РАЗДЕЛ 1. ЦИФРОВАЯ ЭКОНОМИКА

Научная статья

https://doi.org/10.54220/v.rsue.1991-0533.2025.91.3.001
УДК 658.7.01

ИССЛЕДОВАНИЕ РИСКОВ И УГРОЗ ПРИ ВНЕДРЕНИИ ЦИФРОВЫХ ТЕХНОЛОГИЙ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ

Дмитриев А. В.[1]*
[1] *Северо-Западный институт управления – филиал РАНХиГС при Президенте РФ, Санкт-Петербург, Россия*
** dmitriev-av@ranepa.ru*

Аннотация. *Введение.* В статье обсуждаются вопросы обеспечения экономической безопасности в условиях внедрения цифровых технологий в деятельность предприятий и организаций, анализируются сопутствующие этому процессу различные риски и угрозы. *Материалы и методы.* Исследуются основные задачи, связанные с разработкой и внедрением современных цифровых технологий и стимулированием инновационного развития организаций с позиции активного развития цифровой экономики. *Результаты исследования.* Делается акцент на том, что в настоящее время вопросы изучения влияния эффектов цифровой экономики и направлений нейтрализации ее рисков и угроз рассматриваются не только на государственном уровне, но и на уровне отдельных хозяйствующих субъектов. Обосновывается необходимость внедрения инструментов цифровой экономики на микроуровне с точки зрения повышения конкурентоспособности предприятий и организаций, что позволяет увеличить скорость обслуживания клиентов, повысить эффективность процесса товародвижения и предоставления широкого спектра сопутствующих услуг, что, в свою очередь, является залогом востребованности организации на рынке и обеспечивает необходимый уровень экономической безопасности. При этом относительно современных экономических условий цифровая экономика рассматривается не только как один из факторов укрепления и обеспечения экономической безопасности предприятий и организаций, но и как подсистема их цифровой безопасности, являющейся неотъемлемым элементом комплексной безопасности хозяйствующего субъекта, которая, помимо этого, включает кадровую, информационную, технико-технологическую, правовую, экологическую и другие виды безопасности. *Обсуждение и заключение.* Исследуются сущность и содержание современных цифровых рисков и угроз, а также проводится их систематизация по ряду классификационных признаков, в том числе по виду риска, по уровню возникновения, по вероятности наступления риска, по скорости нарастания риска, по продолжительности воздействия, по степени убытка от воздействия риска. Уделено внимание специфике использования инструментов цифровой безопасности организаций.

Ключевые слова: цифровая экономика, экономическая безопасность, цифровая безопасность, риски и угрозы безопасности, цифровые технологии, цифровые инструменты, банковский сектор.

Для цитирования: Дмитриев А. В. Исследование рисков и угроз при внедрении цифровых технологий в кредитно-финансовой сфере. *Вестник Ростовского государственного экономического университета (РИНХ).* 2025;3(32):10-21. doi: 10.54220/v.rsue.1991-0533.2025.2025.91.3.001.

Research article

JEL G32 M15 M21

STUDY OF RISKS AND THREATS IN THE IMPLEMENTATION OF DIGITAL TECHNOLOGIES IN THE CREDIT AND FINANCIAL SPHERE

Dmitriev A.*[1]
[1] *North-Western Institute of Management – branch of RANEPA under President of Russian Federation, St. Petersburg, Russia*
** dmitriev-av@ranepa.ru*

Abstract. *Introduction.* The article discusses the issues of ensuring economic security in the context of the introduction of digital technologies in the activities of enterprises and organizations and analyzes the various risks and threats associated with this process. *Materials and methods.* The main tasks associated with the development and implementation of modern digital technologies and stimulating the innovative development of organizations from the standpoint of active development of the digital economy are studied. *Research results.* Emphasis is placed on the fact that at present, issues of studying the influence of the effects of the digital economy and directions for neutralizing its risks and threats are considered not only at the state level, but also at the level of individual economic entities. The need to introduce digital economy tools at the micro level is substantiated in terms of increasing the competitiveness of enterprises and organizations, which allows increasing the speed of customer service, increasing the efficiency of the goods distribution process and providing a wide range of related services, which, in turn, is the key to the organization's demand in the market and ensures the necessary level of economic security. At the same time, in relation to modern economic conditions, the digital economy is considered not only as one of the factors for strengthening and ensuring the economic security of enterprises and organizations, but also as a subsystem of their digital security, which is an integral element of the comprehensive security of an economic entity, which, in addition, includes personnel, information, technical and technological, legal, environmental and other types of security. *Discussion and conclusion.* The essence and content of modern digital risks and threats are studied, and they are systematized according to a number of classification features, including by type of risk, by level of occurrence, by probability of risk occurrence, by rate of risk increase, by duration of impact, by degree of loss from risk impact. Attention is paid to the specifics of using digital security tools of organizations.

Keywords: digital economy, economic security, digital security, security risks and threats, digital technologies, digital tools, banking sector.

For citation: Dmitriev A. Study of risks and threats in the implementation of digital technologies in the credit and financial sphere. *Vestnik of Rostov State University of Economics (RINH).* 2025;3(32):10-21. doi: 10.54220/v.rsue.1991-0533.2025.91.3.001.

Введение

В соответствии со Стратегией экономической безопасности РФ до 2030 г., одной из основных задач в сфере разработки и внедрения современных технологий и стимулирования инновационного развития является развитие технологий цифровой экономики, что обеспечивает укрепление конкурентных позиций Российской Федерации на глобальных рынках.

Стоит отметить, что вопрос изучения цифровой экономики последние несколько лет остро поднимается с точки

зрения нейтрализации рисков и угроз не только на государственном уровне, но и на уровне отдельных хозяйствующих субъектов. Современный этап технологического развития устанавливает новые цифровые тенденции, которые требуют от экономических субъектов активно внедрять инновационные решения в своей деятельности.

Чтобы оставаться конкурентоспособными, предприятия и организации по всему миру внедряют в свою работу цифровые технологии. Скорость обслуживания клиентов, быстрая доставка продуктов, предоставление широкого функционала необходимых услуг, собранных в одном месте, – все это реалии современного мира, к которым стремятся организации, чтобы оставаться востребованными на рынке и обеспечивать необходимый уровень экономической безопасности [1].

Сегодня цифровая экономика занимает отдельное место и в стратегии развития большинства предприятий. Внедрение искусственного интеллекта и создание отдельных цифровых платформ позволяет не только выделить организацию среди других, тем самым делая рекламу, но и приумножать выручку организаций в несколько раз. Именно поэтому с каждым годом организации закладывают в свой бюджет все больше расходов на цифровое развитие, тем самым проживая процесс цифровизации и цифровой трансформации [2].

В современных экономических условиях цифровая экономика представляет собой один факторов укрепления и обеспечения экономической безопасности предприятий и организаций и входит в подсистему их цифровой безопасности (ЦБ), являющейся неотъемлемым элементом комплексной безопасности хозяйствующего субъекта наряду с кадровой, информационной, технико-технологической, правовой, экологической и другими видами безопасности [3].

Целью исследования является обоснование направлений нейтрализации рисков и угроз экономической и информационной безопасности при внедрении в деятельность предприятий и организаций различных современных инструментов цифровой экономики.

Материалы и методы

Существует довольно много подходов к трактовке термина «цифровая безопасность», которые связаны с рассмотрением ЦБ в качестве объективной реальности, позволяющей найти пути инновационного развития организации [10], фактора повышения эффективности деятельности организации за счет более полного и широкого применения возможностей различных методов и технологий обработки экономической информации [13], современного инструментария, позволяющего эффективно управлять множеством процессов в экономике [7].

Кроме того, вопросам использования цифровых технологий с целью обеспечения экономической безопасности предприятий и организаций также посвящен целый ряд научных исследований.

Работы [6, 8] связаны с выявлением совокупности факторов, оказывающих влияние на принятие решений промышленными субъектами о внедрении современных цифровых технологий на базе искусственного интеллекта, что позволяет оценить эффекты по замещению и дополнению когнитивных способностей у сотрудников предприятий и исследовать перспективы получения конкурентных преимуществ на этой базе.

Авторы [9] рассматривают цифровизацию с позиции одной из важнейших тенденций в развитии общества, которая, наряду с целым рядом положительных последствий для экономической деятельности, сопровождается целым рядом вызовов и угроз, достаточно серьезно влияющих на ход экономических процессов. Исследователи подчеркивают, что цифровизацию можно рассматривать, с одной стороны, как трансформацию любой информации в цифровой формат, предполагающий в дальнейшем эффективное использование данных, представ-

ленных в цифровой форме, с другой стороны, как цифровую форму, порождающую набор новых вызовов, угроз, отрицательных последствий и рисков, определяющих необходимость совершенствования системы кибербезопасности предприятий.

В статье [12] обосновываются направления поиска решения проблем цифровизации предприятий в современных условиях неопределенности и экономической турбулентности, которые вызваны введением все новых пакетов санкций, запретов и ограничений со стороны западных стран и изменениями в геополитическом и геоэкономическом мировом ландшафте. Авторы подчеркивают, что в сложившихся условиях корректный и взвешенный подход к выбору цифровых стратегий и приоритетных направлений цифрового развития становится важным с точки зрения реализации эффективного и сбалансированного управленческого инструментария в сфере промышленного менеджмента. С учетом глобальных трендов на цифровую трансформацию и возрастающего предложения программных продуктов со стороны ИТ-разработчиков ученые обосновывают сферы целесообразного применения программного обеспечения в деятельности конкретных предприятий.

Цифровые данные и цифровые технологии сами по себе также можно рассматривать и как фактор производства в современных экономических условиях. Тем самым предопределяется процесс развития хозяйственной деятельности предприятий и их перехода на инновационные и прогрессивные методы функционирования [5].

Процесс развития цифровой экономики можно наблюдать на разных уровнях, в том числе на макро-, мезо- и микроуровне. В рамках деятельности отдельного предприятия или отдельной организации подобные процессы также имеют важное значение. При изучении отдельных хозяйствующих субъектов на микроуровне цифровизация рассматривается как существенный фактор повышения конкурентоспособности хозяйствующих субъектов на рынке, поэтому обеспечение высокого уровня цифровой безопасности становится объективно необходимым [11].

В настоящем исследовании под цифровой безопасностью как составляющей экономической безопасности будет пониматься состояние защищенности цифровых сведений, устройств и ресурсов хозяйствующего субъекта, включая такие элементы, как личные данные, учетные записи, файлы, фотографии, безналичные и электронные деньги.

Главной задачей внедрения цифровых технологий с позиции обеспечения экономической безопасности становится оптимизация и реинжиниринг бизнес-процессов предприятия. Однако терминологически между понятиями «цифровизация» и «цифровая трансформация» есть некоторые различия. Цифровая трансформация – это глубокие изменения, которые оказывают влияние на все бизнес-процессы организации. Такие процессы характеризуются резким снижением транзакционных издержек за счет новых цифровых платформ, появлением новых моделей деятельности. В результате цифровой трансформации могут получиться абсолютно новые процессы и продукты. В то же время примером цифровизации в компаниях может служить, например, установка корпоративной или CRM-системы. Если эта же организация использует системы искусственного интеллекта в обучении сотрудников, начнется уже цифровая трансформация бизнеса.

Но, как и любое нововведение, цифровизация несет в себе ряд угроз и рисков в системе обеспечения комплексной безопасности организации. Под угрозой следует понимать совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба. Угроза представляет собой высший уровень опасности, т. е. это опасность, переходящая в практическую

плоскость, в то время как риск – это лишь возможность нанесения ущерба в связи с реализацией угрозы.

Существуют различные методы классификации угроз и рисков цифровизации. Во-первых, все риски от внедрения цифровых технологий можно систематизировать по следующим классификационным признаками: по виду риска, по уровню возникновения, по вероятности наступления риска, по скорости нарастания риска, по продолжительности воздействия, по степени убытка от воздействия риска.

Результаты классификации представлены на рисунке 1.

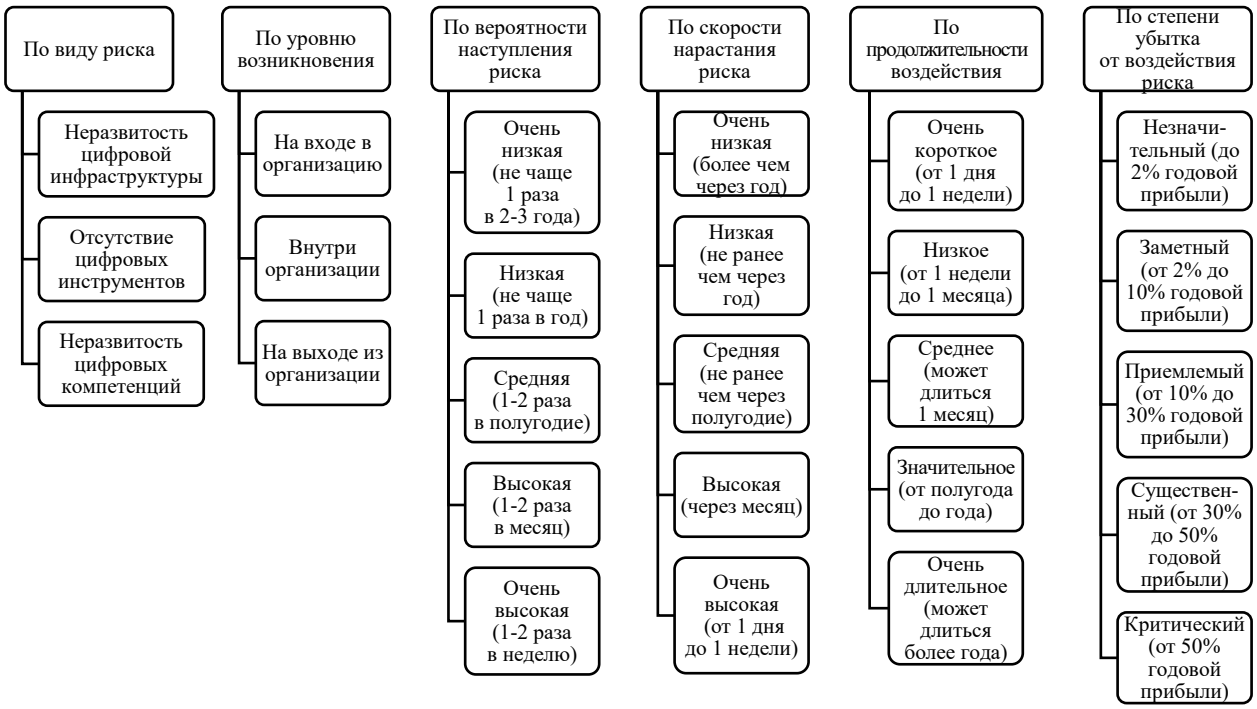


Рисунок 1 – **Классификация рисков и методов их оценки при внедрении цифровых технологий** [4]
Figure 1 – **Classification of risks and methods for assessing them when implementing digital technologies** [4]

Многие цифровые инструменты остаются невостребованными в деятельности организации, что увеличивает вероятность наступления риска ее цифровой безопасности. В связи с этим увеличиваются масштабы компьютерной преступности, особенно в кредитно-финансовой сфере, а также число преступлений, связанных с нарушением конституционных прав и свобод человека при обработке персональных данных с использованием информационно-коммуникационных технологий.

Как видим, большое внимание при внедрении цифровых технологий следует уделить цифровым инструментам. Цифровые инструменты – это программы, приложения и устройства, с помощью которых ведется работа по взаимодействию с цифровыми данными и их защите. Отсутствие и неразвитость цифровых инструментов – это определенные риски в обеспечении комплексной безопасности организации.

Большое значение в предупреждении рисков и угроз цифровой экономики играют и цифровые компетенции сотрудников организаций. В настоящее время в области управления персоналом широко применяется такое понятие, как цифровое неравенство. Особенно ярко это проявляется в вопросах переподготовки сотруд-

ников, которые в силу своего возраста меньше и медленнее осваивают новые цифровые технологии. По своему незнанию в использовании данных работниками могут быть совершены грубые ошибки, которые повлекут за собой существенные проблемы в области цифровой и информационной безопасности.

Внедрение цифровых технологий требует в совокупности больших финансовых вложений, технической оснащенности и наличия цифровой культуры в организации. Организации необходимо создать условия для обеспечения цифровой безопасности как с экономической стороны, так и с позиции технической оснащенности и грамотно обученного персонала. Можно сказать, что синергия данных направлений обеспечивает организации устойчивость и развитие в области цифровой безопасности.

Результаты исследования

Учитывая вышеизложенное, можно отметить, что нейтрализация угроз цифровой экономики и обеспечение цифровой безопасности предприятия определяется взаимодействием целого ряда составляющих: инновационной, технико-технологической, кадровой, кибербезопасности.

ИТ-инфраструктура является основой для внедрения новых технологий и инноваций. Инновационная безопасность организации во многом определяет ее конкурентоспособность на рынке, доступ к информации, а также дополнительные возможности по удаленной работе сотрудников и эффективному использованию технологий. Это всецело можно отнести и к деятельности банковских организаций.

В качестве примера можно рассмотреть специфику создания системы обеспечения цифровой безопасности ПАО «Сбербанк» («Сбер»), в том числе на основе анализа динамики затрат на технологическую трансформацию указанной организации (рис. 2).

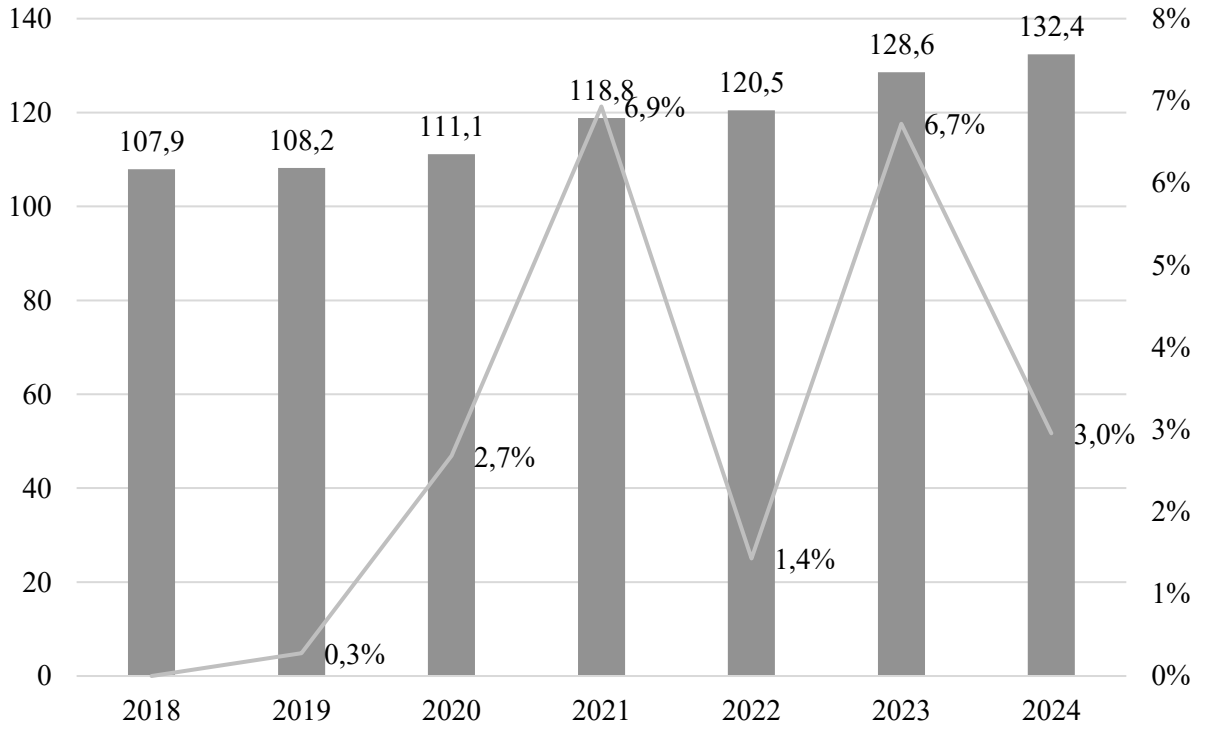


Рисунок 2 – **Затраты ПАО «Сбербанк» на технологическую трансформацию, млрд руб.** [14]

Figure 2 – **Sberbank PJSC's costs for technological transformation, billion rubles** [14]

Результаты исследования показывают, что динамика затрат на технологии носит положительный характер. Ежегодно ПАО «Сбербанк» выделяет большие средства на инновационные разработки, исследования и новые технологии. Для сравнения, в базисном 2018 г. затраты на технологическую трансформацию составляли 107,9 млрд руб., что на 23 % меньше, чем в предыдущем 2024 г. С каждым годом потребность в инновационных технологиях возрастает, и банк активно увеличивает свои затраты на обеспечение данной сферы.

В целях обеспечения безопасности и бесперебойной работы сервисов ПАО «Сбербанк» ускорил, а в некоторых областях только запустил процесс перехода на отечественное программное обеспечение (ПО) и цифровые платформы. Продолжение работы с использованием иностранных технологий несет в себе определенные риски для управления и технического обслуживания систем.

На рисунке 3 представлена схема вендорозамещения на всех уровнях технологического стека в следующем порядке: область замещения – вендоры, прекратившие сотрудничество с ПАО «Сбербанк» – замещающие решения. Очевидно, что организацией были приняты меры по сохранению и обеспечению технико-технологической и информационной безопасности. Удалось смягчить последствия санкционного давления путем разработки собственных платформ и их внедрения в повседневные процессы работы. Более того, ПАО «Сбербанк» стал менее зависим от иностранных поставщиков, что особенно выражалось в использовании оборудования и ПО, в том числе в части программно-аппаратных комплексов и инженерных систем центра обмена данными (ЦОД).

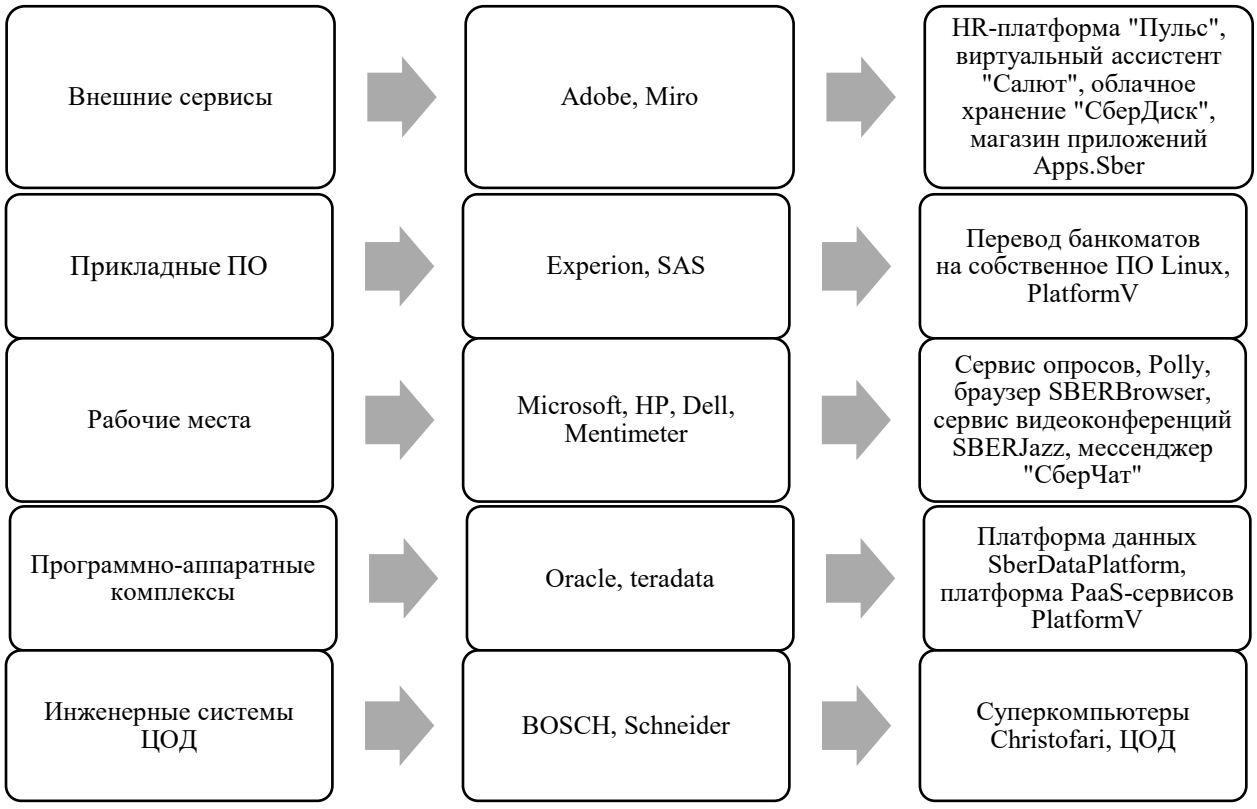


Рисунок 3 – **Вендорозамещение в ПАО «Сбербанк»** [8]
Figure 3 – **Vendor replacement at Sberbank PJSC** [8]

Обсуждение

Безусловно, не все процессы, продукты и программы удалось перевести на отечественные разработки, но организации удалось минимизировать часть возможных будущих рисков, связанных с невозможностью технического обслуживания и дополнительного приобретения комплектующих товаров. Тем не менее удается эффективно поддерживать функциональность цифровой инфраструктуры организации, в том числе работу мобильного приложения «Сбербанк Онлайн» (СБОЛ).

С каждым годом количество уникальных пользователей, которые взаимодействуют с мобильным приложением в течение месяца, только растет. Клиенты активно пользуются цифровой платформой и получают большой спектр услуг без выезда в офис банка. На 30 сентября 2024 г. показатель MUA (Monthly Active Users) достиг отметки 81 млн человек, что на 2,4 млн больше, чем за предыдущий 2023 г. Показатель DAU (Daily Active Users) достиг значения 42,2 млн ежедневных уникальных пользователей (рис. 4).

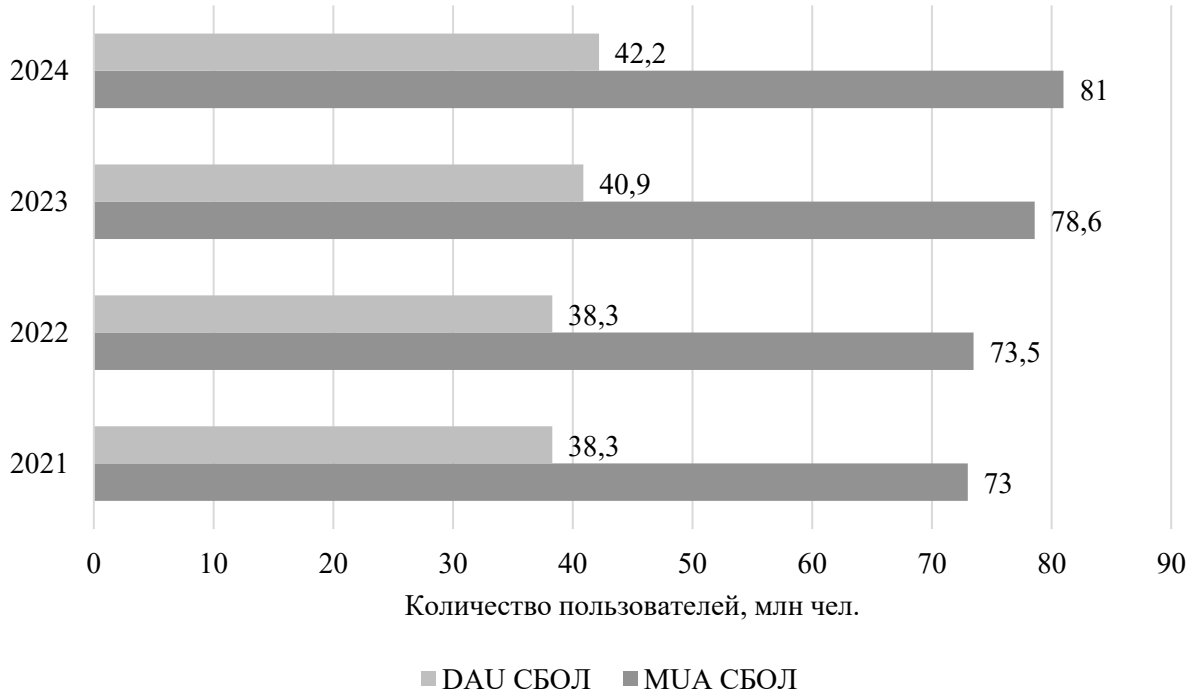


Рисунок 4 – **Количество пользователей мобильного приложения «Сбербанк Онлайн»** [14]

Figure 4 – **Number of users of the Sberbank Online-mobile app** [14]

На фоне успешного перехода организации на отечественное оборудование и популярности использования цифровых платформ возрастают и попытки кибератак на различные сервисы отечественного банковского сектора, в том числе и на ПАО «Сбербанк».

На графике рисунка 5 представлена динамика по количеству крупных DDoS-атак. По данным представленной диаграммы, самое большое количество крупных DDoS-атак – 490 – пришлось на 2024 г., что на 206 % больше, чем за предыдущий 2023 г. Самую мощную атаку «Сбер» зафиксировал в сентябре 2024 г.: она велась 13 часов почти с трех десятков тысяч устройств, расположенных на территории Тайваня, США, Японии и Великобритании. Но стоит отметить, что каждый год количество совершенных атак соответствует количеству отраженных.

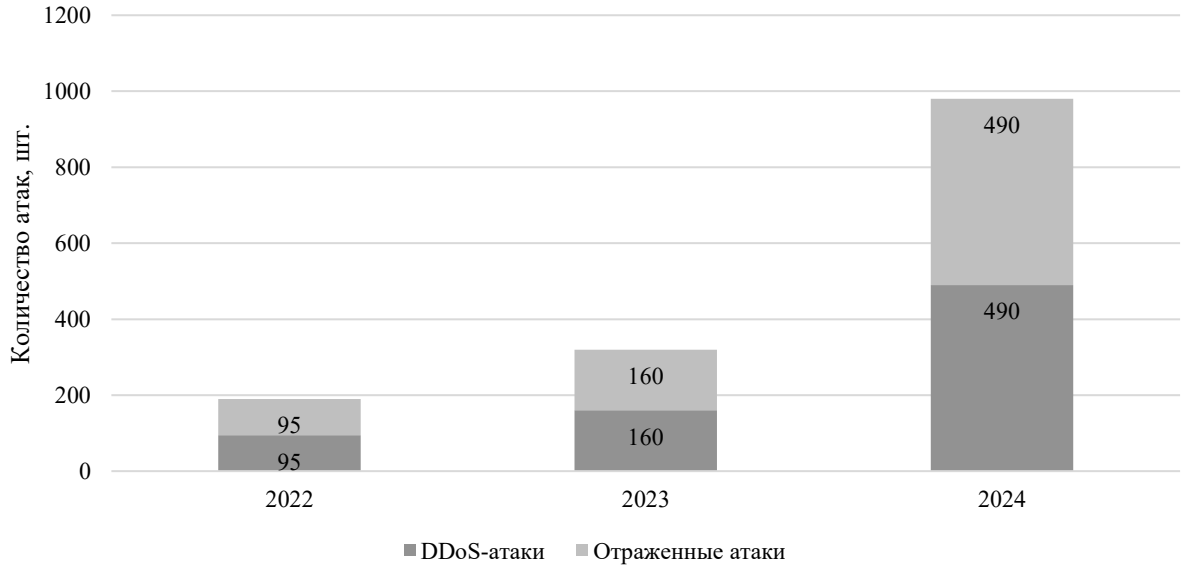


Рисунок 5 – **Динамика DDoS-атак на инфраструктуру ПАО «Сбербанк»** [15]
Figure 5 – **Dynamics of DDoS attacks on the infrastructure of Sberbank PJSC** [15]

Большой вклад в обеспечение информационной безопасности и кибербезопасности вносят ИТ-специалисты. Внедрение новых технологических решений, отражение кибератак, бесперебойная работа банковских сервисов – все это было бы невозможным без квалифицированных кадров в ИТ-индустрии. В данном случае затрагивается аспект кадровой составляющей как одной из частей обеспечения цифровой безопасности.

Сегодня в ПАО «Сбербанк» открыто более тысячи вакансий на должности специалистов по информационной безопасности, аналитиков данных, датасайентистов, программистов, разработчиков и других специальностей из сферы информационных технологий.

Заключение

Проведенное исследование показало высокие результаты уровня цифровизации ПАО «Сбербанк», многие процессы цифровизированы не на 100 % и оставляют за собой использование ручного труда, который замедляет работу многих бизнес-процессов и несет в себе ряд рисков. Кроме того, в анализе были отражены основные направления, которые не затрагивают многие мелкие бизнес-процессы. В ПАО «Сбербанк» есть как сильные стороны с возможностями улучшения, так и слабые стороны с угрозами. Безусловно, большой парк оборудования эквайринга является преимуществом, отличающим ПАО «Сбербанк» от других банков, но стоит помнить, что в современных условиях поставки нового иностранного оборудования постепенно прекращаются, а ремонт действующих терминалов становится все более недоступным из-за дефицита необходимых запчастей и их стоимости.

В целом, если рассматривать банковский сектор как таковой, можно сделать вывод, что несмотря на развитие онлайн-обслуживания часть бизнес-процессов остается на штатных менеджерах. Примером такого процесса является оформление юридическим лицом или индивидуальным предпринимателем контрольно-кассовой техники, которое происходит только в присутствии менеджера банка при наличии личного кабинета клиента.

С точки зрения экономической безопасности отсутствие цифровизации некоторых процессов можно объяснить следующим образом.

1. Неэффективное использование рабочего времени менеджера, который выполняет бумажную работу при наличии онлайн-кабинета в приложении клиента.

2. Возрастание риска утечки данных в связи с постоянным предоставлением клиентом своих персональных данных разным менеджерам.

3. Упущенная возможность в получении прибыли банком в результате ожидания клиентов, а впоследствии ухода в банк-конкурент.

Можно сделать следующие выводы.

1. Для обеспечения инновационной безопасности организаций, в том числе банковского сектора, в рамках осуществления цифровой безопасности необходимо ежегодное увеличение затрат на технологическую трансформацию организации. Это позволит организациям внедрять передовые цифровые продукты и технологии в свою работу.

2. Технико-технологическая составляющая цифровой безопасности в современных условиях обеспечивается переходом на отечественное оборудование, используются ПО/облачные сервисы собственной разработки. Так, организации минимизируют будущие риски, связанные с техническим обслуживанием западного оборудования и новыми поставками. На замену западным технологиям пришли новые продукты, в том числе, например, собственные разработки ПАО «Сбербанк»: SBERBrowser, сервис видеоконференций SBERJazz, мессенджер «СберЧат».

3. По результатам анализа деятельности такой крупной банковской структуры, как ПАО «Сбербанк», было выявлено, что слабые стороны в обеспечении цифровой безопасности, в частности подсистемы экономической безопасности, нашли свое отражение в консерватизме и масштабности структуры, что не позволяет организации оперативно реагировать на изменения меняющейся цифровой среды и принимать быстрые управленческие решения.

4. Угрозы в области цифровой экономики и, как следствие, цифровой безопасности организаций банковского сектора связаны с проведением безналичных платежей с использованием иностранного оборудования – терминалов эквайринга. Значимой угрозой также является утечка данных клиентов в связи с популяризацией оплат с помощью биометрии.

5. Несмотря на наличие слабых сторон и угроз цифровой безопасности, у организаций банковского сектора есть ряд возможностей, связанных с увеличением доли цифровизированных и автоматизированных процессов, а также замены всех терминалов эквайринга зарубежного производства на отечественные, реализация которых позволит повысить не только уровень цифровой безопасности, но и в целом уровень экономической безопасности организации.

Список литературы

1. *Дмитриев, А. В.* Методологические основы управления логистикой транспортно-складских центров // Известия Санкт-Петербургского университета экономики и финансов. – № 6 (78). – С. 76-81.

2. *Дмитриев, А. В.* Диджитализация транспортной логистики. – СПб., 2018.

3. *Дмитриев, А. В., Щербаков, В. В.* Обеспечение экономической безопасности и устойчивости цепей поставок в условиях цифровизации // Вестник факультета управления СПбГЭУ. – № 15. – С. 11-18.

4. Стратегическое управление экономической устойчивостью предприятия в нечетко-логической парадигме / Ю. А. Малюков, А. О. Недосекин, З. И. Абдулаева // Стратегические решения и риск-менеджмент. – № 14 (2). – С. 136-149. – DOI: 10.17747/2618-947X-2023-2-136-149.

5. Национальная экономическая безопасность и государственная политика развития промышленности / В. А. Плотников, В. В. Погодина, А. А. Смирнов // Управленческое консультирование. – № 9. – С. 35-44. – DOI: 10.22394/1726-1139-2023-9-35-44.

6. *Свадковский, В. А.* Применение цифровых двойников для повышения операционной эффективности предприя-

тий добывающих отраслей // Стратегические решения и риск-менеджмент. – 2023. – Т. 14, № 3. – С. 292-311. – DOI: 10.17747/2618-947X-2023-3-292-311.

7. *Соболева, Ю. П., Мосина Д. А.* Цифровая трансформация бизнес-процессов // Экономика и бизнес: цифровая трансформация и перспективы развития : материалы международной научно-практической конференции: в 2-х т., Москва, 14 апреля 2022 г. – М., 2022. – Т. 1. – С. 203-208.

8. *Трачук, А. В., Линдер, Н. В.* Эффекты цифровых платформ для промышленных компаний: эмпирический анализ в условиях внешнего санкционного давления // Стратегические решения и риск-менеджмент. – № 14 (2). – С. 150-163. – DOI: 10.17747/2618-947X-2023-2-150-163.

9. *Халин, В. Г., Чернова, Г. В.* Цифровизация и киберриски // Управленческое консультирование. – № 7. – С. 28-41. – DOI: 10.22394/1726-1139-2023-7-28-41.

10. Цифровая трансформация экономики и промышленности: проблемы и перспективы / А. А. Алетдинова, И. А. Аренков, Р. Р. Афанасьева [и др.]. – СПб., 2017. – 807 с. – DOI: 10.18720/IEP/2017.4.

11. Обеспечение экономической безопасности в логистике гособоронзаказа / Г. Н. Чернышева, Г. А. Лавренова, Ю. А. Савич, Э. Б. Лубянская // Организатор производства. – № 29 (3). – С. 171-184. – DOI: 10.36622/VSTU.2021.47.14.015.

12. *Шабаева, С. В., Шабаев, А. И.* Инструменты реализации стратегий в условиях цифровой трансформации промышленных предприятий // Управленческое консультирование. – № 10. – С. 69-79. – DOI: 10.22394/1726-1139-2023-10-69-79.

13. *Шершнева, А. В., Пальчикова, Н. С.* Трансформация бизнеса в условиях цифровой экономики // Стратегия предприятия в контексте повышения его конкурентоспособности. – 2019. – № 8. – С. 215-219.

14. Прогноз развития рынка кибербезопасности в Российской Федерации на 2022-2026 гг. [Электронный ресурс]. – URL: https://www.csr.ru/ru/research (дата обращения: 29.04.2024).

15. С начала года число DDoS-атак на Сбербанк выросло [Электронный ресурс]. – URL: https://www.interfax.ru/spief 2024/965360 (дата обращения: 24.02.2025).

References

1. *Dmitriev, A.* Methodological foundations of logistics management in transport and warehousing centers // News of St. Petersburg University of Economics and Finance. – № 6 (78). – P. 76-81.

2. *Dmitriev, A.* Digitization of transport logistics. – SPb., 2018.

3. *Dmitriev, A., Shcherbakov, V.* Ensuring economic security and sustainability of supply chains in the context of digitalization // Bulletin of the Faculty of Management, St. Petersburg State University of Economics and Finance. – № 15. – P. 11–18.

4. Strategic management of economic sustainability of an enterprise in a fuzzy-logical paradigm / Yu. Malyukov, A. Nedosekin, Z. Abdulayeva // Strategic Decisions and Risk Management. – № 14 (2). – P. 136-149. – DOI: 10.17747/2618-947X-2023-2-136-149.

5. National economic security and state policy for industrial development / V. Plotnikov, V. Pogodina, A. Smirnov // Management Consulting. – № 9. – P. 35-44. – DOI: 10.22394/1726-1139-2023-9-35-44.

6. *Svadkovsky, V.* Application of digital twins to improve the operational efficiency of extractive industries // Strategic Decisions and Risk Management. – 2023. – Vol. 14, № 3. – P. 292-311. – DOI: 10.17747/2618-947X-2023-3-292-311.

7. *Soboleva, Yu., Mosina, D.* Digital transformation of business processes // Economics and business: digital transformation and development prospects : proceedings of international scientific-practical conference : in 2 vol., Moscow, April 14, 2022. – M., 2022. – Vol. 1. – P. 203-208.

8. *Trachuk, A., Linder, N.* Effects of digital platforms for industrial companies: empirical analysis in conditions of external

sanctions pressure // Strategic Decisions and Risk Management. – № 14 (2). – P. 150-163. – DOI: 10.17747/2618-947X-2023-2-150-163.

9. *Khalin, V., Chernova, G.* Digitalization and cyber risks. Management Consulting. – № 7. – P. 28-41. – DOI: 10.22394/1726-1139-2023-7-28-41.

10. Digital transformation of the economy and industry: problems and prospects / A. Aletdinova, I. Arenkov, R. Afanasyeva [et al.]. – SPb., 2017. – 807 p. – DOI: 10.18720/IEP/2017.4.

11. Ensuring economic security in the logistics of state defense orders / G. Chernysheva, G. Lavrenova, Yu. Savich, E. Lubyanskaya // Production Organizer. – № 29 (3). – P. 171-184. – DOI: 10.36622/VSTU.2021.47.14.015.

12. *Shabaeva, S., Shabaev, A.* Tools for implementing strategies in the context of the digital transformation of industrial enterprises // Management Consulting. – № 10. – P. 69-79. – DOI: 10.22394/1726-1139-2023-10-69-79.

13. *Shershneva, A., Palchikova, N.* Business transformation in the digital economy // Enterprise strategy in the context of increasing its competitiveness. – 2019. – № 8. – P. 215-219.

14. Forecast for the development of the cybersecurity market in Russian Federation for 2022-2026 [Electronic resource]. – URL: https://www.csr.ru/ru/research (date of access: 29.04.2024).

15. Since the beginning of the year, the number of DDoS attacks on Sberbank has increased [Electronic resource]. – URL: https://www.interfax.ru/spief2024/965360 (date of access: 24.02.2025).

Об авторах:

Дмитриев Александр Викторович, *доктор экономических наук, доцент, зав. кафедрой безопасности Северо-Западного института управления – филиала РАНХиГС при Президенте РФ, Санкт-Петербург, Россия, dmitriev-av@ranepa.ru*

Конфликт интересов: автор заявляет об отсутствии конфликта интересов.

Статья опубликована на условиях лицензии Creative Commons Attribution 4.0 International (CC-BY 4.0)

About the Authors:

Alexander Dmitriev, *Dr. Sci. (Econ.), Associate Professor, Head of the Department of Safety, North-Western Institute of Management – branch of RANEPA under President of Russian Federation, St. Petersburg, Russia, dmitriev-av@ranepa.ru*

Conflict of Interest: The author declare no conflicts of interest.

This is an open access article distributed under the terms of Creative Commons Attribution 4.0 International License (CC-BY 4.0)