УДК 330
DOI 10.26118/2782-4586.2025.22.72.092

Айгунова Раиса Саидовна
Дагестанский государственный университет
Мамаева Умукусюм Зайнутдиновна
Дагестанский государственный университет
Хасанова Малика Салиховна
Чеченский государственный университет имени А.А. Кадырова

Система экономической безопасности организации в условиях цифровой трансформации и инновационного развития: интегративный подход»

Аннотация. В условиях ускоренной цифровизации экономики и роста геополитической нестабильности обеспечение экономической безопасности (ЭБ) хозяйствующих субъектов приобретает стратегическое значение. Инновационные и цифровые трансформации порождают как новые возможности для роста, так и специфические угрозы – от киберрисков до зависимости от недоступных технологий. Это требует обновления методологических и структурных подходов к обеспечению ЭБ. Цель исследования – разработать интегративную модель системы экономической безопасности организации, адаптированной к реалиям цифровой и инновационной экономики. Результаты исследования включают обобщение современных подходов к оценке ЭБ, актуализацию угроз микроуровня с учетом цифровых и санкционных вызовов, разработку многоуровневой структуры индикаторов ЭБ, а также предложение принципов построения гибкой организационной и правовой инфраструктуры обеспечения безопасности, ориентированной на проактивное управление рисками. В заключение предложенная модель способствует повышению устойчивости хозяйствующих субъектов за счет синергии экономической, информационной и инновационной безопасности. Адаптация системы ЭБ к условиям цифровой трансформации требует междисциплинарного подхода и постоянного мониторинга внешней и внутренней среды.

Ключевые слова: экономическая безопасность, цифровая трансформация, инновационное развитие, кибербезопасность, индикаторы безопасности, угрозы микроуровня, организационная структура, правовое обеспечение.

Aigunova Raisa Saidovna
Dagestan State University
Mamayeva Umukusium Zainutdinovna
Dagestan State University Russia
Khasanova Malika Salikhovna
Kadyrov Chechen State University

The organization's economic security system in the context of digital transformation and innovative development: an integrative approach"

Abstract. In the context of accelerated digitalization of the economy and growing geopolitical instability, ensuring the economic security of economic entities is becoming strategically important. Innovative and digital transformations generate both new growth opportunities and specific threats, from cyber risks to reliance on inaccessible technologies. This requires updating the methodological and structural approaches to ensuring EB. The purpose of the study is to develop an integrative model of an organization's economic security system adapted to the realities of the digital and innovative economy. The results of the study include a generalization of modern approaches to assessing cyber security, updating micro-level threats

taking into account digital and sanctions challenges, developing a multi-level structure of cyber security indicators, as well as proposing principles for building a flexible organizational and legal security infrastructure focused on proactive risk management. In conclusion, the proposed model contributes to increasing the sustainability of business entities through the synergy of economic, information and innovation security. The adaptation of the EB system to the conditions of digital transformation requires an interdisciplinary approach and constant monitoring of the external and internal environment.

Keywords: economic security, digital transformation, innovative development, cybersecurity, security indicators, micro-level threats, organizational structure, legal support.

Введение

Обеспечение экономической безопасности (ЭБ) организации становится ключевым условием её выживаемости и конкурентоспособности в условиях глубокой трансформации социально-экономической среды. Современные вызовы – геополитическая конфронтация, санкционное давление, ускоренная цифровизация, дефицит критически важных технологий – формируют новую архитектуру рисков, которая требует переосмысления традиционных подходов к защите экономических интересов хозяйствующих субъектов.

Актуальность темы обусловлена тем, что инновационные и цифровые преобразования не только расширяют функциональные возможности организаций, но и порождают новые, зачастую системные угрозы: утечки данных, кибератаки, разрывы цифровых цепочек поставок, технологическая зависимость, устаревание ИТ-инфраструктуры и правовые коллизии в сфере регулирования цифровой среды [14]. В этих условиях ЭБ перестаёт быть исключительно финансовой или производственной категорией и приобретает межфункциональный, системный характер.

Постановка проблемы заключается в отсутствии единой, гибкой и динамически адаптируемой модели системы ЭБ, учитывающей мультипликативное влияние цифровых технологий и инновационных процессов. Многие существующие подходы либо игнорируют новые угрозы, либо фрагментируют систему безопасности, не обеспечивая её целостности и управляемости [2, 9].

Целью данного исследования является развитие методических основ обеспечения ЭБ организации в условиях цифровой и инновационной трансформации. Для достижения этой цели были сформулированы следующие задачи:

– проанализировать современные научные подходы к пониманию ЭБ на микроуровне;

– идентифицировать и систематизировать угрозы, возникающие в результате цифровизации и инновационной активности;

– разработать интегративную структуру системы ЭБ, включающую индикаторы, организационные и правовые механизмы;

– предложить рекомендации по построению адаптивной системы управления ЭБ в условиях нестабильности.

Научная новизна исследования состоит в синтезе экономической, информационной и инновационной безопасности в единую систему, а также в методологической актуализации пороговых значений индикаторов с учётом особенностей цифровой среды.

Степень изученности проблемы

Проблематика экономической безопасности организации в научной литературе активно развивается последние два десятилетия, однако её интерпретация в условиях цифровой трансформации остаётся недостаточно системной. Ранние исследования концентрировались на финансовых и производственных аспектах ЭБ. Так, Л. Н. Мамаева, Я. А. Осипова и С. Е. Хожина предложили трёхкомпонентную модель: финансово-экономическая, производственная и социальная проекции с набором из 24 индикаторов

[2]. Однако такой подход не учитывает специфику цифровых рисков и инновационных процессов.

В последующих работах наметился переход к более широкому пониманию ЭБ. И. Г. Борок ввела в анализ кадровый, экологический и, что особенно важно, цифровой аспекты, подчеркивая растущую значимость защиты информации и ИТ-инфраструктуры [3]. Л. М. Ширко предложила использовать сбалансированную систему показателей (BSC), охватывающую финансы, клиентов, процессы и кадры, что приближает подход к управлению ЭБ к стратегическому уровню [4].

Наиболее перспективным направлением стало выделение внутренних и внешних компонент ЭБ. В частности, Г. И. Хаустова и А. Ю. Шиншинов указывают на необходимость учета инновационной, цифровой, правовой и сетевой составляющих в структуре безопасности [5, 2]. При этом отмечается, что универсальная модель ЭБ для всех типов организаций маловероятна, поскольку специфика отрасли, региона и масштаба деятельности существенно влияет на набор угроз и приоритеты защиты [5].

Особую остроту проблеме придали геополитические события после 2022 года. Санкционное давление, ограничение доступа к передовым технологиям и международным финансовым инструментам выявили уязвимости, которые ранее не рассматривались как системные угрозы [14]. В этом контексте исследования В. А. Тешева, С. А. Хатукай и Э. Б. Бабалян подчеркивают необходимость включения технологического суверенитета в систему ЭБ [3].

Несмотря на рост числа публикаций, остаются пробелы:

– слабо проработана методика оценки цифровой зрелости как компонента ЭБ;

– недостаточно исследована взаимосвязь между инновационной активностью и устойчивостью к внешним шокам;

– отсутствуют комплексные рекомендации по построению организационных структур, способных оперативно реагировать на гибридные угрозы.

Таким образом, современная научная база предоставляет фрагментарные решения, требующие систематизации и интеграции в единую модель, адаптированную к условиям 2025 года и последующих лет.

Методы исследования

В ходе исследования использован системный подход, позволяющий рассматривать организацию как сложную, динамически адаптирующуюся социально-экономическую систему, в которой взаимодействуют финансовые, технологические, кадровые и правовые подсистемы. Применён сравнительно-аналитический метод для обобщения и критического осмысления существующих моделей экономической безопасности. Метод индукции позволил выделить общие закономерности из множества частных случаев угроз и рисков в цифровой среде. Дедуктивный подход использовался для формирования обобщённой структуры системы ЭБ на основе теоретических предпосылок. Также применён метод экспертных оценок при определении пороговых значений индикаторов и приоритетов защиты. Анализ нормативно-правовой базы РФ (включая Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры» и Стратегию экономической безопасности РФ до 2030 г.) обеспечил правовую обоснованность предложенных решений. Наконец, использован элементы сценарного анализа для прогнозирования новых угроз, связанных с дальнейшей цифровизацией и импортозамещением.

Результаты исследования и дискуссия

В условиях ускоренной цифровой трансформации экономическая безопасность организации перестаёт быть статичной и одноаспектной категорией. Сегодня она должна рассматриваться как многоуровневая, динамическая и адаптивная система, способная реагировать на вызовы, возникающие как внутри компании, так и в её внешнем

окружении. Эта система объединяет как традиционные компоненты – такие как финансовая устойчивость и производственная надёжность, - так и новые, обусловленные цифровой средой, – включая кибербезопасность, цифровую зрелость и инновационную активность.

На внутреннем уровне безопасность обеспечивается совокупностью взаимосвязанных элементов. Финансовая стабильность проявляется в достаточной ликвидности, устойчивости к валютным колебаниям и надёжном доступе к источникам финансирования. Кадровая безопасность зависит от стабильности коллектива, наличия ключевых компетенций в области информационных технологий, управления данными и аналитики. Производственно-технологическая независимость всё чаще определяется степенью снижения зависимости от импортных компонентов и уровнем автоматизации процессов. Отдельно выделяются информационная и кибербезопасность – они включают не только защиту конфиденциальных данных, но и устойчивость ИТ-инфраструктуры к сбоям, в том числе к DDoS-атакам, а также наличие систем резервного копирования и восстановления. Инновационная составляющая отражает способность организации генерировать и внедрять новшества, что измеряется темпами обновления технологий, долей расходов на исследования и разработки (R&D) и патентной активностью. Цифровая компонента охватывает общий уровень цифровой зрелости, включая использование Big Data, искусственного интеллекта и облачных решений. Наконец, правовая безопасность обеспечивается соответствием требованиям действующего законодательства и эффективной защитой интеллектуальной собственности.

На внешнем уровне организация сталкивается с рыночными, политическими и сетевыми рисками. Рыночная уязвимость связана с высокой конкуренцией и волатильностью спроса. Политические риски проявляются в виде санкционного давления, изменений налоговой или регуляторной политики. Сетевая зависимость отражает степень уязвимости от сбоев у ключевых поставщиков, партнёров или цифровых платформ, от которых зависит функционирование всей цепочки поставок.

Важнейшей чертой предложенной структуры является принцип синергии: угроза, возникшая в одной подсистеме, способна спровоцировать каскадный эффект, затрагивающий другие компоненты. Например, кибератака на ИТ-системы (информационная угроза) может привести к остановке производственных линий (технологический сбой), нарушению обязательств перед клиентами, росту штрафов и, как следствие, утрате доверия на рынке (рыночный и репутационный ущерб).

С учётом текущей геополитической обстановки и задачи обеспечения технологической автономии на микроуровне особую остроту приобретают несколько ключевых угроз. Технологическая зависимость остаётся критической проблемой: более 60 % российских предприятий среднего и крупного бизнеса продолжают использовать зарубежное программное обеспечение и оборудование, доступ к которым может быть ограничен в любой момент без возможности быстрой замены [14]. Киберугрозы демонстрируют тревожную динамику – по данным Минцифры РФ, в 2024 году число кибератак на российские компании выросло на 45 % по сравнению с 2022 годом, особенно активно атакуются критически важные сектора экономики [11]. Дополнительные риски связаны с утечкой интеллектуальной собственности через облачные сервисы и удалённые рабочие места, где контроль над данными ограничен. Параллельно ощущается острая нехватка квалифицированных кадров в области информационной безопасности и управления данными, что снижает способность компаний противостоять современным угрозам. Ускоренное принятие нового законодательства – в сфере локализации данных, этики искусственного интеллекта или регулирования цифровых финансовых активов – порождает регуляторные риски, особенно для компаний, не готовых к быстрой адаптации. Наконец, всё более реальной становится угроза срыва цифровых цепочек поставок из-за блокировок международных платёжных систем, ограничений на экспорт ИТ-оборудования и санкций против ключевых логистических операторов.

Особое внимание следует уделять гибридным угрозам, сочетающим кибер-, информационные и экономические компоненты. Так, целенаправленная дезинформация в социальных сетях может вызвать панику среди клиентов, спровоцировать массовый отказ от услуг и, как следствие, запустить цепную реакцию, ведущую к кризису ликвидности и потере устойчивости.

На основе анализа, проведённого в работах [5, 9, 13], предлагается адаптированная система индикаторов экономической безопасности, которая сочетает традиционные финансово-экономические метрики с новыми, цифровыми показателями, отражающими уровень зрелости, устойчивости и адаптивности организации в условиях технологической турбулентности.

В условиях цифровой трансформации подход к оценке экономической безопасности должен быть гибким и адаптивным. Вместо использования фиксированных пороговых значений для ключевых индикаторов целесообразно устанавливать диапазоны, отражающие отраслевую специфику, масштаб бизнеса и фазу экономического цикла. Например, для коэффициента текущей ликвидности безопасная зона может варьироваться от 1,5 до 3,0, что позволяет учитывать различия между капиталоёмкими производственными предприятиями и компаниями сферы услуг. В высокотехнологичных отраслях, где инновации являются основой конкурентоспособности, доля расходов на исследования и разработки (R&D) должна составлять не менее 3 % от выручки – однако и здесь допустимы корректировки в зависимости от стадии жизненного цикла продукта или стратегии компании. Такой подход исключает формализм и делает систему индикаторов действительно рабочим инструментом управления.

Для эффективного функционирования такой динамичной системы требуется централизованное, но гибкое управление. В этой связи рекомендуется создание Комитета по экономической безопасности, объединяющего ключевые функциональные направления. В его состав должны войти руководитель по информационной безопасности (CISO), отвечающий за защиту цифровых активов; руководитель по инновациям, обеспечивающий баланс между безопасностью и технологическим развитием; финансовый директор, контролирующий устойчивость и риски; представитель юридической службы, отслеживающий соответствие нормативным требованиям; а также ответственный за кадровую политику, поскольку человеческий фактор остаётся одной из главных уязвимостей. Комитет должен проводить ежеквартальный аудит угроз, своевременно обновлять пороговые значения индикаторов и корректировать стратегию защиты с учётом изменяющейся внешней и внутренней среды. Ключевым принципом его работы должен стать сквозной подход – от формирования стратегических целей до реализации операционного контроля, что обеспечивает целостность и согласованность всех мер безопасности.

Особое значение приобретает правовое обеспечение экономической безопасности. Оно должно опираться не только на общие нормы Гражданского и Трудового кодексов РФ, но и на специализированные нормативные акты, отражающие реалии цифровой эпохи. Среди них – Федеральный закон №152-ФЗ «О персональных данных», регулирующий обработку информации о сотрудниках и клиентах; Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры», обязывающий компании из отдельных секторов внедрять меры защиты; указы Президента РФ, закрепляющие концепцию цифрового суверенитета; а также отраслевые стандарты, такие как ГОСТ Р 57580 в области кибербезопасности. На основе этих документов организация обязана разрабатывать внутренние регламенты: политику кибербезопасности, правила этичного и безопасного использования искусственного интеллекта, а также чёткие процедуры реагирования на инциденты, включая кибератаки и утечки данных.

Однако в этом контексте возникают и дискуссионные аспекты. Так, некоторые исследователи, в частности Ю. Г. Графов, предлагают активно использовать искусственный интеллект для прогнозирования угроз и автоматизации принятия решений

[12]. Хотя такие решения повышают скорость реакции, они несут в себе значительные этические и юридические риски – например, предвзятость алгоритмов или нарушение права на объяснение решений. С другой стороны, как отмечает Т. В. Кикоть-Глуходедова, чрезмерный акцент на цифровом суверенитете может превратиться в новую угрозу: изоляция от глобальных технологических экосистем способна замедлить инновационное развитие и снизить конкурентоспособность [15].

Поэтому главной задачей становится поиск баланса между защитой и развитием. Система экономической безопасности не должна выступать в роли «тормоза» для цифровизации. Напротив, её предназначение – создавать надёжные, предсказуемые и соответствующие законодательству условия для безопасного внедрения новых технологий, позволяя организации не просто выживать в условиях неопределённости, но и уверенно развиваться, формируя устойчивые конкурентные преимущества в новой цифровой реальности.

Выводы и заключение

Проведённое исследование подтвердило, что в условиях 2025 года экономическая безопасность организации не может быть обеспечена в рамках узкоспециализированных подходов. Требуется интегративная модель, объединяющая финансовые, технологические, кадровые, правовые и цифровые аспекты в единую управляемую систему.

Ключевым результатом работы стало обновление структуры системы ЭБ с учётом актуальных вызовов: санкционного давления, роста киберугроз, технологической зависимости и дефицита компетенций. Предложенная модель позволяет не только реагировать на угрозы, но и прогнозировать их, используя адаптивные индикаторы и многоуровневый мониторинг.

Особое значение приобретает организационная гибкость: создание межфункциональных комитетов, постоянное обучение персонала, внедрение сквозных процессов управления рисками. Правовое обеспечение должно быть не формальным, а опережающим, включая внутренние стандарты, соответствующие как российскому, так и международному (в части совместимости) регулированию.

В заключение, система экономической безопасности в эпоху цифровой и инновационной трансформации должна быть проактивной, динамичной и междисциплинарной. Только такой подход обеспечит устойчивость организации перед лицом неопределённости и позволит использовать цифровые возможности без ущерба для её экономических интересов.

Дальнейшие исследования могут быть направлены на разработку автоматизированных платформ мониторинга ЭБ, использующих технологии ИИ и Big Data для анализа угроз в реальном времени.

Список источников

1. Баширзаде, Р. Р. К. Теоретико-методологические положения обеспечения экономической безопасности логистических систем в условиях цифровизации экономики / Р. Р. К. Баширзаде // Вестник ОрелГИЭТ. – 2022. – № 1 (59). – С. 20–25.

2. Шиншинов, А. Ю. Трансформация систем экономической безопасности хозяйствующих субъектов в условии цифровой экономики / А. Ю. Шиншинов, О. Е. Васильева // Организатор производства. – 2023. – Т. 31, № 4. – С. 74–85.

3. Тешев, В. А. Экономическая безопасность в условиях цифровой экономики / В. А. Тешев, С. А. Хатукай, Э. Б. Бабалян // Проблемы научной мысли. – 2022. – Т. 1, № 11. – С. 11–16.

4. Жалсанов, М. К. Органы внутренних дел как субъект обеспечения экономической безопасности в условиях цифровой трансформации: анализ понятий, целей, задач и функций / М. К. Жалсанов // Право и государство: теория и практика. – 2023. – № 6 (222). – С. 297–300.

5. Хаустова, Г. И. Теоретические аспекты обеспечения экономической безопасности организации / Г. И. Хаустова // Инновации и инвестиции. – 2024. – № 6. – С. 202–205.
6. Акимова, Н. В. Цифровой суверенитет и экономическая безопасность в эпоху глобализации / Н. В. Акимова, Р. П. Елисеева-Софронова // Академическая наука. – 2025. – № 3. – С. 9–12.
7. Сулумов, С. Х. Формирование системы экономической безопасности предприятия в условиях цифровизации рынка труда / С. Х. Сулумов, Я. Э. Дадаев // ФГУ Наука. – 2024. – № 3 (35). – С. 81–86.
8. Ворсин, Н. А. Цифровые технологии как фактор эффективного обеспечения финансовой безопасности организации / Н. А. Ворсин, А. А. Криничный, М. И. Голубова // Вестник Института дружбы народов Кавказа (Теория экономики и управления народным хозяйством). Экономические науки. – 2024. – № 3 (71). – С. 98–105.
9. Попов, Е. Д. Анализ влияния цифровой трансформации на экономическую безопасность организации / Е. Д. Попов // Инновации и инвестиции. – 2023. – № 10. – С. 165–168.
10. Смирнов, А. А. Организационно-экономический механизм обеспечения экономической безопасности предприятия в современных условиях / А. А. Смирнов, А. К. Арутюнов // Вестник ГГУ. – 2025. – № 1. – С. 547–555.
11. Стативина, Р. Х. Исследование информационной безопасности в цифровой экономике / Р. Х. Стативина // Экономика и бизнес: теория и практика. – 2024. – № 7 (113). – С. 177–180.
12. Графов, Ю. Г. Основные положения методики оценки уровня экономической безопасности цифровых предприятий на основе методологии исследования угроз / Ю. Г. Графов // Российский экономический интернет-журнал. – 2024. – № 3.
13. Свистунов, В. М. Цифровизация как инструмент экономической безопасности современной организации / В. М. Свистунов, О. А. Агеева, И. Д. Мацкуляк // Вестник университета. – 2025. – № 5. – С. 15–27.
14. Блиничкина, Н. Ю. Проблемы обеспечения экономической безопасности в условиях цифровизации / Н. Ю. Блиничкина // Вестник Таджикского государственного университета права, бизнеса и политики. Серия общественных наук. – 2022. – № 3 (92). – С. 30–40.
15. Кикоть-Глуходедова, Т. В. Цифровизация как направление и угроза экономической безопасности государства / Т. В. Кикоть-Глуходедова // Вестник Московского университета МВД России. – 2025. – № 1. – С. 200–206.
16. Пахарев, А. В. Влияние цифровизации теневой экономики на экономическую безопасность государства / А. В. Пахарев, С. Ю. Александрова // Технико-технологические проблемы сервиса. – 2022. – № 2 (60). – С. 85–92.
17. Кутузов, А. А. Направления повышения экономической безопасности промышленных предприятий в условиях цифровизации / А. А. Кутузов // Russian Economic Bulletin. – 2025. – Т. 8, № 2. – С. 359–366.

Сведения об авторах

Айгунова Раиса Саидовна, к.э.н., доцент кафедры «Экономической безопасности, анализа и аудита», Дагестанский государственный университет, Махачкала, Россия
Мамаева Умукусюм Зайнутдиновна, к.э.н., доцент кафедры «Экономической безопасности, анализа и аудита», Дагестанский государственный университет, Махачкала, Россия
Хасанова Малика Салиховна, ст. преподаватель кафедры «Налоги и налогообложение», Чеченский государственный университет имени А.А. Кадырова, Грозный, Россия

Information about the authors

Aigunova Raisa Saidovna, PhD in Economics, Associate Professor of the Department of Economic Security, Analysis and Audit, Dagestan State University, Makhachkala, Russia

Mamayeva Umukusium Zainutdinovna, PhD in Economics, Associate Professor of the Department of Economic Security, Analysis and Audit, Dagestan State University, Makhachkala, Russia
Malika Salikhovna Khasanova, Senior Lecturer at the Department of Taxes and Taxation, Kadyrov Chechen State University, Grozny, Russia