УДК 338.14

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ И НОВЫЕ УГРОЗЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Селезнева Е.Ю.

к.э.н., доцент,

Вятский государственный университет,

Киров, Россия

Валова Н.А.

студент 4 курса,

Вятский государственный университет,

Киров, Россия

Опарина Э.Н.

студент 4 курса,

Вятский государственный университет,

Киров, Россия

Прозорова С.С.

студент 4 курса,

Вятский государственный университет,

Киров, Россия

Аннотация

В статье исследуется влияние цифровой трансформации на экономическую безопасность Российской Федерации. Целью работы является выявление и систематизация новых угроз, возникающих в процессе цифровизации национальной экономики. Продемонстрирована двойственная природа цифровой трансформации: она выступает драйвером технологического

суверенитета, но одновременно формирует комплекс киберугроз, рисков утечки данных, социально-экономических диспропорций и операционных рисков. Сделан вывод, что экономическая безопасность в цифровую эпоху трансформируется в динамическую адаптивную способность, обеспечиваемую встраиванием защиты на этапе разработки цифровых решений, развитием отечественных технологий и повышением цифровой грамотности специалистов.

Ключевые слова: цифровая трансформация, экономическая безопасность, киберугрозы, технологический суверенитет, управление рисками, цифровизация экономики.

DIGITAL TRANSFORMATION AND NEW THREATS TO ECONOMIC SECURITY

Selezneva E.Yu.
Candidate of Economic Sciences, Associate Professor,
Vyatka State University,
Kirov, Russia

Valova N.A.
4th year student,
Vyatka State University,
Kirov, Russia

Oparina E.N.
4th year student,
Vyatka State University,
Kirov, Russia

Prozorova S.S.
4th year student,
Vyatka State University,
Kirov, Russia

Abstract

The article examines the impact of digital transformation on the economic security of the Russian Federation. The purpose of the work is to identify and systematize new threats that arise during the digitalization of the national economy. The article demonstrates the dual nature of digital transformation: it acts as a driver of technological sovereignty, but at the same time it creates a complex of cyber threats, data leakage risks, socio-economic imbalances, and operational risks. It is concluded that economic security in the digital era is transforming into a dynamic adaptive capacity, which is ensured by embedding protection at the stage of digital solutions development, developing domestic technologies, and increasing the digital literacy of specialists.

Keywords: digital transformation, economic security, cyber threats, technological sovereignty, risk management, and digitalization of the economy.

Цифровая трансформация экономики порождает двойственное явление: наряду с расширением горизонтов для экономического развития, совершенствования операционной деятельности и укрепления рыночных позиций, она одновременно генерирует многоаспектные риски для экономической безопасности, что обуславливает необходимость комплексного исследования и стратегического управления.

Цифровая трансформация в Российской Федерации закреплена в качестве национальной цели развития Указом Президента РФ № 309 (2024), определяющим её как фундаментальное изменение государственного

управления, экономики и социальной сферы на основе внедрения отечественных цифровых технологий [7]. В России это не просто автоматизация, а стратегический шаг к построению цифровой экосистемы, которая гарантирует технологический суверенитет и конкурентоспособность страны перед лицом глобальных угроз. В рамках национальной цели «Цифровая трансформация» 88 регионов утвердили программы цифровой трансформации на период 2026–2028 годов [8].

В настоящее время отсутствует единое, общепризнанное определение термина "цифровая трансформация" в международных нормативных актах и национальном законодательстве. Данное понятие, как правило, интерпретируется в широком смысле, что приводит к вариативности его трактовок в зависимости от контекста. Цифровая трансформация - это недавний термин, описывающий экономические и социальные изменения, вызванные цифровыми инновациями. Он применяется для совершенствования управления через цифровые технологии. Например, Рузина Е.И утверждает, что Цифровая трансформация рассматривается как процесс изменения стратегии, процессов, бизнес-модели и включает в себя цифровизацию (в разрезе использования цифровых технологий) [5]. Шелепаева А.Х называет цифровую трансформацию тенденцией, которая изменяет все аспекты жизнедеятельности человека [9]. Основываясь на анализе отечественных и зарубежных исследований, Темников А.О. формулирует собственное определение: цифровая трансформация - это процесс кардинального изменения бизнес-модели предприятия и её элементов, включая процесс создания и доставки ценности клиенту посредством реализации проектов с использованием цифровых технологий, в основе которых лежит эффективное управление информацией [6].

В современной России экономическая безопасность и цифровая трансформация тесно взаимосвязаны, образуя неразрывное единство. Цифровизация, с одной стороны, служит мощным инструментом для усиления экономической стабильности, а с другой – порождает новые комплексные

угрозы, которые заставляют пересматривать устоявшиеся методы защиты национальных экономических интересов.

Когда экономика становится цифровой, возникают новые угрозы для ее безопасности. Это происходит потому, что меняется всё: как мы ведём дела, какие технологии используем и как создаём что-то ценное. Цифровая трансформация – это не просто добавление новых инструментов, а полное переосмысление того, как устроена экономика, что, конечно же, создаёт новые слабые места и опасности.

Киберугрозы и вопросы информационной безопасности являются наиболее явными и быстрорастущими рисками. Увеличение числа целенаправленных атак на критически важные информационные объекты ставит под угрозу стабильность национальной экономики, так как их нарушение может остановить ключевые экономические процессы. Утечки данных, промышленный шпионаж и несанкционированный доступ к коммерческой информации не только приводят к прямым финансовым потерям, но и подрывают доверие к цифровым сервисам. Это замедляет цифровую трансформацию бизнеса и общества, снижая в долгосрочной перспективе эффективность национальных цифровых проектов.

Цифровая трансформация несёт в себе социально-экономические угрозы. Автоматизация и искусственный интеллект могут привести к массовой потере рабочих мест, вызывая структурную безработицу и социальные конфликты, если не будет создана эффективная система переобучения. Кроме того, углубляющееся цифровое неравенство между регионами и группами населения грозит расколом единого цифрового пространства страны и тормозит развитие национальных цифровых проектов, так как многие люди остаются в стороне от создания и использования цифровых благ. Кроме того, существует реальная угроза исчезновения целого ряда профессий, сред которых сейчас называют секретарей, копирайтеров, редакторов, бухгалтеров, страховых агентов, экскурсоводов. Среди теряющих актуальность рабочих профессий можно

отметить труд почтальонов, лифтеров, охранников, грузчиков, инспекторов ДПС, шахтеров. В настоящее время в перечисленных профессиях трудятся десятки и сотни тысяч людей, поэтому утрата потребности в их труде, безусловно, представляет большую проблему для экономической безопасности [4]. Необходим переход к более гибкой системе подготовки кадров, адаптации образовательных программ к современным реалиям быстро трансформирующегося рынка труда [1].

Стратегические и операционные угрозы проявляются на уровне отдельных организаций и отраслей: невозможность реализации бизнес-стратегий из-за недостаточной цифровой зрелости, уязвимость сетевой инфраструктуры, сбои в производственных процессах, искажение финансовой отчётности и несоответствие быстро меняющимся регуляторным требованиям формируют многоуровневую систему рисков, способных дестабилизировать как отдельные предприятия, так и целые сектора экономики. Плохо разработанные цифровые технологии могут увеличить ошибки обработки. Неэффективные процедуры надзора могут привести к эксплуатационным сбоям. Входные данные, представленные разработчиками для обучения алгоритмов, используемых для цифровых технологий, могут быть устаревшими. Распространение инновационных продуктов и цифровых сервисов может увеличить сложность предоставления финансовых услуг, что затрудняет управление и контроль операционного риска [2].

В России наблюдается стремительный прогресс в области цифровой трансформации, однако это сопряжено с увеличением уязвимости к киберугрозам. В 2025 году в России было зафиксировано 9,3 млн случаев кибератак, затронувших 38,5 тыс. организаций [3]. Обеспечение экономической безопасности в условиях цифровизации предполагает не только оперативное реагирование на инциденты, но и активное создание надёжной экосистемы, в которой технологическое развитие, нормативно-правовое регулирование и подготовка специалистов идут в ногу.

Цифровая трансформация реального сектора превращает традиционную промышленность, логистику и сельское хозяйство в саморегулирующиеся интеллектуальные экосистемы. Предиктивная аналитика и промышленный интернет вещей позволяют прогнозировать аварии за недели, сокращая внеплановые простои на 30–50%, а умные системы управления энергией экономят до четверти ресурсов. Благодаря цифровым двойникам и компьютерному зрению заводы перенесли тестирование и контроль качества в виртуальную среду, отбраковывая 99,9% дефектов на лету и мгновенно перестраивая конвейеры под индивидуальные заказы без потери темпов. Цепочки поставок обрели сквозную прозрачность, точное земледелие подняло урожайность на 40%, одновременно снизив расход агрохимии на треть, а адаптивная логистика и складская роботизация сократили необходимость ручных перемещений в десятки раз. Однако технологический скачок породил и системные уязвимости: физическая инфраструктура стала столь же мишенью для кибератак, как и IT-сектор. Рынок столкнулся с острым дефицитом кадров, вынуждая предприятия переучивать до половины персонала и искать редких специалистов на стыке инженерии и цифровых компетенций. Переход на облачные платформы и подписочные модели ПО стирает грань между владением и арендой оборудования, превращая заводы в зависимых арендаторов, а колоссальные затраты на цифровизацию ускоряют отраслевое расслоение: крупные корпорации наращивают эффективность, тогда как малый и средний бизнес, лишённый ресурсов для трансформации, стремительно теряет конкурентные позиции и рынки сбыта.

В таблице 1 рассмотрим классификацию экономических рисков, которая иллюстрирует двойственный эффект цифровой трансформации: наряду с измеримыми экономическими выгодами (рост производительности, оптимизация логистики и запасов) фиксируется опережающая динамика системных рисков - киберугроз и структурного дефицита кадров. Данные

отражают усреднённые отраслевые оценки и служат основой для баланса между эффективностью и устойчивостью при внедрении технологий.

Таблица 1 - Классификация экономических рисков [12]

Показатель	Эффект от цифровой трансформации	Источник
Рост производительности труда в обрабатывающей промышленности	+4-7% в год (против 1-2% без ЦТ)	McKinsey, 2023 [12]
Снижение логистических издержек	-15-25%	DHL, Tech Report [10]
Сокращение запасов сырья/незавершенки	-20-35% (JIT 4.0)	Siemens [13]
Рост киберинцидентов в промышленности	+300% за 5 лет (целенаправленные атаки)	Kaspersky ICS CERT [11]
Доля рабочих мест, требующих цифровых навыков в промышленности	С 12% (2015) до 58% (2025)	Всемирный банк [14]

Цифровизация, обеспечивая операционную эффективность, одновременно формирует принципиально новый ландшафт угроз экономической безопасности. Киберриски трансформировались из точечных инцидентов в системный вызов: атаки на промышленные системы управления способны провоцировать реальные техногенные аварии, а целевые удары по энерго- и нефтегазовому сектору, авиации и финансам потенциально угрожают экономике потерями до 5,3 трлн рублей (~2,7% ВВП). Особую опасность представляют атаки на цепочки поставок, когда доступ к критической инфраструктуре открывается через уязвимости подрядчиков. Параллельно усиливается скрытая угроза технологической зависимости: события 2022 года продемонстрировали риски отключения от зарубежных платформ, сделав цифровой суверенитет - способность обеспечивать работу экономики собственными технологиями - стратегическим приоритетом, в котором Россия входит в число мировых лидеров. Однако даже суверенные решения не снимают кадровый вызов: дефицит специалистов, способных эксплуатировать и защищать сложные системы, и растущий разрыв между «оцифрованными»

корпорациями и малым бизнесом формируют новые структурные диспропорции. Искусственный интеллект усугубляет эту двойственность: он одновременно усиливает защиту и вооружает злоумышленников инструментами для поиска уязвимостей в режиме, недоступном человеку. Тем не менее, парадоксальным образом именно цифровые технологии становятся ключом к устойчивости: сквозная прозрачность цепочек поставок, предиктивная аналитика и цифровые двойники позволяют не только выявлять угрозы в реальном времени, но и превращают киберустойчивость из опции в условие выживания организации в нестабильной среде.

Цифровая трансформация переписывает правила игры в реальном секторе: на смену планово-реактивному управлению приходит предиктивная экономика, где данные, IoT и алгоритмы позволяют предсказывать сбои, адаптировать логистику на лету и выпускать персонализированный продукт без потери масштаба. Ключевой тренд - переход от продажи «железа» к монетизации результата: клиент платит не за станок, а за обработанную деталь, не за двигатель, а за налёт в час. В таблице 5 - пять сдвигов, которые превращают традиционные отрасли в интеллектуальные экосистемы и задают новые стандарты эффективности.

Таблица 2 - 5 главных эффектов цифровой трансформации на реальный сектор [13]

Сфера	Что меняется	Пример
Производство	От массового выпуска к персонализации без роста затрат	Adidas Speedfactory — кроссовки под ноги конкретного клиента за те же деньги
Обслуживание	От ремонта по плану к предсказанию поломок	Siemens: датчики на турбинах сами вызывают сервисную бригаду за 2 недели до отказа
Логистика	От фиксированных маршрутов к адаптивным в реальном времени	Магистральные грузовики с ИИ-навигацией: экономия топлива 15-20%
Сельское хозяйство	От сплошной обработки полей к точному внесению ресурсов	Дроны и GPS: разная доза удобрений на каждом квадратном метре (урожайность +30%, химикаты –40%)
Бизнес-модели	От продажи оборудования к продаже «мощности в час»	Rolls-Royce «Power by the Hour»: авиакомпания платит только за налёт

		двигателя

Цифровая трансформация в реальном секторе - это не про «внедрение технологий ради технологий», а про измеримый результат: агропром в России показывает +22% к производительности за шесть лет, строительство и логистика экономят до 45% времени на операциях, а промышленность переориентируется с валового роста на качественную эффективность. В таблице 3 - ключевые эффекты по отраслям: где цифра уже даёт отдачу, какие драйверы работают и как меняется экономика процессов.

Таблица 3 - Главные эффекты цифровой трансформации на реальный сектор [3]

Отрасль	Ключевой эффект (рост ПТ)	Драйверы и результаты
АПК	+22% за 6 лет по РФ	АПК лидирует по темпам роста в стране. Цифровизация предприятий дает до +24.8%. Эффект от точного земледелия - +24.8%, роботизированные системы экономят расходы.
Промышленность	В основном качественный рост	Цель - не только рост ПТ, но и снижение издержек и повышение качества продукции, особенно в ВПК. Сокращение затрат в цепочках поставок - на 15-25%.
Строительство, логистика	Более 30% в отдельных операциях	Ускорение выполнения проектов - до 30% при контроле рабочего времени. Снижение простоев - на 45% за счет цифрового мониторинга.

Макроэкономический контекст цифровой трансформации определяется острым кадровым дефицитом: 64% работодателей вынуждены делать ставку на автоматизацию не ради инноваций, а ради физического выживания бизнеса. Однако технологический прогресс демонстрирует парадоксальную природу: в сегменте «белых воротничков» внедрение ИИ порой увеличивает время выполнения задач на 346%, усложняя процессы вместо их упрощения. На этом фоне производительность труда в России, восстановившись после кризисного спада 2022 года, в 2025 году достигла $44,3 в час (по ППС), что соответствует 52-му месту в мире и сохраняет отставание от среднемировых значений. Глобальная динамика также замедлилась до ~1,5% в год, усиливая разрыв

между странами: пока Китай, Вьетнам и Грузия демонстрируют кратный рост за счёт догоняющей модернизации, развитые экономики стагнируют, возлагая надежды на ИИ как на потенциальный драйвер добавления $15,7 трлн к мировому ВВП к 2030 году. Тем не менее, несмотря на технологический ажиотаж, цифровая трансформация пока не обеспечила качественного прорыва ни для российской, ни для мировой экономики, трансформировавшись из инструмента развития в механизм адаптации к структурным ограничениям.

В эпоху цифровой трансформации экономическая безопасность сталкивается с комплексными, взаимосвязанными и постоянно меняющимися угрозами. Это требует перехода от реагирования на инциденты к упреждающему управлению рисками. Необходимо встраивать безопасность с самого начала разработки цифровых решений, развивать собственные технологии и навыки для уменьшения зависимости от внешних источников, создавать гибкое законодательство и инвестировать в обучение людей и культуру кибербезопасности на всех уровнях. Таким образом, экономическая безопасность в цифровую эпоху становится не просто защищенностью, а динамичной способностью системы оставаться стабильной, приспосабливаться и развиваться перед лицом непрерывных вызовов.

Библиографический список:

1. Гудкова О.В. РИСКИ И УГРОЗЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ // Известия ВУЗов ЭФиУП. 2022. №1 (51). URL: https://cyberleninka.ru/article/n/riski-i-ugrozy-ekonomicheskoy-bezopasnosti-rossii-v-usloviyah-tsifrovizatsii-ekonomiki/viewer
2. Кузовкова Т.А., Салютина Т.Ю. Риски цифровой трансформации экономики и общества и инструментарий управления экономической безопасностью бизнеса в цифровой среде // Электронный научный журнал «Век качества». 2024. №1. С. 63-87. Режим доступа: https://www.agequal.ru/pdf/2024/124005.pdf

3. О чём говорят цифры [Электронный ресурс] // Коммерсантъ : [сайт]. — 2025. — 24 янв. URL: https://www.kommersant.ru/doc/8462729
4. Проблемы обеспечения экономической безопасности в условиях цифровой трансформации экономики России // Вестник Тюменского государственного университета. — 2023. — Доступ: https://elib.utmn.ru/jspui/bitstream/ru-tsu/32043/1/ebs_2023_311_321.pdf
5. Рузина Е.И. Цифровизация: об определении понятия, о выгодах и рисках цифровой трансформации / Е.И. Рузина. — EDN OAVVQX // Горизонты экономики. — 2022. — № 5 (71). — С. 96–99.
6. Темников Андрей Олегович СОВРЕМЕННЫЕ ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ТЕРМИНА "ЦИФРОВАЯ ТРАНСФОРМАЦИЯ" // Гуманитарные, социально-экономические и общественные науки. 2023. №3. URL: https://cyberleninka.ru/article/n/sovremennye-podhody-k-opredeleniyu-termina-tsifrovaya-transformatsiya.
7. Указ Президента РФ от 7 мая 2024 года №309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» [Электронный ресурс] // Официальный портал правовой информации. URL: http://www.kremlin.ru/acts/bank/50542
8. Цифровизация субъектов Российской Федерации [Электронный ресурс] // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : официальный сайт. URL: https://digital.gov.ru/activity/czifrovizacziya-gosudarstva/czifrovizacziya-subektov-rossijskoj-federaczii
9. Шелепаева А.Х. Цифровая трансформация: Основные подходы к определению понятия / А.Х. Шелепаева. — DOI 10.22363/2312-8631-2022-19-1-20-28. — EDN XZKKJT // Вестник Российского университета дружбы народов. Серия: Информатизация образования. — 2022. — Т. 19, № 1. — С. 20–28.

10. DHL Trend Research. Digitalization in Logistics: Efficiency Gains and Risk Exposure [Электронный ресурс]. – Bonn : DHL Customer Solutions & Innovation, 2024. – URL: https://www.dhl.com/insights.
11. Kaspersky ICS CERT. Threat Landscape for Industrial Automation Systems: Annual Report 2025 [Электронный ресурс]. – Moscow : Kaspersky Industrial CyberSecurity, 2025. – URL: https://ics-cert.kaspersky.com/reports.
12. McKinsey & Company. The economic potential of generative AI and digital transformation in manufacturing [Электронный ресурс]. – New York : McKinsey & Company, 2023. – URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights.
13. Siemens AG. Digital Enterprise Performance Reports: Operational Efficiency through JIT 4.0 and Digital Twins [Электронный ресурс]. – Munich : Siemens Industry Software, 2023–2024. – URL: https://www.siemens.com/digital-enterprise.
14. World Bank. Digital Dividends in Labor Markets: Skills Transition in Emerging Economies: World Development Report 2025 [Электронный ресурс]. – Washington, D.C. : World Bank, 2025. – URL: https://www.worldbank.org/en/publication/wdr2025.