

Научный журнал «Менеджер». 2025. № 7(113). С. 4-14.

Scientific Journal "Manager". 2025;(7/113):4-14.

Современный менеджмент: проблемы теории и практики

Научная статья

УДК 332.146.2:004.9

JEL: R11, R58

<https://doi.org/10.5281/zenodo.17412400>

РИСКИ ВНЕДРЕНИЯ МЕХАНИЗМОВ ИНФРАСТРУКТУРНОЙ ТРАНСФОРМАЦИИ И ЦИФРОВИЗАЦИИ РЕГИОНОВ

Екатерина Юрьевна Афендикова

Донецкая академия управления и государственной службы, Донецк, ДНР, Россия,

ekaterina-mamchenko@yandex.ru, <https://orcid.org/0000-0001-9371-4851>

Аннотация. Главной целью работы является анализ и выявление рисков внедрения механизмов инфраструктурной трансформации и цифровизации регионов. Анализ нормативно-правовой базы показал, что высокоразвитые государства активно внедряют и регламентируют процессы цифровизации и инфраструктурной трансформации, тем самым придавая данной тенденции всеобщность и глобальность. Было установлено, что инфраструктурная модернизация и цифровизация регионов имеют как положительные, так и отрицательные черты, возможности и перспективы инновационного развития, а также угрозы, свойственные для данных процессов. Статистическое исследование показало, что киберугрозы приобретают всё более массовый характер и становятся тенденцией развития цифрового пространства в государствах. Также были выявлены и другие риски, свойственные для данных процессов и предложены рациональные методы для управления данными рисками.

Ключевые слова: цифровая инфраструктура, цифровизация, киберриски, киберугрозы

Финансирование: исследование выполнено в рамках фундаментальной научно-исследовательской работы «Методологические и организационные процессы формирования финансовой системы», регистрационный номер НИОКТР 124012900537-2.

Для цитирования: Афендикова Е. Ю. Риски внедрения механизмов инфраструктурной трансформации и цифровизации регионов // Научный журнал «Менеджер». 2025. № 7(113). С. 4-14. <https://doi.org/10.5281/zenodo.17412400>.

Original article

RISKS OF IMPLEMENTING MECHANISMS FOR INFRASTRUCTURAL TRANSFORMATION AND DIGITALIZATION OF REGIONS

Ekaterina Yu. Afendikova

Donetsk Academy of Management and Public Administration, Donetsk, DPR, Russia,
ekaterina-mamchenko@yandex.ru, <https://orcid.org/0000-0001-9371-4851>

Abstract. The main goal of this work is to analyze and identify the risks associated with the implementation of mechanisms for infrastructural transformation and digitalization of regions. The analysis of the regulatory framework has shown that highly developed countries are actively implementing and regulating digitalization and infrastructural transformation processes, thereby giving this trend universality and globality. It was established that infrastructural modernization and digitalization of regions have both positive and negative aspects, opportunities and prospects for innovative development, as well as threats inherent to these processes. Statistical research has shown that cyber threats are becoming increasingly widespread and are becoming a development trend in the digital space of states. Other risks inherent to these processes were also identified, and rational methods for managing these risks were proposed.

Keywords: digital infrastructure, digitalization, cyber risks, cyber threats

Funding: the research was carried out within the framework of the fundamental scientific research work "Methodological and Organizational Processes of Financial System Formation", R&D registration number 124012900537-2.

For citation: Afendikova E. Yu. Risks of implementing mechanisms for infrastructural transformation and digitalization of regions // Scientific Journal "Manager". 2025;(7/113):4-14. (In Russ.), <https://doi.org/10.5281/zenodo.17412400>.

Введение

В период научно-технологической революции наблюдается экспоненциальный рост возможностей цифровых и информационно-компьютерных технологий, сопровождающийся инфраструктурной и цифровой трансформацией в жизни современного общества. Как отмечают некоторые исследователи, в период цифровой и инфраструктурной трансформации жизнь человека становится проще, поскольку некоторая часть работ возлагается на силы искусственного интеллекта и компьютерных вычислений, а качество и доступность оказываемых услуг возрастает.

Помимо упрощения жизни человека, научно-технологический прогресс порождает новые формы общественного производства и новые инновационные экономические системы, основанные на инновациях и рациональном использовании знаний, производстве высокотехнологической и наукоёмкой продукции, а также сфере услуг.

Актуальность изучаемой темы заключается во всеобъемлемости и стремительности интеграции процессов инфраструктурной и цифровой трансформации, касающихся всех уровней инновационной экономической системы, включая региональные экономические системы. В большинстве передовых государств наблюдается комплексный переход на новый уровень общественного производства – инновационную экономику, основанную на инновациях и производстве инновационных продуктов, поскольку цифровая трансформация – это ключевая цель инновационной политики высокоразвитых государств, потому что цифровая трансформация повышает конкурентоспособность конечной продукции и снижает диспропорции регионов

в технологическом и экономическом развитии, а инфраструктурные преобразования повысят доступность к оказываемым услугам.

Однако, несмотря на положительные стороны, свойственные для данных процессов, имеют место отрицательные черты данных процессов и моменты с наличием риска, требующие внимания и управления при осуществлении цифровой и инфраструктурной трансформации на всех её этапах, включая внедрение механизмов цифровой трансформации на региональном уровне.

Объектом исследования являются риски внедрения механизмов инфраструктурной трансформации и цифровизации регионов.

Предметом исследования выступают особенности проявления рисками, обусловленные новыми реалиями в эпоху цифровой и инфраструктурной трансформации инновационных экономических систем на региональном уровне, а также закономерности возникновения и механизмы управления выявленными рисками.

Цель и задачи исследования

Целью настоящего исследования считается выявление рисков, свойственных для периода цифровой и инфраструктурной трансформации инновационных экономических систем на региональном уровне, предложение инновационных методов для внедрения в региональную систему риск-ориентированного управления.

Задачами исследования считаются теоретическое исследование цифровизации и инфраструктурной трансформации, в т. ч. их характеристика, анализ нормативно-правовой базы цифровизации и инфраструктурной трансформации в России и в зарубежных странах, выявление наиболее и наименее дигитализованных государств в мире и регионов в Российской Федерации, выявление рисков, связанных с данными процессами и предложение методов по управлению приведенными рисками.

Методы исследования

В научной работе использовались такие методы исследования, как анализ и синтез, индукция и дедукция; эмпирические методы, такие как статистический анализ, сравнительный анализ как статистического, так и нормативно-правового материала, SWOT-анализ внедрения механизмов инфраструктурной и цифровой трансформации.

Результаты исследования и их обсуждение

Экспоненциальный и стремительный научно-технический прогресс порождает новые вызовы и тенденции общемирового развития, заставляя приспосабливаться к изменениям общество и сферы его жизни. Приспособление и внедрение инноваций также касается и инфраструктуры, на которой базируется современное общество. Всеобъемлющая цифровая трансформация затрагивает и финансовую сферу: активно развиваются инновационные финансовые технологии, такие как криптовалюты, блокчейн-технологии, безфилиальные виртуальные финансово-кредитные организации и т. д. Цифровая инфраструктура является необходимым элементом инновационной цифровой экономики, построенной на новшествах и производстве наукоёмкой продукции. При этом единой трактовки данной категории нет. Так, в работе [1] цифровая инфраструктура в рамках регионального инновационного развития представляет собой комплекс технологий и продуктов, основанных на них, обеспечивающих вычислительные, телекоммуникационные и сетевые мощности, функционирующих на цифровой основе. В учебном пособии за авторством Ю. И. Грибанова и М. Н. Руденко понятие цифровой инфраструктуры определяется как система взаимосвязанных баз данных и технических средств для взаимодействия с ними [2], а в учебном пособии за авторством А. С. Нечаева и Ю. Н. Барыкиной [3] категория «цифровая инфраструктура» трактуется как совокупность средств вычислительной техники, телекоммуникационного оборудования, каналов передачи данных и информационных систем, средств коммутации и управления информационными потоками, а также

организационных структур, правовых и нормативных механизмов, обеспечивающих их эффективное функционирование.

Таким образом, можно дать авторское определение данной категории как совокупность технологий и продуктов, основанных на цифровых инновационных системах, обеспечивающих цифровые вычислительные, сетевые и телекоммуникационные мощности, а также взаимосвязь между базами данных и техническими средствами для взаимодействия с данными системами.

К инфраструктуре цифровой экономики следует предъявлять требования, удовлетворяющие духу международных инновационных тенденций в мире. К таким требованиям следует отнести операционную совместимость всех инновационных элементов цифровой инфраструктуры; безопасность; конфиденциальность данных пользователей цифрового пространства; целостность инновационной цифровой инфраструктуры; доступность для максимально возможного количества пользователей; помехоустойчивость инновационных цифровых систем; эффективность функционирования как цифровой инфраструктуры в целом, так и отдельных её элементов; быстрота выхода на рынок, включая мировой; совмещение единообразия и разнообразия цифровых продуктов.

К ключевым элементам цифровой инфраструктуры можно отнести такие компоненты, которые её составляют [1]:

ИТ-инфраструктура региона формируется на основе комплекса технических и программных решений, включающих в себя вычислительные системы, телекоммуникационное оборудование и специализированное программное обеспечение. Основу технологического стека составляют современные цифровые инструменты, обеспечивающие бесперебойную работу информационных систем и защиту данных. Важнейшую роль в функционировании этой экосистемы играет профессиональный персонал, который не только обслуживает инновационные технологии, но и предоставляет экспертную поддержку в использовании цифровых ресурсов. Материальная составляющая данной системы представлена физическим оборудованием, специализированными инструментами и расходными материалами, которые формируют фундамент для развития цифровой экономики региона. Все эти компоненты работают слаженно, обеспечивая надёжность и стабильность функционирования экономической системы в целом;

платформы и экосистемы – данные средства предоставляют возможность эффективного управления ресурсами за счёт усиления автоматизации экономических процессов в хозяйственной деятельности региональных субъектов инновационной экономической системы, создавать инновационную технологическую базу для обеспечения сетевой коммуникации и организации хозяйственной деятельности, привлекать к кооперации независимых субъектов экономической системы региона. Платформа может выступить как определённая группа или совокупность технологий, т. е. выступить как «пакет» цифровых инновационных технологий, и как предприятие, а также в других формах.

Цифровая экосистема представляет собой комплексную технологическую платформу, которая объединяет множество участников цифрового рынка в единую сеть взаимодействия.

Эта система создаёт благоприятные условия для развития разнообразных товаров и услуг, находящихся в тесной взаимосвязи друг с другом. Ключевой особенностью такой экосистемы является возможность совместного использования технологической инфраструктуры и ресурсов различных организаций.

Участники цифрового пространства получают доступ к общей платформе, где могут эффективно взаимодействовать между собой, обмениваться данными и оптимизировать

свои бизнес-процессы. Благодаря такому подходу достигается синергетический эффект, способствующий динамичному развитию всего цифрового рынка.

Электросвязь – она же сетевая связь: подразделяется на локально-вычислительные, территориально распределённые, беспроводные сети и структурированную кабельную систему передачи данных. Представлена в виде высокоскоростных сетей электросвязи последующих поколений, предоставляющие конечному пользователю в любом месте широкополосный доступ к неограниченному спектру услуг и иных благ электросвязи и информационно-коммуникационные технологии, например, сеть «Интернет».

Центры обработки и хранения данных подразделяются на центры обработки данных и на центры обработки и хранения данных. Формирование этих центров обусловлено увеличением количества данных и информации, которую следует обработать и хранить, и предназначены для оптимизации управления и решения реальных задач. С развитием ЦОД (центры обработки данных) и ЦХОД (центры хранения и обработки данных) представляется возможность создавать многофункциональные центры обработки данных, происходит усложнение и уплотнение корпоративных ЦОД. Появление гипермасштабируемых ЦОД, ЦОД по принципу «колокейшн» и пограничных ЦОД является предпосылкой для появления более сложных ИТ-систем, развития более сложных ЦОД для хранения и обработки больших объёмов данных.

Облачные технологии – это возможность предоставления универсального сетевого доступа к вычислительным мощностям и данным, которые обеспечивают эффективное функционирование хозяйствующего субъекта.

Правительства различных государств стремятся к внедрению инновационных технологий в национальные экономические системы, свидетельством которого можно считать принятые нормативно-правовые акты, формирующие юридическую базу инновационного развития. Так, например, в Российской Федерации таковыми считаются Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы», Распоряжение Правительства России от 28 июля 2017 г. № 1632-р, Указ Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», Федеральный закон от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации», Постановление Правительства РФ от 2 марта 2019 г. № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации», Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», Распоряжение Правительства РФ от 26 февраля 2021 г. № 431-р «Об утверждении Концепции цифровой и функциональной трансформации социальной сферы, относящейся к сфере деятельности Министерства труда и социальной защиты Российской Федерации, на период до 2025 года», Распоряжение Правительства РФ от 20 мая 2023 г. № 1315-р «Концепция технологического развития на период до 2030 года» [3].

В США таковыми считаются Федеральный закон о цифровой подписи и электронной идентификации от 1998 г. (Digital Signature and Electronic Authentication Law), Федеральный закон о реформе безопасности в сфере правительственной информации от 2000 г. (Government Information Security Reform Act), Федеральный закон об электронном правительстве от 2002 г. (The E-Government Act of 2002), Федеральный закон о финансовых инновациях и технологиях для XXI века от 2024 г. (Financial Innovation and Technology for the 21st Century Act), Федеральный закон о руководстве и создании

национальной инновационной системы для стабильных криптовалют от 2025 г. (Guiding and Establishing National Innovation for U.S. Stablecoins Act) [13].

В Китае приняты такие нормативно-правовые акты, регулирующие цифровую трансформацию, как Государственная программа «Сделано в Китае 2025», принятая в 2015 году; Закон Китайской Народной Республики о сетевой безопасности от 1 июня 2017 года, Закон КНР об электронной торговле от 31 августа 2018 года, Положение о защите безопасности критической информационной инфраструктуры от 27 апреля 2021 года, Регламент по управлению алгоритмическими рекомендациями в информационных сервисах в интернете от 01 марта 2022 года, Положение об администрировании информационных интернет-сервисов глубокого синтеза информации в интернете от 10 января 2023 года [8].

Таким образом, можно заключить, что цифровая трансформация региональных экономических систем и самой инновационной экономической системы государства в целом – это общемировая тенденция, свойственная как для высокоразвитых государств, так и развивающихся.

В таблице 1 представлен SWOT-анализ внедрения механизмов инфраструктурной трансформации и цифровизации регионов.

Таблица 1 – SWOT-анализ внедрения механизмов инфраструктурной трансформации и цифровизации регионов

Table 1 – SWOT analysis of the implementation of mechanisms for infrastructural transformation and digitalization of regions

Сильные стороны: повышение качества жизни населения; увеличение конкурентоспособности экономик регионов и государства в целом; увеличение продолжительности жизни населения; повышение доступности оказываемых услуг государством	Слабые стороны: переток сельских жителей в высокоурбанизированные города; ресурсоёмкость инфраструктурной и цифровой модернизации; интернет-зависимость субъектов инновационной экономики; необходимость постоянной модернизации
Возможности: перспективные разработки в области генеративного ИИ; переход на квантовые вычислительные мощности в инновационных экономических системах; разработка энергоэффективных компьютерных систем; разработка новых источников энергии	Угрозы: риск кадрового дефицита; снижение значимости сельской местности в государстве; новые виды мошенничества в цифровом пространстве; снижение конфиденциальности среди отдельных представителей населения и повышенная уязвимость граждан к атакам киберпреступников

Исходя из содержания таблицы, можно заключить, что внедрение механизмов инфраструктурной трансформации и цифровизации регионов обладает как рядом преимуществ, так и рядом недостатков, а также угроз, порождающих новые виды риска. На рисунке 1 представлены типовые риски внедрения механизмов инфраструктурной трансформации и цифровизации регионов.

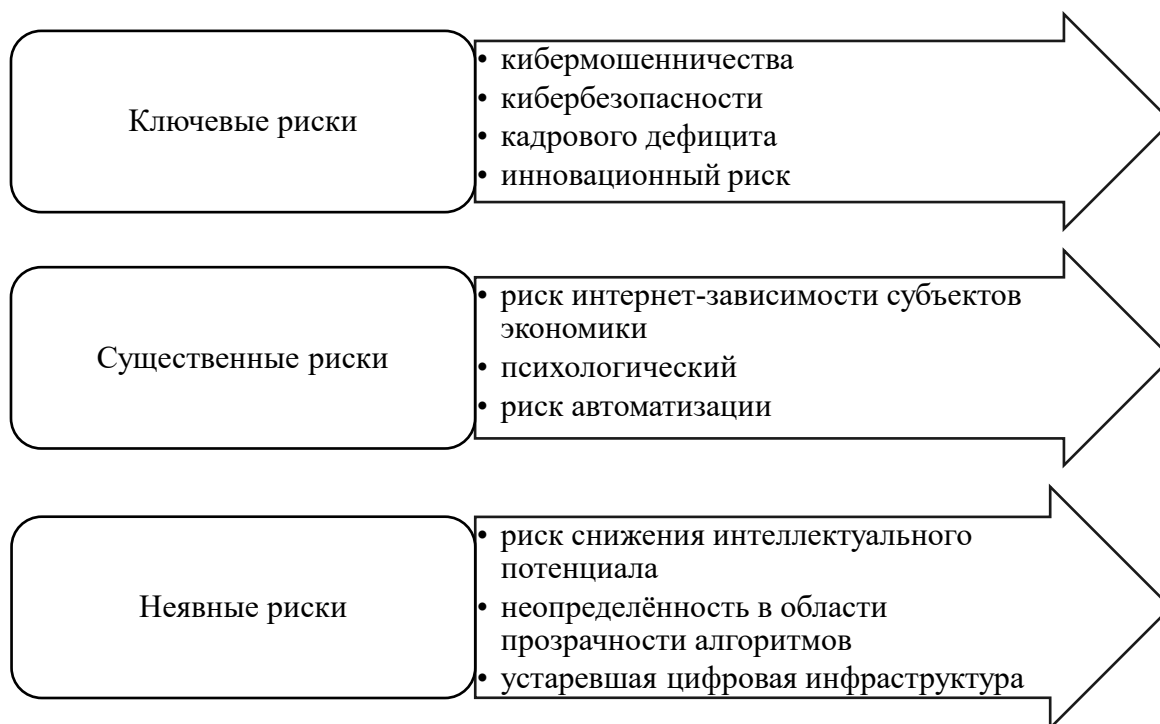


Рисунок 1 – Перечень рисков, свойственных для внедрения механизмов инфраструктурной трансформации и цифровизации регионов

Figure 1 – List of risks inherent in the implementation of mechanisms for infrastructural transformation and digitalization of regions

Исходя из содержания рисунка 1, к ключевым рискам внедрения механизмов инфраструктурной трансформации можно отнести:

риск кибермошенничества – обусловлен распространением цифрового мошенничества в различных формах, как правило, в форме вымогательства, кражи конфиденциальных данных под определённым предлогом и т. п.;

риск кибербезопасности – обусловлен возможностью утечек баз данных субъектов региональной экономики, а также возможностью наступления отказа в обслуживании юридических и физических лиц субъектами цифровой экономической системы в ходе кибератак;

риск кадрового дефицита – обусловлен снижением рождаемости в регионах, ввиду повышения качества оказываемых медицинских услуг и урбанизации государства, перехода на новый индустриальный уклад;

инновационный риск – обусловлен стремительностью технологического развития инновационных экономических систем. Рисковое событие реализуется в случае технологического разрыва между субъектами экономики.

К значимым рискам можно отнести такие риски:

риск интернет-зависимости инфраструктуры – обусловлен реализацией рискового события в случае «паралича» экономической системы, возникшего из-за неполадок и сбоев интернет-соединения или полного отключения субъектов экономики от сети «Интернет»;

психологический риск – обусловлен наличием в цифровом пространстве навязчивой рекламы; материалов, представляющих психологическую угрозу населению; развитием клипового мышления у физических лиц, характеризующийся моментальным, фрагментарным, поверхностным и линейным мышлением, возникающими трудностями в усвоении нового материала;

риск автоматизации – обусловлен стремительным развитием искусственного интеллекта и робототехники, которые заместят низкоквалифицированную рабочую силу в инновационной экономической системе.

К неявным рискам внедрения механизмов инфраструктурной трансформации можно отнести:

риск снижения интеллектуального потенциала – обусловлен снижением когнитивных способностей населения, ввиду распространения автоматизации сложных процессов, их упрощением, отказом общества от решения интеллектуальных задач и т. д.

Некоторые отрицательные тенденции, приведённые выше, можно наблюдать через статистический анализ. Так, анализируя риски кибербезопасности и кибермошенничества [4-12], будет уместно привести потери от кибермошенников в России и в США за последние пять лет (рисунок 2).

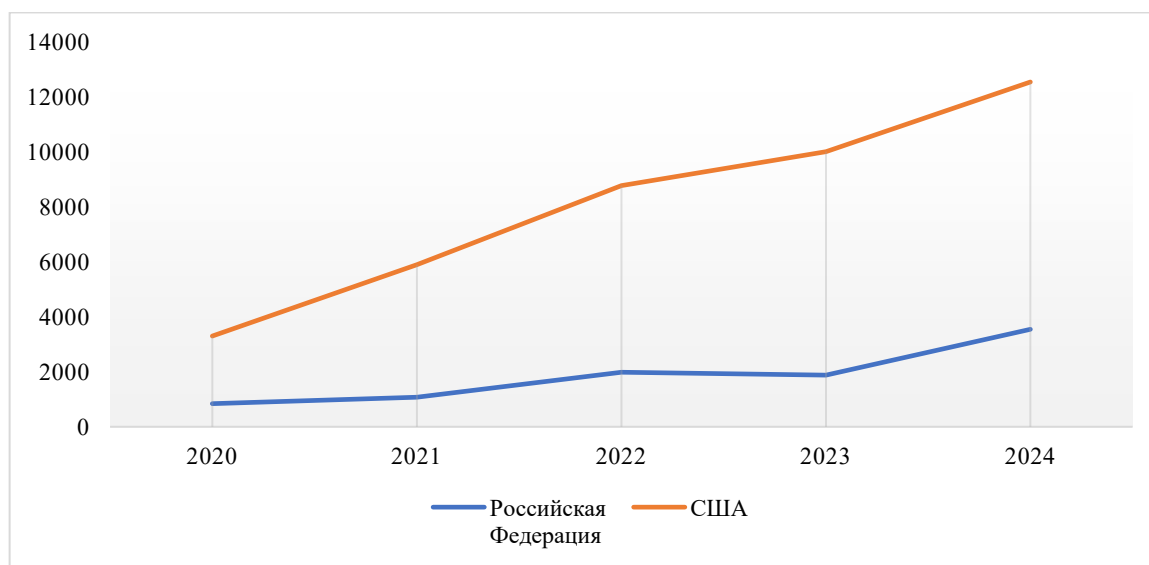


Рисунок 2 – Сравнительный анализ денежных потерь домохозяйств и предприятий от действий киберпреступников в период 2020-2024 гг., млн долл. США

Figure 2 – Comparative analysis of monetary losses of households and enterprises from the actions of cybercriminals in the period 2020-2024, million US dollars

Исходя из проведенного анализа, можно заключить, что в среднем потери от кибермошенничества в США превышают показатели потерь в России в среднем на 550,10 %. Показатель за 2024 год превысил объём потерь на 253,77 %, за 2023 – на 433,60 %, за 2022 – 342,31 %, за 2021 год – 445,10 %, за 2020 год – 292,24 %. Это можно обосновать густонаселённостью государства и высоким уровнем цифровизации в обществе. Если сравнивать показатели потерь в РФ, то показатели окажутся меньше на 84,61 %, поскольку страна менее населённая, но при этом не все процессы были подвержены цифровизации, а наблюдаемый всплеск кибермошенничества в 2022-2023 гг. пришёлся на годы проведения Россией специальной военной операции на Украине.

Что касается потерь фирм от утечек баз данных, то можно привести сравнение суммарных потерь от утечки базы данных в мире за 2023 и 2024 гг., представленное на рисунке 3. Согласно данным издания IBM, общая величина потерь от утечек баз данных в мире в 2024 г. составила 4,88 млн долл. США, что на 9,66 % больше, чем в предыдущем году – 4,45 млн долл. США [13].

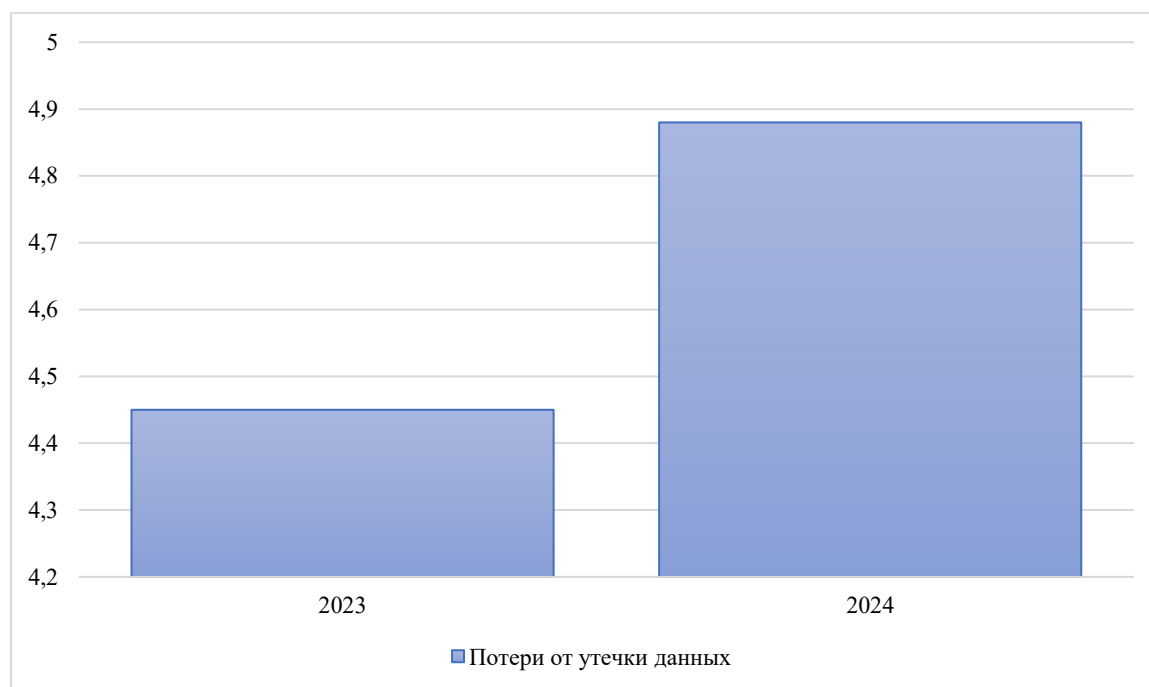


Рисунок 3 – Сравнительный анализ величины финансовых потерь фирм от утечек баз данных в мире, млн долл. США

Figure 3 – Comparative analysis of the magnitude of financial losses of firms from database leaks in the world, million US dollars

Исходя из проведенного сравнительного анализа, можно заключить, что тенденция финансовых потерь в мире положительна, и величина финансовых потерь в среднем возросла на 9,66 %.

Исходя из вышеописанного, можно предложить для решения проблем и управления рисками цифровизации и инфраструктурной трансформации внедрение искусственного интеллекта для определения паттернов поведения с целью выявления мошенничества и дальнейшей блокировки злоумышленника. Для решения рисков кибербезопасности можно предложить внедрение инновационного шифрования с целью обезопасить данные пользователей от утечек баз данных. Для решения проблем повышенного оттока сельского населения в города в результате инфраструктурной модернизации можно предложить трансформацию сельской местности в «города-сады» с развитой инфраструктурой и широкой автономностью, совмещающая в себе черты как города, так и сельской местности, что способствует ликвидации и технологического неравенства городской и сельской местности.

Для решения проблемы инновационного риска необходимо проведение НИОКР в области критических технологий. Для решения проблемы риска интернет-зависимости инфраструктуры можно предложить инновационные системы обеспечения широкополосного доступа к критическим сервисам в период чрезвычайных событий (p2p-сети, mesh-сети).

Для решения проблем демографического риска в условиях цифровой и инфраструктурной трансформации можно предложить реформу налога на доходы физических лиц. Налог на доход физических лиц будет разделяться на III класса, где ставка остаётся прогрессивной, но граждане в зависимости от своего положения будут платить по повышенной или пониженной налоговой ставке, где плательщики, т. е. семейные пары, будут ранжироваться по классам, где I класс – холостяки, II класс – один иждивенец, III класс – два и более иждивенцев.

Выводы

В ходе исследования было установлено, что цифровизация регионов, государств и инфраструктурная трансформация представляет собой основополагающую стратегию инновационного развития в ключевых субъектах международной экономики. Проведенный нормативно-правовой анализ показал, что Российская Федерация, Китайская Народная Республика и Соединённые Штаты Америки станут драйверами международной инфраструктурной трансформации и цифровизации регионов. Анализ проблематики показал, что данные процессы имеют как положительные черты, такие как повышение качества жизни населения; увеличение конкурентоспособности экономик регионов и государства в целом; увеличение продолжительности жизни населения; повышение доступности оказываемых услуг государством, так и отрицательные, такие как снижение рождаемости населения ввиду повышения оказания медицинских услуг, переток сельских жителей в высокоурбанизированные города, ресурсоёмкость инфраструктурной и цифровой модернизации, интернет-зависимость субъектов инновационной экономики, необходимость постоянной модернизации.

Были выявлены возможности и перспективные вектора развития, такие как перспективные разработки в области генеративного ИИ, переход на квантовые вычислительные мощности в инновационных экономических системах, разработка энергоэффективных компьютерных систем, разработка новых источников энергии. Среди угроз следует выделить риск кадрового дефицита, снижение значимости сельской местности в государстве, новые виды мошенничества в цифровом пространстве, снижение конфиденциальности среди отдельных представителей населения и повышенная уязвимость граждан к атакам киберпреступников.

В исследовании были выявлены ключевые, значимые и неявные риски, такие как риск кибермошенничества, риск кибербезопасности, риск кадрового дефицита и т. д. Предложены меры по управлению данными рисками.

Список источников / References

1. Батов Г. Х. Состояние и перспективы развития инфраструктуры цифровой экономики Северо-Кавказского федерального округа // Информационное общество. 2020. № 2. С. 30-38. EDN: LRLBFV.

Batov G. H. The state and prospects of development of the digital economy infrastructure of the North Caucasus Federal District // Information Society. 2020. No. 2. P. 30-38. EDN: LRLBFV. (In Russian)

2. Грибанов Ю. И. Цифровая трансформация бизнеса: учебное пособие. 2-е изд. Москва: Дашков и К, 2021. 213 с. ISBN 978-5-394-04192-1. URL: <https://e.lanbook.com/book/174008>.

Gribanov Yu. I. Digital transformation of business: a textbook. 2nd ed. Moscow: Dashkov and K, 2021. 213 p. ISBN 978-5-394-04192-1. URL: <https://e.lanbook.com/book/174008>. (In Russian)

3. Нечаев А. С. Цифровые финансовые технологии: учебное пособие для. Санкт-Петербург: Лань, 2025. 152 с. ISBN 978-5-507-51634-6. URL: <https://e.lanbook.com/book/455696>.

Nechaev A. S. Digital financial technologies: a textbook for. Saint Petersburg: Lan, 2025. 152 p. ISBN 978-5-507-51634-6. URL: <https://e.lanbook.com/book/455696>. (In Russian)

4. Почти 300 млрд рублей были украдены кибермошенниками у россиян за 2024 год / Андрей Кучеров. Санкт-Петербург: Коммерсантъ, 2025. URL: <https://www.kommersant.ru/doc/7808075?ysclid=mfcpmgvp7y746850106>.

Almost 300 billion rubles were stolen by cybercriminals from Russians in 2024 / Andrey Kuchеров. Saint Petersburg: Kommersant, 2025. URL: <https://www.kommersant.ru/doc/7808075?ysclid=mfcpgmvp7y766850106>. (In Russian)

5. Колокольцев оценил ущерб от киберпреступлений за 2023 год / РИА Новости. Москва, 2024. URL: <https://ria.ru/20240514/kiberprestupleniya-1945888975.html?ysclid=mfcpgu5iis598564081>.

Kolokol'tsev estimated the damage from cybercrimes in 2023 / RIA Novosti. Moscow, 2024. URL: <https://ria.ru/20240514/kiberprestupleniya-1945888975.html?ysclid=mfcpgu5iis598564081>. (In Russian)

6. В Сбере заявили о росте кибератак на бизнес / Лента.ру. Москва, 2022. URL: <https://lenta.ru/news/2022/11/10/kiberataki/?ysclid=mfcptzice1636538701>.

Sberbank announced an increase in cyber-attacks on businesses / Lenta.ru. Moscow, 2022. URL: <https://lenta.ru/news/2022/11/10/kiberataki/?ysclid=mfcptzice1636538701>. (In Russian)

7. Эксперт оценил ущерб от киберпреступлений в России в 2021 году / РИА Новости. Москва, 2021. URL: <https://ria.ru/20211222/kiberprestupleniya-1764832102.html?ysclid=mfcq64cf74933417265>.

An expert assessed the damage caused by cybercrimes in Russia in 2021 / RIA Novosti. Moscow, 2021. URL: <https://ria.ru/20211222/kiberprestupleniya-1764832102.html?ysclid=mfcq64cf74933417265>. (In Russian)

8. CSN Annual Data Book 2024 / Consumer Sentinel Network. Federal Trade Commission, 2025. URL: https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf.

9. CSN Annual Data Book 2023 / Consumer Sentinel Network. Federal Trade Commission, 2024. URL: https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf.

10. CSN Annual Data Book 2022 / Consumer Sentinel Network. Federal Trade Commission, 2023. URL: https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf.

11. CSN Annual Data Book 2021 / Consumer Sentinel Network. Federal Trade Commission, 2022. URL: https://www.ftc.gov/system/files/ftc_gov/pdf/CSN+Annual+Data+Book+2021+Final+PDF.pdf.

12. New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020 / Federal Trade Commission, 2021. URL: <https://www.ftc.gov/news-events/news/press-releases/2021/02/new-data-shows-ftc-received-22-million-fraud-reports-consumers-2020.pdf>.

13. Cost of a Data Breach Report / IBM, 2024. URL: <https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf>.

Информация об авторе

Е. Ю. Афендикова – канд. экон. наук, доцент, доцент кафедры финансов.

Information about the author

E. Yu. Afendikova – Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Finance.

Автор заявляет об отсутствии конфликта интересов.

The author declares no conflicts of interests.

Статья поступила в редакцию 11.09.2025; одобрена после рецензирования 23.09.2025; принята к публикации 24.09.2025.

The article was submitted 11.09.2025; approved after reviewing 23.09.2025; accepted for publication 24.09.2025.