

Научный журнал «Менеджер». 2026. № 2(116). С. 32-46.

Scientific Journal "Manager". 2026;(2/116):32-46.

Современный менеджмент: проблемы теории и практики

Научная статья

УДК 332.13

JEL: L52, O33, H56

EDN: XDWHDE

БАК 5.2.6. Менеджмент

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ КАК ФАКТОР СТРАТЕГИЧЕСКОГО РАЗВИТИЯ И КЛЮЧЕВОЙ ВЫЗОВ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ: СИСТЕМНЫЙ АНАЛИЗ И НАПРАВЛЕНИЯ РЕГУЛИРОВАНИЯ

Ольга Николаевна Николаева¹, Мария Владимировна Гончарова²

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Донецкий институт управления, Донецк, Донецкая Народная Республика, Россия

¹olga-nony@yandex.ru, <https://orcid.org/0009-0002-3180-7627>

²mariya.goncharova.00@mail.ru, <https://orcid.org/0009-0000-1848-1912>

Аннотация. Проблема. Исследование посвящено противоречию, присущему цифровизации экономики. С одной стороны, она выступает ключевым фактором конкурентоспособности и стратегического развития, с другой – генерирует новые системные угрозы экономической безопасности. Для Российской Федерации данная проблема особенно актуальна в контексте санкционного давления и задач по обеспечению технологического суверенитета.

Методология. Исследование проведено в рамках теории экономической безопасности и стратегического управления. Применён комплекс методов: системный анализ (для рассмотрения цифровой трансформации, стратегического развития и экономической безопасности как единой системы), метод анализа рисков (для оценки факторов и угроз), сравнительный анализ (для сопоставления эволюции понятий и адекватности механизмов регулирования), аналитическое обобщение научной литературы, а также анализ нормативных документов Российской Федерации. **Результаты исследования.** Обоснован вывод о необходимости перехода государственного регулирования от реактивной к проактивной модели, функционирующей на принципе «безопасность через развитие». Выявлены ключевые риски и разработан комплекс мер, направленных на их минимизацию в контексте стратегических целей развития страны. **Практическое применение.** Результаты исследования могут быть использованы органами государственной власти для совершенствования механизмов регулирования цифровой трансформации. Предложенные меры нацелены на минимизацию системных угроз и трансформацию вызовов с целью укрепления технологического суверенитета и экономической безопасности России.

Ключевые слова: цифровая трансформация, экономическая безопасность, стратегическое развитие, технологический суверенитет, киберриски, государственное регулирование, Российская Федерация

Для цитирования: Николаева О. Н., Гончарова М. В. Цифровая трансформация как фактор стратегического развития и ключевой вызов экономической безопасности России: системный анализ и направления регулирования // Научный журнал «Менеджер». 2026. № 2(116). С. 32-46. EDN: XDWHDE.



© Николаева О.Н., Гончарова М.В., 2026

Modern management: problems of theory and practice

Original article

**DIGITAL TRANSFORMATION AS A FACTOR OF STRATEGIC DEVELOPMENT
AND A KEY CHALLENGE FOR RUSSIA'S ECONOMIC SECURITY:
SYSTEMIC ANALYSIS AND REGULATORY DIRECTIONS**

Olga N. Nikolaeva¹, Maria V. Goncharova²

Russian Presidential Academy of National Economy and Public Administration, Donetsk Institute
of Management, Donetsk, Donetsk People's Republic, Russia

¹olga-nony@yandex.ru, <https://orcid.org/0009-0002-3180-7627>

²mariya.goncharova.00@mail.ru, <https://orcid.org/0009-0000-1848-1912>

Abstract. Problem. The research addresses the inherent contradiction in the digitalization of the economy. On one hand, it serves as a key factor for competitiveness and strategic development; on the other hand, it generates new systemic threats to economic security. This issue is particularly relevant for the Russian Federation in the context of sanctions pressure and the tasks of ensuring technological sovereignty. **Methodology.** The study was conducted within the framework of economic security theory and strategic management. A comprehensive set of methods was applied: systemic analysis (to consider digital transformation, strategic development, and economic security as a unified system), risk analysis (to assess factors and threats), comparative analysis (to compare the evolution of concepts and the adequacy of regulatory mechanisms), analytical generalization of scientific literature, and analysis of normative documents of the Russian Federation. **Research Results.** The conclusion is substantiated regarding the necessity of transitioning state regulation from a reactive to a proactive model, operating on the principle of "security through development." Key risks have been identified, and a set of measures aimed at their minimization in the context of the country's strategic development goals has been developed. **Practical Application.** The research findings can be utilized by state authorities to improve the regulatory mechanisms for digital transformation. The proposed measures are aimed at minimizing systemic threats and transforming challenges to strengthen Russia's technological sovereignty and economic security.

Keywords: digital transformation, economic security, strategic development, technological sovereignty, cyber risks, state regulation, Russian Federation

For citation: Nikolaeva, O. N., & Goncharova, M. V. (2026). Digital transformation as a factor of strategic development and a key challenge for Russia's economic security: systemic analysis and regulatory directions. *Scientific Journal "Manager"*, 2(116), 32–46. (In Russian). EDN: XDWHDE.

Введение

На современном этапе глобального экономического развития цифровизация является ключевым фактором конкурентоспособности национальных экономик¹. Страны, способные генерировать, внедрять и масштабировать цифровые технологии, определяют векторы технологического прогресса и получают стратегические преимущества на мировой арене² [1; 2; 3]. Процессы цифровой трансформации кардинально меняют традиционные бизнес-модели³, системы государственного управления [4; 5; 6] и социальные взаимодействия [7], формируя новую парадигму экономического роста, основанную на данных, искусственном интеллекте и повсеместном доступе в интернет.



© Nikolaeva, O.N., Goncharova, M.V., 2026

¹ Пакт во имя будущего и его приложения, Глобальный цифровой договор и Декларация о будущих поколениях. Резолюция, принятая Генеральной Ассамблеей 22 сентября 2024 года.

URL: <https://docs.un.org/ru/A/RES/79/1>.

² Цифровизация: от комфортной жизни до обеспечения промпроизводства: Экспертный аналитический доклад. URL: <https://национальныепроекты.рф/upload/doklad-cifra-2025/doklad-cifra-2025.pdf>.

³ Цифровизация малого бизнеса в России 2025: Аналитический отчёт // Соваре, ООО. Санкт-Петербург. Декабрь 2025 года. 28 с. URL: <https://soware.ru/soware-small-business-digitalization-in-russia-2025.pdf>.

Однако применение цифровой среды порождает фундаментальное противоречие. С одной стороны, цифровизация выступает фактором роста производительности, эффективности и инноваций, являясь неперенным условием для стратегического развития [8; 9]. С другой стороны, она же становится источником новых, сложно прогнозируемых и системных угроз экономической безопасности [10; 11]. Эти риски носят комплексный характер – от технологической зависимости и уязвимости критической информационной инфраструктуры (КИИ) до дестабилизации рынка труда и возникновения «цифровых разрывов» [12]. Таким образом, на повестку дня выходит задача не просто ускорения цифровой трансформации, а обеспечения её безопасности и устойчивости.

Для Российской Федерации данная проблема приобретает особую остроту. С одной стороны, государство активно стимулирует цифровизацию в рамках таких стратегических документов, как национальный проект «Цифровая экономика»⁴ и «Стратегия экономической безопасности Российской Федерации на период до 2030 года»⁵. Эти документы фиксируют переход страны к цифровому будущему. С другой стороны, риски, связанные с цифровой зависимостью от иностранных технологий, кибератаками и необходимостью обеспечения технологического суверенитета, многократно возросли [11; 12]. Возникает насущная потребность в синхронизации целей развития и задач безопасности, что и определяет высокую актуальность данного исследования.

Цель и задачи исследования

Целью настоящей статьи является проведение системного анализа взаимосвязи процессов цифровой трансформации, стратегического развития и экономической безопасности Российской Федерации, а также разработка на его основе практических направлений государственного регулирования, нацеленных на минимизацию возникающих рисков.

Для достижения поставленной цели определены следующие задачи:

раскрыть эволюцию и уточнить содержание ключевых понятий исследования – «экономическая безопасность», «стратегическое развитие» и «цифровая трансформация» – в условиях новой технологической парадигмы;

выявить и систематизировать позитивное влияние цифровой трансформации на стратегические показатели развития национальной экономики (производительность, инновации, качество государственного управления и др.);

идентифицировать и проанализировать комплекс угроз экономической безопасности России, порождаемых цифровой трансформацией, с выделением их системного и взаимосвязанного характера;

провести оценку адекватности существующей в России системы государственного регулирования (нормативно-правовой базы и институциональной структуры) вызовам на стыке цифровизации и экономической безопасности и выявить её системные слабости;

разработать комплекс направлений и практических мер по совершенствованию государственного регулирования, направленных на переход от реактивной к проактивной модели управления на принципе «безопасность через развитие».

Решение этих задач позволит минимизировать риски и трансформировать их в импульс для укрепления технологического суверенитета России.

Методы исследования

Комплексный подход к изучению взаимосвязи цифровой трансформации, стратегического развития и экономической безопасности позволил провести системный анализ данной проблемы и разработать научно обоснованные рекомендации. Для достижения поставленной цели в работе использован следующий набор методов: системный анализ (при рассмотрении цифровой трансформации, экономической безопасности и стратегического развития как единой сложной системы, выявлении прямых и обратных связей между её элементами, а также для разработки комплексных мер

⁴ Национальная программа «Цифровая экономика Российской Федерации».

URL: <https://digital.gov.ru/target/naczionalnaya-programma-czifrovaya-ekonomika-rossijskoj-federaczii>.

⁵ Стратегия экономической безопасности Российской Федерации на период до 2030 года. Утверждена Указом Президента Российской Федерации от 15.05.2024 г. № 387.

URL: <http://publication.pravo.gov.ru/document/0001202405150002>.

государственного регулирования); SWOT-анализ (для комплексной оценки текущей ситуации в России и систематизации сильных и слабых сторон, возможностей и угроз цифровизации для национальной экономики); метод анализа рисков (при идентификации, оценке вероятности и возможных последствий конкретных угроз экономической безопасности, возникающих в цифровой среде); сравнительный анализ (при сопоставлении эволюции ключевых понятий «экономическая безопасность» и «стратегическое развитие», а также при оценке адекватности российских механизмов регулирования международным вызовам); аналитическое обобщение (для формирования теоретической базы исследования на основе изучения трудов отечественных и зарубежных учёных, а также при формулировании выводов и практических рекомендаций); анализ нормативных документов (при оценке адекватности существующих в России механизмов правового и институционального регулирования выявленным вызовам на основе стратегий и федеральных законов).

Использование искусственного интеллекта. Авторы заявляют, что генеративные модели искусственного интеллекта не применялись при подготовке данной рукописи.

Результаты исследования и их обсуждение

В рамках качественного анализа феномена цифровой трансформации, рассматриваемого сквозь призму экономической безопасности и стратегического развития, необходимо строгое определение терминологического базиса и методологического анализа. Теоретическую основу настоящего исследования формируют три ключевые дефиниции, эволюционное изменение которых отражает усложнение социально-экономических процессов на современном этапе.

Категория «экономическая безопасность» претерпела существенную содержательную трансформацию. Классическая интерпретация XX столетия трактовала её, прежде всего, как состояние защищённости национальной хозяйственной системы от внешних и внутренних угроз, акцентируя внимание на таких параметрах, как минимизация импортной зависимости по критически значимым товарам, устойчивость финансового сектора и сбалансированность бюджетной системы. Под влиянием глобализационных процессов и перехода к четвёртому технологическому укладу (Индустрия 4.0) данное понятие приобрело более широкое содержание. Современный подход, рассмотренный в работах ряда исследователей, смещает акцент с сугубо защитных механизмов на обеспечение устойчивости и способности экономической системы к саморазвитию в условиях неопределённости и возникновения ранее не существовавших рисков [3; 6; 9]. Ключевое место в структуре современных вызовов занимают цифровые угрозы – кибератаки, технологические блокады, цифровое неравенство [13; 14; 15]. Следовательно, экономическая безопасность в актуальном понимании представляет собой способность системы адаптироваться к цифровой среде, нейтрализуя её деструктивные эффекты и одновременно используя открывающиеся возможности для укрепления национального суверенитета.

Определение «стратегическое развитие» также подверглось концептуальной эволюции. Исторически сложилась традиция отождествлять её с достижением высоких темпов прироста валового внутреннего продукта (ВВП). Однако практика последних десятилетий показала неустойчивость экстенсивного роста, игнорирующего качественные параметры.

Понятие стратегическое развитие также эволюционировало. Исторически его отождествляли с достижением высоких темпов роста валового внутреннего продукта (ВВП). Однако опыт последних десятилетий показал, что экстенсивный рост без учёта качественных параметров неустойчив. Современная парадигма стратегического развития, закреплённая в том числе в Целях устойчивого развития⁶, предполагает смещение фокуса на качественные показатели: инновационность, технологическое лидерство, человеческий капитал, экологическую и социальную устойчивость. В этом контексте развитие измеряется не только объёмом произведённых товаров и услуг, но и способностью экономики к генерации и внедрению прорывных технологий, обеспечению высокого уровня благосостояния населения и сохранению долгосрочного потенциала роста. Цифровая трансформация выступает в качестве ключевого инструмента достижения указанных целей.

⁶ Цели устойчивого развития. URL: <https://www.ungeneva.org/ru/about/topics/sustainable-development-goals>.

Цифровая трансформация выступает системообразующим процессом, интегрирующим два вышеуказанных понятия. Принципиально значимо, что данная категория не тождественна простому «внедрению информационно-коммуникационных технологий». В отличие от цифровизации, которая ограничивается применением цифровых данных для оптимизации уже сложившихся процессов, цифровая трансформация предполагает глубинное изменение бизнес-моделей, механизмов государственного администрирования, социальных институтов и самих принципов создания добавленной стоимости под воздействием цифровых технологий. Речь идёт о системной реорганизации всех общественных сфер. Анализ современных тенденций позволяет выделить несколько ключевых направлений этого влияния (рисунок 1)⁷.



Рисунок 1 – Направления воздействия цифровой трансформации на стратегические показатели развития национальной экономики

Figure 1 – The directions of the impact of digital transformation on the strategic indicators of the development of the national economy

Внедрение цифровых решений вносит принципиальные изменения в организацию как производственных, так и управленческих процессов. Технологии промышленного интернета вещей обеспечивают непрерывный мониторинг работы оборудования, позволяют прогнозировать сроки проведения регламентных работ и оптимизировать логистические маршруты. Применение методов обработки больших данных и прогнозной аналитики даёт хозяйствующим субъектам возможность более точно определять перспективный рыночный спрос, сокращать складские остатки и выстраивать индивидуализированные коммуникации с клиентами. Искусственный интеллект берёт на себя автоматизацию сложных когнитивных операций – от обработки документации до регулирования режимов функционирования энергетических сетей. В соответствии с исследованиями, широкое внедрение искусственного интеллекта может обеспечить до 45 % общего экономического эффекта от цифровизации в России за счёт роста производства [1].

Динамика роста рынка ИИ в России в 2022-2025 гг., а также прогнозные значения финансирования в 2026-2027 гг. отражены на рисунке 2⁸.

Следует отметить, что цифровая трансформация стимулирует возникновение принципиально новых секторов экономики. Трансформация систем управления данными формирует основу для новых финансовых инструментов и сервисов. Цифровые платформы кардинально меняют традиционные рынки, о чём свидетельствует успешный опыт российских компаний, таких как «Яндекс» (транспорт, такси, доставка) и «Сбер» (экосистема финансовых и нефинансовых услуг). Эти компании не просто цифровизируют

⁷ Национальная программа «Цифровая экономика Российской Федерации».

URL: <https://digital.gov.ru/target/naczionalnaya-programma-czifrovaya-ekonomika-rossijskoj-federaczii>.

⁸ Рынок ИИ в России 2025: \$2.1 млрд и рост 45 % в год. РБК Компании.

URL: <https://companies.rbc.ru/news/247rlzqocb/ryinok-ii-v-rossii-2025-21-mlrd-i-rost-45-v-god/>.

существующие услуги, а создают новую ценность для потребителей, трансформируя целые отрасли. Платформенные решения способствуют развитию малого и среднего предпринимательства, предоставляя им доступ к широкой аудитории и инструментам для ведения бизнеса.

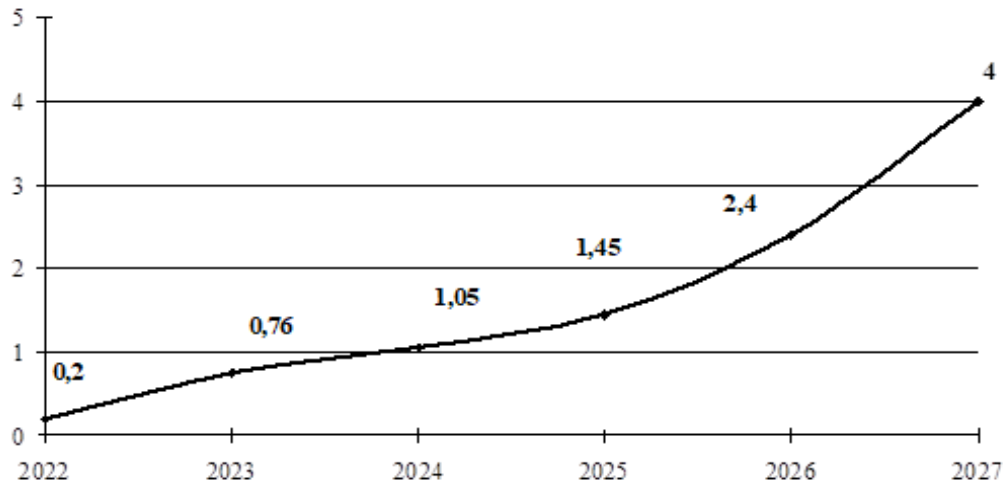


Рисунок 2 – Динамика рынка ИИ в России 2022-2027, млрд долл. США

Figure 2 – Dynamics of AI market growth in Russia 2022-2027, in billion dollars of the USA

Наряду с этим, цифровизация выступает в качестве значимого инструмента повышения результативности функционирования государственных институтов и улучшения качества предоставления публичных услуг. Реализация концепции «цифрового правительства» способствовала заметному сокращению административных барьеров для хозяйствующих субъектов и населения. Наиболее показательным примером служит портал «Госуслуги», выполняющий функции единого окна для доступа к обширному перечню государственных и муниципальных сервисов. Распространение технологий «умного города» – включая интеллектуальные системы управления транспортом, жилищно-коммунальным хозяйством и обеспечением общественной безопасности – оказывает непосредственное воздействие на уровень жизни граждан, что представляет собой один из ключевых индикаторов стратегического развития.

Цифровые технологии радикально сокращают время между фундаментальным исследованием и его коммерциализацией. Виртуальное моделирование, цифровые двойники и технологии быстрого прототипирования ускоряют процессы разработки и тестирования новых продуктов. Одновременно растёт спрос на высококвалифицированных специалистов в области IT, анализа данных и кибербезопасности, что стимулирует инвестиции в образование и переподготовку кадров, способствуя росту человеческого капитала страны [1; 14; 16].

Таким образом, цифровая трансформация выступает мощным катализатором стратегического развития, воздействуя на все его ключевые компоненты: экономический рост, инновационность, качество институтов и человеческий потенциал. Однако для реализации этого потенциала необходима эффективная система управления сопутствующими рисками.

Параллельно с позитивным воздействием, цифровая трансформация порождает комплекс серьёзных вызовов экономической безопасности России. Эти угрозы носят системный характер, взаимосвязаны и способны оказывать дестабилизирующее влияние на всю национальную хозяйственную систему (рисунок 3).

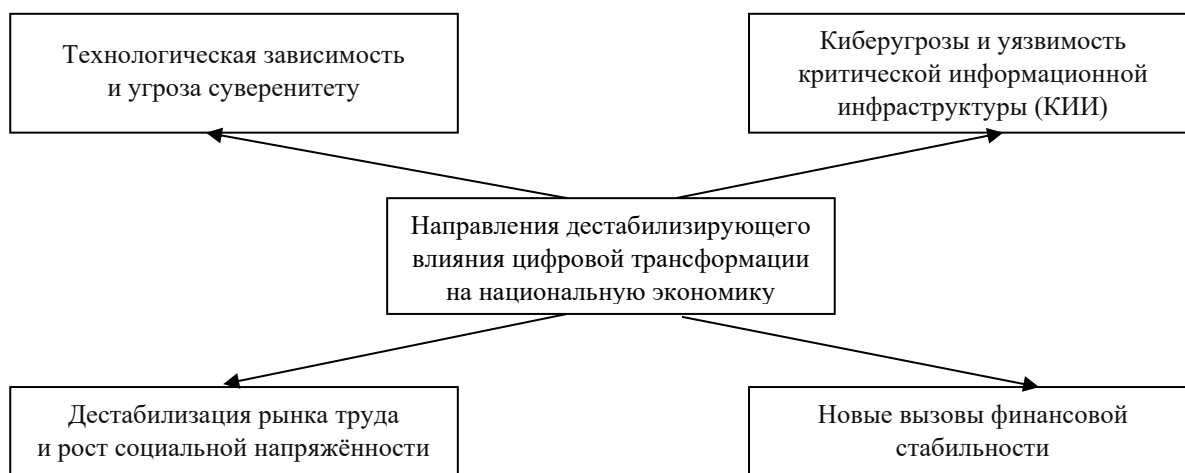


Рисунок 3 – Направления дестабилизирующего влияния цифровой трансформации на национальную экономику

Figure 3 – Directions of the destabilizing effect of digital transformation on the national economy

Наиболее критичным вызовом остаётся высокая зависимость от иностранных технологий, особенно в условиях санкционного давления. Это проявляется на нескольких уровнях [1]:

значительная часть серверного и сетевого оборудования, а также чипов для промышленности имеет иностранное происхождение. Санкции создают риски сбоев в поставках и обслуживании, что угрожает непрерывности бизнес-процессов ключевых отраслей;

доминирование иностранных операционных систем, систем управления предприятиями (ERP, CRM) и инженерного софта создаёт уязвимости. Производитель может дистанционно ограничить доступ к программному обеспечению, как это произошло с приостановкой продаж и поддержки продуктов ряда международных вендоров, что парализует работу компаний;

ускоренное технологическое развитие ведущих стран приводит к углублению разрыва между ними и Россией. Отставание в таких областях, как микроэлектроника, передовая робототехника и квантовые вычисления, может привести к потере конкурентоспособности целых секторов экономики в средне- и долгосрочной перспективе.

По мере цифровизации экономика становится всё более уязвимой для кибератак, масштаб и изощрённость которых постоянно растут [12]:

банки, платёжные системы и фондовый рынок выступают постоянными мишенями для хакерских атак, целью которых является хищение средств, дестабилизация финансовой системы или получение конфиденциальной информации;

результативная атака на ключевые финансовые институты способна вызвать панические настроения и привести к утрате доверия к национальной денежной единице;

наибольшую угрозу несут кибератаки, направленные на объекты энергетики, транспортной инфраструктуры, жилищно-коммунального хозяйства и оборонно-промышленного комплекса. Последствиями подобных действий могут стать не только колоссальные экономические потери из-за остановки производственных процессов, но и прямая опасность для жизни и здоровья граждан, что переводит киберугрозы в разряд вызовов национальной безопасности;

цифровые системы превращаются в канал несанкционированной утечки сведений, составляющих коммерческую и стратегически значимую интеллектуальную собственность, что наносит ущерб инновационному потенциалу государства и ослабляет конкурентные преимущества хозяйствующих субъектов.

Автоматизация технологических и управленческих процессов, внедрение систем искусственного интеллекта влечёт за собой структурные преобразования на рынке труда [1]:

ряд профессий, предполагающих выполнение рутинных физических и умственных операций, оказывается в зоне риска. Указанное обстоятельство создаёт угрозу возникновения массовой структурной безработицы в отдельных отраслях и регионах [15] при отсутствии заблаговременных мер по переподготовке кадров;

повышение спроса на высококвалифицированных специалистов в сфере информационных технологий сопровождается снижением потребности в работниках средней квалификации. Это обостряет социальное неравенство и способно стать источником общественной напряжённости;

распространение платформенной занятости, несмотря на присущую ей гибкость, сопряжено с рисками нестабильности доходов, отсутствием социальных гарантий и размыванием классической модели трудовых отношений [17].

Возникновение цифровых финансовых активов (криптоактивов, стейблкоинов) формирует зоны повышенной непрозрачности и волатильности, которые слабо поддаются регулированию со стороны традиционных финансовых институтов. Это может способствовать оттоку капитала, использованию указанных активов для легализации преступных доходов и финансирования противоправной деятельности, а также образованию «финансовых пузырей» [12].

Перечисленные угрозы не являются изолированными. Технологическая зависимость (угроза 1) повышает уязвимость перед кибератаками (угроза 2), поскольку применяемое импортное оборудование и программное обеспечение потенциально могут содержать недокументированные возможности. В свою очередь, успешная кибератака на объект критической информационной инфраструктуры способна спровоцировать массовые высвобождения персонала (угроза 3) и дестабилизировать ситуацию на финансовом рынке (угроза 4). Следовательно, требуется комплексный, системный подход к нейтрализации данных рисков.

Сложный и системный характер выявленных угроз ставит вопрос о способности действующей системы государственного регулирования адекватно реагировать на них. В Российской Федерации за последние годы сформирован значительный массив нормативных правовых документов и институциональных структур, ориентированных на управление цифровой трансформацией и обеспечение безопасности:

1. Ключевым аспектом выступает нормативно-правовое обеспечение управления процессами цифровизации:

Национальная программа «Цифровая экономика» (обновлённая версия с 2023 г.): определяет стратегические цели по развитию сквозных технологий, инфраструктуры и кадров;

Стратегия экономической безопасности РФ до 2030 года: фиксирует угрозы, связанные с технологической зависимостью и уязвимостью КИИ;

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»: устанавливает требования по защите объектов КИИ;

Концепция развития регулирования цифровых активов и соответствующие законы: создают основу для регулирования цифровых финансов;

2. Сформированы специализированные органы и структуры:

Федеральная служба по техническому и экспортному контролю (ФСТЭК России): отвечает за защиту информации и установление требований к безопасности КИИ;

Федеральная служба безопасности (ФСБ России): противодействует киберугрозам, включая компьютерные атаки;

Министерство цифрового развития, связи и массовых коммуникаций (Минцифры России): отвечает за реализацию политики цифровизации;

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГСОПКА): оперативный контур реагирования на киберинциденты.

Несмотря на прогресс, существующая система регулирования имеет ряд системных проблем:

1. Дисбаланс между целями «развития» и «безопасности». Задачи по ускоренной цифровизации (Минцифры) и по обеспечению безопасности (ФСТЭК, ФСБ) часто реализуются разными ведомствами с разной логикой. Это может приводить к конфликту интересов: требования безопасности воспринимаются как барьер для быстрого внедрения технологий;

2. «Догоняющий» характер регулирования. Правовая база часто формируется постфактум, как реакция на уже возникшие угрозы, что не позволяет создавать упреждающую систему управления рисками в условиях быстро меняющихся технологий;

3. Недостаточная гибкость. Бюрократические процедуры сертификации средств защиты и согласования стандартов не поспевают за скоростью обновления программного обеспечения и появления новых видов киберугроз;

4. Фрагментарность подхода к кадровым рискам. Отсутствует комплексная общегосударственная стратегия опережающей подготовки и переподготовки кадров, которая бы системно решала проблему вытеснения труда и структурной безработицы. Существующие инициативы носят точечный характер;

5. Слабая координация с бизнес-сообществом. Крупные компании, особенно госкомпании, вовлечены в процессы, однако малый и средний бизнес часто остаётся без достаточной методической и финансовой поддержки в вопросах кибербезопасности и импортозамещения, что создаёт «слабые звенья» в общей системе экономической безопасности.

Таким образом, действующая система регулирования демонстрирует способность реагировать на традиционные и уже известные угрозы, но обладает недостаточной гибкостью, проактивностью и системностью для нейтрализации комплексных, эволюционирующих вызовов цифровой эпохи, что указывает на неспособность существующей системы государственного регулирования адекватно отвечать на вызовы цифровой эпохи.

Для преодоления выявленных дисбалансов необходим переход от реактивного (постфактумного) к опережающему управлению, основанному на принципе «безопасность через развитие», который требует не просто ускорения принятия решений, а смены механизмов и инструментов стратегического планирования. Необходим инструмент, позволяющий работать с множественностью будущих состояний системы, а не с единственным прогнозом.

Одним из наиболее адекватных инструментов для оценки реализации опережающего управления в условиях неопределённости, на наш взгляд, является сценарный метод. Это обусловлено множественностью факторов влияния, неподконтрольных национальным регулирующим структурам, многовариантностью сценариев развития событий и неоднозначностью результатов, которые сценарный метод позволяет учесть и предоставить конкретный аналитический аппарат для обоснования предложений.

Анализ и синтез научных работ [1; 6-8] позволил выделить два ключевых направления, пересечение которых формирует четыре сценария долгосрочного развития – от сохранения высокой импортной зависимости до достижения полного технологического суверенитета (технологический суверенитет) и от фрагментированного, реактивного регулирования (дисбаланс между безопасностью и развитием) до интегрированного, опережающего управления на принципе «безопасность через развитие» (качество управления и институциональная гибкость). Матрица сценариев приведена в таблице 1.

Сценарий 1 отвечает реализации предложенного принципа «безопасность через развитие» за счёт создания гибкой системы регулирования (межведомственные рабочие группы, регуляторные песочницы) и достижения высокого уровня технологического суверенитета не через закрытость, а через создание конкурентоспособных отечественных продуктов, интегрированных в мировые экономики других стран (где это возможно).

В данном случае обеспечение безопасности возможно за счёт технологического превосходства и страхования киберрисков. Устранение технологической зависимости может осуществляться за счёт наличия собственных разработок, а не запрета иностранных.

При таком сценарии Россия выступает экспортером цифровых решений (в частности, в области кибербезопасности, ИИ для промышленности, финтех) на рынки стран БРИКС, а также Африки, Азии и Латинской Америки. Цифровая трансформация становится ключевым вектором роста производительности труда, обеспечивая ежегодный прирост ВВП на 1,5-2 % за счёт ИИ и автоматизации.

В социальной сфере при таком варианте реализуется масштабная программа опережающей переподготовки. Структурная безработица нивелируется переходом к

экономике «гибких навыков». Платформенная занятость интегрируется в систему социального обеспечения. Качество госуслуг выходит на принципиально новый уровень.

Таким образом, эффект от реализации данного сценария представляется в виде замкнутого цикла «инвестиции в технологии → рост безопасности → укрепление суверенитета → экспорт компетенций → новые инвестиции».

Таблица 1 – Матрица сценариев обеспечения экономической безопасности через развитие цифровизации
Table 1 – Matrix of scenarios for ensuring economic security through the development of digitalization

	Высокая институциональная гибкость (проактивное управление, синхронизация «развитие-безопасность»)	Низкая институциональная гибкость (реактивное управление, ведомственный дисбаланс)
Высокий технологический суверенитет (дальнейшее развитие механизмов импортозамещения)	СЦЕНАРИЙ 1 «Цифровой лидер» (устойчивое развитие, экспорт технологий, высокое качество жизни, гибкая безопасность)	СЦЕНАРИЙ 2 «Стабильность, но отставание» (относительная стабильность, но изоляция и технологическое отставание в глобальных трендах)
Низкий технологический суверенитет (зависимость от импорта, санкционное давление)	СЦЕНАРИЙ 3 «Адаптивное равновесие» (нестабильность, высокая эффективность в отдельных сегментах, но постоянный поиск компромиссов с внешними партнёрами)	СЦЕНАРИЙ 4 «Уязвимая зависимость» (стагнация, высокая уязвимость критической информационной инфраструктуры, социальное расслоение, риск «цифрового коллапса»)

Реализация сценария 2 предполагает успешное импортозамещение (микроэлектроника, ПО, оборудование, созданное внутри страны), но при сохранении жёсткого, фрагментированного регулирования, что предполагает доминирование ведомств ФСТЭК, ФСБ над ведомствами развития (Минцифры). Принцип «безопасность» подавляет принцип «развитие».

Последствиями такого сценария могут быть:

1. Высокий уровень защищённости критической информационной инфраструктуры, минимизация рисков внешних кибератак и санкционного отключения. При этом обеспечение безопасности возможно посредством огромных бюджетных затрат на поддержание закрытых технологических цепочек;

2. Низкие темпы инноваций из-за отсутствия международной кооперации и ограниченного доступа к глобальным знаниям. Отечественные технологии часто уступают мировым лидерам по функциональности (эффект «догоняющего развития без лидерства»). Рынок информационных технологий становится высоко монополизированным и ориентированным на госзаказ;

3. Сохранение цифрового разрыва между крупными городами (где сосредоточены ресурсы) и регионами. Рынок труда стабилен, но наблюдается отток наиболее талантливых специалистов, не желающих работать в условиях жёсткой регуляторной политики и изоляции;

4. Технологическая стагнация, потеря конкурентоспособности в глобальном масштабе, превращение цифровой среды из инструмента развития в инструмент контроля, что может привести к снижению деловой активности.

При сохранении высокой внешней зависимости (сценарий 3) возникает вынужденная гибкость управления. При реализации данного сценария государство отказывается от жёсткого вертикального контроля в пользу более гибких механизмов, чтобы выжить. Регуляторные песочницы и послабления вводятся не как стратегия развития, а как антикризисные меры.

Последствиями реализации сценария 3 могут стать:

1. Ситуация «управляемого хаоса», при которой безопасность обеспечивается точно – для крупнейших госкорпораций, в то время как средний и малый бизнес предоставлен сам себе и несёт высокие потери от киберпреступности;

2. Разрыв в стратегическом развитии государственного сектора и отдельных частных субъектов (экосистем). В то время как частные экосистемы (банки, маркетплейсы, технологические компании) внедряют передовые решения и формируют новые стандарты взаимодействия, государство остаётся в технологическом прошлом, что снижает качество государственного управления и доверие к нему;

3. Разрыв в цифровой трансформации государственного сектора и частного бизнеса может привести к нарастанию социальной напряжённости вследствие регуляторных барьеров первого и более гибкого, но лишённого социальных гарантий, второго участника отношений («андеркласс») [18];

4. Постоянная турбулентность, отсутствие долгосрочных ориентиров для инвестиций. Невозможность реализации крупных инфраструктурных цифровых проектов из-за несогласованности требований безопасности и условий принятия решений.

Сценарий 4 является наиболее негативным сценарием, в основе которого сохранение импортозависимости (особенно в микроэлектронике и станкостроении) в сочетании с бюрократизацией и конфликтом ведомств. Регулирование остаётся «догоняющим», а координация между Минцифры и силовым блоком отсутствует.

Последствиями реализации такого подхода могут стать:

1. Невозможность обновления критически важной инфраструктуры из-за санкций и отсутствия отечественных аналогов высокой степени сложности. Рост числа успешных кибератак на финансовый сектор и КИИ (энергетика, транспорт) из-за использования устаревшего оборудования;

2. Деиндустриализация цифрового сектора. Рост издержек бизнеса на импортозамещение без ощутимого экономического эффекта и попытки адаптировать иностранный софт под российские реалии без поддержки вендоров. Нарастание технологического отставания;

3. Резкий рост безработицы в сегменте «белых воротничков» (бухгалтеры, операторы, переводчики) из-за автоматизации при отсутствии системы переобучения. Усиление социального неравенства: специалисты сферы информационных технологий, менеджеры ВЭД могут иметь сверхдоходы, тогда как остальные теряют работу;

4. Вероятность отказа оборудования, приводящего к остановке энергоснабжения или банковской системы на федеральном уровне, после чего экономическая безопасность требует уже не регулирования, а чрезвычайного восстановления.

Проведённый анализ показывает, что достижение состояния Сценария 1 («Цифровой лидер») является наиболее предпочтительным с точки зрения стратегического развития и экономической безопасности.

Однако достижение Сценария 1 невозможно без преодоления институционального дисбаланса. Если государственное управление будет демонстрировать жёсткую вертикаль без координации либо хаотичную адаптацию, долгосрочным последствием цифровизации станет либо технологическая стагнация, либо накопление критических уязвимостей, способных привести к системному кризису.

Рассмотренные сценарии подтверждают необходимость перехода к опережающей модели управления по принципу «безопасность через развитие» как единственному условию реализации позитивного долгосрочного прогноза, внедрение которого возможно за счёт как развития существующих, так и внедрения новых инструментов и механизмов, среди которых:

1. Развитие национальной технологической экосистемы (снижение зависимости) [19; 20]:

стимулирование венчурных инвестиций, что предполагает создание фондов с государственным участием, специализирующихся на глубокотехнологичных стартапах (микроэлектроника, отечественное ПО, кибербезопасность);

расширение инструмента «регуляторные песочницы» для тестирования не только финансовых, но и промышленных, медицинских и транспортных технологий в условиях смягченного регулирования, но с обязательным встроенным контролем безопасности;

введение обязательной оценки доли иностранных компонентов и наличия отечественных аналогов при закупках технологий для госсектора и компаний с госучастием.

Отдельного внимания заслуживают экспериментальные правовые режимы (ЭПР), введённые Федеральным законом № 258-ФЗ⁹. Данный инструмент представляет собой уникальное регуляторное решение, позволяющее не только апробировать технологии в условиях изолированной «регуляторной песочницы», но и временно приостанавливать действие общих нормативных предписаний на определённой территории либо в отношении конкретного круга лиц. Вместе с тем в настоящее время сфера применения ЭПР ограничена преимущественно финансовым сектором [19; 20].

Распространение этого механизма на другие области – внедрение ИИ на объектах критической информационной инфраструктуры, использование отечественных решений без сертификации по устаревшим стандартам, тестирование новых моделей социального страхования для платформенной занятости – позволит преодолеть жёсткость регулирования на практике, а не в декларациях. Для этого необходимо создать единого оператора ЭПР при Министерстве экономического развития с участием Минцифры, ФСТЭК и ФСБ. Оператор должен быть наделён полномочиями по ускоренному межведомственному принятию решений. Это сократит сроки согласования с текущих 6-12 месяцев до 30-45 дней и обеспечит оперативную реакцию на технологические изменения.

2. Совершенствование системы управления киберрисками (повышение устойчивости):

развитие рынка страхования киберрисков для субъектов предпринимательской деятельности, что позволит стимулировать компании к вложению средств в защитные механизмы и сформирует финансовый резерв на случай возникновения инцидентов;

законодательное закрепление требования о встраивании средств защиты информации на этапе проектирования, а не после внедрения цифровых продуктов и сервисов, – в особенности для объектов критической информационной инфраструктуры;

формирование отраслевых центров мониторинга, а также площадок для обмена сведениями о киберугрозах между государственными структурами и бизнесом в целях организации коллективного противодействия.

Существенным препятствием для развития рыночного страхования киберугроз выступает вероятность наступления «киберкатастроф» – событий, размер ущерба от которых способен достичь масштабов, создающих угрозу финансовой устойчивости частных страховых организаций. В связи с этим обоснованным представляется создание специализированного государственного фонда перестрахования, действующего по принципу Агентства по страхованию вкладов. Такой механизм позволит распределять крупные риски между государством и рынком. При этом обязательным условием участия в данной системе должно стать наличие у компании подтверждённого по итогам независимого аудита статуса и использование механизмов защиты, интегрированных на стадии внедрения цифровых систем.

3. Формирование кадрового потенциала будущего (смягчение социальных рисков):

запуск масштабной программы опережающей переподготовки кадров для профессий, находящихся в зоне риска автоматизации, с фокусом на развитие цифровой грамотности и «гибких навыков» (soft skills);

введение базовых модулей по цифровой гигиене и основам кибербезопасности в программы высшего и среднего профессионального образования для всех технических и экономических специальностей.

Программы переподготовки кадров останутся малоэффективными, если не привязать их к реальному спросу экономики. Одним из вариантов решения может стать механизм образовательных сертификатов, который предполагает оплату обучения государством после подтверждения трудоустройства по полученной специальности выпускником¹⁰. Данный механизм направлен на стимулирование учебных заведений в подготовке востребованных специалистов и прогнозирование кадровых потребностей на основе реальных данных.

⁹ Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации». URL: <http://www.kremlin.ru/acts/bank/45796>.

¹⁰ Проект Постановления Правительства Российской Федерации «О проведении в 2022-2024 годах эксперимента по приёму на обучение и обучению студентов по образовательным программам высшего образования за счёт бюджетных ассигнований федерального бюджета на основе предоставления образовательных сертификатов». URL: https://fgosvo.ru/files/files/Project_experiment_budget_study.pdf.

4. Создание гибкой и скоординированной системы регулирования:

формирование при Аппарате Правительства РФ постоянных межведомственных рабочих групп (Минцифры, ФСТЭК, ФСБ, Минэкономразвития, бизнес) для синхронизации политики развития и безопасности на этапе формирования инициатив;

дифференциация регуляторных требований к компаниям в зависимости от их значимости для экономики и уровня потенциального ущерба от киберинцидента.

Наряду с формированием межведомственных рабочих групп при Аппарате Правительства считаем целесообразным также предложить создание при Президенте или Председателе Правительства постоянно действующего Совета по технологическому регулированию, в состав которого должны входить не только руководители заинтересованных ведомств, но и представители бизнеса, технологического сообщества и экспертного сообщества. Причём решения этого Совета должны приниматься в ограниченные сроки и быть обязательными для всех органов исполнительной власти. Это позволит преодолеть институциональный дисбаланс.

Реализация предложенных мер позволит не просто минимизировать угрозы, но и трансформировать их в импульс для развития, создавая замкнутый цикл: стимулирование отечественных технологий → повышение безопасности → укрепление суверенитета → дальнейшее развитие.

Выводы

Проведённое исследование подтвердило исходный тезис о двойственной природе цифровой трансформации, которая выступает одновременно как ключевой фактор стратегического развития и как источник системных вызовов экономической безопасности России.

1. Необратимость и стратегическая значимость цифровой трансформации требуют пересмотра традиционных подходов к экономической безопасности. Безопасность должна пониматься не как статичная защита, а как динамическая способность экономической системы к устойчивому развитию в условиях цифровых рисков и высокой неопределённости.

2. Угрозы носят комплексный и взаимообусловленный характер. Технологическая зависимость, уязвимость объектов критической информационной инфраструктуры, дестабилизация рынка труда и риски финансовой сферы взаимно усиливают друг друга, порождая синергетический эффект. Это обуславливает необходимость выработки комплексного, а не отраслевого подхода к управлению данными угрозами.

3. Сложившаяся система государственного регулирования, несмотря на свою развитую институциональную и нормативную базу, содержит существенные пробелы. К числу ключевых проблем относятся дисбаланс между политикой развития и политикой безопасности, «догоняющий» характер нормотворческой деятельности, а также недостаточная степень координации между органами государственной власти и бизнес-сообществом.

4. Эффективная стратегия должна основываться на принципе «безопасность через развитие». Предложенный комплекс мер, включающий стимулирование формирования национальной технологической экосистемы, совершенствование механизмов управления киберрисками, опережающую подготовку кадров и создание гибких регуляторных инструментов, направлен на построение проактивной модели управления, позволяющей трансформировать вызовы в возможности для укрепления технологического суверенитета.

Список источников / References

1. Ларина Е. Б., Орехова Е. А. Цифровизация как фактор повышения конкурентоспособности национальной экономики на мировых рынках // Вестник Саратовского государственного социально-экономического университета. 2019. № 2(76). С. 29-34. [Larina, E. B., & Orekhova, E. A. (2019). Digitalization as a factor in increasing the competitiveness of the national economy in world markets. *Bulletin of the Saratov State Socio-Economic University*, 2(76), 29–34. (In Russian)] EDN: FIVRQC.

2. Глазьев С. Ю. О вызовах экономическому развитию России и ЕАЭС в условиях структурных изменений Мир-Системы // Век глобализации. 2024. № 4(52). С. 3-19. [Glazeyev, S. Yu. (2024). On the challenges to the economic development of Russia and the EAEU in the context of structural changes in the World System. *Century of Globalization*, 4(52), 3–19. (In Russian)] <https://doi.org/10.30884/vglob/2024.04.01>.

3. Глазьев С. Ю., Косакян Д. Л. О развитии нового технологического уклада в экономике России в сравнении с передовыми странами // Российский экономический журнал. 2025. № 4. С. 63-85. [Glazyev, S. Yu., & Kosakyan, D. L. (2025). On the development of a new technological structure in the Russian economy in comparison with advanced countries. *Russian Economic Journal*, 4, 63–85. (In Russian)] https://doi.org/10.52210/0130-9757_2025_4_63.
4. Еленева Ю. Я., Малкова Т. Б., Андреев В. Н., Лукина С. В., Ван Х. Развитие цифровой экономики как условие повышения конкурентоспособности предприятия // Российский экономический интернет-журнал. 2022. № 4. Порядковый номер: 11. [Eleneva, Yu. Ya., Malkova, T. B., Andreev, V. N., Lukina, S. V., & Van, H. (2022). The development of the digital economy as a condition for increasing the competitiveness of the enterprise. *Russian Economic Online Journal*, 4, Article 11. (In Russian)] EDN: JQBXTD.
5. Гао Муян. Цифровая трансформация в обеспечении экономической безопасности государства: автореф. на соиск. ученой степ. канд. экон. наук: 5.2.3 – Региональная и отраслевая экономика (экономическая безопасность) М., 2025. 31 с. [Gao, Muyan. (2025). *Digital transformation in ensuring the economic security of the state* (PhD Thesis). Moscow, 31 p. (In Russian)] URL: <https://dissovet.msu.ru/dissertation/3444>.
6. Экономическая безопасность в условиях цифровой трансформации России: монография / под ред. Малкиной М. Ю., Захарова В. Я. Москва: Русайнс, 2022. 267 с. [Malkina, M. Yu., & Zakharov, V. Ya. (Eds.) (2022). *Economic security in the context of Russia's digital transformation*. Moscow: Rusains, 267 p. (In Russian)] ISBN 978-5-4365-9123-0. URL: <https://book.ru/book/943461>.
7. Экономическая безопасность России: теоретическое обоснование и методы регулирования: монография / под общ. ред. А. Е. Городецкого, И. В. Караваевой. Москва: Институт экономики РАН, 2023. 361 с. [Gorodetsky, A. E., & Karavaeva, I. V. (Eds.) (2023). *Economic security of Russia: theoretical justification and methods of regulation*. Moscow: Institute of Economics of the Russian Academy of Sciences, 361 p. (In Russian)] URL: https://inecon.org/docs/2023/Gorodetsky_Karaeva_book_2023.pdf.
8. Кузнецова М. В. Механизм повышения экономической безопасности на основе инновационных и цифровых преобразований в экономике: дис. ... канд. экон. наук: 08.00.05. М., 2022. 125 с. [Kuznetsova, M. V. (2022). *The mechanism of increasing economic security based on innovative and digital transformations in the economy* (PhD Dissertation). Moscow, 125 p. (In Russian)] URL: https://diss.vlsu.ru/uploads/media/Dissertacija_Kuznecova_Marija_Vladimirovna.pdf.
9. Грачёв А. В., Сикорская Л. В. Взаимосвязь процессов цифровизации экономики и экономической безопасности страны // Известия высших учебных заведений. Серия: Экономика, финансы и управление производством. 2023. № 3(57). С. 35-44. [Grachev, A. V., & Sikorskaya, L. V. (2023). The relationship between the processes of digitalization of the economy and the economic security of the country. *News of higher educational institutions. Series: Economics, Finance and Production Management*, 3(57), 35–44. (In Russian)] <https://doi.org/10.6060/ivecofin.2023573.652>.
10. Гудкова О. В. Риски и угрозы экономической безопасности России в условиях цифровизации экономики // Известия высших учебных заведений. Серия: Экономика, финансы и управление производством. 2022. № 1(51). С. 73-80. [Gudkova, O. V. (2022). Risks and threats to Russia's economic security in the context of the digitalization of the economy. *News of higher educational institutions. Series: Economics, Finance and Production Management*, 1(51), 73–80. (In Russian)] <https://doi.org/10.6060/ivecofin.2022511.587>.
11. Янковская Е. С. Цифровизация и технологический суверенитет России // Учёные записки Санкт-Петербургского имени В. Б. Бобкова филиала Российской таможенной академии. 2023. № 1(85). С. 81-85. [Yankovskaya, E. S. (2023). Digitalization and technological sovereignty of Russia. *Scientific notes of the St. Petersburg named after V. B. Bobkov branch of the Russian Customs Academy*, 1(85), 81–85. (In Russian)] EDN: ILNMUM.
12. Зевелева Е. А., Кокунов К. А. Информационный суверенитет России в эпоху цифровых технологий // Человек. Общество. Инклюзия. 2024. Т. 15, № 2(58). С. 89-96. [Zeveleva, E. A., & Kokunov, K. A. (2024). Information sovereignty of Russia in the era of digital technologies. *Human. Society. Inclusion*, 15(2-58), 89–96. (In Russian)] EDN: KNWNRZ.
13. Медведев В. В. Роль цифрового стратегического планирования в государственном регулировании экономики // Вопросы современной науки и практики. Университет им. В.И. Вернадского. 2024. № 2(92). С. 88-105. [Medvedev, V. V. (2024). The role of digital strategic planning in state regulation of the economy. *Issues of Modern Science and Practice. V.I. Vernadsky University*, 2(92), 88–105. (In Russian)] <https://doi.org/10.17277/voprosy.2024.02.pp.088-105>.
14. Экономическая безопасность в эпоху цифровизации: вызовы, риски и стратегии устойчивого развития: монография / И. С. Ферова, С. А. Козлова, Е. А. Осадченко, Н. Н. Подтихова. М.: Русайнс,

2025. 209 с. [Ferova, I. S., Kozlova, S. A., Osadchenko, E. A., & Podtikhova, N. N. (2025). *Economic security in the era of digitalization: challenges, risks and strategies for sustainable development*. Moscow: Rusains, 209 p. (In Russian)] ISBN 978-5-466-10604-6. URL: <https://book.ru/book/960599>.

15. Носкин С. А. Механизмы обеспечения экономической безопасности региона в условиях цифровых преобразований: автореф. на соиск. ученой степ. канд. экон. наук: 08.00.05 – Экономика и управление народным хозяйством (экономическая безопасность) С.-Пб., 2022. 23 с. [Noskin, S. A. (2022). *Mechanisms for ensuring the economic security of the region in the context of digital transformations*: (PhD Thesis). Saint-Petersburg, 23 p. (In Russian)] URL: <https://unecon.ru/sites/default/files/d07noskinsa.pdf>.

16. Цифровая экономика: 2025: краткий статистический сборник / В.Л. Абашкин [и др.]. Нац. исслед. ун-т «Высшая школа экономики». Москва: ИСИЭЗ ВШЭ, 2025. 120 с. [Abashkin, V. L. [et al.] (2025). *Digital Economy: 2025: a short statistical collection*. National research. University of Higher School of Economics. Moscow: ISIEZ HSE, 120 p. (In Russian)] ISBN 978-5-7598-3025-2. URL: <https://issek.hse.ru/mirror/pubs/share/995751983.pdf>.

17. Парфенов Д. А. Развитие механизма обеспечения экономической безопасности в РФ в условиях цифровизации // Вестник Московского университета. Серия 21. Управление (государство и общество). 2020. № 4. С. 106-122. [Parfenov, D. A. (2020). Development of the mechanism for ensuring economic security in the Russian Federation in the context of digitalization. *Bulletin of the Moscow University. Series 21. Management (State and Society)*, 4, 106–122. (In Russian)] URL: http://vestnik21msu.ru/upload/iblock/ba2/noaddfuvvs2uvvon8dmpx7ckossn2gwo/Ser_21_2020_4_Text_106_122.pdf.

18. Батуренко С. А. Исследования андеркласса в современном российском обществе: основные методологические подходы // Вестник Московского университета. Серия 18. Социология и политология. 2011. № 1. С. 44-52. [Baturenko, S. A. (2011). Underclass research in modern Russian society: basic methodological approaches. *Bulletin of the Moscow University. Series 18. Sociology and Political Science*, 1, 44–52. (In Russian)] EDN: NTLGKP.

19. Понкин И. В., Куприяновский В. П., Понкин Д. И. Fintech, Regtech и регуляторные песочницы: понятие, цифровая онтология, перспективы // Современные информационные технологии и ИТ-образование. 2020. Т. 16, № 1. С. 224-234. [Ponkin, I. V., Kupriyanovsky, V. P., & Ponkin, D. I. (2020). Fintech, Regtech and regulatory sandboxes: concept, digital ontology, prospects. *Modern Information Technologies and IT Education*, 16(1), 224–234. (In Russian)] <https://doi.org/10.25559/SITITO.16.202001.224-234>.

20. Волков А. М. Регуляторные песочницы как инструмент цифровой экономики: российская и зарубежные модели // Право и бизнес. 2025. № 4. С. 19-25. [Volkov, A. M. (2025). Regulatory sandboxes as a tool of the digital economy: Russian and foreign models. *Law and Business*, 4, 19–25. (In Russian)] <https://doi.org/10.18572/2712-8865-2025-4-19-25>.

Информация об авторах

О. Н. Николаева – кандидат наук по государственному управлению, доцент, доцент кафедры менеджмента внешнеэкономической деятельности Донецкого филиала РАНХиГС;

М. В. Гончарова – кандидат экономических наук, доцент, доцент кафедры менеджмента внешнеэкономической деятельности Донецкого филиала РАНХиГС.

Information about the authors

O. N. Nikolaeva – PhD in Public Administration, Associate Professor, Associate Professor of the Department of Foreign Economic Activity Management, Donetsk Branch of RANEPa;

M. V. Goncharova – PhD in Economics, Associate Professor, Associate Professor of the Department of Foreign Economic Activity Management, Donetsk Branch of RANEPa.

Вклад авторов: авторы сделали эквивалентный вклад в подготовку публикации.

Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article.

The authors declare no conflicts of interests.

Статья поступила в редакцию 26.11.2025; одобрена после рецензирования 29.04.2026; принята к публикации 09.06.2026.

The article was submitted 11/26/2025; approved after reviewing 04/29/2026; accepted for publication 06/09/2026.