УДК 330
DOI 10.26118/2782-4586.2025.42.77.073

Курбанова Анжела Магомедовна
Дагестанский государственный медицинский университет
Ибрагимова Элина Саламбековна.
Чеченский государственный университет им. А.А. Кадырова
Султанов Нариман Гарунович
Дагестанский государственный университет

Цифровая трансформация как фактор обеспечения экономической безопасности промышленных предприятий: современные вызовы и стратегические решения

Аннотация. В условиях ускоряющейся цифровизации экономики и глобальных геополитических и технологических вызовов обеспечение экономической безопасности промышленных предприятий приобретает особую значимость. Цифровая трансформация, являясь одновременно драйвером роста и источником новых рисков, требует комплексного подхода к управлению безопасностью на всех уровнях деятельности предприятия. Цель исследования – выявить взаимосвязь между уровнем цифровой зрелости промышленных предприятий и их способностью обеспечивать экономическую безопасность, а также предложить адаптивные механизмы управления в условиях цифровой трансформации. Результаты исследования показали, что интеграция цифровых технологий в производственные, управленческие и контрольные процессы способствует повышению устойчивости предприятия к внутренним и внешним угрозам. В то же время выявлены существенные пробелы в обеспечении кибербезопасности, кадровой устойчивости и этического регулирования использования ИИ и больших данных. Обеспечение экономической безопасности в эпоху цифровой трансформации требует не только технологических, но и организационно-методологических инноваций. Стратегическое планирование, цифровая грамотность персонала и комплексные системы мониторинга рисков становятся ключевыми условиями устойчивого развития промышленных предприятий.

Ключевые слова: экономическая безопасность, цифровая трансформация, промышленное предприятие, кибербезопасность, цифровая зрелость, устойчивое развитие, управление рисками, цифровая грамотность.

Kurbanova Angela Magomedovna
Dagestan State Medical University
Ibragimova Elina Salambekovna
Chechen State University named after A.A. Kadyrov
Sultanov Nariman Garunovich
Dagestan State University

Digital transformation as a factor of ensuring the economic security of industrial enterprises: modern challenges and strategic solutions

Abstract. In the context of the accelerating digitalization of the economy and global geopolitical and technological challenges, ensuring the economic security of industrial enterprises is becoming particularly important. Digital transformation, being both a driver of growth and a source of new risks, requires an integrated approach to security management at all levels of an enterprise. The purpose of the study is to identify the relationship between the level of digital maturity of industrial enterprises and their ability to ensure economic security, as well as to propose adaptive management mechanisms in the context of digital transformation. The

results of the study showed that the integration of digital technologies into production, management and control processes helps to increase the company's resilience to internal and external threats. At the same time, significant gaps have been identified in ensuring cybersecurity, human resource sustainability, and ethical regulation of the use of AI and big data. Ensuring economic security in the era of digital transformation requires not only technological, but also organizational and methodological innovations. Strategic planning, digital literacy of personnel and integrated risk monitoring systems are becoming key conditions for the sustainable development of industrial enterprises.

Keywords: economic security, digital transformation, industrial enterprise, cybersecurity, digital maturity, sustainable development, risk management, digital literacy

Введение

Современные реалии глобальной экономики формируются под влиянием беспрецедентного технологического прогресса, изменений в международной торговле и усиления геополитической напряжённости. В этих условиях промышленные предприятия сталкиваются с новыми вызовами, требующими не только адаптации, но и проактивного переосмысления стратегий обеспечения экономической безопасности. Цифровая трансформация, представляющая собой не просто внедрение ИТ-решений, а фундаментальное изменение бизнес-моделей, процессов и корпоративной культуры, становится ключевым фактором устойчивого развития [3, 9].

Однако, несмотря на очевидные преимущества, такие как повышение производительности, оптимизация логистики и улучшение качества продукции, цифровизация порождает новые уязвимости. Кибератаки, утечки данных, внутренний саботаж, недостаточная цифровая грамотность персонала, а также этические дилеммы, связанные с использованием искусственного интеллекта и автоматизированных систем принятия решений, создают комплексные угрозы экономической безопасности [12, 14].

Проблема заключается в том, что большинство предприятий продолжают рассматривать цифровую трансформацию исключительно как технологический проект, пренебрегая её системным влиянием на все компоненты экономической безопасности – финансовую, кадровую, информационную, технологическую и экологическую [2, 6]. Такой узкий подход снижает эффективность инвестиций и увеличивает риски.

Целью настоящего исследования является выявление и систематизация взаимосвязей между уровнем цифровой зрелости промышленного предприятия и его способностью обеспечивать экономическую безопасность в условиях трансформации.

Для достижения цели были определены следующие задачи:

- проанализировать современное состояние теоретико-методологической базы по проблеме экономической безопасности в условиях цифровой трансформации;
- выявить ключевые риски и угрозы, возникающие на стыке цифровизации и экономической безопасности;
- предложить модель интегрированного управления экономической безопасностью, учитывающую цифровые вызовы;
- обосновать необходимость формирования цифровой культуры и компетенций у персонала как условия устойчивости.

Актуальность исследования подтверждается как научной, так и практической значимостью: научные изыскания в этой области всё ещё недостаточны, особенно в контексте отечественной промышленности, а предприятия нуждаются в конкретных методических и управленческих рекомендациях.

Степень изученности проблемы

Проблематика экономической безопасности предприятий широко представлена в российской научной литературе. В работах Сулумова С. Х. и Голощаповой Л. В. предложена системная модель экономической безопасности, включающая финансовый,

кадровый, информационный и технологический компоненты, что подчёркивает её многомерный характер [2]. Однако авторы не в полной мере учитывают специфику цифровой среды, в которой функционируют современные предприятия.

Анализ работ Гоника Г. Г. и Кравченко Р. Ю. показывает, что в условиях цифровой экономики ключевыми угрозами становятся киберриски и дефицит цифровых компетенций у управленческого персонала [1]. Эти исследования подчёркивают важность контрольных функций и адаптации механизмов внутреннего аудита к новым условиям, однако не предлагают комплексной стратегии интеграции цифровых технологий в систему безопасности.

Нуридинова В. В. и Овсийчук В. В. рассматривают цифровизацию как фактор национальной экономической безопасности, но акцент делается преимущественно на макроуровне, без детализации на уровне отдельных предприятий [3]. Аналогичный подход у Султанова Г. С. и др., которые акцентируют внимание на государственной политике, а не на корпоративных механизмах [10].

Более прикладной характер носят работы Смотровой Т. И. и Шендриковой О. О., где анализируются практические инструменты обеспечения безопасности на этапах внедрения цифровых решений [6]. Авторы отмечают важность анализа готовности предприятия к трансформации, однако не уделяют достаточного внимания человеческому фактору и организационной культуре.

Особую значимость приобретают исследования, рассматривающие этические и правовые аспекты цифровизации. Так, Балог М. М. и соавторы поднимают вопрос ответственного использования ИИ и защиты персональных данных как неотъемлемой части экономической безопасности [9]. Кононенко Р. В. и Наумик-Гладкая Е. Г. предупреждают о росте внутренних угроз, связанных с недостаточной подготовкой персонала и слабостью внутреннего контроля [13].

Тем не менее, в современной научной литературе отсутствует целостная модель, интегрирующая цифровую зрелость предприятия с его способностью противостоять разнообразным угрозам экономической безопасности. Большинство исследований фрагментарны: либо акцентируются на технологиях, либо на рисках, либо на организационных аспектах. В связи с этим назрела необходимость в системном подходе, который бы учитывал как техническую, так и управленческую, и человеческую составляющие цифровой трансформации.

Методы исследования

В ходе исследования были применены общенаучные и специальные методы. Анализ и синтез позволили выделить ключевые компоненты экономической безопасности и их трансформацию под влиянием цифровых технологий. Системный подход использовался для рассмотрения предприятия как сложной адаптивной системы, взаимодействующей с внешней средой. Метод сравнительного анализа помог сопоставить различные модели цифровой зрелости и подходы к управлению безопасностью в зарубежной и отечественной практике. Контент-анализ научных публикаций за период 2022–2025 гг. обеспечил актуальность теоретической базы. Кроме того, применялся метод обобщения эмпирических данных, полученных из отчётов РАНХиГС, Росстата, а также из практики цифровой трансформации на предприятиях машиностроения, металлургии и пищевой промышленности. Особое внимание уделено анализу кейсов российских предприятий, участвующих в национальных проектах «Цифровая экономика» и «Производительность труда».

Результаты исследования и дискуссия

Современная цифровая трансформация промышленных предприятий выходит за рамки автоматизации отдельных процессов. Она включает формирование цифровых двойников, внедрение IoT-решений, использование Big Data и AI для прогнозной

аналитики, а также переход на облачные платформы управления [6]. По данным Минцифры РФ (2024), более 60 % крупных промышленных предприятий России реализуют проекты по созданию цифровых двойников, а 45 % – используют аналитику больших данных для оптимизации логистики и управления запасами. Однако уровень интеграции этих технологий в системы обеспечения экономической безопасности остаётся низким.

Цифровая зрелость предприятия прямо коррелирует с его устойчивостью к экономическим шокам. Как показало исследование РАНХиГС (2024), предприятия с высоким уровнем цифровой зрелости демонстрируют на 30 % более высокую рентабельность и на 25 % выше устойчивость к киберугрозам по сравнению с предприятиями с низким уровнем цифровизации. Это объясняется не столько наличием технологий, сколько системным подходом к их использованию.

Финансовая безопасность. Цифровые технологии позволяют повысить прозрачность финансовых потоков, автоматизировать контрольные процедуры и улучшить прогнозирование ликвидности. Например, использование блокчейн-технологий в цепочках поставок снижает риски мошенничества и задержек расчётов [5]. Однако переход на цифровые финансовые инструменты увеличивает зависимость от стабильности ИТ-инфраструктуры и уязвимость к кибератакам на финансовые системы.

Кадровая безопасность. В условиях цифровой трансформации возрастает значение «цифровой гигиены» персонала. По данным исследования НАУМЕН (2024), 68 % инцидентов информационной безопасности происходят по вине сотрудников – как следствие фишинга, слабых паролей или несанкционированного использования устройств. Это указывает на необходимость не только технической защиты, но и формирования корпоративной цифровой культуры [14].

Информационная безопасность. Здесь наблюдается наиболее острый диссонанс между технологическим потенциалом и реальной защитой. Хотя предприятия активно внедряют SIEM-системы и решения по защите конечных точек, многие из них не имеют чёткой стратегии кибербезопасности, интегрированной в общую стратегию экономической безопасности [12]. Особенно уязвимы предприятия, использующие устаревшее ПО и не обновляющие протоколы шифрования.

Технологическая и экологическая безопасность. Цифровые датчики и системы мониторинга позволяют в реальном времени отслеживать состояние оборудования, предотвращая аварии и снижая экологические риски. Однако зависимость от программного обеспечения и поставщиков ИТ-услуг создаёт новые точки отказа. Примером может служить инцидент на одном из химических предприятий Урала в 2023 году, когда сбой в облачной платформе управления привёл к остановке производства на 36 часов.

Современный этап цифровой трансформации транспортно-логистических экосистем сопровождается не только возможностями повышения эффективности, но и возникновением новых, ранее нехарактерных угроз. Среди них особое внимание заслуживают этические риски, связанные с применением искусственного интеллекта: автоматизированные системы, используемые в кадровом отборе или динамическом ценообразовании, могут воспроизводить скрытые предубеждения, заложенные в обучающих данных, что влечёт за собой не только юридические последствия в виде нарушения принципов равенства и недискриминации, но и серьёзные репутационные потери. Не менее острой проблемой становится зависимость от внешних поставщиков программного обеспечения, особенно в формате SaaS-решений. Несмотря на очевидный прирост операционной эффективности, такая модель снижает уровень контроля организации над своими данными, делая её уязвимой к сбоям, изменению условий обслуживания или даже недобросовестным действиям третьих сторон. Дополнительным внутренним вызовом выступает цифровое неравенство внутри коллектива: значительный разрыв в уровне цифровых компетенций между поколениями сотрудников – от молодых

специалистов, выросших в цифровой среде, до опытных работников, осваивающих технологии с трудом – ведёт к снижению общей производительности, росту недопонимания и усилению внутренних конфликтов.

В ответ на эти вызовы на основе проведённого анализа была разработана комплексная модель обеспечения экономической безопасности цифровой транспортно-логистической экосистемы, построенная на трёх взаимосвязанных уровнях. На технологическом уровне акцент делается на внедрение защищённых ИТ-решений, разработанных в соответствии с принципом «безопасность по умолчанию» (Security by Design), что предполагает встраивание мер защиты на этапе проектирования систем, а не их дооснащение впоследствии. На организационном уровне предполагается формирование единой, сквозной системы управления рисками, которая объединяет финансовый, кадровый, информационный и производственный компоненты в единый управленческий контур, обеспечивая целостный взгляд на устойчивость бизнеса. Наконец, человеческий уровень рассматривается как фундамент всей системы безопасности: повышение цифровой грамотности всего персонала, обучение основам кибергигиены и воспитание культуры личной ответственности за информационную безопасность становятся не дополнительными, а базовыми условиями функционирования в цифровой среде.

Предложенная модель предполагает не разовое внедрение, а непрерывный процесс: регулярный аудит цифровой зрелости организации, оценка текущих и прогнозируемых угроз, а также адаптация защитных мер в динамике. Центральным элементом стратегии выступает создание так называемого «цифрового щита безопасности» – гибкого, масштабируемого комплекса технологий, процедур и управленческих практик, адаптированного под отраслевую специфику, географические особенности и масштаб конкретного предприятия. Такой подход позволяет не только реагировать на инциденты, но и предвосхищать угрозы, обеспечивая устойчивость и конкурентоспособность транспортно-логистической экосистемы в условиях неопределённости и технологической турбулентности.

Выводы и заключение

Цифровая трансформация не является автоматическим гарантом экономической безопасности промышленных предприятий. Напротив, без системного подхода она может стать источником новых, более сложных угроз. Результаты исследования подтверждают, что эффективное обеспечение экономической безопасности в цифровую эпоху требует перехода от реактивной защиты к проактивному управлению устойчивостью.

Ключевыми выводами являются следующие:

Экономическая безопасность в условиях цифровой трансформации должна рассматриваться как междисциплинарная категория, объединяющая ИТ, управление, финансы, право и этику.

Технологические решения сами по себе недостаточны: необходима интеграция в единую стратегию корпоративного управления.

Человеческий фактор остаётся центральным: без подготовки персонала и формирования цифровой культуры даже самые передовые системы безопасности будут неэффективны.

Предприятиям необходимо разрабатывать собственные «дорожные карты цифровой безопасности», учитывающие отраслевую специфику, размер, географию и уровень цифровой зрелости.

Перспективы дальнейших исследований связаны с разработкой методик оценки «цифровой уязвимости» предприятий, а также с изучением роли государственной поддержки в обеспечении киберустойчивости малого и среднего бизнеса, особенно в регионах с низким уровнем цифровой инфраструктуры, таких как Республика Дагестан.

В заключение, можно утверждать, что в современных условиях экономическая

безопасность промышленного предприятия – это не просто защита от угроз, а способность генерировать устойчивую ценность в условиях постоянной цифровой трансформации. Только комплексный, гибкий и человекоориентированный подход позволит предприятиям не только выжить, но и процветать в новой цифровой реальности.

Внедрение цифровых технологий на промышленные предприятия может оказать положительное влияние на обеспечение уровня экономической безопасности. Стоит отметить, что интеграция цифровых технологий является фактором повышения конкурентоспособности предприятия на рынке. Однако, обеспечение экономической безопасности в условиях цифровой трансформации является сложным процессом, затрагивающим многие аспекты производства. Проведенный анализ показал, что большинство предприятий на сегодняшний день в определенной степени уже интегрировали цифровые технологии.

Список источников

1. Гоник, Г. Г. Анализ обеспечения экономической безопасности компаний в условиях цифровой экономики / Г. Г. Гоник, Р. Ю. Кравченко, Д. И. Нечаев // Вестник Академии знаний. – 2024. – № 1 (60). – С. 102–104.
2. Сулумов, С. Х. Структура и составляющие системы экономической безопасности предприятия в современных условиях / С. Х. Сулумов, Л. В. Голощапова, Е. И. Зацаринная // Вестник Чеченского государственного университета им. А.А. Кадырова. – 2025. – № 2 (58). – С. 62–71.
3. Нуридинова, В. В. Влияние цифровизации на экономическую безопасность России / В. В. Нуридинова, В. В. Овсийчук // Вестник Академии управления и производства. – 2023. – № 2. – С. 66–72.
4. Савич, Ю. А. Реализация функции контроля в процессе обеспечения экономической безопасности предприятия в условиях цифровой трансформации / Ю. А. Савич, Н. Н. Голубь // Экономинфо. – 2024. – Т. 19, № 3. – С. 22–33.
5. Дьяков, С. А. Цифровизация деятельности хозяйствующих субъектов в целях повышения экономической безопасности / С. А. Дьяков, Л. Д. Алексеенко, А. В. Анопкин, Д. А. Коровин, Т. А. Шульженко // Труды Кубанского государственного аграрного университета. – 2022. – № 102. – С. 25–30.
6. Смотрова, Т. И. Обеспечение экономической безопасности предприятия в условиях цифровой трансформации / Т. И. Смотрова, О. О. Шендрикова // Экономинфо. – 2025. – Т. 20, № 2. – С. 13–21.
7. Васильчук, А. С. Обеспечение экономической безопасности физических лиц в условиях растущих цифровых угроз / А. С. Васильчук // OpenScience. – 2024. – Т. 6, № 3. – С. 152–163.
8. Ковалева, О. П. Влияние цифровой экономики на формирование экономической безопасности / О. П. Ковалева // Инновационная экономика и общество. – 2025. – № 1 (47). – С. 2–9.
9. Балог, М. М. Экономическая безопасность в контексте цифровизации: подходы, тенденции и угрозы / М. М. Балог, А. В. Бабкин, М. М. Гаджиев // Национальные интересы: приоритеты и безопасность. – 2024. – Т. 20, № 6 (435). – С. 1040–1060.
10. Султанов, Г. С. Цифровая трансформация экономики в контексте обеспечения экономической безопасности / Г. С. Султанов, М. Ш. Абдуллаев, М. М. Эмиров // Прикладные экономические исследования. – 2023. – № S2. – С. 98–104.
11. Маргацкий, Н. А. Формирование цифрового контура управления механизмами экономической безопасности как условие сбалансированности корпоративной стратегии / Н. А. Маргацкий, Г. И. Паламарчук, А. В. Островская, Г. Г. Вукович // Экономика устойчивого развития. – 2025. – № 2 (62). – С. 125–127.
12. Попов, Н. А. Риски и угрозы экономической безопасности в цифровой экономике / Н. А. Попов, З. Х. Иматчоев // Финансово-экономический вестник. – 2023. – № 4-1 (38). –

С. 99–111.

13. Кононенко, Р. В. Безопасность экономической деятельности в условиях цифровизации / Р. В. Кононенко, Е. Г. Наумик-Гладкая // Вестник Белгородского университета кооперации, экономики и права. – 2022. – № 1 (92). – С. 100–110.

14. Науменко, М. И. Внутренние риски кадровой безопасности на предприятии в условиях цифровой трансформации / М. И. Науменко, О. А. Лымарева // Экономика и бизнес: теория и практика. – 2024. – № 1-2 (107). – С. 92–95.

15. Нуретдинова, Ю. В. Влияние цифровой экономики на обеспечение экономической безопасности хозяйствующих субъектов / Ю. В. Нуретдинова, Д. А. Зинченко, Д. И. Нуретдинов // Конкурентоспособность в глобальном мире: экономика, наука, технологии. – 2023. – № 3. – С. 134–135.

16. Бойко, С. В. Структура оценки безопасности в условиях цифровой трансформации экономики знаний и инновационного роста / С. В. Бойко, Н. Н. Покровская, К. С. Лехмус, К. В. Николаева, А. А. Винюков // Научная мысль. – 2022. – Т. 20, № 2-1 (44). – С. 10–16.

17. Агеева, О. А. Специфика обеспечения экономической безопасности в условиях цифровизации / О. А. Агеева, Н. К. Кучукова, Ю. Д. Матыцына // Вестник университета. – 2022. – № 4. – С. 100–106.

Сведения об авторах

Курбанова Анжела Магомедовна, к.ф-м.н., доцент, доцент кафедры биофизики, информатики и медаппаратуры, Дагестанский государственный медицинский университет, Махачкала, Россия

Ибрагимова Элина Саламбековна, ассистент кафедры «Финансы, кредит и антимонопольное регулирование» Чеченского государственного университета им. А.А. Кадырова, Грозный, Россия

Султанов Нариман Гарунович, студент, Факультет информатики и информационных технологий, Дагестанский государственный университет,Махачкала, Россия

Information about the authors

Kurbanova Angela Magomedovna, PhD, Associate Professor, Associate Professor of the Department of Biophysics, Computer Science and Medical Equipment, Dagestan State Medical University, Makhachkala, Russia

Ibragimova Elina Salambekovna. Assistant Professor of the Department of Finance, Credit and Antimonopoly Regulation at the Kadyrov Chechen State University, Grozny, Russia

Sultanov Nariman Garunovich, student, Faculty of Computer Science and Information Technology, Dagestan State University, Makhachkala, Russia