономического положения страны и повысят ее конкурентоспособность по сравнению с другими странами. Несмотря на значительные государственные инвестиции в российскую науку, эта сфера остается недостаточно развитой, не формирует собственной научно-технической базы для постановки и реализации приоритетов, реагирования на «большие вызовы», стоящие перед обществом и государством, не служит двигателем социально-экономического развития. В России до сих пор существует неэффективная модель финансирования науки: 60-70 % всех расходов на НИОКР обеспечивается за счет бюджетных средств. Это противоречит не только мировым тенденциям, но и стратегии инновационного развития Российской Федерации на период до 2020 г.

В качестве направления инновационного развития России необходимо установить такие государственные программы, как «Развитие науки и технологий» на 2023-2030 гг. и «Научно-техническое развитие Российской Федерации». Также можно сделать вывод, что повышение инновационной эффективности высокотехнологичной промышленности России должно быть в тесной связи между правительством, промышленностью, университетом и исследованиями, подчеркивая развитие финансирования науки и технологий, достаточный поток факторов между регионами и выделение средств на инновации и технологии.

Заключение

В заключении проведенного исследования необходимо сделать соответствующие выводы. Так, с учетом стратегии, выработанной Российским правительством, для развития инновационного бизнеса и увеличения его активности, поддержания науки и изменения ситуации в регионах, планируется реализовать следующие шаги в соответствии с государственными программами РФ:

- сформировать компетенции инновационных технологий;
- внедрить новые шаги и реализовать задачи по достижению эффективной науки;
- развивать инфраструктуру;

- разработать программу по территориальным кластерам;
- активизировать патентно-лицензионную деятельность;
- создать институты развития.

Все эти мероприятия направлены на улучшение экономической ситуации в стране и повышение ее конкурентоспособности по сравнению с другими странами. Несмотря на существенные вложения в российскую науку со стороны государства, данная сфера остается недостаточно продуктивной, не формирует собственную научно-технологическую основу для создания и реализации приоритетов, реагирования на «большие вызовы», стоящие перед обществом и государством, не выступает драйвером для социально-экономического развития. Именно поэтому на первый план выходят стимулирование положительного отношения населения РФ к инновациям в технологической сфере, повышение конкуренции внутри инновационного рынка и эффективная защищенность собственников бизнеса и инвесторов, а также четкое определение ключевых стратегий государственного участия в развитии инновационной среды и реализации стратегии Национальной технологической инициативы.

Литература

1. Федеральная служба государственной статистики. – Режим доступа: https://rosstat.gov.ru/
2. Гохберг Л.М., Дитковский К.А., Евневич Е.И. Индикаторы науки: 2021: Статистический сборник. Нац. исслед. ун-т «Высшая школа экономики». – Москва: НИУ ВШЭ, 2021. – 352 с. – Режим доступа: https://issek.hse.ru/news/454933528.html
3. Состояние показателей экономической безопасности России. – Режим доступа: https://schetuchet.ru/sostoyanie-pokazatelej-ekonomicheskoj-bezopasnosti-rossii/
4. Муталиева Ф. М-Б. Необходимость государственной поддержки инновационной деятельности // Потенциал современной науки: материалы Международной (заочной) научно-практической конференции, Прага, 30 ноября 2022 г. – Нефтекамск: Научно-издательский центр «Мир науки» (ИП Вострецов Александр Ильич), 2022. – С. 34-37.
5. Информация о ходе реализации Закона Оренбургской области «О государственной поддержке инновационной деятельности в Оренбургской области» // Развитие инноваций [Электронный ресурс]. – Режим доступа: https://orenburg-gov.ru/activity/1711/

СЕТИ СВЯЗИ

НАСТРОЙКА ДИАГРАММ НАПРАВЛЕННОСТИ АНТЕНН ДЛЯ ШИРОКОВЕЩАТЕЛЬНЫХ КАНАЛОВ УПРАВЛЕНИЯ СЕТИ МАКВИЛ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ

О.А. Шорин, *д.т.н., профессор, Московский технический университет связи и информатики, oshorin@nxtt.org;*
И. Агран, *Московский технический университет связи и информатики.*

УДК 621.391

Аннотация. Разработана методика и программа настройки диаграмм направленности многоэлементных антенных систем базовых станций сети связи МАКВИЛ для организации широковещательных каналов управления. Применена техника машинного обучения, учитывающая технологическую особенность системы, связанную с необходимостью управления диаграммами путем настройки только фаз сигналов, транслируемых в антенных каналах. Установлено, что предложенная методика и получаемые на ее основе диаграммы направленности позволяют в несколько раз сократить количество базовых станций, обслуживающих выделенную территорию. Особенно значимые результаты наблюдаются для территорий со сложным рельефом местности и зонами высокой локальной контрастности плотности размещения абонентов. На примере г. Новороссийска показано, как с помощью двух БС можно обеспечить покрытие 85% городской территории.

Ключевые слова: базовая станция; многоэлементная антенная решетка; диаграмма направленности; весовые коэффициенты; машинное обучение; градиентный адаптивный алгоритм; широковещательный канал управления.

CONFIGURING ANTENNA PATTERNS FOR BROADCAST CONTROL CHANNELS OF THE MCWILL NETWORK BASED ON MACHINE LEARNING

Oleg Shorin, *Doctor of Technical Sciences, Professor, Moscow technical university of communications and informatics;*
Ishrak Agran, *Moscow technical university of communications and informatics.*

Annotation. A methodology and a program for setting up directional patterns of multi-element antenna systems of the base stations of the *McWiLL* communication network for the organization of broadcast control channels has been developed. The machine learning technique is applied, taking into account the technological feature of the system associated with the need to control diagrams by adjusting only the phases of signals transmitted in antenna channels. It has been established that the proposed methodology and the directional patterns obtained on its basis make it possible to reduce the number of base stations serving the allocated territory several times. Particularly significant results are observed for territories with complex terrain and areas of high local contrast density of subscribers. The example of Novorossiysk shows how with the help of two BS it is possible to provide coverage of 85% of the urban area.

Keywords: base station, multi-element antenna array, directional pattern, weight coefficients, machine learning, gradient adaptive algorithm, broadcast control channel.

Введение

Основным требованием, предъявляемым к сетям и системам радиосвязи на современном этапе, является высокая экономическая эффективность. Достигнуть ее возможно только при существенном сокращении затрат, связанных с капитальным строительством (*CAPEX*) и с оплатой арендуемых ресурсов радиоканала (*OPEX*). Поэтому при развертывании и эксплуатации указанных сетей и систем возникает задача максимального сокращения числа базовых станций (БС) при условии сохранения показателей качества связи на обслуживаемой территории. Для систем профессиональной радиосвязи, как правило, не требуется высокая производительность, но сохраняются высокие требования к организации сплошного покрытия.

Система профессиональной связи подвижных абонентов МАКВИЛ не является исключением из общего правила [1, 2]. В отличие от других систем и сетей связи поколения 4*G*, в МАКВИЛ на каждой БС используется многоэлементная антенная решетка, осуществляющая адаптивное управление лучами индивидуальных диаграмм направленности (ДН), сопровождающих перемещающихся абонентов, с одновременным подавлением сигналов в направлениях источников помех[1] [1, 3]. В ближайшие планы входят применение методов пеленга со сверхразрешением [4, 5], подключения полноценного режима MIMO [6-8] и усовершенствованная обработка с применением новых схем модуляции [9-12]. Поэтому энергетический бюджет радиолиний подключения абонентов в МАКВИЛ имеет очень высокие показатели. Число БС, обеспечивающих покрытие территории при работе с абонентами, оказывается в несколько раз меньше числа БС, необходимого для тех же целей в известных системах поколения 4*G* с фиксированной секторной организацией [13]. Главный показатель, определяющий эффективность покрытия сети МАКВИЛ, оказывается связанным с широковещательными каналами управления, которые должны обеспечивать работу с абонентской аппаратурой начальных версий без поддержки адаптивной пространственной селекции сигналов. Дефолтные установки МАКВИЛ, обеспечивающие либо круговую ДН, либо полукруговую ДН для каналов широковещательного управления, зачастую оказываются далеко не оптимальными. Более точные настройки с учетом рельефа местности и локальных концентраций сосредоточения абонентов позволят более эффективно использовать ресурсы радиоканала в целом и сократить требуемое число БС.

Целью данной работы является разработка программно-вычислительного инструмента расчета весовых коэффициентов многоэлементной антенной решетки отдельной БС сети МАКВИЛ, формирующего ДН широковещательных каналов управления, наилучшим образом согласующуюся с эталоном, сгенерированным методами машинного обучения.

Схема формирования диаграммы направленности антенны БС для широковещательных каналов сети МАКВИЛ

На рис. 1а, 1б, 1в показаны типовые многоэлементные антенные системы, применяемые на БС сети МАКВИЛ в диапазонах 350 МГц, 420 МГц и 1800 МГц, соответственно.

[1] ГОСТ Р 58166-2018. Технические требования к радиоинтерфейсу широкополосной подвижной радиосвязи (ШПР). Организация протоколов и алгоритмов работы на канальном и физическом уровнях. Основные параметры и технические требования. – М.: Стандартинформ, 2018. – 142 с.

а) б) в)

Рисунок 1

Формирование ДН широковещательных каналов (к ним относятся сигнал преамбулы и сигнал ВСН, содержащий системную информацию, необходимую для подключения к сети) реализуется в МАКВИЛ цифровым способом путем настройки весовых коэффициентов синфазных $W0\_I_i$ и ортогональных $W0\_Q_i$, квадратурных каналов каждого антенного тракта i=1,2, …, Na, где Na – число антенных элементов. Для стандартной конфигурации Na =8.

На рис. 2 показана укрупненная блок-схема формирования ДН широковещательных каналов сети МАКВИЛ. Настраиваемые весовые коэффициенты $W0\_I_i$ и $W0\_Q_i$ могут принимать значения из диапазона [-1; +1] так, что для каждого канала выполняется неравенство:

$$\left(W0\_I_i^2 + W0\_Q_i^2\right) \le 1 \text{, для любого } i = 1,2,...,N_a. \quad (1)$$

В каждом антенном канале используется собственный усилитель мощности (УМ) с заданным предельным уровнем сигнала, формируемого на выходе. Поэтому, как только для какого-то антенного канала номер i неравенство (1) становится строгим, возникает принудительное уменьшение общей мощности трансляции в широковещательных каналах управления. Такое ограничение не является оправданным, поскольку может приводить только к сокращению зоны обслуживания БС. На этом основании режим управления весами следует производить при ограничениях с заменой условий (1) на равенства. Фактически это означает управление только фазами сигналов на входах УМ антенных каналов. Принудительное уменьшение мощности каналов управления может использоваться только в специфических случаях, требующих специального сокращения зоны обслуживания БС. При этом наиболее рациональным способом такого сокращения представляется использование ограничений вида:

$$\left(W0\_I_i^2 + W0\_Q_i^2\right) = a^2 < 1 \text{, для } i = 1,2,...,N_a. \quad (2)$$

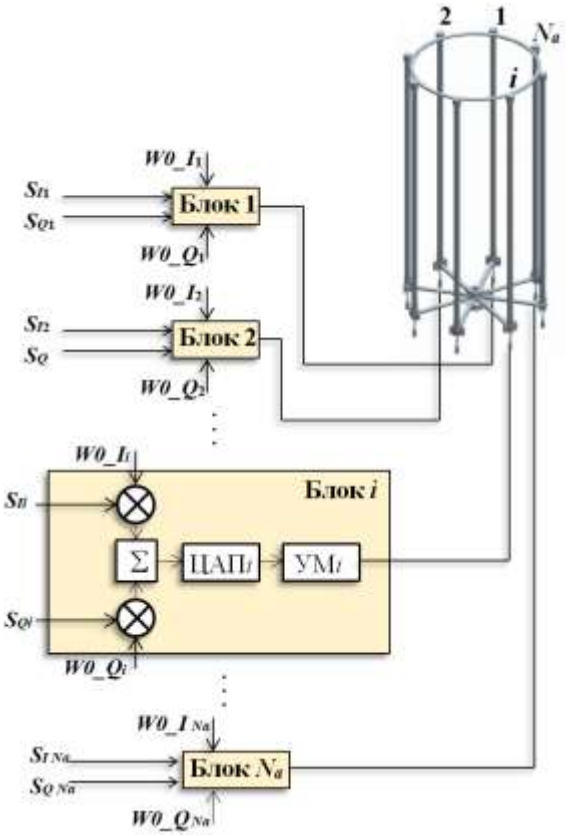

Рисунок 2

Алгоритмы настройки весовых коэффициентов для формирования диаграмм направленности антенн в широковещательных каналах управления

В качестве начальных условий настройки весовых коэффициентов, а вместе с ними и ДН антенной системы БС, использовались:

1) желательная эталонная форма ДН;
2) число антенных элементов, составляющих многоэлементную систему БС;
3) геометрия расположения отдельных антенн, составляющих многоэлементную систему;
4) амплитудная и фазовая составляющие ДН отдельной антенны;
5) функция штрафов за отклонения формируемой ДН от заданной эталонной формы.

Вышеперечисленные показатели задаются оператором, исходя из конкретных условий. На их основе программа машинного обучения в сочетании с алгоритмом адаптивной настройки весов формировала искомую ДН. В качестве указанного алгоритма адаптивной настройки весов использовался градиентный пошаговый алгоритм с набором минимизируемых целевых функций вида:

$$J\left(\vec{W}0\middle|M\right)=\sum_{k=0}^{359}V\left(\varphi_k\right)\left|D_S\left(\varphi_k\right)-D\left(\varphi_k\middle|\vec{W}0,N_a,\vec{P}_x,\vec{P}_y\right)\right|^M, \qquad (3)$$

где: M = 1, 2, 4, 6, 8, 16 – показатель степени, используемый при расчете невязки между эталонной ДН и ДН антенной системы БС, $V\left(\varphi_k\right)$ – функция штрафа за

ошибку настройки ДН в азимутальном направлении $\varphi_k = k \times 1^{\circ}$ $\left(k=0...359\right)$, $D_S\left(\varphi_k\right)$ – желательная эталонная форма азимутальной ДН, построенная в направлениях $\varphi_k = k \times 1^{\circ}$ $\left(k=0...359\right)$, $D\left(\varphi_k \middle| \vec{W}0, N_a, \vec{P}_x, \vec{P}_y\right)$ – азимутальная ДН антенной системы БС, формируемая в направлениях $\varphi_k = k \times 1^{\circ}$ $\left(k=0...359\right)$ для заданных параметров:

1) Na – число антенн;
2) $\vec{W}0 = \left(W0\_I_1,...,W0\_I_{Na},\ W0\_Q_1,...,W0\_Q_{Na}\right)^T$ – вектор весовых коэффициентов;
3) $\vec{P}_x = \left(x_1,...,x_{Na}\right)^T, \vec{P}_y = \left(y_1,...,y_{Na}\right)^T$ – векторы x и y координат оптических центров антенных элементов в проекции на азимутальную плоскость.

Для каждого значения показателя степени M, используемого в (3), градиентный алгоритм настройки весов, с учетом ограничений (3), будет иметь вид [14]:

$$\begin{cases} W0\_I_i\left(n\right) = \cos\left(\psi_i\left(n\right)\right),\ \ W0\_Q_i\left(n\right) = \sin\left(\psi_i\left(n\right)\right), \\ \psi_i\left(n+1\right) = \psi_i\left(n\right) - \mu\left(-\dfrac{\partial J\left(\vec{W}0\left(n\right)\middle|M\right)}{\partial W0\_I_i\left(n\right)} W0\_Q_i\left(n\right) + \dfrac{\partial J\left(\vec{W}0\left(n\right)\middle|M\right)}{\partial W0\_Q_i\left(n\right)} W0\_I_i\left(n\right)\right), \\ i = 1,2,...,N_a,\ \ n = 0,1,2,... \end{cases} \quad (4)$$

где: n – номер шага настройки; $W0\_I_i\left(n\right),\ W0\_Q_i\left(n\right)$ – весовые коэффициенты, сформированные градиентным алгоритмом на шаге настройки n; $J\left(\vec{W}0\left(n\right)\middle|M\right)$ – целевая функция невязки (3), построенная для весового вектора $\vec{W}0\left(n\right) = \left(W0\_I_1\left(n\right),...,W0\_I_{Na}\left(n\right),\ W0\_Q_1\left(n\right),...,W0\_Q_{Na}\left(n\right)\right)^T$; μ – шаг настройки градиентного алгоритма; $\psi_i\left(n\right)$ – вспомогательные параметры фазы, принимающие нулевые значения в начальном состоянии $\psi_i\left(0\right) = 0$.

Остановка работы градиентного алгоритма (4) выполнялась на шаге n по выполнению условия:

$$J\left(\vec{W}0\left(n+1\right)\middle|M\right) > J\left(\vec{W}0\left(n\right)\middle|M\right). \quad (5)$$

При программировании градиентного алгоритма (4) также учитывалась возможность использования антенных элементов с азимутальными ДН, отличными от круговых. Поэтому помимо координат $\vec{P}_x = \left(x_1,...,x_{Na}\right)^T, \vec{P}_y = \left(y_1,...,y_{Na}\right)^T$ оператору предлагается устанавливать азимуты главных лепестков ДН антенных элементов Φ_1, Φ_2, … , Φ_{Na}. Но при использовании штатных антенных элементов МАКВИЛ с круговыми ДН, работа алгоритма и результаты оказываются независящими от указанных азимутальных параметров.

Программа настройки весовых коэффициентов, формирующая диаграммы направленности антенн

Задача формирования ДН антенн для широковещательных каналов не требует решения в реальном масштабе времени. Процедура ввода в эксплуатацию как новых сегментов сетей, так и отдельных БС осуществляется, как правило, поэтапно и занимает от нескольких дней до месяцев. Поэтому к производительности программы настройки ДН широковещательных каналов не предъявляются высокие требования. Вполне допустимыми представляются вычислительные затраты в пределах суток. Поэтому для современных ПК оказалось возможным реализовать работу алгоритмов (4) в сочетании с машинным обучением на базе простых *VBA Excel*-макросов. В течение нескольких часов они формируют оптимизированные решения, генерируют визуализированные отчеты и предоставляют численные оценки достигнутых технических показателей. При этом оказывается возможным использовать удобный интерфейс *Excel*, формировать отчеты с использованием графиков, накладываемых на карты местности, включать дополнительные расчетные показатели в случае необходимости. Широкая и повсеместная освоенность интерфейса *Excel* пользователями ПК снимает психологический барьер начального освоения разработанной программы.

На рис. 3 показан интерфейс программы настройки весовых коэффициентов, формирующей ДН антенн для широковещательных каналов управления сети МАКВИЛ.

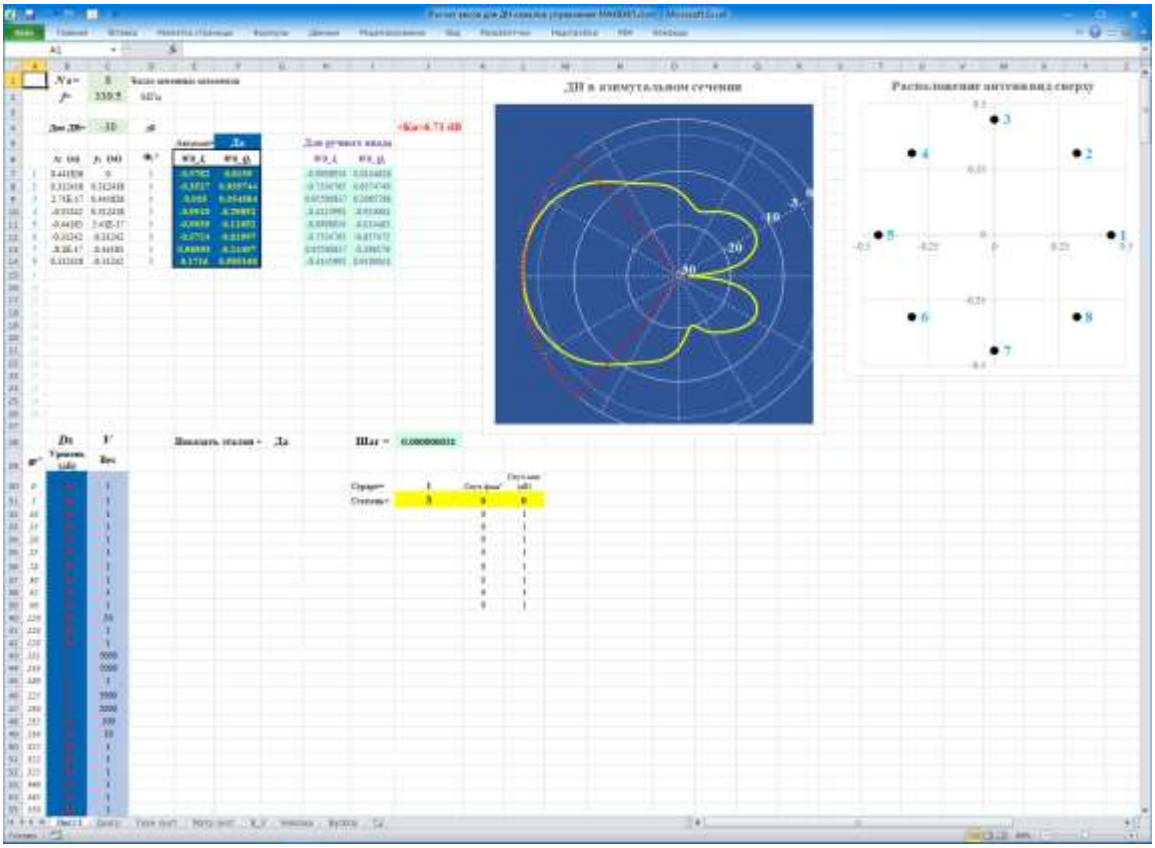

Рисунок 3

Рис. 4 в увеличенном масштабе поясняет как устанавливается: в ячейке «*C*1» – число антенн; в «*C*2» – частота несущего колебания; в диапазоне «*B*7:*C*26» –

координаты расположения антенных элементов в проекции на азимутальную плоскость; в диапазоне «*D*7:*D*26» – углы поворотов главных лепестков ДН антенных элементов. При изменении числа антенных элементов и их координат размещения автоматически корректируется визуальная схема расположения, присутствующая в правой верхней части рис. 3.

На рис. 5 показаны поля установки эталонной формы азимутальной ДН $D_S(\varphi_k)$ и функции штрафов $V(\varphi_k)$ за ошибки настройки. В промежуточных азимутальных позициях между опорными точками эталонной диаграммы, расположенными в столбце «*A*», начиная со строки 30, значения ДН и функции штрафов формируются с помощью линейной интерполяции. Если в ячейке «*G*28» установлено «Да», то на схеме ДН, показанной по центру в верхней части рис. 3, автоматически с помощью штриховой красной линии прорисовывается эталонная ДН. Если в ячейке «*G*28» убрать признак «Да», то на схеме эталонная ДН прорисовываться не будет.

Желтым цветом на схеме ДН отображается синтезированная ДН антенной системы БС МАКВИЛ, соответствующая сформированным весовым коэффициентам, автоматически записываемым алгоритмом настройки в рабочие ячейки области «*E*7:*F*26».

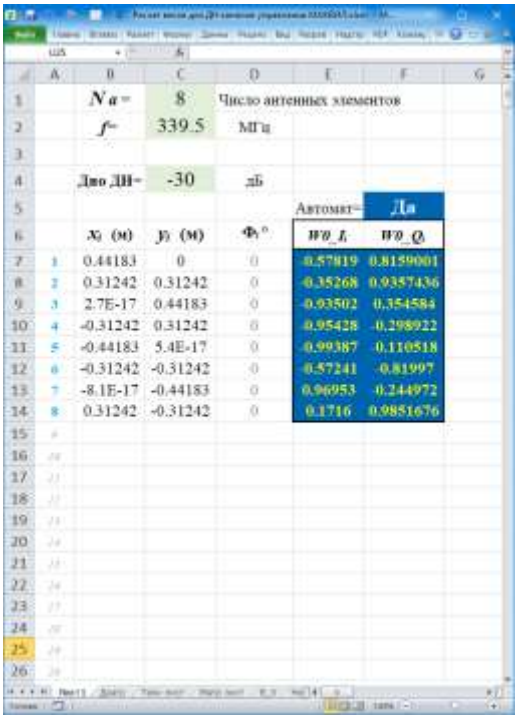

Рисунок 4

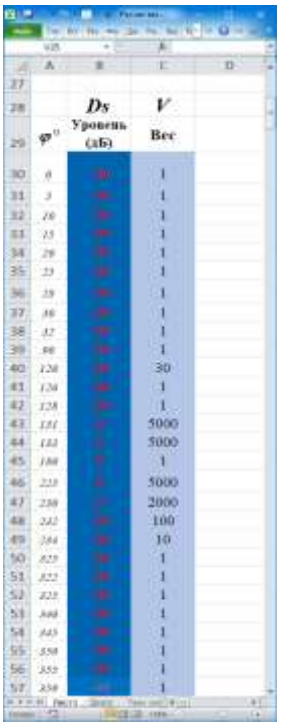

Рисунок 5

В ячейку «*J*4» программа записывает добавку к коэффициенту усиления антенной системы, получаемую за счет настройки ДН в азимутальной плоскости.

Выбирая в ячейках «*K*31», «*L*31» амплитуды случайных погрешностей для коэффициентов усиления и сдвигов фазы в трактах отдельных антенных элементов, можно на схеме ДН наглядно фиксировать искажения ДН антенной системы в целом.

На рис. 6 показана синтезированная ДН широковещательных каналов управления для БС МАКВИЛ, расположенных на телерадиовещательной вышке и в районе нефтебазы г. Новороссийска. При решении практических задач удобно в

качестве фона ДН использовать карты реальной местности, как показано на рис. 6а и 6б, где точки размещения БС совмещены с реальными позициями (г. Новороссийск, телерадиовещательная вышка и район нефтебазы).

а) б)

Рисунок 6

Машинное обучение выполняется путем последовательного проведения серии настроек, каждая из которых осуществляется на основе алгоритма (4) с правилом остановки (5), при случайном выборе показателя *M*. Если очередная настройка не приводит к уменьшению рассогласования ДН с эталоном, то программа восстанавливает значения весовых коэффициентов $W0\_I_1, W0\_Q_1, ..., W0\_I_{Na}, W0\_Q_{Na}$, имевшихся на момент начала последней настройки, исключает из списка допустимых показатель *M* последней настройки и снова переходит к шагу случайного выбора показателя *M* для выполнения следующей попытки настройки. Если все допустимые значения показателя *M* оказываются испытанными и не дают уменьшения рассогласования, процедура обучения останавливается.

На рис. 7 показана блок-схема алгоритма работы программного модуля машинного обучения, формирующего ДН широковещательных каналов управления сети МАКВИЛ.

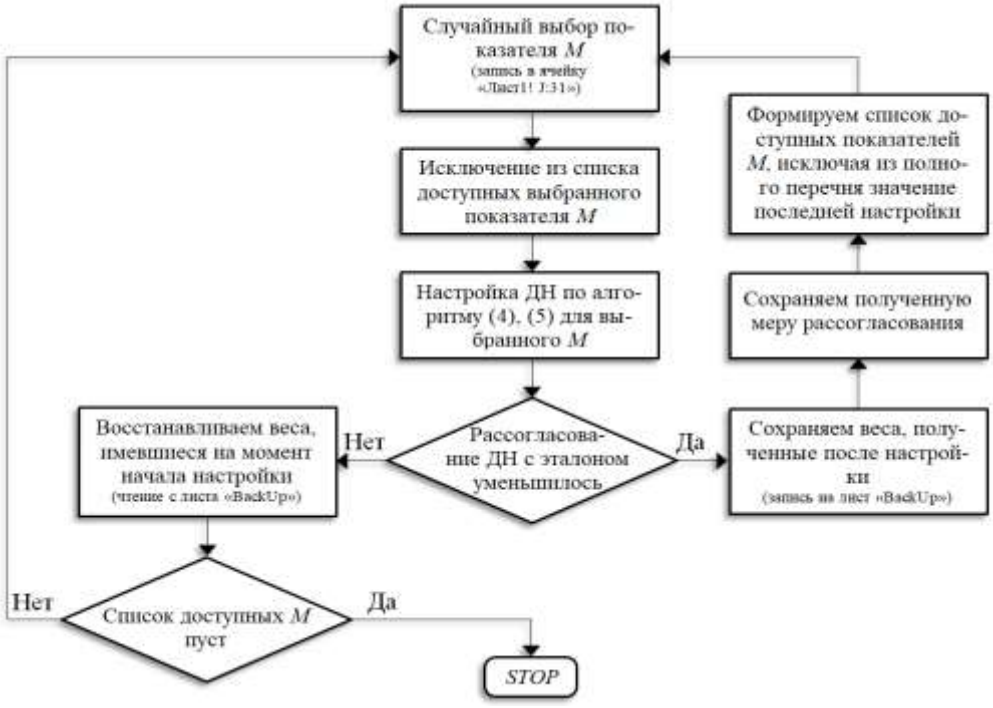

Рисунок 7

Практические результаты настройки диаграмм направленности широковещательных каналов сети МАКВИЛ

Разработанная методика настройки весовых коэффициентов многоэлементных антенн БС МАКВИЛ была применена для ряда практических ситуаций. Наиболее наглядные результаты достигались для территорий со сложным рельефом местности (в основном приморские зоны) и для кварталов городской ультраурбанистической застройки. Ниже в качестве примера приводятся ситуации планирования радиочастотного покрытия г. Новороссийска с акваторией порта и самого высокого небоскреба в Европе «Лахта-центр», расположенного в г. Санкт-Петербург.

Расчет ДН широковещательных каналов управления для г. Новороссийска показал возможность покрытия 85% территории, включая акваторию порта, с помощью только двух БС. Первая из указанных БС размещается на телерадиовещательной башне (рис. 8) с высотой подвеса антенн 154 м. Вторая – в прибрежной зоне на трубе, расположенной на территории нефтебазы (рис. 9).

Рисунок 8

Рисунок 9

Результаты расчета ДН для указанных БС приведены на рис. 6. Полученные весовые коэффициенты даны в табл. 1 для БС на башне, в табл. 2 – для БС на трубе нефтебазы.

Таблица 1.

$W0\_I_i$	$W0\_Q_i$
-0,6663	-0,7452
0,9503	0,3114
-0,6461	0,7623
-0,7693	0,6404
-0,6618	0,7488
0,9456	-0,3247
-0,6592	-0,7522
-0,7523	-0,6598

Таблица 2.

$W0\_I_i$	$W0\_Q_i$
-0,5782	0,8159
-0,3527	0,9357
-0,9350	0,3546
-0,9543	-0,2989
-0,9939	-0,1105
-0,5724	-0,8200
0,9695	-0,2450
0,1716	0,9852

Дополнительное увеличение коэффициентов усиления антенн за счет азимутальной компоненты составило ΔKu = 8,11 дБ – для БС на телерадиовещательной башне и ΔKu = 6,71 дБ – для БС на трубе нефтебазы.

На рис. 10а, показано совместное расположение двух БС, осуществляющих радиочастотное покрытие г. Новороссийска с индивидуальными ДН широковещательных каналов управления (для оптимизированной настройки ДН).

Рисунок 10

Размеры ДН приведены в условном масштабе с учетом увеличений *Ku*, пересчитанных на карту местности для показателя степени затухания на трассах г. Новороссийска, равного 3. Указанный показатель был выявлен на основе драйв-тестов. На рис. 10б показан вариант расположения минимального числа БС (равно трем), которое способно обеспечить радиочастотное покрытие территории г. Новороссийска с акваторией порта при использовании дефолтных установок весов, реализующих круговые или полукруговые ДН широковещательных каналов (для штатных вариантов ДН). Рис. 10 наглядно демонстрирует преимущества предложенной методики оптимизации ДН, приводящей к сокращению минимально необходимого числа БС МАКВИЛ от 3 до 2.

Второй пример применения разработанной методики относится к покрытию высотного здания Лахта-центра. Для таких зданий расположение БС на относительно близких расстояниях приводит к тому, что верхние или нижние этажи выходят за пределы главного лепестка ДН вертикального сечения. Это показано на рис. 11 вверху, где красным цветом помечены этажи Лахта-центра, на которых отсутствовало покрытие при расположении обслуживающей БС на удалении 2,5 км. В ситуации расположения обслуживающей БС по адресу: Гаккелевская ул., 21, удаленность от Лахта-центра составила 4,5 км, и все здание попало в главный лепесток вертикальной ДН. Но для штатной антенны со штатной полукруговой азимутальной ДН бюджет радиоканала даже на предельной мощности трансляции не обеспечил проникновение радиосигнала внутрь здания. Эта ситуация показана в нижней части рис. 11.

На рис. 11 показана проблема радиочастотного покрытия для ультраурбанистической застройки на примере Лахта-центра в г. Санкт-Петербург.

В результате применения разработанной методики настройки были получены оптимальные весовые коэффициенты, приведенные в табл. 3 (БС, расположенной на ул. Гаккелевская, 21, обслуживающей здание Лахта-центра). Соответствующая им азимутальная ДН показана на рис. 12. Дополнительное увеличение коэффициента направленности штатной антенны диапазона 340 МГц, достигаемое за счет фокусировки азимутальной ДН, составило ΔKu =7,95 дБ. Что против штатной полукруговой ДН привело к увеличению мощности приходящего

сигнала на 7,95 дБ -2,47 дБ = 5,48 дБ и обеспечило проникновение внутрь здания, за исключением лифтовых шахт.

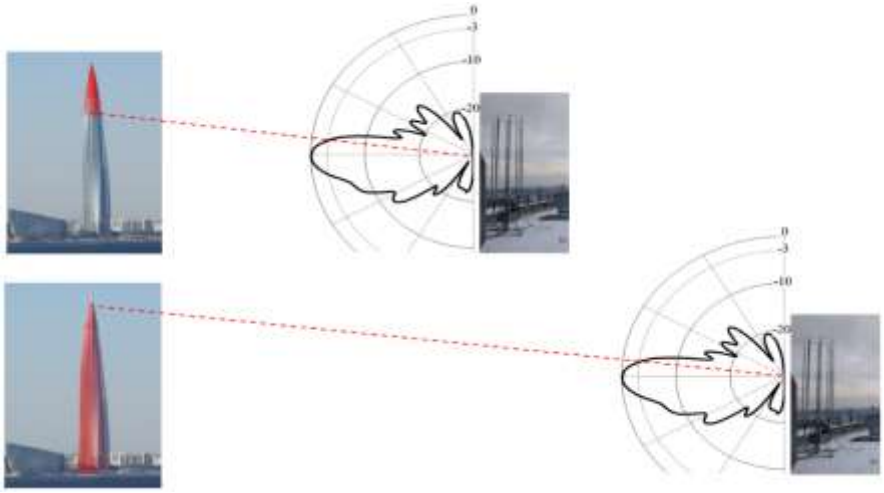

Рисунок 11

Рис. 13 иллюстрирует указанный положительный эффект. Последнее обстоятельство было преодолено уже на этапе развития сети МАКВИЛ путем специально синтезированной для этого антенной системы, показанной на рис. 14. Тем не менее, нужно отметить, что на начальном этапе развертывания сети МАКВИЛ предложенная методика позволила без применения дополнительных БС и специально сконструированных антенн добиться электромагнитного доступа для абонентов практически везде внутри Лахта-центра.

Таблица 3.

$W0\_I_i$	$W0\_Q_i$
-0,9926	0,1214
-0,9234	0,3838
0,6479	0,7617
0,0477	-0,9989
-0,9926	-0,1214
-0,9234	-0,3838
0,6479	-0,7617
0,0477	0,9989

Рисунок 12

Рисунок 13

Рисунок 14

Заключение

В результате проведенного технического анализа сети МАКВИЛ было установлено, что ключевым показателем успешной организации доступа выступает наличие электромагнитного покрытия территории широковещательными каналами управления. В условиях сложного рельефа местности и/или урбанистической застройки заметное улучшение указанного покрытия можно получить при оптимизации формы диаграмм направленности антенн базовых станций. С этой целью были разработаны: специальная методика, алгоритм и программа машинного обучения для точной настройки весовых коэффициентов, при помощи которых в МАКВИЛ реализуется управление диаграммами направленности широковещательных каналов. Экспериментальная проверка показала, что в ряде случаев разработанный подход позволяет в 1,5-2 раза сократить минимально достаточное для реализации покрытия число БС. Приведены примеры покрытий сетью МАКВИЛ территории г. Новороссийск (с акваторией порта) и здания Лахта-центра в г. Санкт-Петербург, полученные с помощью предложенной методики. Показано, что в каждом случае удается сократить необходимое число БС.

Литература

1. Аверьянов Р.С., Бокк Г.О., Володина Е.Е., Кудин А.В., Лохвицкий М.С., Пантикян Р.Т., Смирнов А.В., Шорин А.О. Транкинговая система широкополосного доступа МАКВИЛ // Под ред. О.А. Шорина: Монография. – М.: ООО «Издательский дом Медиа Паблишер», 2021. – 196 с.

2. Шорин О.А., Косинов М.И., Каспари Р.Ю., Осин В.В. Рынок корпоративных пользователей и технология широкополосного мобильного доступа MCWILL // Электросвязь, 2017. – № 1. – С. 16-21.

3. Лохвицкий М.С., Сорокин А.С., Шорин О.А. Мобильная связь: стандарты, структуры, алгоритмы, планирование. – М.: Горячая линия – Телеком, 2019. – 264 с.

4. Аджемов С.С., Бокк Г.О., Зайцев А.Г., Миненко П.В., Струев А.В. Модифицированный алгоритм пространственного разрешения источников

радиоизлучения SDS-MUSIC, работающий при многолучевом распространении сигналов // Радиотехника, 2003. – № 11. – С. 80.
5. Бокк Г.О. Повышение эффективности работы систем связи на основе пространственно-временной обработки и спектрального анализа сигналов/ Диссертация на соискание ученой степени д.т.н.: 05.12.17. – Москва, 2000. – 396 с.
6. Бокк Г.О. MIMO: Оптимизация управления числом логических каналов // Электросвязь, 2017. – № 1. – С. 40-44.
7. Бокк Г.О. MIMO: Оптимизация управления числом логических каналов // В книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) XXXVIII международной конференции РАЕН, 2016. – С. 6.
8. Бокк Г.О. Оптимизация MIMO с введением управления числом логических каналов // В сборнике: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов XXX международной конференции РАЕН. Региональное отделение Российской Академии Естественных Наук «Экономика и качество систем связи» и ЗАО «НИРИТ», 2011. – С. 97-109.
9. Шорин О.А., Бокк Г.О. Аналитическое решение вариационной задачи Шеннона по определению оптимальной структуры сигнала в условиях ограниченной пиковой мощности // Экономика и качество систем связи, 2018. – № 1 (7). – С. 30-39.
10. Шорин О.А., Бокк Г.О. Численные результаты решения вариационной задачи Шеннона определения оптимальной структуры сигнала в условиях ограниченной пиковой мощности // Экономика и качество систем связи, 2018. – № 1 (7). – С. 39-47.
11. 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.
12. Шорин О.А., Бокк Г.О. Оптимальная структура дискретной QAM-модуляции, обеспечивающая максимум информационной производительности радиоканала // Экономика и качество систем связи, 2018. – № 3 (9). – С. 9-17.
13. Sesia S., Toufik I., Baker M. LTE – the UMTS Long Term Evolution: From Theory to Practice // John Wiley&Sons, 2011. – p. 752.
14. Уидроу Б., Стирнз С. Адаптивная обработка сигналов. – М.: Радио и связь, 1989. – 440 с.

ИСПОЛЬЗОВАНИЕ SDR-ТЕХНОЛОГИИ ДЛЯ ЗАДАЧ СЕТЕВОГО ПОЗИЦИОНИРОВАНИЯ: ФОРМИРОВАНИЕ ИНФОРМАЦИОННОГО БЛОКА MIB

Г.А. Фокин, *д.т.н., профессор, 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. Объектом настоящего исследования является *SDR*-демонстратор технологии позиционирования в сети *LTE*, разработанный для

апробации новых технических решений по повышению точности определения местоположения устройств *UE* в существующих сетях 4*G LTE* и в перспективных сетях 5*G NR*. Результатом настоящего исследования является реализация и экспериментальная апробация формирователя блока *MIB* стандарта *LTE*.

Ключевые слова: 4*G*; *LTE*; *SDR*; *MIB*; *PBCH;* позиционирование.

SOFTWARE-DEFINED RADIO NETWORK POSITIONING TECHNOLOGY DESIGN: MIB TRANSCEIVER DEVELOPMENT

Grigoriy Fokin, *Doctor of Science, 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 object of this research is a software-defined radio (*SDR*) *LTE* network positioning technology prototype design for testing new technical solutions to improve the accuracy of *UE* location estimation in existing *LTE* and emerging 5*G NR* networks. The contribution of this research is *MIB* software realization and its experimental validation in laboratory conditions.

Keywords: 4*G*; *LTE*; *SDR*; *MIB*; *PBCH*; positioning.

Введение

В области позиционирования пользовательских устройств *UE* (*User Equipment*) большую роль играет не только точность, но и доступность услуги определения местоположения (ОМП). Позиционирование с использованием сигналов глобальных навигационных спутниковых систем (ГНСС, *GNSS – Global Navigation Satellite System*) обеспечивает приемлемую точность во многих сценариях [1-2]. Однако, устойчивый прием сигналов ГНСС в неблагоприятных погодных условиях и в плотной городской застройке в условиях отсутствия прямой видимости *NLOS* (*Non-Line Of Sight*) зачастую невозможен.

В последние годы высокую актуальность и востребованность приобрел метод сетевого позиционирования *UE* с использованием инфраструктуры базовых станций *eNB* (*Evolved NodeB*) сотовых сетей подвижной радиосвязи *LTE* (*Long-Term Evolution*). Описание данного метода нашло отражение в ряде работ отечественных [1-3] и зарубежных авторов [4-6]. Анализ данных работ позволяет выделить отдельное направление исследований, а именно, использование технологий программно-конфигурируемого радио *SDR* (*Software-Defined Radio*) и модельно-ориентированного проектирования для решения задач сетевого позиционирования.

На данный момент уже существует прототип (демонстратор) [7] программно-аппаратной реализации передатчика и приемника системы позиционирования в сети *LTE*, представляющий собой прототипы базовой станции *eNB* и пользовательского устройства *UE*, соответственно. Настоящая статья является продолжением серии работ, посвященных описанию и экспериментальной апробации разработанного *SDR*-демонстратора.

Для выполнения первичных измерений существующий демонстратор реализует передачу и прием таких сигналов, как сигналы синхронизации (*PSS – Primary Synchronization Signal* и *SSS – Secondary Synchronization Signal*), а также опорных сигналов (*CRS – Cell-Specific Reference Signal* и *PRS – Positioning Reference Signal*).

В текущей реализации демонстратора для приема перечисленных выше сигналов и сбора первичных измерений необходимо вручную выставлять и контролировать параметры нисходящего канала связи *DL* на стороне приемника (*UE*). Для снятия данного ограничения и перехода к автоматической настройке параметров нисходящего канала связи *DL* между прототипами *eNB* и *UE* необходима программная реализация и верификация процедур передачи главного информационного блока *MIB* (*Master Information Block*) вместе с другими необходимыми предварительными процедурами приемного радиоинтерфейса.

Процедуры приема и обработки опорных сигналов стандарта *LTE*

Анализ методов приема опорных сигналов стандарта *LTE* для сетевого позиционирования имеет своим результатом обоснование структуры устройства и последовательность соответствующих этапов и процедур обработки. Рисунок 1 иллюстрирует укрупненную структуру *SDR* приемника опорных сигналов *LTE* для задач позиционирования «на лету» [8].

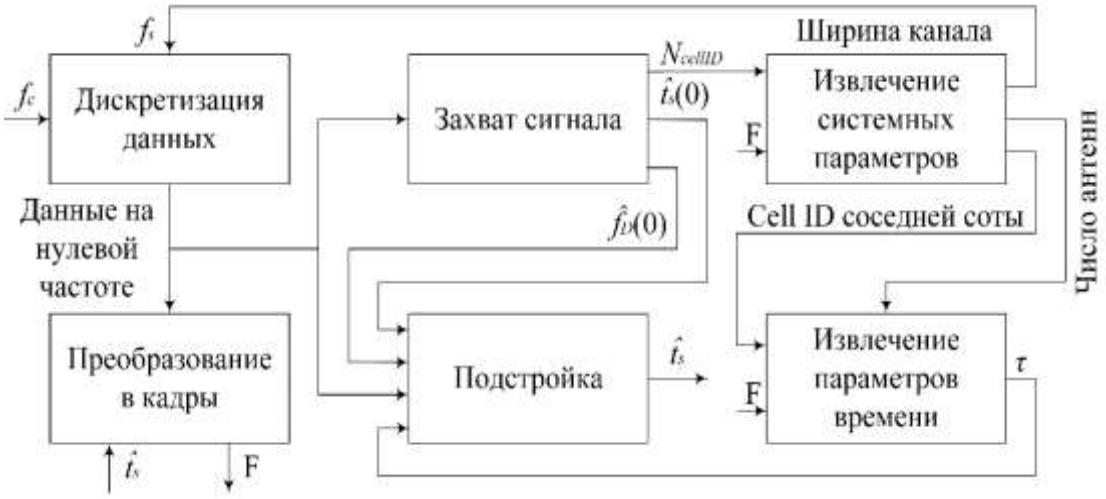

Рисунок 1

На первом этапе выполняется захват радиосигнала на несущей центральной частоте f_c, его перенос в область информационных частот (*baseband*) и дискретизация с частотой f_s. Захват включает грубую оценку времени прихода $\hat{t}_s(0)$ и допплеровского сдвига частоты $\hat{f}_D(0)$ для начальной кадровой синхронизации путем вычисления корреляционных функций принятого сигнала с локальными копиями опорных сигналов первичной *PSS* и вторичной *SSS* синхронизации. Также на первом этапе определяется идентификатор соты *Cell ID*.

На втором этапе производится преобразование выборок принятого *OFDM* сигнала в частотно-временную структуру кадра для последующего извлечения системных параметров из широковещательных каналов на физическом уровне *LTE*, включая ширину канала F.

На третьем этапе осуществляется уточнение захвата и извлечение параметров времени прихода *TOA* τ по опорным сигналам *CRS*.

На четвертом этапе реализуются контуры подстройки для отслеживания кратковременных изменений времени прихода сигнала *TOA* $\hat{t}_s$.

Рассмотрим далее методы и процедуры обработки опорных сигналов на каждом из этапов.

Захват и грубая подстройка

При первоначальном приеме радиосигнала *LTE* пользовательскому устройству *UE* необходимо, в первую очередь, осуществить грубую подстройку к излучаемым базовыми станциями *eNB* широковещательным каналам путем захвата сигналов первичной *PSS* и вторичной *SSS* синхронизации и грубой подстройки к ним [9]. С точки зрения дискретизированного *baseband*-сигнала на нулевой частоте, момент начала захвата может приходиться на произвольный интервал *OFDM* символа произвольного кадра стандарта *LTE*. Рисунок 2 иллюстрирует поток выборок принимаемого сигнала и произвольный момент начала захвата.

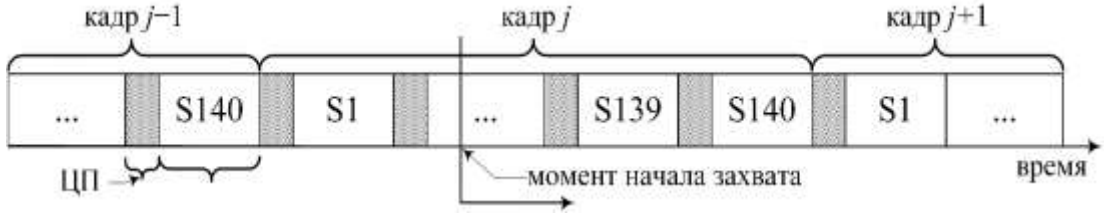

Рисунок 2

Для вхождения в режим приема *SDR* устройству необходимо предварительно установить начало *OFDM* символа с тем, чтобы исключить циклический префикс и затем вычислить быстрое преобразование Фурье (БПФ, *FFT – Fast Fourier Transform*) для преобразования последовательного потока выборок в структуру кадра стандарта *LTE* [10]. Для установления начала *OFDM* символа приемное устройство осуществляет поиск и обнаружение сигнала первичной синхронизации *PSS* в кадре. Используя ортогональные свойства последовательностей Задова-Чу, приемное устройство вычисляет корреляционную функцию принятого сигнала со всеми возможными локальными копиями последовательностей *PSS* согласно выражению [11]:

$$\mathcal{R}(m) = \sum_{n=0}^{N_f-1} r(n) s_{PSS}^*(n+m)_{N_f} = r(m) \circledast_{N_f} s_{PSS}^*(-m)_{N_f}, \quad (1)$$

где: $r(n)$ – принятый сигнал; $s_{PSS}(n)$ – локально сгенерированная копия сигнала *PSS* во временном домене; $N_f = T_f/T_s$ – длина кадра (в числе *OFDM* символов); $(\cdot)^*$ – оператор комплексного сопряжения; $(\cdot)_{N_f}$ – оператор циклического сдвига; $\circledast_N$ – оператор циклической свертки.

Пусть $R(k) = \text{FFT}\{r(n)\}$ и $S_{PSS}(k) = \text{FFT}\{s_{PSS}(n)\}$, тогда справедливо выражение:

$$\mathcal{R}(m) = \text{IFFT}\{R(k) S_{PSS}^*(k)\} \quad (2)$$

Идентификатор соты в пределах группы $N_{ID}^{(2)}$ определяется по максимальному пику корреляционной функции $\mathcal{R}(m)$. Представленная выше корреляционная функция $\mathcal{R}(m)$ на основе БПФ используется также и для обнаружения вторичного сигнала синхронизации *SSS*. Идентификатор группы сот $N_{ID}^{(1)}$ также определяется по максимальному пику корреляционной функции $\mathcal{R}(m)$. После обнаружения первичного *PSS* и вторичного *SSS* сигналов синхронизации, пользовательское устройство *UE* может установить время начала кадра *LTE* и уникальный идентификатор соты *Cell ID* N_{ID}^{Cell} базовой станции *eNB*.

Рисунок 3 иллюстрирует структуру блока захвата и грубой подстройки.

Первичный сигнал синхронизации *PSS* передается два раза за время передачи кадра, поэтому после реализации процедуры захвата на интервале длительности кадра в 10 мс можно наблюдать два корреляционных пика. Последовательности *PSS*, излучаемые базовой станцией *eNB* в 0-м и 10-м слотах, идентичны, поэтому пользовательское устройство *UE* из полученных корреляционных пиков сможет извлечь лишь моменты начала *OFDM* символов, но не их номера. Каждый опорный сигнал стандарта *LTE* передается на специально выделенных ему поднесущих и *OFDM* символах в частотно-временном домене кадра, поэтому пользовательскому устройству *UE* недостаточно знать только начало *OFDM* символа. Для установления номеров *OFDM* символов в каждом принимаемом кадре пользовательское устройство *UE* запускает вычисление корреляционной функции во временном домене для вторичных сигналов синхронизации *SSS*. Последовательность вторичного сигнала синхронизации формируется с учетом номера слота [7], поэтому после вычисления корреляционного пика для *SSS* на интервале передачи кадра *UE* сможет установить номер *OFDM* символа в слоте.

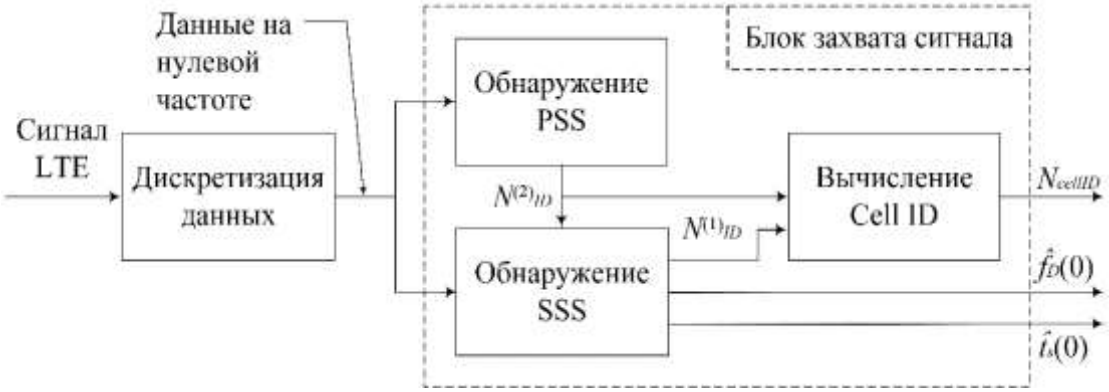

Рисунок 3

Опорные сигналы *PSS* и *SSS* занимают примерно 1 МГц полосы, поэтому при вычислении корреляционных функций полученные в результате корреляционные пики могут достаточно грубо идентифицировать границы кадра *LTE* в условиях многолучевого РРВ. Смещенную оценку временны*х* границ кадра *LTE*, установленную по опорным сигналам синхронизации *PSS* и *SSS*, можно уточнить по опорным сигналам *CRS*, которые занимают значительно более широкую полосу частот. Для обработки сигналов *CRS* «на лету» пользовательскому устройству *UE* необходимо знать занимаемую принимаемым сигналом *LTE* полосу частот. Однако пользовательскому устройству *UE*, не являющемуся абонентом данной сети *LTE*, полоса частот, используемая данным оператором изначально неизвестна. Поэтому *UE* сначала работает на прием в предположении, что используется минимальная полоса частот 1,4 МГц, осуществляет захват сигналов *PSS* и *SSS*, вычисляет *Cell ID*. Далее *UE* выполняет преобразование принятых выборок *OFDM* сигнала в частотно-временную структуру кадра для извлечения системных параметров из широковещательных каналов на физическом уровне *LTE*, в том числе, занимаемой принимаемым сигналом *LTE* полосы частот. После извлечения полосы частот *UE* осуществляется уточнение параметров времени прихода уже по опорным сигналам *CRS*.

Извлечение системных параметров

После захвата и грубой подстройки пользовательскому устройству *UE* необходимо установить ряд параметров сигналов, излучаемых базовыми станциями *eNB* сети *LTE* данного оператора. Рисунок 4 иллюстрирует структуру блока извлечения системных параметров. Для решения задач сетевого позиционирования интерес представляют параметры ширины полосы частот, число передающих антенн и идентификаторы сот *Cell ID* соседних базовых станций. Эти параметры пользовательское устройство *UE* может извлечь из блоков системной информации *MIB* и *SIB* (*System Information Block*), которые транслируются в физическом вещательном канале *PBCH* (*Physical Broadcast Channel*) и физическом разделяемом канале «вниз» *PDSCH* (*Physical Downlink Shared Channel*) соответственно.

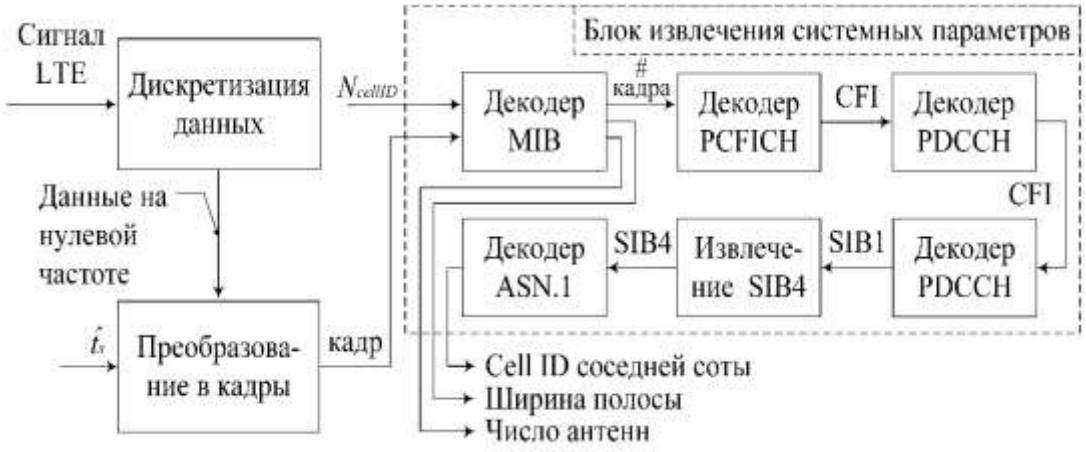

Рисунок 4

Декодирование блока *MIB*

Для использования в задачах сетевого позиционирования более широкополосных по сравнению с *PSS* и *SSS* опорных сигналов *CRS* пользовательскому устройству *UE* необходимо определить ширину полосы частот принимаемого из радиоэфира «на лету» сигнала *LTE*. Параметр ширины полосы частот вместе с числом передающих антенн содержатся в блоке *MIB*, который декодируется *UE* в первую очередь. Чтобы осуществить передачу *MIB* в сети *LTE* необходимо закодировать данный блок системной информации в каналах всех трех уровней: логическом (*BCCH*), транспортном (*BCH – Broadcast Channel*) и физическом (*PBCH*).

Кодирование *MIB* в логическом канале *BCCH* представляет собой формирование информационного пакета данных. Сообщение *MIB* должно состоять ровно из 24-х бит. Более длинные сообщения усекаются до 24-х бит, а более короткие сообщения дополняются нулями до нужной длины.

Пакет *MIB* состоит из следующих полей [12]:

а) Первые три бита отвечают за ширину полосы нисходящего канала связи *DL*, представляют собой двоичное число от 000 до 101, что соответствует множеству полос {6, 15, 25, 50, 75, 100} (в количестве ресурсных блоков); если используется нестандартная ширина полосы (не принадлежит указанному множеству) в первые три бита сообщения *MIB* устанавливаются единицы.

б) Следующий бит отвечает за длительность физического канала *PHICH* (*Physical channel HybridARQ Indicator Channel*) для передачи *HARQ ACK/NACK* в

ответ на передачу информации по восходящей линии связи; может быть нормальным или расширенным, соответственно, 0 или 1.

в) Следующие два бита отвечают за групповой множитель *HICH* (*HybridARQ Indicator Channel*); задается как двоичное число от 00 до 11, что соответствует множителям 1/6, 1/2, 1, или 2.

г) Далее идут восемь бит, кодирующие системный номер кадра *SFN*; несмотря на то, что согласно спецификации, номер кадра может принимать значения от 0 до 1023 (10 бит), стоит отметить, что внутри *MIB* системный номер кадра хранится, как разделенный на 4 и округленный вниз до ближайшего целого.

д) Следующие 10 бит являются зарезервированными и равны нулю.

На первом этапе выполняется проверка циклическим избыточным кодом *CRC* (*Cyclic Redundancy Code*) длины $L = 16$ с использованием полинома $g_{CRC}(D) = D^{16} + D^{12} + D^5 + 1$. Число передающих антенн не транслируется непосредственно в блоке *MIB* из 24 бит; вместо этого данный параметр содержится в маске *CRC*; маска представляет собой последовательность, которая используется для скремблирования битов *CRC*, добавляемых к блоку *MIB*. В зависимости от набора передающих антенн маска *CRC* состоит из: а) всех нулей для одной передающей антенны; б) всех единиц для двух передающих антенн; в) чередования нулей и единиц [0,1,0,1, … ,0,1] для четырех передающих антенн. Для установления числа передающих антенн из принятого сигнала «на лету» пользовательское устройство *UE* выполняет слепой поиск по всем вариантам набора передающих антенн. Затем, путем сравнения локально сгенерированных последовательностей *CRC*, скремблированных маской *CRC* с принятой последовательностью *CRC*, устанавливается число передающих антенн.

На втором этапе выполняется канальное кодирование с использованием сверточного кодера с длиной ограничения 7 и скоростью кодирования 1/3 (

рисунок 5). Кодер инициализируется последними шестью информационными битами входного потока.

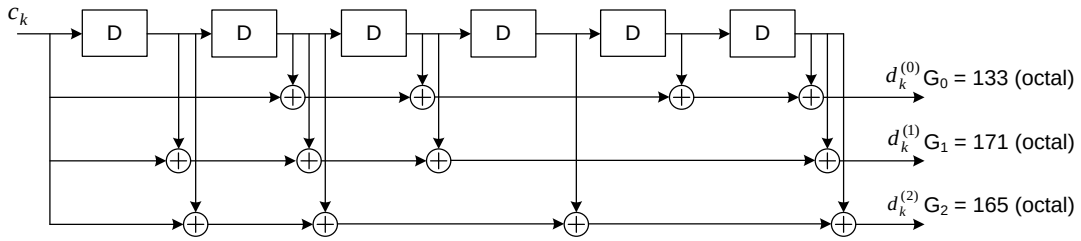

Рисунок 5

Для декодирования канального кода в принятом блоке *MIB* используется метод, показанный на

рисунок 6 [13]: сначала принятая последовательность повторяется один раз; затем расширенная последовательность декодируется декодером Витерби; в завершении средняя часть декодированной последовательности подвергается операции циклического сдвига.

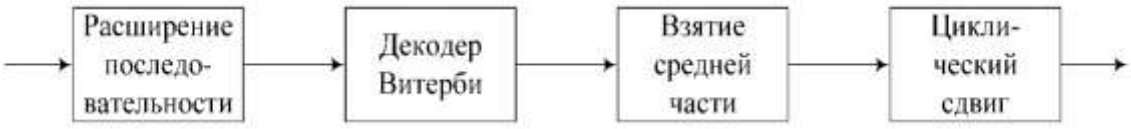

Рисунок 6

Далее на третьем этапе закодированные сверточным кодером биты проходят процедуру согласования скоростей (

рисунок 7). На этапе согласования скоростей закодированные данные сначала перемежаются, после чего потоки результатов перемежения повторяются для получения массива длиной 1920 бит [14].

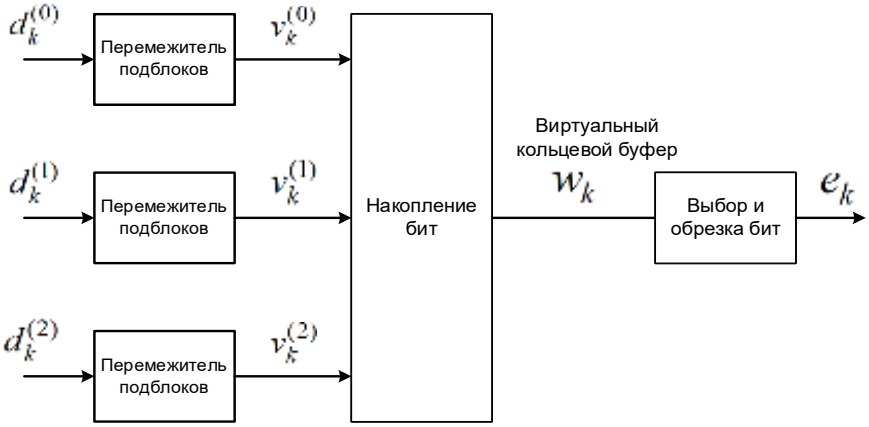

Рисунок 7

На четвертом этапе после согласования скоростей выполняется скремблирование потока псевдослучайной последовательностью, которая инициализируется идентификатором соты *Cell ID*; в результате получается уникальный сигнал для обнаружения всех базовых станций *eNB*.

На пятом этапе над последовательностью из 1920 битов производится квадратурная фазовая манипуляция *QPSK* (*Quadrature Phase Shift Keying*), результатом которой являются 960 комплексных модуляционных символов.

Данные символы на шестом этапе отображаются на различные слои для реализации разнесенной передачи.

После отображения на слои на седьмом этапе выполняется пространственно-временное кодирование *STC* (*Space-Time Coding*), которое служит для компенсации замираний при многолучевом *PPB*.

В заключении, на восьмом этапе комплексные символы отображаются на предварительно выделенные для передачи блока *MIB* поднесущие [14]. Блок *MIB* кодируется и передается на четырех последовательных символах во втором слоте кадра; данные блока *MIB* не занимают ресурсные элементы, выделенные для передачи опорных сигналов.

Рисунок 8 иллюстрирует процедуры кодирования блока *MIB* согласно [15].

Рисунок 8

Декодирование блока *SIB*

Пользовательское устройство при захвате сигнала *LTE* производит установление идентификаторов сот *Cell ID* N_{ID}^{cell} доступных базовых станций *eNB*, излучаемые радиосигналы которых имеют наибольшую мощность при приеме *UE*. Для одновременного приема нескольких сигналов *eNB* пользовательское устройство может осуществлять перебор по всем N_{ID}^{cell}, вычисляя корреляцию по всем опорным сигналам *PSS*, определяя идентификатор соты в пределах группы $N_{ID}^{(2)} \in \{0,1,2\}$ и по всем опорным сигналам *SSS*, определяя идентификатор группы $N_{ID}^{(2)} \in \{0,\dots,167\}$. Однако данный подход ограничивает число *eNB* одним оператором, сигналы которых *UE* может использовать для позиционирования при одновременном приеме в одном диапазоне частот данного оператора. Другим подходом является извлечение информации об идентификаторах N_{ID}^{cell} соседних *eNB* из блока *SIB*, транслируемого основной базовой станцией. Базовые станции других операторов излучают свои опорные сигналы в других диапазонах частот, поэтому данный подход, использующий *SIB*, может использоваться для извлечения идентификаторов N_{ID}^{cell} соседних базовых станций других операторов. Зная идентификаторы *eNB* и их координаты, *UE* может решить задачу определения своего местоположения.

Блок *SIB* содержит следующую информацию: а) базовой станции *eNB*, к которой подключено *UE*; б) соседних базовых станций *eNB* данного оператора, работающих как в данном диапазоне частот, так и в других диапазонах частот; в) в соседних сотах других сетей, например, *UMTS* и *GSM*; г) другую информацию. Блок *SIB* имеет 17 различных форматов от *SIB1* до *SIB17*, которые передаются по разным расписаниям. *SIB1*, передаваемый в субкадре 5 каждого четного кадра, содержит информацию о расписании остальных блоков *SIB*. Данная информация может быть использована для извлечения расписания передачи блока *SIB4*, в котором содержатся сведения об идентификаторах N_{ID}^{cell} соседних сот базовых станций, работающих в данном диапазоне частот. Для декодирования *SIB1* пользовательское *UE* проходит через несколько этапов. На каждом этапе *UE* необходимо декодировать физический канал для извлечения параметра, который требуется для выполнения следующих этапов.

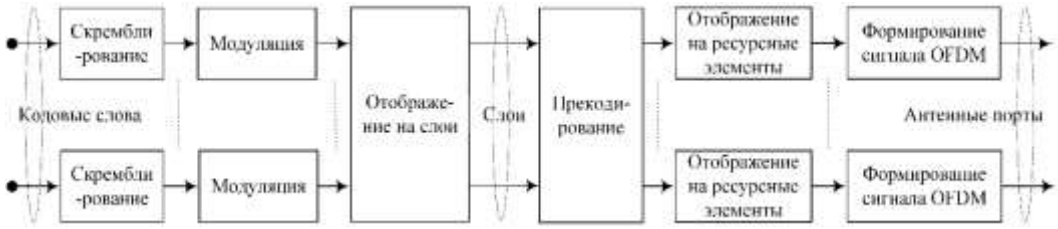

Рисунок 9

Рисунок 9 иллюстрирует последовательность процедур обработки в физических каналах «вниз» *DL* стандарта *LTE*. Несмотря на общую последовательность процедур обработки в *DL*, для каждого физического канала «вниз» отдельные процедуры обработки отличаются.

Демодуляция *PCFICH* и декодирование *CFI*. При демодуляции физического канала управления индикатора формата *PCFICH* (*Physical Control Format Indicator Channel*) пользовательское устройство *UE*, в первую очередь, извлекает индикатор

формата *CFI* (*Control Format Indicator*). Индикатор *CFI* показывает, сколько ресурсных элементов *RE* отводится на физический канал управления «вниз» *PDCCH* (*Physical Downlink Control Channel*); *CFI* может принимать значения 1, 2 или 3. Для декодирования *CFI* пользовательское устройство сначала обнаруживает в кадре *LTE* 16 ресурсных элементов канала *PCFICH*. Затем *UE* выполняет процедуры в обратном порядке по сравнению с последовательностью на

рисунок 9. Результатом декодирования является последовательность из 32 бит. Последовательность, которая может принимать один из трех возможных вариантов, отображается на значение *CFI*.

При использовании канала 1,4 МГц *PDCCH* может занимать от 2 до 4 *OFDM* символов; в остальных случаях (3 МГц, 5 МГц, 10 МГц, 15 МГц и 20 МГц) – от 1 до 3 *OFDM* символов. Размер *PDCCH* канала является динамической величиной и зависит от количества активных соединений. Канал *PCFICH* занимает 16 ресурсных элементов в первом символе каждого подкадра. Эти 16 элементов разбиваются на четыре группы по четыре элемента. Положение групп зависит от ширины канала и физического идентификатора сектора *PCI* (*Physical Cell Identity*). Для передачи *PCFICH* канала используется *QPSK* модуляция, таким образом, в 16 ресурсных элементах можно передать 32 бита. В этих 32-х битах передается *CFI*, который описывает размер *PDCCH* канала в текущем субкадре. Для 1,4 МГц к передаваемому значению *UE* прибавляет единицу; для остальных случаев используется значение, которое передавалось [16].

Демодуляция *PDCCH* и декодирование *DCI*. Зная индикатор *CFI*, пользовательское устройство *UE* может идентифицировать ресурсные элементы *RE* канала *PDCCH* и демодулировать их, получив в результате блок битов *DCI* (*Downlink Control Information*) о канале управления «вниз». Упаковка этих бит может осуществляться в различных форматах на стороне *eNB* и не сообщается *UE*. Для распаковки блока битов *DCI* пользовательское устройство выполняет слепой поиск по всем различных форматам. При этом *UE* проверяет прикрепленные *CRC* биты, и если эти биты скремблированы с помощью определенной последовательности, то этот *DCI* предназначен для данного *UE* и содержит информацию о том, где именно передаются его данные в физическом разделяемом канале «вниз» *PDSCH* (*Physical Downlink Shared Channel*).

Демодуляция *PDSCH* и декодирование *SIB*. Проанализированный индикатор *DCI* обеспечивает *UE* конфигурацию соответствующих ресурсных элементов *RE* физического разделяемого канала «вниз» *PDSCH*, который содержит *SIB*. Биты блока *SIB* декодируются с использованием декодера *ASN.1* (*Abstract Syntax Notation One*), который извлекает системную информацию, передаваемую базовой станцией *eNB* в блоке *SIB*.

Рассмотрев основные процедуры приема и обработки опорных сигналов, включая кодирование блока *MIB*, рассмотрим далее порядок их верификации посредством лабораторных испытаний.

Лабораторные испытания

Лабораторный стенд (

рисунок 10) состоит из:

1. Средства объективного контроля, а именно – векторного анализатора сигналов *Agilent 89600 Vector Signal Analyzer*.

2. ПК с предустановленным СПО *Agilent 89600 Vector Signal Analyzer* [17] для работы с данным анализатором. Анализатор подключен к этому ПК по интерфейсу *FireWire*.

3. Ноутбука с предустановленным СПО *MATLAB*, на котором запущены скрипты формирователя рассматриваемых сигналов.

4. Передающей *SDR*-платы *Ettus USRP B210* [18], подключенной к ноутбуку, в СПО которого формируются сигналы.

5. Коаксиального кабеля (1 м), соединяющего передающий антенный порт *SDR*-платы с входным портом анализатора.

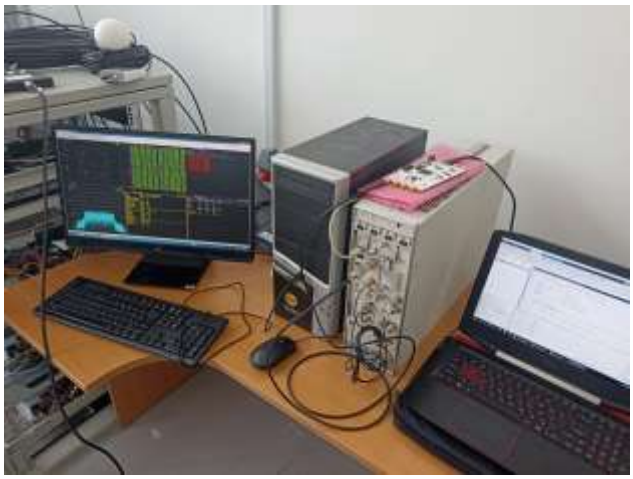

Рисунок 10

Лабораторные испытания заключались в анализе ресурсной сетки *OFDM*-сигнала на предмет наличия в ней сформированного канала *PBCH*, а также в контроле правильности декодирования пакета *MIB* при различных заранее заданных параметрах полей этого пакета.

Также, для формирования сигналов синхронизации и опорных сигналов, был задан идентификатор соты *Cell ID*, равный 9. Идентификатор соты $N_{\mathrm{ID}}^{\mathrm{cell}} = 3N_{\mathrm{ID}}^{(1)} + N_{\mathrm{ID}}^{(2)}$ однозначно определяется числом $N_{\mathrm{ID}}^{(1)}$ в диапазоне от 0 до 167, которое определяет идентификатор группы сот, и числом $N_{\mathrm{ID}}^{(2)}$, находящимся в пределах от 0 до 2 и определяющим идентификатор соты в пределах группы.

Вместе со всем перечисленным была задана нормальная длина циклического префикса.

В рамках испытаний проводилось произвольное изменение полей пакета *MIB* с последующим контролем декодированной информации в программе, работающей с векторным анализатором сигналов *Agilent 89600 Vector Signal Analyzer*. Окно данной программы целиком показано на рис. 11.

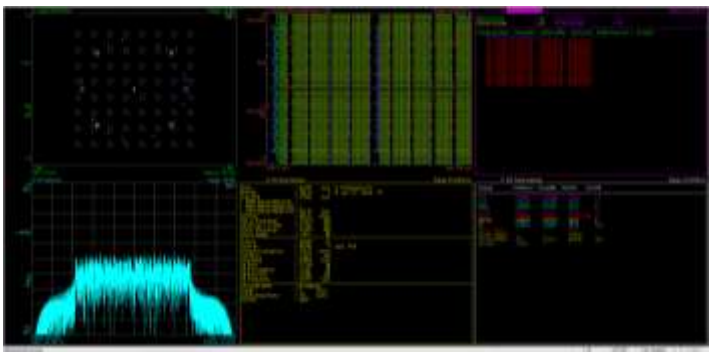

Рисунок 11

В качестве примера проверки корректности работы формирователя на скриншотах ниже (рис. 12 и рис. 13) представлена часть окна программы *Agilent 89600 Vector Signal Analyzer*, в которой показана декодируемая информация из канала *PBCH*. В ходе лабораторных испытаний производилось изменение такого параметра, как длительность *PHICH* с расширенной (*Extended*) на нормальную (*Normal*), также производилось изменение группового множителя *HICH* с 2 на 1.

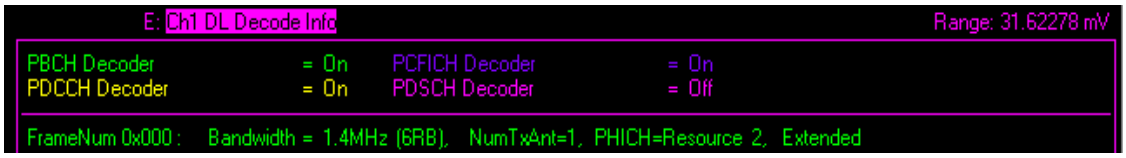

Рисунок 12

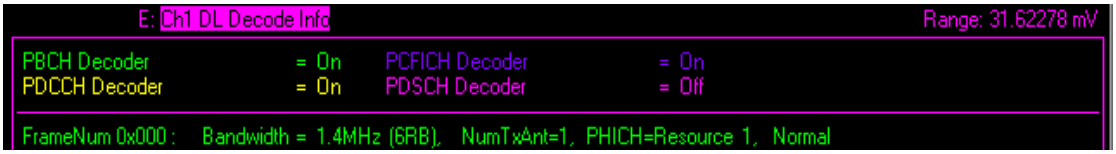

Рисунок 13

В той части окна программы, в которой указан идентификатор соты (
рисунок 14), видно, что *Cell ID* равен 9. Это значение совпадает с установленным предварительно. Более того, видно, что совпадают $N_{\mathrm{ID}}^{(1)}$ и $N_{\mathrm{ID}}^{(2)}$, равные 3 и 0, соответственно, которые однозначно соответствуют идентификатору соты 9. Также наблюдается корректное декодирование длины циклического префикса (*Normal*) и соответствие опорных сигналов позиционирования *PRS* стандартной спецификации 3*GPP* 36.211 [14].

Рисунок 14

Анализируя полученные результаты работы средств объективного контроля в ходе лабораторных испытаний, можно сделать вывод о корректности реализации процедур формирования широковещательного канала *PBCH*, в котором передаются пакеты *MIB*. Кроме того, можно сделать вывод о корректности формирования сигналов синхронизации (*PSS* и *SSS*) и опорных сигналов (*CRS* и *PRS*).

Заключение

В результате данного исследования был реализован и апробирован формирователь главного информационного блока *MIB* стандарта *LTE*. Реализованный на *SDR*-демонстраторе формирователь блока *MIB* позволяет извлекать параметр ширины полосы пропускания и проводить дальнейшие испытания процедур приема опорных сигналов *CRS* макетом пользовательского устройства в полевых условиях. Направлением дальнейших исследований является

реализация полученного кодера главного блока служебной информации *MIB* на ПЛИС, а также реализация декодера блоков *MIB* средствами СПО *MATLAB*.

Литература

1. Фокин Г.А. Технологии сетевого позиционирования. Санкт-Петербург: СПбГУТ, 2020. – 558 с.
2. Фокин Г.А. Технологии сетевого позиционирования 5G. Москва: Горячая Линия – Телеком, 2021. – 456 с.
3. Фокин Г.А. Комплекс моделей и методов позиционирования устройств в сетях пятого поколения. Диссертация на соискание ученой степени доктора технических наук: 05.12.13. Санкт-Петербург, 2021. – 499 с.
4. Zekavat R., Buehrer R.M. Handbook of position location: Theory, practice and advances. John Wiley & Sons, 2019. – 1376 p.
5. Campos R. S., Lovisolo L. RF Positioning: Fundamentals, Applications, and Tools. Artech House, 2015. – 369 p.
6. Sand S., Dammann A., Mensing C. Positioning in Wireless Communications Systems. Wiley, 2014. – 276 p.
7. Фокин Г.А., Волгушев Д.Б., Харин В.Н. Использование SDR технологии для задач сетевого позиционирования. Формирование опорных сигналов LTE // T-Comm: Телекоммуникации и транспорт, 2022. – Т. 16. – № 5. – С. 28-47.
8. Kassas Z.M., Shamaei K., Khalife J. SDR for navigation with LTE signals. Patent US11187774B2. United States. University of California. Publication 30.11.2021.
9. Гельгор А.Л., Павленко И.И., Горлов А.И., Фокин Г.А., Попов Е.А., Лаврухин В.А., Сиверс М.А. Первичная синхронизация с базовыми станциями LTE // Электромагнитные волны и электронные системы, 2014. – Т. 19. – № 7. – С. 54-62.
10. Van de Beek J.J., Sandell M., Borjesson P.O. ML estimation of time and frequency offset in OFDM systems // IEEE Transactions on Signal Processing, 1997. – V. 45. – № 7. – P. 1800-1805.
11. Shamaei K. Exploiting Cellular Signals for Navigation: 4G to 5G. University of California, Irvine, 2020.
12. 3GPP TS 36.331 V17.1.0 (2022-03) Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification (Release 17).
13. Wang Y.-P.E., Ramesh R. To bite or not to bite-a study of tail bits versus tail-biting // Proceedings of PIMRC '96 - 7th International Symposium on Personal, Indoor, and Mobile Communications, 1996. – V. 2. – P. 317-321.
14. 3GPP TS 36.211 V16.7.0 (2021-12). Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation (Release 17).
15. 3GPP TS 36.212 V17.1.0 (2022-03). Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and channel coding (Release 17).
16. Физический канал PCFICH. [Электронный ресурс]. URL: http://anisimoff.org/lte/physical/pcfich.html (Дата обращения 28.10.2022).
17. Agilent 89600 Vector Signal Analyzer. [Электронный ресурс]. URL: https://www.keysight.com/us/en/products/software/pathwave-test-software/89600-vsa-software.html (Дата обращения 11.11.2022).
18. USRP B210 (Board Only). Ettus Research. [Электронный ресурс]. URL: https://www.ettus.com/all-products/ub210-kit/ (Дата обращения 11.11.2022).

АНАЛИЗ ПРИНЦИПОВ РАБОТЫ ФУНКЦИОНАЛА MLB В СЕТЯХ LTE С ПОДДЕРЖКОЙ SON

М.Т. Аскеров, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, marat.askerov.2000@mail.ru.*

УДК 621.391.1

Аннотация. Из-за роста объемов мобильного трафика сети становятся все более сложными системами. Для обеспечения обслуживания всех пользователей и поддержания высокого качества обслуживания развертывается новая инфраструктура и разрабатываются более сложные протоколы. В этой ситуации операторы сталкиваются с ростом операционных и капитальных затрат. Самоорганизующиеся сети появляются как решение для сокращения этих расходов, а также для улучшения использования ресурсов.

Ключевые слова: *SON*; *MLB*; *LTE*; мобильные сети; *eNodeB*; 3*GPP*; алгоритм; *PRB*; *UE*.

ANALYSIS OF MLB FUNCTIONAL PRINCIPLES IN LTE NETWORKS WITH SON SUPPORT

Marat Askerov, *St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich.*

Annotation. Due to the growth of mobile traffic, networks are becoming more and more complex systems. To serve all users and maintain a high quality of service, new infrastructure is being deployed and more sophisticated protocols are being developed. In this situation, operators face rising operating and capital costs. Self-organizing networks are emerging as a solution to reduce these costs as well as improve resource utilization.

Keywords: *SON*; *MLB*; *LTE*; mobile networks; eNodeB; 3*GPP*; algorithm; *PRB*; *UE*.

Введение

В настоящее время актуальной является разработка отечественных решений как в части оборудования сетей *LTE*, так и в части программного обеспечения. В связи с этим важно провести анализ принципов функционирования существующих решений зарубежных вендоров и разработать соответствующие алгоритмы и методы, которые впоследствии могут быть реализованы отечественными производителями оборудования.

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

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

Самооптимизация сетей *SON* с помощью *MLB*

В данной статье рассматривается решение задачи самооптимизации сетей *SON* с помощью одной из ключевых функций этих сетей *Mobility Load Balancing* (*MLB*) – балансировка и перераспределение нагрузки между сотами, которая

позволяет автоматически перенаправлять трафик между сотами, чтобы уменьшить нагрузку на перегруженных сотах и улучшить производительность сети. *MLB* работает на основе анализа данных о состоянии сети и ее нагрузке, и на основе этого принимает решения о перенаправлении трафика между сотами. Это позволяет распределять нагрузку между сотами более равномерно и предотвращать перегрузку отдельных сот (рис. 1) [3].

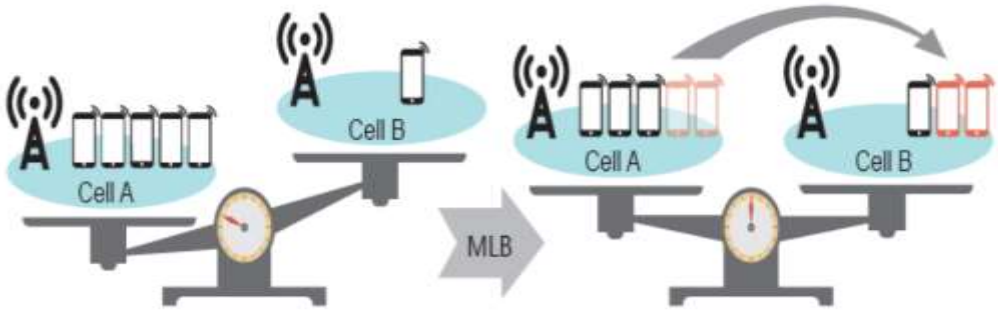

Рисунок 1

На рис. 2 представлен алгоритм балансировки и перераспределения нагрузки между сотами, реализуемый функцией *Mobility Load Balancing* в сетях *LTE* с поддержкой *SON*.

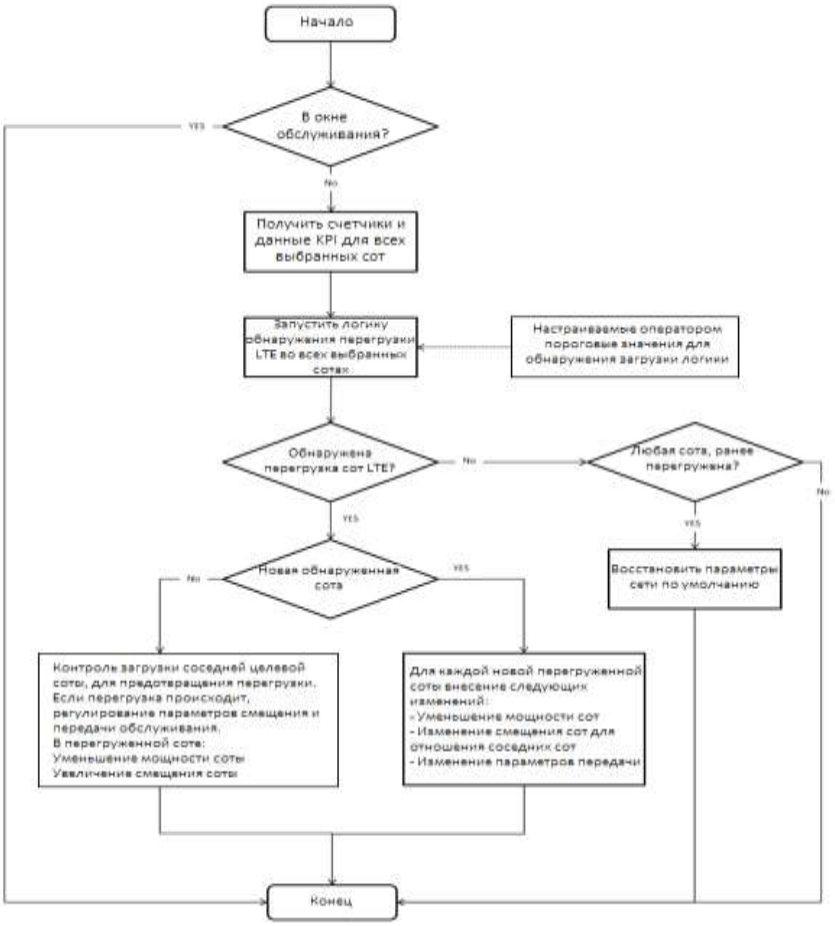

Рисунок 2

Целью применения *MLB* является повышение производительности сети и уменьшение числа неудовлетворенных пользователей. *MLB* включает отчеты о нагрузке между *eNodeB* для обмена информацией об уровне нагрузки и доступной емкости. Периодичность отчетов может быть установлена в диапазоне от 1 до 10 с. Отчет может содержать данные о нагрузке на оборудование, нагрузке на транспортную сеть *S*1 и состоянии радиоресурсов. Отчеты о состоянии радиоресурсов формируются отдельно для восходящего и нисходящего каналов и включают в себя общее распределение трафика с гарантированной и негарантированной скоростью передачи данных, процент выделенного блока физических ресурсов (*Physical Resource Block – PRB*) и процент *PRB*, доступных для балансировки нагрузки. Кроме того, механизмы *MLB* определяют условия дисбаланса нагрузок и работают вместе с планировщиком и контролем доступа. Для пользователей с негарантированной скоростью передачи данных (*non-GBR*) нет ограничений на минимальную производительность, которую получают эти пользователи, за исключением максимального количества пользователей на соту (управление доступом) и минимальной пропускной способности, установленной программным модулем *Schedular* (планировщик). Для пользователей *GBR* планировщик должен гарантировать, что всем однонаправленным радиоканалам предоставлены ресурсы, которые удовлетворяют их конкретной службе. Таким образом, система может считаться «сбалансированной», пока нет пользователей, которым было отказано в ресурсах, и все активные услуги поддерживаются в рамках их потребностей в *QoS*. Простые пороги могут быть реализованы, где условия низкой, средней и высокой нагрузки соответствуют заданному количеству активных пользователей в соте для случая *non-GBR*. Они могут служить триггерами для изменения параметров режима ожидания и/или для передачи обслуживания активных пользователей соседям (т.е., передача обслуживания внутри несущей на границе соты, совмещенная между несущими или совмещенная передача обслуживания между технологиями). Однако для пользователей *GBR* требуется более интеллектуальное измерение, поскольку небольшое количество таких пользователей может «загружать» соту в зависимости от своих требований.

Можно выделить два типа *MLB* [4]:

- *Intra-RAT MLB*, которая передает *UE* в соты *E-UTRAN*.
- *Inter-RAT MLB*, которая передает *UE* в соты других радиотехнологий.

В случае *Inter-RAT* для передачи информации через опорную сеть (*Core*) между базовыми станциями, использующими различные радиотехнологии, будет использоваться протокол управления информацией *RAN (RIM)* с отчетами о нагрузке. Значение класса пропускной способности соты, установленное системой *OAM*, будет использоваться для сравнения и взвешивания пропускной способности радиоинтерфейса различных технологий. В данном случае вся сеть может получить следующие преимущества:

- Снижение нагрузки на соты *E-UTRAN* за счет передачи соответствующих *UE* в соседние соты *inter-RAT*.
- Улучшенное использование ресурсов, увеличение общей емкости сот и улучшенный пользовательский интерфейс.

В случае *intra-rat MLB* достигаются такие преимущества, как:

- Устранение дисбаланса нагрузки между сотами для более эффективного использования ресурсов.

- Улучшение качества обслуживания и средней пропускной способности.
- Снижение риска перегрузки соты.

Существует несколько методов передачи нагрузки. В *MLB* абоненты могут передаваться посредством хэндоверов для *UE* в режиме подключения (*Connected Mode*) и реселекции соты для *UE* в режиме ожидания. С помощью хэндоверов *eNodeB* передает *UE* в определенные соты. Этот метод применим при наличии одной или нескольких целевых сот на соседней частоте *E-UTRA* для *MLB*. Рис. 3 иллюстрирует хэндоверы для *UE* в *Connected Mode*.

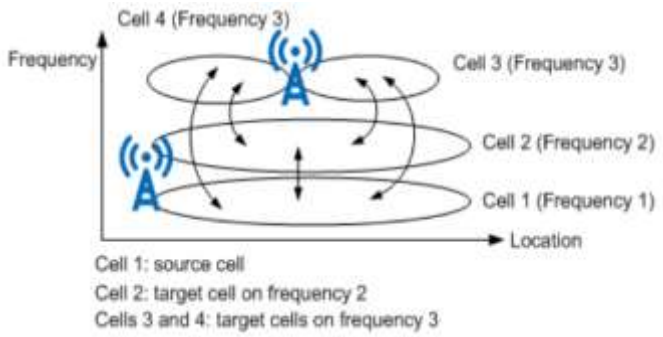

Рисунок 3

При повторном выборе соты *eNodeB* переводит *UE* на необслуживающие частоты. В этом процессе *eNodeB* устанавливает приоритеты повторного выбора соты для некоторых необслуживающих частот выше, чем обслуживающие частоты *UE*, используя сообщения *RRC Connection Release*. Повторный выбор соты применяется, когда только одна целевая сота работает на соседней частоте *E-UTRA*. Рис. 4 иллюстрирует сценарии повторного выбора соты для *UE* в режиме ожидания.

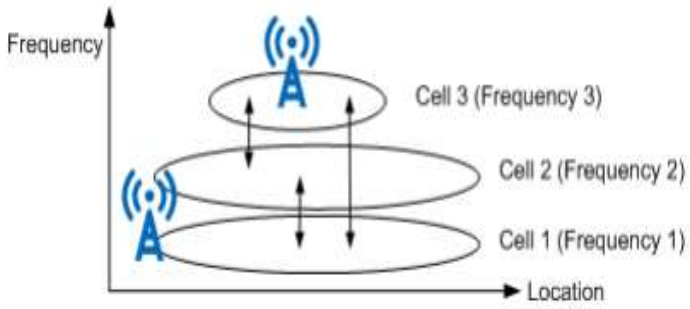

Рисунок 4

По сравнению с хэндоверами для *UE* в подключенном режиме, повторный выбор соты для *UE* в режиме ожидания не требует межчастотных измерений и накладных расходов на хэндовер и оказывает меньшее влияние на работу пользователя во время передачи [5].

Одним из основных способов достижения баланса нагрузки является перевод *UE* в режим ожидания и выравнивание нагрузки в режиме ожидания на основе количества пользователей. Ключевые параметры данного способа в реализации *Huawei* представлены в табл. 1 [6].

Таблица 1.

Имя параметра	*ID* параметра	Опция примечания к настройке
Переключатель алгоритма балансировки нагрузки	*CellAlgoSwitch.MLBAlgoSwitch*	*InterFreqMLBSwitch* Для включения *MLB* необходимо выбрать данную опцию
Режим триггера балансировки нагрузки мобильности	*CellMLB.MLBTriggerMode*	Установить для этого параметра значение *UE_NUMBER_ONLY*
Тип передачи *InterFreq MLB*	*CellMLB.InterFreqUETrsfType*	*IdleUE* Выбрать данную опцию
Усовершенствованный переключатель алгоритма *MLB*	*CellAlgoSwitch.EnhancedMLBAlgoSwitch*	Установить для этого параметра рекомендуемое значение: *ActiveUEBasedLoadEvalSw*
Пороговое значение номера *Inter-Freq idle MLB UE*	*CellMLB.InterFreqIdleMLBUENumThd*	Рекомендуется установить для этого параметра значение 1, если выбрана опция *ActiveUEBasedLoadEvalSw* параметра *CellAlgoSwitch.EnhancedMLBAlgoSwitch.* Если при настройке *MLB* выбрана опция передачи *UE* в режиме ожидания с синхронизацией по восходящей линии, установить для этого параметра значение, меньшее, чем значение параметра *CellMLB.InterFreqMLBUENumThd*
Период оценки межчастотной нагрузки	*CellMLB.InterFreqLoadEvalPrd*	Если для параметра *CellMLB.FreqSelectStrategy* задано значение *PRIORITYBASED* и в качестве целевых частот выбраны как соседняя частота *E-UTRA*, так и соседняя частота *UTRA*, необходимо, чтобы параметры *CellMLB.InterFreqLoadEvalPrd* и *CellMLB.InterRatLoadEvalPrd* были установлены на одно и то же значение
Индикатор настройки приоритета повторного выбора соты	*EutranInterNFreq.CellReselPriorityCfgInd*	Установить этот параметр на *CFG* для частот, участвующих в *MLB*
Приоритет повторного выбора соты	*EutranInterNFreq.CellReselPriority*	Установить этот параметр на основе плана сети
Поправочный коэффициент	*CellMLB.MLBIdleUENumAdjFactor*	Рекомендуемое значение находится в диапазоне от 5 до 10

Имя параметра	*ID* параметра	Опция примечания к настройке
номера *UE* в режиме ожидания *MLB*		
Переключатель статистической оптимизации *MU-MIMO PRB*	*CellMLB.MuMimoPrbStatOpt Switch*	Рекомендуется установить для этого параметра значение *ON* в сценариях *MU-MIMO*. При расчете спектральной эффективности соты общее количество *PRB,* используемых в соте, увеличивается только на единицу, если *PRB* используется несколькими *UE* одновременно

Ключевые параметры конфигурации модуля *MLB* в реализации *Nokia* представлены в табл. 2.

Таблица 2.

Имя параметра	Описание параметра	Значение по умолчанию/диапазон/ шаг
PRB threshold	Порог срабатывания для настройки занятости *PRB* в течение периода измерения	80 0...100 1
Buffer Delay QC1	Максимальное количество времени, в течение которого данные, запланированные для пользователя, могут задерживаться в *eNB*	30 10...100 10
Userdefined_L_RAC	Пороговое значение процентной доли блокировки из-за управления нагрузкой и доступом до активации балансировки нагрузки	5 0...100 1
Userdefined_Time_No_Res	Пороговое значение в процентах для блокировки из-за нехватки ресурсов *eNodeB* в течение периода измерения	5 0...100 1
HOHysteresis	Порог для увеличения частоты отказов НО между целевой и исходной сотой	10 0...100 1
SNRThreshold	Порог допустимого уровня помех для определенного процента всех измерений *SINR* перед уменьшением нагрузки на соту.	10 0...100 1
RedOffset	Значение, на которое может быть уменьшена величина смещения *CIO*	1 0...2 1
IncOffset	Значение, на которое может быть увеличена величина смещения *CIO*	1 0...2 1

Целью *Mobility Load Balancing* является разумное распределение пользовательского трафика по радиоресурсам системы по мере необходимости,

чтобы обеспечить качественное взаимодействие с конечным пользователем и производительность, одновременно оптимизируя пропускную способность системы. Кроме того, *MLB* может потребоваться для формирования нагрузки на систему в соответствии с политикой оператора или для «разгрузки» одной соты или несущей для достижения экономии энергии. Автоматизация этого минимизирует вмешательство человека в задачи управления сетью и оптимизации.

Данные, полученные в результате анализа принципов работы функционала *MLB*, позволяют разработать алгоритмы, которые могут быть использованы отечественными производителями при создании программного обеспечения для сетей мобильной связи *LTE*. Дальнейшие исследования в данном направлении будут посвящены разработке блока имитационной модели сети *LTE*, реализующего функционалы *SON*.

Литература

1. Maria Gonzalez. «Self-Organizing Networks», June, 2018. – pp. 3-9.
2. 3GPP TS 32.500 «Self-Organizing Networks (SON); Concepts and requirements».
3. Huawei technologies co., LTD, eRAN15.1 Draft B (2019-01-10), «Intra-RAT Mobility Load Balancing Feature Parameter Description». – pp. 11-12.
4. Huawei technologies co., LTD, eRAN15.1 Draft A (2019-01-05), «Inter-RAT Mobility Load Balancing Feature Parameter Description». – pp. 5-6.
5. Huawei technologies co., LTD, eRAN15.1 Draft B (2019-01-10), «Intra-RAT Mobility Load Balancing Feature Parameter Description». – pp. 13-14.
6. Huawei technologies co., LTD, eRAN15.1 Draft B (2019-01-10), «Intra-RAT Mobility Load Balancing Feature Parameter Description». – pp. 30-33.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СЕТИ

СТАНДАРТИЗАЦИЯ БЛОКЧЕЙНА В ИНТЕЛЛЕКТУАЛЬНЫХ СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ В УМНЫХ ГОРОДАХ

Е.В. Сюндюкова, *Нижегородский государственный университет им. Н.И. Лобачевского, sundukova234k@gmail.com.*

УДК 004.75:004.08:332.024

Аннотация. Стандартизация в приложениях умного города ограничена конкурентным давлением, связанным с запатентованными инновациями и разделением технологий. Совместимость между сетями, базами данных и программными интерфейсами приложений имеет важное значение для достижения интеллектуальных целей городской среды, поддерживаемой технологиями. В данной статье анализируются проблемы, с которыми сталкиваются умные города, а также использование блокчейна в приложениях интернета вещей. Чтобы решить эти проблемы, в исследовании предлагается рабочая модель бесконечного цикла для создания стандартизированного промежуточного облачного блокчейна для сетей интернета вещей в умных городах. Посредническая функция блокчейна устранит критические пробелы в существующих стандартах умных городов на основе распределенного интернета вещей, устанавливая соединения между узлами, пользователями и поставщиками услуг, которые становятся возможными благодаря автономным, неизменяемым и не подлежащим проверке транзакциям.

Ключевые слова: умный город; интернет вещей; *IoT*; блокчейн; сеть.

STANDARDIZATION OF BLOCKCHAIN IN SMART NETWORKS OF THE INTERNET OF THINGS IN SMART CITIES

E.V. Syundyukova, *Nizhny Novgorod State University N.I. Lobachevsky.*

Annotation. Standardization in smart city applications is limited by the competitive pressures associated with patented innovations and technology separation. Interoperability between networks, databases, and application programming interfaces is essential to achieve the intelligent goals of an urban environment supported by technology. The problems faced by smart cities, as well as the use of blockchain in Internet of Things applications, are analyzed in this article. To solve these problems, the study proposes a working model of an infinite cycle to create a standardized intermediate cloud blockchain for the Internet of Things networks in smart cities. The intermediary function of the blockchain will eliminate critical gaps in the existing standards of smart cities based on the distributed Internet of Things, establishing connections between nodes, users and service providers, which are made possible by autonomous, immutable and non-verifiable transactions.

Keywords: smart city; internet of things; *IoT*; blockchain; network.

Введение

Создание гибкой, адаптируемой и насыщенной информацией среды умного города требует сетевых взаимосвязей. Итеративные прорывы в области пересечения статических и динамических ресурсов произведут революцию в расширении технологических возможностей выбора в сетевой городской среде,

обеспечивая интеллектуальные транзакции с учетом поведения и данных [1]. Несмотря на эти преимущества, конкурентный стимул к разделенным технологическим инновациям может привести к структурному расколу в экосистеме умного города, поскольку проприетарные модули, сети и алгоритмы ограничивают совместимость интеллектуальных узлов и сетевой обмен информацией [2]. Совместимость, определенная *IEEE* 2030.5 управляющего фонда экосистем (*Ecosystem steering committee, ESC*) – это «качество информационных и коммуникационных технологических интерфейсов, которое позволяет двум или более устройствам, или системам устанавливать соединение и успешно взаимодействовать» [3]. Совместимость между сетями, базами данных и программными интерфейсами приложений (*Application programming interface, API*) имеет решающее значение для реализации интеллектуальных целей городской среды с поддержкой технологий. Интернет вещей (*Internet of things, IoT*) реализует всеобъемлющую технологическую цель интегрированной многоузловой связи по разрозненным сетям в умных городах и с помощью маломощных и многофункциональных устройств [4].

Поскольку различные устройства собирают данные об использовании, поведении пользователей и окружающей среде, способность добывать и интерпретировать эти ресурсы данных ограничена из-за отсутствия взаимодействия между проприетарными платформами [5]. С экономической точки зрения, *IoT* – это эффективный источник прибыли, который постоянно развивается и растет [6]. Концепция умных городов значительно расширилась, учитывая сложные задачи, направленные на улучшение качества жизни граждан (*Quality of life, QoL*) и качества обслуживания (*Quality of service QoS*). В докладе Организации объединенных наций (ООН) упоминается, что более половины населения проживает в городских районах, и к 2050 г. ожидается дополнительный рост на 2,5 млрд человек [7]. Эта возросшая урбанизация существенно повлияла на условия жизни из-за увеличения пробок на дорогах, выбросов парниковых газов, углекислого газа и утилизации отходов [8].

Некоторые города признаются умными на основе своих инновационных приложений и определенных характеристик, включая цифровую интеграцию, широкополосную связь и высококвалифицированную рабочую силу. Примеры решений умных городов можно найти по всему миру. Например, технология *Tangle* в Германии используется для автоматизированной транспортной системы [9]. В Амстердаме применение интернета вещей улучшило энергосбережение, способствовало сокращению трафика и повышению уровня безопасности, а в Барселоне сенсорная технология используется для оценки транспортного потока при проектировании новой автобусной сети [10]. Более того, в Корее наряду с автоматизированным строительством используется интеллектуальная система уличного освещения [11], аналогичная Японии, Нидерландам и Англии [12-13].

Технология блокчейн (*Blockchain, BC*) или технология распределенного реестра (*Distributed ledger technology, DLT*) изменит образ жизни людей, поскольку она позволяет осуществлять децентрализованные, безопасные, сохраняющие конфиденциальность и прозрачные транзакции, повышая доверие к приложениям умных городов и, следовательно, ускоряя их внедрение и использование гражданами [14]. Ранее база данных и сети контролировались посредником, однако в *BC* каждый участник вносит свой вклад в сеть и обладает элементами управления. Применение *BC* в умных городах имеет потенциал широкого распространения благодаря его децентрализованному характеру и потенциалу автоматизации [15].

Цель исследования

Совместимость технологий умного города ограничивается корпоративными коммерческими целями, следовательно, для облегчения технологической совместимости необходимо объединяющее решение, которое соединяет узлы интернета вещей по всей городской структуре. Цель данного исследования – критически проанализировать текущий уровень прогресса в решениях для умных городов на основе интернета вещей и обеспечить основу для интеграции блокчейна в приложения для умных городов на основе интернета вещей.

Интернет вещей и умные города

Обычно интернет вещей определяется как широкая система взаимосвязанных вычислительных устройств, которые могут собирать и передавать данные по беспроводной сети без участия человека, обладающая ограниченными возможностями хранения и обработки данных. Целью интеграции интернета вещей в умных городах является повышение производительности, надежности и безопасности инфраструктуры [16]. На рис. 1 показана традиционная сетевая архитектура центров обработки данных.

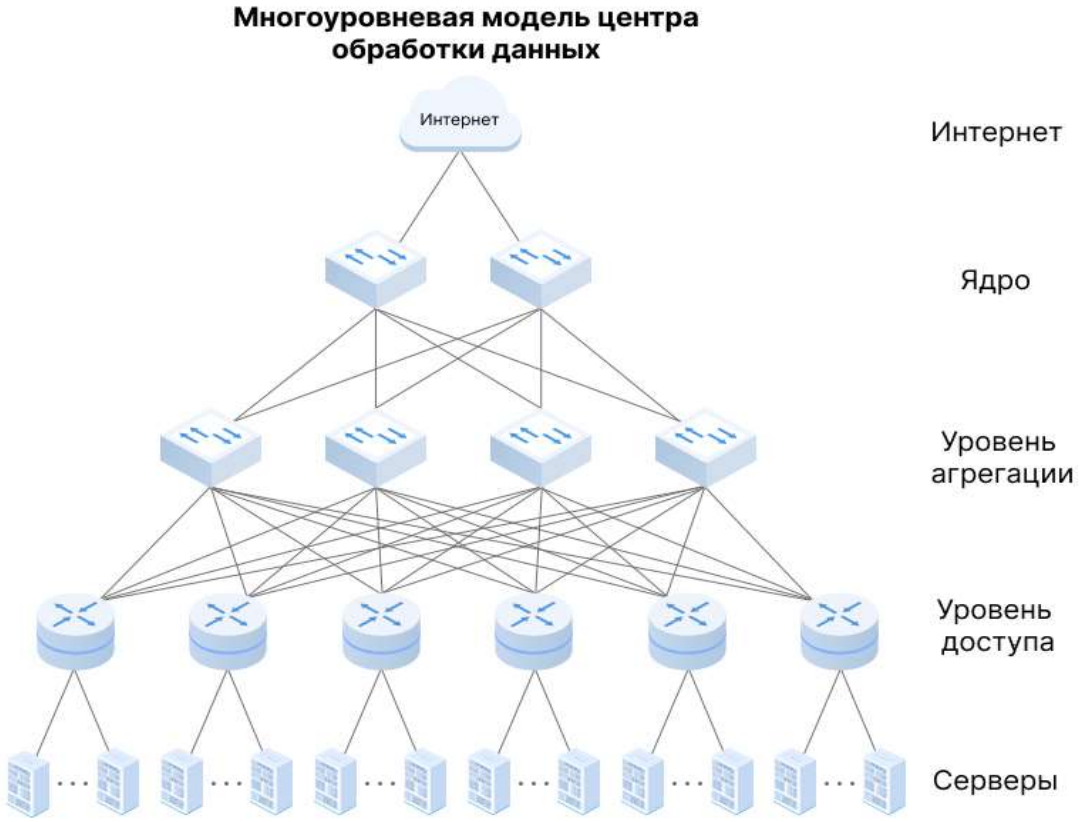

Рисунок 1

При наличии устройств, подключенных к интернету, информация обнаруживается и собирается. *IoT* также распределяет данные через интернет-коммуникационную сеть на различные устройства. Глобальные системы позиционирования, устройства радиочастотной идентификации, камеры и датчики – примеры этих устройств. С точки зрения возможностей работы в сети и ограничений устройств сетевой уровень отвечает за перемещение данных. Для передачи информации от устройства восприятия к ближайшему с помощью шлюза,

который использует коммуникационные возможности, оно интегрируется в комбинацию нескольких сетей ближнего действия, таких как *ZigBee* и *Bluetooth*. *Wi-Fi, 4G* и связь по линии электропередачи используются для передачи данных в более далеком диапазоне [17].

Блокчейн и экосистемы умных городов

Поведение людей, технические узлы и институциональное администрирование – все это интегрировано в единую сервисную архитектуру, как показано на рис. 2, в качестве основного элемента экосистемы умного города. Чтобы соответствовать требованиям системы к предоставлению услуг, эта модель определяет шесть ключевых аспектов эффективного управления данными *BC*: автоматический сбор данных, безопасность данных, распределенность данных, прозрачность и конфиденциальность, надежность, а также демократизированность [18]. На рис. 2 показаны особенности управления и вычислений сервисов совместного использования на основе блокчейна.

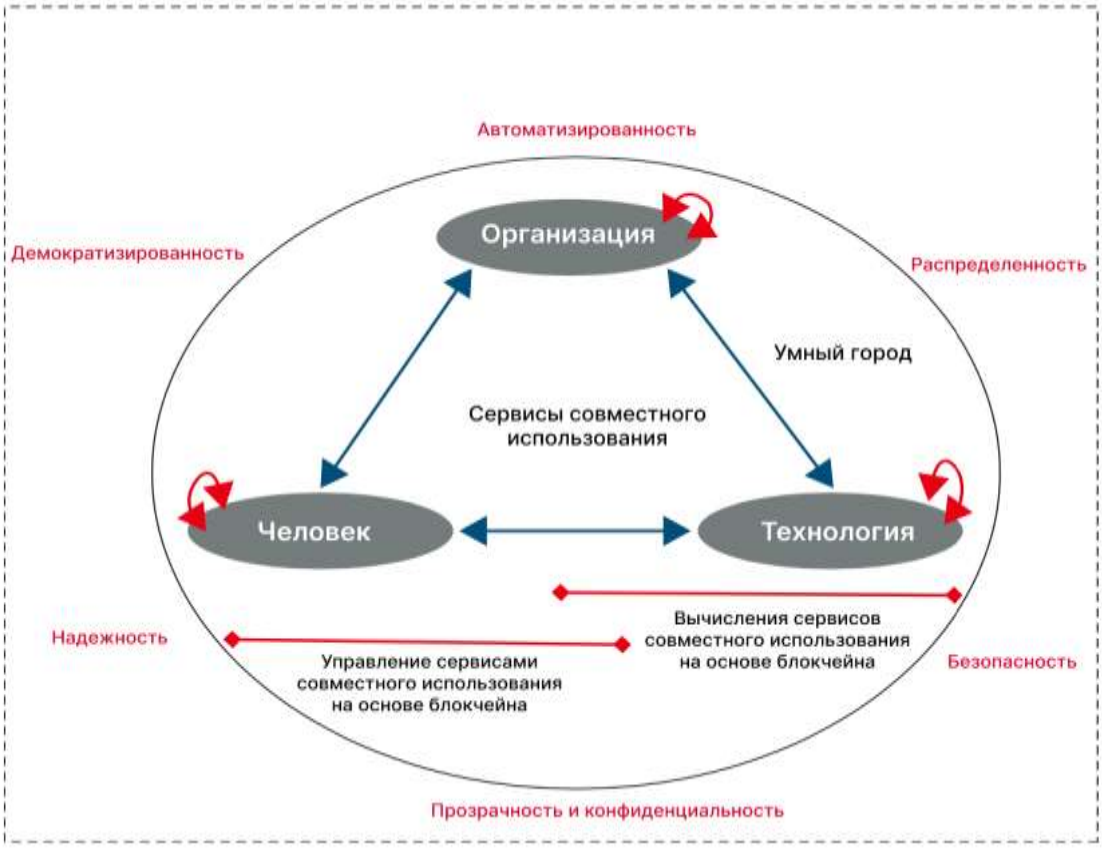

Рисунок 2

В Бруклине была построена энергетическая сеть на основе блокчейна, позволяющая домохозяйствам с солнечными панелями отслеживать выработку и потребление энергии, упрощая подсчет системных кредитов и дебетов. В то же время, аналогичные решения были предложены для других возможностей выставления счетов на уровне обслуживания, таких как здравоохранение. Данная реализация децентрализованной системы взимания платы без посредников в конечном итоге обеспечит эффективность, необходимую для минимизации сетевых затрат [19]. Путем агрегирования данных о расходах на здравоохранение

страховые компании и поставщики услуг смогут взаимодействовать с данными клиентов, отслеживая спрос и предлагая скидки в зависимости от состояния здоровья, эффективности платежей и вовлеченности в сеть (например, при посещении своего поставщика первичной медицинской помощи). Именно объединение служб управления данными с помощью централизованных облачных решений с маршрутизацией по сети обеспечивает бесшовную интеграцию, поскольку потребители добавляют дополнительные уровни технологий и информационных ресурсов к своим сетевым подключениям.

В Европейском союзе проект *DECODE* был разработан в сотрудничестве с региональными правительствами в крупных городских центрах, таких как Барселона, Каталония и Амстердам, чтобы позволить потребителям не только получать доступ к данным, собранным с помощью интернета вещей, но и осуществлять контроль над тем, как эти данные передаются сторонним организациям и поставщики услуг [20]. Потребители получают доступ к сетевым данным с помощью решения *DECODE*, подтверждая свою личность онлайн, что позволяет им напрямую взаимодействовать с программными решениями для управления идентификацией, оплаты и ведения записей. Для потребителей средства контроля конфиденциальности и мониторинга не только обеспечили бы защиту, но и побудили бы предприятия устанавливать более прозрачные стандарты управления информацией в ответ на запросы потребителей и промышленности.

Интегрированный стандарт *BC* для умных городов на основе интернета вещей

Из-за масштаба технологии интернета вещей, ограниченной вычислительной мощности отдельных узлов и уязвимости сетевых подключений крайне важно, чтобы любое координирующее решение касалось уникальных проблем масштабируемости и безопасности интернета вещей. Являясь «узлом с ограниченным доступом», каждое аппаратное устройство интернета вещей обладает недостаточными вычислительными и коммуникационными возможностями, что ограничивает его способность эффективно обеспечивать защиту и мониторинг от нарушений безопасности и незаконной деятельности. В то время как решения *BC* способны облегчить нагрузку на аутентификацию *IoT*, требуется постепенно уменьшать размер выполняемого программного кода, меняя структуру сети подключения с помощью распределенного решения, которое включает в себя как полные (транзакционные), так и легкие (добавляющие) узлы. Эта сетевая конструкция, основанная на протоколе периферийных вычислений, зависит от того, что называют централизованной распределительной сетью и удаленными сайдчейн-сетями, которые соединяют устройства интернета вещей с промежуточными нотариальными узлами в *BC*.

Архитектура проверки перекрестных транзакций, которая является производной от центральной концептуальной основы сети *Helium* и *Tangle* [21], обеспечивает параллельный консенсус и аутентификацию, подтвержденную транзакцией, гарантируя при этом отсутствие конфликта между текущей и любыми предыдущими транзакциями. Технологии *BC* были созданы как децентрализованный ответ на присущую системам онлайн-транзакций уязвимость к нарушениям безопасности. В результате решение проблем безопасности, доверия и интеграции, связанных с проприетарной сетевой архитектурой в инновациях умного города, заключается в построении *BC* как функциональной, стандартизированной промежуточной базы данных.

Как видно из рис. 3, решение представляет собой интегрированную структуру для технологии *BC* в контексте умных городов на основе интернета вещей. Идея централизует процесс передачи данных в однородном, доступном по сети облаке, где владельцы данных и потребители могут предоставлять или ограничивать доступ к своим данным. Как регистр транзакций, *BC* действует как центральное хранилище данных, отслеживая приток и отток пользовательских данных. Хотя опасения по поводу анонимности и мониторинга пользователей реальны, система *BC sensing* позволит избежать необходимости централизованной аутентификации, предоставляя наборы данных с ограниченным доступом и целенаправленным мониторингом для конкретных пользователей. Система требует наличия договорного соглашения между пользователем и программным узлом с поддержкой интернета вещей, который реализуется с помощью прозрачных и адаптивных контрактов конфиденциальности, встроенных в блокчейн-решение. В результате предлагаемая архитектура обеспечивает центральную базу данных *BC* в качестве базового агента для получения и распространения информации о поведении пользователя. *API*-интерфейсы и проприетарное программное обеспечение соединяют периферию базы данных, направляя пользовательские данные через интегрированную экосистему аппаратных узлов. Аутентификация *BC* обеспечивает надежность хранения пользовательской информации и сохранение данных путем цифровой проверки пользовательских соглашений и контрактов с использованием универсального языкового стандарта. Предложения по интеграции, основанные на этой уникальной парадигме, включают интеграцию отслеживания перемещений на основе *GPS*, например, между домом, автомобилем пользователя и его местом работы, тем самым создавая механизм трехточечной оценки для прогнозирования эффективности и быстродействия системы. На рис. 3 показана высокоуровневая модель интеграции блокчейна в рамках умного города на базе интернета вещей.

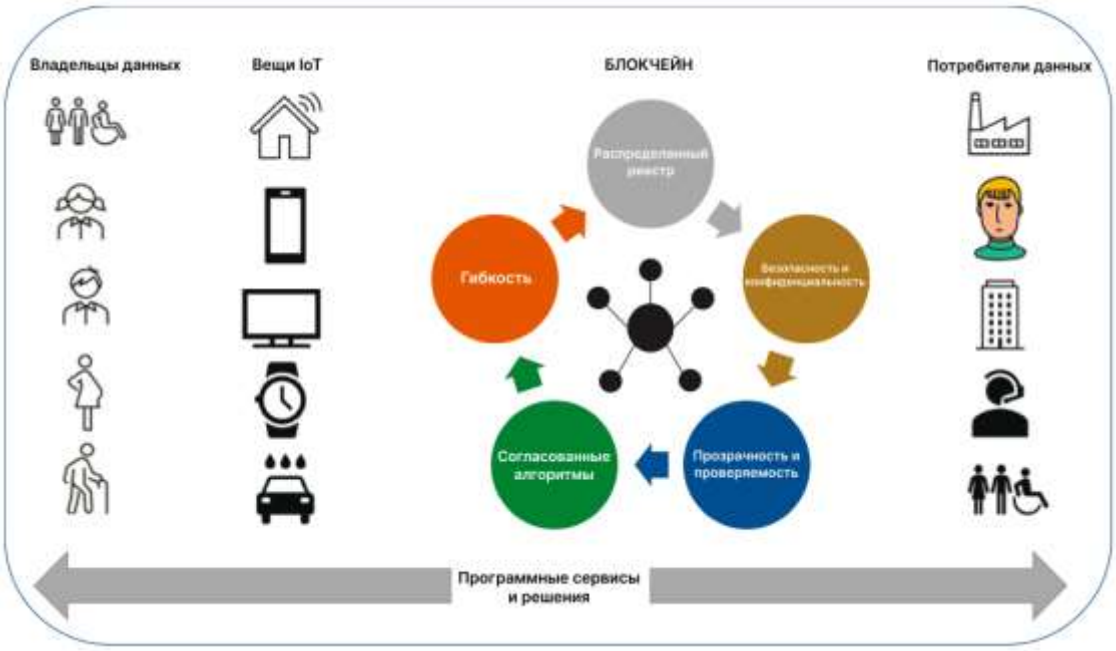

Рисунок 3

Прототип на рис. 4 иллюстрирует предлагаемое сервисное решение *BC*, которое поддерживает совместимость как с открытым исходным кодом, так и с

проприетарным программным обеспечением для пользовательских интерфейсов и *API*, объединяя операции по управлению данными в централизованный реестр. Таким образом, вещи *IoT* будут работать в рамках своего собственного программного обеспечения, но будут инициировать обмен данными в соответствии с протоколом совместного использования, заполняя блокчейн необходимыми наборами данных. Несмотря на то, что это зависит от способа транзакции, который тестируется и исследуется на практике, решение *BC*, основанное на установленном стандарте обмена, таком как *Ethereum*, обеспечивает основу бесконечного цикла для интеграции на основе консорциума *IoT*. На рис. 4 представлено применение интеграции блокчейна в рамках умного города на базе интернета вещей.

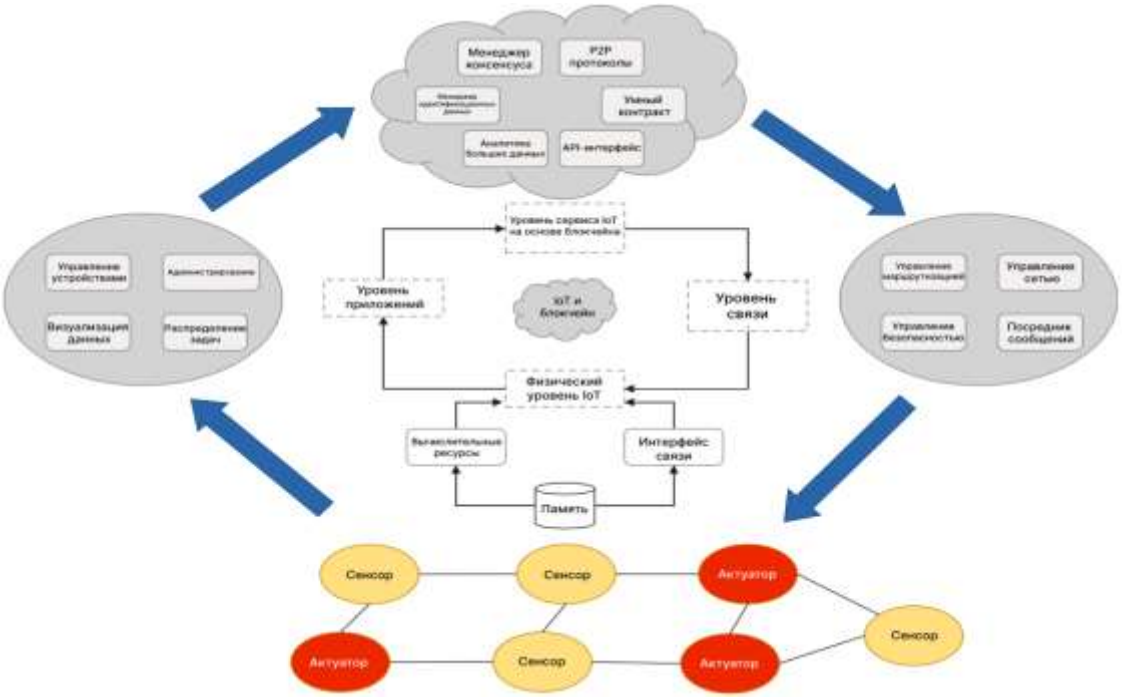

Рисунок 4

Заключение

В данной статье кратко излагаются концептуальные основы решений для умных городов, интеграции интернета вещей и администрирования баз данных с использованием технологии блокчейн. Более насущным требованием является децентрализованный, широкодоступный стандарт проверки безопасности и аутентификации. Исследование, приведенное в статье, продемонстрировало преимущества *BC*, выступающего в качестве стандартной концепции подтверждения работоспособности для легитимизации информационных потоков внутри сети. Исследование также подтвердило, что для того, чтобы решения для умных городов на основе интернета вещей вышли за рамки своих системных ограничений, существует настоятельная необходимость в пересмотренном стандарте практики, который существует за пределами существующего частного состояния систем управления данными, ограниченных разработчиками [22-23].

Литература

1. Gupta A., Christie R. Manjula R. Scalability in the Internet of Things: features, techniques and research challenges. International Journal of Computational Intelligence Research. – Vol. 13. – No. 7. – pp. 1617-1627.

2. Silva B.N., Khan M. Han K. Towards sustainable smart cities: a review of trends, architectures, components, and open challenges in smart cities. Sustainable Cities and Society, 2018. – Vol. 3. – pp. 697-713.
3. Lingjun F., Gil-Garcia J.R., Werthmuller D., Burke G.B. Hong X.F. Investigating blockchain as a data management tool for IoT devices in smart city initiatives, in Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age. – pp. 1-2, Delft, The Netherlands, May 2018.
4. Fraga-Lamas P., Ferna´ndez-Carame´s T., Sua´rez-Albela M., Castedo L., Gonza´lez-Lo´pez M. A review on internet of things for defense and public safety. Sensors, 2016. – vol. 16. – no. 10. – pp. 1644.
5. Hancke G., Silva B. Hancke Jr. G. The role of advanced sensing in smart cities, Sensors, 2013. – vol. 13. – pp. 393-425.
6. Muhammad M.F., Anjum W. Mazhar K.S. A critical analysis on the security concerns of internet of things (IoT), International Journal of Computer Application, 2015. – vol. 111. – pp. 1-6.
7. Finch K., Tene O. Smart cities: privacy, transparency, and community». The Cambridge Handbook of Consumer Privacy. Cambridge University Press, 2018. – p. 125.
8. Намиот Д.Е. Базы данных временных рядов в системах «Интернета вещей». – М.: Синергия, 2017. – 399 с.
9. Traffic T.A. and IOS. The best app selection for Barcelona, Apps4bcn, all the Apps You Need for Barcelona, Available [Online]: http://apps4bcn.cat/en/apps/index/Category:trans port-i-tr-nsit
10. City S., Premsa S. El web de la Ciutat de Barcelona Available [Online]: http://ajuntament.barcelona.cat/premsa/ tag/smart-city/
11. Strickland E. Cisco bets on South Korean smart city, IEEE Spectrum, 2011. – vol. 48. – pp. 11-12.
12. Hancke G., Silva B. and Hancke Jr. G. The role of advanced sensing in smart cities, sensors, 2013. – vol. 13. – pp. 393-425.
13. Bakıcı T., Almirall E. and Wareham J. A smart city initiative: the case of Barcelona, ISSN, 2013. – vol. 4. – pp. 135-148.
14. Ismail L., Materwala H. Article A review of blockchain architecture and consensus protocols: use cases, challenges, and solutions, symmetry, 2019. – vol. 11. – no. 10. – p. 1198.
15. Kitchin R. Getting Smarter about Smart Cities: Improving Data Privacy and Data Security, Department of the Taoiseach, Ireland, 2016, https://www.researchgate.net/publication/
293755608_Getting_smarter_about_smart_cities_
Improving_data_privacy_and_data_security
16. Грингард Сэмюэл. Интернет вещей: Будущее уже здесь. – М.: Альпина Диджитал, 2015. – 426 с.
17. Lee J.-H., Singh K.D., Hadjadj-Aoul Y., Kumar N. Wireless and mobile technologies for the internet of things, mobile Information Systems, 2016. – vol. 2016, – pp. 1-2. Article ID 8206548.
18. Sun J., Yan J., Zhang K.Z. Blockchain-based sharing services: what blockchain technology can contribute to smart cities, Financial Innovation, 2016. – vol. 2. – pp. 1-9.
19. Kundu D. Blockchain and trust in a smart city, environ- ment and Urbanization ASIA, 2019. – vol. 10. – no. 1. – pp. 31-43.
20. Townsend A.M. Smart Cities: Big Data, Civic Hackers, and the Quest for a New utopia, WW Norton & Company, New York, NY, USA, 2013.

21. Как обезопасить Интернет вещей [Электронный ресурс]. URL: http://rusbase.com/story/IoT-security/ (10.02.2023).
22. Проблемы и перспективы Интернета вещей [Электронный ресурс]. URL: http://rusbase.com/opinion/russian-iot/ (10.02.2023).
23. Бренев А. Компоненты для систем EnOcean // Беспроводные технологии, 2014. – № 1. – С. 3-34.

ВЫЯВЛЕНИЕ НЕДОСТАТКОВ НЕКОТОРЫХ РЕШЕНИЙ CLOUD-BASED VIRTUAL LABS

***Д.Б. Горошков**, Московский технический университет связи и информатики, zet.6@yandex.ru.*

УДК 004.75

Аннотация. Решения дистанционного формата обучения на базе облачных технологий последнее время стали активно развиваться, в частности после пандемии *COVID*-19. Подобные решения в будущем позволят увеличить доступность образования для большего количества людей, а также улучшить эффективность и гибкость процесса. В данной статье выявляются основные недостатки пяти решений *Cloud-based virtual labs*, таких как *Cloud-based virtual labs*, таких как *Cisco NetSpace, AWS Educate, Google Cloud Platform Education* (*GCPE*), *Microsoft Azure for Students, Open edX*. Помимо этого, приведено краткое описание этих решений и раскрыто какие возможности они предоставляют.

Ключевые слова: студент; платформа; обучение; ресурс; доступ; инструмент; недостаток; возможность; преподаватель; технология.

IDENTIFICATION OF FAULTS IN SOME CLOUD-BASED VIRTUAL LABS SOLUTIONS

***D.B. Goroshkov,** Moscow Technical University of Communications and Informatics.*

Annotation. Distance learning solutions based on cloud technologies have recently begun to develop rapidly, in particular after the *COVID*-19 pandemic. Such decisions in the future may make it possible to increase the accessibility of education to more people, as well as improve the efficiency and flexibility of the process. This article identifies the main disadvantages of 5 Cloud-based virtual labs solutions such as Cloud-based virtual labs such as Cisco NetSpace, *AWS* Educate, Google Cloud Platform Education (GCPE), Microsoft Azure for Students, Open edX. In addition, a brief description of these solutions and what features they provide is given.

Keywords: student; platform; learning; resource; access; tool; disadvantage; opportunity; teacher; technology.

Введение

Решения дистанционного формата обучения на базе облачных технологий могут включать в себя использование облачных платформ для хранения и доступа к курсам, видеоконференций для онлайн-лекций и взаимодействия студент-преподаватель, а также инструменты для онлайн-обучения, такие как тестирование и обратная связь.

Облачные технологии позволят студентам получить доступ к курсам и материалам обучения из любого места и в любое время, что делает дистанционное обучение более гибким и доступным. Также они позволяют учителям и администраторам отслеживать прогресс студентов и контролировать их успеваемость в реальном времени. В целом, облачные технологии способствуют более эффективному и удобному для всех участников процесса дистанционному обучению [1-3].

Существует множество решений, но в данной статье предлагается рассмотреть инструменты *Cloud-based virtual labs* [4, 5].

Cloud-based virtual labs – это инструменты, которые позволяют студентам воспроизводить эксперименты и практические задания в виртуальной среде, избегая необходимости в оборудовании и материалах.

Cisco NetSpace является онлайн-платформой, которая предоставляет студентам доступ к сетевой инфраструктуре и оборудованию *Cisco* для обучения и тестирования. Это позволяет студентам получить практический опыт в работе с реальным оборудованием *Cisco* и обучаться в соответствии с настоящими индустриальными стандартами. Платформа также может использоваться для проведения сетевых экзаменов и оценки студентов.

Cisco NetSpace предоставляет доступ к реальному оборудованию *Cisco*, включая роутеры, сетевые коммутаторы и коммутаторы, которые настраивают и конфигурируют в режиме реального времени. Это позволяет студентам получить практический опыт в работе с сетевым оборудованием и развить навыки, которые они могут использовать в будущем в своей карьере.

Платформа также включает в себя курсы и учебные материалы, разработанные экспертами *Cisco*, помогающие студентам понять и применять концепции и технологии сетевой инфраструктуры. Это дает студентам возможность изучать в своем темпе и получать обратную связь от инструкторов и других студентов [6-8]. На рис. 1 представлена онлайн-платформа *Cisco NetSpace* [8].

Рисунок 1

Один из недостатков данной платформы является ограниченный доступ к ней, в зависимости от того, где вы находитесь и какой у вас есть доступ к интернету.

Это может затруднить обучение или тестирование для некоторых студентов. Другой недостаток – ограниченное количество доступного оборудования или виртуальных лабораторий, что может затруднить получение достаточного практического опыта для некоторых студентов. Также к недостаткам относится и то, что не все курсы и учебные материалы доступны на разных языках, что может создать трудности для студентов, которые не владеют английским языком.

В целом, *Cisco NetSpace* является полезной платформой для обучения и тестирования в области сетевых технологий, но есть некоторые ограничения, затрудняющие доступ или обучение для некоторых студентов. Это важно принимать во внимание при использовании платформы и изучении на ней.

AWS Educate – это программа образования, которая предлагает студентам и преподавателям доступ к ресурсам *Amazon Web Services* (*AWS*) для обучения и исследования. Она имеет бесплатный доступ к вычислительным ресурсам, базам данных, хранилищу, инструментам для разработки и другим сервисам *AWS*.

Программа предоставляет студентам возможность получить практический опыт с реальными технологиями и инструментами, используемыми в промышленности, а также изучить современные методы и практики разработки и администрирования приложений в облачной среде.

Преподаватели могут использовать платформу *AWS Educate* для создания лабораторных работ и курсов, и для оценки студентов. Программа также предлагает специализированные курсы и материалы для обучения, которые помогут студентам и преподавателям лучше понимать и использовать ресурсы *AWS*.

Кроме того, *AWS Educate* предлагает студентам возможность зарабатывать денежные бонусы, которые можно использовать для оплаты ресурсов *AWS*, и стипендии, чтобы помочь студентам продолжить их образование и исследования [9-11]. На рис. 2 представлена программа образования *AWS Educate* [11].

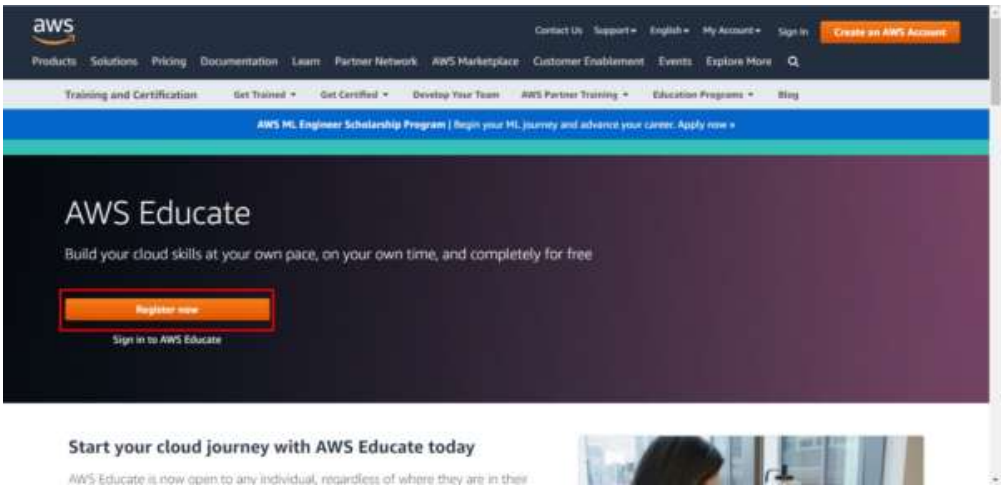

Рисунок 2

Но, как и любой другой онлайн сервис, использование *AWS Educate* имеет некоторые недостатки. Одним из них является возможность возникновения дополнительных затрат на ресурсы, если студенты или преподаватели используют больше выделенных им бесплатных ресурсов. Кроме того, не все курсы и учебные материалы доступны на разных языках, что создает трудности для студентов, которые не владеют английским языком. Также, некоторые студенты или

преподаватели могут иметь ограниченное понимание облачных технологий и испытывают трудности при использовании *AWS Educate.* Но с течением времени и изучением ресурсов программы и практики их использования, эти недостатки становятся устранимыми.

Google Cloud Platform Education (GCPE) – это программа образования, которая предлагает студентам и преподавателям доступ к ресурсам *Google Cloud Platform (GCP)* для обучения и исследования. Она включает в себя бесплатный доступ к вычислительным ресурсам, базам данных, хранилищу, инструментам для разработки и другим сервисам *GCP.*

Программа предоставляет студентам возможность получить практический опыт с инновационными технологиями и инструментами, используемыми в промышленности, и изучить современные методы и практики разработки и администрирования приложений в облачной среде.

Преподаватели могут использовать *GCPE* для создания лабораторных работ и курсов, а также для оценки студентов. Платформа, кроме того, предлагает специализированные курсы и материалы для обучения, которые помогут студентам и преподавателям лучше понимать и использовать ресурсы *GCP* [12-16]. На рис. 3 представлена программа образования *Google Cloud Platform Education.*

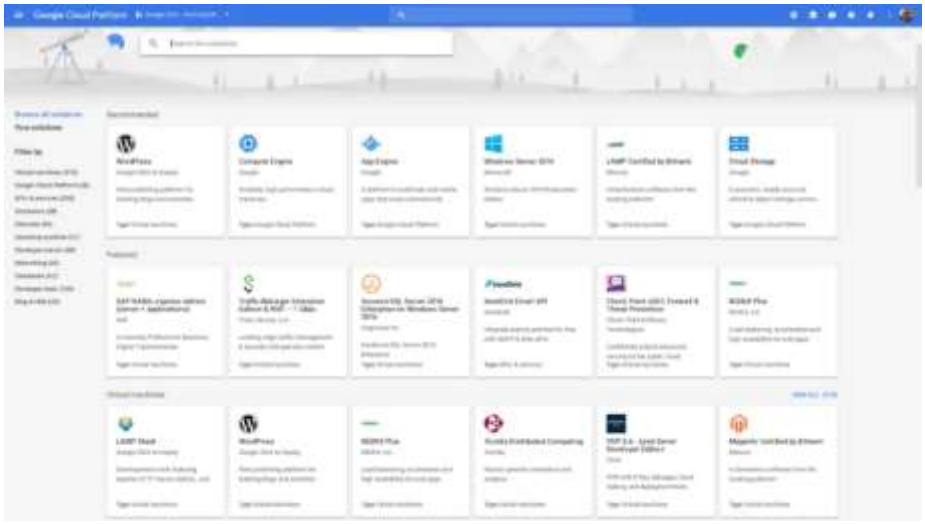

Рисунок 3

GCPE также имеет некоторые недостатки. Одним из них является возможность возникновения дополнительных затрат на ресурсы, если студенты или преподаватели используют больше выделенных им бесплатных ресурсов. Еще одним может быть то, что не все курсы и учебные материалы доступны на разных языках, что может создать трудности для студентов, которые не владеют английским языком.

Microsoft Azure for Students – это программа, которая предлагает студентам бесплатный доступ к ресурсам *Microsoft Azure* для обучения и исследования. С помощью *Microsoft Azure for Students* студенты могут изучать и практиковать современные технологии и инструменты, используемые в промышленности, в том числе машинное обучение, аналитику, интернет вещей, мобильное разработку и многое другое.

Преподаватели также могут использовать *Microsoft Azure for Students* для создания лабораторных работ, курсов и для оценки студентов. Но, как и любой

другой сервис, *Microsoft Azure for Students* имеет недостатки, включая возможность возникновения дополнительных затрат на ресурсы при использовании больше, чем выделенный бесплатный кредит и недоступность некоторых курсов и материалов на разных языках. В тоже время, студенты и преподаватели могут испытывать трудности с пониманием и использованием всех функций и инструментов, которые предлагает *Microsoft Azure* [17-20]. На рис. 4 представлена программа для обучения и исследования *Microsoft Azure for Students* [20].

Рисунок 4

Одних из недостатков *Microsoft Azure for Students:*

1) Недоступность некоторых курсов и материалов на разных языках, что создает трудности для студентов, которые не владеют английским языком.

2) Трудности с пониманием и использованием всех функций и инструментов, которые предлагает *Microsoft Azure*.

3) Возможность испытывать трудности с настройкой и конфигурированием сервисов и инструментов *Azure*.

Open edX – это открытая платформа для онлайн-образования, которая используется для создания и размещения курсов онлайн. Платформа основана на технологии Мозаика *LMS* и предоставляет инструменты для создания и управления курсами, а также для отслеживания и оценки успеваемости студентов.

С помощью *Open edX* можно создавать и размещать курсы в различных форматах, включая видео, аудио, текстовые и изображения, а также добавлять тесты, задания и другие элементы для оценки успеваемости. Платформа поддерживает функцию онлайн общения, которая позволяет студентам общаться и взаимодействовать между собой.

Open edX используется множеством организаций, включая известные университеты, компании и некоммерческие организации, для организации онлайн-образования. Она позволяет им создавать курсы на открытом исходном коде и использовать их бесплатно, а также дает возможность студентам изучать курсы бесплатно. Это делает *Open edX* популярной платформой для доступного и качественного онлайн-образования [21-23]. На рис. 5 представлена платформа для онлайн-образования *Open edX* [23].

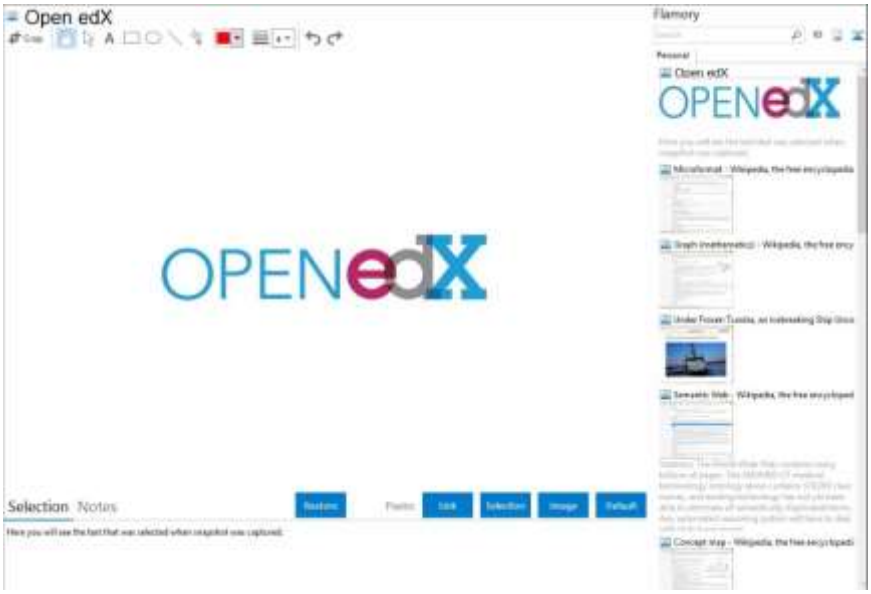

Рисунок 5

Одним из недостатков *Open edX* является то, что платформа может быть сложной для настройки и использования для нетехнических пользователей. Иногда могут возникнуть трудности с настройкой интеграции с другими системами, такими как система контроля доступа (СКД) или платформы для обработки платежей.

Другой недостаток *Open edX* – это то, что платформа может быть медленной и недостаточно гибкой для некоторых типов курсов или сценариев использования. Некоторые пользователи также жалуются на отсутствие некоторых функций, таких как возможность записи и просмотра видео в платформе.

Заключение

В данной статье были выявлены основные недостатки пяти решений *Cloud-based virtual labs*, таких как *Cisco NetSpace, AWS Educate, Google Cloud Platform Education (GCPE), Microsoft Azure for Students, Open edX*. Но несмотря на то, что решения *Cloud-based virtual labs* имеют некоторые недостатки, они обладают множеством преимуществ, включая доступность из любого места и в любое время, экономию затрат на оборудование и поддержку, а также возможность для совместной работы и взаимодействия в реальном времени. Будущее онлайн-образования наверняка будет включать в себя более широкое использование *Cloud-based virtual labs*, так как они предоставляют гибкость и доступность, которые необходимы для современного онлайн-образования.

Литература

1. Облачные решения в сфере образования. Дата просмотра 11.01.2023 cloud.yandex.ru/solutions/education
2. Батаев А.В. Анализ использования облачных технологий в сфере e-learning Текст: непосредственный // Молодой ученый, 2015. – № 18 (98). – С. 245-248. – URL: https://moluch.ru/archive/98/22019/ (дата обращения: 14.01.2023).
3. Сироткин А. Ю. Применение облачных технологий в системе дистанционного обучения // Гаудеамус, 2013. – № 1 (21).

URL: https://cyberleninka.ru/article/n/primenenie-oblachnyh-tehnologiy-v-sisteme-distantsionnogo-obucheniya (дата обращения: 14.01.2023).
4. Xu, Le & Huang, Dijiang & Tsai, Wei-Tek. (2012). V-lab: A cloud-based virtual laboratory platform for hands-on networking courses. 2. 10.1145/2325296.2325357
5. Top 8 Benefits of Switching to Cloud-Based Lab Environments for Software Training. Дата просмотра 11.01.2023 cloudlabs.ai/cloud-based-lab-environments-for-software-training/
6. Cisco NetSpace Quick Start Guide. Дата просмотра 11.01.2023 www.inf.tsu.ru/cisco/students/student_quick_start.pdf
7. Frequently Asked Questions: Cisco NetSpace. Дата просмотра 11.01.2023 www.cisco.com/c/dam/global/de_at/assets/events/ainac2013/pdfs/cisco_netspace_faq-14nov12.pdf
8. User Guide for Cisco netManager - Unified Communications 1.1. Дата просмотра 11.01.2023 www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_netmanager/1-1_voice/user/guide/CnMuguide/1_ov.html
9. AWS Educate. Дата просмотра 11.01.2023 ws.amazon.com/ru/education/awseducate/
10. Как IT-гиганты помогают образованию? Часть 3: Amazon Web Services. Дата просмотра 11.01.2023 habr.com/ru/company/ua-hosting/blog/508650/
11. Cara Daftar Akun Pembelajaran AWS Educate Gratis. Дата просмотра 11.01.2023 dwiay.com/2022/07/21/cara-daftar-akun-pembelajaran-aws-educate-gratis/
12. Powering possibilities with Google Cloud. Дата просмотра 11.01.2023 edu.google.com/google-cloud/
13. Google Cloud Higher Education Programs. Дата просмотра 11.01.2023 cloud.google.com/edu
14. Как IT-гиганты помогают образованию? Часть 1: Google. Дата просмотра 11.01.2023 habr.com/ru/company/ua-hosting/blog/508302/
15. Google Cloud для образования. Как GCP может быть полезным для студентов. Дата просмотра 11.01.2023 cloudfresh.com/ru/cloud-blog/google-cloud-dlya-obrazovanyya-kak-gcp-mozhet-byt-poleznym-dlya-studentov/
16. Лучшие облачные технологии 2017 года. Дата просмотра 11.01.2023 www.andreylavrov.com/2017/12/the-best-cloud-technology-2017.html?m=1
17. Build in the cloud free with Azure for Students. Дата просмотра 11.01.2023 azure.microsoft.com/en-us/free/students/
18. Как пользоваться Azure бесплатно (лайфхак для студентов). Дата просмотра 11.01.2023 habr.com/ru/company/microsoft/blog/352786/
19. What is Microsoft Azure for Students: FAQS, How to Sign-Up and More. Дата просмотра 11.01.2023 azurelessons.com/azure-for-students/
20. Microsoft Azure delivers NoSQL storage via DocumentDB. Дата просмотра 11.01.2023 www.yahoo.com/lifestyle/tagged/travel/ideas/microsoft-azure-delivers-nosql-storage-211300078.html
21. Deliver inspiring learning experiences on any scale. Дата просмотра 11.01.2023 openedx.org
22. Open edX. Дата просмотра 11.01.2023 ru.wikipedia.org/wiki/Open_edX
23. Open edX and Flamory. Дата просмотра 11.01.2023 esivt.com/en/integrations/app/open-edx

АНАЛИЗ СУЩЕСТВУЮЩИХ ПРОБЛЕМ ОТЕЧЕСТВЕННЫХ РЕШЕНИЙ ДИСТАНЦИОННОГО ФОРМАТА ОБУЧЕНИЯ НА БАЗЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Д.Б. Горошков, *Московский технический университет связи и информатики, zet.6@yandex.ru.*

УДК 004.75

Аннотация. В данной статье проводится анализ существующих проблем отечественных решений дистанционного формата обучения на базе облачных технологий. Несмотря на то, что в последнее время отечественная ИТ-индустрия в целом стала активнее развиваться, в данной области в российских решениях можно выявить ряд недостатков. В данной статье также приводятся возможные пути устранения выявленных недостатков. Помимо недостатков приводятся и достоинства, которые могут повлиять при выборе для российских потребителей.

Ключевые слова: обучение; студент; решение; технология; курс; дистанционное обучение; образование; преподаватель; российские решения; качество.

ANALYSIS OF EXISTING PROBLEMS OF DOMESTIC SOLUTIONS OF DISTANCE LEARNING FORMAT BASED ON CLOUD TECHNOLOGIES

D.B. Goroshkov, *Moscow Technical University of Communications and Informatics.*

Annotation. This article analyzes the existing problems of domestic solutions for distance learning based on cloud technologies. Despite the fact that the domestic OT industry as a whole has recently begun to develop more actively, a number of shortcomings can be identified in Russian solutions in this area. This article also provides possible ways to eliminate the identified shortcomings. In addition to the disadvantages, there are advantages that may affect the choice for Russian consumers.

Keywords: training; student; solution; technology; course; distance learning; education; teacher; Russian solutions; quality.

Введение

Исследование решений на базе облачных технологий может помочь в совершенствовании дистанционного формата обучения. Облачные технологии предоставляют доступ к масштабируемым и обновляемым ресурсам, которые могут быть использованы для предоставления качественного образования на расстоянии. Это включает в себя использование виртуальной реальности, мобильных приложений, онлайн-курсов и других инструментов, которые могут помочь учителям и студентам в их обучении.

Использование облачных технологий помогает в создании более гибкой и доступной системы обучения. Студенты получают доступ к курсам и материалам обучения из любой точки мира с помощью интернета, и они могут обучаться в удобное для них время. Также, облачные технологии могут помочь в обмене информацией и сотрудничестве между студентами и преподавателями, давая возможность создавать коллективные проекты и задания [1-4].

Наиболее известными решениями являются следующие:

1) *Learning Management Systems* (*LMS*) – это платформы, которые позволяют преподавателям создавать и управлять курсами, обмениваться материалами со студентами. Примеры таких систем: *Blackboard, Canvas, Moodle* [5, 6].

2) *Virtual Classroom Platforms* – это платформы, которые позволяют проводить онлайн-лекции и вебинары, общаться в режиме реального времени со студентами. Примеры таких систем: *Zoom, Microsoft Teams, Google Meet* [7].

3) *MOOCs* (*Massive Open Online Courses*) – это онлайн-курсы, которые доступны для всеобщего пользования тысяч зарегистрированных студентов. Они обычно предлагают видео-лекции, задания, общение с преподавателем и другими студентами и могут быть бесплатными или платными. Примеры таких платформ: *Coursera, edX, Udemy* [8, 9].

Развитие отечественных решений

Российские решения для дистанционного обучения начинали создаваться еще в 90-х гг. Одним из первых была система «Всероссийская дистанционная школа» (ВДШ), созданная в 1995 г. Она была разработана как инструмент для обеспечения доступности образования в регионах России [10]. На рис. 1 показан сайт российской электронной школы.

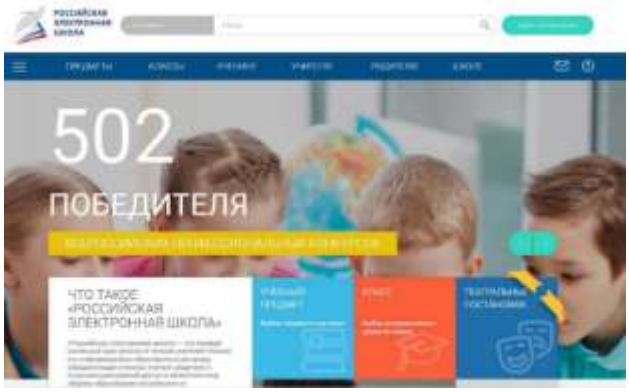

Рисунок 1

Затем в 1998 г. открылся факультет дистанционного обучения в «Российском экономическом университете им. Г.В. Плеханова» [11, 12]. На рис. 2 показан сайт факультета дистанционного обучения в «Российском экономическом университете им. Г.В. Плеханова».

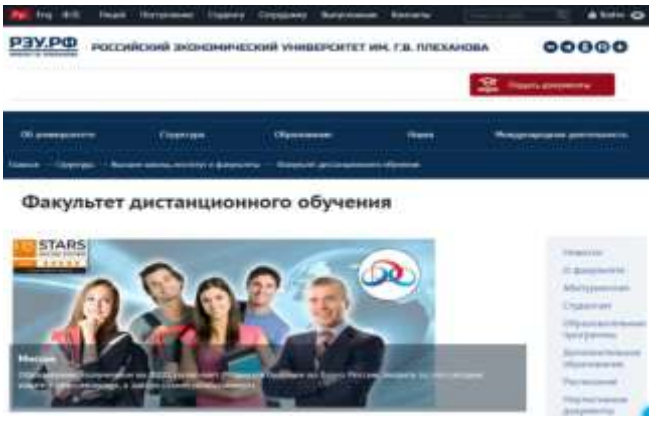

Рисунок 2

В 2010-х гг. начали появляться другие платформы дистанционного образования, такие как «Открытое образование» [13] и др. Эти платформы объединяют множество курсов и материалов различных учебных заведений и предлагают их пользователям бесплатно или за небольшую плату. На рис. 3 показан сайт «Открытое образование».

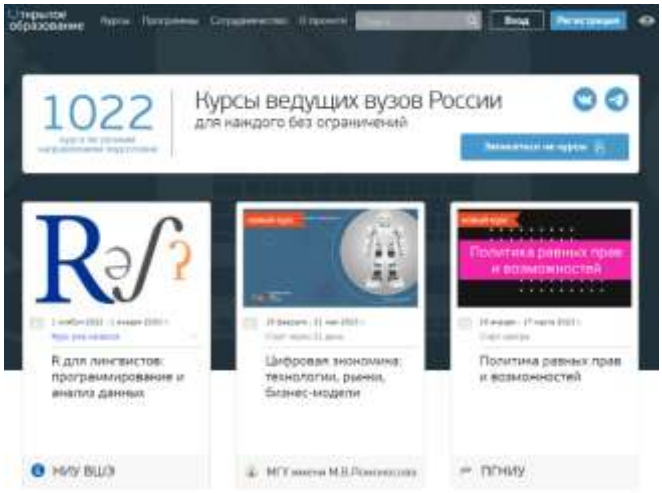

Рисунок 3

В связи с распространением *COVID*-19, использование дистанционного обучения значительно увеличилось, и многие учебные заведения и организации начали использовать облачные технологии для предоставления дистанционного обучения [15, 16].

В российской образовательной сфере есть множество решений для дистанционного обучения, которые были разработаны как государственными учебными заведениями, так и частными компаниями. Они включают в себя онлайн-курсы, видео-уроки, виртуальные классы, онлайн-тестирование и многое другое. Эти решения помогают студентам и профессионалам получить образование в любое время и из любой точки мира, а также обеспечивают интерактивность и доступность образования для всех.

В последнее время отечественная ИТ-индустрия в целом начала развиваться активнее, но российские решения дистанционного обучения на базе облачных технологий содержат много недостатков по сравнению с зарубежными:

1. Недостаточное качество перевода материалов на иностранные языки, которое может привести к недоступности материала для иностранных студентов.

Это связано с отсутствием профессиональных переводчиков или недостаточным качеством их работы. Также, некоторые решения могут не иметь возможности для автоматического перевода, что может привести к недоступности материала для иностранных студентов. Это важно учитывать для образовательных организаций, которые хотят привлечь иностранных студентов и предложить им качественное образование.

Этот недостаток может быть решен несколькими методами. Первым шагом может быть наем квалифицированных и профессиональных переводчиков для перевода материалов на иностранные языки. Это дорого, но гарантирует качество перевода и доступность материала для иностранных студентов.

Другой метод – использование автоматического перевода, но после проверки качества перевода профессионалом и корректировки. Это – более

экономичное решение, но качество перевода ниже, чем с использованием профессиональных переводчиков.

Еще один метод – использование готовых материалов на иностранных языках, которые можно найти в интернете, таких как международные онлайн-курсы или открытые курсы на платформах типа МООС. Это – более эффективное решение, но не столь персонализировано и может не подходить для всех студентов.

Общим для всех методов является то, что необходимо уделять внимание качеству перевода и доступности материала для иностранных студентов, чтобы обеспечить им качественное образование.

2. Ограниченный доступ к международным ресурсам и сетям, которые доступны в зарубежных решениях.

Это ограничивает возможности доступа российских студентов к международной информации и образовательным ресурсам и, как следствие, оказывает негативное влияние на качество их образования.

Этот недостаток может быть решен применением нескольких методов. Первым шагом является поддержка образовательных организаций в получении доступа к международным ресурсам и сетям. Это достигается с помощью сотрудничества с международными образовательными организациями, заключения договоров и соглашений и использования иностранных интернет-ресурсов.

Другой метод – использование виртуальных и дистанционных средств для обхода ограничений доступа к информации и сетям. Это может включать использование виртуальных приватных сетей (*VPN*) для доступа к заблокированным ресурсам и платформам, использование иностранных облачных сервисов для хранения и доступа к данным и общение с международными коллегами и преподавателями через онлайн-коммуникационные инструменты.

Важно отметить, что даже использование виртуальных и дистанционных средств не гарантирует полный доступ к международным ресурсам и сетям из-за ограничений и блокировок, которые могут быть установлены государством.

3. Менее развитая инфраструктура для дистанционного обучения, в том числе менее развитые онлайн-инструменты и технологии.

Российские образовательные организации могут иметь менее развитую инфраструктуру для дистанционного обучения, включая менее развитые онлайн-инструменты и технологии, чем зарубежные аналоги.

Этот недостаток решается с помощью нескольких методов. Первый шаг – инвестиции в инфраструктуру для дистанционного обучения, включая приобретение и обновление онлайн-инструментов и технологий.

Другой метод – сотрудничество с зарубежными компаниями и организациями для доступа к их инфраструктуре и опыту. Также целесообразно проведение тренингов и семинаров для преподавателей и администраторов с целью овладения навыками работы с онлайн-инструментами и технологиями.

Недостаток менее развитой инфраструктуры для дистанционного обучения решается с помощью соответствующих инвестиций и сотрудничества, но это может занять некоторое время.

4. Менее широкий выбор курсов и программ обучения.

Зарубежные решения, как правило, предлагают более широкий выбор курсов и программ обучения, включая различные языки, технологии и дисциплины.

Этот недостаток может быть решен несколькими способами. Один из них – развитие и расширение курсов и программ обучения внутри российских

образовательных организаций, в том числе, внедрение новых технологий, дисциплин и языков в курсы.

Другой способ – сотрудничество с зарубежными образовательными организациями и компаниями для доступа к их курсам и программам обучения. Это может включать в себя партнерство для предоставления дистанционных курсов или программ, обмен студентами и преподавателями.

Также можно создавать онлайн-курсы и программы обучения с использованием отечественных специалистов и инструментов для привлечения студентов из различных стран.

Менее широкий выбор курсов и программ обучения – это действительно недостаток, ограничивающий возможности студентов и преподавателей в России. Но с помощью развития и расширения курсов и программ обучения, сотрудничества с зарубежными организациями и создания онлайн-курсов, можно снизить этот недостаток и улучшить возможности для дистанционного обучения в России.

5. Менее значительное участие и присутствие международных экспертов и преподавателей в российских онлайн-курсах.

Данный недостаток негативно влияет на качество образования и международную привлекательность онлайн-курсов в России. Международные эксперты и преподаватели могут предлагать разнообразный опыт и знания, а также помощь в том, чтобы сделать курсы более международно-привлекательными.

Одним из способов решения этой проблемы является создание сотрудничества с зарубежными организациями и университетами с целью привлечения международных экспертов и преподавателей для ведения курсов и программ обучения. Также можно использовать инновационные технологии, такие как виртуальная и дополненная реальность, чтобы позволить международным экспертам и преподавателям принимать участие в онлайн-курсах без необходимости физического присутствия. В итоге, это может улучшить качество образования и помочь российским онлайн-курсам стать более международно-конкурентоспособными и привлекательными для студентов из разных стран.

Кроме того, возможно создание совместных онлайн-программ с зарубежными университетами, в которых студенты могут получать дипломы от обоих учебных заведений. Это может привлечь иностранных студентов к онлайн-образованию в России и сделать его более международно-привлекательным.

В дополнение к недостаткам российских решений для дистанционного обучения, стоит отметить, что некоторые из них могут иметь ограниченный функционал, не совсем подходящий для всех типов обучения. Например, некоторые решения ориентированы на обучение студентов на определенном уровне или в определенной сфере, или не имеют много возможностей для интерактивности и общения с другими студентами и преподавателями.

Однако, не смотря на перечисленные недостатки отечественные решения имеют и ряд достоинств, такие как:

1) Доступность: российские решения для дистанционного обучения доступны для большего количества студентов из-за более низкой стоимости или бесплатности некоторых курсов и программ.
2) Репутация: российские вузы имеют долгую историю и богатый опыт в области образования, который важен для многих студентов.
3) Локализация: российские решения могут быть более подходящими для студентов, живущих в России или ближнем зарубежье, из-за локализации курсов и материалов на русском языке.

4) Культурное соответствие: российские решения являются более подходящими для студентов, интересующихся российской культурой и историей.
5) Наличие локальных инструментов: российские решения используют локальные инструменты и технологии, которые могут быть более подходящими и эффективными для студентов и преподавателей в России.
6) Возможности для сотрудничества: российские решения более открыты для сотрудничества с другими российскими университетами и образовательными учреждениями, а также для сотрудничества с локальными компаниями и организациями.

Заключение

Однако, с развитием технологий и инфраструктуры многие российские решения для дистанционного обучения становятся все более доступными и качественными и начинают конкурировать с зарубежными решениями.

В целом, российские решения для дистанционного обучения имеют некоторые недостатки по сравнению с зарубежными, но они становятся все более конкурентными и развиваются с использованием новых технологий и улучшением качества образования. Российские компании и организации начинают инвестировать в дистанционное обучение и предлагать все больше курсов и программ для студентов во всех регионах России.

Литература

1. Щербатский В.Б., Кормышев В.М. Облачные технологии в обучении и оценке компетентности специалистов. – М.: LAP Lambert Academic Publishing, 2018. – 152 с.
2. Карр Н. Великий переход. Революция облачных технологий. – М.: Манн, Иванов и Фербер, 2017. – 737 с.
3. Карр Н. Великий переход: что готовит революция облачных технологий. – М.: Машиностроение, 2019. – 722 с.
4. Карр Н. Великий переход. Что готовит революция облачных технологий / Карр Николас. – М.: Манн, Иванов и Фербер, 2018. – 145 с.
5. Большой обзор LMS-систем: виды, поставщики и реальный кейс внедрения. Дата обращения 10.01.2023 vc.ru/education/218817-bolshoy-obzor-lms-sistem-vidy-postavshchiki-i-realnyy-keys-vnedreniya
6. Learning management system. Дата обращения 10.01.2023 en.wikipedia.org/wiki/Learning_management_system
7. Comparing Zoom, Microsoft Teams and Google Meet. Дата обращения 10.01.2023 gcloud.devoteam.com/blog/comparing-zoom-microsoft-teams-and-google-meet/
8. Massive open online course. Дата обращения 10.01.2023 en.wikipedia.org/wiki/Massive_open_online_course
9. МООК, МООС, или массовые открытые онлайн-курсы, и их классификация. Дата обращения 10.01.2023 skillbox.ru/media/education/mook-mooc-ili-massovye-otkrytye-onlaynkursy-i-ikh-klassifikatsiya/
10. Российская электронная школа. Дата обращения 10.01.2023 resh.edu.ru
11. Российский экономический университет имени Г. В. Плеханова. Дата обращения 10.01.2023 ru.wikipedia.org/wiki/Российский_экономический_университет_имени_Г._В._Плеханова.

12. История факультета. Дата обращения 10.01.2023
www.rea.ru/ru/org/faculties/distfak/Pages/history_faculty.aspx
13. Открытое образование. Дата обращения 10.01.2023
wikipredia.net/ru/Open_education
14. Краснова Г.А., Полушкина А.О. Состояние и перспективы дистанционного обучения в период пандемии COVID-19 // Вестник РУДН. Серия: Информатизация образования, 2021. – № 1.
URL: https://cyberleninka.ru/article/n/sostoyanie-i-perspektivy-distantsionnogo-obucheniya-v-period-pandemii-covid-19 (дата обращения: 14.01.2023)
15. Гладков Э.Л. Развитие информационного обеспечения дистанционно-образовательных технологий в эпоху пандемии // Молодой ученый, 2021. – № 17 (359). – С. 97-100. – URL: https://moluch.ru/archive/359/80298/ (дата обращения: 14.01.2023).
16. Гладков Э.Л. Развитие информационного обеспечения дистанционно-образовательных технологий в эпоху пандемии // Молодой ученый, 2021. – № 17 (359). – С. 97-100. – URL: https://moluch.ru/archive/359/80298/ (дата обращения: 14.01.2023).

СПОСОБЫ СОЗДАНИЯ ОНЛАЙН-ТЕСТОВ В CLOUD-BASED LANGUAGE LEARNING TOOLS

Д.Б. Горошков, *Московский технический университет связи и информатики, zet.6@yandex.ru.*

УДК 004.75

Аннотация. Онлайн-тесты являются одним из самых простых и эффективных способов создания проверочных работ в *Cloud-based language learning tools.* Они позволяют быстро и легко оценивать знания студентов и давать им обратную связь на их прогресс. Онлайн-тесты могут быть использованы как в качестве основного способа оценки, так и в качестве дополнительного инструмента для совместного использования с другими методами обучения, такими как занятия с носителем языка или использование книг и аудио-учебников. В данной статье рассмотрены различные способы создания вопросов для онлайн-тестов в *Cloud-based language learning tools* и обсуждены их преимущества и недостатки. Выявлено, что лучший способ зависит от индивидуальных потребностей и целей обучения, а также обсуждено как их можно сочетать для максимальной эффективности.

Ключевые слова: вопрос; студент; язык; использование; онлайн-тест; обучение; онлайн-инструмент; создание; способ.

WAYS TO CREATE ONLINE TESTS IN CLOUD-BASED LANGUAGE LEARNING TOOLS

D.B. Goroshkov, *Moscow Technical University of Communications and Informatics.*

Annotation. Online tests are one of the easiest and most effective ways to create test papers in Cloud-based language learning tools. They allow you to quickly and easily evaluate students' knowledge and give them feedback on their progress. Online tests can

be used both as a primary method of assessment, and as an additional tool to be used in conjunction with other learning methods, such as classes with a native speaker or the use of books and audio tutorials. This article explores the different ways to create questions for online tests in Cloud-based language learning tools, and discusses their advantages and disadvantages. It is considered that the best method depends on individual needs and learning goals, and it is also discussed how they can be combined for maximum effectiveness.

Keywords: question; student; language; use; online test; learning; online tool; creation; method.

Введение

Решения дистанционного формата обучения на базе облачных технологий – это системы и технологии, которые используются для обеспечения дистанционного обучения с использованием облачных сервисов. Они могут включать в себя онлайн-платформы для обучения, видеоконференции, веб-конференции, мобильные приложения и другие инструменты, которые позволяют учителям и студентам общаться и обмениваться информацией в онлайн-режиме. Эти решения позволяют улучшить доступность образования и обеспечить гибкость в планировании и проведении занятий [1-3].

Одним из таких решений является *Cloud-based language learning tools. Cloud-based language learning tools* – это онлайн-инструменты для изучения языка, которые работают на основе облачной инфраструктуры. Они включают в себя различные функции, такие как изучение словарного запаса, тренировку произношения, практику диалогов и доступны из любой точки мира через интернет [4-6].

Внизу показаны некоторые платформы *Cloud-based language learning tools*. На рис. 1 представлен *Linguix* – ассистент для написания текстов [7].

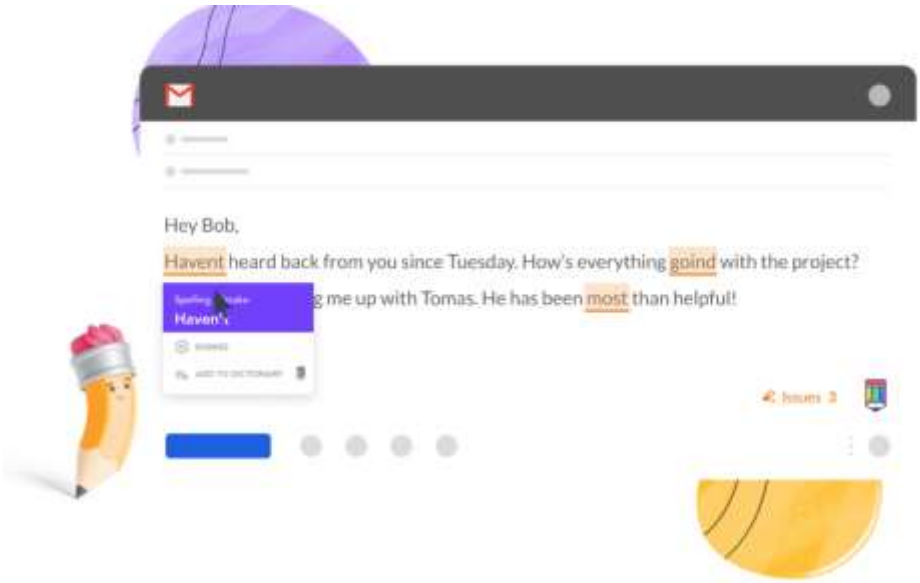

Рисунок 1

На рис. 2 показан *iTalki* – сервис для обучения с носителями языка [7].

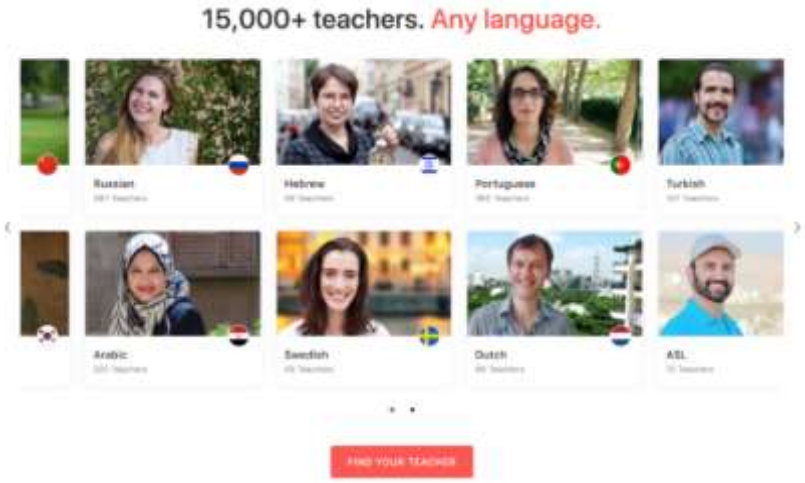

Рисунок 2

На рис. 3 показана *Puzzle English* – платформа для самостоятельного обучения [7].

Рисунок 3

Преимущества и недостатки

Одним из основных преимуществ онлайн-инструментов для изучения языка является то, что они могут быть доступны в любое время и из любой точки мира. Это означает, что студенты могут изучать язык в свое свободное время и в своем удобном темпе. Кроме того, онлайн-инструменты могут предоставлять больше интерактивности и динамичности, чем традиционные методы обучения языку. Например, они могут использовать мультимедийные материалы и игры, чтобы сделать изучение языка более интересным и захватывающим [8-13].

Другим преимуществом онлайн-инструментов для изучения языка является их доступность. Многие инструменты можно использовать бесплатно, или за небольшую плату, что делает их доступными для людей с различными бюджетами. Кроме того, онлайн-инструменты могут помочь студентам изучать язык в международной группе и общаться с носителями языка из разных стран, что может сделать изучение языка более привлекательным и эффективным. То есть, основными преимуществами *Cloud-based language learning tools* являются:

1) Доступность: инструменты доступны из любой точки мира с интернет-соединением.

2) Комфорт: изучение языка может проходить в любое удобное время и место, без необходимости посещать традиционные классы.
3) Разнообразие: множество различных инструментов и ресурсов доступны для изучения языка, включая онлайн-учебники, аудио-учебники, видео-уроки и игры.
4) Персонализация: многие инструменты позволяют настроить уровень сложности и план обучения, чтобы соответствовать индивидуальным потребностям каждого студента [14-17].

Но онлайн-инструменты для изучения языка могут иметь свои недостатки, например, отсутствие личной обратной связи или ограниченные возможности для практики устной речи. Поэтому, использование онлайн-инструментов должно сочетаться с другими методами изучения языка для максимальной эффективности. Например, использование онлайн-инструментов может быть хорошим дополнением к занятиям с носителем языка, чтобы получить личную обратную связь и практику устной речи. Или сочетание онлайн-инструментов и книг или аудио-учебников для получения более глубокого понимания грамматики и словарного запаса. Т.е. основными недостатками *Cloud-based language learning tools:*

1) Отсутствие личной обратной связи: некоторые инструменты могут не предоставлять возможности для личной обратной связи или общения с носителем языка.
2) Ограниченные возможности для практики устной речи: иногда может быть трудно практиковать речь и получить обратную связь на свою речь.
3) Зависимость от технологии: доступность инструментов зависит от качества интернет-соединения и наличия современного оборудования [18-23].

В целом, использование онлайн-инструментов для изучения языка может быть очень полезным, но для достижения максимальной эффективности необходимо сочетать их с другими методами изучения языка, такими как занятия с носителем языка, книги, аудио-учебники и т.д. Важно не забывать о практике устной речи, грамматики и словарного запаса, и обращать внимание на свои ошибки и получать личную обратную связь для их исправления.

Виды проверочных работ

Cloud-based language learning tools имеют различные способы создания проверочных работ, включая:

1) Онлайн-тесты: множество вопросов с выбором одного или нескольких ответов, которые создаются и используются для оценки знаний студентов.
2) Задания на письмо: студенты могут получают задание на написание текста и отправляют его на проверку.
3) Аудио- и видео-задания: студенты получают задание на запись аудио или видео и отправляют его на проверку.
4) Разговорная практика: инструменты включают возможность для студентов практиковать разговорную речь в режиме реального времени с носителями языка или другими студентами.
5) Проверка через искусственный интеллект (ИИ): инструменты используют ИИ для автоматической проверки ответов и обратной связи.

Способы создания онлайн-тестов

Онлайн-тесты являются одним из самых распространенных способов создания проверочных работ в *Cloud-based language learning tools*. Они создаются с использованием различных типов вопросов, включая вопросы с выбором одного или нескольких ответов, вопросы с выбором из списка, вопросы с заполнением пропусков и т.д.

Онлайн-тесты, как правило используются для оценки знаний студентов в различных областях, таких как грамматика, словарный запас, лексика и т.д. В этом случае, они создаются и настраиваются для проведения в различное время и могут быть доступны для студентов в любое время. Результаты тестов автоматически просчитываются и отображаются в виде отчета, используемого для оценки прогресса студентов.

Онлайн-тесты предусмотрены для работы с различными уровнями сложности и могут быть специализированными для различных групп студентов, например, для начинающих или продвинутых студентов. Для этого онлайн-тесты создаются с использованием как стандартных, так и пользовательских вопросов, и могут быть использованы для оценки знаний в различных областях, таких как устная речь, письмо, чтение и слушание.

Вопросы для онлайн-тестов создаются с использованием различных методов и инструментов. Один из способов – это создание вопросов вручную с использованием текстового редактора или специализированного программного обеспечения (ПО) для создания онлайн-тестов. Это включает в себя добавление текста вопроса и вариантов ответов, а также настройку параметров, таких как тип вопроса и уровень сложности.

Другой способ – это использование банка вопросов, который может быть доступен в инструментах для онлайн-обучения. Это включает в себя доступ к базе данных вопросов, используемых для создания тестов, а также инструменты для редактирования и настройки вопросов.

В любом случае, важно обеспечить, что вопросы для онлайн-тестов должны быть созданы с учетом целей обучения и уровня знаний студентов: они должны быть четкими и понятными, а также сбалансированными по сложности и охватывать различные аспекты языка, такие как грамматика, лексика и коммуникация. Кроме того, вопросы для онлайн-тестов должны проверяться на предмет ошибок и редактироваться перед использованием в онлайн-тесте.

Какой лучше способ однозначно сказать нельзя, все зависит от индивидуальных потребностей и целей обучения.

Создание вопросов вручную с использованием текстового редактора или специализированного ПО может быть полезным, если требуется создать вопросы, которые соответствуют точно определенным целям обучения и уровню знаний студентов. Этот способ также позволяет создавать индивидуальные вопросы, что полезно для изучения особо сложных или специфических тем.

Использование банка вопросов может быть полезным, если нужно быстро и легко создать тесты и оценить знания студентов без необходимости создавать вопросы с нуля. Банк вопросов, в таком случае, включает в себя готовые вопросы, которые можно использовать для создания тестов, и это особенно полезно, если необходимо создать большое количество тестов или оценить знания большого количества студентов.

В итоге, оба способа являются полезными в зависимости от конкретной ситуации и потребностей, и использование комбинации этих методов может дать наилучший результат. Важно обдумать, какой метод будет наиболее подходящим

для достижения конкретных целей обучения и как он сочетается с другими методами для максимальной эффективности.

Дополнительно, некоторые онлайн-инструменты изучения языка могут предоставлять функционал для создания и использования вопросов в онлайн-тестах, включая возможность добавлять изображения и аудио, различные типы вопросов (выбор, свободный ответ, последовательность, и т.д.) и автоматическую проверку ответов. Это упрощает и оптимизирует процесс создания и использования вопросов для онлайн-тестов, а также позволяет быстро создать множество вопросов и иметь большой выбор тем. Данный способ полезен, если требуется использовать стандартизированные вопросы для оценки знаний студентов. Но нужно учитывать, что банк вопросов ограничен по своей спецификации, и может не соответствовать индивидуальным потребностям и целям обучения.

В общем, какой способ создания вопросов для онлайн-тестов лучше, зависит от индивидуальных потребностей и целей обучения. Важно, чтобы вопросы были созданы с учетом целей обучения и уровня знаний студентов, были четкими и понятными, а также сбалансированными по сложности и охватывать различные аспекты языка. Важно проверять их на предмет ошибок и редактировать перед использованием в онлайн-тесте.

Заключение

Онлайн-тесты используются для создания индивидуальной оценки и групповой оценки, что делает их очень гибкими и подходящими для различных ситуаций и нужд. Онлайн-тесты должны быть созданы с учетом целей обучения и уровня знаний студентов, чтобы быть действенными и релевантными. Важно обеспечить достаточное количество обратной связи и предоставление рекомендаций для улучшения знаний и навыков студентов.

Нужно отметить, что создание вопросов для онлайн-тестов не является единственным способом оценки знаний студентов. Например, можно использовать систему оценки по компетенциям, где оценивается не только знание языка, но и способность использовать его в реальных ситуациях. Также можно использовать практические задания, которые позволяют студентам применять знания и навыки в реальных ситуациях.

Литература

1. Сироткин А.Ю. Применение облачных технологий в системе дистанционного обучения // Гаудеамус, 2013. – № 1 (21).
URL:https://cyberleninka.ru/article/n/primenenie-oblachnyh-tehnologiy-v-sisteme-distantsionnogo-obucheniya (дата обращения: 15.01.2023).
2. Батаев А.В. Анализ использования облачных технологий в сфере e-learning – Текст : непосредственный // Молодой ученый, 2015. – № 18 (98). – С. 245-248.
URL: https://moluch.ru/archive/98/22019/ (дата обращения: 15.01.2023).
3. Применение облачных технологий в дистанционном обучении. Date Views 11.01.2023.
rep.bntu.by/bitstream/handle/data/36511/Primenenie_oblachnyh_tekhnologij_v_distancionnom_obuchenii.pdf?sequence=1&isAllowed=y
4. Language Learning Software for Cloud. Date Views 11.01.2023 sourceforge.net/software/language-learning/saas/
5. Best Web-Based Language Learning Software. Date Views 11.01.2023 www.capterra.com/language-learning-software/s/web-based/

6. 21 Apps & Web Based Language Learning Tools I Use and Love. Date Views 11.01.2023 eurolinguiste.com/21-apps-web-based-language-learning-tools-i-use-and-love/
7. 6 полезных инструментов для изучения английского языка. Date Views 19.01.2023 habr.com/ru/post/566804/
8. Изучение языков. Date Views 19.01.2023 startpack.ru/category/language-learning.
9. ТОП – 10 сервисов для изучения иностранных языков – 2023. Date Views 19.01.2023 marketing-tech.ru/online-services_tags/learning-foreign-languages/
10. Топ-5 сервисов для изучения иностранных языков. Разбор, плюсы и минусы каждого приложения/сайта. Date Views 19.01.2023 dzen.ru/a/YGWKf5CjmGbk8LTa.
11. Лучшие альтернативы Duolingo для лучшего изучения языка в 2023 году (участники Duolingo). Date Views 19.01.2023 www.bloggersideas.com/ru/duolingo-alternatives/
12. Дубровкина И.Ю. Использование интернет-ресурсов и цифровых инструментов в дистанционном обучении английскому языку // Вестник Шадринского государственного педагогического университета, 2020. – № 3 (47). URL:https://cyberleninka.ru/article/n/ispolzovanie-internet-resursov-i-tsifrovyh-instrumentov-v-distantsionnom-obuchenii-angliyskomu-yazyku (дата обращения: 19.01.2023).
13. Программы обучения иностранному языку. Date Views 19.01.2023 a2is.ru/catalog/samoobuchenie
14. Топ-20 сайтов для изучения иностранных языков. Date Views 19.01.2023 top100lingua.ru/blog/uroki/top-20-sajtov-dlja-izuchenija-inostrannyh-jazykov
15. 10 онлайн сервисов для изучения английского и других языков. Date Views 19.01.2023 blog.themarfa.name/6-onlain-siervisov-dlia-izuchieniia-anghliiskogho-i-drughikh-iazykov/
16. Облачные решения: особенности, виды и преимущества. Date Views 19.01.2023 vc.ru/u/1134941-digex-co/440259-oblachnye-resheniya-osobennosti-vidy-i-preimushchestva
17. Как вести бизнес через облачные сервисы. Date Views 19.01.2023 secrets.tinkoff.ru/razvitie/oblachnye-servisy/
18. Что такое облачные сервисы, их виды, как перейти в облако + программы. Date Views 19.01.2023 zvonobot.ru/blog/oblachnye-servisy-chto-eto-vidy-kak-pereyti-v-oblako/
19. Что такое облачные технологии и как они устроены. Date Views 19.01.2023 practicum.yandex.ru/blog/oblachnye-tehnologii/
20. Облачные вычисления. Date Views 19.01.2023 ru.wikipedia.org/wiki/Облачные_вычисления
21. Облачные сервисы: что такое, какими бывают и кому полезны. Date Views 19.01.2023 skillbox.ru/media/code/oblachnye-servisy-chto-takoe-kakimi-byvayut-i-komu-polezny/
22. Облачные технологии: структура, виды, сферы применения. Date Views 19.01.2023 gb.ru/blog/oblachnye-tekhnologii/
23. Введение в облачные вычисления для всех от инженера Microsoft, Ex-Amazon. Date Views 19.01.2023 habr.com/ru/post/585064/

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

РАЗРАБОТКА МЕТОДИКИ ОБНАРУЖЕНИЯ БЕСПРОВОДНЫХ ПРОКСИ-СТАНЦИЙ В КОРПОРАТИВНОЙ WLAN-СЕТИ

И.Н. Бабков, *к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, ib9809@mail.ru;*
Э.А. Бударин, *к.т.н., доцент, Военная академия связи им. Маршала Советского Союза С.М. Буденного, budarin_ilya@mail.ru;*
А.Ю. Кистуга, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, anton.kistruga@gmail.com;*
М.Э. Бударин, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, budarin.makar@gmail.com.*

УДК 654

Аннотация. Исследованы признаки несанкционированного доступа нелегитимного устройства к *WLAN*-сети посредством подключения к легитимному устройству, работающему в режиме точки доступа *Wi-Fi*. Предложена методика обнаружения нелегитимного устройства по данным признакам.

Ключевые слова: информационная безопасность; безопасность беспроводных сетей; признаки; методика; точки доступа; прокси-станции; беспроводные сети.

DEVELOPMENT OF WIRELESS PROXY STATION DETECTION METHODOLOGY IN THE CORPORATE WLAN NETWORK

Ivan Babkov, *Ph.D., Associate Professor, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich;*
Eduard Budarin, *Ph.D., Associate Professor, in Military Sciences, Department of Security of Special Purpose Infocommunication Systems, The S.M. Budyonny Military Academy of the Signal Corps;*
Anton Kistruga*, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich;*
Makar Budarin, *St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich.*

Annotation. Signs of unauthorized access of a rogue device to the *WLAN* network by connecting to a legitimate device operating as a *Wi-Fi* access point were investigated. A methodology for detecting a rogue device based on these signs has been developed.

Keywords: information security; wireless network security; signs; methodology; access points; proxy stations; wireless networks.

Введение

В современных условиях развития технологий все чаще применяются беспроводные локальные сети. С их помощью можно объединить большое количество устройств, наладить их совместную работу и быструю коммуникацию. В настоящее время практически в любой сфере деятельности встречается использование беспроводных локальных сетей, в частности, в крупных компаниях, которым необходимо организовать работу сотрудников в офисе [1]. Корпоративная

WLAN (*Wireless Local Area Network*) может быть как замкнута на территории соответствующего помещения, так и иметь доступ к сети интернет. Основным достоинством такой беспроводной сети является мобильность всех сотрудников, так как доступ к информации у них будет из любой точки помещения, где имеется сигнал, мощности которого достаточно для подключения к сети. Но у беспроводной сети есть существенный недостаток – слабая защищенность при недостаточной работе над администрированием. Тем не менее, все большее количество компаний внедряют в своих офисах подобный способ организации сети.

Уязвимость корпоративной *WLAN*

Беспроводные сети постоянно совершенствуются, каждый год идет работа над их улучшением, повышается функциональность и внедряются новые технологии защиты информации. Однако, даже со всеми современными методами защиты нельзя с полной уверенностью утверждать, что беспроводные локальные сети являются полностью безопасными [2]. С использованием *WLAN* в офисе организации появляется серьезная уязвимость для несанкционированного доступа в закрытую сеть, заключающаяся в подключении к легитимному устройству сотрудника, работающего в режиме точки доступа *Wi-Fi*. Для дальнейшего исследования введем термин «беспроводная прокси-станция» для подобных устройств. В статье была смоделирована и исследована данная уязвимость, проведена симуляция вышеописанной ситуации, приведены меры профилактики, а также предложен способ обнаружения присутствия в корпоративной сети нелегитимного устройства, использующего данную уязвимость [12].

Описание проблемы

Чаще всего в корпоративных беспроводных сетях используют всевозможные современные методы защиты. Однако, злоумышленники могут находить обходные пути для получения доступа [3]. Один из них заключается в особенностях работы устройств в режиме точки доступа *Wi-Fi* (*WLAN-WLAN* тетеринг беспроводной прокси-станции). Предположим, сотруднику компании, будучи подключенным к корпоративной *WLAN*, понадобилось параллельно включить на своем устройстве подобный режим точки доступа. Тогда стороннее устройство, которое подключается к данной *Wi-Fi* сети, получает доступ к корпоративной *WLAN*. Более того, трафик стороннего устройства будет присутствовать в сети организации с *MAC*-адресом и *IP*-адресом легитимного устройства, работающего в режиме прокси-станции, что сильно усложняет выявление подобных инцидентов [4]. Эта проблема может привести к серьезным последствиям для компании, включая утечку конфиденциальных данных и вредоносных атак на сеть. Кроме того, подключение нелегитимного устройства может снизить производительность сети и повлиять на качество работы, что в свою очередь повлечет за собой финансовые и репутационные потери, так как вызовет снижение доверия клиентов к организации.

Меры профилактики

Стоит отметить, что в первую очередь в подобных ситуациях виноват будет сотрудник, развернувший на своем устройстве ненадежную точку доступа *Wi-Fi*, тем самым сделав корпоративную сеть незащищенной [5]. В таком случае, первоначальной целью злоумышленника станет подключение к этой точке доступа.

Во избежание таких ситуаций изначально следует провести инструктаж по сетевой безопасности для всех сотрудников, имеющих доступ к сети. В инструктаж необходимо включить блоки, разъясняющие опасность создания точек доступа, памятки по созданию надежного пароля, а также советы по целесообразному использованию корпоративной сети. Большинство инцидентов, связанных с проникновением в сеть через точку доступа *Wi-Fi*, происходят по причине очень простого, либо вовсе отсутствующего пароля на развернутой сотрудником точке доступа [9], в то время как сам сотрудник может даже не подозревать, что таким образом он подвергает опасности всю корпоративную сеть. Даже, если пароль назначен, злоумышленник может применить метод подбора пароля «грубой силой» (*Brute force*) [18].

Следующим шагом необходимо ввести новые правила пользования корпоративной сетью. Существует несколько вариантов вводимых изменений. Наиболее надежным и радикальным методом является запрет на подключение к сети с личных устройств, а на корпоративной технике – отключение функции точки доступа на программном уровне. Менее радикальный метод – разрешить подключение к сети с личных устройств, но запретить создание точек доступа внутри этой сети. Такой вариант будет менее надежным, так как у сотрудников останется возможность создавать точки доступа, а контроль выполнения правил потребует дополнительных технических решений.

Все введенные правила необходимо зафиксировать во внутренних документах компании, ввести санкции за их нарушение и потребовать сотрудников ознакомиться, а также дать соглашение и расписаться.

Выявление беспроводных прокси-станций

Несмотря на все меры профилактики инцидентов, могут происходить случаи нарушения предписаний: сотрудник создает слабозащищенную точку доступа *Wi-Fi* внутри корпоративной сети, а злоумышленник, с легкостью подобрав к ней пароль, подключается и получает доступ к сети [6].

Для таких случаев требуется разработать методику обнаружения устройств внутри сети, работающих в режиме точки доступа *Wi-Fi* и подключенных к ним нелегитимных устройств для дальнейшего предотвращения несанкционированного доступа к целевой *WLAN*. Необходимо определить признак создания мобильной точки доступа, либо подключения третьего устройства к ней, а также выявить создавшего точку доступа сотрудника. Для выполнения вышеперечисленных задач, в первую очередь, используется специализированное программное обеспечение для мониторинга сетевого трафика – *Wiresha*rk. Проводится анализ сетевого трафика на предмет нестандартных запросов и ответов, анализ *IP* и *MAC* адресов, обнаружение нескольких подключений с одних и тех же адресов, сопоставление адресов с запросами [7].

Методика исследования

За основу исследования взята легенда: в офисе компании налажена *WLAN*-сеть для внутренней работы сотрудников и взаимосвязи отделов. Некоторый сотрудник, будучи подключенным к данной сети со своего устройства, параллельно включает режим точки доступа *Wi-Fi*. Третье лицо, являющееся злоумышленником, цель которого – получение доступа к закрытой корпоративной сети, подключается к точке доступа *Wi-Fi* сотрудника компании. Данная схема изображена на рис. 1.

Рисунок 1

Для симуляции атаки было использовано следующее оборудование:

- Виртуальная машина в целевой сети с установленным *Kali Linux*, используемая для перехвата и анализа трафика.
- Беспроводная сетевая карта – *Mercusys MW*300*UH*.
- *Wi-Fi* роутер – *Eltex NTU-RG*-1402*G-W* (в качестве точки доступа к корпоративной *WLAN*).
- Смартфон под управлением ОС *Android* (в качестве легитимного устройства сотрудника с развернутой точкой доступа).
- Ноутбук под управлением ОС *Windows* (в качестве нелегитимного устройства злоумышленника).

В последующих пунктах описана работа на виртуальной машине с *Kali Linux* [16]. Алгоритм анализа трафика для выявления присутствия нелегитимного устройства в сети [17]:

1. Для анализа сетей и перехвата трафика необходимо переключить беспроводную сетевую карту в режим монитора. Это делается командой «*airmon-ng start wlan*0», где *wlan*0 – имя сетевой карты (рис. 2).

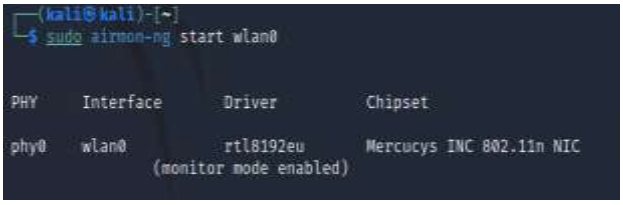

Рисунок 2

2. Для захвата пакетов беспроводных сетей в радиусе действия необходимо ввести команду «*airodump-ng wlan*0». Имя целевой сети, работающей в качестве корпоративной – «*BudWiFi*» (рис. 3).

Рисунок 3

3. Для запуска захвата трафика *Wi-Fi* сети «*BudWiFi*» необходимо ввести команду «*airodump-ng --bssid 'A8:F9:4B:CE:91:19' --essid 'BudWiFi' -c* 1 *-w /usr/BudWiFicaptures wlan*0», где:

- *A8:F9:4B:CE:91:19 – BSSID* нашей сети из таблицы выше;
- *BudWiFi – ESSID* нашей сети из таблицы выше;
- *1* – значение *CH* из таблицы выше;
- */usr/BudWiFicaptures* – каталог для сохранения (рис. 4).

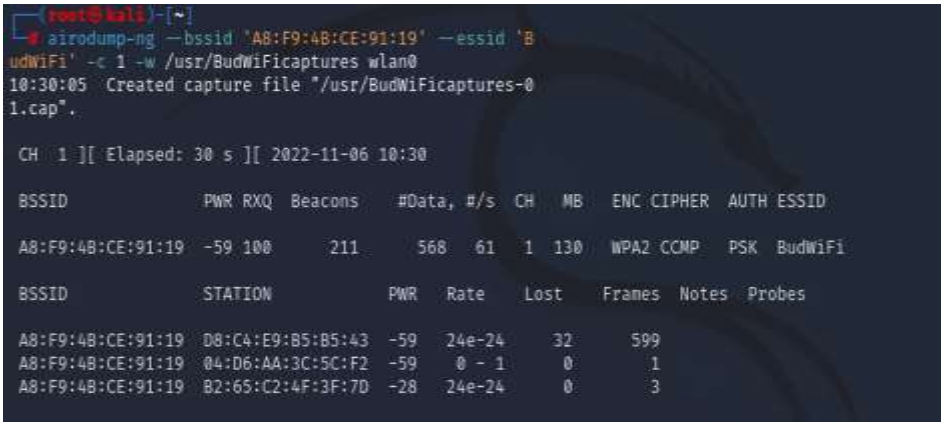

Рисунок 4

4. Необходимо ожидать некоторое время процесса захвата, в течение которого симулировать работу с устройств сотрудника и злоумышленника – обращаться к различным сетевым сервисам, открывать веб-страницы и т.п. Для того, чтобы полученный трафик было возможно расшифровать, должно произойти «рукопожатие» (*Handshake*) – подключение любого устройства к целевой *Wi-Fi* сети во время перехвата. Таким образом происходит общение клиента и роутера во время подключения, т.е., передача зашифрованного пароля во время аутентификации. В данном случае было произведено самостоятельное подключение к сети третьего устройства (рис. 5).

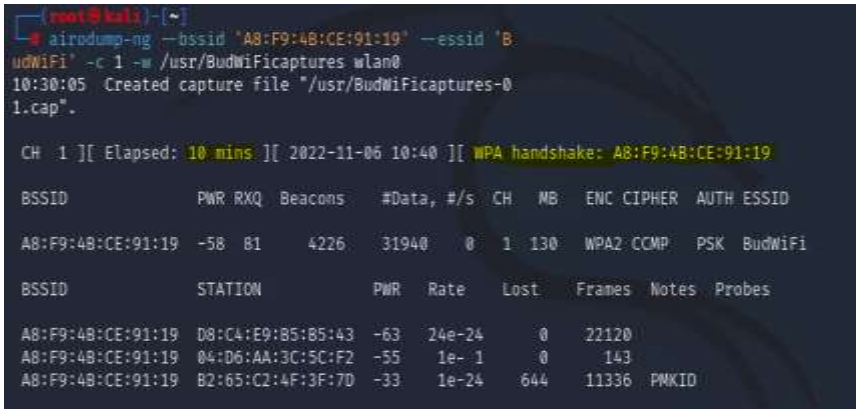

Рисунок 5

5. Для анализа полученного трафика необходимо открыть *Wireshark* и провести настройку для дешифрования: *Edit – Preferences – Protocols – IEEE* 802.11 *– Enable decryption – Edit...* (рис. 6).

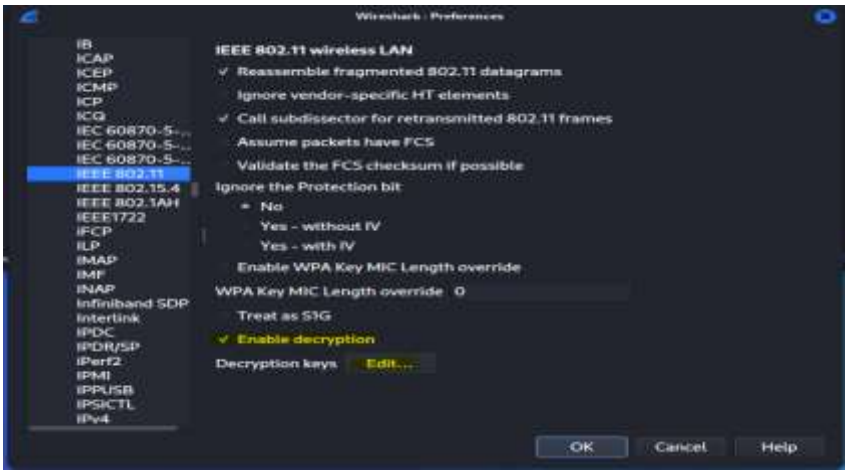

Рисунок 6

6. На данном этапе необходимо ввести пароль целевой *Wi-Fi* сети. В *Key type* нужно выбрать *wpa-pwd* для ввода пароля и имени сети в простом буквенном виде, после ввести данные в поле *Key* (рис. 7).

Рисунок 7

7. Далее необходимо открыть *.cap* файл, полученный с захвата трафика сети (рис. 8).

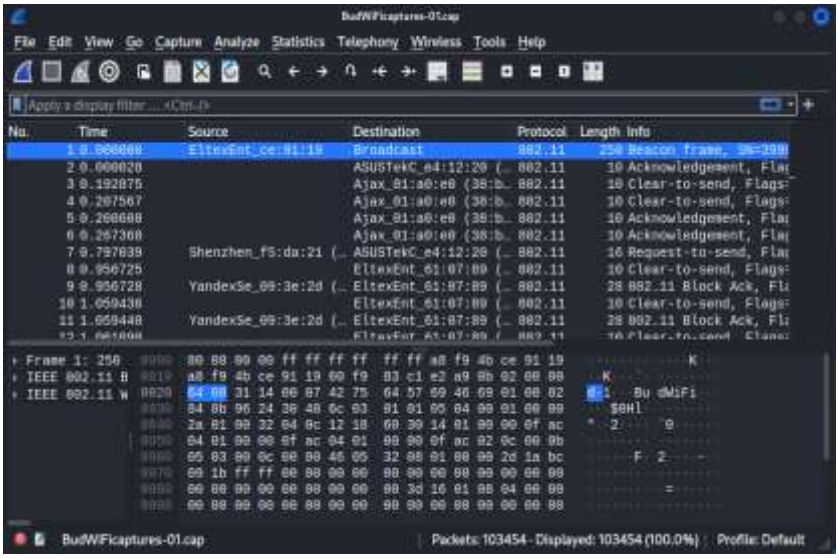

Рисунок 8

После специалистом производится анализ сетевого трафика на предмет нестандартных запросов и ответов, анализ *IP* и *MAC* адресов, обнаружение нескольких подключений с одних и тех же адресов, сопоставление адресов с запросами [19].

Признак присутствия в сети точки доступа с нелегитимным подключением

В ходе исследования был обнаружен признак, по которому можно определить, что в сети присутствует нелегитимное подключение через точку доступа, развернутую на легитимном устройстве. Данный способ уже на протяжении долгого времени используют операторы мобильной связи для предотвращения «раздачи» мобильного интернета клиентом несанкционированно подключенным устройствам [10]. Способ основан на анализе параметра пакета данных на сетевом уровне и полностью применим к исследуемой проблеме.

TTL (*Time To Live*) – это предельный период времени, за который пакет данных может существовать до своего исчезновения. На разных устройствах значения *TTL* разнятся. К примеру, на устройствах под управлением ОС *iOS* и *Android TTL* по умолчанию равен 64, на ПК и ноутбуках под ОС *Windows* – 128. Для описанного метода выявления нелегитимного подключения значение *TTL* в соответствии с типом устройства не играет большой роли [13].

При работе устройства в режиме точки доступа, всем пакетам сторонних подключенных к этой точке доступа устройств присваивается значение на единицу меньше соответствующего им *TTL*. Каждый переход через дополнительную точку доступа будет дальше уменьшать данный показатель. Если произойдет множество скачков от одного клиента к другому, значение станет равным 0 – в таком случае все данные в пакете уничтожатся. Рассмотрим ситуацию на примере исследованной схемы работы *TTL* (рис. 9).

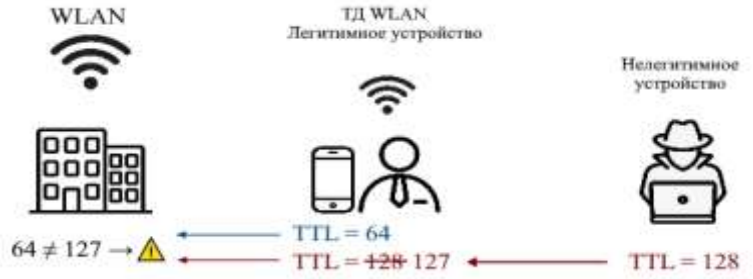

Рисунок 9

Если легитимное устройство не работает в режиме точки доступа *Wi-Fi* или работает в пассивном режиме (т.е. подключенные к нему сторонние устройства отсутствуют), то во всех заголовках соответствующих ему пакетах можно наблюдать одно и то же значение *TTL* (в данном случае – 64). Если же при анализе трафика обнаруживается несоответствие значений *TTL* в разных захваченных пакетах, и при этом *IP* и *MAC* адреса отправителей совпадают, то наверняка можно сделать вывод, что в сети присутствует нелегитимное подключение. В данном случае видно, что итоговые значения в разных пакетах – 64 и 127, соответственно, пакеты были отправлены с двух разных устройств, хотя их *IP* и *MAC* адреса совпадают [14].

После обнаружения подобного инцидента необходимо незамедлительно принять меры по его устранению. Следует зафиксировать данные отправителя и

сохранить пакеты, указывающие на инцидент, после чего немедленно прервать подключение устройства в режиме беспроводной прокси-станции к корпоративной *WLAN*-сети. По зафиксированным *IP* и *MAC* адресам можно выявить сотрудника, развернувшего точку доступа *Wi-Fi* [8].

Недостаток метода

Данный метод полностью соответствует методу обнаружения тетеринга (использования мобильного телефона в качестве точки доступа других устройств к услугам сети передачи данных оператора) операторами мобильной связи, поэтому обладает тем же недостатком, заключающемся в подмене значения *TTL* по умолчанию на нелегитимном устройстве. Рассмотрим ситуацию на примере исследованной схемы при подмене *TTL* (рис. 10).

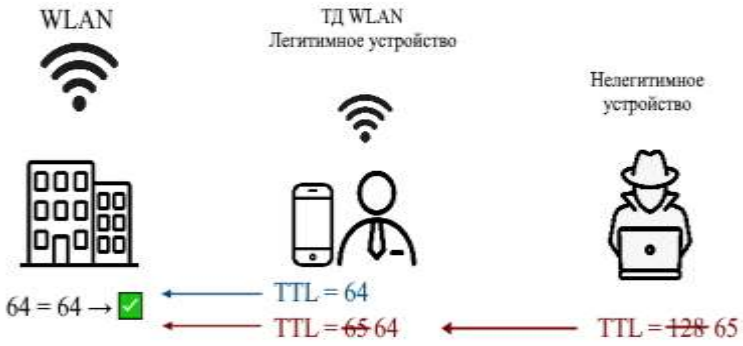

Рисунок 10

Для того, чтобы значение *TTL* соответствовало значению легитимного устройства после прохождения трафика к целевой *WLAN*, на нелегитимном устройстве устанавливается значение *TTL* устройства, работающего в режиме точки доступа с добавленной единицей. В данном случае *TTL* на легитимном устройстве равно 64, поэтому для соответствия значений на нелегитимном устройстве задается *TTL*, равный 65 по умолчанию. Таким образом, в анализируемом трафике во всех пакетах будет фигурировать одно и то же значение, соответствующее легитимному устройству, что полностью исключает обнаружение стороннего подключения к корпоративной *WLAN* данным методом [15].

Заключение

В статье рассмотрена проблема безопасности корпоративных *WLAN*, изучена уязвимость беспроводных корпоративных сетей при использовании в них беспроводных прокси-станций, приведены меры профилактики, а также предложена методика обнаружения использования данной уязвимости в сети. Методика позволяет выявить нелегитимное подключение к легитимному устройству, работающему в режиме точки доступа *Wi-Fi* и подключенному к корпоративной *WLAN*-сети, но только в случае, если на нелегитимном устройстве не проводилась подмена значения *TTL*. Для обеспечения безопасности корпоративных сетей необходимо внедрять данную методику, но также следует изучать и разрабатывать и другие способы предотвращения доступа к закрытым сетям. В будущих исследованиях планируется изучить возможность выявления подобных инцидентов и по другим признакам.

Литература

1. Ковцур М.М., Юркин Д.В., Герлинг Е.Ю., Ахрамеева К.А. Безопасность беспроводных локальных сетей – Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург, 2021. – С. 1.
2. Сергеев А.Н. Основы локальных компьютерных сетей. – Лань, 2022. – С. 1-2.
3. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах – М.: ДМК Пресс, 2011. – С. 2.
4. Петрова Т.В., Ковцур М.М., Карельский П.В., Поляничева А.В. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети // В книге: Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. Санкт-Петербург, 2022. – С. 2.
5. Кистружа А.Ю., Ковцур М.М., Оганесян А.Г. Исследование устойчивости точек доступа в режиме PSK к DOS атакам на беспроводную сеть // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей: в 4х томах. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург, 2021. – С. 2.
6. Ковцур М.М., Кириллов Д.И., Михайлова А.В., Потемкин П.А. Исследование подходов анализа трафика беспроводных сетей с использованием библиотеки Pandas // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей: в 4х томах. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург, 2021. – С. 2-3.
7. Юркин Д.Ю., Ворошнин Г.Е., Ковцур М.М., Мисливский Б.С. Исследование влияния атак Arpinject и Associationflood в беспроводных сетях на базе оборудования Mikrotik // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. – С. 3.
8. Дрепа В.Е., Кистружа А.Ю., Ковцур М.М., Кузьмина О.И., Петров В.А. Исследование метода Fingerprinting для определения местоположения беспроводного клиента IEEE 802.11 – Заметки ученого, 2022. – С. 8.
9. Докшин А.Д., Ковцур М.М., Прудников С.В., Таргонская А.И. Исследование подходов для аутентификации пользователей беспроводной сети с применением различных LDAP решений // Наукоемкие технологии в космических исследованиях Земли, 2021. – С. 4.
10. Steffen Schulz, Hossen A. Mustafa, Wenyuan Xu, Ahmad-Reza Sadeghi, Maria Zhdanova, Vijay Varadharajan Tetherway: A Framework for Tethering Camouflage // Conference: Wireless Network Security (WiSec), 2012. – С. 7-9.
11. Kovtsur M.M., Muthanna A., Karelsky P., Kozmyan A., Voroshnin G., Al-Khafaji H.M.R. IPTV access methods with RADIUS-server authorization // Journal of Information Technology Management, 2022. – С. 7-9.
12. Анализ безопасности корпоративной беспроводной сети // Habr URL https://habr.com/ru/articles/427393/ (дата обращения – март 2023 г.). – С. 2-3.
13. Я всегда с собой беру… // Habr URL https://habr.com/ru/companies/ruvds/articles/598493/ (дата обращения – апрель 2023 г.). – С. 7-9.
14. Что такое TTL и как с его помощью обхитрить провайдера // IT Knowledge Base URL https://disnetern.ru/ttl/ (дата обращения – апрель 2023 г.). – С. 7-9.

15. Как изменить TTL в Windows 10 и раздать безлимитный интернет со смартфона на компьютер // Timeweb Community URL https://timeweb.com/ru/community/articles/kak-izmenit-ttl-v-windows-10-i-razdat-bezlimitnyy-internet-so-smartfona-na-kompyuter (дата обращения – апрель 2023 г.). – С. 7-9.
16. Герлинг Е.Ю., Зебзеев Е.А., Киструга А.Ю. Разработка метода анализа трафика беспроводной сети на базе WPA2 ENTERPRISE // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. – С. 4-7.
17. 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. 4-7.
18. Коцыняк М.А., Бударин Э.А., Карпов М.А., Муртазин И. Р., Иванов Д. А. Воздействие нарушителя на беспроводные сети передачи данных по уровням эталонной модели взаимодействия открытых систем // В сборнике: Состояние и перспективы развития современной науки по направлению информационная безопасность. Анапа, 2020. – С. 4.
19. Новиков П.А., Лепешкин О.М., Шуравин А.С., Бударин Э.А. Модель сетевого мониторинга защищенности сети передачи данных // В сборнике: Неделя науки СПбПУ. Санкт-Петербург, 2020. – С. 4-7.

ИССЛЕДОВАНИЕ ВЛИЯНИЯ АТАК НА БЕСПРОВОДНЫЕ СЕТИ WI-FI 6E

***М.М. Ковцур**, к.т.н., Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, maxkovzur@mail.ru;*
***С.А. Винников,** Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, vinnikovsema@mail.ru;*
***В.И. Трезоров**, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, trezorov.v.i@yandex.ru;*
***А.Ю. Киструга,** Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, anton.kistruga@gmail.com.*

УДК 004.056.53

Аннотация. В данной работе рассматривается влияние различных атак на функционирование беспроводной сети, работающей на базе стандарта *IEEE* 802.11*ax*. В результате исследования сделан вывод об актуальности некоторых существующих распространенных атак для сетей *Wi-Fi* 6*E*.

Ключевые слова: *Wi-Fi; Wi-Fi* 6*E*; *IEEE* 802.11*ax*; атаки на беспроводные сети.

INVESTIGATION OF THE IMPACT OF ATTACKS ON WI-FI 6E WIRELESS NETWORKS

***M.M. Kovtsur,** Ph.D., St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich;*

S.A. Vinnikov, *St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich;*
V.I. Trezorov, *St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich;*
A.Y. Kistruga, *St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich.*

***Annotation*.** This paper examines the impact of various attacks on the functioning of a wireless network based on the *IEEE* 802.11*ax* standard. The study concludes the relevance of some existing common attacks to *Wi-Fi* 6*E* networks.

***Keywords*:** *Wi-Fi; Wi-Fi* 6*E*; *IEEE* 802.11*ax*; attacks on wireless networks.

Введение

Благодаря развитию мобильных электронно-вычислительных устройств особое распространение получила реализация технологий беспроводной передачи данных, известная как «*Wi-Fi*». *Wi-Fi* частично реализует технологии, описанные в стандарте *IEEE* 802.11 и во множестве поправок к нему. В настоящее время последней широко распространенной поправкой является поправка *IEEE* 802.11*ax*, получившая название «*Wi-Fi* 6*E*». В сетях *Wi-Fi* следует руководствоваться принципами информационной безопасности, которые состоят в обеспечении конфиденциальности и целостности информации, а также доступа к этой информации. Эти принципы могут быть нарушены злоумышленниками, использующими уязвимости указанных беспроводных сетей. В связи с этим вопрос безопасности беспроводных сетей всегда остается актуальным [1].

По статистике Лаборатории Касперского, представленной на рис. 1, за февраль 2023 г. сетевые атаки составили 6% от общего числа киберугроз [2].

Рисунок 1

Количество произведенных устройств, поддерживающих последнее поколение сетей *IEEE* 802.11*ax*, растет с каждым годом (рис. 2) [3]. Изучению беспроводных сетей посвящено достаточно много статей [4-7], однако в них не

исследовался стандарт *IEEE* 802.11*ax*. Цель данной работы заключается изучении влияния атак на *Wi-Fi* 6*E*.

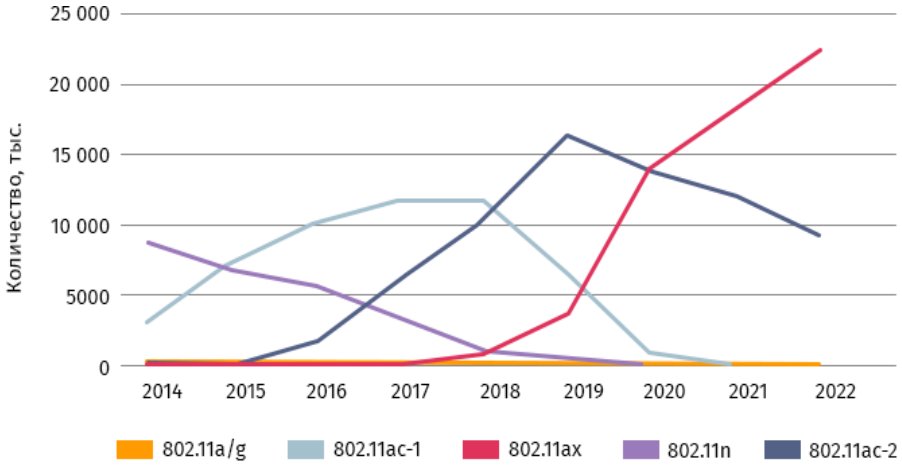

Рисунок 2

Атака деаутентификации

Чтобы выяснить, чем *IEEE* 802.11*ax* отличается от других стандартов *IEEE* 802.11 в контексте безопасности и какие угрозы остались актуальными, следует обратиться к официальному документу от организации *IEEE*. Данный стандарт вводит новый частотный диапазон 6 ГГц и запрещает для него использование некоторых *pre-RSNA* (*WEP, Shared Key Authentication, Open System Authentication without encryption*) и *RSNA* (*WEP, TKIP*) алгоритмов, а также добавляет обязательную защиту кадров управления [8].

Для частотных диапазонов 2,4 ГГц и 5 ГГц в контексте безопасности не было добавлено улучшений, из чего можно сделать предположение, что популярные атаки остаются актуальными для последнего поколения сетей. Чтобы проверить это, была реализована атака деаутентификации. Выбор атаки обусловлен простотой ее реализации и тем, что она дополняет атаку *Evil Twin* [4].

Принцип действия атаки представлен на рис. 3. Имеется точка доступа и пользователи, которые к ней подключены. Во время атаки злоумышленник отправляет на точку доступа кадры деаутентификации, после чего соединение между клиентами и точкой доступа обрывается. Для подключения требуется повторное прохождение аутентификации. Если отправлять кадры безостановочно, то это вызовет отказ в обслуживании точки доступа [9].

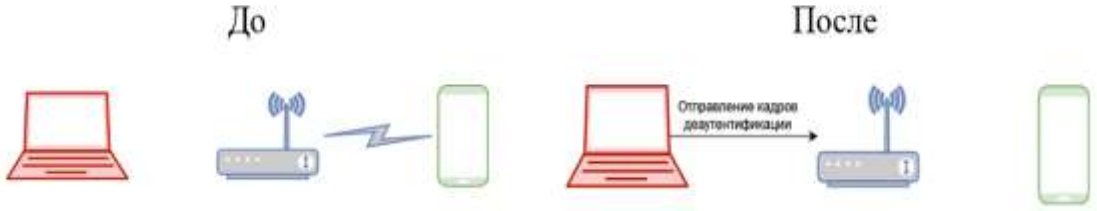

Рисунок 3

Из дампа на рис. 4, видно, что после отправки на точку доступа кадров деаутентификации клиентское устройство заново отправляет кадры

аутентификации и ассоциации, что говорит о том, что соединение было разорвано, и атака прошла успешно.

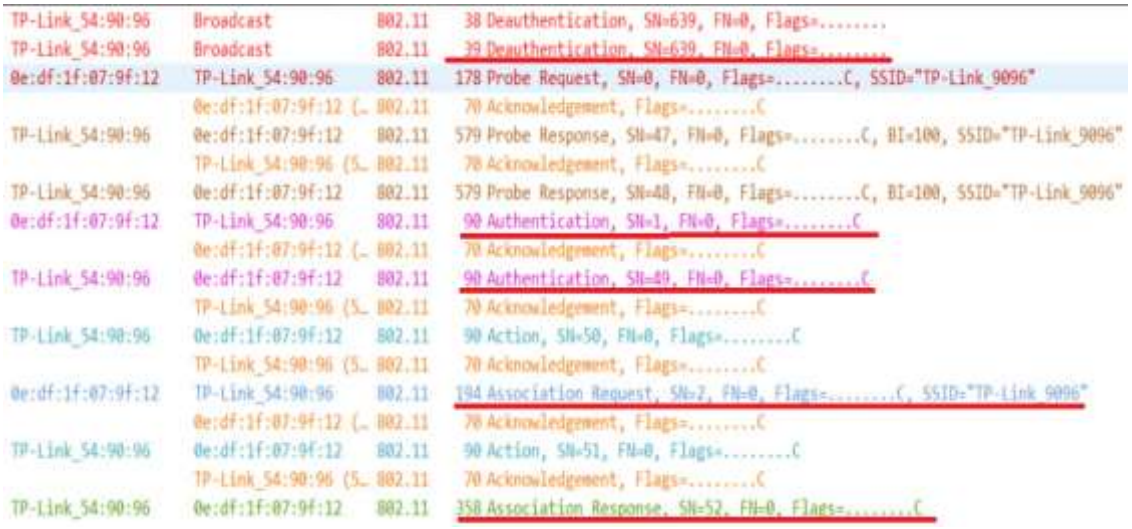

Рисунок 4

Поколение *Wi-Fi* 5 в корпоративных сетях

По данным исследования «Внедрение нового стандарта *Wi-Fi* 6 в России» от «*T*1 Интеграция», *Huawei* и *GlodalCIO*|*DigitalExperts* [10] на момент 2021 г. лишь в 10% организаций было введено новое поколение сетей. Решение о выделении диапазона 5,9-6,4 ГГц в России было принято лишь в декабре 2022 г. Поскольку большая часть корпоративных сетей базируется на *Wi-Fi* 5, новый частотный диапазон 6 ГГц остается недоступным для инфраструктуры. В связи с этим большую угрозу представляют атаки, основанные на создании поддельных точек доступа.

Атака *Evil Twin*

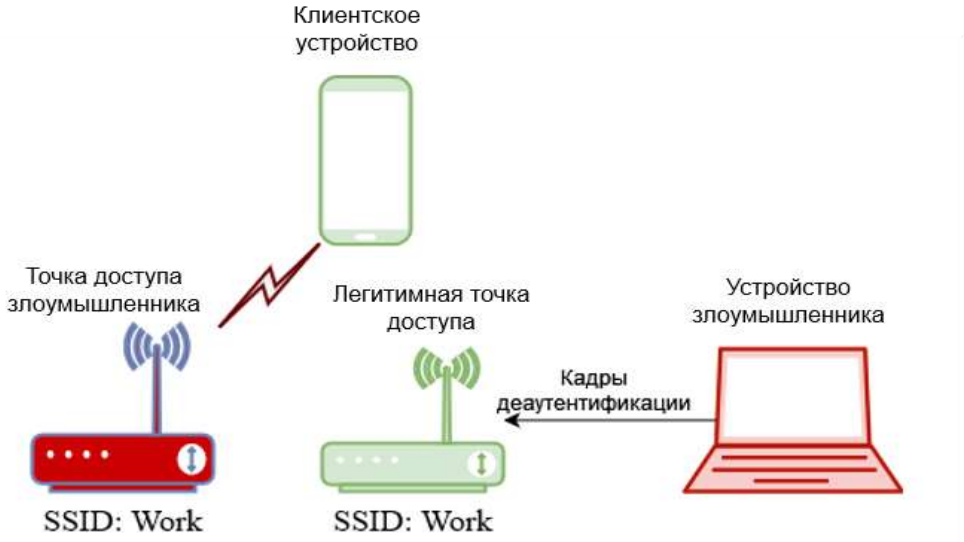

Рисунок 5

На рис. 5 представлена схема атаки «злой двойник». Злоумышленник создает точную копию легитимной точки доступа, к которой в дальнейшем

подключается клиент, тем самым давая атакующему доступ к конфиденциальной информации. Атака деаутентификации дополняет злого двойника, вызвав отказ в обслуживании легитимной точки доступа, чтобы пользователь с большей вероятностью подключился к двойнику.

Главная угроза заключается в новом частотном диапазоне. На рынке представлены точки доступа, способные работать на 6 ГГц, также новейшие пользовательские устройства, поддерживающие *Wi-Fi* 6*E*, но как было сказано выше, корпоративное сетевое оборудование не поддерживает данный диапазон, поэтому обнаружить угрозу становится затруднительно.

На данный момент существует три возможных способа обнаружения нелегитимной точки доступа согласно разделу 11 официальной поправки *IEEE* 802.11*ax* [7]:

1. Пассивное сканирование внутри диапазона. Обнаружение кадров *FILS* и незапрашиваемых кадров *Probe Response*. Они представляют из себя уменьшенные маячковые кадры и на их обработку уходит меньше времени (6ГГц).
2. Активное сканирование внутри диапазона. Сканирование предпочтительных каналов (5, 21, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213 и 229). Выбор каналов обусловлен тем, что они выступают в качестве основного для объединения каналов в 80 МГц (6 ГГц) [11].
3. Обнаружение совместно расположенных точек доступа с помощью *Reduced Neighbor Report* вне диапазона (5 ГГц).

Заключение

Рассмотрена официальная поправка для *Wi-Fi* 6*E* от *IEEE*. Протестирована атака деаутентификации на оборудовании *TP-Link*. Результаты показали, что атаки остаются актуальными для сетей последнего поколения и оказывают негативное влияние на работоспособность. Рассмотрена угроза нового частотного диапазона 6 ГГц: основная проблема заключается в том, что оборудование в корпоративных сетях базируется на *Wi-Fi* 5 и не работает на 6 ГГц. Перечислены способы обнаружения атаки «злой двойник».

Литература

1. Кирилова К.С. Проблема обезвреживания руткитов уровня ядра в системах специального назначения // I-methods, 2020. – Т. 12. – № 3. – С. 1-9.
2. Consumer WLAN Infrastructure // 650 group URL: https://650group.com/reports/consumer-wlan infrastructure/ (дата обращения: 21.02.2023).
3. Serure list // Kaspersky URL: https://statistics.securelist.com/ru/intrusion-detection-scan/month (дата обращения: 28.02.2023).
4. Кистружа А.Ю., Ковцур М.М., Оганесян А.Г. Исследование устойчивости точек доступа в режиме PSK к DOS атакам на беспроводную сеть // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей: в 4х томах. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Санкт-Петербург, 2021. – С. 485-489.
5. Кистружа А.Ю., Ковцур М.М., Петров М.П., Шабанов В.П. Методика обнаружения местоположения нарушителя, реализующего атаку деаутентификации на сеть IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-

техническая и научно-методическая конференция // Сборник науч. ст. в 4-х т. СПб.: СПбГУТ, 2022. – С. 561-564.
6. Balueva A., Desnitsky V., Ushakov I. Approach to detection of denial-of-sleep attacks in wireless sensor networks on the base of machine learning, 2020. – Т. 868. – С. 350-355.
7. Ушаков И.А., Котенко И.В., Овраменко А.Ю., Преображенский А.И., Пелевин Д.В. Комбинированный подход к обнаружению инсайдеров в компьютерных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2020. – № 4. – С. 66-71.
8. 802.11ax-2021 - IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN // IEEE STANDARTS ASSOCIATION URL:https://ieeexplore.ieee.org/document/9442429 (дата обращения: 05.02.2023).
9. Deauthentication // Aircrack-ng URL: http://aircrack-ng.org/doku.php?id=deauthentication (дата обращения: 20.02.2023).
10. T1 Интеграция, Huawei, Global CIO: крупный бизнес не спешит переходить на Wi-Fi 6 // T1 Интеграция URL: https://t1-integration.ru/press/news/t1-integratsiya-huawei-i-global-cio-krupnyy-biznes-ne-speshit-perekhodit-na-wi-fi-6-/(дата обращения: 21.02.2023).
11. Architecting Next Generation Wireless Network with Catalyst Wi-Fi 6E Access Points // Cisco Live URL: https://www.ciscolive.com/c/dam/r/ciscolive/global-event/docs/2022/pdf/BRKEWN-2024.pdf (дата обращения: 23.02.2023).
12. Ахрамеева К.А., Ворошнин Г.Е., Ковцур М.М. Исследование уязвимостей оборудования mikrotik к атакам на беспроводные сети // X Международная научно-техническая и научно-методическая конференция. Сборник науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. – С. 57-64.
13. Герлинг Е.Ю., Кулишкина Е.И., Бирих Э.В., Виткова Л.А., Модели нарушителей информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности, 2017. – Т. 35. – № 1. – С. 27-30.
14. Юркин Д.В. Системы обнаружения вторжений в сетях широкополосного радиодоступа стандарта IEEE 802.11 // Информационно-управляющие системы, 2014. – № 2 (69). – С. 44-49.
15. Миняев А.А. Метод и методика оценки эффективности системы защиты территориально-распределенных информационных систем // Информатизация и связь, 2020. – № 6. – С. 29-36.
16. Ахрамеева К.А., Ворошнин Г.Е., Ковцур М.М. Исследование устойчивости оборудования mikrotik к атаке association flood на беспроводную сеть семейства ieee 802.11 // Региональная информатика и информационная безопасность.: Сб. трудов. СПб.: СПбГУТ, 2021. – С. 354-358.
17. Герлинг Е.Ю., Модели нарушителей информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности, 2017. – Т. 35. – С. 27-30.

ИССЛЕДОВАНИЕ АКТУАЛЬНОГО ИНСТРУМЕНТАРИЯ KALI LINUX ДЛЯ ПРОВЕДЕНИЯ ТЕСТОВ НА ОЦЕНКУ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ

М.М. Ковцур, *к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, maxkovzur@mail.ru;*
А.А. Миняев*, к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, minyaev@gmail.com;*
В.А. Цыганов*, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, cyganov.vladimir.@gmail.com.*

УДК 004.056.5

Аннотация. В настоящее время актуальность безопасности в проводных и беспроводных сетях является одним из самых важных вопросов в сфере информационной безопасности. Многие организации используют для проверки сетей операционную систему *Kali Linux.* Она предназначена для проведения тестов на оценку безопасности, в том числе беспроводных сетей. В состав инструментов *Kali Linux* входит несколько инструментов, работающих как из командной строки, так и из базового графического интерфейса. Эти инструменты можно использовать для перевода сетевого интерфейса в режим перехвата беспроводного трафика. В данной работе представлены результаты исследований актуального инструментария в *Kali Linux* для проведения тестов на оценку безопасности беспроводных сетей.

Ключевые слова: *Kali Linux*; набор инструментов; тест на проникновение; несанкционированный доступ; проверка безопасности; сеть.

EXPLORING THE LATEST KALI LINUX TOOLKIT FOR CONDUCTING REVERSE SECURITY TESTS FOR WIRELESS NETWORKS

Maxim Kovtsur, *Ph.D., Associate Professor, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich;*
A.A. Minyaev*, Ph.D., Associate Professor, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich;*
V.A. Tsyganov*, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich.*

Annotation. Currently, the relevance of security in wired and wireless networks is one of the most important issues in the field of information security. Many organizations use the Kali Linux operating system to check networks. It is designed to conduct tests for conducting security assessment tests, including wireless networks. The Kali Linux tools include several tools that work both from the command line and from the basic graphical interface. These tools can be used to switch the network interface to wireless traffic interception mode. This paper presents the results of research on the current tools in Kali Linux for conducting tests to assess the security of wireless networks.

Keywords: Kali Linux; toolset; pentesting; unauthorized access; security check; network.

Введение

Беспроводные сети являются одним из наиболее уязвимых компонентов в сфере информационной безопасности. Это связано с тем, что они работают на открытых частотах и могут быть доступны для любого желающего. Кроме того, многие беспроводные сети не защищены должным образом, что делает их уязвимыми для атак.

Инструментарий *Kali Linux*

Kali Linux – дистрибутив *Linux*, специально разработанный для тестирования на проникновение и оценку безопасности. Кроме того, *Kali Linux* содержит большой набор инструментов для тестирования беспроводных сетей.

Из публикаций Храмцова Д.О., Миняева А.А. [1-2] была выявлена проблема в использовании устаревшего инструментария *Kali Linux* для проведения тестов на проникновение.

Целью проведения исследования является выявление актуальных инструментов для проведения тестирований беспроводных сетей.

Задачами являются рассмотрение стандартных инструментов *Kali Linux* и их виды атак, а также проведение анализа популярности запросов в поисковой системе *Yandex* среди пользователей.

В данном исследовании были рассмотрены инструменты, которые идут по умолчанию в *Kali Linux.* Ниже представлена таблица, в которой указан инструмент и его вид атаки на беспроводную сеть. В табл. 1 приведены инструменты и виды их атак.

Таблица 1.

Инструмент	Вид атаки
Airgeddon	Деаутентификация и извлечение хеша (*WPA/WPA*2/*PSK*) трафика
Airmon-ng	Управление беспроводными интерфейсами (перевод в режим мониторинга)
Airserv-ng	Запуск сервера для захвата пакетов
Airodump-ng	Сбор информации о беспроводных сетях
Bully	Атака на *WPS* (брут-форс *WPS*)
Cowpatty	Атака на протокол *WPA/WPA*2
Fern Wifi Cracker	Атака на *WEP/WPA/WPA*2 с помощью словаря
GISKismet	Сбор информации о беспроводных сетях
Hostapd-wpe	Создание ложной точки доступа с поддержкой *WPE*
Iw	Управление беспроводными интерфейсами
Kismet	Сбор информации о беспроводных сетях
Kismetdb	Сбор информации о беспроводных сетях

Инструмент	Вид атаки
Mdk3	Отказ в обслуживании (*DoS*)
Minidwep-gtk	Атака на *WEP*-защищенные сети
Pixiewps	Атака на *WPS*-защищенные беспроводные сети
Pyrit	Атака на *WPA/WPA2-PSK* сети
Reaver	Атака на *WPS*-защищенные беспроводные сети
Wifiphisher	Фишинговая атака на беспроводные сети
Wifite	Атака на *WEP, WPA/WPA2-PSK* сети

После изучения базовых инструментов *Kali Linux* и видов атак, было проведено исследование по оценке актуальности каждого инструмента с помощью сервисов *Wordstat.yandex.* и *Google Trands*. Данные сервисы показывают статистику запросов в поисковой системе *Yandex* и *Google* за последний месяц. В табл. 2 представлена статистика запросов в поисковой системе *Yandex* за период 09.03.2023-09.04.2023.

Таблица 2.

Инструмент	Количество запросов в поисковой системе *Yandex,* шт.
Airgeddon	627
Airmon-ng	618
Airserv-ng	2
Airodump-ng	549
Bully	97
Cowpatty	182
Fern Wifi Cracker	384
GISKismet	2
Hostapd-wpe	19
Iw	70
Kismet	4823
Mdk3	118
Minidwep-gtk	9

Инструмент	Количество запросов в поисковой системе *Yandex*, шт.
Pixiewps	352
Pyrit	667
Reaver	349
Wifiphisher	1601
Wifite	3535

В табл. 3. Представлена статистика запросов в поисковой системе *Google* за период 09.03.2023-09.04.2023.

Таблица 3.

Инструмент	Количество запросов в поисковой системе *Google*, шт.
Airgeddon	329
Airmon-ng	518
Airserv-ng	0
Airodump-ng	385
Bully	33
Cowpatty	71
Fern Wifi Cracker	201
GISKismet	0
Hostapd-wpe	4
Iw	43
Kismet	961
Mdk3	322
Minidwep-gtk	11
Pixiewps	352
Pyrit	667
Reaver	349

Инструмент	Количество запросов в поисковой системе *Google*, шт.
Wifiphisher	774
Wifite	1011

По результатам сбора статистики запросов в поисковых системах *Yandex* и *Google* (табл. 2, табл. 3) были составлены гистограммы, в которых наглядно представлены результаты статистики запросов в поисковых системах *Yandex* и *Google* за период 09.03.2023-09.04.2023. На рис. 1 представлена гистограмма по количеству запросов в поисковой системе *Yandex* за период 09.03.2023-09.04.2023.

Рисунок 1

На рис. 2 представлена гистограмма по количеству запросов в поисковой системе *Google* за период 09.03.2023-09.04.2023.

Рисунок 2

На рис. 3 представлена гистограмма по количеству запросов в поисковой системе *Google* и *Yandex* за период 09.03.2023-09.04.2023.

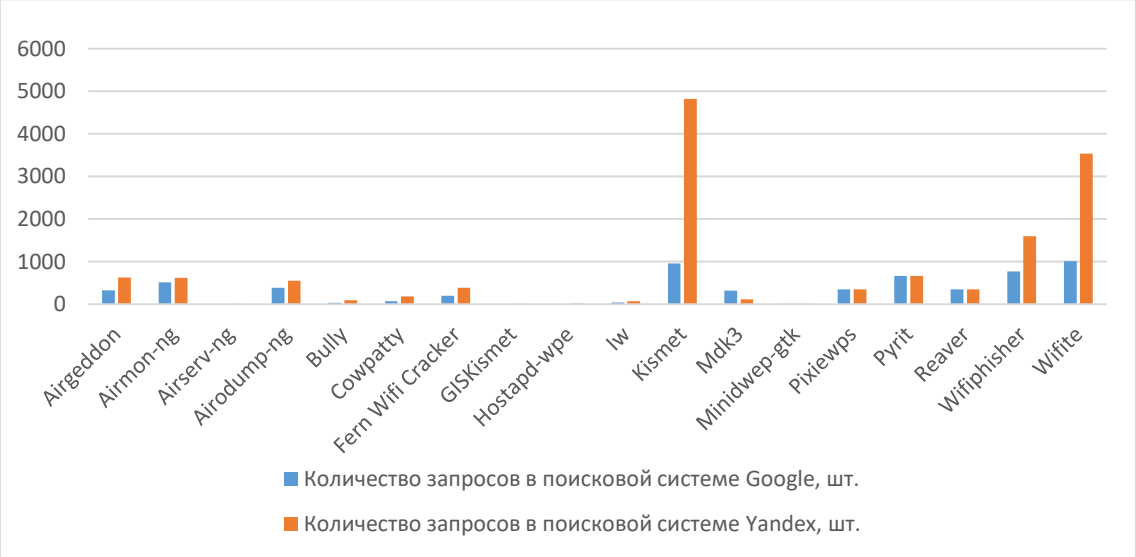

Рисунок 3

Заключение

Исходя из проведенного исследования сделан вывод, о том, что одними из актуальных инструментов для проведения тестов на безопасность сетей являются *Kismet, Wifite, Wifiphisher*. Для выполнения поставленной цели выявление актуальных инструментов для проведения тестирований беспроводных сетей были выполнены соответствующие задачи рассмотрения стандартных инструментов *Kali Linux* и видов их атак, а также проведения анализа популярности запросов в поисковой системе *Yandex* среди пользователей.

Литература

1. Буянов Д.С. Информационная безопасность в социальных сетях. Молодой ученый, 2018. – № 39 (225). – С. 14-16. (дата обращения: 09.04.2023).
2. Храмцова Д.О., Миняева А.А. Проблемы безопасности, связанные с использованием сетей семейства стандартов IEEE 802.11, информационная безопасность регионов России (ИБРР-2021). – С. 395. (Дата обращения: 09.04.2023).
3. Balueva A., Desnitsky V., Ushakov I. Approach to detection of denial-of-sleep attacks in wireless sensor networks on the base of machine learning. Studies in Computational Intelligence, 2020. – 868. – С. 350-355.
4. Герлинг Е.Ю., Зебзеев Е.А., Киструга А.Ю. Разработка метода анализа трафика беспроводной сети на базе WPA2 ENTERPRISE // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. – С. 334-339.
5. Федорова А.Э., Герлинг Е.Ю., Ахрамеева К.А., Андрианов В.И. Разработка структуры веб-интерфейса для системы анализа трафика беспроводной сети // Информационная безопасность регионов России (ИБРР-2021). Материалы XII Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 2021. – С. 394.

6. Штеренберг С.И., Москальчук А.И., Красов А.В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения. Информационные технологии и телекоммуникации, 2021. – Т. 9. – № 1. – С. 47-58.
7. Дрепа В.Е., Киструга А.Ю., Ковцур М.М., Кузьмина О.И., Петров В.А. Исследование метода FINGERPRINTING для определения местоположения беспроводного клиента IEEE 802.11 // Заметки ученого, 2022. – № 3-2. – С. 137-141.

РАЗРАБОТКА КОНЦЕПЦИИ ЗАЩИЩЕННОГО ЦЕНТРАЛИЗОВАННОГО ВЗАИМОДЕЙСТВИЯ РАСПРЕДЕЛЕННЫХ УСТРОЙСТВ

М.М. Ковцур, *к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, maxkovzur@mail.ru;*
А.А. Браницкий, *к.т.н., Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, branitskiy@comsec.spb.ru;*
Н.И. Казаков, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, kazakov.ni2.18@gmail.com.*

УДК 004.057.4

Аннотация. С растущим количеством веб-сервисов возникают вопросы обеспечения безопасности передачи данных между клиентом и сервером. В данной статье рассматривается организация защищенной передачи данных в сети, состоящей из сенсоров и центрального сервера под управлением одного лица. Рассмотрены механизмы защиты с сессионного уровня и выше.

***Ключевые слова*:** централизованная сеть; *REST API*; веб-сертификаты; *JWT*.

DEVELOPMENT OF A CONCEPT OF CENTRLALIZED NETWORKING OF DISTRIBUTED DEVICES

Maxim Kovtsur, *Ph.D., Associate Professor, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich;*
Aleksandr Branitskiy, *Ph.D., St. Petersburg Federal Research Centerof the Russian Academy of Sciences (SPC RAS);*
Nikita Kazakov, *St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich.*

Annotation. With the growing number of web services, there are questions about the security of data transmission between the client and the server. This article discusses the organization of secure data transmission in a network consisting of sensors and a central server managed by one person. Protection mechanisms from the session level and above are considered.

Keywords: centralized network*; REST API;* web-certificates; *JWT*.

Введение

В современном мире растет количество больших распределенных систем, применяемых, в частности, в Интернете вещей и облачных сервисах [1-5]. Это порождает вопрос обеспечения безопасной передачи данных в сети таких систем

[6,7]. Подавляющее большинство систем используют клиент-серверную архитектуру, в которой множество клиентов отправляют запросы к центральному серверу, на котором работает определенное приложение. Помимо этого, распространение получили сети сенсоров, также состоящие из множества микрокомпьютеров, которые собирают, обрабатывают и передают данные центральному серверу, который осуществляет дополнительную обработку, агрегацию и их хранение. Такие сети могут отслеживать физические характеристики среды (освещенность, влажность, температура), уровень излучения на различных частотах, а также информацию о беспроводных сетях. Ее в дальнейшем можно использовать для улучшения характеристик беспроводной сети (исключение «слепых зон»), обнаружения вторжений и контроля местоположения легинтимных клиентов. В данной работе рассматривается подход к организации передачи данных приложений высокого уровня в сети сенсоров с центральным сервером.

В существующих исследованиях [8] организация предлагаемой системы описана не полно. Существуют работы, исследующие отдельные механизмы защиты на разных сетевых уровнях [9-11] и приводящие их сравнение [12, 13], а также предлагающие новые механизмы [14-16]. Однако они не предоставляют полного решения по обеспечению защищенного взаимодействия.

Подавляющая масса приложений высокого уровня используется для передачи данных *HTTP* [8]. Приложение исследуемой сети построено с использованием концепции *REST API*. *REST* (*Representational State Transfer*) – это концепция построения сетевого взаимодействия сервисных компонентов. Ее основными принципами является отсутствие состояния, модель клиент-сервер и единообразие интерфейса как модели взаимодействия. Передача данных в *REST* осуществляется с помощью *HyperText Transfer Protocol* (*HTTP*). Однако, так как сам по себе *HTTP* никак не защищен, вместо него рекомендуется применять *HTTPS* (*HTTP Secure*). Он добавляет поддержку шифрования и обеспечивает защиту от атак прослушивания сетевого трафика.

Так как протокол *HTTPS* сам по себе подвержен атакам *Man in the Middle* (*MITM*), для организации безопасной передачи данных от сенсоров к серверу и минимизации рисков внешнего вмешательства в сеть предлагается использовать следующий комплекс мер:

1) *HTTPS*;
2) двухсторонняя аутентификация подключения по сертификатам;
3) токены с возможностью отзыва.

HTTPS – протокол передачи гипертекста поверх криптографических протоколов *SSL/TLS*. Он обеспечивает достаточную защиту передаваемой информации при условии корректной авторизации и проверки сертификатов. Так как все сертификаты и серверы, и сенсоры в исследуемой системе будут контролироваться одним лицом, данные уязвимости можно считать неактуальными.

Авторизация сервера и сенсоров осуществляется с помощью сертификатов, выпущенных одним Центром Сертификации (ЦС) или цепочкой доверенных ЦС. В первую очередь, создается корневой сертификат организации. Затем с помощью него по цепочке выпускаются сертификаты доверенных серверов, к которым уже обращаются клиенты. Сертификаты клиентов так же должны быть выпущены корневым ЦС или доверенными ЦС.

С точки зрения сенсора достоверность сервера подтверждается доверенностью его сертификата – он должен быть выпущен тем же ЦС, что и сертификат сенсора. Для аутентификации сенсора с точки зрения сервера используется аналогичная проверка – сенсор при подключении предоставляет свою цепочку сертификатов, а сервер проверяет корректность цепочки и то, что сертификат выдан доверенным ЦС [17]. Таким образом реализуется двухсторонняя аутентификация.

Для контроля сессии после аутентификации и оптимизации повторных подключений предлагается использовать токены. Одним из наиболее распространенных видов токенов являются *JSON Web Token* (*JWT*).

JWT – это набор информации в формате *JSON*, который опционально может быть зашифрован и подписан. Он считается безопасным способом передачи данных между двумя участниками.

Для создания *JWT* токена используются:

- заголовок (*header*), содержащий общую информацию о токене;
- полезные данные (*payload*), которые включают в себя информацию о пользователе и его авторизационные данные;
- подпись (*signature*).

Все элементы записаны в формате *JSON*, закодированы в *base*64 и объединены через точку. Пример готового токена:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYW1lIjoidGVzdCJ9.ml0QsTms3K9wMygTu41ZhKlTyjmW9zHQtoS8FusCCjU

Выпущенный и подписанный токен прикрепляется к отправляемым запросам. Сервер при приеме такого запроса до обработки может проверить, что в токене содержатся корректные идентифицирующие клиента данные, а также проверить подпись, сравнив ее с собственной, которую он вычисляет хэшированием. При совпадении сервер делает вывод о том, что запрос поступил действительно от того клиента, которому изначально был выдан токен.

JWT хранит в себе всю информацию о клиенте и не сохраняет состояния (*stateless*). Дополнительной мерой защиты в таком случае может являться сохранение сгенерированных токенов [18] в базе данных (БД) сервера, их текущего состояния и времени истечения. Это позволит вести полный учет всех подключений и самостоятельно отзывать токены до срока их истечения. Схема взаимодействия компонентов в такой системе представлена на рис. 1. При успешном запросе сервер отправляет статус 200. Если клиент получает в ответ статус 403 *Forbidden*, это означает, что предоставленный токен не валиден и клиент должен авторизоваться заново.

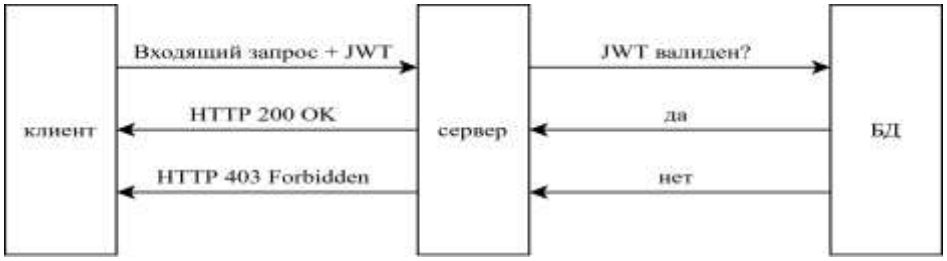

Рисунок 1

Для ускорения повторных авторизаций предлагается использовать *Refresh token*. Это долгоживущий одноразовый токен, который позволяет получить новую пару токенов без ввода аутентификационных данных. На рис. 1 показана схема проверки валидности токена.

Рассмотрим практическую реализацию предлагаемой схемы. Для этого созданы и объединены в сеть виртуальные машины сервера и сенсоров. На рис. 2 представлена схема собранного стенда.

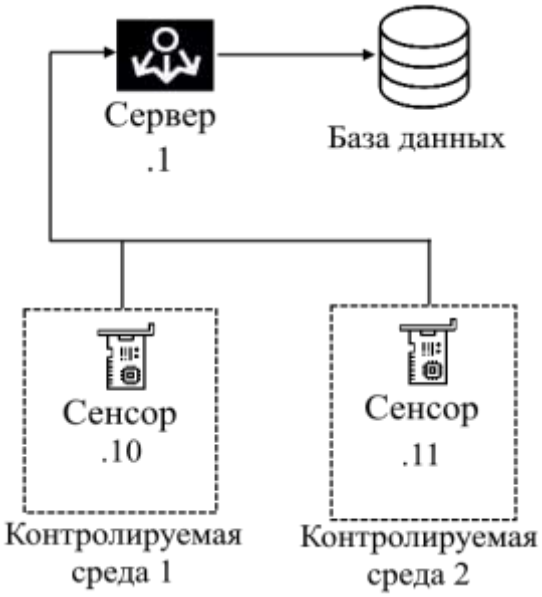

Рисунок 2

Для создания стенда использованы следующие инструменты:

- *Python* – основной язык приложений сервера и клиента.
- *Flask* – веб-фреймворк со встроенным сервером.
- *Ubuntu* – операционная система, на которой развернуты сервер и клиент.
- *Vmware* – платформа виртуализации.

В реализованной схеме клиент собирает определенную информацию, включая параметры загрузки *CPU* и *RAM* своей системы, статистику по окружающим беспроводным сетям, и в виде *POST*-запроса отправляет ее на сервер с определенной периодичностью.

Заключение

В результате данной работы описан подход к организации защищенного взаимодействия в сети, состоящей из сенсоров и центрального сервера. Конфиденциальность и целостность данных предлагается обеспечивать с помощью использования *HTTPS*. Для двухсторонней аутентификации предлагается использовать механизм сертификатов. Контроль сессий предлагается обеспечивать с помощью *JWT*. Собран стенд и реализованы описанные механизмы защиты. Если в полной мере осуществляется контроль выпуска доверенных сертификатов и контроль чтения из базы данных, система демонстрирует высокий уровень защищенности.

Литература

1. Василишин Н.С., Ушаков И.А., Котенко И.В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // Информационные технологии в управлении (ИТУ-2016). Материалы 9-й конференции по проблемам управления. Председатель президиума мультиконференции В.Г. Пешехонов, 2016. – С. 670-675.
2. Браницкий А.А. Архитектура сетевой системы обнаружения атак на основе использования методов машинного обучения и технологий обработки больших данных // Инновации в информационных технологиях, машиностроении и автотранспорте (ИИТМА-2020). Сборник материалов IV Международной научно-практической конференции с онлайн-участием. Кемерово, 2020. – С. 160-162.
3. Альшаев И.А., Красов А.В., Ушаков И.А. Исследование принципов работы протокола openflow в программно-конфигурируемых сетях // Труды учебных заведений связи, 2017. – Т. 3. – № 2. – С. 16-27.
4. Дубровин Н.Д., Ушаков И.А., Чечулин А.А. Применение технологии больших данных в системах управления информацией и событиями безопасности // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей V международной научно-технической и научно-методической конференции, 2016. – С. 348-353.
5. Котенко И.В., Ушаков И.А. Использование технологий больших данных для мониторинга инцидентов информационной безопасности // В сборнике: Региональная информатика «РИ-2016». Материалы конференции, 2016. – С. 168-169.
6. Крылов А.В., Ушаков И.А. Метрика защищенности интернет вещей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2022). XI Международная научно-техническая и научно-методическая конференция. Том 1. Санкт-Петербург, 2022. – С. 622-626.
7. Дешевых Е.А., Конюхов В.М., Крылов К.Ю., Ушаков И.А. Исследование методов защиты от инсайдерских атак // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: Сборник научных статей в 2 томах, 2015. – С. 310-313.
8. Бабков И.Н., Пудов К.А., Коновалова В.В., Дибиров Г.М. Исследование способов взаимодействия сетевых устройств на базе микрокомпьютеров // Научные известия, 2022. – № 26. – С. 35-38.
9. Vratonjic N., Freudiger J., Bindschaedler V., Hubaux J. The inconvenient truth about web certificates // В книге: Economics of information security and privacy III, Springer New York, 2013. – С. 79-117.
10. Rahmatulloh A., Gunawan R., Nursuwars F.M. Performance comparison of signed algorithms on JSON Web Token // В книге: IOP Conference Series: Materials Science and Engineering, Том 550, н. 1. IOP Publishing, 2019. – С. 012023.
11. Torrano-Giménez C., Perez-Villegas A. and Maranón G.A. An anomaly-based approach for intrusion detection in web traffic // Dynamic Publishers, 2010.
12. Лазарева М.В. Сравнительный анализ методов аутентификации пользователей: сессии и токены // Информационные технологии в науке, бизнесе и образовании. проблемы обеспечения цифрового суверенитета государства. Материалы XIII Международной научно-практической конференции студентов, аспирантов и молодых ученых. Под общей редакцией А.М. Прохорова, А.В. Царегородцева. Москва, 2022. – С. 40-44.

13. Visočnik V. Comparison of JWT and OAuth 2.0 authorisation and authentication techniques in REST services // Дис. докт. техн. наук; 2018; Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko.
14. Leiding B., Cap C.H., Mundt T. Rashidibajgan Authcoin: validation and authentication in decentralized networks // arXiv preprint arXiv:1609.04955, 2016.
15. Dietz M., Czeskis A., Balfanz D., Wallach D. Origin-bound certificates: A fresh approach to strong client authentication for the web // 21st USENIX Security Symposium, 2012.
16. Story H., Harbulot B., Jacobi I., Jones M. Foaf+ssl: Restful authentication for the social web // В книге: Proceedings of the First Workshop on Trust and Privacy on the Social and Semantic Web (SPOT2009), 2009.
17. URL Концепции безопасности при использовании сертификата X.509 в Центре Интернета вещей Azure https://learn.microsoft.com/ru-ru/azure/iot-hub/iot-hub-x509ca-concept (дата обращения – апрель 2023 г.).
18. Дибиров Г.М., Бабков И.Н., Ковцур М.М. Сравнительный анализ решений для контейнеризации // Молодежная школа-семинар по проблемам управления в технических системах имени А.А. Вавилова, 2022. – Т. 1. – С. 27-29.

КОНТЕКСТ КАК ИНДИКАТОР ВРЕДОНОСНОГО КОНТЕНТА

В.Н. Максименко, *к.т.н., доцент, Московский технический университет связи и информатики, vladmaks@yandex.ru.*

УДК 004

Аннотация. Качество информационных услуг оценивается на этапах обработки и передачи. Для расчета стандартных показателей качества «из конца в конец» учитывают только показатели технических средств. Считается, что информация всегда является правдивой. С развитием социальных сетей и электронных средств доставки возросли требования к защите конфиденциальной информации. Существующие методы защиты конфиденциальной информации, использующие шаблоны документов или ключевые слова, не учитывают контекст, который помогает оценить полезность информации по таким критериям как хороший – плохой, правдивый – ложный, интересный – скучный.

Ключевые слова: контент; контекст; доверие; защищенность информации; качество информационной услуги.

CONTEXT AS AN INDICATOR OF MALICIOUS CONTENT

Vladimir Maximenko, *Ph.D., Associate Professor, Moscow technical university of communications and informatics.*

Annotation. The quality of information services is assessed at the stages of processing and transmission. To calculate the standard quality indicators "from end to end", only the indicators of technical means are taken into account. It is believed that the information is always true. With the development of social networks and electronic means of delivery, the requirements for the protection of confidential information have increased. Existing methods of protecting confidential information using document templates or keywords do not take into account the context, which helps to assess the

usefulness of information by criteria such as good – bad, truthful – false, interesting – boring.

Keywords: content; context; trust; information security; quality of information services.

Введение

Сочетание компьютерных, телекоммуникационных, информационных и навигационных технологий создает предпосылки для создания высокопроизводительных распределенных информационных систем и систем реального масштаба времени. Класс инфокоммуникационных услуг сетей сотовой подвижной связи (СПС) характеризуется тем, что предоставляется путем последовательного использования технологических свойств специальных серверов приложений и сетевых сервисов СПС. Использование технологий искусственного интеллекта становится одним из приоритетных направлений в защите информации и инфраструктуры распределенных информационных систем и сетевых приложений. Специфика информационной безопасности состоит в том, что она является составной частью информационных технологий – области, развивающейся очень высокими темпами, при этом современные технологии программирования не позволяют создавать безошибочные программы, что приводит к появлению уязвимостей информационной системы. В инфокоммуникационной услуге к сетевой составляющей услуги относится только доступ абонента в сеть оператора, остальная же часть услуги предоставляется с помощью серверов сети. Обобщенная структурная схема сети связи с оказанием информационных услуг приведена на рис. 1.

Информационная безопасность в показателях качества услуг

Качество абонентской услуги зависит от качества на каждом шаге оказания услуги [1]. Например, доступность абонентской услуги определяется не только доступностью сети, но и доступностью каждого из серверов, участвующих в процессе оказания услуги.

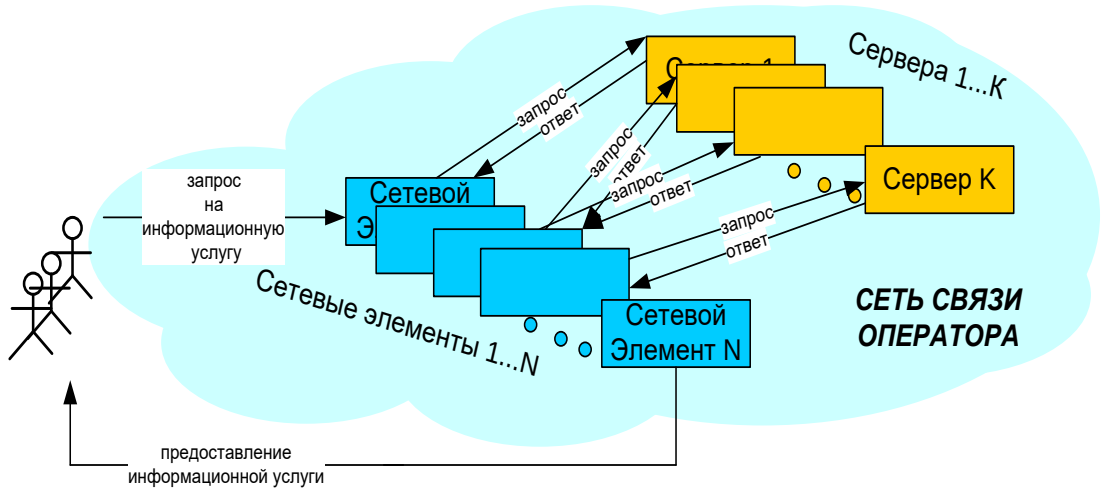

Рисунок 1

Для того чтобы оценить качество такой абонентской услуги в стандартизованных категориях (доступность, целостность, непрерывность), используют метод ее декомпозиции на элементы, качество которых поддается оценке в указанных категориях качества. Для таких элементов вводится понятие

«сервис». Ограничиваясь пока только техническими аспектами качества абонентской услуги, под сервисами понимаются отдельные технологические свойства сетевых элементов, с использованием и во взаимодействии которых предоставляется абонентская услуга. Сами сетевые элементы выступают в качестве ресурсов. На рис. 1 представлена обобщенная структурная схема сети связи с оказанием информационных услуг.

Проектирование информационных услуг на сетях подвижной связи начинается с разработки диаграммы вариантов использования. Главный прецедент определяет основную цель информационной услуги. Вспомогательные прецеденты определяют требования, которые должны быть выполнены для достижения цели.

Обобщенная диаграмма прецедента услуги на основе определения местоположения приведена на рис. 2. Требования информационной безопасности на диаграмме рис. 2 представлены прецедентами авторизации и получение доступа к системе, реализующей информационную услугу.

Первое, с чем сталкивается пользователь при доступе к любому информационному сервису является проверка превентивными мерами информационной безопасности сервиса аутентификации. Существует множество механизмов аутентификации, каждый из которых можно оценить посредством качественных показателей доступности, таких как вычислительная сложность и время проверки. Сервисы безопасности используются и на других этапах обработки и передачи информации при оказании услуг, и поэтому должны учитываться при оценке качества информационных услуг.

Для того чтобы управлять информационной безопасностью необходимо выполнить ряд операций сбора, обработки и выдачи управляющих воздействий в информационной системе.

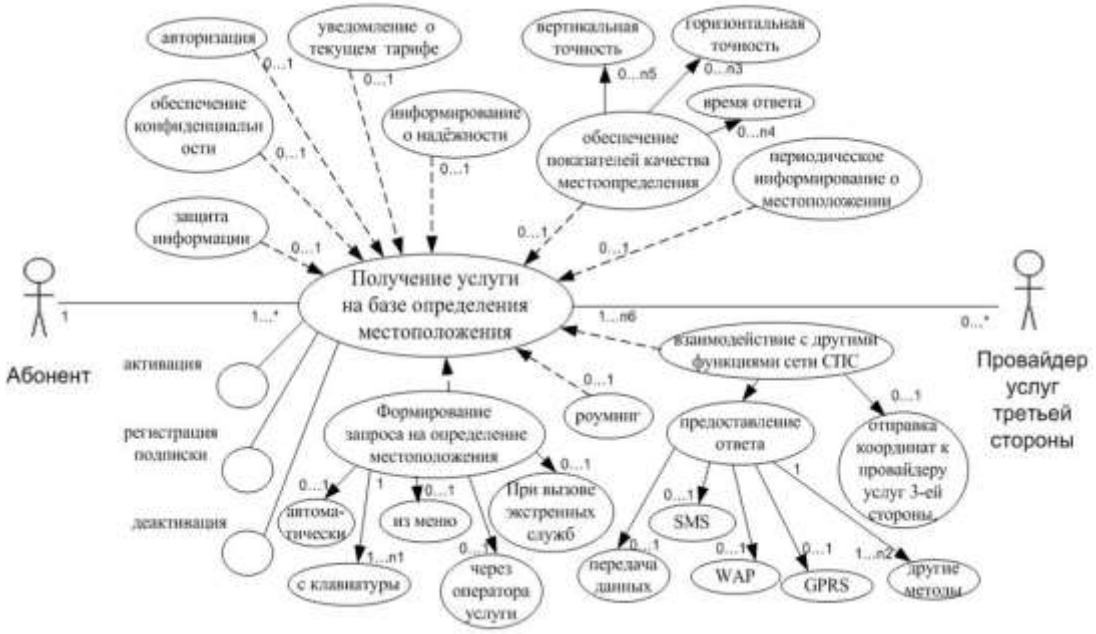

Рисунок 2

Основную часть этих действий выполняет система мониторинга. Система мониторинга – это система, которая работает с большим количеством информации в реальном масштабе времени. Для снижения требований производительности

системы мониторинга используют принцип декомпозиции по функциональному принципу, используя показатели: ресурсы, сервисы и услуги (приложения) [2].

Концептуальная модель подсистемы информационной безопасности представляет собой *UML*-диаграмму классов. Основными действующими лицами являются: владелец системы и злоумышленник (агент угроз). Учитывая функциональною декомпозицию, активы компании представлены в виде классов ресурсов сети, сервисов сети и услуг связи, образующими классы инвентаризации ресурсов, сервисов и услуг.

Агент угрозы создает угрозы, которые направлены на ресурс сети, сервис сети или/и услуги сети используя, для этого имеющиеся в информационной системе уязвимости. Каждая угроза безопасности увеличивает информационные риски, которые могут привести к потерям ресурсов, сервисов и услуг системы. Очевидно, что наибольший ущерб наносят угрозы, направленные на ресурсы сети.

Роль контекста в показателях качества контента (услуг)

Контент может состоять из разной информации: хорошей и плохой, правдивой и ложной, интересной и скучной. Но необходимо, чтобы этот контент был полезен тем людям, которым он адресован. Под нежелательным можно считать контент, содержащий информацию, которая может навредить человеку психологически, а также содержащий призывы к действиям, которые могут нанести вред самому человеку или же иному лицу (группе лиц).

Контент сайта – это любая информация, размещенная на нем. Без качественного и регулярного обновляемого контента практически невозможно повысить эффективность онлайн-бизнеса и вывести сайт в топ поисковых рейтингов. Любая информация, которую сайт предлагает пользователю должна быть полезной. Контент сайта – это его информационное наполнение. Содержимое сайта должно соответствовать уровню целевой аудитории.

Содержимое сайта должно периодически меняться, чтобы привлекать внимание. Если нет положительной информации, то используют отрицательную зловредную информацию. Поэтому необходимо разработать методы обнаружения зловредного злонамеренного контента. Качество услуги или информационной безопасности оценивается показателями доступности, целостности и конфиденциальности. Эти показатели не отражают свойства самой информации, насколько она является истинной или ложной. Оценить это можно только по косвенным признакам, таким как компетентность автора в области рассматриваемой информации, и комментарии читателей, на сколько мы можем доверять автору и читателям – субъектам информационных отношений. Этот вопрос выходит за пределы оценки качества и информационной безопасности информационной системы и находится в области оценки доверия к субъектам информационных отношений.

Полезность информации определяется ее истинностью или ложностью для отдельного субъекта информационных отношений или отдельной организации. Информация делится на общедоступную и конфиденциальную. Конфиденциальная информация является объектом защиты. Одним из методов нарушения конфиденциальной информации является передача такой информации с нарушением политики безопасности. Признаки конфиденциальной информации – шаблоны документов или ключевые слова, которые образуют библиотеку критериев информационной безопасности. Автоматизация выявления защищаемой информации обеспечивается путем сравнения контента с перечнем шаблонов и ключевых слов.

Основные методы выявления нежелательного контента для таких информационных материалов, как текст и изображение сводятся к очистке текста от служебных символов языка разметки гипертекста *HTML* и передаче очищенного текста для последующего сравнения слов текста с ключевыми словами из списка нежелательных слов.

Совпадение слова на странице со словом из некоторого списка нежелательных слов увеличивает негативный рейтинг текста. Когда относительное количество нежелательных слов превышает заданный порог, то делается вывод о том, что контент на данном веб-сайте относится к нежелательному [3]. Другие методы основаны на похожести одного текста на другой. Здесь не проверяется наличие в тексте чего-то заранее определенного негативного, а выполняется сравнение текстов. Похожесть может оцениваться по-разному, чаще всего речь идет о принадлежности текста к какой-то категории, т.е., сводится к задаче классификации [3, 4].

В последнее время шаблон документа и состав ключевых слов в нем не в полной мере обеспечивают защищенность конфиденциальной информации. Очень многое зависит от контекста, т.е. от обрамления контента, от того, кто является источником информации и в каких условиях и среде эта информация появилась. На первый план выходит показатель доверия. В докладе представлен анализ типов доверия и обзор алгоритмов методов оценки доверия.

Социальная сеть – это программно-техническая платформа для функционирования социальных сообществ, в которых зарегистрированные пользователи социальной сети объединяются в устойчиво функционирующие группы на основе взаимных интересов отдельных членов сообщества или степени доверия к источникам информации.

В настоящее время можно выделить три основных типа доверия: субъект-объект, объект-объект и субъект-субъект. В качестве «субъекта» выступает «человек», а «объектом» является «компьютер». Доверие среди пользователей в социальных сетях представляет большой интерес в области информационной безопасности. Поскольку социальные сети зачастую используют для распространения мнений определенной направленности, что объясняется пониженной критичностью восприятия пользователями информации [3]. Знания о доверии в социальных сетях также могут использоваться в системах рекомендаций.

Есть два основных типа доверия: прямое доверие и доверие к рекомендациям. Прямое доверие – доверие на основании личного опыта. Доверие к рекомендациям – доверие, основанное на мнении авторитета, группы людей, пропаганды (если *A* доверяет *B*, а *B* доверяет *C*, то *A* в некоторой степени тоже доверяет *C*) [5].

Существует три важных аспекта доверия: доверие зависит от поведения пользователя, доверие является динамичным и доверие зависит от контекста.

Важный элемент определения социального доверия – это контекст. Например, член *X* в сообществе доверяет рекомендациям другого члена *Y* по поводу автомобилей. Но в то же время, *X* не может доверять рекомендациям *Y* по поводу компьютерных игр или музыки.

Другим важным аспектом доверия является то, что оно зависит от времени. Взаимодействие, которое произошло в последнее время, может иметь большую ценность чем те, которые произошли некоторое время назад. Поэтому время является важным фактором для фиксации изменения в поведении индивида. Например, член *X* может иметь хорошие отношения с другим членом *Y* во время *t*, но эта связь может ослабевать, при отсутствии взаимодействия между ними.

Существует два типа взаимодействий: активный и пассивный. Пример активного взаимодействия включает в себя большое количество друзей, регулярные публикации, комментирование других членов и т.д. Однако не все члены сообщества – активные участники. Есть значительное количество членов, которые являются пассивными участниками сообщества. Взаимодействие пассивных членов в сообществе включает чтение статей, регулярные посещения сообщества и т.д. Эти члены могут не участвовать или не делиться своим опытом или чувствами, но они являются потребителями информации, что тоже очень ценно. Эти два типа взаимодействия коллективно создают социальный капитал сообщества и используются для оценки социального доверия.

Заключение

Без доверия люди не захотят делиться своими знаниями и опытом из-за страха, что их публикации и идентификационные данные будут использованы неправильно или даже незаконно. Таким образом, актуальной становится задача построения сети доверия. Алгоритмы путей создания сообществ доверия в социальной сети представлены в работе [5]. Реализация этих путей представляет сложную задачу по сбору исходных данных и автоматизации обработки.

Литература

1. Максименко В.Н., Васильев М.А. Методика расчета стандартных показателей качества дополнительных услуг на сетях подвижной связи // T-Comm: Телекоммуникации и транспорт, 2011. – Т. 5. – № 4. – С. 26-28.
2. Максименко В.Н. Конвергенция сервисов качества и защиты информации в сетях сотовой подвижной связи на этапах проектирования // T-Comm: Телекоммуникации и транспорт, 2018. – Т. 12. – № 11. – С. 57-64.
3. Шелухин О.И., Смычек М.А., Симонян А.Г. Фильтрация нежелательных приложений интернет-ресурсов в целях информационной безопасности // «Наукоемкие технологии в космических исследованиях, 2018. – Т. 10. – № 2. – С. 87-98.
4. Галимова А.Г., Симонян А.Г. Методы выявления нежелательного контента в тексте и изображениях // Сборник трудов XV Международной отраслевой научно-технической конференции «Технологии информационного общества». Москва. 03-04 марта 2021. – С. 151-152.
5. Максименко В.Н., Долгова Н.Д. Анализ алгоритмов вычисления уровня доверия к пользователю в социальной сети // Экономика и качество систем связи, 2018. – № 4 (10). – С. 23-30.

ПРЕДСТАВЛЕНИЕ И ПРЕДОБРАБОТКА ДАННЫХ ДИНАМИЧЕСКОЙ ПОДПИСИ ЧЕЛОВЕКА

В.Н. Максименко, *к.т.н., доцент, Московский технический университет связи и информатики, vladmaks@yandex.ru;*
Р.Н. Дзямко-Гамулец, *Московский технический университет связи и информатики, roman.dzyamko-gamulets@outlook.com.*

УДК 004.056

Аннотация. Предварительная обработка данных является одним из первых

этапов при выделении уникальных биометрических признаков человека. От качества и количества предварительных данных зависит точность работы биометрического метода аутентификации пользователя по его рукописной подписи. В данной работе описаны этапы предобработки данных, приводится обоснование их необходимости, представлены формулы преобразования данных. Указаны случаи, когда предобработка необходима полностью или частично.

Ключевые слова: предобработка; тензоры; масштабирование; угол подписи; признаки.

REPRESENTATION AND PREPROCESSING OF HUMAN DYNAMIC SIGNATURE DATA

Vladimir Maximenko, *Candidate of Technical Sciences, docent, Moscow Technical University of Communications and Informatics;*
Roman Dzyamko-Gamulets, *Moscow Technical University of Communications and Informatics.*

Annotation. Data preprocessing is one of the first steps in identifying unique biometric features of a person. The accuracy of the biometric method of authenticating a user by his handwritten signature depends on the quality and quantity of preliminary data. This paper describes the stages of data preprocessing, provides a justification for their necessity, and presents data transformation formulas. The cases when preprocessing is necessary in whole or in part are indicated.

Keyword: preprocessing; tensors; scaling; signature angle; features.

Введение

Биометрические методы аутентификации отличаются крайне высокой сложностью фальсификации, так как в качестве ключа используются уникальные биометрические характеристики человека. На данный момент происходит активное внедрение статических и динамических методов аутентификации в современные электронные устройства и информационные системы.

В данной статье рассматривается биометрический метод аутентификации человека на основе его рукописной подписи в онлайн режиме. Общий подход заключается в получении набора экземпляров подписи пользователя, вычисления усредненного варианта и сравнение его с тестируемыми экземплярами. Для сравнения подпись требуется формализовать, а именно – выделить набор признаков, которые можно сравнивать [1].

Признаки представляются в виде набора чисел – тензоров, их сравнение происходит на основании нормы тензора, представляющего разность соответствующих признаков. В частных случаях тензор признака может быть числом, вектором или матрицей. Однако для корректного сравнения необходимо совершить предобработку данных подписей.

Подпись представляется в виде двух функций зависимостей координат x и y от времени, из них и происходит выделение признаков для дальнейшего анализа. Но в первоначальном виде функции непригодны для выделения признаков или, по крайней мере, пригодны далеко не для всех возможных признаков. Одна из причин заключаются в том, что подпись может быть введена на экранах, которые сильно отличаются по размеру, а также само устройство ввода может иметь разный угол поворота. Также следует учитывать, что в зависимости от обстоятельств возможна

различная скорость написания подписи.

Стоит иметь ввиду, что устройство считывания данных не всегда может фиксировать точки координат подписи через равные промежутки времени. В итоге это приводит к тому, что при полностью одинаковом повторении подписи, координаты ее точек будут постоянно различными [2].

Таким образом, сами функции могут сильно отличаться, и чтобы сравнение было полным, необходимо привести эти функции к единому виду, который сохранял бы саму структуру зависимости координат точек от времени (без учета масштабирования). Поэтому для полноценного сравнения необходимо из имеющихся двух функций получить две новые, из которых уже и будет происходить выделение признаков. В данной работе преобразованные функции координат от времени называются нормализованными, сам процесс же – нормализацией, термин «предобработка», встречающийся в дальнейшем, обозначает получение данных в необходимом виде до начала процесса выделения признаков.

Стоит отметить, что сами исходные данные тоже имеют ценность и некоторые признаки требуется получать именно из них. Например, общая длина подписи в некоторых случаях может быть информативна, но нормализация лишает этих данных. Отдельно стоит учитывать временной промежуток, затраченный на написание самой подписи, так как при большой разнице от оригинала недоверие к экземпляру увеличивается [3].

Формулировка задачи и ее этапы

Имеются две функции *x(t)* и *y(t)* – зависимости координат подписи от времени, $t \in I$, где I – некоторый временной интервал. Временной интервал для каждой подписи может быть свой. В нормализованном виде будем считать, что каждая подпись находится в интервале $t \in [0;\ 1]$. В итоге, математическая формулировка задачи предобработки сводится к получению новой пары функций из пары исходных:

$$x = \overline{x}(t),$$
$$y = \overline{y}(t),$$

где: $t \in [0;\ 1]$.

Стоить иметь ввиду, что здесь подразумеваются зависимости координат от времени именно в виде непрерывных функций. В действительности, измерения происходят дискретно на устройстве, имеется лишь список точек с временными метками их получения. Поэтому необходимо из одного списка точек создать новый, где координаты и временные метки будут преобразованы к необходимому виду.

В итоге, первая задача, которую следует выполнить – привести этот список к некоторому стандарту. Для этого выбирается заранее сколько точек необходимо для использования. Чем их больше, тем точнее результат, но и больше требований к вычислительным ресурсам, поэтому обработка может занять больше времени [4]. Необходимое количество точек находится в пределах 100-150, но если предполагается обрабатывать достаточно длинные и сложные подписи, то значение увеличивается до 200 или 250 точек. Причем число точек должно быть одинаковым для всех экземпляров подписей (не только для конкретного пользователя, а для всех).

После получения точек необходимо решить следующую проблему – подписи могут быть написаны с немного разными углами. Это приведет к сильному

искажению координат *x* и *y* и невозможности полноценного их сравнения. Чтобы это исключить, необходимо все подписи преобразовать так, чтобы они были повернуты на один и тот же угол относительно выбранной системы координат, которая не зависит от геометрических характеристик самой подписи. Возникает необходимость определения угла поворота подписи [5].

Под поворотом пары функций *x(y)* и *y(t)* подразумевается получение из них новой пары функций, где для каждого значения аргумента новых функций будет преобразование поворота относительно некоторого выбранного центра от старых значений функций.

Для удобства работы с функциями мы будем считать, что все они должны иметь область определения $[0;\ 1]$ и область значения $[0;\ 1]$. То есть рассматриваем функции на квадрате:

$$T \times V\ =\ [0;\ 1] \times [0;\ 1],$$

где: T – область определения функции (временной интервал, на котором заданы функции координат подписи), V – область значения функции (координаты точек на экране).

Для преобразования к такому виду следует произвести параллельный перенос функции так, чтобы начало по временной оси (ось абсцисс) было в нуле, а также минимальное значение функции было также в нуле по оси ординат. После чего необходимо произвести масштабирование по каждой из осей, что позволит получить новую функцию, целиком находящуюся в единичном квадрате [6].

В итоге, предварительная обработка подписи состоит из следующих этапов:

1. Масштабирование временной оси.
2. Получение заранее выбранного количества новых точек и их координат на основе интерполяции исходных данных.
3. Вычисление угла подписи и поворот ее на этот угол – для получения условного нулевого поворота.
4. Сдвиг подписи в начало выбранной системы координат.
5. Масштабирование подписи.

Стоит отметить, что хоть эти этапы и предполагается проводить до выделения признаков, некоторые признаки можно получать после определенных этапов или вообще до начала предобработки. Например, если использовать в качестве признака сам угол поворота подписи, то его можно получить уже после 2-го этапа и до 3-го, так как в будущем он будет равен нулю или близок к этому значению. Также общее время написания экземпляра подписи необходимо получать до предобработки, так как после 1-го шага эта информация будет потеряна.

Масштабирование временной оси

Для начала временная ось масштабируется таким образом, чтобы область определения функций *x(t), y(t)* была отрезком $[0;\ 1]$. Для этого используется формула:

$$t_i' = \frac{t_i - t_1}{t_N - t_1},\ i = \overline{1..N},$$

где: t_i' – новая временная метка для i-й точки, t_i – старая временная метка для i-й точки.

В дальнейшем предполагается, что буква со штрихом обозначает новую переменную после преобразования, а без штриха – старую. Это будет справедливо для каждого преобразования и для каждого этапа. При таком преобразовании временная метка для первой точки будет равна 0, а для последней – 1.

Получение новых точек путем интерполяции исходных

Изначально имеется список исходных данных – точек, зафиксированных в различные моменты времени. Необходимо создать новый список точек для заранее выбранного их количества *N*. Для этого в новый список копируется первая и последняя точка из исходного набора. Временные метки остальных точек в новом списке будут иметь вид:

$$t_i = \frac{1}{N-1} \cdot i, \ \overline{i = 1 .. N - 2}.$$

Чтобы их найти, следует определить, между какими ближайшими двумя точками из необработанных данных находится выбранная точка, и, используя линейную интерполяцию, определить необходимое значение:

$$x_i' = x_{il} + \frac{x_{ir}-x_{il}}{t_{ir}-t_{il}} \cdot (t_i - t_{il}),$$
$$y_i' = y_{il} + \frac{y_{ir}-y_{il}}{t_{ir}-t_{il}} \cdot (t_i - t_{il}),$$

где: x_i', y_i' – значения координат определяемого множества точек для i-й точки; x_{il}, y_{il} – координаты ближайшей точки сырых данных, временная метка которой $t_{il} < t_i$; x_{ir}, y_{ir} – координаты ближайшей точки сырых данных, временная метка которой $t_{ir} \geq t_i$, t_i – временная метка новой точки; индекс l – означает ближайшую точку слева (*left*), а *r* – справка (*right*).

Вычисление угла подписи и поворот

Необходимо определить такое понятие, как угол подписи между ней и осью абсцисс. Полагается, что координаты подписи заданы списками из *N* точек, равноудаленных друг от друга по оси абсцисс, то есть временные метки находятся через равные промежутки на временной оси. Это то представление, которое должно быть после применения предыдущего шага [7].

Пусть t_c – середина временного интервала подписи. Находим все точки (x_i, y_i) такие, что их временная метка $t_i < t_c$, а также все такие точки (x_j, y_j), для которых $t_j > t_c$. Получаются два множества: множество точек *I*, полученных в первой половине временного интервала написания подписи, и множество точек *J*, полученных во второй половине временного интервала. Если есть такие точки, что $t_k = t_c$, то их можно отбросить.

В каждом из этих двух множеств точек *I*, *J* вычисляется геометрический центр по формулам:

$$x_{1c} = \frac{\sum_{i=1}^{|I|} x_i}{|I|}, \quad x_{2c} = \frac{\sum_{i=1}^{|J|} x_i}{|J|},$$
$$y_{1c} = \frac{\sum_{i=1}^{|I|} y_i}{|I|}, \quad y_{2c} = \frac{\sum_{i=1}^{|J|} y_i}{|J|},$$

где: $|I|$ – мощность (количество элементов) первого множества; $|J|$ – второго; x_{kc},

y_{kc} – координаты центра k-го множества; $k = \overline{1..2}$.

Теперь, имея две точки (x_{1c}, y_{1c}) и (x_{2c}, y_{2c}), можно провести прямую. Угол между этой прямой и осью абсцисс будем называть углом наклона подписи к оси абсцисс. Он показывает угол поворота подписи по отношению к условному нулевому углу. То есть, для нормализации поворота подписи и получения «нуля», подпись следует повернуть на угол, противоположный найденному. Значение угла находится по формуле:

$$\alpha = tan^{-1}\left(\frac{y_{2c} - y_{1c}}{x_{2c} - x_{1c}}\right)(\pm\pi),$$

где: число π добавляется либо вычисляется в зависимости от четверти.

Здесь предполагается, что $x_{1c} \neq x_{2c}$. Если это не так, то:

$$\alpha = \frac{\pi}{2} \text{ при } y_{2c} > y_{1c},$$
$$\alpha = -\frac{\pi}{2} \text{ при } y_{2c} < y_{1c},$$
$$\alpha = 0 \text{ при } y_{2c} = y_{1c}.$$

Поворот подписи осуществляется вокруг ее геометрического центра, который находится по формулам:

$$x_c = \frac{\sum_{i=1}^{N} x_i}{N},$$
$$y_c = \frac{\sum_{i=1}^{N} y_i}{N}.$$

Для нахождения координат точек после поворота используются следующие выражения:

$$x_i' = (x_i - x_c) \cdot cos\alpha - (y_i - y_c) \cdot sin\alpha + x_c,$$
$$y_i' = (y_i - y_c) \cdot sin\alpha + (x_i - x_c) \cdot cos\alpha + y_c.$$

Сдвиг в начало координат

Для осуществления преобразования сдвига для каждой точки применяется преобразование по следующим формулам:

$$x_i' = x_i - min\{x_i\},$$
$$y_i' = y_i - min\{y_i\},$$

где: $min\{x_i\}$, $min\{y_i\}$ – минимальные значения соответствующих координат на всем множестве точек, $i = \overline{1..N}$.

Масштабирование

Для того, чтобы область значений функций координат укладывалась в отрезок $[0; 1]$, необходимо произвести масштабирование для каждой точки по следующим формулам:

$$x_i' = \frac{x_i}{\max\{x_i\}},$$

$$y_i' = \frac{y_i}{\max\{y_i\}},$$

где: $max\{x_i\}$, $max\{y_i\}$ – максимальные значения соответствующих координат на всем множестве точек.

Заключение

Предобработка данных подписи является очень важным этапом в процессе аутентификации пользователя по его рукописной подписи. Основная идея алгоритмов аутентификации сводится к сравнению различных экземпляров подписи в виде списков точек с временными метками [8].

Но многие из этих алгоритмов требуют, чтобы оба списка точек имели одинаковый вид. Под этим подразумевается одинаковое количество точек для обоих экземпляров, одинаковый временной интервал написания подписи, одинаковые размеры области, в которой находятся подписи, а также исключение влияния поворота подписи, которое зависит от поворота устройства, на котором происходит ввод подписи.

Исходные данные, полученные от устройства ввода, обычно не удовлетворяют всем условиями, поэтому их надо предварительно обработать таким образом, чтобы алгоритмы сравнения могли ими оперировать.

Литература

1. Сулавко А.Е., Еременко А.В., Самотуга А.Е. Исключение искаженных биометрических данных из эталона субъекта в системах идентификации // Информационные технологии и вычислительные системы. ЛЕНАНД. – Москва, 2013. – № 3. – С. 96-101.

2. Волошина Т.С., Максименко В.Н. Анализ системы распознавания лиц по алгоритму нейронной сети // В сборнике: Технологии информационного общества. Материалы XIII Международной отраслевой научно-технической конференции. – М.: 2019. – С. 341-344.

3. Ложников П.С., А.И. Иванов, Е.И. Качайкин, А.Е. Сулавко. Биометрическая идентификация рукописных образов с использованием корреляционного аналога правила Байеса // Вопросы защиты информации. ФГУП «ВИМИ». – Москва, 2015. – № 3. – С. 48-54.

4. Ручай А.Н. Инварианты как метод верификации по статической подписи // Материалы всероссийской конференции с международным участием «Знания-Онтологии-Теории» (ЗОНТ-09). Новосибирск: ИМ СО РАН, 2009. – С. 212-215.

5. Ложников П.С., Сулавко А.Е., Еременко А.В., Волков Д.А. Экспериментальная оценка надежности верификации подписи сетями квадратичных форм, нечеткими экстракторами и персептронами // Информационно-управляющие системы, 2016. № 5. – С. 73-85.

6. Пинтусов Д.Н. Информационная система идентификации рукописной подписи: автореф. дисс. магистра информатики и вычислительной техники: 1-40 81 01 / Д. Н. Пинтусов; науч. рук. Т.В. Тихоненко. – Минск: БГУИР, 2020. – 15 с.

7. Способ биометрической аутентификации по почерку в компьютеризированной системе контроля доступа: пат. 2469397C1, Рос. Федерация: МПК G06 9/00. [Текст]. Милых В.А., Лапина Т.И., Лапин Д.В.; патентообладатель ФГБОУ ВПО «Юго-Западный государственный университет» (ЮЗГУ). – № RU 2 469 397; заявл. 30.09.2011; опубл. 10.12.2012.

8. Гмурман В.Е. Теория вероятностей и математическая статистика: учеб. пособие для вузов. – М.: Высшая школа, 2004. – 479 с.