DOI 10.37882/2223-2974.2026.02.27

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ КАК ФАКТОР ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ САМАРСКОГО РЕГИОНА

DIGITAL TRANSFORMATION AS A FACTOR IN ENSURING ECONOMIC SECURITY IN THE SAMARA REGION

E. Rusakova
E. Dmitrieva
I. Grigoryants

Summary. The article examines digital transformation as a systemic driver of economic security in the Samara region. It analyzes the dual impact of digitalization: the development of new protective instruments and the emergence of vulnerabilities, including cyber threats, dependence on imported technologies, and shortages of qualified personnel. Drawing on regional strategic documents and a SWOT analysis, the study identifies key risks and opportunities. Practical recommendations for 2026–2027 are proposed, including stimulating demand for domestic IT solutions, establishing a «Digital Academy», and creating a regional cyber range to strengthen technological sovereignty and resilience.

Keywords: digital transformation, economic security, Samara region, import substitution, technological sovereignty, regional development.

Русакова Екатерина Викторовна
Кандидат экономических наук, доцент, Самарский государственный экономический университет
rusakova_e_v@mail.ru
Дмитриева Елена Олеговна
кандидат экономических наук, доцент, Самарский государственный технический университет
dmitr-el@mail.ru
Григорьянц Игорь Александрович
кандидат экономических наук, доцент, Самарский национальный исследовательский университет имени академика С.П. Королева
market@ofernio.su

Аннотация. В статье представлены результаты исследования цифровой трансформации как системного фактора экономической безопасности Самарской области, анализируются противоречивые эффекты цифровизации: создание новых инструментов защиты и возникновение уязвимостей (киберугрозы, зависимость от импортного ПО, кадровый дефицит). На основе данных Росстата, региональных стратегий и SWOT-анализа выявлены ключевые риски и возможности и предложены практические рекомендации на 2026–2027 гг., включая стимулирование спроса на отечественные IT-решения, создание «Цифровой академии» и регионального киберполигона для усиления технологического суверенитета и устойчивости.

Ключевые слова: цифровая трансформация, экономическая безопасность, Самарская область, киберугрозы, импортозамещение, IT-кластер, SWOT-анализ, технологический суверенитет, региональное развитие.

Введение

В условиях формирования технологического суверенитета и санкционного давления цифровая трансформация перестает быть вопросом исключительно эффективности, становясь критическим фактором национальной и региональной экономической безопасности. Для Самарской области — одного из ключевых промышленных и научных центров России с концентрированными активами в автопроме, аэрокосмической отрасли и химическом комплексе — устойчивость цифровой инфраструктуры и технологическая независимость определяют не только конкурентоспособность, но и базовую способность экономики функционировать в условиях гибридных угроз. Процессы цифровизации носят дуалистичный характер: с одной стороны, они создают новые инструменты для мониторинга, прогнозирования и нейтрализации рисков (от логистических сбоев до кибератак), с другой — формируют принципиально новые уязвимости, связанные с зависимостью от иностранного ПО, утечкой данных и эксплуатацией слабостей киберзащиты.

Вопросы экономической безопасности регионов получили фундаментальную разработку в трудах классиков отечественной экономической мысли, таких как В.К. Сенчагов, С.Ю. Глазьев и д.р. В современных условиях акцент исследований сместился на анализ влияния цифровой трансформации на региональную безопасность, что отражено в значительном массиве публикаций 2023–2025 годов. Теоретико-методологические аспекты взаимосвязи цифровизации и экономической безопасности региона исследуются в работах М.М. Балога и А.В. Бабкина, С.В. Балалаева и И.В. Игольниковой, А.С. Васильчука, О.И. Голикова и О.В. Голиковой [2, 3, 5]. Прикладные вопросы, включая управление безопасностью в новых условиях, моделирование угроз и институциональные факторы, нашли отражение в исследованиях С.О. Булавиной, Д.О. Добренького и Д.М. Простовой, Н.Б. Дроковского, П.Г. Исаевой, Н.А. Кулагиной и Е.М. Че-

пиковой, О.Г. Кучмистой и Н.Д. Родина, М.И. Чижиковой [2, 6–8,10, 11]. Отдельного внимания заслуживает работа А.В. Котанджяна, посвященная влиянию цифровизации на социально-кадровую составляющую безопасности [9].

Несмотря на высокую активность научной дискуссии, комплексный анализ, рассматривающий цифровую трансформацию именно как системный фактор, одновременно формирующий и угрозы, и инструменты защиты экономической безопасности конкретного промышленного региона, представлен в литературе фрагментарно. Особую актуальность такой анализ приобретает в среднесрочной перспективе 2026–2027 гг. применительно к Самарской области, чья экономическая структура и статус делают её репрезентативным объектом для подобного исследования

Целью исследования, результаты которого представлены в данной статье, являлась оценка влияния процессов цифровой трансформации на состояние экономической безопасности Самарской области и разработка практико-ориентированных рекомендаций по ее укреплению.

Материалы и методы исследования

Исследование базируется на системном и структурно-функциональном подходах, его эмпирическую базу составили данные Росстата, Минцифры РФ, отчетов Правительства Самарской области и значимых для исследования региональных стратегических документов. Применялись методы сравнительного и нормативно-правового анализа, метод кейсов (на примере конкретных предприятий и инфраструктурных проектов), а также SWOT-анализ для комплексной оценки ситуации.

Результаты и обсуждения

Комплексное исследование цифровой трансформации как фактора экономической безопасности требует перехода от теоретического концептуализации к диагностике конкретной ситуации. Для оценки текущего положения Самарской области в 2024 году и формирования базиса для прогноза на 2025–2026 гг. был проведен анализ ключевых количественных и качественных индикаторов, динамика отдельных показателей представлена на рис. 1.

По данным Росстата и Минцифры РФ, Самарская область демонстрирует достаточно неоднородную цифровую зрелость: с одной стороны, регион занимает 21 место по индексу цифровизации госуслуг на начало 2025 года [15], а охват домохозяйств широкополосным интернетом превышает 85 %, но, с другой стороны, глубина цифровой трансформации бизнеса варьируется. Крупные предприятия-флагманы региона (АО «АвтоВАЗ», АО «РКЦ «Прогресс») активно внедряют цифровые двойники, промышленный IoT и системы предиктивной аналитики, часто в рамках сотрудничества с резидентами IT-кластера «Жигулевская долина». Вместе с тем, сегмент МСП, особенно в сфере услуг и традиционной промышленности, зачастую ограничивается базовой цифровизацией (1С, онлайн-кассы и т.д.), что создает «цифровые разрывы» в экономической ткани региона и снижает ее общую устойчивость. В современных условиях цифровая трансформация дает возможность региону реализовать на практике конкретные инструменты для усиления экономической безопасности, такие как импортозамещение, развитие ситуационных центров, защита КИИ (критической информационной структуры) и т.д. Регион обладает уникальным активом — IT-кластером «Жигулевская долина», который трансформируется из центра разработки в центр внедрения отечественных ре-

Рис. 1. Динамика отдельных показателей уровня цифровизации Самарской области в 2021–2026 гг. (* отмечены прогнозные значения показателей)

шений, а успешные кейсы внедрения российских CAD/CAE-систем на машиностроительных предприятиях и отечественных ERP-платформ в логистических компаниях снижают критическую зависимость от иностранного ПО, являясь практическим вкладом в технологический суверенитет. Ситуационный центр (далее — СиЦ) сегодня выходит за рамки мониторинга ЧС, так как на основе агрегации больших данных от различных ведомств и открытых источников с применением технологий AI он способен моделировать социально-экономические последствия кризисов (от перебоев в цепочках поставок сырья для химических заводов до всплеска безработицы в моногородах), обеспечивая проактивное, а не реактивное управление. Реализация требований ФЗ-187 «О безопасности КИИ» на таких объектах, как АО «Куйбышевский НПЗ» или Самарская ТЭЦ, в настоящее время переводит киберзащиту из IT-задачи в разряд стратегических приоритетов промышленной безопасности всего региона [12–14].

Анализ цифровой зрелости региона и выявленные диспропорции и зависимости формируют новый ландшафт угроз, в котором технологические уязвимости трансформируются в прямые экономические риски, ведь наряду с возможностями, цифровая трансформация генерирует комплекс новых и усиливает традиционные угрозы экономической безопасности Самарской области, которые можно структурировать по следующим группам: технологические и кибернетические риски; социально-экономические и кадровые риски; правовые и регуляторные риски.

Технологические и кибернетические риски, в первую очередь включают риски целенаправленных кибератак на объекты КИИ. Промышленные предприятия области относятся к высокоприоритетным целям для сложных APT-атак, которые могут вызвать каскадный мультипликативный эффект по всей региональной экономике, включая кооперационные цепочки тысяч МСП. По данным исследований, наблюдается рост сложных целевых атак на промышленные объекты на 35 % в 2024 году по сравнению с предыдущим периодом [1, 12–16].

Продолжающаяся зависимость ряда ключевых производств от специализированного иностранного ПО и «недружественного» оборудования создает угрозу остановки в случае ужесточения санкций (отключение от сервисов обновления, техподдержки), так как процесс импортозамещения в высокотехнологичных сегментах требует времени и значительных инвестиций, создавая «окно уязвимости». Концентрация данных в цифровых системах (от интеллектуальной собственности предприятий до персональных данных граждан) повышает ценность таких активов для злоумышленников, в свою очередь утечка может привести как к прямым финансовым потерям, так и к подрыву доверия к региону как к площадке для инвестиций.

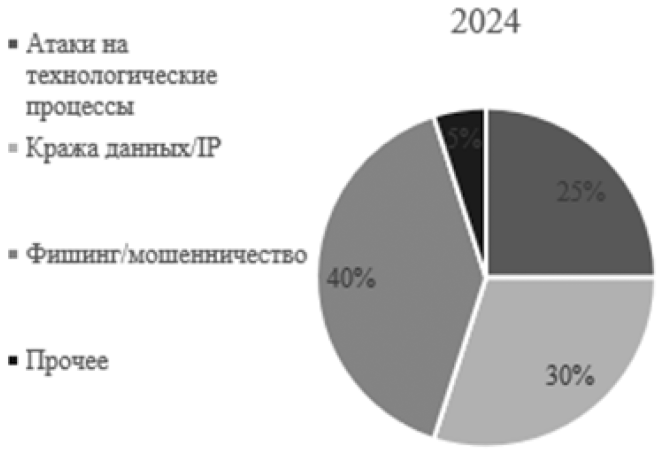

Рис. 2. Структура зафиксированных киберинцидентов в Самарской области по типу цели, 2024 гг.

Социально-экономические и кадровые риски в первую очередь включают. риски углубления цифрового неравенства и дефицит кадров.

Существенный разрыв в цифровых компетенциях и доступе к инфраструктуре между Самарой, Тольятти и малыми городами или сельскими районами (например, северо-восток области) ведет к асимметричному развитию, ограничивает возможности удаленной занятости и увеличивает социальную напряженность. Регион сталкивается с острой нехваткой специалистов в области кибербезопасности, Data Science и разработки сложного промышленного ПО, при этом объективно существует риск «утечки мозгов» наиболее квалифицированных IT-кадров в столичные агломерации или за рубеж, что подрывает основу для собственного технологического развития.

Рассматривая правовые и регуляторные риски необходимо отметить, что динамичное развитие цифровой среды зачастую опережает формирование соответствующей правовой базы, а неопределенность в вопросах регулирования оборота данных, ответственности за решения, принятые системами на основе AI, и межведомственного взаимодействия при киберинцидентах создает «серые зоны», затрудняющие эффективное управление цифровыми рисками на региональном уровне.

Выявление спектра угроз актуализирует задачу поиска балансирующих механизмов. Парадоксально, но именно цифровая трансформация, порождая риски, предоставляет и наиболее эффективные инструменты для защиты экономического суверенитета, что, в свою очередь, создает сложную, диалектическую среду для управления безопасностью.

Для систематизации выявленных противоречивых тенденций и формирования целостного стратегическо-

го взгляда авторами составлен сводный SWOT-анализ влияния цифровой трансформации на экономическую безопасность Самарской области (Таблица 1).

Таблица 1.

SWOT-анализ влияния цифровой трансформации на экономическую безопасность Самарской области

Сильные стороны	Слабые стороны
Наличие мощного IT-кластера («Жигулевская долина») как центра компетенций	Критическая зависимость ряда градообразующих предприятий от импортного ПО и комплектующих
Высокая концентрация промышленных предприятий — потенциальных полигонов для внедрения решений.	Значительное отставание в цифровизации сектора МСП и социальной сферы
Развитая система высшего технического образования	Дефицит кадров в области промышленной кибербезопасности и Data Science
Функционирующий современный Ситуационный центр.	Недостаточная координация между научными, образовательными и производственными звеньями
Возможности	**Угрозы**
Федеральные программы финансирования импортозамещения и цифровизации	Эскалация санкционного давления в IT-сфере и «цифровая блокада».
Рост спроса на отечественные безопасные IT-решения	Усиление частоты и сложности APT-атак на объекты КИИ.
Возможность стать пилотным регионом по внедрению стандартов «цифровой устойчивости»	«Утечка» высококвалифицированных IT-кадров в столичные агломерации.
Развитие удаленной занятости для нивелирования кадрового дисбаланса	Правовое отставание в регулировании новых цифровых отношений

Проведенный SWOT-анализ позволяет сделать вывод, что основная задача для региона на среднесрочную перспективу заключается в трансформации внутренних сильных сторон (IT-кластер, образование) в инструменты для нейтрализации внешних угроз (кибератаки, санкции) и преодоления внутренних слабостей (кадры, зависимость) и именно на этом принципе должны базироваться практические меры.

Выводы

Проведенный анализ позволяет констатировать, что к 2025 году цифровая трансформация для Самарской области превратилась в системный фактор, который необходимо управляемо интегрировать в стратегию экономической безопасности. Цифровая среда формирует новое «поле битвы», где традиционные промышленные активы региона становятся мишенями для кибератак, а технологическая зависимость — критической уязвимостью, в то же время данная среда предлагает и мощные инструменты защиты: от отечественного ПО для импортозамещения до аналитических платформ для предиктивного управления. Ключевой вызов заключается в синхронизации темпов цифровизации (прежде всего, в сегменте МСП и социальной сфере) с мерами по обеспечению технологического суверенитета и киберустойчивости. В рамках проведенного исследования авторами был разработан ряд рекомендаций на краткосрочную перспективу 2026–2027 гг. в регионе: стимулирование спроса на безопасные цифровые решения (внедрение целевых региональных субсидий и налоговых льгот не столько для IT-компаний, сколько для потребителей — промышленных предприятий и организаций соцсферы, внедряющих аккредитованное отечественное ПО и сервисы киберзащиты позволит создать рыночный спрос и ускорит импортозамещение); развитие кадрового суверенитета (инициирование создания на базе кооперации ведущих Вузов региона и IT-компаний специализированной «Цифровой академии», задача которой будет заключаться к практико-ориентированной подготовке и переподготовке специалистов по сквозным цифровым профилям (цифровой инжиниринг, промышленная кибербезопасность и т.д.), с обязательством трудоустройства выпускников на предприятия региона); создание регионального киберполигона (на базе IT-кластера представляется целесообразным создать инфраструктуру для регулярного тестирования систем киберзащиты ключевых предприятий и органов власти, что позволит в режиме контролируемых учений выявлять и устранять уязвимости до реальных атак. Перспективным видится углубленное моделирование социально-экономических последствий гипотетических масштабных кибератак на ключевые активы региона, а также оценка экономического эффекта от предлагаемых мер поддержки в формате пилотных проектов.

ЛИТЕРАТУРА

1. Актуальные киберугрозы: I–II кварталы 2025 года. Отчет исследовательской группы Positive Technologies. Режим доступа: https://ptsecurity.com/research/analytics/aktual-nye-kiberugrozy-i-ii-kvartaly-2025-goda/. (Дата обращения: 20.12.2025)
2. Балалаев С.В., Игольникова И.В. Основные подходы к угрозам экономической безопасности регионов // Управление и цифровизация: национальное и региональное измерение: сборник статей IV национальной научно-практической конференции с международным участием. Брянск, 2024. С. 34–41.
3. Балог М.М., Бабкин А.В. Детерминанты ускорения процессов цифровизации в контексте обеспечения экономической безопасности региона // π-Economy. 2024. Т. 17. № 3. С. 33–51.
4. Булавина С.О. Особенности управления экономической безопасностью региона в условиях цифровой трансформации // Молодежь в фокусе научных перемен: идеи и открытия. электронный сборник статей по материалам студенческой конференции. Волжский, 2023. С. 8–13.
5. Васильчук А.С., Голиков О.И., Голикова О.В. Влияние основных трендов цифрового развития на экономическую безопасность региона // Вестник Волжского университета им. В.Н. Татищева. 2024. Т. 2. № 1 (53). С. 6–17.
6. Добренький Д.О., Простова Д.М. Влияние цифровизации на экономическую безопасность региона // Инфокоммуникационные технологии: актуальные вопросы цифровой экономики: сборник научных трудов V Международной научно-практической конференции. Екатеринбург, 2025. С. 226–229.
7. Дроковский Н.Б. Цифровые технологии и экономическая безопасность региона // Цивилизационный потенциал Российского региона: структура, состояние и перспектива роста: материалы III Всероссийской научно-практической конференции. Калининград, 2023. С. 120–124.
8. Исаева П.Г. Развитие региона в условиях цифровой экономики и приоритеты государственного управления в интересах экономической безопасности // Инновационная экономика: информация, аналитика, прогнозы. 2024. № 5. С. 33–38.
9. Котанджян А.В. Факторы влияния цифровой трансформации на социально-кадровую безопасность субъекта РФ // Управление рисками: новые вызовы, проблемы и решения (РИСК'Э-2023): труды IX научно-практической конференции с зарубежным участием, под научной редакцией доктора технических наук, профессора С. Г. Опарина. Санкт-Петербург, 2024. С. 62–67.
10. Кулагина Н.А., Чепикова Е.М. Цифровая трансфорация в контексте обеспечения экономической безопасности региона // Вызовы цифровой экономики: технологический суверенитет и экономическая безопасность: сборник статей VI Всероссийской научно-практической конференции с международным участием. Брянск, 2023. С. 317–320.
11. Кучмистая О.Г., Родин Н.Д. Цифровизация институциональной среды как фактор повышения экономической безопасности региона // Актуальные вопросы экономики и управления: теоретические и прикладные аспекты: материалы X Международной научно-практической конференции. Горловка, 2025. С. 40–45.
12. Постановление Правительства Самарской области от 14.10.2025 № 625 «Об итогах социально-экономического развития Самарской области за восемь месяцев 2025 года и ожидаемых итогах развития за 2025 год, прогнозе социально-экономического развития Самарской области на 2026 год и плановый период 2027 и 2028 годов». Режим доступа: https://economy.samregion.ru/upload/iblock/95d/wfobja70ffmofvfa2rkud5q9jea43o74/PPSO-_-626-ot-14.10.2025.pdf
13. Прогноз социально-экономического развития Самарской области на 2026–2028 годы// Министерство экономического развития и инвестиций Самарской области. Режим доступа: https://economy.samregion.ru/activity/ekonomika/prognoz_razvitia/srednesrochnij_prognoz/prognz-sotsialno-ekon646/
14. Прогноз социально-экономического развития Самарской области на период до 2034 года /Министерство экономического развития и инвестиций Самарской области. Режим доступа: https://economy.samregion.ru/activity/ekonomika/prognoz_razvitia/dolgosrochnyy-prognoz/prognoz-sotsialno-ekonomicheskogo-razvitiya-samarskoy-oblasti-na-period-do-2034-goda/
15. Рейтинг цифровизации и внедрения ИИ в регионах России (январь — апрель 2025 года) // Регионы России. Режим доступа: https://rrmag.ru/2025/05/19/rejting-czifrovizaczii-i-vnedreniya-ii-v-regionah-rossii-yanvar-aprel-2025-goda/. (Дата обращения: 20.12.2025)
16. Самарская область в цифрах //Министерство экономического развития и инвестиций Самарской области. Режим доступа: https://economy.samregion.ru/activity/ekonomika/values_so/
17. Чижикова М.И. Моделирование экономической безопасности региона в условиях цифровой трансформации // Научные перспективы в области учета, анализа, контроля и аудита: сборник научно-исследовательских работ молодых ученых. Москва, 2025. С. 191–196.