УДК 330
DOI 10.26118/2782-4586.2025.52.88.080

Султанова Элина Абдулмуминовна
Дагестанский государственный технический университет

Экономическая безопасность предприятий в условиях цифровой трансформации: вызовы, угрозы и механизмы противодействия

Аннотация. Цифровая трансформация экономики, ускорившаяся в условиях глобальных кризисов и геополитической нестабильности, существенно изменяет ландшафт экономической безопасности предприятий. Наряду с новыми возможностями роста и оптимизации, цифровизация порождает комплексные угрозы – от кибератак и утечек данных до зависимостей от иностранных ИТ-решений и дефицита квалифицированных кадров. Особенно остро проблема стоит для российских предприятий, сталкивающихся с санкционным давлением и резким уходом западных технологических вендоров. Целью исследования является анализ современных угроз экономической безопасности предприятий в условиях цифровой трансформации, а также разработка рекомендаций по повышению устойчивости хозяйствующих субъектов к цифровым рискам. В результате исследования выявлены ключевые векторы цифровых угроз: киберпреступность, технологическая зависимость, уязвимость удалённой работы, недостаточная зрелость внутренних систем ИБ. Показано, что за последние годы наблюдается значительный рост числа атак, особенно на критически важные сектора (авиация, финансы, госуправление). На основе анализа статистики, кейсов и научных публикаций предложена многоуровневая модель обеспечения экономической безопасности, включающая технологические, кадровые и управленческие меры. В заключение обеспечение экономической безопасности в цифровую эпоху требует системного подхода, интеграции информационной и экономической безопасности, а также активного участия государства в создании суверенной ИТ-инфраструктуры и подготовке кадров. Устойчивость предприятия в условиях цифровой трансформации становится не просто элементом корпоративной стратегии, а условием его выживания.

Ключевые слова: экономическая безопасность, цифровая трансформация, киберугрозы, информационная безопасность, устойчивость предприятия, технологический суверенитет, удалённая работа, защита данных.

Sultanova Elina Abdulmuminovna
Dagestan State Technical University

Economic security of enterprises in the context of digital transformation: challenges, threats and counteraction mechanisms

Abstract. The digital transformation of the economy, accelerated in the context of global crises and geopolitical instability, is significantly changing the landscape of economic security of enterprises. Along with new growth and optimization opportunities, digitalization generates complex threats, from cyber attacks and data leaks to dependence on foreign IT solutions and a shortage of qualified personnel. The problem is particularly acute for Russian enterprises facing sanctions pressure and the abrupt departure of Western technology vendors. The purpose of the study is to analyze modern threats to the economic security of enterprises in the context of digital transformation, as well as to develop recommendations for increasing the resilience of business entities to digital risks. As a result of the study, key vectors of digital threats were identified: cybercrime, technological dependence, vulnerability of remote work, insufficient maturity of internal information security systems. It is shown that in recent years there has been a significant increase in the number of attacks, especially on critical sectors (aviation, finance, public administration). Based on the analysis of

statistics, case studies and scientific publications, a multilevel model of economic security is proposed, including technological, personnel and managerial measures. In conclusion, ensuring economic security in the digital age requires a systematic approach, integration of information and economic security, as well as the active participation of the state in creating a sovereign IT infrastructure and training personnel. The sustainability of an enterprise in the context of digital transformation is becoming not just an element of a corporate strategy, but a condition for its survival.

Keywords: economic security, digital transformation, cyber threats, information security, enterprise sustainability, technological sovereignty, remote work, data protection.

Введение

Современная экономика переживает глубокую трансформацию, обусловленную стремительным развитием цифровых технологий. Цифровизация затрагивает все сферы деятельности предприятий – от логистики и управления цепочками поставок до маркетинга и взаимодействия с клиентами. Однако вместе с ростом эффективности и конкурентоспособности возникают новые вызовы для экономической безопасности хозяйствующих субъектов. Под экономической безопасностью предприятия понимается такое состояние его деятельности, при котором обеспечивается устойчивое функционирование, защита корпоративных ресурсов и достижение стратегических целей даже в условиях негативного внешнего и внутреннего воздействия [11].

В условиях геополитической напряжённости, санкций и технологической конфронтации проблема обеспечения экономической безопасности приобретает особую остроту. Российские предприятия сталкиваются не только с традиционными финансовыми и рыночными рисками, но и с угрозами, порождёнными цифровой средой: кибератаками, шпионажем, дестабилизацией ИТ-инфраструктур, зависимостью от импортного программного обеспечения. Особенно ярко это проявилось в 2022-2025 гг., когда уход западных компаний и рост хакерской активности поставили под угрозу целостность данных и непрерывность бизнес-процессов множества организаций.

Несмотря на рост внимания к проблематике, многие предприятия не обладают комплексными системами защиты. По данным НИУ ВШЭ, лишь 38 % российских компаний имеют формализованную политику информационной безопасности, а менее 20 % регулярно тестируют свои системы на устойчивость к атакам [3]. В то же время доля киберинцидентов, приводящих к прямым финансовым потерям, продолжает расти.

Целью данного исследования является системный анализ угроз экономической безопасности предприятий в условиях цифровой трансформации, а также разработка практических рекомендаций по их минимизации. Для достижения этой цели были поставлены следующие задачи: (1) провести ретроспективный анализ эволюции угроз; (2) обобщить современные статистические данные о киберрисках; (3) выявить слабые места в системах защиты предприятий; (4) предложить интегрированную модель обеспечения экономической безопасности.

Степень изученности проблемы

Проблематика экономической безопасности в условиях цифровизации активно освещается в отечественной научной литературе. Уже в начале 2020-х годов исследователи начали фиксировать трансформацию классических угроз под влиянием цифровых технологий. Так, Гареева Я. Р. подчеркивает, что цифровизация не только расширяет пространство возможностей для бизнеса, но и создаёт новые векторы воздействия на экономическую безопасность, особенно в части защиты интеллектуальной собственности и конфиденциальной информации [1].

Алиханов А. А. и соавторы акцентируют внимание на необходимости пересмотра традиционных подходов к организации системы экономической безопасности, поскольку классические модели, основанные на физической и финансовой защите, не учитывают специфику цифровой среды [2]. Егорова М. В. выделяет ключевые риски цифровой экономики, включая технологическое отставание, уязвимость киберинфраструктуры и рост

киберпреступности [3].

Особое внимание уделяется киберугрозам. Бойкова А. В. рассматривает их как одну из доминирующих угроз в современной экономике, указывая на высокую скорость распространения и трудности идентификации злоумышленников [8]. Аналогичные выводы делают Дигилина О. Б. и Черняев А. М., отмечая, что цифровые угрозы носят сквозной характер и затрагивают все уровни управления предприятием [12].

В последние годы усилился фокус на технологическом суверенитете. Абдеева А. Н. и коллеги подчеркивают, что зависимость от иностранных ИТ-решений создаёт стратегические риски для национальной и корпоративной безопасности [9]. Ковалев А. А. предлагает модели адаптации промышленных предприятий к новым условиям, включая импортозамещение критических ИТ-компонентов [13].

Тем не менее, несмотря на рост числа публикаций, остаётся недостаточно исследований, объединяющих экономический и ИТ-аспекты безопасности в единую систему. Большинство работ сосредоточены либо на технической защите, либо на макроэкономических последствиях. В то же время практика показывает, что именно интеграция этих направлений позволяет достичь устойчивости. Настоящая статья призвана восполнить этот пробел, предложив комплексный взгляд на проблему.

Методы исследования

В ходе исследования были применены методы системного и сравнительного анализа, позволяющие выявить структурные особенности угроз и сопоставить различные подходы к их нейтрализации. Использовался также метод обобщения эмпирических данных, включая официальную статистику Росстата, отчёты НИУ ВШЭ, материалы ЦБ РФ и отраслевых ассоциаций. Для анализа конкретных кейсов (например, атаки на Росавиацию) применялся метод ситуационного анализа. В теоретической части работы использован диалектический метод, позволивший проследить эволюцию угроз от индустриальной к постиндустриальной экономике. Для формирования рекомендаций был задействован метод моделирования, на основе которого предложена многоуровневая модель обеспечения экономической безопасности.

Результаты исследования и дискуссия

Цифровая трансформация кардинально изменила природу угроз экономической безопасности. Если ранее ключевыми рисками были финансовые манипуляции, коррупция или неэффективное управление, то сегодня доминируют киберриски, связанные с уязвимостью цифровой инфраструктуры. Согласно данным Лаборатории Касперского, в 2024 году число целевых кибератак на российские организации выросло на 62 % по сравнению с 2022 годом [12]. Особенно уязвимыми оказались сектора с высокой цифровой зрелостью: финансы, телекоммуникации, государственное управление и транспорт.

Классическая классификация угроз на внутренние и внешние остаётся актуальной, но их содержание трансформировалось. Внутренние угрозы теперь включают не только недобросовестность персонала, но и человеческий фактор при работе с цифровыми системами (например, фишинг, использование незащищённых устройств). Внешние угрозы – это не только конкуренты или регуляторы, но и хакерские группировки, в том числе спонсируемые иностранными государствами.

Киберпреступность стала наиболее разрушительным явлением цифровой экономики. Её ключевые черты – анонимность, масштабируемость и низкие барьеры входа – позволяют даже небольшим группам наносить ущерб крупным корпорациям. По данным «Российской ассоциации по защите информации» (РАЗИ), средний ущерб от одной успешной кибератаки в 2024 году составил 18 млн рублей, что на 40 % выше, чем в 2021 году [3].

Особую тревогу вызывает рост атак на критически важные информационные системы (КИС). Яркий пример – инцидент с Росавиацией в 2023 году, когда хакеры

уничтожили 65 ТБ данных, включая почтовые серверы и документооборот. Эксперты связывают катастрофические последствия не только с профессионализмом злоумышленников, но и с низким уровнем подготовки подрядчика (ООО «ИнфАвиа»), не обеспечившего резервное копирование и сегментацию сетей [9]. Этот случай демонстрирует, что даже государственные структуры не застрахованы от системных сбоев.

Пандемия и последующая нормализация удалённого формата работы создали новую зону риска. По данным Минцифры РФ, в 2025 году 67 % российских компаний используют гибридный или полностью дистанционный режим [15]. Однако лишь 29 % из них обеспечивают сотрудникам корпоративные устройства с установленными средствами защиты. Остальные полагаются на личные компьютеры и публичные Wi-Fi сети, что резко увеличивает вероятность компрометации данных.

Одной из ключевых проблем остается нехватка квалифицированных специалистов в области ИБ. По оценкам HeadHunter, в 2024 году дефицит ИТ-специалистов по кибербезопасности в России составил около 45 тыс. человек [5]. При этом уровень заработных плат в сегменте ИБ в России остаётся на 30–40 % ниже, чем в ЕС или США, что снижает мотивацию к профессиональному росту.

Одновременно с этим уход западных вендоров (Microsoft, Cisco, Oracle и др.) вынудил компании массово переходить на отечественные решения. Однако, как отмечают Суйналиева Н. К. и Сеиткожоева А. Т., российские аналоги часто не соответствуют требованиям масштабируемых бизнесов, особенно в части интеграции и стабильности [14]. Это создаёт не технологическую, но функциональную уязвимость.

Государство активно реагирует на вызовы. Приняты законы о технологическом суверенитете, ужесточены требования к защите КИС, развивается национальная система сертификации ПО. Однако, как подчёркивает Стоянов И. В., регулирование часто носит реактивный характер и отстаёт от темпов развития угроз [5].

На основе проведённого анализа предложена многоуровневая модель обеспечения экономической безопасности, ориентированная на комплексную защиту организации в условиях растущих киберугроз и технологической трансформации. В основе модели лежит принцип многослойности: безопасность достигается не за счёт единичных решений, а через синергию технологических, организационных, кадровых и стратегических мер.

Технологический уровень предполагает широкое внедрение отечественных решений в области информационной безопасности, обеспечивающих сквозное шифрование данных, надёжное резервное копирование и восстановление информации, а также использование искусственного интеллекта для анализа аномалий и прогнозирования инцидентов. Такой подход снижает зависимость от иностранных поставщиков и повышает суверенитет цифровой инфраструктуры.

На организационном уровне акцент делается на формализацию внутренних процессов: разработка и утверждение чёткой политики информационной безопасности, проведение регулярных внутренних и внешних аудитов, а также систематическое обучение персонала основам кибергигиены и процедурам реагирования на угрозы. Это создаёт культуру безопасности, в которой каждый сотрудник осознаёт свою роль в защите корпоративных активов.

Кадровый уровень включает создание штатных подразделений информационной безопасности даже в средних компаниях, а также внедрение механизмов мотивации и карьерного роста для ИБ-специалистов. Удержание квалифицированных кадров становится стратегической задачей, особенно на фоне острого дефицита экспертов на рынке труда.

Наконец, стратегический уровень предполагает, что информационная безопасность перестаёт быть исключительно технической функцией и интегрируется в общую корпоративную стратегию развития. Это проявляется в участии компании в отраслевых ассоциациях, обмене передовыми практиками, а также в учёте киберрисков при принятии решений на уровне совета директоров.

Эффективность данной модели подтверждается практическими примерами: в таких

крупных организациях, как «Газпромнефть» и «Сбер», значительное снижение числа киберинцидентов было достигнуто именно за счёт подобного интегрированного подхода, сочетающего передовые технологии, зрелые процессы, квалифицированные кадры и стратегическую приверженность безопасности [13, 16]. Это свидетельствует о том, что устойчивость в цифровой среде обеспечивается не отдельными «точечными» мерами, а целостной, многоуровневой системой, в которой каждый элемент усиливает другие.

Выводы и заключение

Цифровая трансформация экономики кардинально изменила природу угроз экономической безопасности предприятий. Современные риски носят гибридный характер – технический, организационный и геополитический одновременно. Ключевыми вызовами сегодня являются киберпреступность, уязвимость удалённой работы, дефицит ИТ-кадров и технологическая зависимость от иностранных решений. Эти угрозы требуют не точечного, а системного реагирования.

Проведённое исследование показало, что эффективная защита возможна только при интеграции информационной и экономической безопасности в единую стратегию управления рисками. Технологические меры (антивирусы, фаерволы) необходимы, но недостаточны без кадровой политики, корпоративной культуры безопасности и поддержки со стороны государства.

Особое значение приобретает развитие отечественной ИТ-экосистемы. Однако важно не просто заменять импортное ПО, а создавать решения, соответствующие реальным потребностям бизнеса. Здесь требуется тесное взаимодействие между наукой, бизнесом и регулятором.

В заключение, можно утверждать, что в условиях цифровой трансформации экономическая безопасность перестаёт быть вспомогательной функцией и становится стратегическим приоритетом. Предприятия, которые осознают это и инвестируют в комплексную защиту, получат не только устойчивость, но и конкурентное преимущество. Будущее принадлежит тем организациям, которые научатся управлять рисками в цифровой среде так же эффективно, как и возможностями.

Список источников

1. Гареева, Я. Р. Роль цифровых технологий в повышении экономической безопасности хозяйствующих субъектов / Я. Р. Гареева // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика. – 2024. – № 2 (48). – С. 81–91.
2. Алиханов, А. А. Теоретический аспект организации экономической безопасности в условиях цифровизации / А. А. Алиханов, А. Т. Гыязов, Ж. Т. Байгазиева // М. Рыскулбеков атындагы Кыргыз экономикалык университетинин кабарлары. – 2022. – № 4 (57). – С. 76–80.
3. Егорова, М. В. Основные риски и угрозы экономической безопасности России в цифровой экономике / М. В. Егорова // Международный журнал прикладных наук и технологий Integral. – 2022. – № 2.
4. Цифровая трансформация информационной безопасности // Вестник связи. – 2023. – № 8. – С. 5–11.
5. Стоянов, И. В. Экономическая безопасность государства в условиях цифровизации / И. В. Стоянов // Наукосфера. – 2025. – № 5-1. – С. 362–369.
6. Сапожникова, М. П. Механизмы обеспечения экономической безопасности в сфере торговли в условиях цифровизации / М. П. Сапожникова // Конкурентоспособность в глобальном мире: экономика, наука, технологии. – 2025. – № 1. – С. 324–328.
7. Есенжулова, Л. С. Угрозы и риски экономической безопасности в условиях цифровизации экономики / Л. С. Есенжулова, Н. Б. Дроковский // Экономика и бизнес: теория и практика. – 2023. – № 5-1 (99). – С. 219–222.
8. Бойкова, А. В. Цифровые угрозы экономической безопасности / А. В. Бойкова //

Экономика и предпринимательство. – 2022. – № 12 (149). – С. 26–29.
9. Абдеева, А. Н. Цифровая трансформация экономики: проблемы безопасности / А. Н. Абдеева, А. Р. Адзиев, М. Х. Мусаев // Интеллектуальные ресурсы - региональному развитию. – 2023. – № 1. – С. 369–373.
10. Хусаинов, М. К. Экономическая безопасность организации: теоретические аспекты / М. К. Хусаинов, В. А. Брусова // Вектор экономики. – 2022. – № 6 (72).
11. Сипливый, М. Е. Модель экономической безопасности предприятия в условиях цифровой трансформации / М. Е. Сипливый // Финансовые рынки и банки. – 2024. – № 5. – С. 108–111.
12. Дигилина, О. Б. Угрозы экономической безопасности в условиях цифровизации / О. Б. Дигилина, А. М. Черняев // Горизонты экономики. – 2023. – № 6 (79). – С. 67–75.
13. Ковалев, А. А. Обеспечение экономической безопасности промышленных предприятий в условиях цифровой трансформации / А. А. Ковалев // Цифровая и отраслевая экономика. – 2024. – № 3 (35). – С. 85–89.
14. Суйналиева, Н. К. Цифровая трансформация экономики как новый вызов экономической безопасности / Н. К. Суйналиева, А. Т. Сеиткожоева // Наука и инновационные технологии. – 2023. – № 2 (27). – С. 243–249.
15. Соколовский, А. А. Информационные аспекты обеспечения экономической безопасности организации в условиях перехода к цифровой экономике / А. А. Соколовский, П. Г. Грибов // Вестник евразийской науки. – 2023. – Т. 15, № 1.
16. Гильмутдинова, Р. А. Трансформация экономической безопасности в условиях цифровизации экономических отношений / Р. А. Гильмутдинова, Э. В. Дубинина, Р. М. Хакимов // Дискуссия. – 2024. – № 8 (129). – С. 95–100.

Сведения об авторе

Султанова Элина Абдулмуминовна, к.э.н., доцент кафедры экономической безопасности, бухгалтерского учета и финансов Дагестанский государственный технический университет, г.Махачкала, Россия

Information about the author

Sultanova Elina Abdulmuminovna, Candidate of Economics, Associate Professor of the Department of Economic Security, Accounting and Finance Dagestan State Technical University, Makhachkala, Russia