ЭКОНОМИКА И КАЧЕСТВО СИСТЕМ СВЯЗИ ***№ 2(20) / 2021***

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»

Главный редактор
Е.Е. Володина, д.э.н., акад. РАЕН

Редакционная коллегия:
Бабенко Л.К., д.т.н.
Бокк Г.О., д.т.н.
Борох Н.В., д.э.н.
Гуревич В.Э., к.т.н.
Дворянкин С.В., д.т.н.
Зубарев Ю.Б., д.т.н., чл.-корр. РАН
Качалов Р.М., д.э.н.
Кобылко А.А., к.э.н.
Косинов М.И., к.т.н.
Кудин А.В., к.т.н.
Лившиц В.Н., д.э.н.
Панов С.А., д.т.н.
Петров Д.А., к.ф.-м.н., Финляндия
Салютина Т.Ю., д.э.н.
Сю Гуан Хань, IEEE Fellow, Китай
Шорин О.А., д.т.н.
Эмиль Кине, Ph. D., Франция

Ведущий редактор *Дуничева Н.С.* ***Редактор*** *Федорова О.В.*

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./факс: *8 (495)133-38-99 (282)* ***e-mail:*** *ekss@nirit.org* ***сайт:*** *http://nirit.org/*

СОДЕРЖАНИЕ

ЭКОНОМИКА И УПРАВЛЕНИЕ В ИНФОКОММУНИКАЦИЯХ

Е.Г. Кухаренко, Ю.Н. Соломина
Трансформация моделей ведения бизнеса в условиях цифровизации 3-12

В.В. Макаров, Т.А. Блатова, Е.Ю. Ворошилова
Ускоренное развитие информационных технологий в период пандемии 12-19

Г.П. Платунина, А.С. Старовойтова
Монетизация криптосайтов как новый способ заработка в условиях цифровой экономики 19-26

А.С. Дунаев
К вопросу об использовании радиоэлектронных средств российского происхождения в рамках развития перспективных радиотехнологий в Российской Федерации 26-31

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Г.П. Платунина, Д.С. Ермоленко
Кибербезопасность: искусная защита цифровой экономики 32-40

К.А. Ахрамеева, Д.Ю. Мицковский
Исследование возможности использования метрики RIBES для оценки лингвистических стегосистем 40-46

СЕТИ И СИСТЕМЫ СВЯЗИ

Р.Е. Кротов, А.И. Рыбаков
Повышение помехоустойчивости в коротковолновом радиоканале при помощи CRC и LDPC кодов 47-52

М.С. Лохвицкий, В.О. Шорин
Мобильный ретранслятор с функцией определения местоположения 52-56

ЭКОНОМИКА И УПРАВЛЕНИЕ В ИНФОКОММУНИКАЦИЯХ

ТРАНСФОРМАЦИЯ МОДЕЛЕЙ ВЕДЕНИЯ БИЗНЕСА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Е.Г. Кухаренко, *к.э.н., доцент, Московский технический университет связи и информатики, e.g.kukharenko@mtuci.ru;*
Ю.Н. Соломина, *РЭУ им. Г.В. Плеханова, solomina.yulia96@yandex.ru.*

УДК 338.47

Аннотация. Цифровизация экономики базируется на современных информационных и телекоммуникационных технологиях, создающих инфраструктурный инструментарий для инновационного развития предприятий всех отраслей и сфер деятельности. Несмотря на насыщение рынка и снижение доходов от услуг подвижной связи, дальнейшее развитие этого сегмента инфокоммуникационного рынка остается важнейшей государственной задачей. Демонополизация рынков, появление новых технологий, изменение регуляторной политики в отрасли инфокоммуникаций способствовали расширению моделей ведения бизнеса, одной из новых моделей является модель *MVNO*. При создании виртуального оператора как элемента цифровой экосистемы необходимо учитывать преимущества и ограничения типов бизнес-моделей *MVNO,* его роль в цифровой экосистеме, потенциал расширения абонентской базы экосистемы в целом и увеличения лояльности потребителей.

Ключевые слова: цифровая трансформация; бизнес-модель; цифровая экосистема; сотовая подвижная связь; виртуальный оператор; бизнес-модель *MVNO.*

TRANSFORMATION OF BUSINESS MODELS IN THE CONTEXT OF DIGITALIZATION

Elena Kukharenko, *Ph. D. in Economics, associate Professor, Moscow Technical University of Communications and Informatics;*
Yulia Solomina, *Plekhanov Russian University of Economics.*

Annotation. The digitalization of the economy is based on modern information and telecommunications technologies that create infrastructure tools for the innovative development of enterprises in all industries and spheres of activity. Despite the saturation of the market and the decline in revenues from mobile services, the further development of this segment of the infocommunication market remains the most important state task. The demonopolization of markets, the emergence of new technologies, and changes in the regulatory policy in the infocommunication industry have contributed to the expansion of business models, one of the new models is the *MVNO* model. When creating a virtual operator as an element of the digital ecosystem, it is necessary to take into account the advantages and limitations of the types of *MVNO* business models, its role in the digital ecosystem, the potential to expand the subscriber base of the ecosystem as a whole and increase consumer loyalty.

Keywords: digital transformation; business model; digital ecosystem; cellular

mobile communications; virtual operator; *MVNO* business model.

Цифровая трансформация – основное направление развития национальной экономики России. Внедрение технологий искусственного интеллекта, блокчейн, индустриального интернета вещей, робототехники, *BigData*, интегрированных инженерных программных платформ способствует цифровым преобразованиям различных отраслей промышленности, инфраструктурных отраслей и других сфер деятельности [1-5]. Комплексные стратегии цифровизации в противовес использованию отдельных цифровых инструментов, способствующие повышению эффективности применения цифровых технологий, разработка средств производства, соответствующих требованиям и технологическим стандартам Индустрии 4.0, модернизация внутренних бизнес-процессов и механизмов взаимодействия с потребителями, поставщиками, подрядчиками, партнерами, другими субъектами внешней среды, позволяют предприятиям и организациям выйти на принципиально новый уровень конкурентоспособности [6-10]. Цифровые преобразования государственного и муниципального управления, здравоохранения, образования способствуют повышению эффективности взаимодействия населения и государства и обеспечивают повышение качества решения государственных задач [11-14].

Цифровизация базируется на современных информационных и телекоммуникационных технологиях, создающих инфраструктурный инструментарий для инновационного развития всех отраслей национальной экономики. И это обусловливает высокие темпы развития предприятий и организаций инфокоммуникационного и *IT* сектора. Формирование обоснованной стратегии инновационного развития, внедрение технологических и организационно-управленческих инноваций способствует не только повышению конкурентоспособности ИКТ-компаний, но и создает высокий внеотраслевой эффект от функционирования предприятий инфокоммуникационной отрасли [15-20].

Развитие сотовой подвижной связи в Российской Федерации началось чуть более 25 лет назад, но за этот период она превратилась в ключевой компонент инфокоммуникационной отрасли. В конце 1990-х гг. – начале 2000-х гг. сотовая связь являлась самым быстрорастущим сегментом и российского, и мирового инфокоммуникационного рынка. Пройдя этапы формирования, бурного развития, создания и функционирования огромного количества операторов, использующих различные технологии подвижной связи, рынок услуг сотовой подвижной связи вступил в фазу зрелости, характеризующуюся высоким уровнем проникновения и господствующим положением четырех федеральных операторов: «Мобильные ТелеСистемы», «ВымпелКом», «МегаФон», «Теле2». Каждая компания владеет масштабной инфраструктурой, обеспечивает огромную зону покрытия, предлагает клиентам широкий спектр услуг и разнообразную линейку тарифных планов.

За последнее десятилетие изменилась динамика доходов подвижной связи. На рис. 1 показана динамика доходов от услуг подвижной связи, в том числе от населения (составлено авторами по данным отраслевой статистики [20]).

Если до 2013 г. наблюдался устойчивый рост показателей, хотя после 2008 г. темпы роста доходов сократились, то последние 8 лет размер доходов подвижной связи ежегодно сокращается. По предварительным итогам, в 2020 г. доля доходов подвижной связи составила 22% от общих доходов инфокоммуникационной отрасли, в то время как в 2003 г. этот показатель равнялся 35,4%. При этом плотность подвижной связи остается очень высокой – в 2019 г. этот показатель

достиг отметки 211 абонентских устройств на 100 жителей.

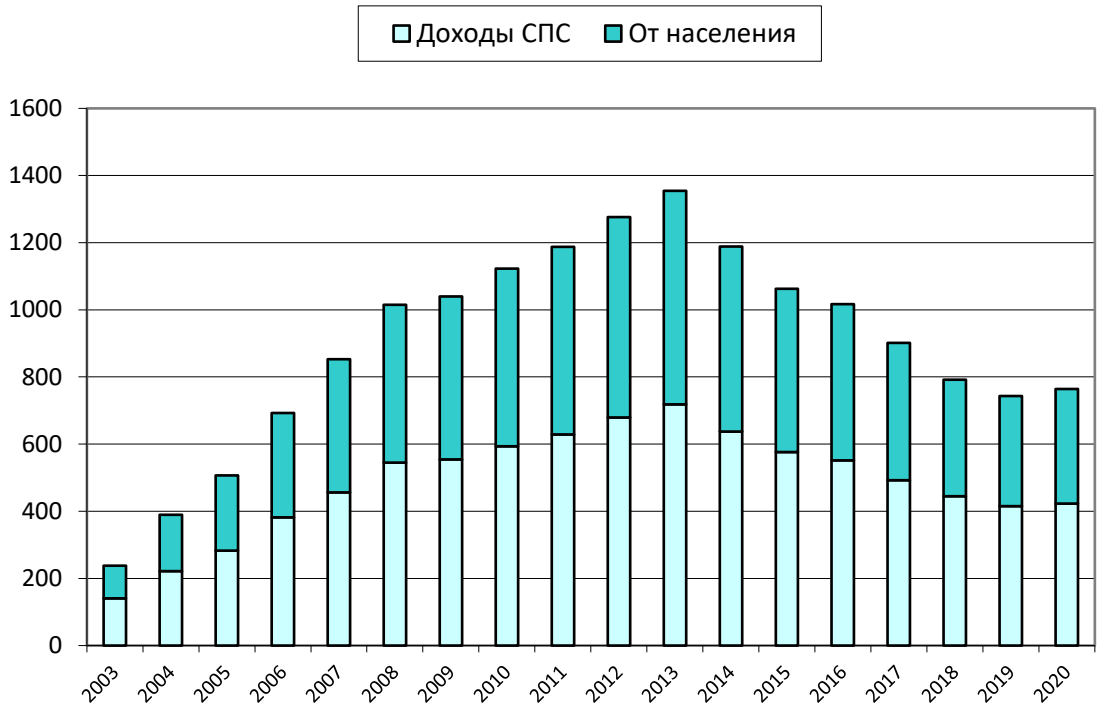

Рисунок 1

На рис. 2 показана динамика показателя плотности подвижной связи (количество АУ/100 жителей (составлено авторами по данным отраслевой статистики [19]). В 2019 г. также на 22,7% увеличился объем введенных в действие мощностей подвижной радиотелефонной связи [20].

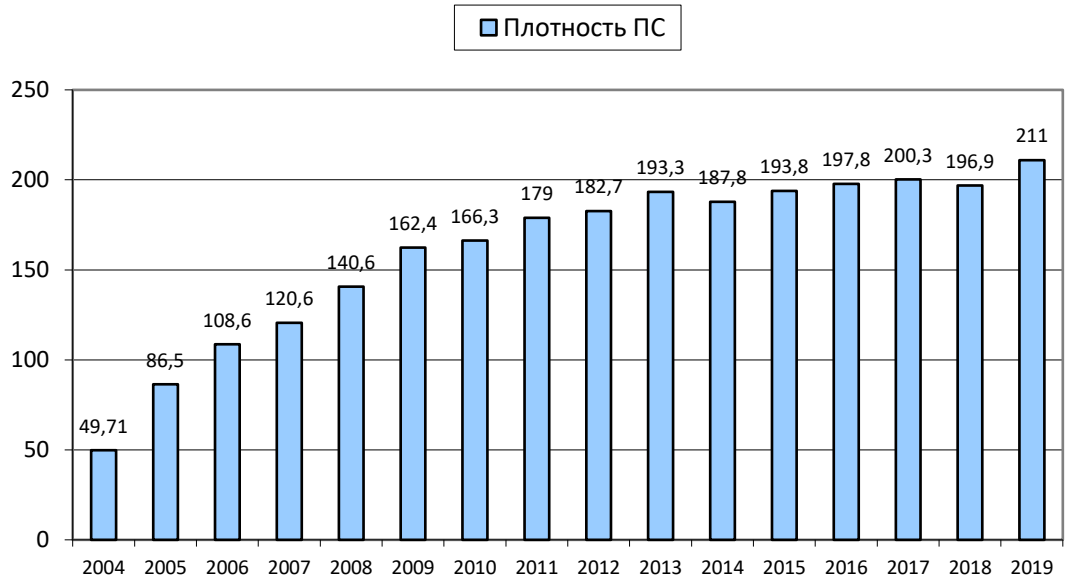

Рисунок 2

Цифровая экономика нуждается в «конкурентоспособной, устойчивой и безопасной инфраструктуре высокоскоростной передачи данных, доступной для всех граждан, бизнеса и органов власти» [20-23]. И сотовая подвижная связь остается важным элементом инфокоммуникационной инфраструктуры нашей страны. Для каждого человека мобильный телефон является «точкой доступа» к огромному количеству новых услуг и возможностей. По предварительным данным

на конец 4 квартала 2020 г. число активных абонентов подвижной связи, использующих услуги доступа в глобальную сеть интернет с заявленной скоростью более 256 кБит/с достигло 145,9 млн, в то время как число активных абонентов фиксированного широкополосного доступа к сети интернет составляет только 33,7 млн, то есть в четыре раза меньше [20]. Кроме того, обеспечение жителей России современными услугами подвижной связи, в том числе мобильного широкополосного доступа к сети интернет, способствует устранению цифрового неравенства и ликвидации цифрового барьера среди различных групп населения нашей страны. Поэтому дальнейшее развитие подвижной связи остается важнейшей государственной задачей.

С течением времени под воздействием факторов внешней среды изменялись не только применяемые технологии, но и методы управления производственной деятельностью операторов подвижной связи, механизмы взаимодействия с другими участниками межсетевого пространства, модели ведения бизнеса [24-29].

Производственная деятельность оператора сотовой подвижной связи (СПС) включает такие направление как создание, техническая поддержка, модернизация и развитие сети, осуществление взаимодействия и взаиморасчетов с участниками межсетевого пространства; подключение и взаимодействие с абонентами; маркетинг и продвижение услуг; создание и внедрение новых сервисов и продуктов. Каждое направление включает совокупность разнообразных бизнес-процессов, для осуществления которых формируются громоздкие организационные структуры оператора традиционного типа. Учитывая высокие затраты и определенную «неповоротливость» таких структур, отсутствие мобильности и быстрого реагирования на новые запросы рынка, еще в середине 1990-х гг. появилась бизнес-модель, базирующаяся на разделении основных функций и ориентации на выполнение отдельных функций или бизнес-процессов. Компании, использующие новую бизнес-модель, получили название виртуальных операторов СПС или *MVNO* (*Mobile Virtual Network Operator*). *MVNO* не владеют лицензией на частотный диапазон, продают услуги СПС под своим собственным брендом, используя сетевые ресурсы оператора традиционного СПС в качестве опорной сети. Такая бизнес-модель предусматривает заключение двусторонних соглашений между виртуальным оператором и лицензированным оператором СПС (*Mobile Network Operator, MNO*) на приобретение сетевой емкости или покупку трафика и последующее оказание услуг своим собственным абонентам [30]. Модель организации бизнеса традиционного *MNO*, так же, как и оператора местной или междугородной фиксированной связи ранее была единой: строительство сети, получение лицензии, эксплуатация сети, продажа услуг и работа с абонентами. Демонополизация рынков, появление новых технологий, изменение регуляторной политики в отрасли инфокоммуникаций способствовали расширению моделей ведения бизнеса, и *MVNO* является одной из них.

Первый виртуальный оператор подвижной связи появился в России в конце 1990-х гг. Развитие этой бизнес-модели в первое время ограничивала действовавшая в тот период нормативно-правовая база. Сейчас в нашей стране реализовано более 40 проектов создания виртуальных операторов, однако далеко не все проекты были успешными. В последние годы к этой деятельности активно подключились крупнейшие финансово-кредитные организации, создающие *MVNO* в качестве элементов своих цифровых экосистем.

Цифровая экосистема – это инновационная модель ведения бизнеса в эпоху цифровой трансформации экономики, модель, проверенная и активно внедряемая компаниями различных отраслей. К флагманам в этом направлении можно отнести

финансово-кредитные организации. Банковский сектор является ключевым элементом рыночной инфраструктуры, поэтому в ускорении процессов цифровизации в этой области заинтересованы как сами организации, так и государство. Наиболее активно программы цифровизации реализуют крупнейшие российские банки. Процесс цифровизации банковской деятельности обычно начинается с внутренних бизнес-процессов, а в дальнейшем вектор инновационного развития направлен на создание цифровой экосистемы [31]. Цифровая экосистема – это, по сути, объединение множества партнеров и направлений деятельности на основе единой информационно-технологической инфраструктуры. В рамках данной концепции виртуальный оператор рассматривается не просто как новая стратегическая бизнес-единица, а как важный элемент системы, синергетический эффект от функционирования которой превышает эффект отдельно взятого бизнеса. По этому пути пошли ряд российских банков, создавших в рамках своих цифровых экосистем *MVNO* Тинькофф Мобайл, СберМобайл, ВТБ Мобайл, и активно поддерживающих и продвигающих эти проекты.

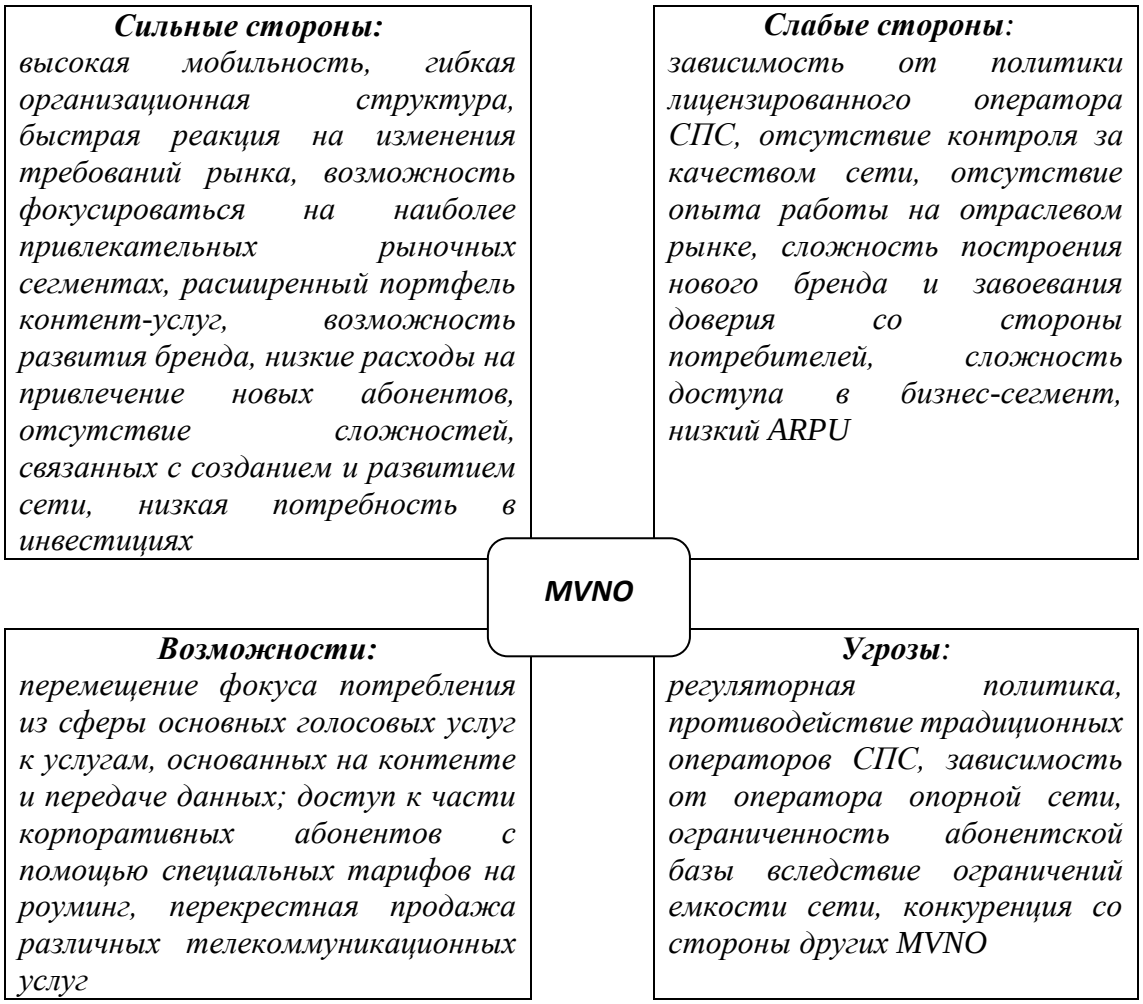

Рисунок 3

Однако создание виртуального оператора – сложная задача, успешное решение которой вовсе не гарантировано. Об этом свидетельствуют многочисленные приостановленные или закрытые российские проекты, в частности *MVNO* ряда крупных торговых сетей. При создании виртуального

оператора необходимо не только учитывать преимущества данной бизнес-модели, но и тщательно просчитывать все возможные риски. Анализ основных возможностей и ограничений бизнес-модели *MVNO* представлен на рис. 3.

Укрупненная бизнес-модель *MVNO* может реализовываться разными способами, исходя из возможностей доступа к базовой сетевой инфраструктуре и функций, которые готов осуществлять виртуальный оператор. Каждый способ связан с различными объемами первоначальных инвестиций, что также может стать ограничивающим фактором при выборе частной бизнес-модели.

Помимо владения и обслуживания элементов сети, виртуальный оператор может заниматься формированием пакетных предложений, тарифных планов, биллингом, продажами, продвижением, управлением взаимоотношениями с клиентами. Исходя из закрепляемых функций можно условно выделить такие типы *MVNO*, как «чистый продавец», «поставщик услуг», «расширенный поставщик услуг», «полный *MVNO*» В табл. 1 представлено сравнение типов бизнес-моделей виртуальных операторов.

MVNO – «чистый продавец» специализируется исключительно на потребительских аспектах, занимаясь продажами, брендингом и управлением взаимоотношениями с клиентами. Эта бизнес-модель не подразумевают аренду или покупку элементов сети сотовой подвижной связи. Такой подход предполагает минимальные стартовый капитал и предпринимательские риски.

«Поставщик услуг», помимо вышеназванных функций, занимается выделением своего собственного номерного ресурса, программированием и брендированием *SIM*-карт оператора СПС, пакетированием услуг, формированием собственных тарифных планов.

Таблица 1.

Компоненты бизнес-модели	Чистый продавец	Поставщик услуг	Расширенный поставщик услуг	Полный MVNO
Элементы сетевой инфраструктуры			+	+
Услуги, тарифы, биллинг		+	+	+
Продажи, продвижение, работа с абонентами	+	+	+	+

«Расширенный поставщик услуг» и «полный *MVNO*» от предыдущих типов отличаются наличием элементов сети подвижной связи в собственности или аренде, а между собой – количеством этих элементов. Соответственно вместе с увеличением компонентов бизнес-модели растут, с одной стороны, рентабельность операционной деятельности, а с другой – финансовые и регуляторные риски *MVNO*.

Операционная эффективность функционирования виртуального оператора зависит от ряда факторов и, прежде всего, это размер абонентской базы и средний доход на одного абонента. Различные модели *MVNO* характеризуются различным

значением показателя *ARPU*, что обусловлено перечнем, качественными и ценовыми характеристиками предлагаемых абонентам пакетов услуг и возможностями влиять на этот компонент бизнес-модели. Разные типы *MVNO* характеризуются разным уровнем операционных расходов и разными возможностями их оптимизации, что напрямую связано с рентабельностью затрат. Также надо учитывать, что «расширенный поставщик услуг» и «полный *MVNO*» могут иметь различный состав элементов сети, находящихся в их собственности. Для каждого типа бизнес-модели характерны разные уровни контроля качества предоставляемых услуг и зависимость от оператора базовой сети подвижной связи. Наличие собственного оборудования, с одной стороны, увеличивает операционные расходы виртуального оператора, а с другой, – позволяет предоставлять своим абонентам более широкий спектр услуг, гарантировать и контролировать качество их предоставления [32, 33]. Учет вышеназванных факторов необходим при разработке проекта создания виртуального оператора на этапе технико-экономического обоснования проекта.

Заключение

Создание виртуального оператора как элемента цифровой экосистемы требует использования расширенного подхода к оценке экономической эффективности подобного проекта. В данном случае должна быть оценена роль *MVNO* в цифровой экосистеме, потенциал расширения абонентской базы экосистемы в целом и увеличения лояльности потребителей.

Литература

1. Gorodnichev M.G., Kukharenko E.G., Salutina T.U., Moseva M.S., Kukharenko A.M. Features of the development of information systems for working with blockchain technology / В сборнике: Journal of Physics: Conference Series. International Scientific Conference "Conference on Applied Physics, Information Technologies and Engineering - APITECH-2019". Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations; Polytechnical Institute of Siberian Federal University, 2019. – С. 33039.
2. Gorodnichev M., Kukharenko A., Kukharenko E., Salutina T. Methods of developing systems based on bockchain // Conference of Open Innovation Association. FRUCT, 2019. – № 24. – С. 613-618.
3. Kuzovkova T.A., Saliutina T.Y., Kukharenko E.G., Sharavova O.I. Mechanism of interconnected management of development of networks and platforms of the internet of things on the basis of evaluation of synergetic efficiency // В сборнике: 2020 Wave Electronics and its Application in Information and Telecommunication Systems, WECONF, 2020. – С. 9131158.
4. Маньков В.А., Кухаренко Е.Г. Технологии цифровизации бизнес-процессов инфокоммуникационной компании / в сборнике: технологии информационного общества. Сборник трудов XV Международной отраслевой научно-технической конференции «Технологии информационного общества», 2021. – С. 266-268.
5. Володина Е.Е. Прогнозирование развития инновационных услуг в сфере инфокоммуникаций // Инновационное развитие экономики, 2017. – № 5 (41). – С. 7-16.
6. Кузовкова Т.А., Кухаренко Е.Г., Салютина Т.Ю. Обоснование эволюции критериев цифрового развития экономики и общества // Экономика и качество систем связи, 2019. – № 2 (12). – С. 13-20.
7. Кузовкова Т.А., Салютина Т.Ю., Кухаренко Е.Г., Шаравова О.И. Механизм

управления эффективностью применения цифровых технологий // Инновации в менеджменте, 2020. – № 2 (24). – С.36-45.
8. Кухаренко А.М., Анохина М.Е. Роль единого информационного пространства предприятия в повышении эффективности бизнеса // В сборнике: Технологии информационного общества. Сборник трудов XII Международной отраслевой научно-технической конференции, 2018. – С. 339-340.
9. Кухаренко Е.Г. Управление конкурентоспособностью компании на инфокоммуникационном рынке / В сборнике: Технологии информационного общества. Сборник трудов XII Международной отраслевой научно-технической конференции, 2018. – С. 346-347.
10. Кухаренко Е.Г., Андержанова Г. CRM в телекоммуникациях как фактор повышения эффективности бизнеса / В сборнике: Технологии информационного общества. Сборник трудов XII Международной отраслевой научно-технической конференции, 2018. – С. 357-359.
11. Кухаренко Е.Г., Аношкина Е.С. Повышение эффективности управления регионом на основе информационно-телекоммуникационных технологий. / В сборнике: Технологии информационного общества. Сборник трудов XII Международной отраслевой научно-технической конференции, 2018. – С. 354-356.
12. Кухаренко Е.Г., Асташков К.В. Актуальность проблемы совершенствования модели проектного управления PMBOK в Российских инфокоммуникационных компаниях // В книге: Мобильный бизнес: Перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов XL Международной конференции РАЕН. Москва, 2017. – С.66-69.
13. Кухаренко Е.Г., Янкевский А.В., Аминев О. Нормативно-правовое обеспечение функционирования инфокоммуникационных систем в области государственного и муниципального управления / В сборнике: Технологии информационного общества. Сборник трудов XII Международной отраслевой научно-технической конференции, 2018. – С. 351-353.
14. Володина Е.Е., Веерпалу Д.В. Анализ развития цифрового телевидения в мире и в России // T-Comm: Телекоммуникации и транспорт, 2013. – Т. 7. – № 12. – С. 23-26.
15. Анохина М.Е., Кухаренко А.М. Совершенствование организационно-управленческой деятельности компаний на инфокоммуникационном рынке / В книге: Мобильный бизнес: Перспективы развития и реализации систем радиосвязи в России и за рубежом Сборник материалов (тезисов) XLII Международной конференции РАЕН, 2018. – С. 101-104.
16. Кухаренко А.М. Организационно-управленческие инновации на телекоммуникационном рынке // В книге: Мобильный бизнес: Перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов XL Международной конференции РАЕН. Москва, 2017. – С. 71-74.
17. Кухаренко А.М., Салютина Т.Ю. Стратегическое обоснование инновационного развития – основа эффективного управления инфокоммуникационными компаниями // В сборнике: технологии информационного общества. Сборник трудов XIV Международной отраслевой научно-технической конференции, 2020. – С. 355-357.
18. Кухаренко Е.Г. Исследование эволюции маркетинговых концепций в инфокоммуникационном бизнесе // T-Comm: Телекоммуникации и транспорт, 2015. – Т. 9. – № 9. – С. 72-75.
19. Кухаренко Е.Г., Чугин И.С., Аношкина Е.С. Телекоммуникации как основа функционирования ситуационных центров глав субъектов Российской Федерации

// Экономика и качество систем связи, 2017. – № 4 (6). – С.10-19.
20. Кухаренко Е.Г., Асташков К.В. Применение проектного управления в инфокоммуникациях / В сборнике: Технологии информационного общества. Сборник трудов XII Международной отраслевой научно-технической конференции, 2018. – С. 348-350.
21. https://digital.gov.ru/ru/activity/statistic/. Дата обращения 18.05.2021.
22. Веерпалу В.Э., Володина Е.Е., Девяткин Е.Е., Девяткина М.Е. Инновационные методы регулирования использования радиочастотного спектра // Электросвязь, 2014. – № 10. – С. 17-21.
23. Володина Е.Е., Кузовкова Т.А., Нарукавников А.В. Возмещение использования радиочастотного спектра как экономический метод эффективного управления ограниченным природным ресурсом // Вестник РАЕН, 2011. – Т. 11. – № 4. – С. 103-108.
24. Кухаренко Е.Г., Токмачев С.С. Сравнительный анализ методических подходов к управлению проектами и их применение в инфокоммуникациях // T-Comm: Телекоммуникации и транспорт, 2012. – Т. 6. – № 12. – С. 64-65.
25. Кухаренко Е.Г. Анализ бизнес-моделей построения мульти-операторских сетей подвижной связи // В книге: Мобильный бизнес: Перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов XLII Международной конференции РАЕН. Москва, 2018. – С. 104-107.
26. Кухаренко Е.Г., Гервер В.А. Оценка эффекта от внедрения агрегационной модели кросс-функционального взаимодействия участников рынка мобильного контента // T-Comm: Телекоммуникации и транспорт, 2014. – Т. 8. – № 7. – С. 57-59.
27. Кухаренко Е.Г., Гервер В.А. Разработка модели кросс-функционального взаимодействия операторов на рынке услуг мобильного контента / В сборнике: Труды Московского технического университета связи и информатики. – М.: «ИД Медиа Паблишер», 2008. – Т. 2. – С. 240-243.
28. Кухаренко Е.Г., Иванченко П.А. Развитие методов управления производственной деятельностью компании на рынке услуг подвижной связи на основе управления жизненным циклом новых услуг. – М.: Компания Спутник +, 2005. – 52 с.
29. Кухаренко Е.Г., Сундикова Е.В. Тенденции развития мобильного бизнеса // В книге: Мобильный бизнес: Перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов XLII Международной конференции РАЕН. Москва, 2018. – С. 131-135.
30. Кухаренко Е.Г., Бецков Г.А. Проблемы и перспективы развития виртуальных операторов сотовой подвижной связи в России и в мире//Труды Московского технического университета связи и информатики. – М.: "ИД Медиа Паблишер", 2007. – С. 302-306.
31. Кухаренко Е.Г., Николаева Е.А. Тенденции развития цифрового бизнеса в банковской сфере россии / В сборнике: Технологии информационного общества. Сборник трудов XV Международной отраслевой научно-технической конференции «Технологии информационного общества», 2021. – С. 264-265.
32. Кухаренко Е.Г., Бецков Г.А. Исследование бизнес-стратегий мобильных операторов наложенных сетей в России / В сборнике: Труды Московского технического университета связи и информатики. – М.: "ИД Медиа Паблишер", 2008. – Т. 2. – С. 231- 239.
33. Кухаренко Е.Г., Бецков Г.А. Исследование факторов, влияющих на деятельность мобильных операторов наложенных сетей в России // T-Comm:

Телекоммуникации и транспорт, 2009. – № S3. – С. 21-22.

УСКОРЕННОЕ РАЗВИТИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПЕРИОД ПАНДЕМИИ

В.В. Макаров, *д.э.н., профессор, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, akad.makarov@mail.ru;*
Т.А. Блатова, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, nsnlon@gmail.com;*
Е.Ю. Ворошилова, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, ekon_up@sut.ru.*

УДК 330.341.42

Аннотация. Пандемия показала, что рынок информационных технологий способен быстро и эффективно адаптироваться к меняющимся условиям. Самыми популярными направлениями прошлого года стали искусственный интеллект, облачные сервисы, приложения для видеоконференцсвязи и решения для обеспечения информационной безопасности в домашней сети. В настоящее время их популярность продолжает расти.

Ключевые слова: информационные технологии; пандемия; искусственный интеллект; цифровизация, блокчейн.

ACCELERATED DEVELOPMENT OF INFORMATION TECHNOLOGY DURING THE PANDEMIC

Vladimir Makarov, *St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich;*
Tatyana Blatova, *St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich;*
Ekaterina Voroshilova, *St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich.*

Annotation. The pandemic has shown that the information technology market is able to adapt quickly and effectively to changing conditions. The most popular areas of the last year were artificial intelligence, cloud services, video conferencing applications and solutions for ensuring information security in the home network. Currently, their popularity continues to grow.

Keywords: information technology; pandemic; artificial intelligence; digitalization; blockchain.

Введение

Весь мир вот уже второй год живет в условиях пандемии. Нынешние обстоятельства кардинально меняют нашу жизнь и заставляют нас приспосабливаться к новой реальности. Распространение *COVID*-19 произошло в период активной фазы цифровой трансформации бизнеса в различных странах мира и невольно ускорило реализацию накопленного потенциала использования информационных технологий во многих секторах экономики. Гораздо более активно, чем до пандемии, информационные технологии стали использовать в

здравоохранении, образовании, государственном управлении, финансах, торговле и т. д. Активно пересматриваются подходы к развитию телекоммуникационной инфраструктуры, защите персональных данных и другим смежным вопросам.

Влияние пандемии на развитие информационных технологий

Проблемы, связанные с оптимизацией бизнеса актуальны всегда, но в такие периоды времени, как сейчас, они стоят особенно остро. Сегодня, как никогда, важно для пострадавших от пандемии компаний быстро находить точки оптимизации, а для компаний, показавших рост (фармацевтические компании, интернет-магазины, телекоммуникации и др.), важно поддерживать высокий уровень качества обслуживания клиентов. С помощью информационных технологий эти вопросы можно решать достаточно быстро и эффективно.

Пандемия *COVID*-19 не только поставила общество перед лицом новых глобальных вызовов, но и спровоцировала ускоренное развитие некоторых технологических тенденций, например, таких, как онлайн-платежи, телемедицина и робототехника. В конце 2002 г. вспышка атипичной пневмонии (*SARS-CoV*) привела к значительному увеличению числа онлайн-торговых платформ в Китае, как в секторе *B*2*B*, так и в секторе *B*2*C*. Точно так же *COVID*-19 превратил онлайн-продажи из дополнительной выгоды в абсолютную необходимость для бизнеса по всему миру [1].

Одной из наиболее заметных тенденций стал спрос на общедоступные облачные сервисы и технологии. Этот сегмент показал сильный рост в последние годы – только в России облачный хостинг *IaaS, PaaS* и другие инфраструктурные услуги выросли, по данным РАЭК, на 19% в 2019 г. Внутреннее исследование *Red Hat Global Customer Tech Outlook* 2020 показало, что 31% клиентов выбрали гибридно-облачную модель своей структуры, а 18% запустили проекты цифровой трансформации, и это еще до пандемии [2].

В первой половине 2020 г. мы увидели огромный рост интереса к облачным и цифровым платформам. Раньше компании использовали собственные серверы для разработки и обслуживания процессов, но теперь им нужны облачные платформы для обеспечения удаленной работы сотрудников в офисах, центрах обработки вызовов, отделах обслуживания клиентов, доступа к *CRM*-системам, корпоративным каталогам и приложениям. Встал вопрос об оптимизации рутинных процессов, таких как мониторинг и обслуживание инфраструктуры.

Очевидно, что потребность в облачных сервисах сохранится еще долгие годы. Облачные приложения станут незаменимыми в здравоохранении, недвижимости, телекоммуникациях и других отраслях.

Облачные сервисы, искусственный интеллект и другие новые цифровые технологии положили начало второй эпохе цифровизации, которая становится вызовом экономической политике [3]. В период пандемии информационные технологии помогают уменьшить распространение вируса, одновременно позволяя предприятиям поддерживать свою деятельность. Кроме того, такие технологии могут помочь обществу стать более гибким и устойчивым и к другим угрозам. Информационные технологии не только играют решающую роль в поддержании устойчивого функционирования общества в условиях карантина и вынужденной изоляции во время пандемии, но и могут оказывать более долгосрочное воздействие после окончания *COVID*-19.

Существующие ИТ-решения

Пандемия *COVID*-19 выявила настоятельную необходимость перестройки системы общественного здравоохранения с реактивной на проактивную и разработки инноваций, которые будут предоставлять информацию в режиме реального времени для проактивного принятия решений на местном, государственном и национальном уровнях систем общественного здравоохранения. *COVID*-19 отличается от хронических заболеваний тем, что он очень заразен, может передаваться от человека к человеку и имеет высокий уровень смертности. Кроме того, поскольку *COVID*-19 является новым заболеванием, научное понимание вируса и действия правительств и организаций по его предотвращению продолжают развиваться.

Некоторые новые технологические приложения, такие как мобильные приложения для отслеживания контактов *COVID*-19 и чат-боты, были недавно разработаны для борьбы с пандемией. Применение этих технологий может помочь уменьшить влияние пандемии коронавируса на людей, организации и общество. Эффективное и инновационное использование новейших технологий может помочь выявить распространение коронавируса в обществе, контролировать состояние инфицированных пациентов и помочь в разработке медицинских методов лечения и вакцин.

Технологии, основанные на искусственном интеллекте (ИИ), включая машинное обучение, распознавание изображений и алгоритмы глубокого обучения, могут быть использованы для раннего обнаружения и диагностики инфекции. Несколько компаний уже перепрофилировали существующие системы искусственного интеллекта, которые первоначально были разработаны для других областей, чтобы помочь в обеспечении соблюдения социального дистанцирования и отслеживании контактов [4].

Технология 3*D*-печати может помочь сделать маски для лица и другие средства индивидуальной защиты для медицинских работников. Анализ больших данных может быть использован для идентификации людей, нуждающихся в карантине, на основе их истории путешествий для прогнозирования кривой *COVID*-19.

HPC-инфраструктуры и суперкомпьютеры необходимы для решения сложных научных задач и обработки больших массивов данных в более короткие сроки для ускорения разработки противовирусных препаратов и вакцин. Консорциум высокопроизводительных вычислений *COVID*-19 был создан для использования вычислительных ресурсов и суперкомпьютеров в США и включает в себя 16 государственных и частных организаций.

Мобильные приложения с помощью смартфонов и средств видеоконференцсвязи могут использоваться для отслеживания перемещений людей, оповещения людей о посещении «горячих точек» *COVID*-19, помощи врачам в диагностике пациентов с помощью видеосервисов и телемедицины, поддержки жизнедеятельности людей с помощью онлайн-покупок, электронного обучения, онлайн-конференций и удаленной работы.

Роботы были применены для борьбы со вспышкой коронавируса. Например, больницы используют роботов в качестве вспомогательных систем для доставки еды и лекарств, дезинфекции помещений без непосредственного взаимодействия человека с пациентами. Дроны также используются для доставки медикаментов, патрулирования общественных зон, отслеживания несоблюдения карантинных предписаний и т. д.

Интернет вещей (*IoT*) может быть использован для наблюдения за людьми, инфицированными коронавирусом, чтобы уменьшить распространение коронавируса. *IoT* состоит из нескольких функциональных компонентов: сбора, передачи, анализа и хранения данных. Для сбора данных могут использоваться датчики Интернета вещей, установленные на смартфонах, роботах или мониторах здоровья, которые затем отправляются на облачный сервер для обработки, анализа и принятия решений. Например, *IoT* помогает проверить, соблюдают ли пациенты требования карантина. *IoT* также можно использовать для измерения температуры удаленных пациентов, а затем передавать данные через мобильные устройства врачам для мониторинга, отслеживания и оповещения, снижая при этом вероятность заражения коронавирусом. Дополнительные роли технологий Интернета вещей включают использование интеллектуальных носимых устройств при ранней диагностике *COVID*-19, карантине и после выздоровления [5].

Блокчейн можно сравнить с технологией распределенной бухгалтерской книги, в которую записывается онлайн-транзакции. В блокчейн применяется высокая степень шифрования данных, почти полностью защищающая их от несанкционированного доступа. В период пандемии было разработано приложение для смартфонов, использующее технологии блокчейн и искусственного интеллекта. Технология блокчейн позволяет приложению предоставлять каждому участнику «цифровую идентификацию», контролируемую закрытым ключом, который обеспечивает доступ к цифровой версии бумажных сертификатов, выданных правительством, например, для возможности выхода из дома на работу.

В ряде стран были разработаны и внедрены приложения отслеживания контактов в качестве стратегии общественного здравоохранения. Для отслеживания контактов использовались различные технологии и функции, встроенные в платформы мобильных телефонов, такие как *GPS, Bluetooth, Wi-Fi* и *QR*. Однако очень быстро встали вопросы по конфиденциальности и безопасности данных, так как начали появляться многочисленные сообщения о взломах, ошибках и неправильном использовании данных. Некоторые из этих приложений были запрещены. Исследование существующих и потенциальных применений технологии блокчейн для медицинской помощи показало, как распределенная структура управления и сохраняющие конфиденциальность функции блокчейна могут быть использованы для создания систем, которые могут помочь разрешить напряженность между поддержанием конфиденциальности и удовлетворением потребностей общественного здравоохранения в борьбе с *COVID*-19 [6].

Все вышеперечисленные технологии и созданные на их базе решения для борьбы с пандемией представлены в табл. 1.

Таблица 1.

Технологии	**Решения для борьбы с *COVID*-19**	**Данные**
Машинное обучение/Глубокое обучение	Анализ эпидемических ситуаций	Информация в режиме реального времени
	Диагностический и прогностический анализ	Изображения компьютерной томографии
	Автоматическое обнаружение случаев *COVID*-19	Необработанные рентгеновские снимки

Технологии	Решения для борьбы с *COVID*-19	Данные
	Ранняя сортировка критически больных пациентов с *COVID*-19	Медицинские карты лабораторно подтвержденных госпитализированных пациентов
	Раннее выявление и диагностика	Интеллектуальная трассировка контактов на основе данных мобильных датчиков и других данных наблюдения
Аналитика больших данных	Отслеживание перемещений людей, понимание эпидемических тенденций	Данные от смартфонов, умных браслетов и часов пользователей
Роботы	Доставка продуктов питания и медикаментов, дезинфекция помещений	
Технология 3*D*-печати	Производство средств индивидуальной защиты	
Цифровая технология отслеживания контактов	Отслеживание перемещения людей, предупреждение о посещении «горячих точек» *COVID*-19	Мобильные данные, данные социальных сетей
Блокчейн	«Цифровая идентификация» людей	Данные о здоровье, связанные с *COVID*-19

***Zoom Video Communications* – бенефициар пандемии**

В период пандемии *Zoom* стал одним из ведущих инструментов, с помощью которых предприятия продолжали работать, а школьники и студенты продолжали учиться. По данным исследовательской фирмы *Apptopia,* 11 марта 2020 г. приложение *Zoom* скачали 343 000 человек по всему миру. Всего два месяца до этого эта цифра составляла 90 000 человек во всем мире [7].

В 2020 г. *Zoom* стал «социальной средой *COVID*-19»: он не только превзошел корпоративных конкурентов, таких как *Webex, Skype* и *Google Meet*, но и стал частью жизни людей [8].

По итогам работы в 2020 г. выручка компании *Zoom Video Communications* выросла на 326% и составила $2,65 млрд, в четвертом квартале – на 369%, до $882,5 млн. Годовая чистая прибыль составила $671,5 млн, квартальная чистая прибыль выросла в 17 раз, до $260,4 млн. Скорректированная прибыль *Zoom* приблизилась к отметке в $1 млрд – она составила $995,7 млн по сравнению со $101,3 млн годом ранее. После публикации отчетности акции компании выросли на 11%, в ходе торгов они достигли $416,2 за акцию [9].

Финансовому подъёму компании способствовала пандемия *COVID*-19, которая привела к резкому росту спроса на услуги видеоконференцсвязи. А некогда слабый контроль конфиденциальности помог сделать *Zoom* чрезвычайно простым в использовании, что стало одной из причин его популярности для проведения онлайн-занятий и деловых встреч. Кроме того, *Zoom* предлагает бесплатную версию своего сервиса, что является еще одним неоспоримым плюсом.

Издание *Financial Times* отмечает, что аналитики прогнозируют сервису спад на фоне перехода работы и обучения обратно в офлайн-формат. Сама компания, однако, прогнозирует дальнейший рост выручки на 43% до $3,76-3,78 млрд [10].

Проблемы при внедрении информационных технологий

В настоящее время большинство информационных систем и приложений, которые использовались для борьбы с пандемией, слабо взаимосвязаны, поскольку они разрабатываются различными правительственными учреждениями, органами здравоохранения и организациями. Не хватает систематических инструментов для достижения интеграции различных технологий в рамках глобального реагирования на пандемические вызовы. Из-за отсутствия стандартов интеграция нескольких источников данных для обеспечения интероперабельности является сложной задачей. Существует также необходимость в создании стандартизированных протоколов для облегчения связи между системами без ущерба для информационной безопасности данных.

Информационная безопасность является всегда проблемой для любой организации, которая использует ИКТ. Данные должны быть надежно защищены, интернет-соединения должны быть защищены от атак, новых вирусов и других видов вредоносных программ, которые появляются почти каждый день [11].

Пандемия обозначила такую проблему, как цифровой разрыв. В широком смысле он означает неравномерный доступ к цифровому контенту или соединению. Способность людей эффективно использовать технологии остается неодинаковой (например, малоимущие слои населения, пожилые люди и лица с ограниченными возможностями). По мере того, как новые технологии, такие как мобильные приложения, ИИ, *IoT* и аналитика больших данных все чаще используются для борьбы с пандемией, существующие различия, неравенство и предубеждения еще больше усиливаются.

Цифровизация госсектора в России

В России с приходом пандемии резко ускорилась давно назревавшая цифровизация государственного сектора. Процесс цифровизации госсектора начался задолго до пандемии *COVID*-19: в 2017 г. Правительство РФ утвердило программу «Цифровая экономика Российской Федерации», цель которой – построение экосистемы цифровой экономики. Коронакризис ускорил цифровизацию и побудил правительство пересмотреть ранее принятые подходы [12].

В России реакция цифрового государства на пандемию была не идеальна. С введением пропусков многие регионы дали возможность оформить их в цифровом виде только после появления больших очередей за бумажными документами. В Москве приложение по контролю за соблюдением изоляции зараженных инфекцией граждан «Социальный мониторинг» неоднократно штрафовало пользователей, которые не нарушали правил, правда в последствии штрафы все же отменяли. Однако позже по номеру штрафа стало возможным получить доступ к личным данным пользователя. Государственные сайты не работали должным образом из-за большого количества запросов.

Но в то же время спустя пару месяцев российским чиновникам удалось продвинуться в вопросах цифровизации государственного управления. В конце марта 2020 г. был принят ряд документов о государственной поддержке отдельных групп населения. Для своевременного выполнения этих обязательств

правительство начало расширять использование онлайн-инструментов при предоставлении государственных услуг.

Основной площадкой для внедрения новых услуг остался портал «Госуслуги», на котором сразу появились все меры поддержки, вводимые государством [13]. Процедура получения «коронавирусных» пособий разрабатывалась с учетом дистанционного формата. Кроме того, на сайте можно было также удаленно подать заявление на пособие по безработице и получить больничный

Заключение

До начала пандемии коронавируса бизнес жил по известным правилам, с определенным образом выстроенными процессами. Например, бизнес практически не обращал внимания на инструменты удаленной работы. Подходы к формированию ИТ-инфраструктуры во многих компаниях были консервативными и основывались на приоритете информационной безопасности.

Пандемия изменила все. ИТ-индустрия стала одним из основных драйверов экономики. Организации, даже далекие от ИТ, остались на плаву только потому, что смогли быстро перевести сотрудников на удаленную работу и перенаправить свои производственно-сбытовые цепочки в цифровое пространство. Технологические решения обеспечили инфраструктуру и непрерывность процессов при работе в сети.

ИТ-индустрия как в мире, так и в России, достаточно уверенно пережила первую и вторую волны пандемии. В первую очередь рост обеспечили решения, связанные с цифровой трансформацией компаний. Ситуация с коронавирусом резко ускорила цифровизацию даже традиционных отраслей экономики. Основными точками роста в постковидном мире в сфере информационных технологий станут направления, которые помогают бизнесу нормально функционировать в новых условиях – облачные и периферийные вычисления, кибербезопасность, аналитика, искусственный интеллект, Интернет вещей, мобильные решения и другие технологии.

Очевидно, изменятся и требования к созданию информационных систем и сервисов для государства. Пандемия показала, что многие системы не выдерживают пиковых нагрузок. Это означает, что многим системам регионального и федерального уровней необходимо будет пересмотреть обеспеченность аппаратными мощностями, отказоустойчивость и функциональность ранее разработанных платформ и решений. Это может стать катализатором импортозамещения.

Аргументы в пользу цифровой трансформации никогда не были актуальнее, чем сейчас. Цифровые технологии не смогут предсказать «следующую пандемию», но они обеспечат гибкость и мобильность, которые позволяют справляться с *COVID*-19 сейчас.

Литература

1. Цифровизация и COVID-19: 10 технологических трендов в период пандемии // Rights Business Standard URL: https://rbs.partners/mediatsentr/tsifrovizatsiya-i-covid-19-10-tekhnologicheskikh-trendov-v-period-pandemii (дата обращения: 06.06.2021).
2. Исследование РАЭК: Экономика Рунета в эпоху COVID-19 растем и трансформируемся // Ассоциация электронных коммуникаций (РАЭК) URL: https://raec.ru/live/raec-news/11580/ (дата обращения: 05.06.2021).

3. Блатова Т.А., Макаров В.В., Шувал-Сергеева Н.С. Количественные и качественные аспекты измерения цифровой экономики // Радиопромышленность, 2019. – № 4. – С. 63-72.
4. Sipior J.C. Considerations for development and use of AI in response to COVID-19 // International Journal of Information Management, 2020. – Т. 55. – С. 102170.
5. Nasajpour M. et al. Internet of Things for current COVID-19 and future pandemics: An exploratory study // Journal of healthcare informatics research, 2020. – С. 1-40.
6. Khurshid A. Applying blockchain technology to address the crisis of trust during the COVID-19 pandemic // JMIR medical informatics, 2020. – Т. 8. – № 9. – С. e20477.
7. Главный сервис на время пандемии: как Zoom попал в тройку самых скачиваемых приложений // Forbes URL: https://www.forbes.ru/milliardery/395573-glavnyy-servis-na-vremya-pandemii-kak-zoom-popal-v-troyku-samyh-skachivaemyh (дата обращения: 01.06.2021).
8. Стал синонимом видеосвязи за 2020 год: что помогло Zoom обогнать Microsoft и Cisco и сможет ли он удержать лидерство // VC URL: https://vc.ru/services/187670-stal-sinonimom-videosvyazi-za-2020-god-chto-pomoglo-zoom-obognat-microsoft-i-cisco-i-smozhet-li-on-uderzhat-liderstvo (дата обращения: 02.06.2021).
9. Выручка Zoom выросла в четыре раза по итогам 2020 года // Sostav URL: https://www.sostav.ru/publication/vyruchka-zoom-47537.html (дата обращения: 05.06.2021).
10. Годовая прибыль Zoom приблизилась к $1 млрд // ТЕЛЕЦЕНТРЪ URL: https://tele-center.ru/news/godovaya-pribyl-zoom-priblizilas-k-1-mlrd-/ (дата обращения: 05.06.2021).
11. Шувал-Сергеева Н.С., Блатова Т.А., Макаров В.В. Внедрение информационнокоммуникационных технологий в организации: от оптимизации структуры до повышения конкурентоспособности // Радиопромышленность, 2017. – № 2. – С. 101-106.
12. Пандемия ускорила цифровую трансформацию госуправления // Аналитический центр при Правительстве Российской Федерации URL: https://ac.gov.ru/comments/comment/26560 (дата обращения: 05.06.2021).
13. Дмитрий Чернышенко: Цифровая платформа «Госуслуги. Решаем вместе» будет запущена во всех субъектах страны // Правительство России URL: http://government.ru/news/41722/ (дата обращения: 05.06.2021).

МОНЕТИЗАЦИЯ КРИПТОСАЙТОВ КАК НОВЫЙ СПОСОБ ЗАРАБОТКА В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Г.П. Платунина, *старший преподаватель, Московский технический университет связи и информатики, g.p.platunina@mtuci.ru;*
А.С. Старовойтова, *студент, Московский технический университет связи и информатики, star.anyta@yandex.ru.*

УДК 338

Аннотация. В данной статье приведен список лучших крипто-рекламных сетей для монетизации сайтов, обоснованы основные причины их использования. Выдвинуты гипотезы о дальнейшей судьбе существования данных платформ. Рассмотрена и проанализирована актуальная информация о текущем положении некоторых крипто-рекламных сервисов.

Ключевые слова: монетизация; крипто-реклама; блокчейн; цифровые технологии.

MONETIZATION OF CRYPTOSITES AS A NEW WAY OF EARNING IN THE CONDITIONS OF THE DIGITAL ECONOMY

Galina Platunina, *senior lecturer, Moscow Technical University of Communications and Informatics;*
Anna Starovoitova, *student, Moscow Technical University of Communications and Informatics.*

Annotation. This article provides a list of the best crypto-advertising networks for monetization of sites, justifies the main reasons for their use. Hypotheses are put forward about the future of the existence of these platforms. The current information about the current situation of some crypto-advertising services is considered and analyzed.
Keywords: monetization; crypto-advertising; blockchain; digital technologies.

В настоящее время, если у вас есть веб-ресурс, который посвящен обсуждению последних новостей о криптовалютах и блокчейне, то вполне реально получить от этого доход. Выгодно вести торговлю при помощи цифровой валюты в ситуации отсутствия допуска к данным было бы невозможно. Но каждый раз при посещении подобных сайтов появляется вопрос, об источниках их дохода.

Имеется ряд способов извлечения прибыли, которые используют инновационные сервисы, чтобы вознаграждать труд тех, кто каждодневно трудится над контентом. Потому что благодаря этим людям, происходит получение ограниченных знаний о рынке, которые так ценятся в настоящий момент.

В статье рассмотрены лучшие способы заработка с помощью крипто-сервисов, а также сделан анализ данной отрасли.

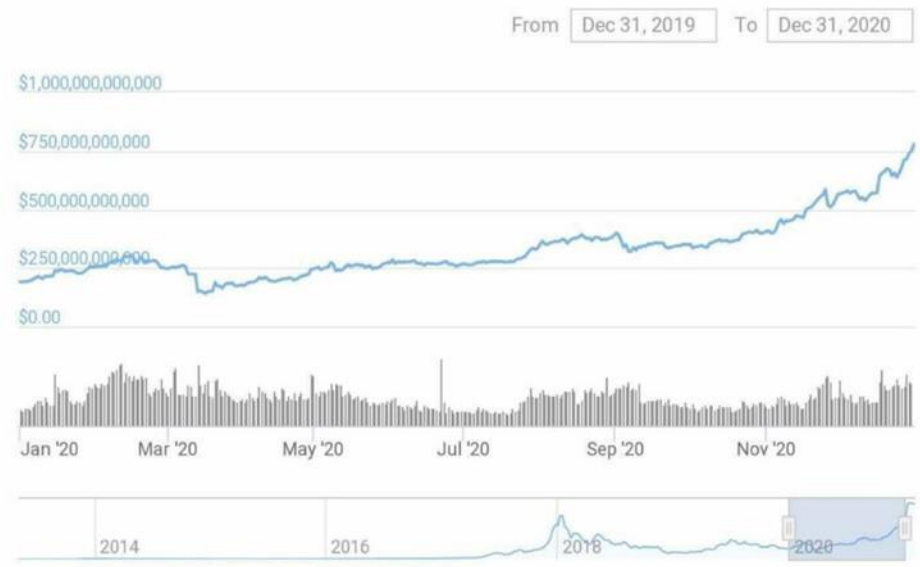

Рисунок 1

Криптовалюта приобрела небывалую популярность, чем когда-либо ранее. Но сейчас зарабатывают миллионы те, кто заранее вложил свои деньги в биткоин или эфириум. Трейдеры, устремляющиеся диверсифицировать собственные цифровые активы, переходят на другие денежные единицы, поэтому в

определенных населенных пунктах возникают биткойн-банкоматы. На рис. 1 показан график изменения общей капитализации криптовалют в 2020 г. [1].

Блокчейн эфириум является базой для огромного количества альткоинов, с помощью которых миллионы долларов уходят в сеть. В случае, если вы пишите о трендах криптовалют в сети, говорите об этом в *YouTube*, то существует большое количество методов монетизировать подписчиков. Для начала, необходимо поговорить о классических способах привлечения средств с помощью партнерских программ.

Именно с помощью таких программ удается стимулировать цифровую экономику [2-9]. Если вам необходимо приобрести какой-либо кейс, то вы всегда идете в интернет, например, Яндекс или *Google.* На данных страничках вы заметите гиперссылки на конкретные товары. Если перейти по данным ресурсам, то откроется соответствующая страница маркетплейса. Это и есть наглядный пример партнерских ссылок. Данные сайты предоставляют место для торговых площадок, и если вы приобретаете товары после перехода по их партнерской ссылке, то они получают хорошую скидку. Практически невозможно путешествовать по интернету, не встречаясь с партнерскими ссылками.

Однако в сфере криптовалют существование данных партнерских программ является довольно неоднозначным. *Google* воспрепятствовал использованию крипто-рекламы на своих сервисах, наряду с ним *Twitter* и *Facebook* имеют такую же точку зрения. Цифровые гиганты заявляют, что данное решение сопряжено с опасениями возникновения неконтролируемых афер на блокчейне, что в принципе обоснованно. Такие сайты, как *Bitconnect,* уличаются в том, что они являются финансовыми пирамидами, где трейдеры могут получить доход в случае, если они убедят других клиентов присоединиться. Но у *Google* могут быть также и иные причины не давать крипто-рекламе места на своих платформах.

Криптовалюты функционируют на технологии блокчейна, осуществляя сложнейшие вычислительные процессы. Рассредоточенная сущность данной технологии способна переломить многочисленные финансовые и политические концепции. *Google* – это цифровой лидер централизованных вычислений, и он с каждым днем старается приблизиться или даже перегнать блокчейн. *Google* поставил перед собой задачу сдержать пользователей от криптовалют вплоть до той поры, пока у них самостоятельно не получится извлечь прибыль из данной технологии. Спрос на криптовалютные сайты с каждым годом растет в геометрической прогрессии, поэтому увеличивая предложение подобных ресурсов, довольно рационально привлечь монетизацию [10].

Рекламная сеть с классическими алгоритмами, такая как *Google Adsense*, а также крипто-сервис *Conzilla* основана на рекламе, которая постоянно обновляется. Владелец предоставляет место для рекламы на своем сервисе, а рекламная сеть подбирает потенциальных покупателей, разделяя при этом полученные деньги с учетом существующих тарифов. При поддержке партнерских программ, таких как *Factbar,* у вас есть возможность регулировать контент, при этом все упоминания и ссылки всегда одобрены. Вы не получаете средства, когда пользователи читают или посещают ваш блог, но при совершении покупки криптовалют или перехода по рекламной ссылке возможно получить доход. Это является своеобразной гарантией качества того, что вы продвигаете или выставляете на своем веб-ресурсе [11,12].

На основе имеющихся данных, составлен список 10 лучших крипто-рекламных сетей для монетизации:

1. *Ad Dragon.*
2. *BitMedia.*

3. *CoinZilla.*
4. *Adshares.*
5. *A-Ads.*
6. *Cointraffic.*
7. *TokenAd.*
8. *Bitraffic.*
9. *AdEx.*
10. *CoinAd.*

Ad Dragon – это новейший сервис, а также первая площадка *DeFi.* Это одноранговая маркетинговая платформа. Она обладает значительным превосходством, так как считается инновационной, а не подобием сервиса *Google.*

Продавцы формируют интернет-магазин на платформе *Ad Dragon* и реализуют свои рекламные услуги. У них имеется абсолютная свобода оценивать свой товар так, как пожелают, ибо они могут продавать практически любую услугу, которую они хотят. На данной площадке рекламодатели оценивают рынок и подбирают различные способы продвижения собственного крипто-бизнеса в устраивающем их ценовом сегменте [13].

Ad Dragon имеет огромное преимущество относительно своей платежной системы. Ибо его платформа базируется на эфириуме, который знаменит своей децентрализацией кошелька. Это увеличивает скорость операции в десятки раз. Если вы разыскиваете что-то новое и действенное, то вам необходимо обратить внимание на *Ad Dragon.*

BitMedia – это еще одна платформа для выгрузки крипто-рекламы, которая предлагает пользователям получить запрашиваемую услугу за невысокую стоимость. Различные типы таргетинга доступны рекламодателям, который учитывает геопозицию, устройство и время подключения. На данный момент, *Bitmedia* предоставляет рекламу только в текстовой и баннерной форме.

Bitmedia.io старается предоставить своим пользователям максимально правдивую и качественную рекламу, поэтому любое коммерческое предложение проходит жесткий контроль по следующим пунктам: время выполнения запроса, стороннее управление трафиком, пост-верификация трафика, а также ручная настройка показов.

Данные проверки предусмотрены с целью фильтрации коммерческого трафика, скрытых показов рекламы и ботов. Покупатели получают компенсацию в случае ошибочных показов, и помимо этого рекламодатели могут не вносить оплату по причине некачественного предоставления услуги для бизнеса [14].

Coinzilla – одна из самых популярных и проверенных крипто-рекламных сетей. Несмотря на то, что она появилась сравнительно недавно, все равно смогла завоевать доверие пользователей и рекламодателей. *Coinzilla* является частью *AdSelvo*, главной задачей которой было продвижение крипто-рынка, это в свою очередь помогло с решением многих маркетинговых проблем.

Данная крипто-рекламная сеть занималась продвижением около 200 брендов и содействовала партнерству со многими рекламодателям в процессе монетизации.

Если вы желаете присоединиться к сети *Coinzilla,* то ваш веб-сайт обязан существовать более трех месяцев, иначе невозможно будет пройти модерацию. Эффективность и показатели данной платформы завоевали доверие пользователей, так как с его помощью происходит взаимодействие между реальными людьми, а не машинами.

Adshares начало свое зарождение с небольшого масштаба, но с полной уверенностью того на какой технологии работать, и выбор был сделан в пользу блокчейна. Именно поэтому существует возможность заключать прямые сделки с рекламодателями.

Adshares предоставляет клиентам корректную, дешевую и независимую от цензуры рекламу. Блокчейн данной платформы может подвергать обработке одновременно около одного миллиона переводов в секунду, благодаря этому он способен управлять мировым рекламным рынком.

Помимо этого, *Adshares* является одним из самых высокотехнологичных проектов. Благодаря ему происходит разрешение трудностей на цифровом рынке [15, 16]. Его суть сконцентрирована на маркетинговой системе, т.е. транзакции между рекламодателями происходят в криптовалютах.

Самое приятное, что *Adshares* функционирует только лишь в то время, если пользователь запускает *Adblocker*. Это дает возможность издателям получать доход моментально или же ежечасно.

A-Ads принято считать первой крипто-рекламной сетью на рынке, которая появилась в 2011 г. и с этих времен хранит идеальную бизнес репутацию. В настоящее время *A-Ads* пользуется огромной популярностью, о чем свидетельствует статистика. Более 100 млн показов собирается каждый день. На рис. 2 показана статистика показов рекламной сети *A-Ads* [17].

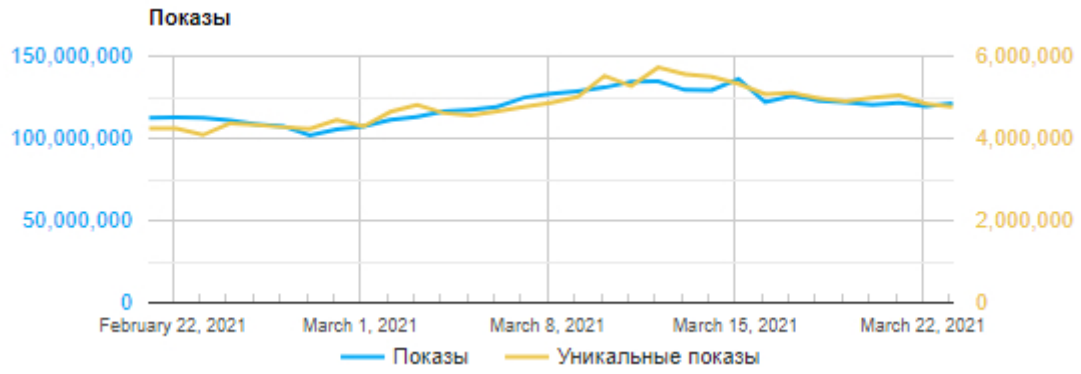

Рисунок 2

Данная площадка имеет наглядный интерфейс и проста в использовании, поэтому, чтобы создать рекламную интеграцию вам понадобится пару минут. *A-Ads* дает возможность выделять определенных рекламодателей, чтобы их быстро различать. Для этого вводятся специальные теги, и при желании можно настроить фильтр для рекламы с желаемой тематикой.

Cointraffic – весьма знаменитая платформа для крипто-рекламы, основанная в Таллинне. Она была создана для облегчения публикации баннеров и рекламных интеграций издателями. Это содействует развитию вашего веб-сайта.

Cointraffic является престижным цифровым партнером в крипто-сфере. Взаимодействия между пользователями контролируются обученными менеджерами, которые и будут нести ответственность за продвижение рекламной компании.

TokenAd входит в список лучших крипто-рекламных платформ для издателей, трудящихся в маркетинговой сфере *RTB*, которая в существенной мере сконцентрирована на продвижении криптовалютных новостей и сервисов.

TokenAd вмещает в себя различные типы рекламы, например, баннерную или традиционную. Сервис имеет довольно доступный интерфейс и дает возможность отображать на веб-сайте только крипто-рекламу.

Bidtraffic, выпущенная в ноябре 2017 г. крипто-рекламная платформа считается самой крупной, функционирующей на просторах 2700 веб-сайтах. Она имеет огромное практическое значение в вопросах, касающихся развития торговли, токенов, игр и прочих приложений. *Bidtraffic* оснащен анти-ботовой технологией и гарантирует высокий уровень показа каждый день [18].

AdEx – это прогрессивная рекламная сеть, базирующаяся на цифровых цепочках. Главной задачей, которой является контроль проблем, оказывающих влияние на эффективность рекламных интеграций [19].

Платформа оснащена большим количеством инструментов, позволяющих выполнять поставленную задачу быстро и качественно. Благодаря этому, в 2021 г. показатели стоимости *AdEx Network* стремительно растут. На рис. 3 показана динамика стоимости *AdEx Network* [20].

Рисунок 3

CoinAd является крипто-рекламной платформой, имеющей ряд довольно жестких правил для рекламодателей. Так как утверждение на публикацию проходят сайты, имеющие рейтинг *Alexa* ниже 100К и уровнем показов в день не ниже двухсот. Также существует ограничение по времени существования. Новые веб-сайты не допускаются к рассмотрению. Новые рекламодатели могут получить доступ только по приглашению, так как система является закрытой. Несмотря на затруднительную систему вступления, издание на данном ресурсе считается престижным и надежным.

Заключение

Проблемы, связанные с монетизацией крипто-сайтов, остро ощущаются в наши дни. Несмотря на тотальный отказ цифровых гигантов на осуществление рекламной кампании по отношению к криптовалютам, индустрия по продвижению биткоин-трафика набирает обороты с каждым днем.

В случае отсутствия подходящих платформ для размещения, все больше и больше компаний начнут отдавать предпочтение сетям, обеспечивающим хороший трафик и надежную информацию. Но перед началом использования рекламной сети, необходимо здраво оценить положительные и отрицательные черты каждой из них, проследить показы и качество публикуемой информации.

Очевидно, что сейчас подобные сервисы обошли традиционные СМИ и развиваются в ускоренном темпе, и поэтому путь к прибыли сейчас открыт как никогда раньше.

Литература

1. URL https://changehero.io/blog/ru/2021-top-crypto-predictions/ (Дата обращения 20.03.2021).
2. Платунина Г.П., Васильева И.А. Проблемы информационной безопасности России в условиях кризисного развития мирового экономического сообщества на современном этапе // В книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) XLIII международной конференции РАЕН, 2019. – С. 73-77.
3. Володина Е.Е., Веерпалу Д.В. Анализ развития цифрового телевидения в мире и в России // T-Comm: Телекоммуникации и транспорт, 2013. – Т. 7. – № 12. – С. 23-26.
4. Володина Е.Е. Прогнозирование развития инновационных услуг в сфере инфокоммуникаций // Инновационное развитие экономики, 2017. – № 5 (41). – С. 7-16.
5. Девяткин Е.Е., Володина Е.Е., Бессилин А.В. Прогноз развития рынка услуг наземной подвижной связи в России // Труды Научно-исследовательского института радио, 2010. – № 4. – С. 3-9.
6. Володина Е.Е., Девяткин Е.Е., Суходольская Т.А. Анализ развития интеллектуальных транспортных систем // Экономика и качество систем связи, 2017. – № 1 (3). – С. 40-46.
7. Володина Е.Е. Прогнозирование развития рынка услуг новых технологий мобильной связи / В сборнике: Стратегическое планирование и развитие предприятий. Материалы Восемнадцатого всероссийского симпозиума. Под редакцией Г.Б. Клейнера, 2017. – С. 921-925.
8. Volodina E.Eu. Models for predicting the development of the new mobile communication technologies market // Электросвязь, 2018. – № 2. – С. 60-66.
9. Володина Е.Е., Девяткин Е.Е., Суходольская Т.А. Перспективные радиотехнологии (сети 5G/IMT-2020, интернет вещей) в социально-экономическом развитии страны // В книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) XLII международной конференции РАЕН, 2018. – С. 135-138.
10. URL https://beincrypto.ru/learn/prognoz-kursa-bitkoina-btc-mneniya-ekspertov/ (Дата обращения 20.03.2021).
11. Платунина Г.П. Применение интерактивных технологий в процессе преподавания дисциплины «Интернет-реклама и PR» и совершенствование содержания курса // В сборнике: Технологии Информационного Общества. Сборник трудов XIV Международной отраслевой научно-технической конференции, 2020. – С. 571-572.
12. Платунина Г.П. CRM-система как средство повышения эффективности бизнеса // В книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом сборник материалов (тезисов) 45-й международной конференции РАЕН, 2020. – С. 55-59.
13. Григоренко Е.Р., Платунина Г.П. Методические основы и инструменты реинжиниринга бизнес-процессов деятельности компании // В сборнике: Технологии Информационного Общества. Сборник трудов XIV Международной отраслевой научно-технической конференции, 2020. – С. 327-329.
14. Платунина Г.П., Старовойтова А.С. Оценка регулирования антимонопольной политики России в условиях кризиса // В сборнике: Технологии Информационного Общества. Сборник трудов XIV Международной отраслевой научно-технической конференции, 2020. – С. 365-367.

15. Платунина Г.П., Васильева И.А. Управление бизнес-процессами инфокоммуникационных компаний в условиях трансформации мирового экономического общества // Экономика и качество систем связи, 2020. – № 1 (15). – С. 22-29.
16. Салютина Т.Ю., Платунина Г.П. Методические основы формирования параметров модели оценки инвестиционной привлекательности телекоммуникационной компании // В книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 46-й международной конференции. Москва, 2020. – С. 67-70.
17. URL https://a-ads.com/stats (Дата обращения 21.03.2021).
18. URL https://profinvestment.com/cryptocurrency-earnings/ (Дата обращения 23.03.2021).
19. Платунина Г.П., Добычина И.В. Методические аспекты курсового проектирования по дисциплине "Экономика инфокоммуникаций и отраслевые рынки" для бакалавров направления "Прикладная информатика" // В сборнике: Технологии Информационного Общества. Материалы XIII Международной отраслевой научно-технической конференции, 2019. – С. 385-387.
20. URL https://coinmarketcap.com/ru/currencies/adx-net/ (Дата обращения 21.03.2021).

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ РОССИЙСКОГО ПРОИСХОЖДЕНИЯ В РАМКАХ РАЗВИТИЯ ПЕРСПЕКТИВНЫХ РАДИОТЕХНОЛОГИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ

А.С. Дунаев, *директор по правовым вопросам ООО «НСТТ», das@nxtt.org.*

УДК 621.391

Аннотация. В статье поднимаются вопросы, затрагивающие интересы российских производителей радиооборудования, предназначенного для развития новых инфокоммуникационных сетей 5-го поколения. Отмечаются противоречия в целях и задачах, поставленных регулятором, и мер реализуемых ГКРЧ, не способствующих, а тормозящих деятельность российских производителей в развитии российских инфраструктурных сетей.

Ключевые слова: цифровая экономика*; 5G;* российское производство; локализация; радиочастотный спектр; ГКРЧ (Государственная комиссия по радиочастотам).

TO THE QUESTION OF THE USE OF RADIO ELECTRONIC MEANS OF RUSSIAN ORIGIN IN THE FRAMEWORK OF THE DEVELOPMENT OF PERSPECTIVE RADIO TECHNOLOGIES IN THE RUSSIAN FEDERATION

Andrey Dunaev, *Director of Legal Affairs, LLC «NXTT».*

Annotation. The article discusses questions that affect the interests of Russian manufacturers of radio equipment intended for the development of new information communication networks of the 5th generation. There are contradictions in the goals and

objectives set by the regulator, and the measures implemented by the *SCRF*, which do not contribute to, but slow down the activities of Russian manufacturers in the development of Russian infrastructure networks.

Keywords: digital economy; 5*G*; Russian manufacture; localization; radio frequency spectrum; *SCRF* (State Commission on Radio Frequencies).

Цифровая экономика, инновационное развитие, создание и развитие новых высокотехнологичных производств, импортозамещение, поддержка отечественного производителя, создание конкурентоспособных технологий, связь 5*G*, энергосбережение, безопасный город и т.д. – всё это не просто модная терминология, это государственные программы развития, приоритетные и стратегические задачи, направленные на укрепление безопасности и суверенитета страны [1-4].

С печальной и постоянной повторяемостью правильные по своим целям государственные мероприятия превращаются в лозунги, устаревающие и сменяемые свежими декларациями.

Одной из основных причин отсутствия значимых результатов является недооценка ресурсов для реализации подобных программ: организационных, производственных, финансовых, интеллектуальных, информационных, и т.д. Причем, часто проблемой является не столько ошибка планирования в оценке необходимости и наличия ресурсов, а явная несостоятельность отраслевых регуляторов в организации процессов и мобилизации того немного, чем располагают государство и игроки на рынке [5-7].

Иллюстрацией заведомо ошибочной оценки ресурсов является, например, избранная регулятором форма реализации «Концепции создания и развития сетей 5*G/IMT*-2020 в Российской Федерации» [8, 9].

В соответствии с мартовским 2020 г. решением ГКРЧ операторам связи для развития технологии 5*G* предложен диапазон радиочастот 24,25-24,65 ГГц и уже имеющиеся в их распоряжении частоты. При этом при построении сетей 5*G* операторы обязаны использовать радиоэлектронные средства исключительно российского происхождения.

По поводу данного решения опубликовано значительное количество экспертных оценок с изложением причин, по которым мартовское решение ГКРЧ приведет всего лишь к «очень ограниченному развитию стандарта 5*G* в России»: это отсутствие у операторов необходимого для демонстрации реальных преимуществ 5*G* полосы радиочастот шириной 80-100 МГц, необходимость строительства значительного количества базовых станций, находящихся в прямой видимости из-за чувствительности радиосигнала в диапазоне 24,25-24,65 ГГц к любым препятствиям, полное отсутствие декларируемой госрегулятором «конверсии» частот, из-за чего такие перспективные диапазоны как 3,4-3,8 ГГц останутся занятыми силовыми ведомствами, отсутствие на мировом рынке оборудования 5*G* для диапазона 24,25-24,65 ГГц, т.к. будущие страны лидеры в мобильных подключениях 5*G*, такие как США, Китай, Южная Корея, Япония и страны ЕС, используют иные диапазоны частот [10-14]. Дополнительно экспертами разобраны все возможные экономические модели развития сетей 5*G* в различной комбинаторике как по способам кооперации операторов при построении сетей 5*G*, так и по идеологиям использования частот и замены существующего оборудования. По данным сценариям и оценкам сроки окупаемости затрат операторов на освоение технологии 5*G* колеблются от 2040 г. до «никогда».

По совокупности проблем, созданных указанным решением ГКРЧ, большинством специалистов сделан вывод: в России (в Москве) все же будет 5*G*, но очень ограниченно, очень дорого и не очень скоро.

Если принять во внимание дополнительное требование ГКРЧ «использовать при построении сетей 5*G* радиоэлектронные средства исключительно российского происхождения», можно было бы принять данные выводы в отношении возможности освоения технологии 5*G* наивно-оптимистичными, но содержание условия о российской локализации настолько нереалистично и нежизнеспособно, что серьезные люди просто понимают, что надо немного подождать соответствующих разъяснений о том, каким образом на продукцию *Huawei* можно будет повесить бирку «российский производитель» либо иных маневров ГКРЧ и Минкомцифры в отношении модификации и толкования собственного решения.

В этой связи, продолжение госрегулятором вектора поддержки отечественного производителя в форме озадачивания и бюджетного финансирования Ростеха в объеме 21,4 млрд. руб. в течение трех лет на создание собственной российской технологии и опытной сети 5*G* уже в 2022-2024 гг., исходя из того же ресурсного подхода, воспринимается скорее, как *PR*-акция в рамках модной программы с неизвестным, но вряд ли впечатляющим результатом.

Представители «Ростеха» заявляют, что общий бюджет всех мероприятий по развитию 5*G* в России, включая частные инвестиции, составляет 42,9 млрд. руб. На эти деньги планируется не только разработать отечественное оборудование, но также обеспечить его продвижение на зарубежном рынке. Для сравнения компания *Huawei,* которая борется за лидерство на рынке 5*G*-технологий, согласно информации на её сайте, планирует годовой объем затрат на научные исследования и опытно-конструкторские разработки (НИОКР или *R&D*) до 15-20 млрд. долл., при этом в НИОКР заняты около 80 тыс. ее сотрудников или порядка 45% от всего штата компании. У *Huawei* все в порядке с ресурсами: деньгами, интеллектуальной собственностью, научным потенциалом, материально-элементной базой, с эффективностью управления процессами и проектами, а также с мировой кооперацией.

В любом случае, сотовые операторы не будут ждать конца эксперимента с Ростехом они вынуждены будут расставить все приоритеты уже сегодня.

Скепсис в отношении возможностей Ростеха создать в полном объеме российский аппаратно-программный комплекс для технологии 5*G*, основан на сложившейся практике игнорирования «российского производителя», государственная поддержка которого осуществляется в виде лозунгов, компаний, эпизодически, непоследовательно и непродуктивно, а его дискриминация напротив проявляется системно, постоянно и комплексно.

Если в отношении отечественных разработчиков программного обеспечения в последнее время в связи с явными угрозами в области информационной безопасности приняты и нормативно закреплены меры государственной поддержки, в частности в Национальной программе «Цифровая экономика Российской Федерации», то в отношении производителей радиоэлектронного оборудования государством осуществляется политика двойных стандартов и дискриминации. Существующая нормативная среда, включая основополагающий Федеральный закон «О связи», и сложившаяся модель поведения отраслевых государственных органов власти ставят их в существенно неравное положение по сравнению с иностранными производителями и стимулируют импорт иностранного оборудования.

В соответствии с Федеральным законом «О связи» выделение полосы радиочастот решением ГКРЧ осуществляется не только для оказания услуг радиосвязи, но и для разработки, модернизации, производства в Российской Федерации и (или) ввоза в Российскую Федерацию радиоэлектронных средств с определенными техническими характеристиками. Это нормативное положение означает, что российский производитель вправе начать разработку или производство радиоэлектронного оборудования только после получения соответствующего разрешения ГКРЧ – коллегиального и очень эпизодически собирающегося органа, который по замыслу его создателей должен осуществлять только технические задачи регулирования использования радиочастотного спектра, т.е. определять кто и каким организационного-техническим образом может использовать радиочастотное пространство.

И в данном аспекте речь идет не о потенциальной возможности такого органа как ГКРЧ прямо вмешиваться в деятельность российских производителей еще на фазе их научных исследований и разработок, а о реальной практике правоприменения, причем, как часто встречается, с выходом за пределы его полномочий и разумных границ.

Например, 24 октября 2013 г. ГКРЧ своим решением выделила полосу радиочастот 9 кГц-275 ГГц неопределенному кругу лиц для разработки, модернизации и производства РЭС гражданского назначения на территории Российской Федерации для целей экспорта. Т.е. ГКРЧ разрешил всем разрабатывать РЭС, но возникают вопросы: почему только для целей экспорта и на каком основании данный государственный орган вообще диктует российскому производителю, что и для каких рынков сбыта ему создавать?

Ещё пример, 22 октября 2019 г. ГКРЧ в ответ на заявку Завода «Эталон» выносит решение: отказать ООО «Завод «Эталон» в выделении полос радиочастот 1785-1790 МГц и 1800-1805 МГц для проведения научных, исследовательских, опытных, экспериментальных и конструкторских работ в целях разработки и производства радиоэлектронных средств широкополосного беспроводного доступа на территории Российской Федерации.

Что делать заводу Эталон? Заключать соглашение на разработку и производство с братским народом Казахстана, с целью дальнейшего экспорта? Российский производитель просил разрешение не только на исследования и конструкторские работы, но и на производство и применение РЭС. В результате получил разрешение только на исследования в диапазоне радиочастот 1790-1800 МГц с фактическим запретом на производство и полный запрет на любую исследовательскую и производственную активность в диапазонах 1785-1790 МГц и 1800-1805 МГц.

В отношении любого зарубежного радиооборудования позиция российского регулятора гораздо более лояльная. Во всех решениях на использование радиочастотного ресурса ГКРЧ стандартно разрешает ввоз на территорию Российской Федерации РЭС, технические характеристики которых соответствуют техническим характеристикам, утвержденным решениями ГКРЧ. Это означает, что любое заинтересованное лицо вправе ввезти РЭС любого иностранного производителя, сертифицировать его на соответствие определенным техническим характеристикам и далее свободно, любыми партиями продолжать его ввоз и использование на территории России.

При наличии процедуры обязательной сертификации РЭС с целью их применения возникает вопрос – с какой целью и на каком основании такой орган как ГКРЧ занимается регулированием научно-исследовательской, опытно-

конструкторской и производственной деятельности российских коммерческих производителей?

Почему завод Эталон лишили права конкурировать с оборудованием, производимым *Huawei* не на этапе торгов по закупке РЭС, а еще на этапе исследований и производства.

Отсутствие системной поддержки отечественных производителей ощущается даже на примере документов стратегического характера, таких как Национальная Программа «Цифровая экономика Российской Федерации». Программа включает, в частности, проекты «Нормативное регулирование цифровой среды» и «Информационная инфраструктура», содержащие требования по созданию правовых условий для реализации Программы. Перечисленные мероприятия затрагивают, кажется, все, что хоть как-то сочетается с термином «цифровая экономика», все за исключением базового положения – производство отечественного оборудования, обеспечивающего выполнение задач Программы, в том числе содержащихся в разделе Информационная безопасность.

Между тем, такие области как бытовое применение технологий радиосвязи, всеобщий доступ к интернету и иное использование стандартным потребителем любых цифровых завоеваний цивилизации вполне могут обходиться без участия российского производителя. Потребитель вправе выбирать лучшее, что ему предложит мировой рынок. Наличие отечественного производителя в этом сегменте приветствуется только с точки зрения общего здоровья экономики в целом и поддержки отраслевого научного и промышленного потенциала.

Однако в таких важнейших сферах как технологические и иные сети связи, обслуживающие критически важные объекты, технологическая зависимость от иностранных производителей программного обеспечения и радиоэлектронных средств, обессмысливает все иные государственные мероприятия, направленные на обеспечение как суверенитета и безопасности государства, так целостности, устойчивости и безопасности таких сетей связи.

При существующей невнятной нормативной базе, деятельность такого регулятора как ГКРЧ, наделенного «всей полнотой полномочий», его бесконтрольное и нерациональное влияние на деятельность отечественных производителей, вне зависимости от формально декларируемых им целей и задач, фактически способствует формированию импортозависимости от иностранного радиооборудования. В свою очередь, импортозависимость в таких высокотехнологичных отраслях как производство РЭС, лишает государство возможности реализовать любую национальную программу в области, связанной с использованием такого высокотехнологичного оборудования.

Заключение

В рамках действующей нормативной базы предлагается принять основополагающий подход, при котором любое выделение полосы радиочастот для использования неопределенным кругом лиц либо конкретным лицом автоматически означает, что любой отечественный производитель вправе разрабатывать и производить радиоэлектронные средства с учетом установленных решением ГКРЧ технических параметров для выделенной полосы радиочастот.

Литература

1. Володина Е.Е., Веерпалу Д.В. Анализ развития цифрового телевидения в мире и в России // T-Comm: Телекоммуникации и транспорт, 2013. – Т. 7. – № 12. – С. 23-26.

2. Володина Е.Е. Прогнозирование развития инновационных услуг в сфере инфокоммуникаций // Инновационное развитие экономики, 2017. – № 5 (41). – С. 7-16.
3. Девяткин Е.Е., Володина Е.Е., Бессилин А.В. Прогноз развития рынка услуг наземной подвижной связи в России // Труды Научно-исследовательского института радио, 2010. – № 4. – С. 3-9
4. Девяткин Е.Е., Иванкович М.В., Володина Е.Е. Стратегическое управление сетями связи российской федерации как главная задача развития информационной инфраструктуры // Электросвязь, 2020. – № 9. – С. 24-29.
5. Володина Е.Е., Девяткин Е.Е., Юшков С.В. Экономико-правовые вопросы использования радиочастотного спектра в российской федерации // Электросвязь, 2014. – № 6. – С. 43-46.
6. Володина Е.Е., Гасс Я.М. Анализ развития перспективных радиотехнологий и проблемы их внедрения в регионах российской федерации // T-Comm: Телекоммуникации и транспорт, 2013. – Т. 7. – № 12. – С. 27-29.
7. Володина Е.Е. Прогнозирование развития рынка услуг новых технологий мобильной связи // В сборнике: Стратегическое планирование и развитие предприятий. Материалы Восемнадцатого всероссийского симпозиума. Под редакцией Г.Б. Клейнера. 2017. – С. 921-925.
8. https://digital.gov.ru/uploaded/files/proekt-kontseptsii-sozdaniya-i-razvitiya-setej-5g-imt-2020-v-rossijskoj-federatsii.pdf.
9. Володина Е.Е., Девяткин Е.Е., Суходольская Т.А. Перспективные радиотехнологии (сети 5G/IMT-2020, интернет вещей) в социально-экономическом развитии страны // В книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) XLII международной конференции РАЕН, 2018. – С. 135-138.
10. Володина Е.Е. Анализ особенностей радиочастотного спектра и потребностей в нем как производственном ресурсе // Вестник РАЕН, 2018. – Т. 18. – № 2. – С. 10-17.
11. Volodina E.Eu. Models for predicting the development of the new mobile communication technologies market // Электросвязь, 2018. – № 2. – С. 60-66.
12. Бутенко В.В., Веерпалу В.Э., Володина Е.Е., Девяткин Е.Е., Харитонов Н.И. Перспективные методы управления использованием радиочастотного спектра // Электросвязь, 2009. – № 5. – С. 9-13.
13. Бутенко В.В., Веерпалу В.Э., Харитонов Н.И., Володина Е.Е., Девяткин Е.Е., Бессилин А.В. Распределение частотного ресурса между РЭС гражданского назначения в конверсионных полосах частот для обеспечения развития перспективных радиотехнологий // Труды Научно-исследовательского института радио, 2008. – № 3. – С. 19-25.
14. Веерпалу В.Э., Володина Е.Е., Девяткин Е.Е., Девяткина М.Е. Инновационные методы регулирования использования радиочастотного спектра // Электросвязь, 2014. – № 10. – С. 17-21.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

КИБЕРБЕЗОПАСНОСТЬ: ИСКУСНАЯ ЗАЩИТА ЦИФРОВОЙ ЭКОНОМИКИ

Г.П. Платунина, *Московский технический университет связи и информатики, g.p.platunina@mtuci.ru;*
Д.С. Ермоленко, *Московский технический университет связи и информатики, dariya.ermolenko@yandex.ru.*

УДК 338

Аннотация. В данной статье рассматриваются тренды кибербезопасности цифровой экономики на 2021 г., а также выявлены успехи в сфере кибербезопасности за последние три года и рассмотрен прогноз затрат на кибербезопасность до 2024 г.

Ключевые слова: кибербезопасность; цифровая экономика; тренды; *covid*-19.

CYBER SECURITY: ARTIFICIAL PROTECTION OF THE DIGITAL ECONOMY

Galina Platunina, *Moscow Technical University of Communications and Informatics;*
Daria Ermolenko, *Moscow Technical University of Communications and Informatic.*

Annotation. This article examines the cybersecurity trends of the digital economy for 2021, as well as identifies the successes in the field of cybersecurity over the past 3 years and considers the forecast of cybersecurity costs until 2024.

Keywords: cybersecurity; digital economy; trends; covid-19.

Введение

Все большее количество жизненно важных услуг зависит от цифровых систем – коммерческих операций, здравоохранения, безопасности и других, которые способствуют нашему общему благополучию [1-9]. Нарушения этих систем – будь то преднамеренные кибератаки, стихийные бедствия или технические сбои, могут нанести серьезный экономический и социальный ущерб. Кроме того, неуверенность пользователей в безопасности онлайн-сервисов и защите конфиденциальности угрожает использовать весь потенциал информационных и коммуникационных технологий для стимулирования инноваций, экономического роста и прогресса.

Новые технологии и бизнес-модели, а также высокие темпы их внедрения несут новые риски, однако кибербезопасность делает быстрые цифровые изменения безопаснее. На рис. 1 показана роль у *CISO* в организации.

В 2020 г. нарушение информационной безопасности является лидирующем направлением спуфинг-атак. Многие компании столкнулись с «цифровой пандемией», такой же коварной и трудно поддающейся предотвращению, как и *Covid*-19. Злоумышленники часто нацелены на поставщиков медицинских услуг, поскольку медицинские записи являются бестселлерами в темной сети, их трудно отследить, и можно продать по цене до 1000 долл. за штуку.

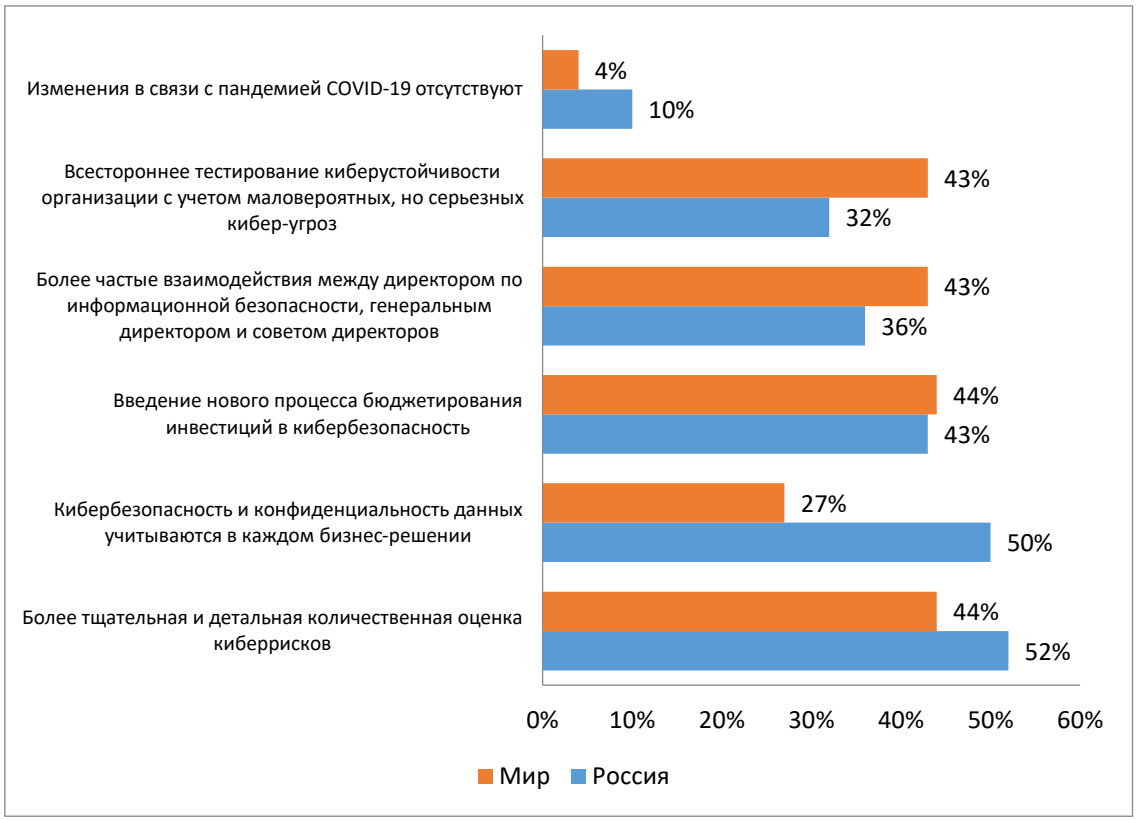

Рисунок 1

Кибератаки, спонсируемые государством, обнаруженные ранее, добавляют новое измерение во все более стремительно развивающуюся гонку вооружений.

- Последний опрос *PwC* показал, что 96% руководителей изменили свою стратегию кибербезопасности из-за *Covid*-19, а 40% руководителей заявили, что ускоряют цифровизацию.
- *IDC* ожидает, что глобальные расходы на безопасность достигнут 174,7 млрд. долл. в 2024 г., при среднегодовом темпе роста (*CAGR*) 8,1% за прогнозируемый период 2020-2024 гг.
- 57% российских компаний во время пандемии сделали кибербезопасность одним из основных стратегических приоритетов [10].

Инновации меняют правила игры в кибербезопасность, принося новые преимущества защитникам и позволяя им играть на равных с злоумышленниками. Количество стартапов в области кибербезопасности растет в геометрической прогрессии. Компании, которые первыми перешли на новые решения, оказались в лучшем положении. Но что еще более важно, они инвестируют в классическую триаду цифровой трансформации: люди, процессы и технологии [11, 12]. Таким образом удается преодолеть разрыв, который долгое время оставался между защитниками и нападающими. Инвестирование во все возможные преимущества технологий, процессов и навыков вашего персонала становится предпосылкой для целенаправленного движения по преодолению разрыва с злоумышленниками. Также важны навыки ИТ-директора как оперативного лидера [13]. Успехи в кибербезопасности за последние три года приведены на рис. 2.

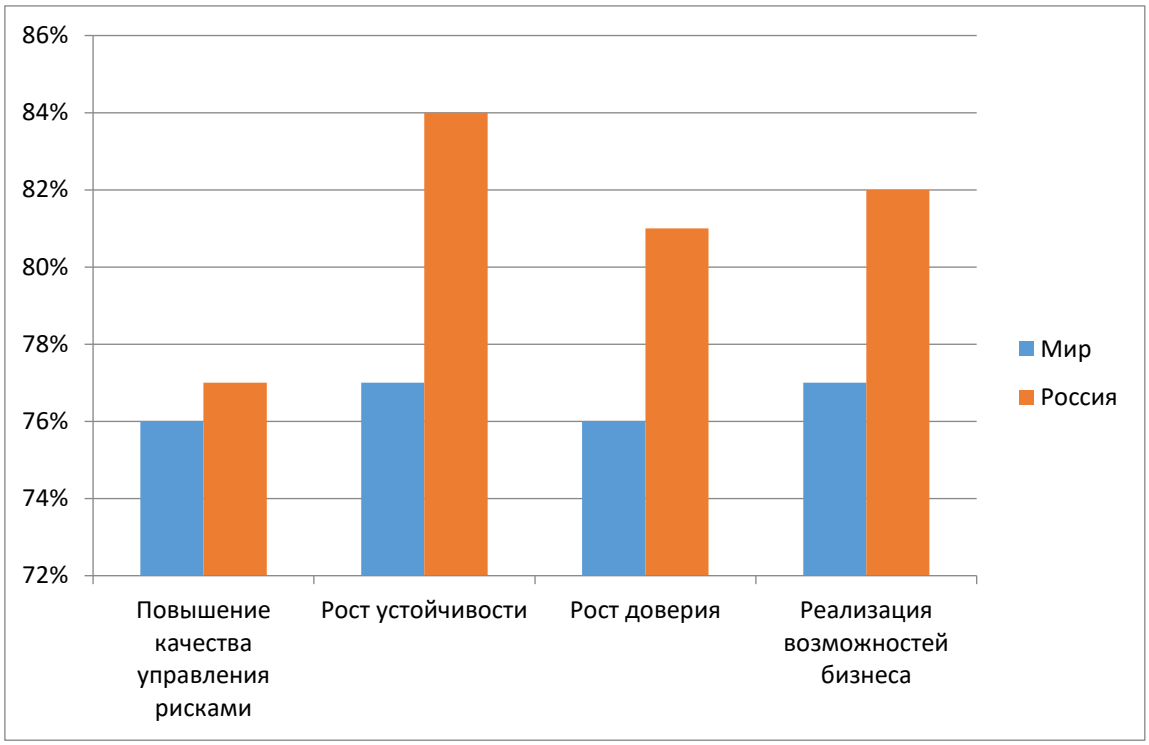

Рисунок 2

Повышение качества управления рисками:

- снижение нагрузки на сотрудников;
- снижение затрат на соблюдение законодательных и нормативных требований;
- снижение затрат на управление рисками.

Рост устойчивости:

- сокращение времени реагирования на инциденты и прерывания;
- сокращение времени простоя и связанных с этих затрат;
- уменьшение количества успешных атак.

Рост доверия:

- повышение лояльности клиентов;
- повышение индекса лояльности потребителей;
- более строгое соблюдение;
- повышение уверенности руководства.

Реализация возможностей:

- ускорение выхода на новые рынки;
- ускорение вывода на рынок новых продуктов;
- улучшение качества обслуживания клиентов;
- улучшение опыта сотрудников;
- более удачные преобразования.

Следующие прогнозы дают представление о том, как будет развиваться кибербезопасность в 2021 г.:

1. Бюджеты на кибербезопасность вырастут более чем у половины компаний. В 2021 г. 55% бизнес-лидеров планируют увеличить свои бюджеты на кибербезопасность, а 51% планируют добавить штатных сотрудников кибербезопасности (рис. 3). Совершенно очевидно, что кибербезопасность стала важнее, чем когда-либо в бизнесе. Получение максимальной отдачи от каждого рубля, вложенного в кибербезопасность, становится все более важным по мере оцифровки бизнеса: каждый новый цифровой актив создает новую уязвимость для кибератак. На рис. 2 приведен бюджет на кибербезопасность в 2021 г.

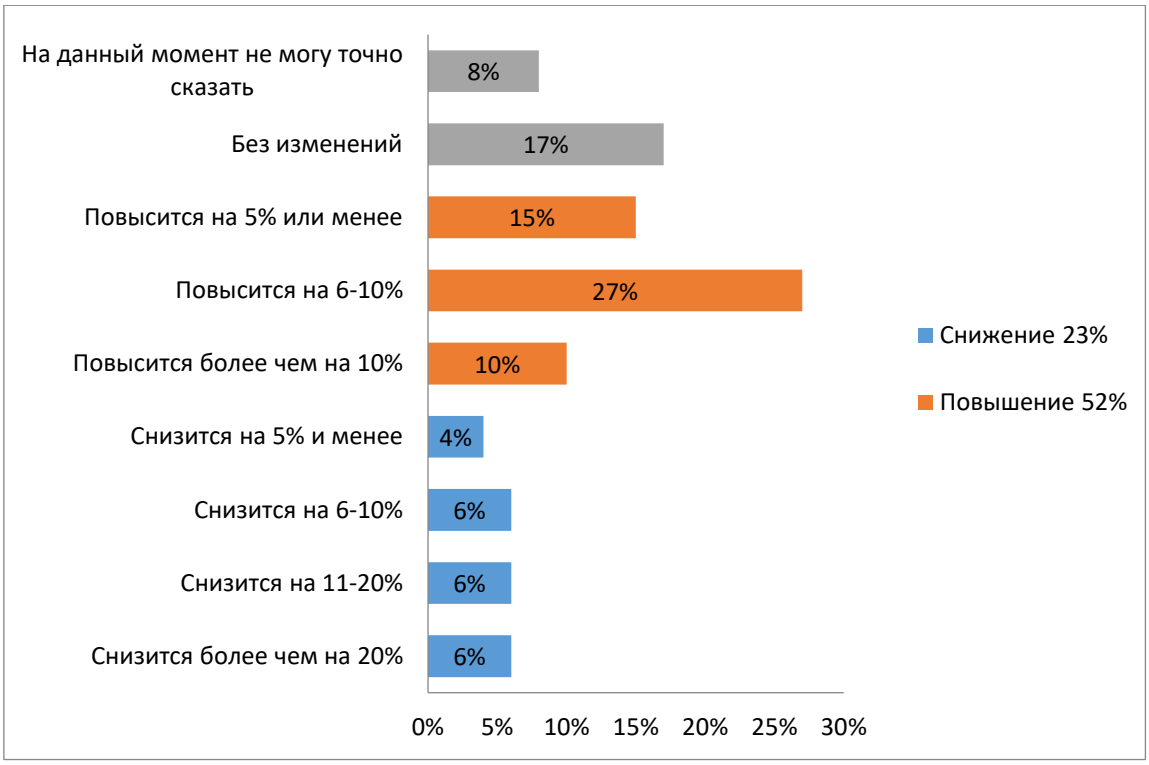

Рисунок 3

2. Управление идентификацией и доступом нового поколения, безопасность электронной почты и сетевая безопасность – три горячих точки для расходов на кибербезопасность бизнеса в 2021 г. В этой области *McKinsey* прогнозирует безопасность периметра и конечных точек, безопасную автоматизацию и безопасность для доверенных третьих сторон [14].

Основываясь на этих тенденциях и других недавних мероприятиях, можно сделать вывод, что директора по информационной безопасности и группы кибербезопасности будут продолжать уделять приоритетное внимание следующим нишам безопасности расходов [15, 16]:

- *Инструменты идентификации и контроля доступа нового поколения.* Компании, которые отложили добавление *MFA* в унаследованные системы, ускоряют их внедрение или переход на облачные платформы. По мере того как все больше сотрудников работают удаленно, команды, управляющие критически важными для бизнеса системами, переосмысливают, кто получает привилегированный доступ. Директора по информационной безопасности на среднем рынке, вероятно, будут отдавать приоритет решениям по управлению привилегированным доступом и управлению идентификацией, которые интегрируются с информацией о безопасности,

инструментами управления событиями и расширенной аналитикой безопасности, чтобы сэкономить время и деньги [17, 18].

- *Удаленный доступ.* Директора по информационной безопасности продолжат поддерживать виртуальные обходные пути для сотрудников службы поддержки, которые обычно работают в офисе. Служба поддержки *Virtual Security* помогает удаленным сотрудникам решать проблемы доступа, которые также поддерживают производительность, такие как токены безопасности электронной почты и доступ к удаленному рабочему столу. В частности, в компаниях малого и среднего бизнеса мы ожидаем увидеть расходы выше среднего на услуги *MFA*, которые интегрируются с инструментами совместной работы и решениями типа «система как услуга», включая совместное использование файлов, инфраструктуру виртуальных рабочих столов и коммуникационные платформы.
- *Безопасность для доверенных третьих лиц.* Компании, которые предоставляют доступ к сети подрядчикам или другим доверенным партнерам, должны защищать эти стороны от внешних атак, поскольку такие угрозы могут повлиять на их собственную безопасность. Мы ожидаем, что компании увеличат мониторинг потенциальных угроз, что может увеличить бюджеты на инструменты оценки безопасности кликов, оценки рисков безопасности и инструменты отчетности по безопасности – однако эти затраты вряд ли будут приоритетными до тех пор, пока какие-либо технические пробелы в безопасности не станут более актуальными *COVID*-19 (например, безопасность удаленного доступа, многофакторная аутентификация).
- *Автоматизация.* Компании, автоматизирующие рутинные задачи, могут высвободить время для другой работы, которая увеличивает ценность. Мы ожидаем, что для организаций, осуществляющих аутсорсинг, руководители по информационной безопасности попросят поставщиков управляемых услуг компенсировать возросшую рабочую нагрузку путем добавления автоматизированных услуг, таких как средства управления безопасностью и автоматизации реагирования, вместо увеличения штата или бюджета.

3. *IDC* прогнозирует, что услуги безопасности станут крупнейшим и наиболее быстрорастущим сегментом рынка безопасности, на который будет приходиться около половины всех расходов в прогнозируемый период 2020-2024 гг. (рис. 4), а среднегодовой темп роста за пять лет составит 10,5% [19]. Управляемые услуги безопасности – однопользовательские решения, которые управляются сторонними поставщиками и размещаются у клиента (устройства клиента), являются самой большой категорией расходов на безопасность, за которой следуют интеграция и консультационные услуги. Управляемые услуги безопасности также будут самым быстрорастущим сегментом со средним показателем за пять лет 13,6%. Программное обеспечение станет вторым по величине сегментом рынка безопасности, во главе которого стоит программное обеспечение для обеспечения безопасности конечных точек и анализа безопасности, анализа, реагирования и оркестровки. *IDC* – постоянный спрос будет стимулировать устойчивый рост продуктов и услуг безопасности, согласно новому руководству *IDC* по расходам [20].

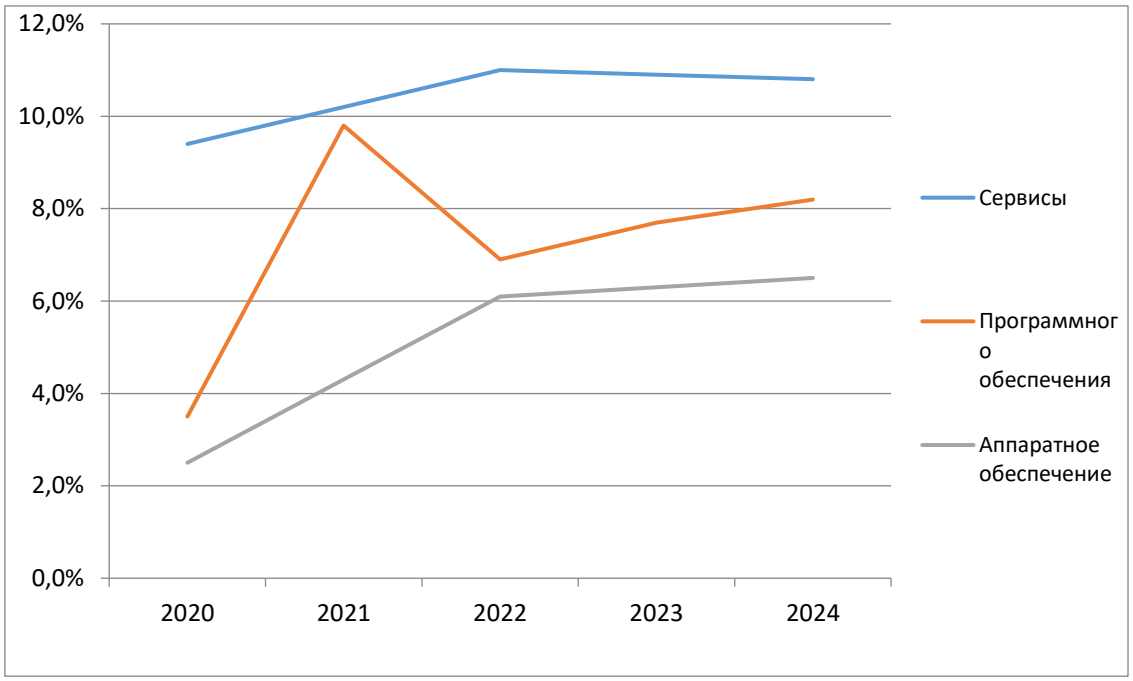

Рисунок 4

4. *Analysys Mason* прогнозирует, что расходы малого и среднего бизнеса (*SMB*) на кибербезопасность (включая аппаратное обеспечение, программное обеспечение и услуги) во всем мире вырастут в среднем на 10% в период с 2019 по 2024 г. (рис. 5), превратившись за четыре года в рынок стоимостью 80 млрд. долл. Расходы *SMB* на облачные решения безопасности будут опережать расходы на локальное оборудование и программное обеспечение, основанные на прогнозе фирмы. Аналитики Мейсон учли, насколько существенно изменение рабочих привычек, вызванное ограничениями *Covid*-19, увеличивает спрос на решения в области кибербезопасности, особенно на управляемые службы безопасности и облачные решения [21].

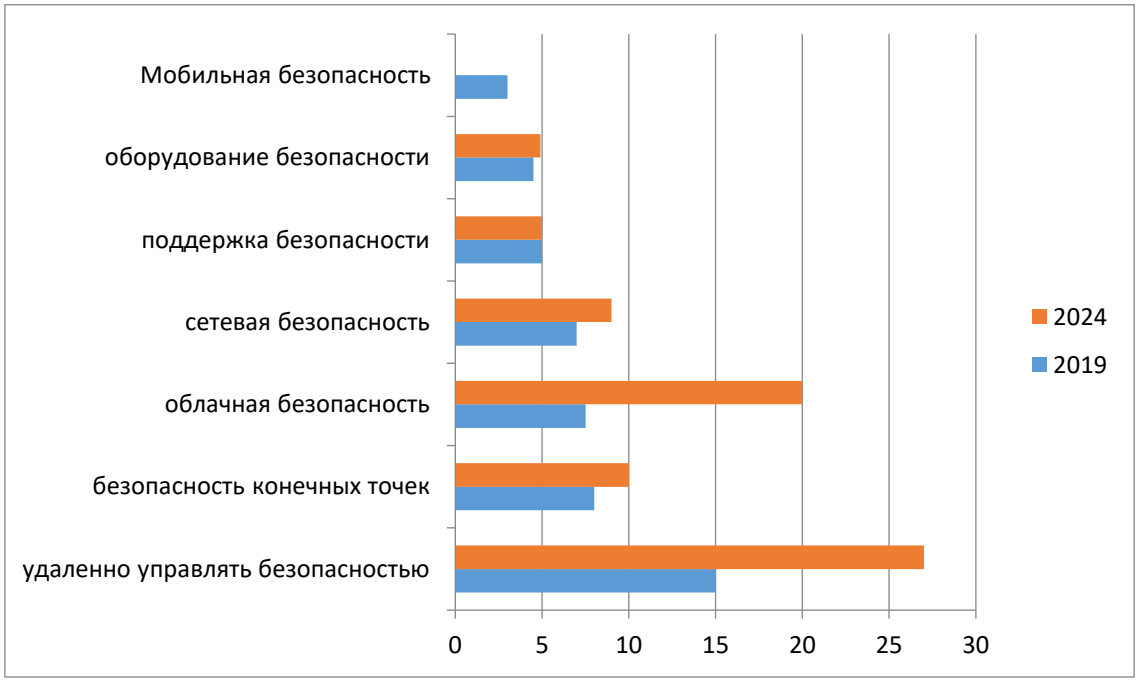

Рисунок 5

5. В 2021 г. достижения в области искусственного интеллекта и машинного обучения позволят устройствам исцелять и защищать себя до 80%, позволяя им устанавливать правила и знать, что их устройства и данные в безопасности. Это не только означает, что они могут сосредоточиться на преобразовании своего бизнеса, чтобы быть более конкурентоспособным на своем рынке, но и пользователи могут рассчитывать на более увлекательный и персонализированный опыт работы с устройством, на котором они могут оставаться продуктивными независимо от того, где они работают или используют [22, 23].

Заключение

Проблемы, с которыми сталкиваются организации, занимающиеся кибербезопасностью, переместились на поставщиков технологий. Эти компании предпринимали собственные меры и стратегии, чтобы идти в ногу с меняющимися потребностями клиентов и внедрять новые способы ведения бизнеса. Чтобы добиться успеха в эпоху после *COVID*-19, поставщики технологий должны переосмыслить свои стратегии и предложения, чтобы адаптироваться к новому ландшафту безопасности [22], продолжать отслеживать потребности клиентов и соответствующим образом корректировать продажи, обслуживание и обучение. Директора по информационной безопасности, которые быстро переориентировали безопасность на удаленных сотрудников и на обеспечение непрерывности бизнеса во время кризиса *COVID*-19, теперь должны подготовиться к будущему. Эта подготовка включает определение того, как распределить ограниченные бюджеты на кибербезопасность для поддержки дополнительных изменений. Поставщикам кибербезопасности необходимо изменить свой подход, став надежными партнерами и влиятельными лицами, чтобы помочь клиентам максимизировать затраты в ожидании следующего нормального явления [23].

Литература

1. Володина Е.Е. Прогнозирование развития инновационных услуг в сфере инфокоммуникаций // Инновационное развитие экономики, 2017. – № 5 (41). – С. 7-16.
2. Девяткин Е.Е., Володина Е.Е., Бессилин А.В. Прогноз развития рынка услуг наземной подвижной связи в России // Труды Научно-исследовательского института радио, 2010. – № 4. – С. 3-9.
3. Володина Е.Е., Девяткин Е.Е., Суходольская Т.А. Анализ развития интеллектуальных транспортных систем // Экономика и качество систем связи, 2017. – № 1 (3). – С. 40-46.
4. Володина Е.Е., Девяткин Е.Е., Пастух С.Ю., Девяткина Е.М., Плосский А.Ю. Рыночный потенциал интернета вещей // T-Comm: Телекоммуникации и транспорт, 2016. – № 9. – С. 28.
5. Володина Е.Е., Девяткин Е.Е., Девяткина М.Е. Влияние научно-технического прогресса на развитие рынка услуг и показатели деятельности операторов сотовой подвижной связи // Экономика и качество систем связи, 2016. – № 1 (1). – С. 24-29.
6. Володина Е.Е., Девяткин Е.Е., Суходольская Т.А. Перспективные радиотехнологии (сети 5G/IMT-2020, интернет вещей) в социально-экономическом развитии страны / В книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) XLII международной конференции РАЕН, 2018. – С. 135-138.

7. Девяткин Е.Е., Иванкович М.В., Володина Е.Е. Стратегическое управление сетями связи Российской Федерации как главная задача развития информационной инфраструктуры // Электросвязь, 2020. – № 9. – С. 24-29.
8. URL https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets (Дата обращения 22.03).
9. URL https://www.forbes.com/sites/louiscolumbus/2020/12/15/the-best-cybersecurity-predictions-for-2021-roundup/?sh=7fe684115e8c (Дата обращения 22.03).
10. URL https://hr-media.ru/rashody-na-kiberbezopasnost-strategicheskiy-prioritet-korporatsiy-v-2020-godu (Дата обращения 22.03).
11. Григоренко Е.Р., Платунина Г.П. Методические основы и инструменты реинжиниринга бизнес-процессов деятельности компании // В сборнике: Технологии Информационного Общества. Сборник трудов XIV Международной отраслевой научно-технической конференции, 2020. – С. 327-329.
12. Салютина Т.Ю., Платунина Г.П. Методические основы формирования параметров модели оценки инвестиционной привлекательности телекоммуникационной компании // В книге: мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 46-й международной конференции. Москва, 2020. – С. 67-70.
13. Платунина Г.П., Васильева И.А. Управление бизнес-процессами инфокоммуникационных компаний в условиях трансформации мирового экономического общества // Экономика и качество систем связи, 2020. – № 1 (15). – С. 22-29.
14. URL https://www.pwc.ru/ru/publications/dti-2021/e-version-digital-trust-insights-2021-in-russian.pdf (Дата обращения 22.03).
15. Платунина Г.П., Добычина И.В. Методические аспекты курсового проектирования по дисциплине "Экономика инфокоммуникаций и отраслевые рынки" для бакалавров направления "Прикладная информатика" // В сборнике: Технологии Информационного Общества. Материалы XIII Международной отраслевой научно-технической конференции, 2019. – С. 385-387.
16. Платунина Г.П., Васильева И.А. Проблемы информационной безопасности России в условиях кризисного развития мирового экономического сообщества на современном этапе // В книге: Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) XLIII международной конференции РАЕН, 2019. – С. 73-77.
17. Платунина Г.П., Ермоленко Д.С. Тренды в развитии цифровой экономики // Экономика и качество систем связи, 2021. – № 1 (19). – С. 13-20.
18. Платунина Г.П., Ермоленко Д.С. Цифровая трансформация бизнес-моделей в условиях кризисного развития мирового экономического общества на современном этапе // В сборнике: Технологии Информационного Общества. Сборник трудов XV Международной отраслевой научно-технической конференции «Технологии информационного общества», 2021. – С. 273-275.
19. URL https://www.idc.com/getdoc.jsp?containerId=prUS46773220 (Дата обращения 22.03).
20. Платунина Г.П. CRM-система как средство повышения эффективности бизнеса // В книге: Мобильный Бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом сборник материалов (тезисов) 45-й международной конференции РАЕН, 2020. – С. 55-59.
21. URL https://www.analysysmason.com/research/content/comments/smb-security-spending-ren04/ (Дата обращения 22.03).

22. Платунина Г.П. Применение интерактивных технологий в процессе преподавания дисциплины «Интернет-реклама и PR» и совершенствование содержания курса // В сборнике: Технологии Информационного Общества. Сборник трудов XIV Международной отраслевой научно-технической конференции, 2020. – С. 571-572.
23. Платунина Г.П., Ермоленко Д.С. Анализ факторов, влияющих на поведение производителя в условиях чистой монополии и на макроуровне в условиях кризиса // В сборнике: Технологии Информационного Общества. Сборник трудов XIV Международной отраслевой научно-технической конференции, 2020. – С. 360-362.

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ МЕТРИКИ RIBES ДЛЯ ОЦЕНКИ ЛИНГВИСТИЧЕСКИХ СТЕГОСИСТЕМ

К.А. Ахрамеева, *доцент, к.т.н., Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, oklaba@mail.ru;*
Д.Ю. Мицковский, *Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, denism111198@yandex.ru.*

УДК 004.7

Аннотация. В данной статье представлены результаты исследования использования метрики *RIBES* для оценки стеготекста лингвистических стегосистем, а также приводится оценка метрики *RIBES* в качестве оценки текста.

Ключевые слова: лингвистическая стеганография; метрика *RIBES*; метрики оценки перевода.

RESEARCH ON EVALUATING THE SAFETY OF LINGUISTIC STEGOSYSTEMS BASED ON THE RIBES METRIC

Kseniya Ahrameeva, *associate professor, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich;*
Denis Mickovskij, *St. Petersburg National Research University of Information Technologies, Mechanics and Optics.*

Annotation. This article presents the results of a study of the use of the *RIBES* metric for evaluating the stegotext of linguistic stegosystems, and also provides an assessment of the *RIBES* metric as a text evaluation.

Keywords: linguistic steganography; *RIBES* metric; translation evaluation metrics.

Лингвистическая стеганография является перспективным направлением в защите информации ввиду сложности стегоанализа данных стегосистем, однако вместе с тем оценка безопасности данных систем является проблематичной, ввиду необходимости каким-либо образом точно определить качество стеготекста. Для осуществления такой проверки в масштабах сети необходима программа, а для программы нужна определённая метрика – числовой показатель, который может отразить оценку качества стеготекста, примерно совпадающую с оценкой стеготекста человеком, поскольку, программа не может «понять» смысл слов в

стеготексте. Необходимость нахождения программного решения подтверждается наличием множества исследований в данной области, например в работах [1-4]. В качестве одного из решений для программной реализации оценивания предлагается использовать метрику оценки перевода *RIBES*.

Лингвистическая стеганография скрывает стеганограмму, изменяя информацию, которая кодируется на основе лингвистического порядка текста. То есть, для скрытия сообщений изменяется сам текст оригинального сообщения – контейнера. Одним из основных преобразований, используемых в лингвистической стеганографии, является, например, замена синонимов, предполагающая использование пар синонимов для передачи стеганограмм. Например, в тексте «Дэвид завел машину и, въехав во двор, поставил ее под каштаном у фасада, затем вытащил чемодан, портфель и висевший на вешалке джинсовый костюм и понес в дом». Можно использовать пары абсолютных синонимов (выражения, которые можно заменить другим выражением в любом контексте без изменения его смысла) «машина-автомобиль», «затем-потом», «портфель-сумка» для передачи бит, где первое слово из пар синонимов принимается за 0, а второе – за 1. Например: Дэвид завел автомобиль и, въехав во двор, поставил ее под каштаном у фасада, затем вытащил чемодан, сумку и висевший на вешалке джинсовый костюм и понес в дом. В данном случае передаётся 101, то есть можно передать, как минимум, три бита.

Ещё одним методом лингвистической стеганографии является стеганография с изменением порядка слов. Для передачи стегосообщения используется порядок слов в предложении. Например:

<u>В четверг</u>, <u>в центральной части города</u> <u>проходят</u> <u>фестивали</u> и <u>ярмарки</u>.

L *T* *V* *S* *M*

Данное предложение можно преобразовать в «В центральной части города, в четверг, проходят ярмарки и фестивали». Что даёт последовательность *TLVMS*. И так далее. Всего, при данном разделении, возможно 5! = 120 перестановок, но вариаций, при которых сохраняется естественность текста, гораздо меньше, а именно 8: *LTVSM, LTVMS, TLVMS, TLVSM, TVMSL, TVSML, LVMST, LVSMT*. То есть в предложение можно вложить три бита [6]. Описанные выше методы являются одними из основных типов изменений стеготекста, поэтому данные преобразования были рассмотрены при изучении работы метрики.

Используемые до сих пор методы оценки безопасности лингвистических стегосистем можно разделить на две категории: автоматическая оценка и оценка человеком. Для автоматической метрики используются метрики оценки машинного перевода (такие как *BLEU* [4]).

Метрика *RIBES* фокусируется на порядке слов. Для расчёта используются коэффициенты ранговой корреляции, ρ – коэффициент Спирмена, показывающий насколько порядковый номер слова в стеготексте отличается от порядкового номера слова в эталоне, и τ – коэффициент Кендалла, показывающий в каком направлении порядок слов стеготекста отличается от эталона – в отрицательном или в положительном. Коэффициенты вычисляются по формулам (1-4)

$$\rho = 1 - 6\frac{\sum d^2}{n^3 - n}, \quad (1)$$

$$\tau = \frac{\sum S - \sum Q}{\frac{1}{2}n(n-1)}, \quad (2)$$

где: d – различия в значениях рангов, n – общее количество рангов, S – количество рангов после n-го ранга, превышающих значение n-го ранга, Q – количество рангов после n-го ранга, чьё значение меньше значения n-го ранга

Эти Ранговые меры могут быть нормализованы для обеспечения положительных значений:

- нормализованный коэффициент Спирмена ρ (*NSR*):

$$NSR = \frac{\rho+1}{2} \quad (3)$$

- нормализованный коэффициент Кендалла τ (*NKT*):

$$NKT = \frac{\tau+1}{2} \quad (4)$$

Для учёта изменений слов в метрике также учитывается точность. С учётом нормализованных ранговых коэффициентов и точности метрика *RIBES* вычисляется по формуле (5) [5]. Чем выше значение метрики, тем лучше оцениваемый текст.

$$RIBES = \frac{NSR_1 * P^{\alpha} + NST_1 * P^{\alpha}}{2}, \quad (5)$$

где: α – параметр в диапазоне $0 < \alpha < 1$.

В табл. 1 представлен расчёт метрик *RIBES* для стеготекста с изменением порядка слов.

Таблица 1.

Слово предложения	Первое предложение	Второе предложение
Нормализованный коэффициент Спирмана	0,97	0,99
Нормализованный коэффициент Кендалла	0,94	0,96
Точность	1	1
RIBES	96%	98%
Общее значение *RIBES*	97%	

$$RIBES_1 = \frac{NSR_1 * P^{\alpha} + NST_1 * P^{\alpha}}{2} = \frac{0.97*1 + 0.94*1}{2} = 0{,}96 \quad (6)$$

$$RIBES_2 = \frac{NSR_2 * P^{\alpha} + NST_2 * P^{\alpha}}{2} = \frac{0.99*1 + 0.96*1}{2} = 0{,}98 \quad (7)$$

$$RIBES_{\text{общ}} = \frac{RIBES_1 + RIBES_2}{2} = \frac{0.96+0.98}{2} = 0{,}97 \quad (8)$$

Исследование производится на основе текста, который преобразовывается с помощью двух разных лингистических стегосистем (синонимическая и на основе изменения порядка слов текста), а также комбинации изменений.

К тексту подбираются четыре ссылочных текста, которые используются метриками оценки текста для совершения расчёта. Расчёты *RIBES* и ранговых коэффициентов представлены в табл. 1-4.

Так, как и у стеготекста, и у эталона полностью совпадают слова, то очевидно, что точность будет равна единице для обоих предложений. При этом значения *RIBES* при всех значениях коэффициента α будут равны.

RIBES рассчитывается согласно ранжированию слов, исходя из их порядка в предложениях эталона и стеготекста, при этом в расчёте также учитываются совпадения слов с помощью использования точности в расчётах, чтобы текст, с полным совпадением порядка нескольких слов, находящихся и в стеготексте, и в эталоне, но с большим числом случайных слов, не могли быть оценены

положительно. Чем больше совпадений в порядке слов и больше совпадений слов в текстах, тем выше значение *RIBES*.

Для стеготекста на основе замены синонимов расчеты гораздо более тривиальны. Так как порядок всех не заменённых слов совпадает, то очевидно, что сумма коэффициента $\sum d^2$ будет равна, соответственно коэффициент Спирмана $\rho = 1 - 0 = 1$, как и нормализованный коэффициент $NSR = \frac{1+1}{2}$ = 1 для обоих предложений.

Расчёт метрики *RIBES* для стеготекста с изменением порядка слов представлен на формулах (6-8). Для стеготекста с заменой синонимов для первых и вторых предложений были получены значения точности 0,73 и 0,91 соответственно. Расчёт метрики *RIBES* представлены на формулах (9-17).

Для стеготекста с комбинированием изменений для первых и вторых предложений также были получены значения точности 0,73 и 0,91, так как точность при изменении порядка слов не изменилась относительно исходного предложения. Расчёт метрики *RIBES* представлен проведен с помощью формул (18-26).

В табл. 2 представлен расчёт метрик *RIBES* для стеготекста с заменой синонимов.

Таблица 2.

Слово предложения	Первое предложение	Второе предложение
Нормализованный коэффициент Спирмана	1	1
Нормализованный коэффициент Кендалла	1	1
Точность	$\frac{11}{15}$ = 0,73	$\frac{21}{23}$ = 0,91
RIBES (при α = 0)	100%	100%
RIBES (при α = 0,5)	85%	95%
RIBES (при α = 1)	73%	91%
Общее значение *RIBES* (при α = 0)	100%	
Общее значение *RIBES* (при α = 0,5)	90%	
Общее значение *RIBES* (при α = 1)	82%	

$$RIBES_1(\alpha = 0) = \frac{NSR_1 * P^{\alpha} + NST_1 * P^{\alpha}}{2} = \frac{1*0{,}73^0 + 1*0{,}73^0}{2} = 1 \quad (9)$$

$$RIBES_2(\alpha = 0) = \frac{NSR_2 * P^{\alpha} + NST_2 * P^{\alpha}}{2} = \frac{1*0{,}91^0 + 1*0{,}91^0}{2} = 1 \quad (10)$$

$$RIBES_1(\alpha = 0.5) = \frac{1*0{,}73^{0,5} + 1*0{,}73^{0,5}}{2} = 0{,}85 \quad (11)$$

$$RIBES_2(\alpha = 0.5) = \frac{1*0{,}91^{0,5} + 1*0{,}91^{0,5}}{2} = 0{,}95 \quad (12)$$

$$RIBES_1(\alpha = 1) = \frac{1*0{,}73^1 + 1*0{,}73^1}{2} = 0{,}73 \quad (13)$$

$$RIBES_2(\alpha = 1) = \frac{1*0{,}91^1 + 1*0{,}91^1}{2} = 0{,}91 \quad (14)$$

$$RIBES_{\text{общ}}(\alpha = 0) = \frac{RIBES_1 + RIBES_2}{2} = \frac{1+1}{2} = 1 \quad (15)$$

$$RIBES_{общ}(\alpha = 0.5) = \frac{0,85+0,95}{2} = 0,9 \quad (16)$$

$$RIBES_{общ}(\alpha = 1) = \frac{0,73+0,91}{2} = 0,82 \quad (17)$$

В талб. 3. представлен расчёт метрик *RIBES* для стеготекста с заменой синонимов и изменением порядка слов.

Таблица 3.

Слово предложения	Первое предложение	Второе предложение
Нормализованный коэффициент Спирмана	1	0,98
Нормализованный коэффициент Кендалла	0,98	0,95
Точность	$\frac{11}{15}$ = 0,73	$\frac{21}{23}$ = 0,91
RIBES (при α = 0)	99%	97%
RIBES (при α = 0,5)	85%	92%
RIBES (при α = 1)	73%	88%
Общее значение *RIBES* (при α = 0)	98%	
Общее значение *RIBES* (при α = 0,5)	89%	
Общее значение *RIBES* (при α = 1)	81%	

$$RIBES_1(\alpha = 0) = \frac{NSR_1 * P^{\alpha} + NST_1 * P^{\alpha}}{2} = \frac{1*0,73^0 + 0,98*0,73^0}{2} = 0,99 \quad (18)$$

$$RIBES_2(\alpha = 0) = \frac{NSR_2 * P^{\alpha} + NST_2 * P^{\alpha}}{2} = \frac{0,98*0,91^0 + 0,95*0,91^0}{2} = 0,97 \quad (19)$$

$$RIBES_1(\alpha = 0,5) = \frac{1*0,73^{0,5} + 0,98*0,73^{0,5}}{2} = 0,85 \quad (20)$$

$$RIBES_2(\alpha = 0,5) = \frac{0,98*0,91^{0,5} + 0,95*0,91^{0,5}}{2} = 0,92 \quad (21)$$

$$RIBES_1(\alpha = 1) = \frac{1*0,73^1 + 0,98*0,73^1}{2} = 0,73 \quad (22)$$

$$RIBES_2(\alpha = 1) = \frac{0,98*0,91^1 + 0,95*0,91^1}{2} = 0,88 \quad (23)$$

$$RIBES_{общ}(\alpha = 0) = \frac{RIBES_1 + RIBES_2}{2} = \frac{0,99+0,97}{2} = 0,98 \quad (24)$$

$$RIBES_{общ}(\alpha = 0,5) = \frac{0,85+0,92}{2} = 0,89 \quad (25)$$

$$RIBES_{общ}(\alpha = 1) = \frac{0,73+0,88}{2} = 0,81 \quad (26)$$

При расчёте значений для текста со случайными изменениями была получена схожая точность (поскольку часть слов оригинального текста не заменялась), лишь с небольшим уменьшением по значению. Но при этом в связи со случайными изменениями в порядке слов сильно уменьшились значения нормализованных коэффициентов, в связи с чем снизилось и само значение метрики. Это показывает, что основную функцию определения несоответствий выполняют именно коэффициенты ранговой корреляции. Расчёты метрики *RIBES* основаны на формулах (27-35).

В табл. 4 представлен расчёт метрик *RIBES* для стеготекста со случайными заменами слов и их порядка.

Таблица 4.

Слово предложения	Первое предложение	Второе предложение
Нормализованный коэффициент Спирмана	0,74	0,75
Нормализованный коэффициент Кендалла	0,69	0,75
Точность	$\frac{11}{15}$=0,73	$\frac{17}{23}$=0,74
RIBES (при α = 0)	72%	75%
RIBES (при α = 0,5)	61%	65%
RIBES (при α = 1)	52%	56%
Общее значение *RIBES* (при α = 0)	74%	
Общее значение *RIBES* (при α = 0,5)	63%	
Общее значение *RIBES* (при α = 1)	54%	

$$RIBES_1(\alpha = 0) = \frac{NSR_1 * P^{\alpha} + NST_1 * P^{\alpha}}{2} = \frac{0{,}74 * 0{,}73^0 + 0{,}69 * 0{,}73^0}{2} = 0{,}72 \quad (27)$$

$$RIBES_2(\alpha = 0) = \frac{NSR_2 * P^{\alpha} + NST_2 * P^{\alpha}}{2} = \frac{0{,}75 * 0{,}74^0 + 0{,}75 * 0{,}74^0}{2} = 0{,}75 \quad (28)$$

$$RIBES_1(\alpha = 0{,}5) = \frac{0{,}74 * 0{,}73^{0{,}5} + 0{,}69 * 0{,}73^{0{,}5}}{2} = 0{,}61 \quad (29)$$

$$RIBES_2(\alpha = 0{,}5) = \frac{0{,}75 * 0{,}74^{0{,}5} + 0{,}75 * 0{,}74^{0{,}5}}{2} = 0{,}65 \quad (30)$$

$$RIBES_1(\alpha = 1) = \frac{0{,}74 * 0{,}73^1 + 0{,}69 * 0{,}73^1}{2} = 0{,}52 \quad (31)$$

$$RIBES_2(\alpha = 1) = \frac{0{,}75 * 0{,}74^1 + 0{,}75 * 0{,}74^1}{2} = 0{,}56 \quad (32)$$

$$RIBES_{\text{общ}}(\alpha = 0) = \frac{RIBES_1 + RIBES_2}{2} = \frac{0{,}72 + 0{,}75}{2} = 0{,}74 \quad (33)$$

$$RIBES_{\text{общ}}(\alpha = 0{,}5) = \frac{0{,}61 + 0{,}65}{2} = 0{,}63 \quad (34)$$

$$RIBES_{\text{общ}}(\alpha = 1) = \frac{0{,}52 + 0{,}56}{2} = 0{,}54 \quad (35)$$

В результате исследования было выяснено, что метрика *RIBES* является эффективной для использования в оценке лингвистических стегосистем при определённом значении коэффицента учёта точности. Метрика *RIBES* при коэффициенте учёта точности α равного 0 не учитывает изменения слов, поэтому показывает более высокие оценки, в том числе для текста со случайными преобразованиями. Учёт точности также недостаточен при коэффициенте 0,5. Однако для коэффициента равного 1 метрика *RIBES* показывает наиболее точные оценки. Оценки для стеготекстов меняются незначительно для разных стегопреобразований, при этом текст со случайными преобразованиями получает достаточно низкую оценку.

Литература

1. Zachary M. Ziegler, Yuntian Deng, Alexander M. Rush., 2019. Neural Linguistic Steganography.
2. Ching − Yun Chang, Stephen Clark, 2012, The Secret's in the Word Order: Text-to-Text Generation for Linguistic Steganography.
3. Ching − Yun Chang, Stephen Clark, 2014, Practical Linguistic Steganography using Contextual Synonym Substitution and a Novel Vertex Coding Method.
4. Ахрамеева К.А., Герлинг Е.Ю., Мицковский Д.Ю., Прудников С.В. Использование метрики BLEU для оценки естественности текста лингвистических стегосистем // Вестник Российского нового университета, серия «Сложные системы: модели, анализ и управление», 2020. – 5 с.
5. Krzysztof Wołk. Machine Learning in Translation Corpora Processing, 2019. – 264 p.
6. Коржик В.И., Небаева К.А., Герлинг Е.Ю., Догиль П.С., Федянин И.А. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стеганография. [монография]: – СПбГУТ. – СПб., 2016. – 226 с.
7. Красов А.В., Штеренберг С.И., Фахрутдинов Р.М., Рыжаков Д.В., Пестов И.Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-Comm: Телекоммуникации и транспорт, 2018. – Т. 12. – № 10. – С. 36-40.
8. Коржик В.И., Нгуен З.К., Годлевский А.К. Оценка стегоключей для стегосистем, использующих стойкое шифрование вложенных сообщений // Проблемы информационной безопасности. Компьютерные системы, 2018. – № 3. – С. 26-36.
9. Сахаров Д.В., Левин М.В., Фостач Е.С., Виткова Л.А. Исследование механизмов обеспечения защищенного доступа к данным, размещенным в облачной инфраструктуре // Наукоемкие технологии в космических исследованиях Земли, 2017. – Т. 9. – № 2. – С. 40-46.
10. Герлинг Е.Ю., Ахрамеева К.А. Метод Лингвистической стеганографии, основанный на опорном слове // I-methods, 2019. – Т. 11. – № 4. – С. 1-9.
11. Герлинг Е.Ю. Исследование эффективности методов обнаружения стегосистем, использующих широкополосное вложение // Телекоммуникации, 2014. – № 1. – С. 6-12.

СЕТИ И СИСТЕМЫ СВЯЗИ

ПОВЫШЕНИЕ ПОМЕХОУСТОЙЧИВОСТИ В КОРОТКОВОЛНОВОМ РАДИОКАНАЛЕ ПРИ ПОМОЩИ CRC И LDPC КОДОВ

Р.Е. Кротов, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, ub1cag@yandex.ru;*
А.И. Рыбаков, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, lexeus.r1@gmail.com.*

УДК 654.739

Аннотация. Целью исследовательской работы авторов является анализ методов повышения помехоустойчивости в коротковолновых каналах радиосвязи. В работе детально рассматриваются использование циклического избыточного кода (*CRC*) и кода с малой плотностью проверок на четность (*LDPC*), передача сообщений при помощи 4-х и 8-ми тональной частотной манипуляцией (*CPFSK*). Последовательно представлен математический аппарат генерации высокочастотного сигнала. Методы обнаружения и декодирования сигналов основаны на гибридном подходе, который сочетает в себе некогерентное блочное обнаружение, односимвольное обнаружение, корреляционное обнаружение полученных сегментов сообщения, что позволяет ощутимо повысить чувствительность декодера. Используя модель радиоканала, предложенной МСЭ, проведены математические расчеты чувствительности декодера для разных регионов планеты.

Ключевые слова: *CRC; LDPC; CPFKS;* методы обнаружения; модель радиоканала; декодер.

IMPROVING NOISE IMMUNITY IN A SHORTWAVE RADIO CHANNEL USING CRC AND LDPC CODES

R.E. Krotov, *St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich.*
A.I. Rybakov, *St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich.*

Annotation. The purpose of the research work is to consider methods for increasing noise immunity in short-wave radio communication channels. The paper discusses in detail the use of cyclic redundancy check (*CRC*) and low density parity check (*LDPC*). Transmission of messages using 4 and 8-tone frequency-shift keying (*CPFSK*). The mathematical apparatus for generating a high-frequency signal is consistently presented. Signal detection and decoding methods are based on a hybrid approach that combines non-coherent block detection, single-character detection, correlation detection of received message segments, which can significantly increase the decoder's sensitivity. Using the radio channel model proposed by the *ITU*, mathematical calculations of the decoder sensitivity for different regions of the planet were carried out.

Keywords: *CRC; LDPC; CPFKS;* detection methods; radio channel model; decoder.

Введение

*FT*4 и *FT*8 – это цифровые протоколы, предназначенные для связи в условиях слабых сигналов. Информация обычно состоит из позывных, четырехсимвольных локаторов Мейденхеда и самого сообщения.

В этой работе приводится техническое описание протоколов *FT*4 и *FT*8, а также подробные измерения производительности, основанные на моделировании аддитивного канала белого гауссова шума (*AWGN*) и ряде стандартных моделей Международного союза электросвязи (*ITU*) для распространения в КВ диапазоне.

Структурирование и кодирование сообщения

Размер сообщений *FT*4 и *FT*8 всегда составляет ровно 77 бит пользовательской информации.

Основная цель состоит в том, чтобы дать 77-битной информационной полезной нагрузке максимальную «компактность», необходимую для контактов между операторами радиостанций. Чтобы облегчить эффективное сжатие сообщений для ряда целевых задач, выделяется 3 бита для указания одного из восьми возможных типов сообщений. Остальные 74 бита предназначены для информации о пользователе.

Обнаружение и исправление ошибок

14-битная циклическая проверка избыточности (*CRC*) добавляется к каждому 77-битному информационному пакету для создания 91-битного слова «сообщение + *CRC*». *CRC* вычисляется по исходному кодированному сообщению с нулевым расширением от 77 до 82 бит. Алгоритм *CRC* [1, 2] использует полином 0x6757 (шестнадцатеричный) и начальное значение, равное нулю. Еще 83 бита добавляются для прямого исправления ошибок, создавая 174-битное кодовое слово.

Прямая коррекция ошибок выполняется с использованием кода *LDPC*, разработанного специально для *FT*8 и *FT*4. Код определяется двумя матрицами: порождающей матрицей, используемой для вычисления 83 битов четности, добавляемых к каждому 91-битному сообщению плюс *CRC*-слову, и матрицей четности, которая может быть использована для определения того, является ли данная 174-битная последовательность допустимым кодовым словом. Все значения в обеих матрицах равны либо 0, либо 1, и связанные с ними операции используют двоичную арифметику по модулю 2. Порождающая матрица состоит из 83 строк и 91 столбца [2]. Ненулевые значения в строке *i*-й матрицы определяют, какой из 91 битов сообщения плюс *CRC* должен быть суммирован по модулю 2 для получения *i*-го бита проверки четности. Расположение единиц в каждой строке этой матрицы определяет, какие биты 174-битного кодового слова должны суммироваться (по модулю 2) до нуля. 174-битное слово является допустимым кодовым словом только в том случае, если все 83 суммы равны нулю.

Символы каналов и модуляция

Сообщения *FT*8 передаются с помощью 8-тональной непрерывной фазовой частотной манипуляции (*CPFSK*). Каждый передаваемый тон или символ канала передает 3 бита. Последовательность из 174 битов кодового слова отображается на последовательность из 174/3 = 58 символов канала a_n, причем n от 0 до 57. Значение каждого символа соответствует индексу тона в диапазоне от 0 до 7. Группы из 3-х последовательных битов сообщения сопоставляются с символами канала с помощью кода Грея, определенного столбцами 1 и 2 табл. 1. Это отображение

гарантирует, что битовые триады, связанные с соседними тонами, различаются только в одной битовой позиции, тем самым улучшая производительность декодирования на каналах, где доплеровский разброс сопоставим с разделением тонов.

*FT*4 аналогичен, но использует 4-х тональный *CPFSK*, поэтому каждый символ канала передает только 2 бита сообщения. Последовательность из 174 битов кодового слова отображается на последовательность из 174/2 = 87 символов канала a_n, n = 0, 1, 2, ..., 86, с каждым значением символа целочисленный индекс тона в диапазоне 0-3. Пары последовательных битов сообщения сопоставляются символам канала в соответствии с кодом Грея, определенным столбцами 1 и 3 табл. 1. В табл. 1 представлена двунаправленная карта Грея между битами сообщения и символами канала.

Таблица 1.

Channel Symbol	*FT*8 *Bits*	*FT*4 *Bits*
0	000	00
1	001	01
2	011	11
3	010	10
4	110	
5	100	
6	101	
7	111	

Тональные паттерны, известные как массивы Костаса, встроены в сигналы *FT*8 и *FT*4, чтобы позволить принимающему программному обеспечению правильно синхронизироваться с принимаемыми сигналами как во времени, так и в частоте. Для *FT*8 используется 7-ми тональная последовательность 3, 1, 4, 0, 6, 5, 2 которая вставляется в начало, середину и конец передаваемого сигнала. Если последовательность синхронизации обозначается S, а первая и вторая половины информационных символов $M_A = \{a_0, a_1, \dots, a_{28}\}$ и $M_B = \{a_{29}, a_{30}, \dots, a_{57}\}$, полный набор из 79 передаваемых символов может быть записан в виде последовательности $b_n = \{S, M_A, S, M_B, S\}$.

Генерирование сигналов

Оба протокола используют непрерывную фазовую частотную манипуляцию, которая подразумевает генерацию сигналов вида:

$$s(t) = A\cos\left(2\pi f_c t + \phi(t)\right).$$

Здесь A – амплитуда сигнала, f_c – несущая частота, t – время, а $\varphi(t)$ – фаза. Фазовое слагаемое может быть записано как интеграл мгновенной девиации частоты, $f_d(t)$:

$$\phi(t) = 2\pi\int_0^t f_d(\tau)\,d\tau, \quad t \geq 0.$$

Девиация частоты $f_d(t)$ оценивается как взвешенная сумма последовательности импульсов $p(t)$:

$$f_d(t) = h\sum_n b_n p(t - nT).$$

Здесь h называется индексом модуляции, весовой коэффициент b_n – значениями символов канала, $p(t)$ – формой импульса отклонения частоты, а T – сигнальным интервалом. T – это величина, обратная скорости манипуляции (Бод)). Девиация частоты импульса нормализуется на единицу площади:

$$\int_{-\infty}^{\infty} p(t)\,dt = 1,$$

Таким образом, импульс, взвешенный коэффициентом b_n, заставляет несущую фазу продвигаться на $2\pi h b_n$ радиана в течение длительности импульса.

На рис. 1 показан средний спектр сигнала $FT4$ (пунктирная линия) и спектр эквивалентной стандартной формы сигнала FSK (сплошная линия).

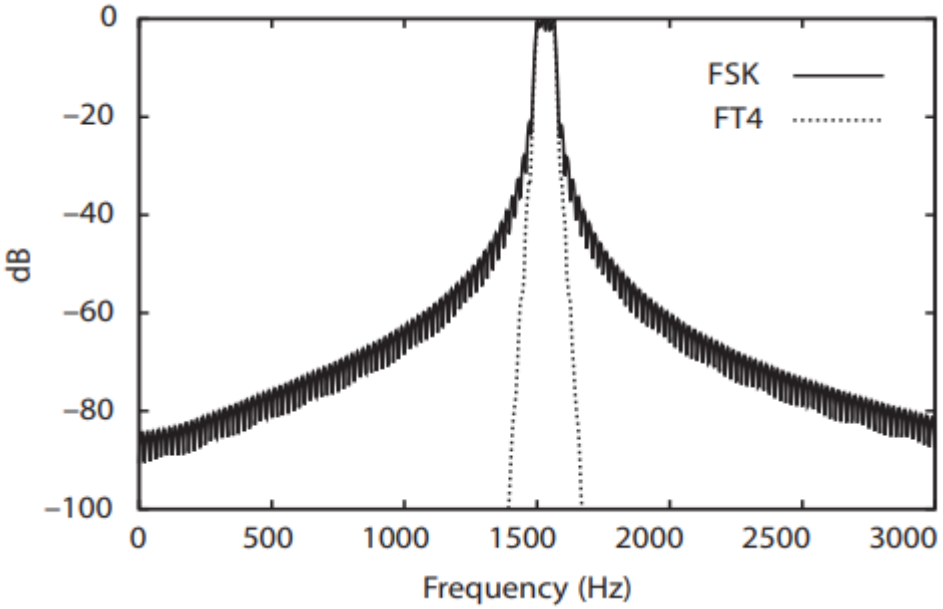

Рисунок 1

Обнаружение и декодирование символов

Некогерентное блочное обнаружение последовательностей двух или более символов канала повышает чувствительность по сравнению с односимвольным обнаружением, когда принятый сигнал поддерживает фазовую когерентность по нескольким символам [3]. Односимвольное обнаружение обеспечивает надежное обнаружение на быстро исчезающих каналах, в то время большие длины блоков обеспечивают лучшую чувствительность в условиях медленного затухания. Здесь используются длины блоков $N = 1$, 2 и 3 символа для $FT8$ и $N = 1$, 2 и 4 для $FT4$.

Обнаружение блока осуществляется путем корреляции полученных сегментов сигнала, охватывающих N символов, с локально генерируемыми формами сигнала, соответствующими каждой из M^N возможных последовательностей символов. Здесь M – количество различных модуляционных сигналов (тонов), используемых для каждого режима, $M = 8$ для $FT8$ и $M = 4$ для $FT4$.

Выход из блочного детектора представляет собой набор M^N положительных реальных значений корреляции. Они используются для получения мягких решений для каждого из $N \cdot log_2 M$ битов, передаваемых последовательностью N-символов.

Для каждого размера блока получается набор из 174 мягких решений. Они передаются в декодер, начиная с набора для $N = 1$. Если декодер возвращает кодовое слово, 77-битное сообщение которого создает 14-битный CRC,

соответствующий декодированному *CRC*, алгоритм завершается, и декодированное сообщение распаковывается и отображается пользователю.

В декодере реализован гибридный подход, который сочетает в себе быстрый, итеративный алгоритм распространения доверия (*BP*) [4] с более чувствительным, но вычислительно дорогостоящим алгоритмом декодирования упорядоченной статистики (*OSD*) [4]. Декодеры могут опционально использовать так называемую априорную информацию (*AP*), поскольку она накапливается во время сеанса двусторонней связи [5].

В табл. 2 представлены пороговые значения декодирования для трех различных каналов и трех схем декодирования.

Таблица 2.

Decoding Algoritm	*AWGN (dB)*	*Mid-latitude Disturbed (dB)*	*High-Latitude Moderate (dB)*
*FT*4:			
N=1; *BP*	-15,3	-12,7	-10,4
N=1, 2, 4; *BP*	-16,9	-14,0	-10,5
N=1,2,4; *BP*+*OSD*	-17,5	-15,2	-12,2
*FT*8:			
N=1; *BP*	-19,6	-16,5	-
N=1, 2, 4; *BP*	-20,3	-17,0	-
N=1,2,4; *BP*+*OSD*	-20,8	-18,6	-8,6

В табл. 2 показаны измеренные пороги декодирования для *FT*4 и *FT*8, полученные в результате моделирования для полосы 2500 Гц и вероятности декодирования 0,5. Числа в первой строке таблицы для каждого режима представляют базовый случай с односимвольным обнаружением *N*=1 и декодированием *BP*. Следующие две строки добавляют блок детектирования и блок детектирования с гибридным (*BP* и *OSD*) декодированием. В колонке 2 приведены результаты для канала не затухающего аддитивного белого гауссовского шума (*AWGN*), а в колонках 3 и 4 – для каналов с частотными разбросами 1 Гц и 10 Гц соответственно. Видно, что на канале *AWGN* блок обнаружения повышает чувствительность на 1,6 дБ и 0,7 дБ для *FT*4 и *FT*8 соответственно. Добавление гибридного декодирования обеспечивает еще 0,6 дБ и 0,5 дБ. В целом блочное обнаружение и гибридный декодер обеспечивают улучшение чувствительности на 2,2 и 1,2 дБ по сравнению с базовым случаем для *FT*4 и *FT*8 соответственно.

Моделирование радиоканала

При проектировании *FT*4 и *FT*8 использовано моделирование каналов, основанное на подходе, рекомендованном МСЭ, для оценки производительности, которая может быть достигнута в реальных условиях (рис. 2).

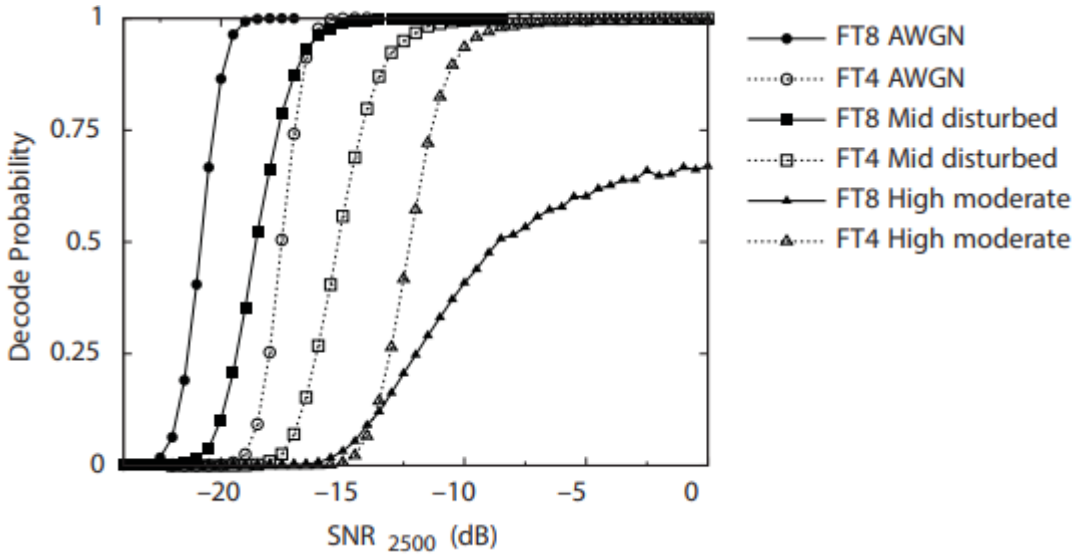

Рисунок 2

Заключение

Измеренная вероятность декодирования в зависимости от *SNR* для *FT*8 и *FT*4 основана на моделировании для трех каналов распространения: аддитивного белого гауссова шума (*AWGN*) и стандартов МСЭ для среднеширотных возмущенных и высокоширотных умеренных условий. Для этих измерений чувствительности не использовалась информация *AP*.

Литература

1. URL: https://www.zlib.net/crc_v3.txt (Дата обращения - февраль 2021).
2. URL: http://physics.princeton.edu/pulsar/k1jt/ft4_ft8_protocols.tgz (Дата обращения - февраль 2021).
3. Марвин Симон, Дариуш Дивсалар, Maximum-Likelihood Block Detection of Noncoherent Continuous Phase Modulation, IEEE Transactions on Communications, 1993. – В. 41. – № 1. – С. 90-98.
4. Шу Линн, Даниель Костелло мл. Error Control Coding: Fundamentals and Applications, 2-издание, Pearson Prentice Hall, 2004.
5. Йинкуан Ву, Христофорос Хаджикостис, Soft-Decision Decoding of Linear Block Codes Using Preprocessing and Diversifi cation, IEEE Transactions on Information Theory, 2007. – В. 53. – № 1. – С. 378-393.

МОБИЛЬНЫЙ РЕТРАНСЛЯТОР С ФУНКЦИЕЙ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ

М.С. Лохвицкий, *к.т.н., доцент, Московский технический университет связи и информатики, msl1945@mail.ru;*
В.О. Шорин, *Московский технический университет связи и информатики.*

УДК 621.396

Аннотация. Рассматривается мобильный ретранслятор в сетях сотовой связи без использования систем спутниковой связи. Такая работа возможна на судах каботажного плавания при использовании в ретрансляторе системы определения местоположения.

Ключевые слова: мобильный ретранслятор; сотовые системы связи; определение местоположения.

MOBILE REPEATER WITH LOCATION FUNCTION

Mikhail Lokhvitskiy, *Ph.D., associate professor, Moscow Technical University of Communications and Informatics;*
V.O. Shorin, *Moscow Technical University of Communications and Informatics.*

Annotation. A mobile repeater in cellular networks without the use of satellite communication systems is considered. Such work is possible on coastal vessels when using a repeater with location function.
Keywords: mobile repeater; cellular communication systems; location function.

На конференции «Мобильный бизнес: «Перспективы развития и реализации систем радиосвязи в России и за рубежом»» в октябре 2020 г. доклад «Ретранслятор для сетей мобильной связи с использованием систем определения местоположения» вызвал определенный интерес, и вместе с тем доклад вызвал много вопросов [1]. Поэтому авторы подготовили ответы и разъяснения ряда аспектов, связанных с ретранслятором.

Первое, что следует уточнить, что все изложенное в докладе относится к мобильным ретрансляторам. Т.е., к таким ретрансляторам, которые необходимо перемещать в пространстве. Если ретранслятор – стационарный, то необходимость в определении местоположения отпадает. Параметры работы такого ретранслятора настраиваются один раз при установке [2-4]. Эти параметры необходимо изменять только при переключении ретранслятора на работу с другой базовой станцией. Поэтому было изменено и название ретранслятора, лучше сказать «уточнено» название «мобильный». Покажем, где можно использовать мобильный ретранслятор.

Ретрансляторы нужно использовать там, где невозможно соединение мобильных терминалов с базовой станцией напрямую. Чаще всего невозможность установления соединения связана с большим расстоянием до ближайшей базовой станции. Для увеличения этого расстояния в [5] было предложено перенести на мобильные терминалы определение расстояния до базовой станции. Различные аспекты использования этой идеи рассмотрены в работах [6-9]. Все дело в том, что в большинстве стандартов сотовой связи необходима синхронизация работы мобильных терминалов с базовой станцией. Нужно вычислить величину времени упреждения и уровень сигнала мобильных терминалов. Эти характеристики являются функцией от расстояния между базовой станцией и соответствующим мобильным терминалом. Если вычисление времени упреждения проблем в мобильном терминале не представляется, то увеличение уровня сигнала требует использования специальных терминалов, и это является основной проблемой для внедрения изобретения [5]. В этой работе рассматривается ситуация, когда такое использование идеи изобретения [5] не вызывает особых проблем и, вместе с тем, весьма полезно.

Рассмотрим случай, когда нужно организовать связь для абонентов, находящихся на корабле, который располагается на относительно небольшом расстоянии от берега, так называемое каботажное плавание. Если это расстояние меньше предельного размера радиуса соты, то естественно, что связь между мобильными терминалами, находящимися на корабле, и базовой станцией

осуществляется непосредственно. Если же расстояние больше радиуса соты, то необходимо использовать ретранслятор. Так как корабль перемещается в акватории, то обычный ретранслятор не применим, так как его работу нужно непрерывно синхронизировать с базовой станцией. Назовем такой ретранслятор мобильным. Дальше мы рассмотрим, как нужно организовать работу такого ретранслятора.

В [1] был предложен ретранслятор сотовой связи со спутниковой системой позиционирования. В соответствии с вышесказанным, будем называть такой ретранслятор мобильным. Блок-схема мобильного ретранслятора изображена на рис. 1.

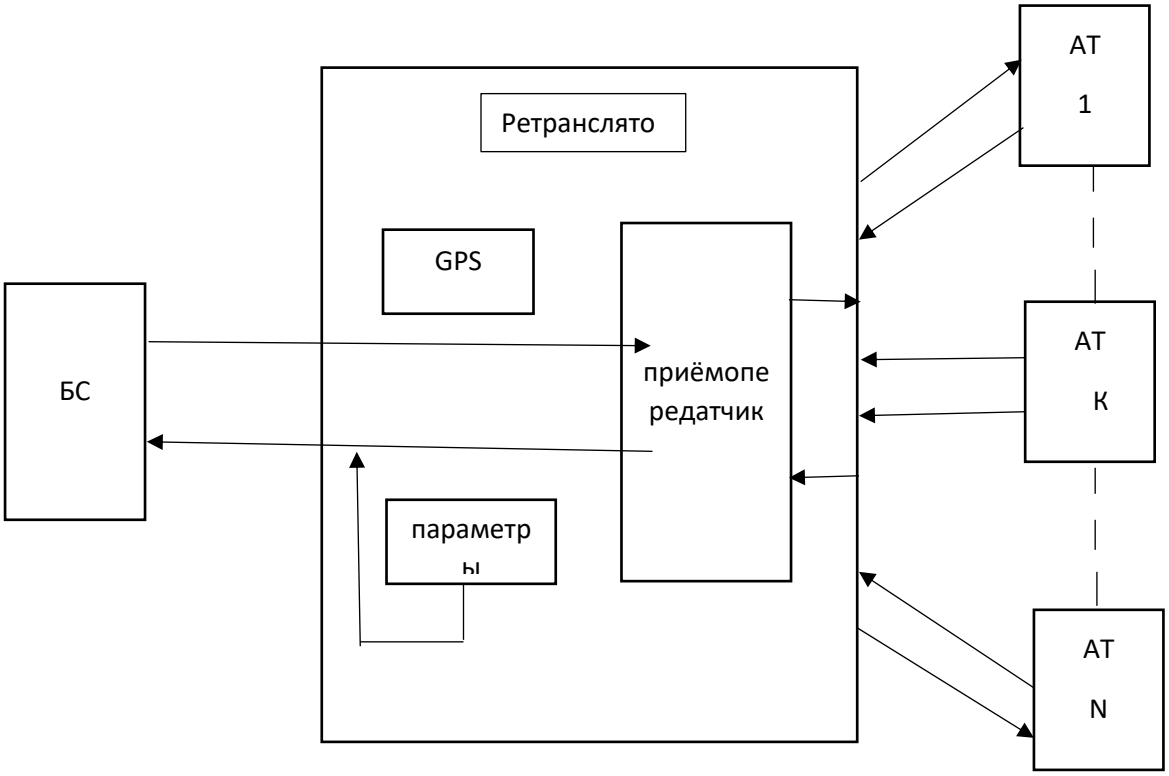

Рисунок 1

На рис. 1 изображены базовая станция (БС), абонентские терминалы (*АТ* 1, …, *АТ К*, …, *АТ N*), мобильный ретранслятор. В ретрансляторе – приёмопередатчик сигнала от (к) базовой станции и от (к) абонентским терминалам, приемник спутникового сигнала и блок вычисления параметров.

Специфика мобильного ретранслятора заключается в том, что он содержит приемник сигнала *GPS/GLONASS*, с помощью которого определяются географические координаты местоположения ретранслятора. Кроме приемника спутникового сигнала в ретрансляторе находится программа вычисления параметров синхронизации с базовой станцией (блок параметров). Эти параметры используются и в ретрансляторе, и передаются на базовую станцию. Для определения параметров синхронизации необходимо вычислять расстояние до ближайших базовых станций. А для этого нужно знать географические координаты этих станций. Получить эти координаты можно двояко: 1) каждая базовая станция передает данные координат (свои и ближайших станций) в информационном

пакете, который периодически передает каждая базовая станция; 2) информация с координатами всех возможных базовых станций заносится в память блока вычисления параметров синхронизации ретранслятора. Для вычисления расстояния до базовой станции предварительно в этом блоке вычисляют угловую разницу между точками на сфере:

$$\Delta\sigma = 2\arcsin\left\{\sqrt{\sin^2\frac{\phi-\phi_0}{2}+\cos\phi\cos\phi_0\sin^2\frac{\Delta\lambda}{2}}\right\} \quad (1)$$

где: ϕ, λ; ϕ_0, λ_0 – широта и долгота ретранслятора и базовой станции соответственно (в радианах);

$\Delta\lambda$ – разница координат по долготе.

Для вычисления расстояния S до базовой станции, необходимо угловую разницу умножить на радиус Земли, (R=6371 км). Время упреждения, определяется по формуле:

$$\Delta T = S / V \quad (2)$$

где: $V = 3\cdot10^8$ м/с – скорость распространения сигнала по радиоканалу.

В соответствии с изменением расстояния нужно изменять и мощность передаваемого сигнала. В качестве альтернативного решения можно составить карту прибрежной акватории с разбиением на соты. Если эта карта занесена в блок вычисления параметров ретранслятора, то можно определить, используя координаты местоположения ретранслятора, в какой соте в данный момент он находится. Таким образом, нет необходимости в поиске ближайшей базовой станции. Ближайшая станция определяется в этом случае автоматически. В этом случае облегчается и алгоритм хэндовера. Если ретранслятор обнаружит пересечение границы между сотами (из анализа своих географических координат), то он обращается к текущей базовой станции с запросом о хэндовере.

При запросе указывается идентификационный номер целевой станции. Именно такого типа алгоритм для хэндовера необходим, так как обычный алгоритм хэндовера здесь может не работать. Дело в том, что в обычном алгоритме хэндовер заключается в сравнении уровней мощности двух сигналов. Первый сигнал поступает от базовой станции, с которой в данный момент работает терминал. Второй сигнал поступает от целевой станции. Если мощность сигнала от целевой станции превышает мощность своей станции на пять процентов (значение по умолчанию), то делается запрос на хэндовер. Но уровень сигнала базовых станций специально для ретранслятора увеличивается в соответствии с величиной расстояния между базовой станцией и ретранслятором. Так как целевая станция до момента хэндовера не связана с ретранслятором, то уровень её сигнала может быть недостаточным для совершения хэндовера.

Заключение

В [5, 7, 8] предложенный в этой статье метод был использован в мобильных аппаратах абонентов. Однако, применить его в данной ситуации может не представиться возможности. Дело в том, что для такой операции необходимо внести необходимые дополнения в программы мобильных аппаратов. Далеко не все пользователи будут согласны это сделать, и не все пользователи сумеют это сделать. Тем более, что эти действия нужно сделать заранее, и, возможно, что, например, для разовой поездки совершать эти действия пользователи не захотят. В

то же время, использование мобильного ретранслятора предоставит пользователям все те же услуги, которыми он пользовался в обычной сотовой сети.

Использование мобильного ретранслятора с функцией систем определения местоположения позволяет существенно расширить области (как правило, имеется в виду акватории, примыкающие к береговым линиям, на которых установлены базовые станции мобильных сетей), в которых будут применяться обычные мобильные аппараты. Предложенный метод позволяет без больших изменений использовать существующее оборудование мобильных операторов. Таким образом, мобильный ретранслятор представляет собой альтернативу для существующих систем спутниковой связи.

Литература

1. Лохвицкий М.С., Шорин В.О. Ретранслятор для сетей мобильной связи с использованием систем определения местоположения / В книге: «Мобильный бизнес: Перспективы развития и реализации систем радиосвязи в России и за рубежом. РАЕН, 2020. – С. 8-11.
2. Лохвицкий М.С., Сорокин А.С., Шорин О.А. Мобильная связь: стандарты, структуры, алгоритмы, планирование. – М.: – Горячая линия – Телеком, 2018. – С. 264.
3. Лохвицкий М.С., Мардер Н.С. Сотовая связь: от поколения к поколению. – М.: Икар, 2014. – С. 236.
4. Шорина О.А. Транкинговая система широкополосного доступа МАКВИЛ. – М.: Медиа Паблишер, 2021.
5. Лохвицкий М.С., Шорин А.О. Способ сотовой связи. Патент на изобретение № 2667390 ru. НИРИТ.
6. Лохвицкий М.С., Кудин А.В., Евсеева А.А. Определение области с фиксированным временем упреждения в сотовой связи / В книге: «Мобильный бизнес: Перспективы развития и реализации систем радиосвязи в России и за рубежом. РАЕН. 2018. – С. 33-38.
7. Лохвицкий М.С. Синхронизация работы мобильных терминалов в сотовой связи с использованием спутниковых систем // Экономика и качество систем связи, 2017. – № 3(9). – С. 13-14.
8. Lokhvitskiy M.S., Shorin O.A., Shorin A.O. Implementation of the invention "Method of cellular systems". Time advance calculation. 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2019. 2019. – С. 8706788.
9. Лохвицкий М.С., Евсеева А.А. Определение области с фиксированным временем упреждения в сотовой связи // Экономика и качество систем связи, 2018. – № 1 (7). – С. 48-53.