

Научная статья

УДК 338.2:004

<https://doi.org/10.36511/2588-0071-2024-3-120-130>

Влияние рисков цифровизации на обеспечение экономической безопасности региона

Васильчук Андрей Степанович

Российский университет кооперации, Мытищи, Россия, workvasilchuk@gmail.com

Аннотация

В статье рассматриваются вопросы влияния рисков цифровизации на обеспечение экономической безопасности регионов. Актуальность темы исследования обусловлена изменениями трендов развития экономических отношений, связанных с цифровизацией экономики. В статье отмечается, что выявление рисков и угроз позволяет разработать процедуры минимизации рисков, составить тактические и стратегические планы, ориентированные на предотвращение рисков и угроз (*Mitigation*), второй этап предусматривает мероприятия и процедуры, если рискованная ситуация уже наступила и необходимо ликвидировать последствия или минимизировать потери от наступления рискованного случая (*Contingency*). Особое внимание в статье уделено классификации типов и видов рисков цифровизации. На основании проведенных исследований выделены основные типы рисков: риски использования туманных и облачных технологий; риски мошенничества и нарушения конфиденциальности информации; риски технологического отставания, распределенные по подгруппам: программные и аппаратные. Отмечается, что совершенствование процедур цифровизации повышает удобство расчетов и качество жизни, позволяет оптимизировать процессы в деятельности как хозяйствующих субъектов, так и граждан, одновременно оказывает существенное влияние на экономическую безопасность юридических и физических лиц в связи с высоким уровнем риска. В заключение приведены примеры минимизации рисков цифровизации и предложены инструменты и механизмы минимизации рисков.

Ключевые слова: экономическая безопасность, цифровизация, цифровая трансформация, риски цифровизации, цифровые технологии, криптокастодиан

Для цитирования

Васильчук А. С. Влияние рисков цифровизации на обеспечение экономической безопасности региона // На страже экономики. 2024. № 3 (30). С. 120–130. <https://doi.org/10.36511/2588-0071-2024-3-120-130>.

Original article

The impact of digitalization risks on ensuring the economic security of the region

Andrey S. Vasilchuk

Russian University of Cooperation, Mytishchi, Russian Federation,
workvasilchuk@gmail.com

© Васильчук А. С., 2024

Abstract

The article discusses the impact of digitalization risks on ensuring the economic security of regions. The relevance of the research topic is due to changes in the trends in the development of economic relations related to the digitalization of the economy. The article notes that the identification of risks and threats makes it possible to develop risk minimization procedures, draw up tactical and strategic plans focused on the prevention of risks and threats (“Mitigation”), the second stage - providing for measures and procedures if a risky situation has already occurred and it is necessary to eliminate the consequences or minimize losses from the occurrence of a risky event (“Contingency”). Special attention is paid to the classification of types and types of risks of digitalization. Based on the conducted research, the main types of risks are identified: the risks of using foggy and cloud technologies; the risks of fraud and violation of information confidentiality; the risks of technological lag, distributed by sub-groups: software and hardware. It is noted that the improvement of digitalization procedures increases the convenience of calculations and the quality of life, allows you to optimize the processes in the activities of both legal entities and individuals, at the same time, has a significant impact on the economic security of legal entities and individuals, due to the high level of risk. In conclusion, examples of minimizing the risks of digitalization are given and tools and mechanisms for minimizing risks are proposed.

Keywords: economic security, digitalization, digital transformation, risks of digitalization, digital technologies, cryptocastodian

For citation

Vasilchuk A. S. The impact of digitalization risks on ensuring the economic security of the region. *The Economy under Guard*, 2024, no. 3 (30), pp. 120–130. (In Russ.). <https://doi.org/10.36511/2588-0071-2024-3-120-130>.

Изменение трендов развития экономических отношений в последние десятилетия сопряжено с цифровизацией экономики. Внедрение интернета и мобильной связи повлекло за собой развитие цифровой экономики (*Digital economy*). Наибольший удельный вес услуг, связанных с продвижением цифровых технологий, сопряжен с расширением спектра финансовых услуг (онлайн – банкинг / интернет-банкинг) и других банковских услуг, с получением и выдачей кредитов, страхованием, инвестициями и т. д.), что позволило распространить применение цифровых технологий в жизнедеятельности физических и юридических лиц.

С целью обеспечения экономической безопасности региона необходимо выявить угрозы и риски, которые могут оказать влияние на безопасность граждан и юридических структур, связанных со всеми видами деятельности, в том числе цифровизацией. Выявление рисков и угроз позволяет разработать процедуры минимизации рисков, составить тактические и стратегические планы, ориентированные на предотвращение рисков и угроз (в экономической литературе этот этап представлен термином *Mitigation* (смягчение)). Если проблема или рисковый случай наступили (в экономической литературе описывают как *Contingency* (наступившая проблема / наступивший рисковый случай)), то возникает необходимость минимизировать потери и ликвидировать последствия.

Риски цифровизации и их влияние на развитие региональных экономических политик связывают в первую очередь с основными трендами, которые являются одновременно сквозными цифровыми технологиями: в национальной программе

«Цифровая экономика Российской Федерации» [1, 2], в частности *Big Data*, квантовые технологии, технологии виртуальной и дополненной реальностей, нейротехнологии и искусственный интеллект, технологии беспроводной связи, системы распределенного реестра, промышленный интернет, новые производственные технологии, компоненты робототехники и сенсорики.

Совершенствование процедур цифровизации повышает удобство расчетов и качество жизни, позволяет оптимизировать процессы в деятельности как юридических, так и физических лиц, одновременно оказывая существенное влияние на их экономическую безопасность в связи с высокой степенью риска. Анализ экономической литературы [3–14] показывает, что при описании цифровых технологий наиболее часто обращают внимание на высокий уровень риска утечки информации и законодательных ограничений, которые могут быть связаны в том числе с санкционной политикой. В данном случае необходим мониторинг рисков и угроз, связанных с цифровизацией, и классификация рисков (рис. 1). Например, в связи с восьмым пакетом санкций Европейского союза введены ограничения (запреты) на операции с криптовалютой и обслуживание криптокошельков граждан и резидентов Российской Федерации. С целью минимизации уровня риска по данному вопросу в Экспертном совете при рабочей группе по законодательному регулированию криптовалюты и майнинга Государственной Думы Российской Федерации были разработаны меры, направленные на снижение уровня риска по вопросам регулирования операций с криптовалютой. В деловой оборот введена новая дефиниция «криптокастодиан» – это новый субъект государственного регулирования, связанный с хранением цифровых активов и криптовалют как частного вида цифровых активов.

Важной проблемой внедрения в оборот цифровых валют является проблема хранения цифровых валют и соблюдение требований законодательства. Высокие риски хранения криптовалют на иностранных площадках влекут за собой необходимость предоставления российским гражданам сервиса хранения криптовалют. Предоставление альтернативных площадок российским гражданам, а также предоставление возможности осуществлять свою деятельность по хранению криптовалют операторам цифровых торговых платформ при соблюдении требований законодательства Российской Федерации будет направлено на обеспечение экономической безопасности финансовых средств граждан Российской Федерации и позволит предоставить аналогичные сервисы владельцам криптовалют в Российской Федерации [2]. Риски, связанные с цифровизацией, описывают в экономической литературе как связанные с увеличением безработицы, технологическим отставанием в программных продуктах и информационных технологиях, увеличением уровня мошеннических схем, разглашением персональных данных, ограничением получения любых видов информационных услуг, включая государственные услуги, только при наличии сети «Интернет» и т. д.

Как показывают проведенные исследования, сокращение численности рабочих мест при выполнении работ и оказании услуг в ручном режиме повлекло за собой создание большого количества дополнительных рабочих мест, связанных с расширением информационных сервисов, развитием цифровых услуг и значительным увеличением объемов производства и реализации товаров, работ и

услуг, связанных с расширением возможностей распространения информации, в том числе рекламы и электронных торговых площадок.

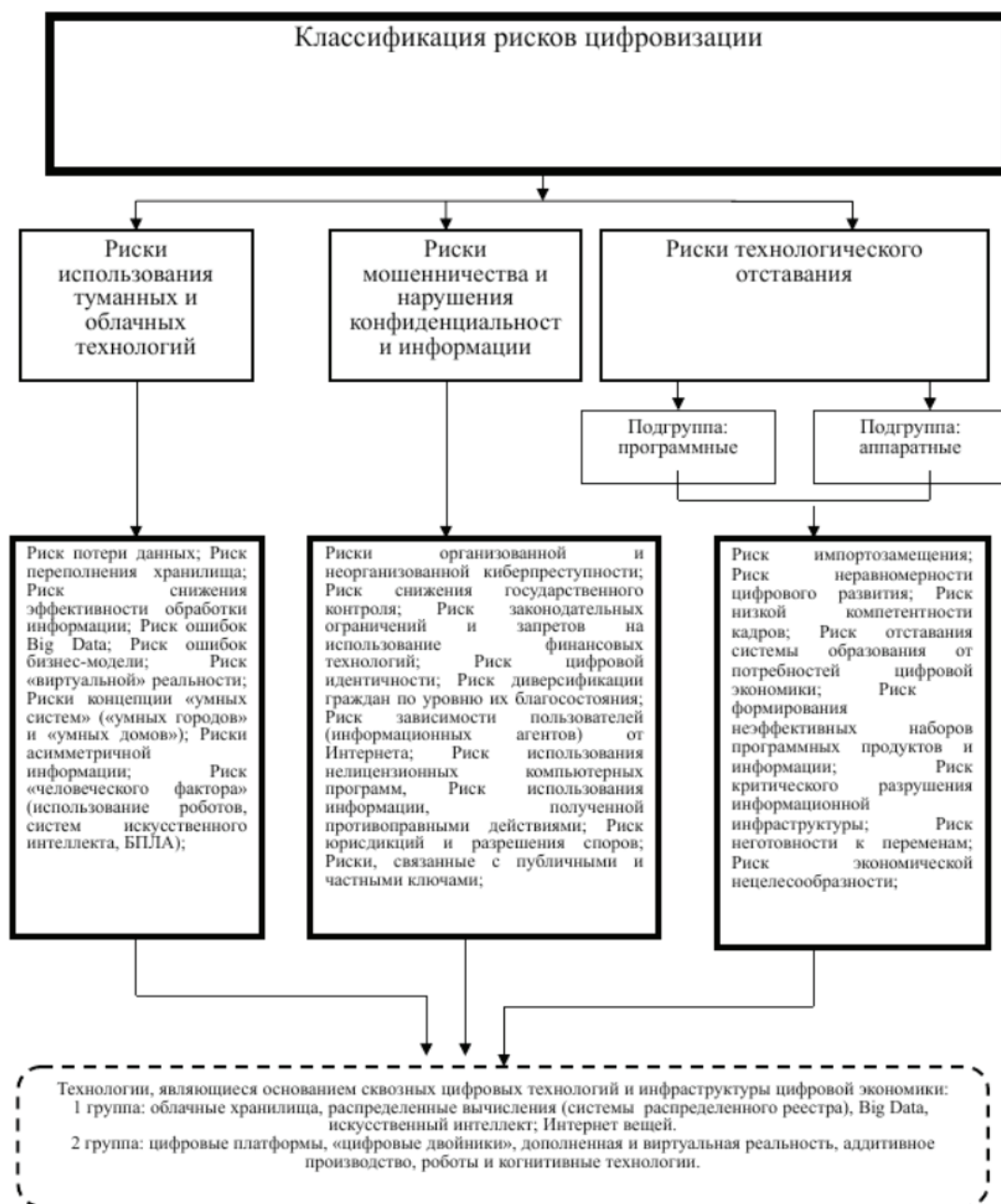


Рис. 1. Структурно-видовая схема классификации рисков цифровизации

Fig. 1. Structural and specific scheme for classifying digitalization risks

Составлено: [6, 10, 11, 13, 15–17]

Риски, связанные с технологическим отставанием в программных продуктах и информационных технологиях, можно разделить их на две группы:

— первая группа – риски, связанные с программными продуктами и созданием программного обеспечения;

— вторая группа – риски, связанные с аппаратной составляющей процесса цифровизации.

Первая группа рисков технологического отставания в программных продуктах, связанная с проблемами в создании софта, не относится к группе с высоким уровнем риска, так как российские разработчики-программисты являются высококвалифицированными специалистами.

Правительство Российской Федерации приняло ряд мер, направленных на минимизацию риска недостатка квалифицированных кадров в сфере ИТ-индустрии. Министерство цифрового развития, связи и массовых коммуникаций (далее — Минцифры России) совместно с Министерством обороны Российской Федерации (далее — Минобороны России) предусмотрело разработку образовательных программ («Цифровые профессии», «Готов к цифре», CDO) и осуществляет подготовку ИТ-специалистов. По состоянию на 2023 год более 343 тысяч человек приняты на обучение по образовательным программам высшего образования в сфере информационных технологий за счет средств федерального бюджета (с нарастающим итогом с 2019 года) (в том числе в 2022 году — 117 тысяч человек) [5]. Подготовку осуществляют 800 российских высших учебных заведений, что составляет более 60 % учебных заведений высшего образования Российской Федерации, включая филиалы. К 2024 году на обучение планируется принять не менее 500 тысяч человек [5].

Важным этапом выполнения программ обучения специалистов для ИТ-индустрии можно назвать проект «Цифровые кафедры», согласно которому к 2025 году квалификации ИТ-специалистов должны получить 385 тысяч человек, а к 2030 году — 900 тысяч человек.

Развитие программных технологий также связано с требованиями Федерального закона от 5 апреля 2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», который регулирует импортозамещение в сфере программного обеспечения в Российской Федерации, согласно которому участники контрактной системы должны обеспечивать использование отечественного программного обеспечения в целях осуществления государственных и муниципальных закупок. Введение ограничения на привлечение импортного программного обеспечения позволило акцентировать важность и актуальность разработки отечественной системы программного обеспечения [2].

Высокий уровень риска имеет подгруппа, связанная с техническим обеспечением процедур информатизации. Импортозамещение, связанное с антироссийскими санкциями, приводит к тому, что возникает необходимость привлечения долгосрочных и существенных инвестиций в разработку аппаратных комплексов. Высокая степень риска обусловлена тем, что процедуры научно-исследовательских разработок предполагают типовые этапы (идея — прототип — испытания — тестирование и моделирование в различных условиях эксплуатации).

По мнению специалистов, продвижение ИТ-технологий будет тесно связано с интернет-торговлей (IoT). По прогнозам международных экспертов, в 2023 году между собой могут взаимодействовать более 50 триллионов устройств — от бытового оборудования и смартфонов до станков, автономного транспорта и производственных роботов [14].

Импортозамещение необходимо не только для аппаратной составляющей ИТ-технологий (компьютеры, датчики, сенсоры и т. д.), но и для инфраструктуры (сети и системы), которая может обеспечить передачу больших объемов данных. Лидерами в этой области в настоящее время являются Китайская Народная Республика (КНР), Республика Корея.

Способами минимизации рисков в аппаратной области называют преодоление в технологическом отставании за счет информационных технологий и облачных сервисов [14].

Риски, связанные с увеличением мошеннических схем, имеют наибольший удельный вес в группе рисков, так как связаны с необходимостью обеспечения информационной безопасности во всех отраслях и сферах деятельности физических и юридических лиц. Мошеннические схемы получили распространение по следующим направлениям: использование нелегальных компьютерных программ, использование информации, полученной противоправными действиями (взлом электронной почты и т. д.), а также в мессенджерах, в социальных сетях, на маркетплейсах, досках объявлений и интернет-аукционах (брашинг), с платежными картами (кардинг), с банковскими счетами (интернет-банкинг), с цифровой валютой, сообщения о чрезвычайных ситуациях, социальная инженерия, телефонное мошенничество (вишинг), фишинг и другие.

В Российской Федерации введены меры ответственности за мошенничество как вид преступления в сфере компьютерной информации. В Уголовном кодексе Российской Федерации (далее — УК РФ) предусмотрен ряд статей за мошенничество в сфере компьютерной информации (например, ст. 159.6, 272, 273, 274¹ УК РФ) [18]. К преступлениям, которые связаны с информационными технологиями, относят распространение вредоносных («вирусных») программных продуктов, взлом паролей, кражу и неправомерное использование сведений о номерах банковских карт, банковских реквизитов и т. д. Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, дополнительно квалифицируется по статьям 272, 273 или 274¹ УК РФ. Отдельным видом преступлений в сфере компьютерной информации является распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и др.) [18].

Важным способом минимизации рисков с целью защиты данных является криптографическая защита данных. Для защиты средств цифровой валюты предложено дополнить законопроект о цифровом рубле требованиями к российским кастодиальным сервисам, в частности, в сфере ПОД/ФТ (дословно расшифровывается как противодействие отмыванию денег и финансированию терроризма) и безопасности, а также наделить кастодиана рядом публично-правовых функций в целях обеспечения полноценного оборота криптоактивов (взаимодействие с ФССП при необходимости наложения ареста или взыскания, хранения для государственных целей при конфискации или обеспечении удобной процедуры наследования, формирование налогооблагаемой базы) [2, 18].

Правительство Российской Федерации осуществляет последовательно продвижение цифровых валют и цифровых активов, констатируя, что использование

цифровой валюты для расчетов по внешнеторговым сделкам будет направлено на минимизацию рисков от введения антироссийских санкций, следовательно, может быть эффективным инструментом, позволяющим разработать комплекс мер для сокращения негативных последствий рестрикционной политики.

Среди наиболее важных преимуществ развития цифровизации в расчетах, включая расчеты в цифровой валюте, можно обозначить механизмы минимизации рисков, направленные: на противодействие кредитных организаций незаконным финансовым операциям [19]; возможность монетизации расходов на электроэнергию в ряде регионов и устранение дефицита электрической энергии, которая может возникать в процессе деятельности нерегулируемых майнеров [2]; снижение спроса на наличные деньги (в Швеции, Норвегии) или сокращение их использования в обозримом будущем (в Японии, Евросоюзе) [1, 2, 15, 19]; эффективность расчетов за счет снижения конвертационных и транзакционных издержек, сокращения операционных и кредитных рисков [19]; увеличение доходов бюджета за счет появления новых категорий налогоплательщиков, связанных с криптовалютами, которые выйдут из серой (теневой) экономики [2]; возможность осуществить расчеты за товары (работы, услуги) с иностранными партнерами, что позволит обойти антироссийские санкции [11].

С целью развития информатизации российской финансовой системы в настоящее время разрабатывается пакет федеральных законов, который будет связан с признанием, регулированием, контролем и минимизацией рисков цифровых финансовых активов. Согласованная позиция с субъектами государственного регулирования (Минфин России, Банк России, Росфинмониторинг, ФНС России, ФСБ России) будет предусматривать минимизацию рисков, возникающих в процессе выпуска цифровой валюты в России, в части регулирования майнинга, контролирование операций в расчетах с цифровыми активами в международных расчетах, внедрение цифрового рубля в расчетах между хозяйствующими субъектами, физическими лицами, в бюджетных расчетах [2].

Основные проблемы цифровой экономики связаны с информационными утечками и правовыми ограничениями в некоторых отраслях законодательства. Исследование проблем рисков мошенничества и нарушения конфиденциальности информации показывает, что можно выделить следующие типы и виды рисков: риск диверсификации граждан по уровню их благосостояния: в информационном поле осуществляется анализ стоимостного размера покупок граждан, проводится незаконное анкетирование о предпочтениях граждан в сфере торговли и услуг. Данные действия направлены на удовлетворение потребностей граждан в товарах и услугах более дорогих, чем предлагают физическим лицам; риск зависимости пользователей (информационных агентов) от интернета; риск законодательных ограничений и запретов на использование финансовых технологий; риск использования информации, полученной противоправными действиями; риск использования нелегальных компьютерных программ; риск снижения государственного контроля; риск цифровой идентичности; риск юрисдикций и разрешения споров; риски организованной и неорганизованной киберпреступности; риски, связанные с публичными и частными ключами.

По мнению автора, наибольшую актуальность в настоящее время приобретают риски использования технологий (туманных и облачных), которые аккумули-

руют риски и угрозы всех видов и типов цифровизации. В свою очередь, можно выделить технологии, являющиеся основанием сквозных цифровых технологий и инфраструктуры цифровой экономики: облако, распределенные вычисления (системы распределенного реестра), большие данные и искусственный интеллект; интернет-вещи [6; 20].

Во вторую по важности группу технологий входят: цифровые платформы, «цифровые двойники», дополненная и виртуальная реальность, аддитивное производство, роботы и когнитивные технологии [20].

Экономическая безопасность региона должна быть обеспечена мониторингом (точечным или на постоянной основе) программного обеспечения, строительством инфраструктуры, взаимодействием всех служб и структур, обеспечивающих оказание цифровых услуг.

По мнению автора, экономическая безопасность региона в условиях цифровизации — это комплексная, эшелонированная и многоуровневая защита (локальные сети, туманные технологии, облачные вычисления) жизнедеятельности и имущества граждан и хозяйствующих субъектов (учреждений, предприятий и организаций), выстраиваемая по заданным параметрам потребностей региона в условиях цифровых преобразований. Обеспечение экономической безопасности граждан (имущества и жизнедеятельности) и хозяйствующих субъектов средствами цифровизации носит комплексный характер. Например, с целью быстрого реагирования на различные ситуации, которые могут повлечь за собой потерю объектов (в том числе за счет хищений имущества) или урон имуществу граждан и юридических лиц (пожар, разрушение и т. д.), выявления незаконных мусорных свалок, защиты наземных, подземных и воздушных объектов от внешнего разрушительного воздействия, минимизацию рисков обеспечивают посредством системы видеонаблюдения. Как показывает практика, системы видеонаблюдения с целью обеспечения экономической безопасности региона целесообразно отстраивать на основе концепции *Fog computing* (Туманные вычисления) (данная концепция позволяет осуществлять обработку информации как локально, так и через сеть «Интернет», что может быть осуществлено в облачных сервисах или только в конечных устройствах). *Fog computing* (туманные вычисления) применяют для видеонаблюдения посредством видеокамер, средств роботизации, беспилотных летательных аппаратов и т. д.

Посредством внедрения туманных вычислений можно обеспечить защиту всего периметра объектов мониторинга и охраны, а также всей территории внутри периметра как отдельного объекта (например, завода, строительной площадки, железнодорожного узла, аэропорта, торгового центра и т. д.), так и всего региона в целом. Например, в случае хищения имущества (угона автомобиля или другого транспортного средства) системы видеонаблюдения позволяют вычислить, отследить, вести цель, сопровождать объект до момента задержания похитителей. Роботы и дроны (БПЛА) широко используются для проведения инвентаризаций как промышленных предприятий и сельскохозяйственных земель, так и для инвентаризации территорий региона, включая автомобильные и железнодорожные сети, сети электропередач и т. д. Сопровождение региональными органами власти механизмов решения проблем экономической безопасности регионов посредством различных способов и методов цифровизации позволяет

повышать экономическую безопасность региона за счет снижения влияния наступления случаев риска. Таким образом, механизм цифровизации должен быть направлен в том числе на обеспечение экономической безопасности региона, что зависит от достоверности данных и от конкретных условий, избранной тактики и разработанных стратегий цифровизации. Стратегия цифровизации региона, направленная на экономическую безопасность граждан, хозяйствующих субъектов и региональной экономики в целом, должна предусматривать анализ и прогнозирование (сценарии) развития событий, установление связи между ними. Процедуры обработки информации на основе механизма цифровизации позволяют разработать и выдать рекомендации по снижению нейтрализации случаев и событий по разным видам и уровням риска. Быстрое реагирование и ликвидация последствий рисков цифровизации позволяют провести оценку влияния рисков цифровизации на экономическую безопасность региона.

Список источников

1. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России). URL: <https://digital.gov.ru/ru/ministry/common/> (дата обращения: 09.11.2023).
2. URL: <http://aklugovoy.ru/> (дата обращения: 09.11.2023).
3. Богатырев А. В., Бардаков А. А., Бубнова О. Ю. Актуальные вопросы обеспечения экономической безопасности предприятий промышленности // Экономика и управление в машиностроении. 2023. № 4. С. 8–12.
4. Богатырев А. В., Харитонов А. О. Концепция процессного подхода к обеспечению экономической безопасности // Перспективные направления совершенствования управления органами внутренних дел в современных условиях: сборник статей по материалам международной научно-практической конференции, Нижний Новгород, 16 июня 2022 года. Нижний Новгород: Нижегородская академия МВД России, 2023. С. 10–15.
5. Чернышенко Д. До конца 2025 года «Цифровые кафедры» выпустят свыше 385 тысяч человек. URL: <http://government.ru/news/49345/> (дата обращения: 09.11.2023).
6. Калаврий Т. Ю., Гордячкова О. В. Инструменты цифровой экономики: учебное пособие. Москва: Мир науки, 2022. URL: <https://izd-mn.com/PDF/66MNNPU22.pdf> (дата обращения: 09.11.2023).
7. Минаков А. В., Суглобов А. Е. Проблемы развития цифровой экономики регионов России // Вопросы региональной экономики. 2022. № 4 (53). С. 63–72.
8. Серебрякова Т. Ю., Гордеева О. Г. Риски организации: их учет, анализ и контроль: монография. Москва: НИЦ Инфра-М. 2019. 233 с.
9. Серебрякова Т. Ю., Анисимов А. С. Методические аспекты риск-ориентированного мониторинга экономической безопасности управляющих компаний многоквартирных домов // Экономический анализ: теория и практика. 2023. Т. 22. № 3 (534). С. 521–533.
10. Шаблаков А. Д., Соловьева И. А. Оценка рисков внедрения сквозных цифровых технологий в промышленности // Вестник Южно-Уральского государственного университета. Серия: Экономика и менеджмент. 2023. Т. 17. № 2. С. 133–143.
11. Экономическая безопасность хозяйствующих субъектов: современные подходы / Н. Н. Макарова, Г. В. Тимофеева, С. В. Банк, С. А. Хмелев. Москва: Издательский Центр ПРИОР, 2022. 148 с.

12. Эскиндаров М. А., Масленников В. В., Масленников О. В. Риски и шансы цифровой экономики в России. Финансы: теория и практика. URL: <https://doi.org/10.26794/2587-5671-2019-23-5-6-17> (дата обращения: 09.11.2023).

13. Economic Security in International Cooperation: Risk Overview and Risk Management Perspectives / A. E. Suglobov, D. M. Pimenov, S. A. Hmelev [and other] // Cooperation and Sustainable Development: conference proceedings, Moscow, 15–16 декабря 2020 года. Vol. 245. Cham: Springer Nature Switzerland Publ., 2022. Pp. 1061–1067.

14. IT поможет преодолеть технологическое отставание России в аппаратной области. URL: <https://www.vnedra.ru /novosti/it-pomozhet- preodolet- tehnologicheskoe-otstavanie- rossii-v-apparatnoj-oblasti- 10828/?ysclid= lon0ldse51938563267> (дата обращения: 09.11.2023).

15. Касперская Н. «О рисках цифровизации». URL: https://dzen.ru /a/YMowT_ fdxm Sxzg2l (дата обращения: 09.11.2023).

16. Четвертая промышленная революция. Целевые ориентиры развития промышленных технологий и инноваций. URL: http://www3.weforum.org /docs/WEF _ %D0%A7 (дата обращения: 09.11.2023).

17. Одиннадцать рисков при работе с big data. URL: <https://rb.ru/opinion/data-risks/> (дата обращения: 09.11.2023).

18. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ. URL: <https://base.garant.ru/10108000/> (дата обращения: 09.11.2023).

19. Родина И. Б. Преимущества и риски цифровой национальной валюты в условиях глобальных рисков // Фундаментальные исследования. 2021. № 12. С. 186–191; URL: <https://fundamental-research.ru/ru/article/view?id=43174> (дата обращения: 09.11.2023).

20. Сергеев Л. И., Юданова Л. И. Цифровая экономика: учебник для вузов / под ред. Л. И. Сергеева. Москва: Издательство Юрайт, 2022. 332 с.

References

1. Ministry of Digital Development, Communications and Mass Media of the Russian Federation (Ministry of Finance of Russia): official website. Moscow. Updated during the day. URL: <https://digital.gov.ru/ru/ministry/common/> (accessed 19.11.2023). (In Russ.)

2. URL: <http://aklugovoy.ru/> (accessed 19.11.2023). (In Russ.)

3. Bogatyrev A. V., Bardakov A. A., Bubnova O. Y. Actual issues of ensuring economic security of industrial enterprises. Economics and Management in mechanical engineering, 2023, no. 4, pp. 8–12. (In Russ.)

4. Bogatyrev A. V., Kharitonov A. O. The concept of a process approach to ensuring economic security. Promising directions for improving the management of internal affairs bodies in modern conditions: a collection of articles based on the materials of the International Scientific and Practical Conference, Nizhny Novgorod, June 16, 2022. Nizhny Novgorod: Nizhny Novgorod Academy of the Ministry of Internal Affairs of the Russian Federation Publ., 2023. Pp. 10–15. (In Russ.)

5. Chernyshenko D. By the end of 2025, over 385 thousand people will graduate from Digital departments. URL: <http://government.ru/news/49345/> / (accessed 19.11.2023). (In Russ.)

6. Kalavry T. Yu., Gordyachkova O. V. Tools of the digital economy. Moscow: Mir nauki Publ., 2022. URL: <https://izd-mn.com/PDF/66MNNPU22.pdf> (accessed 19.11.2023). (In Russ.)

7. Minakov A. V., Suglobov A. E. Problems of development of the digital economy of the regions of Russia. *Issues of regional economics*, 2022, no 4 (53), pp. 63–72. (In Russ.)
8. Serebryakova T. Yu., Gordeeva O. G. Risks of the organization: their accounting, analysis and control: monograph. Moscow: SIC Infra-M Publ., 2019. 233 p. (In Russ.)
9. Serebryakova T. Y., Anisimov A. S. Methodological aspects of risk-based monitoring of economic security of management companies of apartment buildings. *Economic analysis: theory and practice*, 2023, vol. 22, no. 3 (534), pp. 521–533. (In Russ.)
10. Shablakov A. D., Solovyova I. A. Risk assessment of the introduction of end-to-end digital technologies in industry. *Bulletin of the South Ural State University. Series: Economics and Management*, 2023, vol. 17, no. 2, pp. 133–143. (In Russ.)
11. Economic security of economic entities: modern approaches / N. N. Makarova, G. V. Timofeeva, S. V. Bank, S. A. Khmelev. Moscow: RIOR Publ., 2022. 148 p. (In Russ.)
12. Eskindarov M. A., Maslennikov V. V., Maslennikov O. V. Risks and chances of the digital economy in Russia. *Finance: Theory and Practice*, 2019, no 23 (5), pp. 6–17. URL: <https://doi.org/10.26794/2587-5671-2019-23-5-6-17> (accessed 19.11.2023). (In Russ.)
13. Economic Security in International Cooperation: Risk Overview and Risk Management Perspectives / A. E. Suglobov, D. M. Pimenov, S. A. Hmelev [and other]. Cooperation and Sustainable Development: conference proceedings, Moscow, December 15–16, 2020. Vol. 245. Cham: Springer Nature Switzerland Publ., 2022. Pp. 1061–1067. (In Russ.)
14. IT will help to overcome Russia's technological lag in the hardware field. URL: <https://www.vnedra.ru/novosti/it-pomozhet-preodolet-tehnologicheskoe-otstavanie-rossii-v-apparatnoj-oblasti-10828/?ysclid=lon0ldse51938563267> (accessed 19.11.2023). (In Russ.)
15. Kaspersky N. On the risks of digitalization. URL: https://dzen.ru/a/YMowT_fdxmSxzg2l (accessed 19.11.2023). (In Russ.)
16. The Fourth Industrial Revolution. Targets for the development of industrial technologies and innovations. URL: <http://www3.weforum.org/docs/WEF> (accessed 19.11.2023). (In Russ.)
17. Eleven risks when working with big data. URL: <https://rb.ru/opinion/data-risks/> (accessed 19.11.2023). (In Russ.)
18. The Criminal Code of the Russian Federation no. 63-FZ of June 13, 1996. URL: <https://base.garant.ru/10108000/> (accessed 19.11.2023). (In Russ.)
19. Rodina I. B. Advantages and risks of digital national currency in the context of global risks. *Fundamental research*, 2021, no. 12, pp. 186–191. URL: <https://fundamental-research.ru/ru/article/view?id=43174> (accessed 19.11.2023). (In Russ.)
20. Sergeev L. I., Yudanov A. L. Digital economy: textbook for universities / ed. by L. I. Sergeev. Moscow: Yurait Publ., 2022. 332 p. (In Russ.)

Статья поступила в редакцию 23.06.2024; одобрена после рецензирования 05.07.2024; принята к публикации 24.09.2024.

The article was submitted 23.06.2024; approved after reviewing 05.07.2024; accepted for publication 24.09.2024.