ИССЛЕДОВАТЕЛЬСКАЯ СТАТЬЯ
https://doi.org/10.31063/AlterEconomics/2023.20-1.11
УДК 330.341
JEL O32

Концептуально-аналитические подходы к возникновению потенциальных угроз в цифровой экономике[1]

Виталий Б. КРИШТАНОСОВ [1)]✉, **Наталья А. БРОВКО** [2)]
[1)]*Белорусский государственный технологический университет, г. Минск, Республика Беларусь*
[2)]*Кыргызско-Российский Славянский университет им. Б. Н. Ельцина, г. Бишкек, Кыргызская Республика*
[1)]*https://orcid.org/0000-0002-1146-368X*
✉ *krishtanosov@mail.ru*
[2)]*https://orcid.org/0000-0003-4376-9103*

Для цитирования: Криштаносов, В. Б., Бровко, Н. А. (2023). Концептуально-аналитические подходы к возникновению потенциальных угроз в цифровой экономике. *AlterEconomics, 20*(1), 216–245. https://doi.org/10.31063/AlterEconomics/2023.20-1.11

Аннотация. Актуальность исследования обусловлена широким и системных внедрением цифровых технологий во все сфере экономической и социальной деятельности современных государств и связанными с цифровыми инновациями рисками и угрозами функционирования различных систем и институтов. Цель исследования — выделить потенциальные угрозы цифровизации, связанные с этим макроэкономические риски, а также актуальные подходы по управлению ими. Предметом исследования являются риски и угрозы цифровизации. При проведении исследования использована эволюционно-институциональная методология и системный анализ. В статье исследована трансформация концепции риска и современные подходы к оценке через призму бизнеса, социальных, экономических, инвестиционных, военных и политических угроз. Среди ключевых рисков цифровизации выделены киберриски, которые являются составляющей стратегического риска на уровне предприятий, кредитного и регуляторного рисков, оказывают влияние на рынки и формируют системный риск, генерируя вероятность разрушения элементов инфраструктуры или рынка. Отмечен системный характер рисков цифровизации, охватывающих более одной страны, более одного сектора экономики и оказывающих влияние на природные, технологические и социальные системы. Проведен анализ актуальных методов оценки рисков цифровизации (STRIDE, CIA, OCTAVE), отмечены особенности качественных и количественных методов оценки цифровых угроз. Выделены современные подходы к управлению киберрисками, включая построение моделей угроз и уязвимостей, направленных на выявление и классификацию угроз в разрезе их приоритетности, принятие мер по выборочному снижению рисков с наивысшим приоритетом в условиях ограниченности ресурсов организаций. Исследованы концепции CBDC, FinTech в разрезе генерируемых потенциальных рисков стабильности функционирования финансовой системы не только на национальном, но и международном уровне. Отмечена роль концепции E-Government в контексте потенциала для роста угроз, выделены этапы эволюции E-Government, для каждого из которых сформирован комплекс рисков ущерба в отношении различных систем государственного управления.

Ключевые слова: цифровизация, риски, e-government, методы оценки, управление рисками, киберпреступления, OCTAVE, STRIDE и CIA

[1] © Криштаносов В. Б., Бровко Н. А. Текст. 2023.

RESEARCH ARTICLE

Conceptual-Analytical Approaches to Threats in the Digital Economy

Vitaly B. KRISHTANOSOV [1)]✉, Natalya A. BROVKO [2)]

[1)] Belarusian State Technological University, Minsk, Republic of Belarus

[2)] Kyrgyz-Russian Slavic University named after the first president of Russian Federation B. N. Yeltsin, Bishkek, Kyrgyz Republic

[1)] https://orcid.org/0000-0002-1146-368X

✉ *krishtanosov@mail.ru*

[2)] https://orcid.org/0000-0003-4376-9103

For citation: Krishtanosov, V. B. & Brovko, N. A. (2023). Conceptual-Analytical Approaches to Threats in the Digital Economy. *AlterEconomics, 20*(1), 216–245. https://doi.org/10.31063/AlterEconomics/2023.20-1.11

Abstract. The study's relevance is determined by the significant impact that digitalization has on the economic and social activities of modern states, which engenders new risks and threats to the functioning of various systems and institutions. Based on the evolutionary-institutional analysis and systems analysis methods, the study identifies the threats of digitalization and the associated macroeconomic risks and describes the current approaches to digital risk management. The evolution in the understanding of risk and contemporary approaches to risk assessment is traced in relation to business, social, economic, investment, military, and political threats. Among the critical risks of digitalization, an important place is occupied by cyber risks, which are part of the strategic risks of enterprises, credit risks and regulatory risks. These risks affect markets and create a systemic risk stemming from the possible damage to elements of the infrastructure and market. Technology-driven risks have a systemic character as they may affect more than one country, economic sector, as well as a wide range of natural, technological, and social systems. The study offers an analysis of digitalization risk assessment methods (STRIDE, CIA, OCTAVE) and provides an overview of the qualitative and quantitative methods used to assess digital threats. Modern approaches to cyber risk management include modeling threats and vulnerabilities. These methods may prove especially useful to identify, classify and prioritize threats and to develop selective risk reduction measures. The concepts of FinTech and Central Bank Digital Currency (CBDC) are discussed in relation to the associated risks to the stability of national and international financial systems. The study also considers the concept of e-government, the stages of the evolution of e-government characterized by different risks to systems of public administration.

Keywords: digitalization, risks, e-government, assessment methods, risk management, cybercrime, OCTAVE, STRIDE and CIA

1. Введение

Цифровизация современной экономики является важнейшим трендом, обуславливающим ее развитие и формирование новых характеристик, особенностей всей экономической системы. Взаимодействия экономических субъектов на основе информационно-коммуникативных технологий (ИКТ) оказывают как положительное (рост производительности труда, сокращение производственных издержек, повышение качественных характеристик продукции и услуг, их кастомизация, простота масштабирования бизнес-процессов), так и разрушительное воздействие на многие отрасли, предприятия и сферы деятельности, в том числе производство, связь, торговлю, научные исследования, финансовые системы. Все это значительно увеличивает риски, связанные не только со стабильным развитием макро- и микроэкономических субъектов в цифровой экосистеме, но и их уязвимостью по причине возникновения кибератак, киберугроз национальной безопасности, и прежде всего в критической инфраструктуре. По данным отчета о Глобальных рисках

в 2022 году (WEF, 2022) отмечено, что на региональном уровне «угрозы кибербезопасности» входят в пятерку основных рисков в Восточной Азии и Тихоокеанском регионе, а также в Европе. Многие небольшие экономики с высоким уровнем цифровизации, такие как Дания, Израиль, Япония, Тайвань (Китай), Сингапур и Объединенные Арабские Эмираты, также поставили этот риск в пятерку основных опасений. Четыре страны — Австралия, Великобритания, Ирландия и Новая Зеландия — поставили его на 1 место.

Следует отметить, что концепция риска претерпела ряд трансформаций и в настоящее время «отражает ряд контекстов, включая предпринимательский, социальный, экономический, безопасности, инвестиционный, военный, политический и т. д.» (Авдийский, 2013)[1]. В.И. Авдийский добавляет: «Концепция риска возникла в XVII в. с математикой, связанной с азартными играми. Риск относится к комбинации между вероятностью и величиной потенциальных прибылей и убытков. В XVIII в. риск как концепция все еще рассматривался как выгоды, так и убытки и использовался в бизнесе морского страхования. Риск в изучении экономики возник в XIX в. Понятие риска, которое в настоящее время воспринимается более негативно, заставило предпринимателей требовать специальных стимулов для принятия риска, связанного с инвестициями. К XX в., когда речь шла о результатах риска в технике и науке, была сделана полная отрицательная коннотация, особенно в отношении опасностей, связанных с современными технологическими разработками, такими как нефтехимическая и атомная промышленность».

Риск присущ любой неавтоматизированной (т. е. требующей выбора из альтернатив) деятельности, осуществляемой в условиях неопределенности и направленной в будущее. В узком смысле, риск — вероятность возникновения убытков или недополучения доходов по сравнению с прогнозируемым вариантом[2]. В широком смысле, риски, как отмечает В.Н. Кузнецов, — «это комплекс (система) социальных, экономических, политических, духовных, техногенных и экологических явлений и процессов, разрушающим образом воздействующих на социальные организации и структуры, трансформируя их элементы и нарушая нормальное функционирование, что, в конечном счете, приводит социальные системы к упадку и распаду»[3].

Всякая система подчинена внешним условиям или факторам формирования неопределенности и рисков, ее поведение, близкое к точкам неустойчивости (бифуркации), может зависеть от поведения немногих переменных. Поскольку цифровизация является переходом на новый уровень развития экономических систем, переход к цифровой экономике и внедрение новых технологий генерирует неустойчивость к внешним угрозам и рискам. К.В. Павлов (2009) высказал гипотезу, что в переходном режиме уровень неопределенности выше, чем на старте или финише цикла. Конечную неопределенность N_k в системе отношений можно выра-

[1] Авдийский, В. И. (2013). *Риски хозяйствующих субъектов: теоретические основы, методология анализа, прогнозирования и управления*. Учебное пособие. Москва: Финансовый университет, 232.

[2] Стоянова, Е. С. (ред.) (1993). *Финансовый менеджмент: теория и практика*. Учебник. Москва: Перспектива, 74.

[3] Кузнецов, В. Н. (2009). *Мир после кризиса. Основные гуманитарные тенденции становления в XX веке концепции культуры развития человека, общества и цивилизации*. URL: https://spkurdyumov.ru/biology/mir-posle-krizisa/ (дата обращения: 24.05.2019).

зить как закон роста энтропии или как сумму меры исходной неопределенности $N_и$ и неопределенности переходного периода $N_{п.\,п.}$: $N_и + N_{п.\,п.} = N_к$. В этой связи одно из ограничений оценки рисков — асимметрия выборки анализируемых событий, характерная для неустойчивых и кризисных состояний экономических систем.

На международной практике используется стандарт ISO 31000, который характеризует риск «как влияние неопределенности на цели и выражается в виде сочетания последствий события (включая изменение обстоятельств) и связанной с этим вероятности возникновения»[1]. В зарубежной практике также известны такие стандарты управления рисками, как FERMA — стандарт Федерации европейских ассоциаций риск-менеджмента (*Federation of European Risk Management Associations*); принятая Комитетом спонсорских организаций Комиссии Тредвея (*The Committee of Sponsoring Organizations of the Treadway Commission*) интегрированная модель управления рисками COSO-ERM и COSO-II, специфика которой создание специального подразделения внутреннего контроля, уполномоченного осуществлять мониторинг и контроль за эффективностью и продуктивностью предприятий, распределением его ресурсов, финансовой отчетностью, соблюдением законов и регламентов; Basel II — методические рекомендации Банка международных расчетов (*Bank for International Settlements, BIS*) в отношении измерения достаточности капитала.

Международный совет по управлению рисками (*Information Risk Governance Committee, IRGC*) выделяет риски, имеющие системный характер и распространяющиеся на несколько государств одновременно, затрагивающие несколько отраслей экономики и влияющие на различные технологические и социальные системы[2]. Вероятность возникновения данных рисков может быть невысокой, однако они оказывают значительное негативное влияние в сфере безопасности, экономической и социальной стабильности. IRGC классифицирует ряд категорий технологических рисков, включая угрозы «неопределенного, системного и неожиданного воздействия»[3].

Рамезани, Камарина-Матос (2020) классифицирут риски эндогенного и экзогенного характера на уровне *Enterprise risk management (ERM)*. К эндогенным рискам относятся:

1) риски, связанные с организационной сетью, включая любые неопределенности, возникающие в результате взаимодействия между организациями в рамках бизнес-экосистемы;

2) риски, связанные с бизнес-процессами, такими как сбои во внутренних операциях (продукт (услуга), процесс (контроль)), материальный, финансовый и информационный потоки, а также риски, связанные с принятием решений;

3) риски, связанные с цепочкой поставок, включая риски со стороны предложения (спроса), такие как банкротство поставщика, сбои распределенных или транспортных поставщиков и т. д.;

---

[1] International Organization for Standardization (ISO) (2009). *Risk Management — Principles and Guidelines: ISO 31000*. URL: https://www.iso.org/iso-31000-risk-management.html (дата обращения: 11.04.2020).

[2] International Risk Governance Council (IRGC) (2010). *The Emergence of Risks. Contributing Factors*. URL: https://irgc.org/wp-content/uploads/2018/09/irgc_ER_final_07jan_web.pdf (дата обращения: 10.02.2020).

[3] International Risk Governance Council (IRGC) (2011). *Improving the Management of Emerging Risks. Risks from new technologies, system interactions, and foreseen or changing circumstances*. URL: https://irgc.org/wp-content/uploads/2018/09/irgc_er2conceptnote_2011.pdf (дата обращения: 10.02.2020).

4) риски, связанные с безопасностью, включая злонамеренные угрозы (преднамеренные и непреднамеренные, такие как кража, саботаж, промышленный шпионаж, кибератака и т. д., а также сбои в инфраструктуре, включая ИТ, и финансовые риски.

Экзогенные риски:

1) риски, связанные с окружающей средой в целом, которые возникают в результате взаимодействия бизнес-экосистемы с окружающей средой;

2) стихийные бедствия, такие как эпидемические заболевания, ураганы, наводнения, торнадо и т. д.;

3) социально-экономические риски, такие как политические риски (эмбарго, война, терроризм и т. д.), экономические риски (рецессия, колебания валютных курсов, высокие банковские интересы и нехватка средств и т. д.) и политические риски (регулирующие, правовые и бюрократические);

4) инфраструктурные риски, включая глобальные сбои инфраструктуры, такие как Интернет, электрические сети и т. д (Криштаносов, 2021).

2. Кибербезопасность и ее угрозы

В современной экономике большое внимание с учетом повсеместного внедрения цифровых инноваций уделяется проблеме кибербезопасности. Современные киберпреступники получили технологии, обеспечивающие возможность нанесения значительного ущерба как информационной, так и производственной сети. Если в прежних производственных укладах промышленные системы управления (*industrial control systems, ICS*) функционировали в изолированных средах, то в соответствии с функциональными требованиями ИКТ в настоящее время ICS динамично и комплексно переводятся в общедоступную сеть для обеспечения удаленного контроля и надзора за инфраструктурами. С учетом растущего внимания к преступлениям в сфере ИТ, сформировано понятие «киберпреступление», которое можно определить как «компьютерные и информационно-технологические правонарушения, которые включают несанкционированный доступ к пользовательским данным, изменение или нарушение электронных коммуникаций с использованием пользовательских данных для личной выгоды или получения финансовой выгоды» (Ali et al., 2019).

Термин «киберриск» Национальный институт стандартов и технологий США (NIST) определяет как «риск, возникающий из-за потери конфиденциальности, целостности или доступности информации или информационных систем и отражающие потенциальные неблагоприятные воздействия на деятельность организации (например, миссию, функции, имидж или репутацию), активы организации, отдельных лиц, другие организации и страну» (Hunton, 2012).

Согласно NIST (2012) главные компоненты киберриска включают:

1) угрозы — любые обстоятельства или события, которые могут оказать неблагоприятное воздействие на деятельность и активы организации, отдельных лиц, другие организации или нацию через несанкционированный доступ к информационной системе, уничтожение, разглашение или изменение информации и (или) отказ в обслуживании (*Denial of Service, DoS*);

2) уязвимости — слабость информационной системы, процедур безопасности системы, внутреннего контроля или реализации, которые могут быть использованы источником угрозы;

3) вероятность возникновения — взвешенный фактор риска, основанный на анализе вероятности того, что данная угроза способна использовать данную уязвимость (или набор уязвимостей).

Цифровизация экономики и связанные с данной тенденцией риски и угрозы могут оказывать негативное влияние на различные рынки, генерируя системные риски, имеющий потенциал каскадного распространения и разрушения целых систем или рынков. В данном контексте актуальной представляется проблематика управления рисками как на уровне государства, так и отрасли или предприятия. Действия в целях снижения уровня неопределенности и нарастания порядка в сложной системе могут осуществляться только при регулировании рисков. Общества по анализу рисков (*The Society for Risk Analysis, SRA*) предлагает следующее определение анализу рисков — «это отдельная наука, охватывающая оценку рисков, восприятие, коммуникацию, управление, руководство и политику в контексте рисков, вызывающих озабоченность отдельных лиц, организаций государственного и частного секторов и общества на местном, региональном, национальном или глобальном уровне, это применение принципов управления для идентификации, оценки, управления и передачи риска»[1]. Как отмечает Скардови: «… управление рисками включает в себя совокупность действующих лиц, правил, соглашений, процессов и механизмов, связанных с тем, как собирается, анализируется и распространяется соответствующая информация о рисках и принимаются управленческие решения. Управление рисками лежит в основе глобальной финансовой системы, работы ее международных рынков капитала, транснациональных, региональных и местных игроков, а также основных продуктов и услуг» (Scardovi, 2017). Кроме того, формирование рисковой политики является важнейшей стратегической задачей для построения системы регулирования рисков на макроуровне.

IRGC разработал модель управления рисками, которая направлена на формирование стратегий оценки и управления рисками и включает три основных этапа: предварительная оценка, окончательная оценка и управление[2].

Вместе с тем, как показал проведенный анализ, в научной литературе при оценке безопасности выделяют «два основных подхода: качественный и количественный. Количественная оценка риска — это использование измеримых, объективных данных для определения стоимости активов, вероятности потерь и связанного с ними риска (рисков). Количественные методы варьируются от ранжирования рисков, корреляций рисков, сравнительного анализа и анализа сценариев до генерации прогнозных точечных оценок, а затем до генерации прогнозных распределений (вероятностных моделей). Качественные подходы к риску, как правило, применяются к тем рискам, которые трудно определить количественно. Качественные подходы заменяют количественные значения, присваивая субъективно определенное значение, такое как высокое, среднее или низкое» (Криштаносов, 2021).

---

[1] Society for Risk Analysis (SRA) (2020). *Risk Analysis Introduction*. URL: https://www.sra.org/risk-analysis-introduction/ (дата обращения: 23.05.2020).

[2] «При оценке рисков, как правило, используется формула: (*R*): $R = T \times D$, где T — вероятность наличия опасности, а D — оценка потерь в случае повреждения системы» (International Risk Governance Council (IRGC) (2005). *White Paper on Risk Governance. Towards an Integrative Approach*. URL: https://irgc.org/wp-content/uploads/2018/09/IRGC_WP_No_1_Risk_Governance__reprinted_version_3.pdf (дата обращения: 04.06.2020)).

Мак-Кинси использует матричную сетку рисков, направленную на выявления потенциально наиболее серьезных рисков. Они затрагивают возможное негативное воздействие на организацию в целом (по вертикали) и вероятность наступления нежелательного события (по горизонтали) (Nauck, Usher et al., 2020). Boston Consulting Group для оценки рисков цифровизации предлагает использовать инструментарий «Cyber Doppler», который предполагает расчет функции, включающей частоту и влияние успешных кибератак в отношении предприятия, относительно ожидаемых киберпотерь (Wray, 2021).

Международные организации и специализированные национальные агентства в условиях динамичной цифровизации разрабатывают комплексные подходы оценки рисков, среди которых выделяют стандарты серии ISO 27000X, предполагающтие «непрерывный процесс структурированных последовательностей действий для организаций всех форм и размеров» (Aminzade, 2021). На национальном уровне NIST разработал такие методы оценки, как платформы «800–53» и «Структуру кибербезопасности» (*Cybersecurity Framework, CSF*) и рекомендует их в качестве «модели международного сотрудничества по укреплению критически важной инфраструктуры кибербезопасности» (NIST, 2020).

Национальный инфраструктурный консультативный совет при Президенте США (*The President's National Infrastructure Advisory Council, NIAC*) предложил Общую систему оценки уязвимостей (*Common Vulnerability Scoring System, CVSS*), которая предполагает разработку и внедрение механизмов открытой стандартизированной оценки уязвимостей программного продукта (Ruan, 2021).

На микроуровне получил распространение метод оценки рисков в отношении критически важных активов OCTAVE (*The Operationally Critical Threat, Asset, and Vulnerability Evaluation*, разработанный Университетом Карнеги-Меллона по заказу Министерства обороны США для планирования механизмов защиты против кибератак. Структура методологии включает ряд этапов «создание профилей угроз на основе активов; выявление уязвимостей инфраструктуры; и разработка стратегии и планов безопасности» (Криштаносов, 2021).

Гергом и Конфельдером (Microsoft) разработан метод оценки рисков — STRIDE (*Spoofing, Tampering, Repudiation, Information disclosure, Denialof Service, Elevationof Privilege*), который «классифицирует угрозы безопасности по таким категориям, как подмена, фальсификация, отказ, раскрытие информации, отказ в обслуживании, повышение привилегий» (Microsoft, 2020).

Триада CIA (*confidentiality, integrity and availability*): конфиденциальность, целостность и доступность, используется в качестве комплексной методологии идентификации угроз, классифицированных по уровню воздействия на систему по шкале как низкий, средний или высокий уровень.

В рамках проекта Всемирного экономического форума (*The World Economic Forum, WEF*) «Партнерство для киберустойчивости» (*Partnering for Cyber Resilience*) (WEF, 2012) предложена модель количественной оценки финансового воздействия киберугроз с использованием вероятности кибератак и потенциальных потерь за определенный период времени.

Ряд исследований (Pursiainen, 2018) в своих рекомендациях в отношении противодействия цифровым угрозам обосновывают необходимость отказа от управления рисками в пользу управления устойчивостью. Отмечается, что объектом управления по временной шкале должна выступать не только непосредственная

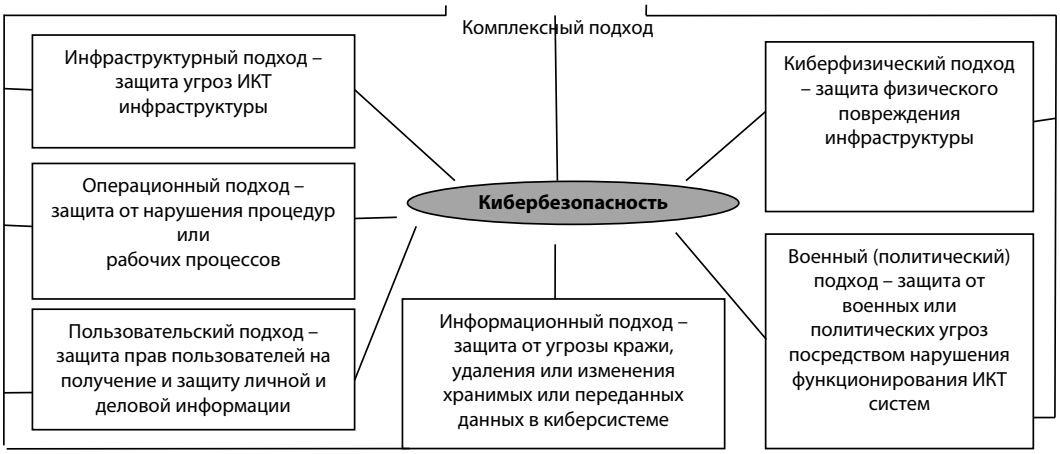

Рис. 1. *Подходы к понятию «кибербезопасность»*
Источник: разработано автором на основе (ENISA, 2015).
Fig. 1. *Approaches to the Concept of Cyber Security (compiled by the authors based on (ENISA, 2015))*

фаза кризиса, но и посткризисное обеспечение устойчивости. В рамках данного направления выделяют несколько подходов, определяющих способность восстановления устойчивости системы, включая возможность восстановления после сбоя и (или) атаки; возвращаться к новому состоянию равновесия, а также противостоять внешней атаке с последующей адаптацией и трансформацией.

В международной практике к понятию «кибербезопасность» применяются различные подходы, включая инфраструктурный, операционный, информационный, киберфизический, военный (политический). Вместе с тем, с учетом стремительного развития угроз в киберпространстве, представляется целесообразным дополнить данную классификацию комплексным и пользовательским подходами (рис. 1).

С учетом предложенных подходов к определению «кибербезопасность» возможно классифицировать законодательное регулирования данного понятия в ряде стран (табл. 1).

Таблица 1

Подходы к определению понятия «кибербезопасность»

Table 1

Approaches to the Concept of Cyber Security

Определение кибербезопасности	Страна	Подход
Информационная безопасность (кибербезопасность) — состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз	Республика Беларусь[1]	Информационно-инфраструктурный
Кибербезопасность (узкое определение) — деятельность или процесс, возможность, способность или состояние, в результате чего информационные и коммуникационные системы и информация в них содержащаяся, защищены от повреждений, несанкционированного использования или модификации	США	Информационно-инфраструктурный

Окончание табл. на след. стр.

Окончание табл. 1

Определение кибербезопасности	Страна	Подход
Кибербезопасность (широкое определение) — стратегия, политика и стандарты, касающиеся безопасности и операций в киберпространстве, и охватывающие полный спектр снижения угроз, снижения уязвимости, сдерживания, международного взаимодействия, ответного отклика, устойчивости политики и мероприятий по восстановлению, включая операции в отношении компьютерной сети, обеспечение сохранности информации, правовой ответственности, дипломатии, военных и разведывательных миссий, поскольку они относятся к безопасности и стабильности глобальной информационной и коммуникационной инфраструктуры	США	Комплексный
Кибербезопасность — означает мероприятия, необходимые для защиты сетевых и информационных систем, пользователей таких систем и других лиц, пострадавших от киберугроз	ЕС	Информационно-инфраструктурный, пользовательский
Информационная безопасность — это состояние защищенности общества и государства, отдельного гражданина от информационно-технического воздействия на информационную инфраструктуру. То есть это состояние защищенности общества от недобросовестной информации либо от ее разглашения (Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»)	РФ	Информационно-инфраструктурный, пользовательский
Защита информации (как информационная безопасность) — совокупность обязательных действий владельца информации не только по ее защите (защита от уничтожения, распространения, копирования и т. д. (ч. 1 ст. 16 Закон № 149-ФЗ)), но и реализации права на доступ к ней.	—	Операционный, пользовательский
Информационная безопасность — основа стабильности в стране, для поддержания которой необходимо предотвращать любые виды вмешательства в политическую, социальную и культурную жизнь государства. Данная стратегия подразумевает деятельность, направленную не только на обеспечение кибербезопасности страны, но и на защиту законных прав своих граждан в сети Интернет	КНР	Комплексный
Кибербезопасность предполагает защиту информационных систем (аппаратного, программного обеспечения и связанной инфраструктуры), данных о них и услуг, которые они предоставляют, от несанкционированного доступа, вреда или неправильного использования. Это включает в себя вред, причиненный умышленно оператором системы или случайно, в результате неспособности следовать процедурам безопасности	Великобритания	Информационно-инфраструктурный

[1] Концепция информационной безопасности Республики Беларусь: постановление Совета Безопасности Республики Беларусь №1 от 18 марта 2019. URL: https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf (дата обращения: 25.05.2021).

Источник: разработано автором на основе (Носов, 2021; Fuster, Jasmontaite, 2020; Добродеев, 2021)).

Как показано в таблице 1, понятие «кибербезопасность» в законодательстве отдельных стран заменяется «информационной безопасностью», при этом контекстуально они практически совпадают (в Республике Беларусь используются оба варианта как синонимы). Особенностью «информационной безопасности» является акцент на информационную защиту, с учетом ее социальной и политической значимости. По этой причине именно данное понятие используется в странах со значительным государственным регулированием (в том числе информационно-идеологической сферы), включая Республику Беларусь, Российскую Федерацию и КНР. Анализ данных таблицы показывает, что подходы к регулированию кибербезопасности в различных странах отличаются, что находит отражение в определениях данного понятия. При этом с учетом развития ИКТ и проникновениям цифровых инноваций во все сферы человеческой деятельности наиболее перспективным является именно комплексный подход, применяемый в настоящее время в США и КНР (в меньшей степени).

В этой связи представляется целесообразным использовать подход к кибербезопасности как к комплексной системной деятельности на уровне государства, и предприятий, направленной на обеспечение защиты ИКТ инфраструктуры, информации с учетом ее закрытости и возможных рисков неправомерного использования для интересов страны, юридических и физических лиц, с использованием всего спектра мероприятий и механизмов (политики, стратегии, стандартов, сертификации, регламентов и практик, международного взаимодействия) по нивелированию потенциальных угроз и рисков для национальной безопасности.

3. Макроэкономические риски цифровизации

Следует отметить, что особенностью рисков на уровне макроэкономики является их системный (с возможным перерастанием в каскадный) характер и значительный потенциал генерирования соответствующего урона для экономического развития страны, критически важных секторов и сегментов экономики, социальной и общественной сферы, ее экономической безопасности. В этой связи задачей органов государственного управления является прогнозирование соответствующих рисков при планировании имплементации цифровых инноваций (реализации цифровых концепций) для национальной экономики с целью выработки соответствующих решений, направленных на нивелирование (минимизацию) цифровых угроз. Правильное выставление приоритетов регулирования, их градации с учетом вероятности угроз и масштаба урона для страны позволяют оптимизировать финансовые и человеческие затраты государства, выстроить современную систему реагирования и повысить эффективность управления данной системой по противодействию цифровым рискам и угрозам.

Поскольку макроэкономика как наука изучает поведение экономической системы в целом, охватывая сложные и взаимосвязанные отношения между домашними хозяйствами, экономическими структурами (хозяйствующими субъектами) и органами государственного управления, концепция *E-Government* входит в объект исследования, формируя новую цифровую инфраструктуру взаимодействия экономических агентов и государства. Кроме того, данная концепция является одной из наиболее уязвимых с точки зрения потенциала возможного ущерба государству. Важно отметить, что на внешний контур, фактически впервые в истории государственного управления, выносится широкий спектр функционала госре-

гулирования, что значительно повышает требования к безопасности системы, ее устойчивости к угрозам.

Органы государственного управления абсорбируют и хранят массивы персональных данных, которые являются уязвимыми для кражи данных или манипулирования. Внедрение технологий *E-Government* создает серьезные вызовы как в контексте безопасности, так и устойчивости системы управления на макроуровне.

Важно отметить, что функционально системы *E-Government* выполняют три базовые операции: аккумулирование (хранение) данных, анализ данных, предоставление данных по запросу. В данном контексте основными проблемами *E-Government* являются угрозы безопасности, конфиденциальности и функциональной совместимости. Потенциальные кибератаки в адрес *E-Government* также являются сложными и нацеленными на конечных пользователей, инфраструктуру связи и внутренние серверы.

Комплексный подход к проблеме безопасности цифрового правительства предполагает выделение угроз в следующих измерениях.

1. Технологическое: обеспечение стабильности системы, гарантирование сохранения конфиденциальности данных.

2. Организационное: актуализация информации, обеспечение совместимости систем, систематизация взаимодействия различных владельцев информации, обеспечение документооборота цифровых документов.

3. Правовое: обеспечение конфиденциальности служебной и персональной информации, обеспечение циркуляции цифровых документов.

4. Экономическое: в зависимости от глубины и комплексности внедренной технологии возникает риск мультисекторальной дестабилизации. Различные модели, известные как модели зрелости *E-Government (eGMM)*, определяют направления и комплексность развития технологий цифрового правительства с точки зрения управления. Если для уровня *E-Government* 1.0 риски и угрозы негативного влияния нарушения стабильного функционирования системы на различные экономические сферы, социальные сектора и государственное управление являются минимальными, то для E-Government 4.0 дестабилизация системы может нанести разнообразный урон на национальном уровне (табл. 2).

Таблица 2

Риски и угрозы E-Government в зависимости от модели зрелости

Table 2

Risks and Threats to E-Government for Different Maturity Models

По секторам / сегментам	Модели зрелости			
	E-Government 1.0	**E-Government 2.0**	**E-Government 3.0**	**E-Government 4.0**
Экономическая среда	Отсутствует	Снижение качества предоставляемых экономических субъектам онлайн-услуг	Дестабилизация организационных процессов, краткосрочное снижение налоговых поступлений	Финансовый ущерб экономическим субъектам и физическим лицам в случае взлома системы цифровой идентификации

Окончание табл. на след. стр.

Окончание табл. 2

По секторам / сегментам	Модели зрелости			
	E-Government 1.0	**E-Government 2.0**	**E-Government 3.0**	**E-Government 4.0**
Социальная среда	Отсутствует	Снижение качества предоставляемых социальных услуг населению	Рост социальной напряженности в случае продолжительного периода дисфункции системы	Дестабилизация низовых инициатив в случае взлома систем двустороннего взаимодействия граждан и правительства (например, для проведения онлайн-голосования)
Государственное управление	Отсутствует	Отсутствует	Репутационный ущерб в случае кражи личных данных граждан и коммерческой информации экономических субъектов	Принятие ошибочных управленческих решений в случае взлома системы автоматического сбора цифровых данных систем IoT, экономические потери в случае невозможности заключения публичных тендерных контрактов и сбоя систем автоматизации торгов; налоговые потери в случае нарушения функционала поддержки систем контроля и аудита

Источник: разработано автором.

На уровне макроэкономики одним из самых акутальных в разрезе возможных угроз является концепция государственных цифровых валют (*Central Bank Digital Currency, CBDC*), обладающих значительным потенциалом генерирования системных рисков для функционирования национальных финансовых институтов. Так, согласно исследованию Федеральной резервной системы США именно риски, связанные с инфраструктурой финансового рынка, «являются критически важными для устойчивости финансовой системы» (Federal Reserve, 2021). Отмечается, что «…типологически риски включают кредитный риск, операционный риск, риск ликвидности и юридический риск. Эмпирический анализ позволяет отнести тенденции валютной цифровизации к операционному риску, который связан с недостатками в информационных системах или внутренних процессах, человеческими ошибками, сбоями в управлении или сбоями в результате внешних событий» (Криштаносов, Новикова, 2021).

Кроме того, согласно проведенному анализу «…дополнительные риски генерирует выбор определенного механизма реализации концепции CBDC. В случае

использования прямой модели эмиссии и оборота CBDC может значительно ослабнуть роль коммерческих банковских учреждений с точки зрения финансовой интермедиации. Последующее сокращение банковских депозитов и снижение доходов, полученных от предоставления данной финансовой услуги, будет стимулировать увеличение процентной ставки по банковским кредитам, снижение объема кредитования и негативно повлияет на экономический рост» (Криштаносов, Новикова, 2021). Так, по прогнозу экспертов Центра макроэкономического анализа и краткосрочного прогнозирования, внедрение цифрового рубля в России приведет до конца 2024 г. к оттоку ликвидности из российских банков размере 9 трлн. рос. руб. Нехватка ликвидности станет причиной снижения объемов банковского кредитования в размере 4–5 % и сокращения прибыли банков на 10 %[1]. По мнению экспертов Европейского центрального банка: «…замещение депозитов до востребования более дорогими источниками финансирования (кредитом центрального банка или выпуском банковских облигаций) приведет к росту затрат на банковское финансирование и Центральный банк будет вынужден компенсировать данное ужесточение финансовых условий путем снижения процентной ставки в рамках денежно-кредитной политики. Ввиду того, что банковское финансирование является лишь частью общего финансирования экономики, Центральный банк не будет снижать краткосрочные процентные ставки таким образом, чтобы затраты на банковское финансирование были компенсированы только частично. Следовательно, в новом равновесии банки потеряют конкурентоспособность и некоторую долю рынка по сравнению с другими формами финансирования (через рынки капитала и небанковских посредников)» (Bindseil, 2020).

Исследование, проведенное Ассоциацией банков России в январе 2021 г., показало, что «…основной риск внедрения CBDC заключается в обеспечении безопасности криптокошельков. Несовершенная система и низкая квалификация специалистов могут стать главными факторами появления рисков для стабильности финансовой системы. Кроме этого, есть опасность появления вредоносного программного обеспечения, направленного на взлом криптокошельков и похищение денежных средств»[2].

Эксперты Центра исследования финансовых технологий и цифровой экономики, созданного Московской школой управления «Сколково» и Российской экономической школой в исследовании «Цифровые валюты центральных банков: типология, дизайн и российская специфика», к основным рискам введения новой формы расчетов относят следующее:

а) прямое вовлечение центральных банков в рынок финансовых услуг. Это может привести к потере регулятором роли независимого участника финансового рынка и подорвать доверие с точки зрения выполнения регуляторной функции;

б) введение CBDC может казаться слишком сложным для отдельных групп населения;

---

[1] Литова, Е., Шелудченко, С. (2021). После внедрения цифрового рубля из банков может утечь 9 трлн рублей. *Ведомости*. URL: https://www.vedomosti.ru/finance/articles/2021/11/01/893920-iz-bankov-posle-vnedreniya-tsifrovogo-rublya-mozhet-utech-9-trln (дата обращения: 11.11.2021).

[2] Примером может служить использование китайской CBDC для отмывания денег группой мошенников в 2020–2021 гг. (WHATTONEWS (2021)). *Банки опасаются внедрения цифрового рубля*. URL: https://whattonews.ru/banki-opasajutsja-vnedrenija-cifrovogo-rublja/ (дата обращения: 15.01.2021)).

в) осуществление эмиссии CBDC центральным банком генерирует риск его конкуренции с рыночными предложениями финансовых услуг»[1].

Для построения эффективной системы CBDC BIS выделяет следующие принципы:

1) Центральный банк не должен ставить под угрозу денежно-кредитную или финансовую стабильность при выпуске CBDC;

2) CBDC должна сосуществовать с действующими формами денег и дополнять их;

3) CBDC должна способствовать инновациям и эффективности» (BIS, 2020).

Эмитенты цифровой валюты и поставщики платежных услуг должны гарантировать устойчивость к кибератакам, и в случае кибератаки должны быть в состоянии обеспечить быстрое восстановление и защиту целостности данных. Платежные системы должны быть устойчивыми перед лицом других внешних факторов, таких как стихийные бедствия. Одним из способов достижения этого в цифровых платежных средствах является включение функций, которые позволяют системе функционировать в автономном режиме, по крайней мере, временно.

В контексте необходимости моделирования рисков и потенциально проблемных аспектов использования CBDC в финансовой системе эксперты Форума официальных валютных и финансовых учреждений (*Official Monetary and Financial Institions forum, OMFIF*) рекомендуют «…использование специализированных сред тестирования, таких как «нормативные (регуляторные) песочницы» или инновационные центры, позволяющие оценить производительность, преимущества и риски, которые могут служить ориентиром для дальнейшего развития» (Digital Monetary Institute, 2020). Центральные банки и регулирующие органы обладают компетенцией разработки соответствующих правил, адаптированных к уровням риска, которые они наблюдают. В настоящее время центральные банки и регулирующие органы более 50 стран ввели «песочницы» финансового регулирования или аналогичные инициативы. Таким образом, имплементация механизмов CBDC позволяет финансовому регулятору снизить риск возможного доминирования альтернативных расчетных единиц на национальном уровне.

Широкое использование цифровых платежных инструментов, таких как мобильные деньги и криптовалюты, ведет к возникновению рисков финансовой дестабилизации. Как отмечает Совет по финансовой стабильности (Financial Stability Board, 2022), рынки криптоактивов стремительно развиваются и, в скором времени, будут представлять угрозу для глобальной финансовой стабильности из-за их масштаба, структурных уязвимостей и повышения взаимосвязанности с традиционной финансовой системой. Быстрая эволюция и международная природа этих рынков также повышают потенциал для регуляторных пробелов, фрагментации или арбитража.

Цифровые инновации могут повлиять на функционирование денежно-кредитной политики и эффективность инструментов политики центрального банка. Мобильные деньги могут по-разному влиять на денежную массу в экономике в зависимости от действующего регулирования и механизма хранения мобильных денег в банковской системе. Высокая степень замещения мобильными деньгами фи-

[1] Казарновский, П., Кошкина, Ю. (2021). *Эксперты назвали главные риски внедрения цифрового рубля в России*. URL: https://www.rbc.ru/finances/12/01/2021/5ffc4caf9a79470d03a85b55 (дата обращения: 15.01.2021).

атных валют или банковских депозитов может ослабить контроль центрального банка над совокупной денежной массой, увеличить скорость денежных операций, а также повлиять на доходы центральных банков от сеньоража. Рост использования мобильных денег также актуализирует проблему налогообложения экономической деятельности, поскольку операции переходят зону действия альтернативных платежных систем.

Необходимо выделить следующие риски, связанные с услугами мобильных платежей и затрагивающие макроэкономический уровень воздействия:

1) системные риски, которые могут вызвать разрушение финансовой системы или «запустить» в системе негативный сценарий развития кризиса;

2) риски ликвидности, которые снижают способность банка или поставщика (агента) мобильных финансовых услуг выполнять денежные обязательства по требованию и в зависимости от величины данной организации вызывать системные сбои в макроэкономической системе страны;

3) трансграничные риски, которые позволяют распространить системный риск за пределы одного государства;

4) риски платежных систем, которые могут привести к неспособности платежных систем проводить расчеты по мере наступления срока платежа;

5) операционные риски, которые наносят ущерб способности одного из заинтересованных лиц эффективно управлять своим бизнесом, или риск, который приводит к прямым или косвенным потерям в результате неудачных внутренних процессов, людей, систем или внешних событий, в результате чего могут возникать лавинообразные последствия, затрагивающие экономику страны в целом;

6) репутационные риски, которые наносят ущерб имиджу финансовой системы.

Замещение фиатных суверенных валют частными цифровыми платежными средствами также может повлиять на денежно-кредитную политику и генерировать новые риски для стабильности финансовой системы страны. Таким образом, в финансовой сфере имплементация технологии Blockchain связана с макроэкономическими рисками:

1) системные риски — вероятность дестабилизации финансовой системы при условии допуска к свободному обращению криптовалют на внутреннем рынке. Расширение использования криптовалюты в качестве средства оплаты товаров и услуг приведет к конкуренции с фиатной валютой, будет влиять на ее стоимость и в конечном итоге — на монетарную политику, проводимую центральным банком (Baur, Hong, et al., 2017). Многие центральные банки и финансовые регулирующие органы обеспокоены перспективой появления новых монетарных инструментов со стороны частного сектора, которые могут подорвать их способность проводить денежно-кредитную политику и поддерживать ценовую и финансовую стабильность. Кроме того, для государства возникает дополнительный риск неконтролируемого вывода финансовых активов из страны, не подвергаясь ограничениям, накладываемым на движение денежных средств. Отмечается тенденция стирания грани между традиционными и новыми финансовыми организациями: все более распространенными становятся FinTech кредитование в криптовалютах и банковские операции с частичным резервированием криптовалюты;

2) рыночные риски — высокая волатильность рынка криптовалют создает риски одномоментной потери части спекулятивных инвестиционных активов, существует угроза формирования «криптовалютного пузыря» и его негативного влияния

на стабильность финансовой системы как на наднациональном, так и страновом уровнях. Схемы финансовой пирамиды (Понци) часто маскируются как «высокодоходные» инвестиционные программы. Комиссия по ценным бумагам и биржам США (*U. S. Securities and Exchange Commission, SEC*) определяет финансовую пирамиду следующим образом: схема Понци — это инвестиционное мошенничество, которое включает в себя выплату предполагаемой прибыли существующим инвесторам из средств, внесенных новыми инвесторами. Организаторы схемы Понци часто привлекают новых инвесторов, обещая инвестировать средства в возможности, которые, как утверждают, приносят высокую прибыль практически без риска. Схемы Понци практически не имеют законных доходов или не имеют их, поэтому для продолжения работы требуется постоянный поток денег от новых инвесторов. Схемы Понци неизбежно рушатся, чаще всего, когда становится трудно привлекать новых инвесторов или когда большое количество инвесторов просит вернуть свои средства. Распространение смарт-контрактов создает новые возможности для мошенников, предоставляя следующие возможности цифровых технологий: инициатор схемы Понци может оставаться анонимным, поскольку для создания контракта и обналичивания не требуется раскрытие личности. Поскольку смарт-контракты являются «немодифицируемыми» и «неостанавливаемыми», регуляторы не смогут прекратить выполнение схемы или обратить ее последствия, чтобы возместить расходы пострадавшим. Инвесторы могут получить ложное чувство доверия из-за того, что код смарт-контрактов является публичным и неизменным и их исполнение автоматически обеспечивается. В 2020 году криптоактивы на сумму более 4,2 млрд. долларов были конфискованы китайской полицией в результате расследования финансовой пирамиды PlusToken (FCA (2021).[1];

3) технологические риски — недостаточная зрелость криптовалютного инструментария и инфраструктуры генерирует потенциальные угрозы для стабильного развития национальных денежно-кредитных систем в случае их интеграции. Кроме того, в случае потери личного ключа доступ к криптовалютам становится безвозвратным для пользователей.

В меньшей степени влияют на макроэкономические условия риски имплементации технологии Blockchain более низкого порядка:

1) энергосистемные риски — непродуктивный расход электроэнергии при майнинге создает неконтролируемый рост нагрузки для энергосистем страны дислокации криптовалютных ферм. Согласно отчету об устойчивом развитии в январе 2018 г. потребление энергии в биткойнах за одну транзакцию увеличилось на 53 % и составило 397 кВт•ч, что достаточно для питания одного домохозяйства США в течение более 13 дней. В феврале 2018 г. потребление электроэнергии биткойнами возросло до 764 кВт•ч на одну уникальную транзакцию. Годовое потребление электроэнергии биткойном увеличилось с 9,5 ТВт•ч до 50,8 ТВт•ч за последние 12 месяцев, и в феврале 2018 года биткойн потребляет 0,23 % мирового потребления электроэнергии. Точно так же увеличение было очевидно для Ethereum с 2,3 ТВт•ч до 14,5 ТВт•ч в год. По данным Кембриджского центра альтернативных финансов (Cambridge Center for Alternative Finance, CCAF), биткойн в настоящее время потребляет около 110 ТВт•ч — 0,55 % мирового производства электроэнергии, что при-

[1] FCA warns consumers of the risks of investments advertising high returns based on cryptoassets. URL: https://www.fca.org.uk/news/news-stories/fca-warns-consumers-risks-investments-advertising-high-returns-based-cryptoassets (дата обращения: 12.02.2021)).

мерно эквивалентно годовому потреблению энергии в небольших странах, таких как Малайзия или Швеция.

2) ПОД-ФТ[1] риски — дополнительный финансовый механизм отмывания денег и финансирования терроризма[2]. Проведенный США анализ киберпреступлений показал, что злоумышленники все чаще используют криптовалюту для облегчения международного финансирования терроризма, распространения оружия, уклонения от санкций и транснационального отмывания денег. Согласно исследованию CipherTrace, банки в настоящее время не в состоянии проконтролировать подавляющее большинство подозрительных сделок (Cipher Trace, 2019), связанных с криптовалютами;

3) риски формирования рынков нелегальных товаров и услуг. Анонимность в качестве функциональной и технологической особенности криптовалют стимулирует их использование в качестве платежного средства для транзакций в незаконном обороте отдельных товаров и услуг. В криптомаркетах онлайновые торговые площадки, расположенные в даркнете, которые облегчают торговлю различными нелегальными товарами, в основном наркотиками. На этих торговых площадках также предлагаются различные другие товары и продукты, связанные с мошенничеством с финансами или идентификацией, а также огнестрельное оружие, контрафактные товары, допинговые продукты. В отличие от обычных сайтов продаж, криптомаркеты облегчают обмен в контексте, где анонимность администраторов и участников защищена благодаря комбинации функций шифрования. Предлагаются нелегальные услуги и продукты, а также контрафактные товары. По одной из отраслевых оценок, около 1 % от общего объема рыночных транзакций в 2019 г., или 10 млрд долл. США, было незаконным. FinCEN выявил около 119 млрд долл. США, связанных с подозрительной деятельностью с использованием криптовалют, которая полностью или в значительной степени осуществляется в Соединенных Штатах, что составляет около 11,9 % от общей активности на рынке криптовалют. США отмечают, что злоумышленники использовали криптовалюты для содействия международному финансированию терроризма, распространению оружия, уклонению от санкций и транснациональному отмыванию денег, а также в отношении покупки и продажи контролируемых веществ, украденных и поддельных документов, удостоверяющих личность, устройств доступа, поддельных товаров, вредоносных программ и других компьютерных хакерских инструментов, огнестрельного оружия и токсичных химикатов. По одной из оценок, сумма, связанная с нелегальными онлайн-рынками (криптомаркетами), составляет около 860 млрд долл. США (Acin, 2019). Примером использования криптовалюты для оборота на нелегальном рынке являлся онлайн рынок SilkRoad[3]. По оценкам ФБР, в период функционирования SilkRoad около 5 % всей экономики биткойн было связано с данной платформой. Согласно данным отчета компании по Blockchain-анализу Chainalysis (Crypto Crime Report, 2022), Восточная Европа проявляет «наибольшую активность на глобальном рынке даркнета по сравнению с каким-либо другим регионом». Платформа Hydra ориентирована исключи-

[1] ПОД-ФТ — подход FATF к «противодействию отмыванию денег и финансированию терроризма»

[2] Исследование Foley показывает, что около четверти пользователей Биткойн и половина транзакций Биткойн связаны с незаконной деятельностью, стоимость которой достигает 72 млрд долл. США в год.

[3] Веб-сайт был запущен в феврале 2011 г. и использовался для продажи наркотиков. В октябре 2013 г. ФБР закрыло сайт.

тельно на страны Восточной Европы и входит в число крупнейших даркнет-рынков в мире. По данным аналитиков, за период с июня 2019 г. по июль 2020 г. объем сделок на платформе Hydra составил более 1,2 млрд долл. США в криптовалюте. В 2020 году объем сделок в криптовалюте на платформе Hydra достиг 1,37 млрд долл. США. По мнению ряда исследователей, данная платформа является крупнейшей за всю историю, в настоящее время недельный объем следок в криптовалюте достигает 125 млн долл. США.

В зависимости от уровня угроз для национальной безопасности возможно дифференцировать риски использования технологии Blockchain от минимальных до предельных, где наиболее существенными из них являются ПОД-ФТ, преодоление санкционных ограничений на уровне государств и компаний, опосредованное стимулирование формирования рынка краденых цифровых активов, осуществление мошеннических операций[1], расширение использования программ вымогателей.

Следует также выделить ряд рисков, генерируемых инструментарием DeFi, основными из которых являются валютный и платформенный. Как отмечает МВФ[2], деятельность DeFi особенно уязвима к рыночным рискам, рисками ликвидности и киберугрозам. Кибератаки, представляющие серьезную угрозу для традиционных банков, зачастую могут стать фатальными для таких платформ и привести к краже финансовых активов и подрыву доверия пользователей.

Важно отметить, что с учетом наращивания технологического потенциала регуляторов киберпреступники расширяют использование ряда цифровых решений:

1) технологии смешивания (миксеры) — сервисы, предназначенные для скрытия взаимосвязи между адресами в последовательных транзакциях. Услуги смешивания направлены на решение проблем с отслеживанием криптовалют путем объединения нерелевантных транзакций. Два типичных типа смешивания — это своппинг и CoinJoin. Сервис микширования на основе свопинга принимает депозиты от пользователей на один из адресов в адресном пуле и снимает их с другого. В результате, нивелируется связь между адресами ввода и вывода. Сервисы смешивания с использованием свопинга включают BitcoinFog, BitLaundry и Helix. Механизм CoinJoin позволяет объединить две или более отдельных транзакций в одну транзакцию CoinJoin, которая имеет такое же присутствие в Blockchain, как обычная транзакция с несколькими входами и несколькими выходами. Следовательно, связь между реальными парами ввода–вывода неясна. Сервисы на основе CoinJoin включают JoinMarket, CoinShuffle и SharedCoin Blockchain.info (обслуживание прекращено).

2) альткойны с внутренними конструкциями, повышающими конфиденциальность. К данным альткойнам относятся Zerocoin, Zerocash, и Dash; дизайн CryptoNote[3], включая Monero, Bytecoin и DigitalNote. Zcash позволяет пользовате-

[1] В 2021 году в мире было похищено в криптовалюте на сумму более 7,7 млрд долл. США (рост на 81 % по сравнению с 2020 г.). Только благодаря российской финансовой пирамиде Finiko произошло хищения более 1,1 млрд долл. США .

[2] Pascual, A., Natalucci, F. (2022). Fast-Moving FinTech Poses Challenge for Regulators. *IMF Blog*. URL: https://blogs.imf.org/2022/04/13/fast-moving-fintech-poses-challenge-for-regulators/ (дата обращения: 08.04.2022).

[3] Криптовалюты, подобные CryptoNote, такие как Monero, используют другую технологию — кольцевую подпись, чтобы усложнить записи транзакций, не вызывая больших вычислительных затрат. Транзакция Monero позволяет объединить несколько выходов из предыдущих транзакций в качестве входов, но только некоторые из входов могут быть «обманчивыми», поскольку их значения никогда не передаются в выход.

лям хранить и осуществлять транзакции ZEC, то есть криптовалюту Zcash с двумя типами адресов (прозрачными и защищенными). «Прозрачные» адреса передают значения на другие адреса, по сути так же, как биткойн, в то время как «защищенные» адреса совершают транзакции в «защищенных пулах». В частности, при внесении депозита в пул получатель указывается с использованием экранированных адресов, т. е. Z-адреса, который скрывает получателя, но по-прежнему раскрывает отправителя, а выход из пула скрывает отправителя, но раскрывает получателя. Криптографическая основа защищенного пула — это практические доказательства с нулевым разглашением, называемые zfc-SNARK. С точки зрения моделей данных транзакции Zcash напоминают схему пула смешивания подкачки.

Отмечается тенденция стирания грани между традиционными и новыми финансовыми организациями: все более распространенными становятся FinTech кредитование в криптовалютах и банковские операции с частичным резервированием криптовалюты.

Исследования МВФ (IMF, 2015) показывают, что усиление роли FinTech расширяет доступ населения к кредитам, что в сочетании с низким качеством банковского надзора за FinTech организациями ставит под угрозу макрофинансовую стабильность в стране.

В отчете Совета по финансовой стабильности (FSB) были определены в т. ч. следующие риски, связанные с FinTech (Financial Stability Board, 2017).

1. Рост кредитования онлайн-платформ в условиях слабых стандартов кредитования повышает вероятность того, что широко распространенные дефолты могут спровоцировать кризис.

2. Секьюритизация кредитов, предоставляемых кредиторами на рынке FinTech, может быть особенно рискованной, поскольку потенциальные дефолты заемщиков приведут к снижению кредитоспособности системы и снижению цен на эти активы.

3. Потенциальный пузырь в государственных или частных акциях FinTech компаний может привести к негативным последствиям для финансовой системы.

Как отмечает Скардови (Scardovi, 2017), стабильность глобальной финансовой системы все в большей степени зависит от растущего цифрового характера рисков:

1) вводящая в заблуждение информация о состоянии кредитного рынка может привести к невозможности сбалансировать предложение на кредитование на платформах P2P и реальной способности заемщиков погасить свой долг. Теоретически взаимодействие спроса и предложения на кредитование на платформах P2P должно иметь тенденцию приспосабливаться к реальной способности заемщиков погасить свой долг (как мера с помощью более информированных и более интеллектуальных инструментов оценки поведения, основанных на ML / AI и использующих структурированные и неструктурированные данные), с учетом отдачи, которую они могут получить от своих инвестиционных проектов или моделей потребления, что соответствует их экономическому жизненному циклу.

2) центральным банкам становится сложнее контролировать показатели кредитования, поскольку кредитная активность FinTech организаций частично зависит от базовой процентной ставки экономики, не регулируется инструментарием минимальных резервных требований, определяемых регулятором в отношении банков;

3) FinTech организациям постепенно переходит ответственность за преобразование сроков погашения долгов, что может привести к нехватке ликвидности

и рыночным крахам, если большинство выданных FinTech ссуд станут невозвратными и потребуется реструктуризация и списание долгов, особенно с учетом внезапных изменений процентной ставки экономики (если инфляция снижается, долги по фиксированным ставкам становятся все менее устойчивыми);

4) увеличение скорости использования капитала, обусловленное финансовыми инновациями, может стать важным компонентом цифровых рисков. Высокочастотная торговля, пулы и использование альтернативных торговых площадок становятся управляемыми сверхскоростными алгоритмами, генерируемыми искусственным интеллектом, которые могут потенциально разрушить рынки в случае цифровых ошибок в используемых алгоритмах.

МВФ отмечает рост системной значимости цифровых банков на национальных финансовых рынках. При этом FinTech организации более подвержены рискам, связанным с потребительским кредитованием, которое, как правило, предоставляется без залогового обеспечения, а также рискам ликвидности, поскольку объем ликвидных активов у таких организаций ниже, чем у традиционных банковских институтов. Кроме того, FinTech усиливают конкуренцию в отрасли, снижая рентабельность традиционных банков и подвергая системным рискам банковский сектор.

Отдельным фактором развития FinTech становится его подверженность монополизации, поскольку цифровые данные становятся самым ценным активом, способствующим росту прибыльности в различных секторах и цепочках создания стоимости.

Alphabet (Google), Apple, Microsoft, Facebook, Amazon контролируют большое количество данных, их экономия от масштаба вызывает беспокойство со стороны регуляторов, ответственных за поддержание конкуренции, поскольку их размер и охват усугубляются всевозможными сетевыми эффектами. Конкурентное преимущество обусловлено владением большими данными, которое предоставляет возможность (или угрозу) для создания непреодолимого конкурентного «разрыва», используемого немногими владельцами мегаданных «разделяй и властвуй» (разделяя конкурентов и остальную часть рынка, чтобы в конечном итоге доминировать над обоими).

Выход крупных технологических компаний на рынок финансовых услуг делает этот рынок эффективнее, но в то же время создает риски для финансовой стабильности и конкуренции. Крупные технологические компании на рынке финансовых услуг предлагают различного рода FinTech инструменты, включая банковские, платежные и краудфандинговые сервисы, кредиты, страховки, возможности для управления активами. При этом глобальные игроки благодаря инновационности используемых бизнес-моделей, технологий и сетевых эффектов, которые усиливаются недостаточным регулированием и возможностью регуляторного арбитража, имеют возможность монополизации кредитного рынка, отводя традиционным банковским институтам лишь роль источника фондирования. Кроме того, FinTech компании имеют возможность манипулировать поведением своих пользователей, создавать собственные платежные системы с эмиссией стейблкойнов, предназначенных для эксклюзивного использования в этих системах (DeFi), что обеспечивает дополнительные их конкурентные преимущества на рынке. Профессор Принстонского универси-

тета Бруннермайер[1] убежден, что объективные рыночные преимущества FinTech приведут к еще большей концентрации рыночной власти у нескольких компаний и фрагментации денежно-кредитной системы, а также эрозии монетарного суверенитета стран. Возможность такого развития FinTech поддерживает и управляющий BIS Карстенс, который отмечает, что технокомпании крайне быстро переходят из категории «слишком мелких, чтобы о них думать» (*too small to care*) в категорию «слишком больших, чтобы их игнорировать» (*too big to ignore*), а затем и «слишком больших, чтобы допустить их банкротство» (*too big to fail*).

В настоящее время внедрение ИТ технологий в производственные процессы и связанная с ними цифровизация и виртуализация определяют три разнонаправленные тенденции, каждая из которых может стать как доминирующей, так и внешней тенденцией в зависимости от проводимой в стране экономической политики.

Первая тенденция — высвобождение рабочей силы, поскольку потребность экономики в физическом труде уменьшается. Преобладание этой тенденции, как отмечают Путилов, Бугаенко и Тимохин (Putilov, Bugaenko, et al., 2018) «…увеличивает безработицу в экономике, приводит к снижению спроса на национальном рынке и в конечном итоге может вызвать экономическую деградацию». В исследовании, проведенном McKinsey Global Institute (Manyika et al., 2017), отмечено, что во многих отраслях промышленности к 2030 году благодаря появлению новых технологий и автоматизации вероятно сокращение 73 млн. рабочих мест. Исследование перспективы автоматизации с помощью цифровых технологий, робототехники и AI, проведенное Фреем и Осборном (Frey & Osborne, 2017) показало, что 47 % рабочих мест в США рискуют стать избыточными[2]. Цифровизация затронет рабочие места во многих отраслях и секторах, включая промышленное производство, логистику, образование, госуправление, здравоохранение.

Вторая тенденция связана с повышением производительности труда. Так, «… рост производительности труда в масштабах национальной экономики ведет к ужесточению конкуренции, снижению затрат и цен на инновационную продукцию, а также обеспечивает укрепление конкурентных позиций национального производителя в мировой экономике» (Putilov, Bugaenko, et al., 2018). Национальная рабочая сила востребована как ресурс для мирового производства, что увеличивает спрос на нее, ведет к повышению заработной платы и покупательной способности занятых. По мнению WEF (WEF Report, 2020), синергия технологий и человека дает устойчивый прирост производительности, в то время как автоматизация ради сокращения рабочей силы дает только временные улучшения. Ряд исследований подчеркивают, что инвестиции в цифровые технологии (роботы, 3D печать, IoT), которые подпитывают текущую промышленную революцию, положительно влияют на занятость высококвалифицированных работников и отрицательно влияют на занятость низкоквалифицированных работников. Ожидается, что как в развитых, так и в странах с формирующейся экономикой быстрый переход к удаленной работе приведет к долгосрочному повышению производительности, но при этом рискует создать новые разрывы между специалистами и теми, кто занят в производственных секторах и не может работать удаленно, либо могут не иметь цифровых навы-

[1] Волкова, О. (2021). Бигтехи на финансовом рынке: риски и вызовы для регуляторов. *Эконс*. URL: https://econs.online/articles/regulirovanie/bigtekhi-na-finansovom-rynke/ (дата обращения: 23.03.2022).

[2] В 2000 году компания Goldman Sachs имела в штате шестьсот трейдеров, а благодаря внедрению AI в 2017 году корпорация смогла сократить число трейдеров-людей до двух.

ков и инструментов для поиска другой работы в таких областях, как производство, розничная торговля и некоторые области здравоохранения. Расширение разрыва в цифровой грамотности создает риск создания «цифрового низшего класса».

Третья тенденция связана с изменением структуры экономики и рынка труда. Так, «…увеличивается доля занятых высококвалифицированных кадров, наблюдается рост инновационных отраслей экономики» (Putilov, Bugaenko, et al., 2018). С развитием интеллектуальных систем все большее число услуг будет доступно через интеллектуальные устройства и интернет. К 2025 году в результате разделения труда между людьми, машинами и алгоритмами может появиться 97 млн новых рабочих мест (WEF Report, 2020). Компании будут стремиться использовать преимущества AI по следующим направлениям:

а) увеличивая разрыв в заработной плате между квалифицированным и неквалифицированным трудом, так как последний предположительно более заменим AI, чем первый;

б) автоматизируя контрольные задачи;

в) поощряя самозанятость. По данным отчета Мак-Кинси, COVID-19 ускорил внедрение автоматизации и AI, поскольку предприятия стремятся контролировать свои затраты и повышать эффективность за счет сокращения доли занятых, выполняющих рутинные задачи.

Компании достигают поставленной задачи двумя способами: внедрением технологий автоматизации и изменением рабочих процессов[1]. AI, таким образом, становится важным инструментом, который будет замещать такие направления деятельности, как бухгалтерский и складской учет, логистика, внутренний и внешний аудит, административный и торговый функционал, клиентское обслуживание, банковская сфера, страховое обслуживание, юриспруденция и пр. Востребованность на рынке приобретут специальности на стыке ИТ технологий (AI, ML, BDA), аналитики, теории и практики функционирования современных бизнес-моделей. В разрезе профессий до 2030 года под влиянием ускоренной цифровизации и внедрения новых технологий после пандемии COVID-19 прогнозируется положительный сдвиг в занятости в таких профессиях, как врачи и медсестры, научные и технические специалисты, менеджеры, а также креативные профессии. Сократится спрос на занятых в коммунальном хозяйстве, строителей, офисных работников, ресторанном бизнесе, сельском хозяйстве.

Наиболее вероятной представляется определенная конвергенция трех тенденций, которая будет проявляться в структурной трансформации экономик развитых государств, росте сектора ИКТ и цифровых сегментов традиционных отраслей, требующих высококвалифицированных специалистов. При этом будет отмечаться снижение занятости в отраслях первичного сектора экономики и перетекание трудовых ресурсов в сектор услуг, который в наименьшей мере будет в среднесрочной перспективе подвержен тотальной цифровизации. В данном контексте задачей государства является обеспечение плавного перетока трудовых ресурсов из менее производительных секторов в более производительные. Лица, которые по объективным (субъективным) причинам не способны освоить цифровые навыки, станут фокусной группой для государственной поддержки. Одним из механизмов социального обеспечения для дан-

[1] В рамках международного исследования в июле 2020 г. из 800 руководителей различных компаний 2/3 заявили, что они активизируют свою деятельность и вложения в автоматизацию и искусственный интеллект — частично или значительно (McKinsey Global Institute, 2021).

ной группы граждан может служить базовый доход. Обеспечение плавного перехода к цифровым технологиям и снижение рисков для социальной стабильности из-за цифрового разрыва потребует со стороны государства системного управления инновациями, не ограничивая их, например, настаивая на безопасности и конфиденциальности при разработке новых технологий и цифровых услуг.

Кейс Республики Беларусь

В Республике Беларусь как на уровне макроэкономики, так и социальной среды важнейшее влияние цифровизации будет также проявляться в расширении «цифрового разрыва»[1] как между различными категориями граждан и внутри отраслей (сегментов) экономики страны, обостряя цифровое неравенство, положительно влияя на занятость высококвалифицированных работников и отрицательно влияя на занятость низкоквалифицированных работников. Экстраполяция выявленных тенденций и динамки цифровизации передовых стран Европы, Азии и США на рынок труда Республики Беларусь позволяет прогнозировать к 2030 г. положительный сдвиг занятости в таких профессиях, как медицинские работники, научные и технические специалисты, персонал креативных отраслей. Вместе с тем также высока вероятность сокращения спроса на рынке труда в коммунальном хозяйстве, строительстве, образовании, офисного и торгового персонала, складской логистике, сельском хозяйстве. В случае если будут доминировать характеристики трансформации рынка труда, свойственные развивающимся странам (Индии и КНР), сокращение затронет, главным образом, сектор сельского хозяйства Беларуси в объеме около 8 %, или около 30 тыс. человек (отталкиваясь от статистических показателей 2019 года). Кроме того, в зоне риска находятся также рабочие места в сфере администрирования, общественного питания, продаж и складской логистики. Ускорение и углубление цифровизации повысит требования к занятым во многих отраслях и секторах, включая промышленное производство, образование, госуправление, здравоохранение, стимулируя рост безработицы среди низкоквалифицированной рабочей силы.

Резюмируя разнонаправленные эффекты цифровизации экономики, Глобальный экономический форум (Global Risks Report, 2021) среди актуальных рисков внедрения цифровых инноваций выделяет в краткосрочной перспективе (0–2 лет) недостаточную кибербезопасность и цифровое неравенство[2]; в среднесрочной перспективе (3–5 лет) — взлом ИТ-инфраструктуры, недостаточная кибербезопасность и ошибки в управлении технологиями[3]; долгосрочные риски (5–10 лет) — неблагоприятные технологические достижения[4]. В авторитарных государствах существует угроза того, что правительства попытаются захватить главные платформы и поставщиков услуг,

[1] Разрыв в цифровом образовании, в условиях доступа к цифровым услугам и продуктам и, как следствие, разрыв в уровне благосостояния.

[2] Фрагментированный и (или) неравный доступ к важнейшим цифровым сетям и технологиям между странами и внутри стран в результате неравных инвестиционных возможностей, отсутствия необходимых навыков у рабочей силы, недостаточной покупательной способности, государственных ограничений и (или) культурных различий.

[3] Отсутствие общепринятых структур, институтов или правил для использования критически важных цифровых сетей и технологий в результате того, что разные государства или группы государств принимают несовместимую цифровую инфраструктуру, протоколы и (или) стандарты.

[4] Преднамеренные или непреднамеренные негативные последствия технического прогресса для людей, бизнеса, экосистем и (или) экономики: AI, биотехнологии, геоинженерия, квантовые вычисления и т. д.

тем самым консолидируя свою власть по ограничению доступа в Интернет, цензуре информации и сокращению коммуникаций. Пути к будущим экономическим и социальным выгодам в этих условиях будут под угрозой.

Агрегируя данные проведенного анализа, можно выделить следующие макроэкономические угрозы цифровизации в отношении различных аспектов экономического развития страны (табл. 3).

Таблица 3

Риски и угрозы цифровизации в разрезе макроэкономического развития

Table 3

Risks and Threats of Digitalization in the Macro-Economic Context

Макроэкономические показатели	Направление влияния рисков и угроз	
	препятствующее росту	стимулирующее рост
Инфляция	—	Расширение кредитно-финансовой деятельности FinTech, в особенности с использованием криптовалюты, может привести к перетоку фиатных денежных активов в криптоактивы, стимулируя инфляцию
Национальный доход	Рост темпов автоматизации и цифровизации приведет к цифровому разрыву и высвобождению рабочей силы и падению доходов низкоквалифицированной рабочей силы; развитие FinTech индустрии будет способствовать снижению процентов по кредитам	—
ВВП	Сокращение показателей национального дохода может оказать негативное влияние на рост ВВП	—
Международная торговля	Несогласованное на международном уровне внедрение концепции CBDC приведет к негативному влиянию на международные платежи, препятствуя росту международной торговли	—
Международные финансы	Расширение использования CBDC, укрепление доверия и стабилизация криптовалютных рынков приведет к трансформации текущей мировой финансовой системы, возможной ее дестабилизации	—
Безработица	—	Автоматизация и цифровизация все большего количества производственных и бизнес-процессов, внедрение FinTech инноваций, E-Government будут стимулировать расширение цифрового разрыва населения, росту безработицы низкоквалифицированной рабочей силы

Окончание табл. на след. стр.

Окончание табл. 3

Макроэкономические показатели	Направление влияния рисков и угроз	
	препятствующее росту	стимулирующее рост
Сбережения и инвестиции	Внедрение технологий CBDC сокращает кредитные ресурсы коммерческих банков за счет «отмены» традиционных депозитных механизмов	Аккумулирование значительных финансовых ресурсов глобальными ИКТ компаниями (их капитализация) приведет к росту инвестиций в цифровой сфере

Источник: разработано автором.

4. Заключение

Цифровизация создает определенные риски и угрозы на уровне макроэкономики, затрагивая такие ее элементы, как инфляция, национальный доход, ВВП, международная торговля, международные финансы и безработица. При этом наиболее уязвимыми элементами макроэкономики для цифровых рисков являются международные финансы и безработица. Технологии AI / ML, IoT, BDA, концепции CBDC, FinTech позволяют автоматизировать бизнес-процессы, сократить количество рутинных операций, меняя, тем самым, рынок труда, генерируя новые вызовы в отношении государственной социальной политики.

В Республике Беларусь можно с высокой степенью уверенности прогнозировать сокращение спроса на персонал в коммунальном хозяйстве, строительстве, образовании, офисном и торговом администрировании, складской логистике. В наибольшей степени риску сокращения рабочих мест подвержено сельское хозяйство, где количество занятых в ближайшие годы может уменьшиться на 8 %, или около 30 тыс. человек.

Концепции CBDC, FinTech создают потенциальные риски для стабильности функционирования финансовой системы не только на национальном, но и международном уровне, формируя новые цифровые рынки мобильных денег и криптовалют. В этой связи актуализируется проблематика качества банковского надзора, цифровых компетенций регулятора. Высокая динамика имплементации цифровых концептов, рост скорости использования капитала вызывают необходимость трансформации подходов и инструментария кредитно-денежной политики центральных банков.

Концепция E-Government, формируя новую цифровую инфраструктуру взаимодействия экономических агентов и государства, создает потенциал для роста рисков и угроз в контексте как безопасности, так и устойчивости системы госуправления. Как показал анализ eGMM, наибольший многосторонний потенциальный ущерб для различных систем государственного управления связан с имплементацией E-Government 4.0 как самой комплексной версией концепта. Данный факт предопределяет необходимость детальной системной проработки государством данного концепта в разрезе рисков и угроз на технологическом, организационном, правовом и экономическом уровнях с целью нивелирования (минимизации) урона экономической, социальной средам и системе госуправления.

Цифровизация широкого спектра экономических, социальных и политических отношений актуализирует проблематику развития национальных систем подготовки кадров для новой экономики, а также программ переобучения трудовых ресурсов с целью повышения их цифровых навыков. Страны и регионы, которые

смогут в кратчайшие сроки реализовать данные программы, сформируют эффективные системы адаптации образовательных систем к новым требованиям экономики, получат конкурентное преимущество в международном разделении труда и станут привлекательными территориями для размещения инновационных производств и стартапов в среднесрочной перспективе.

Список источников

Добродеев, А. Ю. (2021). Кибербезопасность в Российской Федерации. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века. *Вопросы кибербезопасности, 4* (44), 61–72. DOI: 10.21681/2311-3456-2021-4-61-72.

Криштаносов, В. Б. (2021). Методология оценки и управления цифровыми рисками. *Труды БГТУ. Сер. 5, Экономика и управление, 2* (250), 15–36.

Новикова, И. В., Криштаносов, В. Б. (2021). Цифровые валюты центральных банков: современные тенденции и возможности имплементации в Республике Беларусь. *Банковский вестник, 4* (693), 13–20.

Носов, С. (2021). Система кибербезопасности в Китае. *Зарубежное военное обозрение, 2,* 17–24. URL: http://factmil.com/publ/strana/kitaj/sistema_kiberbezopasnosti_v_kitae_2021/59-1-0-1833 (дата обращения: 03.03.2022).

Павлов, К. В. (2009). Экономические «черная дыра» и экстремальный уровень неопределенности производственных процессов и экономической среды. *Национальные интересы: приоритеты и безопасность, 11* (44), 28–36.

Acin, V. (2019). Making sense of the dark web. *Computer Fraud & Security,* 17–19. DOI:10.1016/s1361-3723(19)30075-2.

Ali, M. A., Azad, M. A., Parreno Centeno, M., Hao, F., van Morsel, A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems, 100,* 408–427. https://doi.org/10.1016/j.future.2019.03.041

Aminzade, M. (2018). Confidentiality, integrity and availability — finding a balanced IT framework. *Network Security, 5,* 9–11. https://doi.org/10.1016/S1353-4858(18)30043-6

Financial Stability Board (2022). *Assessment of Risks to Financial Stability from Crypto-assets,* 26. URL: https://www.fsb.org/wp-content/uploads/P160222.pdf (дата обращения: 15.05.2022).

Baur, D., Hong, K., Lee, A. (2017). Bitcoin: Medium of Exchange or Speculative Assets? *Journal of International Financial Markets, Institutions & Money, 54,* 177–189. https://doi.org/10.1016/j.intfin.2017.12.004

Bindseil, U. (2020). Tiered CBDC and the financial system. *European Central Bank Working Paper Series, 2351,* 41. DOI: https://doi.org/10.2866/134524. URL: https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf (дата обращения: 27.08.2021).

Bank for International Settlements (2020). *Central bank digital currencies: foundational principles and core features*. URL: https://www.bis.org/publ/othp33.pdf (дата обращения: 07.01.2022).

CipherTrace (2019). *Cryptocurrency anti-money laundering report, 2019 Q4*. URL: https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/ (дата обращения: 25.07.2020).

Brookson, C., Cadzow, S. et al. (2015). *Definition of Cybersecurity. Gaps and overlaps in standardisation. V1.0.* https://doi.org/10.2824/4069

Federal Reserve Policy on Payment System Risk (2021). URL: https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf (дата обращения: 03.02.2022).

Financial Stability Board (2017). *Financial stability implications from FinTech*. URL: http://www.fsb.org/wp-content/uploads/R270617.pdf (дата обращения: 02.03.2020).

Frey, C. B., Osborne, M. A. (2017). The future of employment: how susceptible are jobs to computerization? *Technological Forecasting and Social Change, 114,* 254–280. https://doi.org/10.1016/j.techfore.2016.08.019

Fuster, G. G., Jasmontaite, L. (2020). Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. *The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, vol 21*. Cham, Switzerland: Springer, 97–115. https://doi.org/10.1007/978-3-030-29053-5_5

Hunton, P. (2012). Data attack of the cybercriminal: Investigating the digital currency of cybercrime. *Computer Law & Security Review, 28* (2), 201–207. DOI: https://doi.org/10.1016/j.clsr.2012.01.007.

Introduction to Threat Modeling. Microsoft (2020). URL: https://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Introduction_to_Threat_Modeling.ppsx (дата обращения: 10.01.2020).

Manyika, J., Lund, S., Chui, M. et al. (2017). *Jobs lost, jobs gained: Workforce transitions in a time of automation*. URL: https://www.mckinsey.com/~/media/mckinsey/industries/public%20and%20social%20sector/our%20insights/what%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/mgi-jobs-lost-jobs-gained-executive-summary-december-6-2017.pdf (дата обращения: 26.04.2018).

Nauck, F., Usher, O., Weiss, L. (2020). *The disaster you could have stopped: Preparing for extraordinary risks*. URL: https://www.mckinsey.com/business-functions/risk/our-insights/the-disaster-you-could-have-stopped-preparing-for-extraordinary-risks?cid=other-eml-nsl-mip-mck&hlkid=061d027268294196b455863b2fa7bbd6&hctky=11708326&hdpid=89044107-4811-4e7a-a384-9ca7c398bac6 (дата обращения: 13.03.2020).

NIST (2012). *Guide for Conducting Risk Assessments*. Washington DC: Special Publication 800–30 Rev, 195. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (дата обращения: 01.03.2020).

Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction, 27,* 632–641. https://doi.org/10.1016/j.ijdrr.2017.08.006

Putilov, A. V., Bugaenko, M. V., Timokhin, D. V. (2018). Development of Russian labor market in the context of informatization and computerization of the economy. *Procedia Computer Science, 145* (6), 169–176. https://doi.org/10.1016/j.procs.2018.11.035

Ramezani, J., Camarinha-Matos, L. (2020). Approaches for resilience and antifragility in collaborative business ecosystems. *Technological Forecasting & Social Change, 151,* 119846 https://doi.org/10.1016/j.techfore.2019.119846

Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience (2012). Cologny, Switzerland: World Economic Forum, 48. URL: https://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf (дата обращения: 09.02.2019).

Ruan, K. (2019). Cyber Risk Management: A New Era of Enterprise Risk Management. *Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomics*. Cambridge: Elsevier Inc, 49–73. DOI: 10.1016/B978-0-12-812158-0.00003-X.

Sahay, R., Čihák, M. et al. (2015). Financial Inclusion: Can It Meet Multiple Macroeconomic Goals? *SDN/15/17,* 33. URL: https://www.imf.org/external/pubs/ft/sdn/2015/sdn1517.pdf (дата обращения: 20.12.2019).

Scardovi, C. (2017). *Digital Transformation in Financial Services*. Cham, Switzerland: Springer International Publishing AG, 236. https://doi.org/10.1007/978-3-319-66945-8

NIST (2020). *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST Special Publication 800–53, Rev. 5, 492. https://doi.org/10.6028/NIST.SP.800-53r5

Chainalysis (2022). *The Crypto Crime Report*. URL: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf (дата обращения: 03.04.2022).

World Economic Forum (2020). *The Future of Jobs. Report*. URL: http://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf (дата обращения: 13.05.2021).

Digital Monetary Institute (2020). *The Future of Payments*. URL: https://www.omfif.org/wp-content/uploads/2020/12/The-Future-of-Payments.pdf (дата обращения: 11.11.2020).

Lund, S., Madgavkar, A. et al. (2021). *The postpandemic economy. The Future of Work after COVID 19*. McKinsey Global Institute, 152.

World Economic Forum (2022). *The Global Risks Report 2022, 17th Edition.* URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (дата обращения: 19.01.2022).

World Economic Forum (2021). *The Global Risks Report 2021, 16th Edition.* URL: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (дата обращения: 03.02.2022).

Wray, P., Schneuwly, A., Chan, S., Ahuja, M., Choy, D. (2021). *Technology Risk and Regulatory Compliance. Impact During COVID-19.* Boston Consulting Group. URL: https://web-assets.bcg.com/e4/46/273331fd49cd888586ac90921291/technology-risk-and-regulatory-compliance-impact-during-covid-19.pdf (дата обращения: 13.10.2021).

References

Acin, V. (2019). Making sense of the dark web. *Computer Fraud & Security,* 17–19. DOI:10.1016/s1361-3723(19)30075-2

Ali, M. A., Azad, M. A., Parreno Centeno, M., Hao, F. & van Morsel, A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems, 100,* 408–427. https://doi.org/10.1016/j.future.2019.03.041

Aminzade, M. (2018). Confidentiality, integrity and availability — finding a balanced IT framework. *Network Security, 5,* 9–11. https://doi.org/10.1016/S1353-4858(18)30043-6

Bank for International Settlements (2020). *Central bank digital currencies: foundational principles and core features.* Retrieved from: https://www.bis.org/publ/othp33.pdf (Date of access: 07.01.2022).

Baur, D., Hong, K. & Lee, A. (2017). Bitcoin: Medium of Exchange or Speculative Assets? *Journal of International Financial Markets, Institutions & Money, 54,* 177–189. https://doi.org/10.1016/j.intfin.2017.12.004

Bindseil, U. (2020). Tiered CBDC and the financial system. *European Central Bank Working Paper Series, 2351,* 41. https://doi.org/10.2866/134524. Retrieved from: https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf (Date of access: 27.08.2021).

Brookson, C., Cadzow, S. et al. (2015). *Definition of Cybersecurity. Gaps and overlaps in standardisation. V1.0.* https://doi.org/10.2824/4069.

Chainalysis (2022). *The Crypto Crime Report.* Retrieved from: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf (Date of access: 03.04.2022).

CipherTrace (2019). *Cryptocurrency anti-money laundering report, 2019 Q4.* Retrieved from: https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/ (Date of access: 25.07.2020).

Digital Monetary Institute (2020). *The Future of Payments.* Retrieved from: https://www.omfif.org/wp-content/uploads/2020/12/The-Future-of-Payments.pdf (Date of access: 11.11.2020).

Dobrodeev, A. Yu. (2021). Kiberbezopasnost' v Rossiyskoy Federatsii. Modnyy termin ili prioritetnoe tekhnologicheskoe napravlenie obespecheniya natsional'noy i mezhdunarodnoy bezopasnosti XXI veka [Cybersecurity in Russian Federation. A trendy term or the priority technologic area of enhancing national and international security of the XXI century]. *Voprosy kiberbezopasnosti [Cybersecurity issues], 4* (44), 61–72. DOI:10.21681/2311-3456-2021-4-61-72. (In Russ.)

Federal Reserve Policy on Payment System Risk (2021). Retrieved from: https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf (Date of access: 03.02.2022).

Financial Stability Board (2017). *Financial stability implications from FinTech.* Retrieved from: http://www.fsb.org/wp-content/uploads/R270617.pdf (Date of access: 02.03.2020).

Financial Stability Board (2022). *Assessment of Risks to Financial Stability from Crypto-assets,* 26. Retrieved from: https://www.fsb.org/wp-content/uploads/P160222.pdf (Date of access: 15.05.2022).

Frey, C. B. & Osborne, M. A. (2017). The future of employment: how susceptible are jobs to computerization? *Technological Forecasting and Social Change, 114,* 254–280. https://doi.org/10.1016/j.techfore.2016.08.019.

Fuster, G. G. & Jasmontaite, L. (2020). Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. *The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, vol 21.* Cham, Switzerland: Springer, 97–115. https://doi.org/10.1007/978-3-030-29053-5_5.

Hunton, P. (2012). Data attack of the cybercriminal: Investigating the digital currency of cybercrime. *Computer Law & Security Review, 28* (2), 201–207. https://doi.org/10.1016/j.clsr.2012.01.007

Introduction to Threat Modeling. Microsoft (2020). Retrieved from: https://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Introduction_to_Threat_Modeling.ppsx (Date of access: 10.01.2020).

Kryshtanosau, V. B. (2021). Metodologiya oczenki i upravleniya czifrovymi riskami [Methodology for assessment and management of digital risks]. *Trudy BGTU [Proceedings of BSTU, issue 5, Economics and Management], 2* (250), 15–36. (In Russ.)

Lund, S., Madgavkar, A. et al. (2021). *The postpandemic economy. The Future of Work after COVID 19.* McKinsey Global Institute, 152.

Manyika, J., Lund, S., Chui, M. et al. (2017). *Jobs lost, jobs gained: Workforce transitions in a time of automation.* Retrieved from: https://www.mckinsey.com/~/media/mckinsey/industries/public%20and%20social%20sector/our%20insights/what%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/mgi-jobs-lost-jobs-gained-executive-summary-december-6-2017.pdf (Date of access: 26.04.2018).

Nauck, F., Usher, O. & *Weiss, L. (2020). The disaster you could have stopped: Preparing for extraordinary risks*. Retrieved from: https://www.mckinsey.com/business-functions/risk/our-insights/the-disaster-you-could-have-stopped-preparing-for-extraordinary-risks?cid=other-eml-nsl-mip-mck&hlkid=061d027268294196b455863b2fa7bbd6&hctky=11708326&hdpid=89044107-4811-4e7a-a384-9ca7c398bac6 (Date of access: 13.03.2020).

NIST (2012). *Guide for Conducting Risk Assessments*. Washington DC: Special Publication 800–30 Rev, 195. Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (Date of access: 01.03.2020).

NIST (2020). *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST Special Publication 800–53, Rev. 5, 492. https://doi.org/10.6028/NIST.SP.800-53r5

Nosov, S. (2021). Sistema kiberbezopasnosti v Kitae [China's Cybersecurity system]. *Zarubezhnoe voennoe obozrenie [Foreign military review], 2,* 17–24. Retrieved from: http://factmil.com/publ/strana/kitaj/sistema_kiberbezopasnosti_v_kitae_2021/59-1-0-1833 (Date of access 03.03.2022) (In Russ.)

Novikova, I. & Krishtanosov, V., (2021). Czifrovye valyuty czentralnykh bankov: sovremennye tendenczii i vozmozhnosti implementaczii v Respublike Belarus [Digital Currencies of Central Banks: Modern Trends and Possibilities of Implementation in the Republic of Belarus]. *Bankovskij vestnik [Bank Bulletin Journal], 4* (693), 13–20. (In Russ.)

Pavlov, K. V. (2009). Ekonomicheskie "chernaya dyra" i ekstremal'nyy uroven' neopredelennosti proizvodstvennykh protsessov i ekonomicheskoy sredy [Economic "Black Hole" and Extreme Uncertainty Level of Manufacture and Economic Environment]. *Natsional'nye interesy: prioritety i bezopasnost' [National Interests: Priorities and Security], 11* (44), 28–36. (In Russ.)

Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction, 27,* 632–641. https://doi.org/10.1016/j.ijdrr.2017.08.006

Putilov, A. V., Bugaenko, M. V. & Timokhin, D. V. (2018). Development of Russian labor market in the context of informatization and computerization of the economy. *Procedia Computer Science, 145* (6), 169–176. https://doi.org/10.1016/j.procs.2018.11.035

Ramezani, J. & Camarinha-Matos, L. *(2020). Approaches for resilience and antifragility in collaborative business ecosystems. Technological Forecasting & Social Change, 151,* 119846. https://doi.org/10.1016/j.techfore.2019.119846.

Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience (2012). Cologny, Switzerland: World Economic Forum, 48. Retrieved from: https://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf (Date of access: 09.02.2019).

Ruan, K. (2019). Cyber Risk Management: A New Era of Enterprise Risk Management. *Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomics*. Cambridge: Elsevier Inc, 49–73. DOI: 10.1016/B978-0-12-812158-0.00003-X.

Sahay, R., Čihák, M. et al. (2015). Financial Inclusion: Can It Meet Multiple Macroeconomic Goals? *SDN/15/17,* 33. Retrieved from: https://www.imf.org/external/pubs/ft/sdn/2015/sdn1517.pdf (Date of access: 20.12.2019).

Scardovi, C. (2017). *Digital Transformation in Financial Services*. Cham, Switzerland: Springer International Publishing AG, 236. https://doi.org/10.1007/978-3-319-66945-8

World Economic Forum (2020). *The Future of Jobs. Report.* Retrieved from: http://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf (Date of access: 13.05.2021).

World Economic Forum (2021). *The Global Risks Report 2021, 16th Edition.* Retrieved from: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (Date of access: 03.02.2022).

World Economic Forum (2022). *The Global Risks Report 2022, 17th Edition.* Retrieved from: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (Date of access: 19.01.2022).

Wray, P., Schneuwly, A., Chan, S., Ahuja, M. & Choy, D. (2021). *Technology Risk and Regulatory Compliance. Impact During COVID-19.* Boston Consulting Group. Retrieved from: https://web-assets.bcg.com/e4/46/273331fd49cd888586ac90921291/technology-risk-and-regulatory-compliance-impact-during-covid-19.pdf (Date of access: 13.10.2021).

Информация об авторах

Криштаносов Виталий Брониславович — кандидат экономических наук, докторант, Белорусский государственный технологический университет; https://orcid.org/0000-0002-1146-368X (Республика Беларусь, 220006, г. Минск, ул. Свердлова, 13а; e-mail: Krishtanosov@mail.ru).

Бровко Наталья Анатольевна — доктор экономических наук, декан, профессор, Кыргызско-Российский Славянский университет имени первого Президента Российской Федерации Б. Н. Ельцина; https://orcid.org/0000-0003-4376-9103 (Кыргызская Республика, 720000, г. Бишкек, ул. Киевская, 44; e-mail: nbrovko@list.ru).

About the authors

Vitaly B. Krishtanosov— Cand. Sci. (Econ.), Doctoral Student, Belarusian State Technological University; https://orcid.org/0000-0002-1146-368X (13a, Sverdlova St., Minsk, 220006, Republic of Belarus; e-mail: Krishtanosov@mail.ru).

Natalya A. Brovko— Dr. Sci. (Econ.), Dean, Professor, Kyrgyz-Russian Slavic University named after the first president of Russian Federation B. N. Yeltsin; https://orcid.org/0000-0003-4376-9103 (44, Kievskaya St., Bishkek, Kyrgyz Republic; e-mail: nbrovko@list.ru).

Дата поступления рукописи: 21.11.2022.
Прошла рецензирование: 26.12.2022.
Принято решение о публикации: 15.02.2023.
Received: 21 Nov 2022.
Reviewed: 26 Dec 2022.
Accepted: 15 Feb 2023.