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.

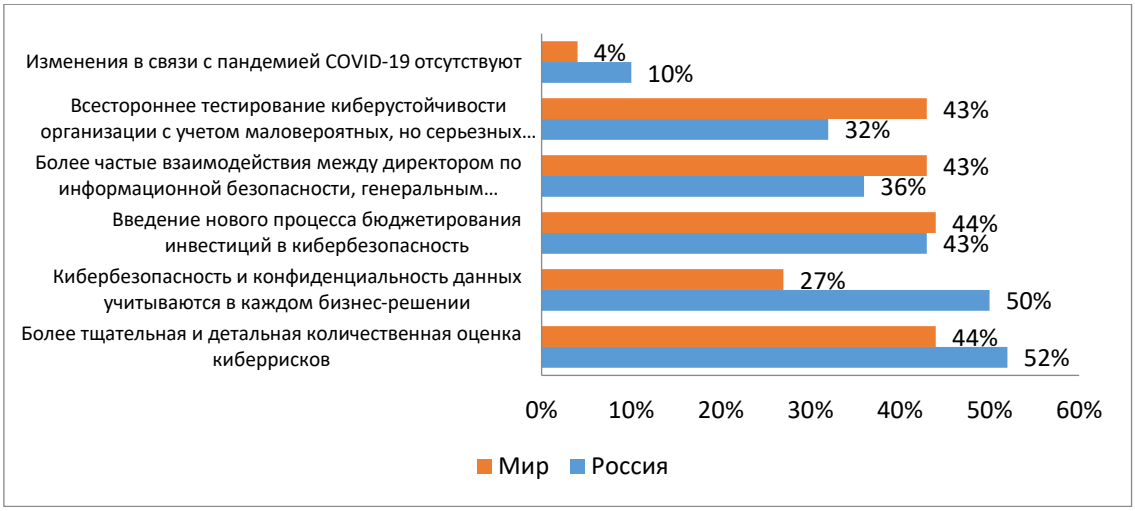

Рисунок 1

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].

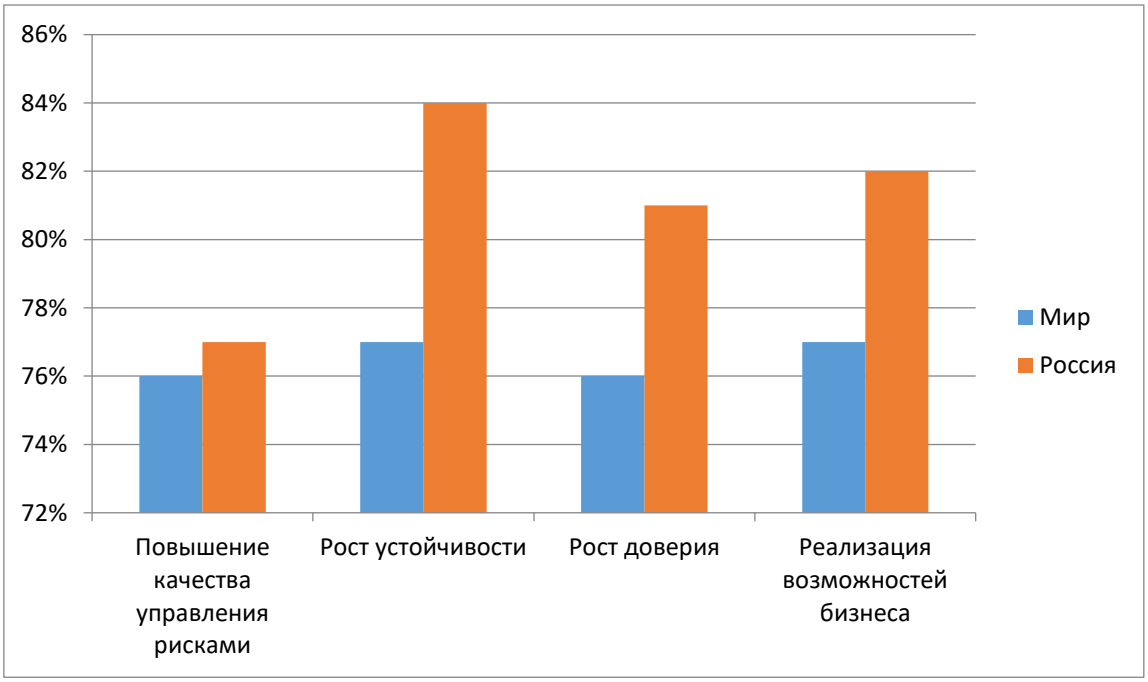

Рисунок 2

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.

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.

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].

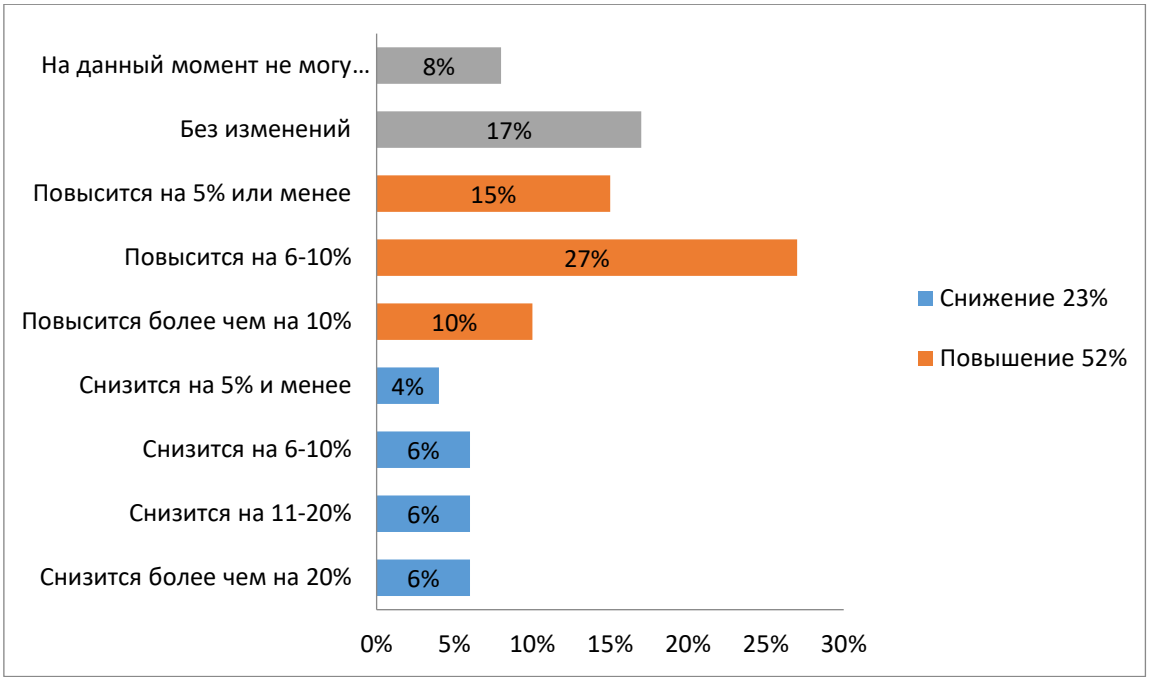

Рисунок 3

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].

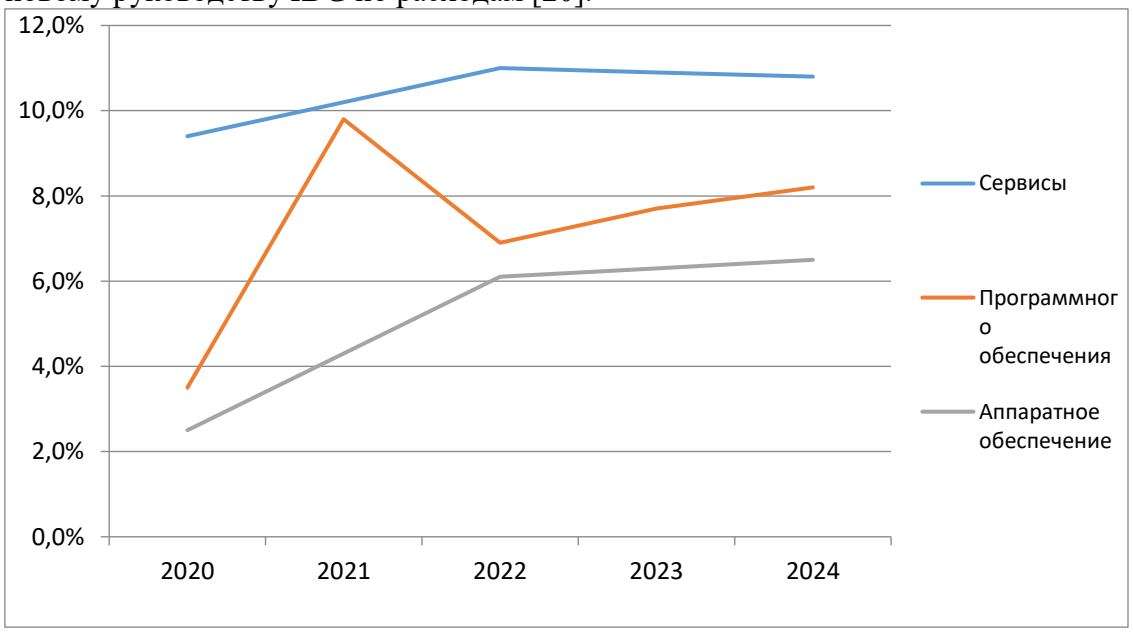

Рисунок 4

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].

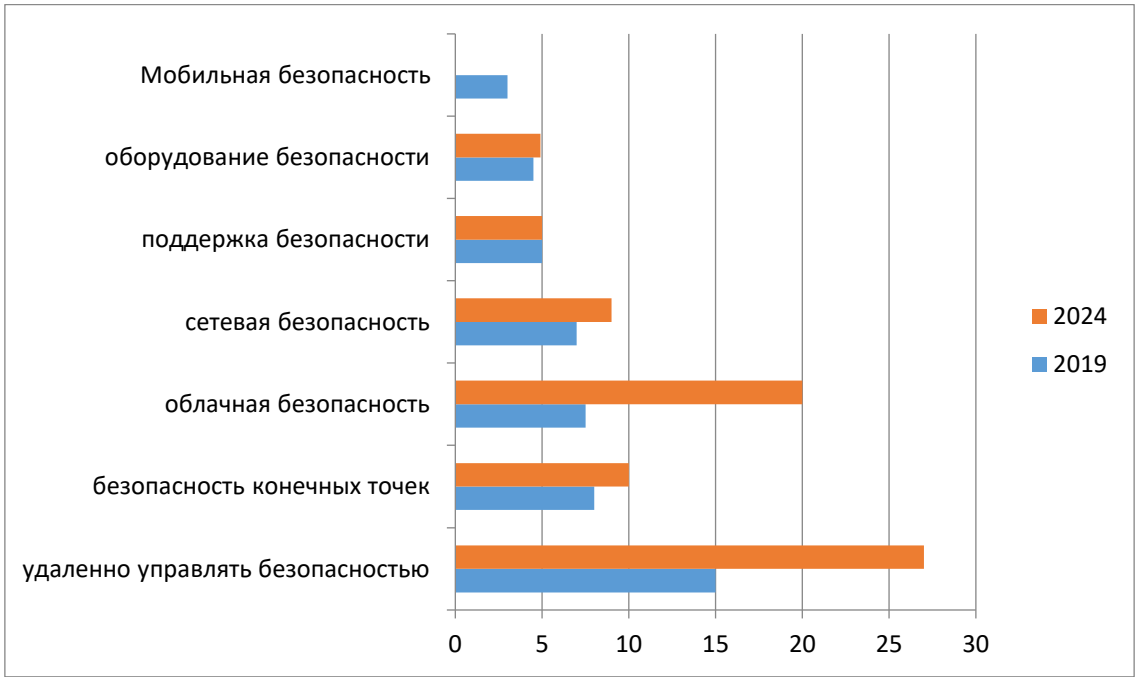

Рисунок 5

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.