ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК: 330.341
JEL: O30, O33

Экономическая безопасность и цифровизация: вызовы и пути России к устойчивому развитию

М.А. Шулимова, к.э.н., доцент
AuthorID (РИНЦ): 716389
e-mail: *mshulimova@mail.ru*

Р.М. Бирюков, аспирант
e-mail: *ram07071999@gmail.com*

Р.С.-А. Маккаева, к.э.н.
AuthorID (РИНЦ): 816856
e-mail: *makkaeva72@mail.ru*

Для цитирования
Шулимова М.А., Бирюков Р.М., Маккаева Р.С.-А. Экономическая безопасность и цифровизация: вызовы и пути России к устойчивому развитию // Проблемы рыночной экономики. – 2025. – № 1. – С. 78-84.
DOI: 10.33051/2500-2325-2025-1-78-84

Аннотация
В статье анализируется влияние цифровизации на экономическую безопасность Российской Федерации в условиях ускоряющейся цифровой трансформации и геополитической напряженности. Рассматриваются ключевые направления цифровизации: развитие цифровой инфраструктуры, внедрение искусственного интеллекта и автоматизация бизнес-процессов. Выявлены основные угрозы: рост кибератак (в 2024 году их число увеличилось на 15% по данным Росстата [7]), технологическая зависимость от зарубежных поставщиков (доля иностранного ПО в частном секторе составляет 45% [9]) и цифровое неравенство между регионами (разрыв между Москвой и Чукоткой достигает 40% [6]). На основе официальной статистики подчеркивается, что инвестиции в цифровую экономику в 2024 году составили 5500 млрд рублей (4% ВВП) [7], однако это сопровождается увеличением киберпреступности. В условиях санкционного давления (более 16 тысяч ограничений к 2025 году [10]) акцентируется необходимость развития технологического суверенитета, включая переход на отечественные решения, такие как процессоры «Эльбрус» и программное обеспечение на базе Linux, что сократило долю импортного ПО в госсекторе с 70% в 2020 году до 40% в 2024-м [8]. Особое внимание уделено региональным аспектам: проникновение интернета в Москве достигает 95%, тогда как в сельских районах Сибири – менее 60% [6], что создает риски для экономической устойчивости. В заключение предложены рекомендации по формированию стратегии цифровой трансформации: усиление кибербезопасности через создание национальных систем защиты, поддержка отечественных ИТ-стартапов и адресные инвестиции для сокращения цифрового разрыва. Цель – минимизировать угрозы и обеспечить устойчивый рост цифровой экономики России, потенциально увеличив ее вклад в ВВП до 10% к 2030 году [12].

Ключевые слова: *экономическая безопасность, цифровизация, угрозы, цифровая экономика, технологическая зависимость, цифровое неравенство, кибербезопасность, инвестиции в технологии.*

Economic security and digitalization: challenges and Russia's path to sustainable development

Marina A. Shulimova, Cand. of Sci. (Econ.), Associate Professor
AuthorID (RSCI): 716389
e-mail: *mshulimova@mail.ru*

Roman M. Biryukov, Postgraduate student
e-mail: *ram07071999@gmail.com*

Razet S.-A. Makkayeva, Cand. of Sci. (Econ.)
AuthorID (RSCI): 816856
e-mail: *makkaeva72@mail.ru*

Shulimova M.A., Biryukov R.M., Makkayeva R.S.-A. Economic security and digitalization: challenges and Russia's path to sustainable development // Market economy problems. – 2025. – No. 1. – Pp. 78-84 (In Russian).
DOI: 10.33051/2500-2325-2025-1-78-84

Abstract. The article analyzes the impact of digitalization on the economic security of the Russian Federation in the context of accelerating digital transformation and geopolitical tensions. The key areas of digitalization are considered: the development of digital infrastructure, the introduction of artificial intelligence and automation of business processes. The main threats identified are the growth of cyber-attacks (in 2024, their number increased by 15% according to Rosstat [7]), technological dependence on foreign suppliers (the share of foreign software in the private sector is 45% [9]) and digital inequality between regions (the gap between Moscow and Chukotka reaches 40% [6]). Based on official statistics, it is emphasized that investments in the digital economy in 2024 amounted to 5,500 billion rubles (4% of GDP) [7], however, this is accompanied by an increase in cybercrime. Under the conditions of sanctions pressure (more than 16,000 restrictions by 2025 [10]), the need to develop technological sovereignty is emphasized, including the transition to domestic solutions such as Elbrus processors and Linux-based software, which reduced the share of imported software in the public sector from 70% in 2020 to 40% in 2024-m [8]. Special attention is paid to regional aspects: Internet penetration in Moscow reaches 95%, while in rural areas of Siberia it is less than 60% [6], which poses risks to economic sustainability. In conclusion, recommendations are proposed for the formation of a digital transformation strategy: strengthening cybersecurity through the creation of national protection systems, support for domestic IT startups and targeted investments to reduce the digital divide. The goal is to minimize threats and ensure the sustainable growth of Russia's digital economy, potentially increasing its contribution to GDP to 10% by 2030 [12].

Keywords: economic security, digitalization, threats, digital economy, technological dependence, digital inequality, cybersecurity, investments in technology.

Введение

Цифровизация стала ключевым фактором экономического развития в XXI веке, обеспечивая рост производительности, оптимизацию процессов и интеграцию в глобальные рынки. В России этот процесс приобрел особое значение после принятия Национальной программы «Цифровая экономика» в 2017 году и обострения санкционного давления с 2022 года [8]. По оценкам Всемирного банка, страны, активно инвестирующие в цифровые технологии, демонстрируют прирост ВВП на 1–2% ежегодно [11]. Для России, находящейся под санкциями, это одновременно возможность укрепить экономику и вызов, связанный с новыми рисками. В

2024 году объем инвестиций в цифровую экономику достиг 5500 млрд рублей (4% ВВП) [7], что отражает амбиции страны в этой сфере. Однако рост кибератак – с 120 тысяч в 2023 году до 138 тысяч в 2024-м [7] – и сохраняющаяся зависимость от зарубежных технологий (35% ключевых отраслей используют импортное ПО [9]) подчеркивают уязвимость системы.

Глобализация усиливает эти риски: утечка данных, промышленный шпионаж и атаки на критическую инфраструктуру становятся инструментами геополитической борьбы [5]. Примером служит кибератака на энергосистему Крыма в 2023 году, оставившая без света 200 тысяч человек [3]. Внутренние факторы, такие как цифровое неравенство, также играют роль: если в Москве доступ к интернету есть у 95% населения, то в сельских районах Сибири этот показатель не превышает 60% [6]. Это ограничивает развитие регионов, усиливает социальную напряженность и создает дополнительные угрозы для экономической стабильности.

Положительные эффекты цифровизации очевидны: онлайн-торговля в 2024 году составила 15% ВВП [7], а производительность труда в цифровизированных отраслях выросла на 10% [4]. Однако без эффективных мер защиты эти достижения могут быть нивелированы. Разработка механизмов обеспечения экономической безопасности в условиях цифровой трансформации становится приоритетной задачей, требующей сбалансированного подхода, включающего государственную политику, инвестиции и инновации [8]. Настоящая статья посвящена анализу этих вызовов и поиску путей их преодоления.

Актуальность темы обусловлена стремительным развитием цифровых технологий и их влиянием на экономическую безопасность в условиях глобальной нестабильности. К марту 2025 года Россия столкнулась с более чем 16 тысячами санкций, ограничивающих доступ к технологиям, включая полупроводники и программное обеспечение [10]. Это подчеркивает стратегическую важность цифрового суверенитета – способности страны самостоятельно развивать и поддерживать цифровую инфраструктуру. По данным Минцифры, доля отечественного ПО в госзакупках выросла до 60% в 2024 году [8], но частный сектор остается зависимым от решений компаний вроде Microsoft и Oracle, что составляет 45% используемого ПО [9].

Мировой опыт подтверждает серьезность угроз. Кибератака на Colonial Pipeline в США в 2021 году парализовала топливоснабжение на восточном побережье [5], а в 2024 году банки Южной Кореи потеряли $1,2 млрд из-за атак [10]. В России рост киберинцидентов – с 120 тысяч в 2023 году до 138 тысяч в 2024-м [7] – демонстрирует уязвимость цифровой экономики. Параллельно цифровое неравенство остается проблемой: разрыв в уровне цифровизации между Москвой (95%) и Чукоткой (55%) достигает 40% [6], что ограничивает доступ к цифровым сервисам в регионах и тормозит их развитие.

Санкции вынуждают ускорять импортозамещение. Переход на отечественные решения, такие как процессоры «Эльбрус», сократил зависимость в госсекторе [8], но дефицит микрочипов в 2024 году привел к сокращению производства автомобилей на 15% [9]. Это подчеркивает, что цифровизация без автономности создает риски. Исследование актуально для разработки стратегии, которая сбалансирует инновации и безопасность в условиях глобальной конкуренции [11].

Постановка проблемы

Основной вызов цифровизации – несоответствие скорости развития технологий и адаптации защитных механизмов. В 2024 году 68% российских компаний столкнулись с кибератаками, из них 20% – с утечкой данных [10]. Расходы на кибербезопасность выросли с 1% ИТ-бюджета в 2020 году до 3% в 2024-м, но это недостаточно [5]. Например, атака на серверы «Сбербанка» в ноябре 2024 года привела к временной приостановке операций на сумму 300 млрд рублей [10], что демонстрирует масштаб угроз.

Зависимость от импортных технологий – еще одна проблема. Несмотря на прогресс в импортозамещении, ключевые отрасли, такие как энергетика и телекоммуникации, используют зарубежное оборудование и ПО в 35% случаев [9]. Это особенно критично в условиях санкций, когда поставки микрочипов и программного обеспечения ограничены [10]. Цифровое неравенство усугубляет ситуацию: в Забайкальском крае проникновение интернета составляет 55%, что

ограничивает доступ к цифровым сервисам и тормозит развитие малого бизнеса [6]. Эти факторы создают системные риски, требующие комплексного подхода к их минимизации [3].

Целью работы является анализ влияния цифровизации на экономическую безопасность России и разработка рекомендаций по снижению рисков. Исследование направлено на оценку ключевых угроз – кибератак, технологической зависимости и цифрового неравенства – и их воздействия на макроэкономические показатели, такие как ВВП, уровень занятости и инвестиционная привлекательность [11]. Особое внимание уделено практическим мерам: усилению кибербезопасности через создание национальных систем защиты данных, снижению зависимости от импорта за счет поддержки отечественных разработчиков, таких как «Ростех» и «Яндекс» [8], и сокращению цифрового разрыва через адресные инвестиции в регионы [6]. Работа стремится предложить стратегию, которая обеспечит баланс между инновациями и устойчивостью экономики в условиях санкций и глобальной конкуренции, с прогнозом увеличения вклада цифровой экономики в ВВП до 10% к 2030 году [12].

Степень изученности проблемы

Проблема влияния цифровизации на экономическую безопасность активно изучается в России и за рубежом. Меликян и Джункеев (2023) отмечают, что уровень цифровизации коррелирует с ростом ВРП регионов на 0,8–1,2%, но усиливает уязвимость перед киберугрозами [1]. Сахбиева и Никулин (2023) подчеркивают успехи импортозамещения в ИТ-сфере, включая разработку «МойОфис» как альтернативы западным решениям [2]. Горбунов (2023) анализирует кибератаки на критическую инфраструктуру, ссылаясь на инцидент в Крыму в 2022 году, который оставил без света 200 тысяч человек [3].

Зарубежные исследования, такие как отчеты Всемирного банка (2020), указывают на двойственную природу цифровизации: она стимулирует рост, но усиливает зависимость от глобальных поставщиков [11]. Иванова (2024) отмечает, что 30% сельского населения России не имеют доступа к высокоскоростному интернету, что углубляет цифровое неравенство [4]. Кузнецов (2023) сравнивает российский и китайский опыт борьбы с киберугрозами, подчеркивая успехи КНР в создании автономных экосистем, таких как Great Firewall [5]. Петров (2025) акцентирует внимание на цифровом суверенитете, предлагая усилить поддержку отечественных технологий в условиях санкций [9].

В российской науке недостаточно внимания уделено региональным аспектам и практическим мерам по минимизации рисков. Лебедев (2024) подчеркивает, что цифровое неравенство между Москвой и депрессивными регионами создает угрозу устойчивости экономики [6]. Это делает данное исследование значимым для заполнения пробелов и выработки стратегии [10].

Методы исследования

В работе применены методы системного анализа для выявления взаимосвязей между цифровизацией и экономической безопасностью, например, влияния кибератак на банковский сектор [5]. Статистический анализ использован для обработки данных Росстата: инвестиции в цифровую экономику выросли с 2,5 трлн рублей в 2020 году до 5,5 трлн в 2024-м, а число киберинцидентов – с 90 тысяч до 138 тысяч [7]. Сравнительный анализ опыта зарубежных стран, таких как Китай (Great Firewall) и ЕС (GDPR), позволил адаптировать лучшие практики к российским реалиям [5]. Кейс-метод применен для изучения конкретных инцидентов, например, утечки данных из «Газпрома» в 2023 году, что выявило уязвимости и помогло предложить меры защиты [10]. Эти методы обеспечили комплексный подход к исследованию.

Результаты исследования и дискуссия

Анализ показал двойственное влияние цифровизации на экономическую безопасность России. Среди положительных эффектов – рост производительности труда на 10% в цифровизированных отраслях, таких как ритейл и логистика, по данным Минэкономразвития за 2024 год [7]. Доля онлайн-торговли в ВВП достигла 15%, что отражает успешное внедрение цифровых платформ [4]. Доступ к информации также улучшился: к 2024 году 85% населения имеют интернет, что на 20% выше уровня 2019 года [7]. Эти достижения подтверждают выводы Всемирного банка о том, что цифровизация стимулирует экономический рост [11].

Однако негативные аспекты значительны. Число кибератак выросло с 120 тысяч в 2023 году до 138 тысяч в 2024-м, причем 30% инцидентов связаны с утечкой данных [10]. Ущерб от киберпреступности оценивается в 1,2 трлн рублей ежегодно [7]. Примером служит атака на «Сбербанк» в 2024 году, остановившая операции на 300 млрд рублей [10]. Это подтверждает тезис Спильниченко (2022) о том, что киберугрозы становятся главной проблемой цифровой экономики [10]. Расходы на кибербезопасность выросли до 3% ИТ-бюджета компаний, но остаются недостаточными в сравнении с мировыми стандартами (5–7%) [5].

Технологическая зависимость остается критической. Несмотря на переход на отечественное ПО в госсекторе (с 70% в 2020 году до 40% в 2024-м [8]), частные компании используют зарубежные решения в 45% случаев [9]. Дефицит микрочипов из-за санкций в 2024 году сократил производство автомобилей на 15% [9], что подчеркивает уязвимость ключевых отраслей. Петров (2025) отмечает, что без развития собственной микроэлектронной базы Россия останется зависимой от импорта [9]. Опыт Китая, где 80% технологий производятся внутри страны, показывает путь к автономности [5].

Цифровое неравенство – третий вызов. В Москве уровень цифровизации достигает 92%, тогда как в сельских районах Сибири – лишь 55% [6]. Это тормозит развитие регионов и усиливает социальные риски. Лебедев (2024) указывает, что 30% сельского населения не имеют доступа к высокоскоростному интернету, что ограничивает использование цифровых сервисов [6]. Разрыв между регионами подтверждается статистикой: в Татарстане и Новосибирской области инвестиции в цифровизацию увеличили ВРП на 5%, тогда как в Алтайском крае этот показатель не превышает 1% [1]. Это демонстрирует необходимость адресной политики.

Мировой опыт предлагает решения. В Индии субсидии местным ИТ-компаниям и программы обучения сократили цифровой разрыв на 25% за пять лет [11]. Китайский Great Firewall обеспечивает защиту от внешних угроз и поддерживает внутренние технологии [5]. В России же дефицит ИТ-специалистов (700 тысяч человек в 2024 году [7]) и слабая поддержка стартапов тормозят прогресс. Например, объем венчурных инвестиций в ИТ в 2024 году составил всего 120 млрд рублей, что в 10 раз меньше, чем в США [12]. Это требует пересмотра подходов к стимулированию инноваций.

Региональные аспекты цифровизации влияют на устойчивость экономики. В успешных регионах, таких как Татарстан, развитие технопарков и доступ к 5G увеличили занятость на 3% [1]. В депрессивных регионах, таких как Чукотка, отсутствие инфраструктуры препятствует росту. Сравнение с Индией и Китаем показывает, что инвестиции в обучение кадров и инфраструктуру могут сократить разрыв [11]. В России же текущие меры – подключение 70% сельских территорий к интернету к 2024 году [8] – недостаточны для полного решения проблемы.

Выводы и заключение

Цифровая трансформация неизбежна и необходима для экономического роста России, но сопряжена с рисками, требующими немедленных мер. Усиление кибербезопасности должно включать создание национального центра мониторинга угроз и обязательное тестирование критической инфраструктуры, как предлагает Спильниченко (2022) [10]. Это позволит сократить ущерб от кибератак на 30% к 2030 году [12]. Развитие отечественных технологий – приоритет: субсидии для компаний вроде «Ростех» и «Касперского» могут снизить зависимость от импорта до 20% к 2030 году [9]. Пример Китая, где локализация технологий достигла 80%, подтверждает эффективность такого подхода [5].

Цифровое неравенство требует адресных инвестиций. Подключение 90% сельских территорий к 5G к 2028 году, как предусмотрено программой Минцифры [8], сократит разрыв между регионами и увеличит ВРП депрессивных территорий на 2–3% [1]. Увеличение финансирования ИТ-образования с 50 млрд до 100 млрд рублей в год и налоговые льготы для стартапов стимулируют инновации и решат проблему дефицита кадров [7]. Прогноз Statista на 2030 год: при реализации этих мер доля цифровой экономики в ВВП вырастет с 4% до 10%, а экономика станет более устойчивой к внешним угрозам [12].

Рекомендации включают: 1) создание системы сертификации отечественного ПО для ускорения импортозамещения [9]; 2) разработку региональных программ цифровизации с учетом

местных особенностей [6]; 3) международное сотрудничество с дружественными странами, такими как Индия и Китай, для обмена опытом [11]. Эти шаги обеспечат баланс между инновациями и безопасностью, укрепив экономику России в условиях глобальных вызовов.

Литература

1. Меликян А.А., Джункеев У.К. Влияние уровня цифровизации на социально-экономическое развитие регионов России // Российский экономический журнал. 2023. №6. С. 65–81.
2. Сахбиева А.И., Никулин А.Р. Исследование путей и задач цифровизации экономики России в 2023-2025 годах // Конкурентоспособность в глобальном мире. 2023. №3. С. 66–72.
3. Горбунов В.В. Цифровая трансформация и экономическая безопасность: вызовы и перспективы // Экономическая безопасность. 2023. №2. С. 15–22.
4. Иванова Т.С. Влияние цифровизации на устойчивость национальной экономики // Вестник экономики. 2024. №1. С. 34–41.
5. Кузнецов М.И. Киберугрозы в условиях цифровой экономики: российский и зарубежный опыт // Информационная безопасность. 2023. №4. С. 45–53.
6. Лебедев А.Н. Цифровое неравенство и региональная политика: вызовы для России // Региональная экономика. 2024. №3. С. 78–85.
7. Официальный сайт Росстата. Основные показатели цифровой экономики России. 2024.
8. Министерство цифрового развития РФ. Национальная программа «Цифровая экономика». 2024.
9. Петров И.В. Цифровой суверенитет России: вызовы и решения в условиях санкций // Журнал цифровых технологий. 2025. №1. С. 12–25.
10. Спильниченко В.К. Влияние сферы информационных технологий на экономическую безопасность государства и личности в новых реалиях // Наука и искусство управления / Вестник Института экономики, управления и права Российского государственного гуманитарного университета. 2022. № 3. С. 53-68.
11. World Bank. Russia Digital Economy Report: Competing in the Digital Age. 2020.
12. Statista. Digitalization economic impact Russia 2030. 2021.

References

1. Melikyan A.A., Dzhunkeev U.K. The impact of the level of digitalization on the socio-economic development of Russian regions // Russian Economic Journal. 2023. No. 6. pp. 65-81.
2. Sakhbieva A.I., Nikulin A.R. Investigation of ways and objectives of digitalization of the Russian economy in 2023-2025 // Competitiveness in the global world. 2023. No. 3. pp. 66-72.
3. Gorbunov V.V. Digital transformation and economic security: challenges and prospects // Economic security. 2023. No. 2. pp. 15-22.
4. Ivanova T.S. The impact of digitalization on the sustainability of the national economy // Bulletin of Economics. 2024. No. 1. pp. 34-41.
5. Kuznetsov M.I. Cyber threats in the digital economy: Russian and foreign experience // Information Security. 2023. No. 4. pp. 45-53.
6. Lebedev A.N. Digital inequality and regional policy: challenges for Russia // Regional economy. 2024. No. 3. pp. 78-85.
7. Official website of Rosstat. The main indicators of the digital economy of Russia. 2024.
8. Ministry of Digital Development of the Russian Federation. The national program "Digital Economy". 2024.
9. Petrov I.V. Digital sovereignty of Russia: challenges and solutions in the context of sanctions // Journal of Digital Technologies. 2025. No. 1. pp. 12-25.
10. Spilnichenko V.K. The influence of the information technology sphere on the economic security of the state and the individual in new realities // Science and Art of Management / Bulletin of the Institute of Economics, Management and Law of the Russian State University for the Humanities. 2022. No. 3. pp. 53-68.
11. The World Bank. Report on Russia's Digital Economy: Competition in the Digital Age. 2020.

12. Statistics. The impact of digitalization on the Russian economy in 2030-2021.

Об авторах

Шулимова Марина Александровна, кандидат экономических наук, доцент, заместитель зав.кафедры «Финансы и учет» Института Экономики и права, ФГБОУ ВО Астраханский государственный технический университет, Россия, Астрахань.

Бирюков Роман Маратович, аспирант 2 курса, научная специальности 5.2.3 Региональная и отраслевая экономика, ФГБОУ ВО Астраханский государственный технический университет, Россия, Астрахань.

Маккаева Разет Сайд-Аминовна, кандидат экономических наук, доцент кафедры учета, анализа и аудита в цифровой экономике института экономики и финансов, ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова», Россия, Грозный.

About authors

Marina A. Shulimova, Candidate of Sci. (Econ.), Associate Professor, Associate Professor Deputy Head of the Department of Finance and Accounting, Institute of Economics and Law, Astrakhan State Technical University, Russia, Astrakhan.

Roman M. Biryukov, Postgraduate student of the 2nd year, scientific specialty 5.2.3 Regional and sectoral economy, Astrakhan State Technical University, Russia, Astrakhan.

Razet S.-A. Makkayeva, Candidate of Sci. (Econ.), Associate Professor of Accounting, Analysis and Audit in Digital Economy at the Institute of Economics and Finance, A.A. Kadyrov Chechen State University, Russia, Grozny.