ISSN 2073-5537 (Print), ISSN 2309-9798 (Online)

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ: ЭКОНОМИКА, ПРЕДПРИНИМАТЕЛЬСТВО, ТЕХНОЛОГИИ, ИННОВАЦИИ

DIGITAL TRANSFORMATION: ECONOMICS, ENTREPRENEURSHIP, TECHNOLOGY, INNOVATION

Научная статья
УДК 658.7.01
https://doi.org/10.24143/2073-5537-2025-3-26-35
EDN ANDACQ

Внедрение инструментов цифровой безопасности в деятельность организаций

Александр Викторович Дмитриев

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Санкт-Петербург, Россия, dmitriev-av@ranepa.ru

Аннотация. Рассматриваются проблемы обеспечения экономической безопасности в условиях внедрения цифровых технологий в деятельность предприятий и организаций и анализируются сопутствующие этому процессу различные риски и угрозы. Исследуются основные задачи, связанные с разработкой и внедрением современных цифровых технологий и стимулированием инновационного развития организаций, с позиции активного развития цифровой экономики. Ставится 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. 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. В части выводов и рекомендаций по итогам проведенного исследования отмечено, что в целях поддержания цифровой безопасности организациям банковского сектора требуется ежегодно осуществлять мониторинг затрат на технологическую и инновационную трансформацию, при необходимости увеличивать и направлять их на внедрение передовых цифровых продуктов и технологий в свою работу.

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

Для цитирования: *Дмитриев А. В.* Внедрение инструментов цифровой безопасности в деятельность организаций // Вестник Астраханского государственного технического университета. Серия: Экономика. 2025. № 3. С. 26–35. https://doi.org/10.24143/2073-5537-2025-3-26-35. EDN ANDACQ.

Original article

Digital security tools implementation in the activities of organizations

Alexander V. Dmitriev

The Russian Presidential Academy of National Economy and Public Administration,
Saint Petersburg, Russia, dmitriev-av@ranepa.ru

Abstract. The problems of ensuring economic security in the context of the introduction of digital technologies into the activities of enterprises and organizations are considered and various risks and threats accompanying this process are analyzed. The main tasks related to the development and implementation of modern digital technologies and stimulating the innovative development of organizations are studied from the perspective of the active development of the digital economy. The emphasis is placed on the fact that currently the issues of studying the effects of the digital economy and ways to neutralize its risks and threats are being considered not only at the state level, but also at the level of individual business entities. The necessity of introducing digital economy tools at the micro level is substantiated from the point of view of increasing the competitiveness of enterprises and organizations, which makes it possible to increase the speed of customer service, increase the efficiency of the product distribution process and provide 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 of 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 integrated security of an economic entity, which, in addition, includes personnel, information, technical and technological, legal, environmental and other types security. The essence and content of modern digital risks and threats are investigated, and their systematization is carried out according to a number of classification criteria, including the type of risk, the level of occurrence, the likelihood of risk, the rate of risk increase, the duration of exposure, and the degree of loss from exposure to risk. Attention is paid to the specifics of using the digital security tools of organizations. In terms of the conclusions and recommendations based on the results of the study, it was noted that in order to maintain digital security, banking sector organizations need to monitor the costs of technological and innovative transformation annually, if necessary, increase and direct them to the introduction of advanced digital products and technologies in their work.

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

For citation: Dmitriev A. V. Digital security tools implementation in the activities of organizations. *Vestnik of Astrakhan State Technical University. Series: Economics*. 2025;3:26-35. (In Russ.). https://doi.org/10.24143/2073-5537-2025-3-26-35. EDN ANDACQ.

Введение

В соответствии со «Стратегией экономической безопасности Российской Федерации на период до 2030 года» 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 РФ 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].

Материалы исследования

Сегодня цифровая экономика занимает особое 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 из факторов укрепления и обеспечения экономической безопасности предприятий и организаций и входит в подсистему их цифровой безопасности, являю-

щейся неотъемлемым элементом комплексной безопасности хозяйствующего субъекта наряду с кадровой, информационной, технико-технологической, правовой, экологической и другими видами безопасности [3].

Существует довольно много подходов к трактовке термина «цифровая безопасность», которые связаны с рассмотрением ее в качестве объективной реальности, позволяющей найти пути инновационного развития организации [4], фактора повышения эффективности деятельности организации за счет более полного и широкого применения возможностей различных методов и технологий обработки экономической информации [5], современного инструментария, позволяющего эффективно управлять множеством процессов в экономике [6]. Кроме того, вопросам использования цифровых технологий с целью обеспечения экономической безопасности предприятий и организаций также посвящен целый ряд научных исследований.

Работы [7, 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 множеством положительных последствий для экономической деятельности, сопровождается целым рядом вызовов и угроз, достаточно серьезно влияющих на ход экономических процессов. Исследователи подчеркивают, что цифровизацию, с одной стороны, можно рассматривать как трансформацию любой информации в цифровой формат, предполагающий в дальнейшем эффективное использование данных, представленных в цифровой форме, с другой стороны, цифровая форма порождает набор новых вызовов, угроз, отрицательных последствий и рисков, определяющих необходимость совершенствования системы кибербезопасности предприятий.

В статье [10] 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, а также 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 IT-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 [11].

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 [12].

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.

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. 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 рис. 1.

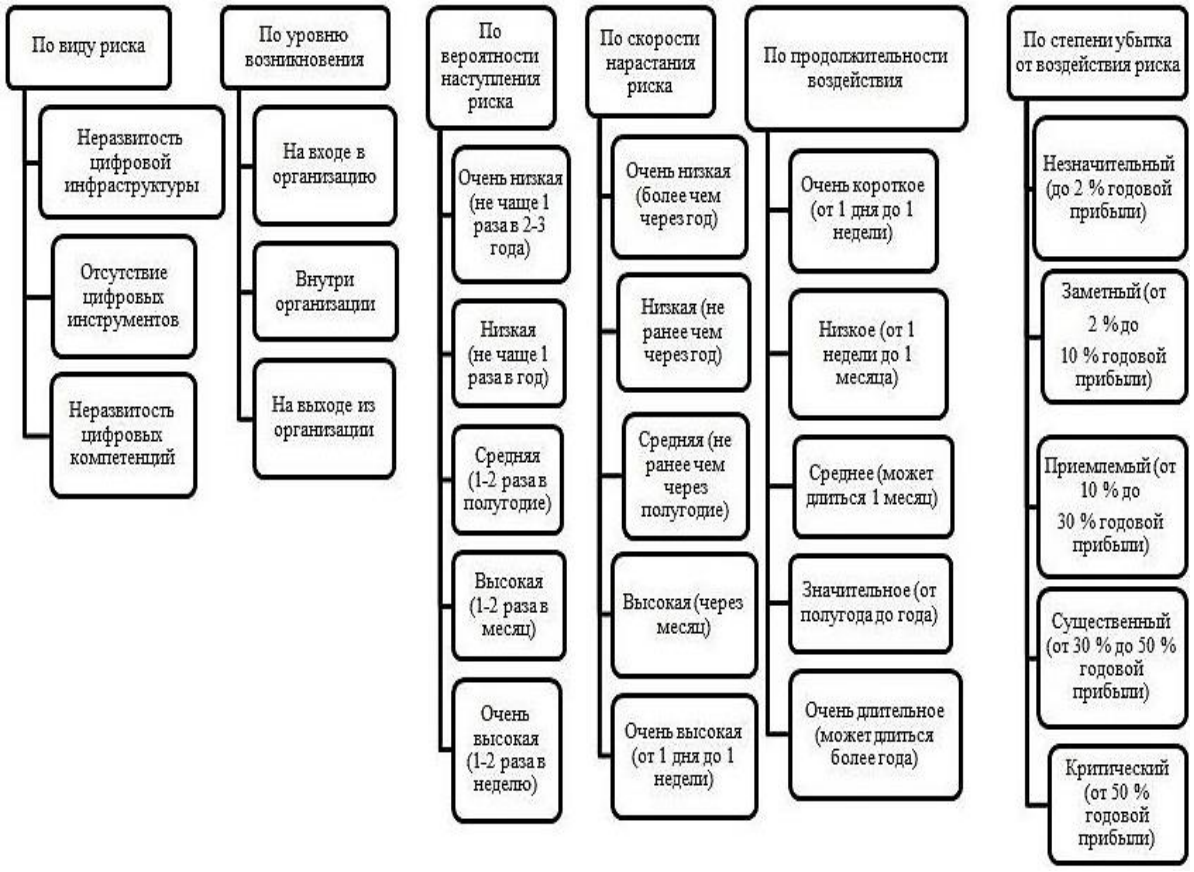

Рис. 1. Классификация рисков при внедрении цифровых технологий [13]

Fig. 1. Classification of risks in the implementation of digital technologies [13]

Очевидно, что при внедрении цифровых технологий следует уделить большее внимание именно 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.

Кроме того, 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.

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 сотрудников, 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.

Учитывая вышеизложенное, можно отметить, что нейтрализация угроз цифровой экономики и обеспечение цифровой безопасности предприятия определяется взаимодействием целого ряда составляющих: инновационная, технико-технологическая, кадровая, кибербезопасность.

Основой для внедрения новых технологий и инноваций является IT-инфраструктура. 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).

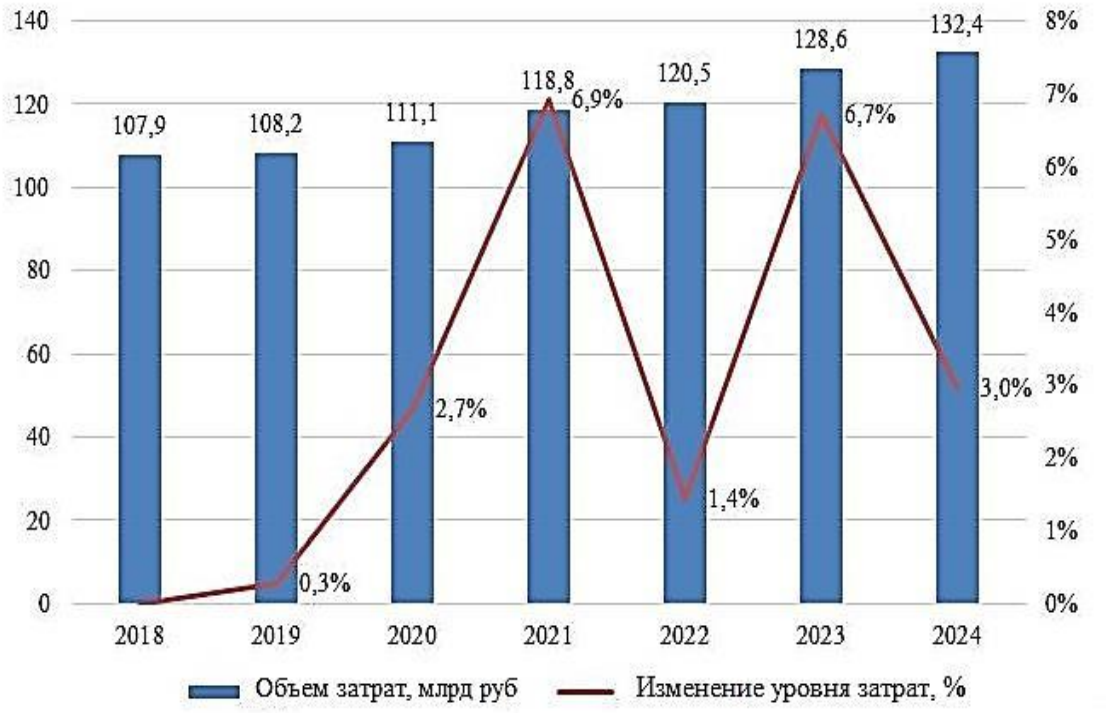

Рис. 2. Затраты ПАО «Сбербанк» на технологическую трансформацию [14]

Fig. 2. Costs of Sberbank PJSC for technological transformation [14]

Результаты исследования подтверждают, 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 и цифровые платформы. Продолжение работы с использованием иностранных технологий несет в себе определенные риски для управления и технического обслуживания систем. На рис. 3 представлена схема вендорозамещения на всех уровнях технологического стека в следующем порядке: область замещения – вендоры, прекратившие сотрудничество с ПАО «Сбербанк» – замещающие решения.

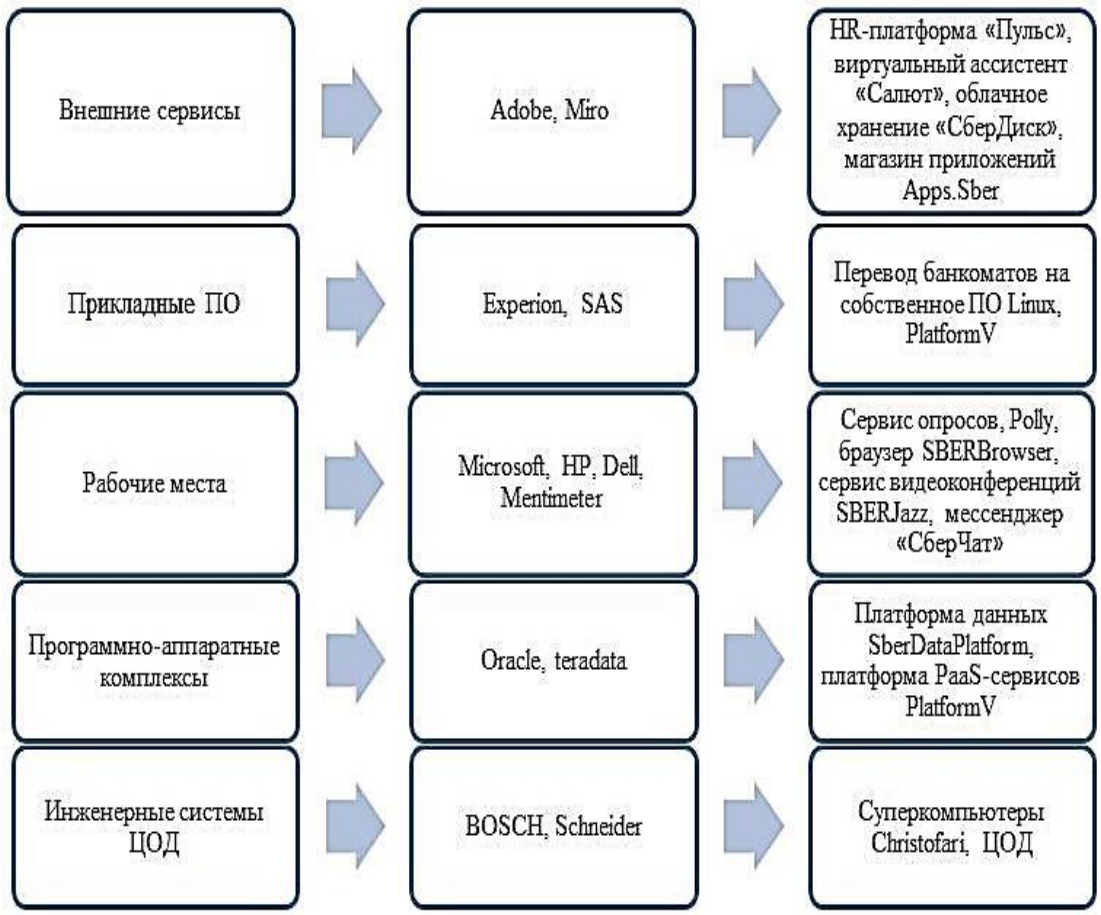

Рис. 3. Вендорозамещение в ПАО «Сбербанк» [8]

Fig. 3. Vendor substitution in Sberbank PJSC [8]

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 программного обеспечения, в том числе в части программно-аппаратных комплексов и инженерных систем центра обмена данными (ЦОД).

Безусловно, не все процессы, продукты и программы удалось перевести на отечественные разработки, но организация смогла 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 увеличивается. 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).

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 рис. 5 представлена динамика по количеству крупных DDoS-атак.

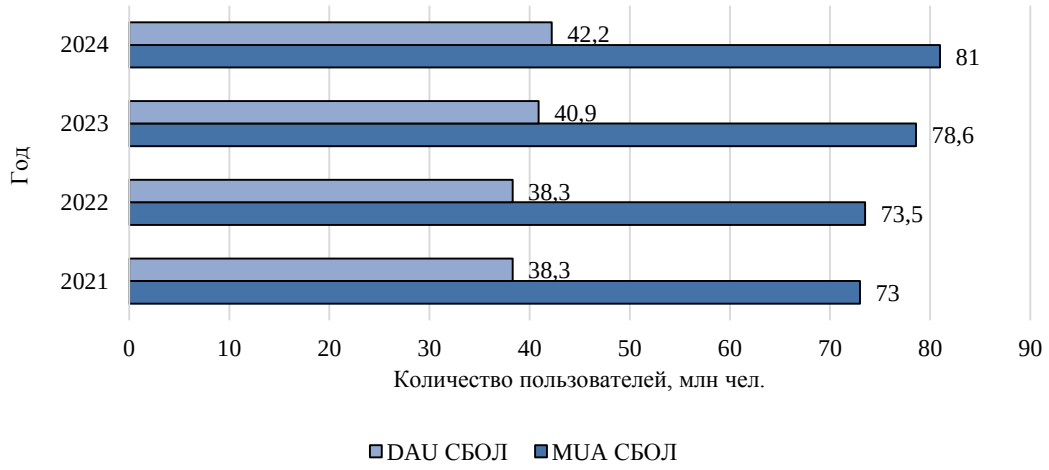

Рис. 4. Количество пользователей мобильного приложения «Сбербанк Онлайн» [14]

Fig. 4. The number of users of the Sberbank Online mobile application [14]

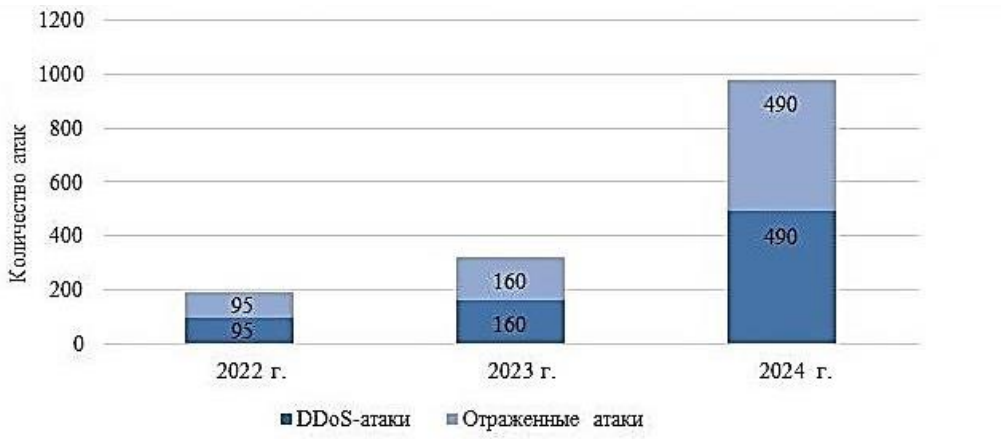

Рис. 5. Динамика совершенных и отраженных крупных DDoS-атак на ПАО «Сбербанк» [15]

Fig. 5. Dynamics of committed and reflected major DDoS attacks on Sberbank PJSC [15]

Согласно данным 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 ч 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.

Большой вклад в обеспечение информационной безопасности и кибербезопасности вносят IT-специалисты. Внедрение новых технологических решений, отражение кибератак, бесперебойная работа банковских сервисов – все это было бы невозможным без квалифицированных кадров в IT-индустрии. В данном случае затрагивается аспект кадровой составляющей как одной из частей обеспечения цифровой безопасности. Сегодня в ПАО «Сбербанк» открыто более 1 тыс. вакансий на должности специалистов по информационной безопасности, аналитиков данных, дата-сайентистов, программистов, разработчиков и других специальностей из сферы информационных технологий.

Таким образом, проведенное исследование подтвердило 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 этого, 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 эквай-

ринга 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 о том, 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 в последствии ухода в банк-конкурент.

Выводы

1. Для обеспечения инновационной безопасности организаций, в том числе банковского сектора, для поддержания 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 программное обеспечение / облачные сервисы собственной разработки. Так организация минимизирует будущие риски, связанные с техническим обслуживанием западного оборудования и новыми поставками. На замену западным технологиям пришли новые продукты, например собственные разработки ПАО «Сбербанк»: SBERBrowser, сервис видеоконференций SBERJazz, мессенджер «СберЧат».

3. В результате анализа деятельности крупной банковской структуры 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 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 уровень не только цифровой безопасности, но и экономической безопасности организации в целом.

Список источников

1. Дмитриев А. В. Методологические основы управления логистикой транспортно-складских центров // Изв. Санкт-Петербург. ун-та экономики и финансов. 2012. № 6 (78). С. 76–81.

2. Дмитриев А. В. Диджитализация транспортной логистики. СПб.: Изд-во СПбГЭУ, 2018. 161 с.

3. Дмитриев А. В., Щербаков В. В. Обеспечение экономической безопасности и устойчивости цепей поставок в условиях цифровизации // Вестн. фак. упр. Санкт-Петербург. гос. экон. ун-та. 2023. № 15. С. 11–18.

4. Алетдинова А. А., Аренков И. А., Афанасьева Р. Р. и др. Цифровая трансформация экономики и промышленности: проблемы и перспективы. СПб.: Изд-во СПбПУ Петра Великого, 2017. 807 с. DOI 10.18720/IEP/2017.4.

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

6. Соболева Ю. П., Мосина Д. А. Цифровая трансформация бизнес-процессов // Экономика и бизнес: цифровая трансформация и перспективы развития: материалы Междунар. науч.-практ. конф.: в 2-х т. (Москва, 14 апреля 2022 г.). М.: Изд-во Ин-та бизнеса и дизайна, 2022. Т. 1. С. 203–208.

7. Свадковский В. А. Применение цифровых двойников для повышения операционной эффективности предприятий добывающих отраслей // Стратег. решения и риск-менеджмент. 2023. № 14 (3). С. 292–311. DOI 10.17747/2618-947X-2023-3-292-311.

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

9. Халин В. Г., Чернова Г. В. Цифровизация и киберриски // Управлен. консультирование. 2023. № 7. С. 28–41. https://doi.org/10.22394/1726-1139-2023-7-28-41.

10. Шабаева С. В., Шабаев А. И. Инструменты реализации стратегий в условиях цифровой трансформации промышленных предприятий // Управлен. консультирова-

ние. 2023. № 10. С. 69–79. https://doi.org/10.22394/1726-1139-2023-10-69-79.

11. Плотников В. А., Погодина В. В., Смирнов А. А. Национальная экономическая безопасность и государственная политика развития промышленности // Управлен. консультирование. 2023. № 9. С. 35–44. https://doi.org/10.22394/1726-1139-2023-9-35-44.

12. Чернышева Г. Н., Лавренова Г. А., Савич Ю. А., Лубянская Э. Б. Обеспечение экономической безопасности в логистике гособоронзаказа // Организатор пр-ва. 2021. № 29 (3). С. 171–184. DOI 10.36622/VSTU.2021.47.14.015.

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

14. Прогноз развития рынка кибербезопасности в Российской Федерации на 2022–2026 годы. URL: https://www.csr.ru/ru/research/ (дата обращения: 29.04.2024).

15. С начала года число DDoS-атак на Сбербанк выросло. URL: https://www.interfax.ru/spief2024/965360 (дата обращения: 24.02.2025).

References

1. Dmitriev A. V. Metodologicheskie osnovy upravleniia logistikoi transportno-skladskikh tsentrov [Methodological foundations of logistics management of transport and warehouse centers]. *Izvestiia Sankt-Peterburgskogo universiteta ekonomiki i finansov*, 2012, no. 6 (78), pp. 76-81.

2. Dmitriev A. V. *Didzhitalizatsiia transportnoi logistiki* [Digitalization of transport logistics]. Saint Petersburg, Izd-vo SPbGEU, 2018. 161 p.

3. Dmitriev A. V., Shcherbakov V. V. Obespechenie ekonomicheskoi bezopasnosti i ustoichivosti tsepei postavok v usloviiakh tsifrovizatsii [Ensuring economic security and sustainability of supply chains in the context of digitalization]. *Vestnik fakul'teta upravleniia Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta*, 2023, no. 15, pp. 11-18.

4. Aletdinova A. A., Arenkov I. A., Afanas'eva R. R. i dr. *Tsifrovaia transformatsiia ekonomiki i promyshlennosti: problemy i perspektivy* [Digital transformation of the economy and industry: problems and prospects]. Saint Petersburg, Izd-vo SPbPU Petra Velikogo, 2017. 807 p. DOI 10.18720/IEP/2017.4.

5. Shershneva A. V., Pal'chikova N. S. Transformatsiia biznesa v usloviiakh tsifrovoi ekonomiki [Business transformation in the digital economy]. *Strategiia predpriiatiia v kontekste povysheniia ego konkurentosposobnosti*, 2019, no. 8, pp. 215-219.

6. Soboleva Iu. P., Mosina D. A. Tsifrovaia transformatsiia biznes-protsessov. Ekonomika i biznes: tsifrovaia transformatsiia i perspektivy razvitiia [Digital transformation of business processes. Economics and business: digital transformation and development prospects]. *Materialy Mezhdunarodnoi nauchno-prakticheskoi konferentsii: v 2-kh tomakh (Moskva, 14 aprelia 2022 g.)*. Moscow, Izd-vo Instituta biznesa i dizaina, 2022. Vol. 1. Pp. 203-208.

7. Svadkovskii V. A. Primenenie tsifrovykh dvoinikov dlia povysheniia operatsionnoi effektivnosti predpriiatii dobyvaiushchikh otraslei [The use of digital twins to improve the operational efficiency of extractive industries]. *Strategicheskie resheniia i risk-menedzhment*, 2023, no. 14 (3), pp. 292-311. DOI 10.17747/2618-947X-2023-3-292-311.

8. Trachuk A. V., Linder N. V. Effekty tsifrovykh platform dlia promyshlennykh kompanii: empiricheskii analiz v usloviiakh vneshnego sanktsionnogo davleniia [Effects of digital platforms for industrial companies: an empirical analysis under external sanctions pressure]. *Strategicheskie resheniia i risk-menedzhment*, 2023, no. 14 (2), pp. 150-163. https://doi.org/10.17747/2618-947X-2023-2-150-163.

9. Khalin V. G., Chernova G. V. Tsifrovizatsiia i kiberriski [Digitalization and cyber risks]. *Upravlencheskoe konsul'tirovanie*, 2023, no. 7, pp. 28-41. https://doi.org/10.22394/1726-1139-2023-7-28-41.

10. Shabaeva S. V., Shabaev A. I. Instrumenty realizatsii strategii v usloviiakh tsifrovoi transformatsii promyshlennykh predpriiatii [Tools for implementing strategies in the context of digital transformation of industrial enterprises]. *Upravlencheskoe konsul'tirovanie*, 2023, no. 10, pp. 69-79. https://doi.org/10.22394/1726-1139-2023-10-69-79.

11. Plotnikov V. A., Pogodina V. V., Smirnov A. A. Natsional'naia ekonomicheskaia bezopasnost' i gosudarstvennaia politika razvitiia promyshlennosti [National economic security and State industrial development policy]. *Upravlencheskoe konsul'tirovanie*, 2023, no. 9, pp. 35-44. https://doi.org/10.22394/1726-1139-2023-9-35-44.

12. Chernysheva G. N., Lavrenova G. A., Savich Iu. A., Lubianskaia E. B. Obespechenie ekonomicheskoi bezopasnosti v logistike gosoboronzakaza [Ensuring economic security in the logistics of the state defense order]. *Organizator proizvodstva*, 2021, no. 29 (3), pp. 171-184. DOI 10.36622/VSTU.2021.47.14.015.

13. Maliukov Iu. A., Nedosekin A. O., Abdulaeva Z. I. Strategicheskoe upravlenie ekonomicheskoi ustoichivost'iu predpriiatiia v nechetko-logicheskoi paradigme [Strategic management of an enterprise's economic stability in a fuzzy-logical paradigm]. *Strategicheskie resheniia i risk-menedzhment*, 2023, no. 14 (2), pp. 136-149. https://doi.org/10.17747/2618-947X-2023-2-136-149.

14. *Prognoz razvitiia rynka kiberbezopasnosti v Rossiiskoi Federatsii na 2022–2026 gody* [Forecast of the development of the cybersecurity market in the Russian Federation for 2022-2026]. Available at: https://www.csr.ru/ru/research/ (accessed: 29.04.2024).

15. *S nachala goda chislo DDoS-atak na Sberbank vyroslo* [Since the beginning of the year, the number of DDoS attacks on Sberbank has increased]. Available at: https://www.interfax.ru/spief2024/965360 (accessed: 24.02.2025).

Статья поступила в редакцию 17.03.2025; одобрена после рецензирования 23.05.2025; принята к публикации 09.09.2025
The article was submitted 17.03.2025; approved after reviewing 23.05.2025; accepted for publication 09.09.2025

Информация об авторе / Information about the author

Александр Викторович Дмитриев – доктор экономических наук, доцент; заведующий кафедрой безопасности; Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации; dmitriev-av@ranepa.ru

Alexander V. Dmitriev – Doctor of Economic Sciences, Assistant Professor; Head of the Department of Security; The Russian Presidential Academy of National Economy and Public Administration; dmitriev-av@ranepa.ru