УДК:338
DOI 10.26118/2783.2025.29.94.029

Сулейманова Динара Абдулбасировна
Дагестанский государственный университет,
Алиев Магомед Абдулхалимович
Дагестанский государственный университет
Магомедова Мадина Абдусаламовна
Дагестанский государственный университет

Роль кибербезопасности в обеспечении устойчивости и конкурентоспособности цифровой экономики

Аннотация. Актуальность исследования обусловлена стремительной цифровизацией всех секторов экономики, сопровождающейся резким ростом числа и сложности киберугроз, наносящих значительный ущерб как частному, так и государственному секторам. По оценкам международных организаций, совокупные глобальные потери от киберпреступности в 2024 году достигли 13,8 трлн долларов США, что подчеркивает необходимость системного подхода к обеспечению кибербезопасности [4]. Целью исследования является анализ роли кибербезопасности как ключевого фактора устойчивого развития и конкурентоспособности цифровой экономики в условиях современных вызовов, а также формулирование рекомендаций по совершенствованию стратегий защиты на национальном и корпоративном уровнях. В ходе исследования использованы методы системного анализа, сравнительного анализа, статистической обработки данных, а также методы контент-анализа научных публикаций и нормативно-правовых актов. Научная новизна исследования заключается в комплексном синтезе актуальных статистических данных за 2024-2025 гг., выявлении новых трендов в структуре киберинцидентов и обосновании необходимости интеграции квантовых технологий и ИИ-ориентированных систем защиты в национальные стратегии кибербезопасности. К результатам исследования относятся обновлённая статистика по киберугрозам в РФ и мире, выявление роста доли инцидентов до 9-12%, а также подтверждение эффективности государственного регулирования, киберстрахования и международного сотрудничества как ключевых инструментов снижения рисков. В заключении подчёркивается, что устойчивость цифровой экономики возможна только при обеспечении многоуровневой, адаптивной и предиктивной модели кибербезопасности, основанной на синергии государственных, корпоративных и образовательных инициатив.

Ключевые слова: кибербезопасность, цифровая экономика, устойчивое развитие, киберугрозы, искусственный интеллект, блокчейн, киберстрахование, цифровая трансформация.

Suleymanova Dinara Abdulbasirovna
Dagestan State University,
Aliev Magomed Abdulkhalimovich
Dagestan State University
Magomedova Madina Abdusalamovna,
Dagestan State University,

The role of cybersecurity in ensuring the sustainability and competitiveness of the digital economy

Abstract. The relevance of the study is due to the rapid digitalization of all sectors of the economy, accompanied by a sharp increase in the number and complexity of cyber threats, causing significant damage to both the private and public sectors. According to estimates by international organizations, the total global losses from cybercrime in 2024 reached 13.8 trillion US dollars, which underscores the need for a systematic approach to cybersecurity [4]. The purpose of the study is to

analyze the role of cybersecurity as a key factor in the sustainable development and competitiveness of the digital economy in the face of modern challenges, as well as to formulate recommendations for improving protection strategies at the national and corporate levels. The research uses methods of system analysis, comparative analysis, statistical data processing, as well as methods of content analysis of scientific publications and regulatory legal acts. The scientific novelty of the study lies in the comprehensive synthesis of relevant statistical data for 2024-2025, the identification of new trends in the structure of cyber incidents and the justification of the need to integrate quantum technologies and AI-oriented protection systems into national cybersecurity strategies. The results of the study include updated statistics on cyber threats in the Russian Federation and the world, identification of an increase in the proportion of incidents to 9-12%, as well as confirmation of the effectiveness of government regulation, cyber insurance and international cooperation as key risk reduction tools. In conclusion, it is emphasized that the sustainability of the digital economy is possible only with the provision of a multi-level, adaptive and predictive cybersecurity model based on the synergy of government, corporate and educational initiatives.

Keywords: cybersecurity, digital economy, sustainable development, cyber threats, artificial intelligence, blockchain, cyber insurance, digital transformation.

Введение

Современное развитие мировой экономики невозможно представить без цифровых технологий, которые трансформировали не только бизнес-процессы, но и государственное управление, здравоохранение, образование и социальные сферы. Цифровая экономика, основанная на данных, облачных сервисах, интернете вещей и искусственном интеллекте, становится главным двигателем роста национальных экономик. Однако вместе с этим растёт и уязвимость – киберугрозы приобрели беспрецедентный масштаб, сложность и экономическое воздействие [12].

По данным Cybersecurity Ventures, к 2025 году ежегодные глобальные потери от киберпреступности достигнут 10,5 трлн долларов, а к 2028 году могут превысить 15 трлн долларов [15]. В России число зарегистрированных киберинцидентов, по данным Национального координационного центра по компьютерным инцидентам (CERT.GOV.RU), выросло на 37% в 2024 году по сравнению с 2022 годом [8]. Особенно заметен рост атак категории High – с 2% до 9% за один квартал, что демонстрирует смещение тактики злоумышленников в сторону целевых и критических атак [4].

В этих условиях кибербезопасность перестаёт быть исключительно технической задачей и становится стратегическим императивом обеспечения экономической устойчивости, инвестиционной привлекательности и национальной безопасности. Государственные программы, такие как «Цифровая экономика Российской Федерации», выделяют значительные ресурсы на развитие отечественных решений в области информационной безопасности, включая поддержку разработчиков ПО, внедрение стандартов киберстрахования и подготовку кадров [2].

Цель настоящего исследования – проанализировать роль кибербезопасности как фактора устойчивого развития цифровой экономики, обновить статистическую и нормативную базу на основе данных 2021–2025 гг., а также выявить наиболее эффективные стратегии противодействия киберугрозам в условиях геополитической нестабильности и технологической трансформации.

Обзор литературы

Исследования последних лет подчёркивают тесную взаимосвязь между уровнем кибербезопасности и устойчивостью цифровой экономики. По мнению Абян и соавт., защита экономических данных от кибератак является необходимым условием сохранения конкурентоспособности организаций [1]. Аналогичную позицию занимают Корнеев и Черпаков, указывая, что кибербезопасность формирует «доверительный климат» для цифровых транзакций и инвестиций [10].

Особое внимание в научной литературе уделяется технологическим решениям. Так,

Верников и Еремеев отмечают, что инвестиции в кибербезопасность напрямую влияют на устойчивость экономики, особенно в условиях санкционного давления [6]. Блокчейн рассматривается как ключевая технология для обеспечения прозрачности и целостности данных, особенно в финансовых и логистических цепочках [3]. Однако его массовое внедрение сдерживается высокой стоимостью и нехваткой квалифицированных специалистов [5].

Отдельное направление – человеческий фактор. Исследования Исламгереевой и Эдисултановой показывают, что до 80% успешных атак связаны с ошибками сотрудников, что подчёркивает важность повышения киберграмотности [9]. Образовательные инициативы, включая программы в МГУ и СПбГУ, рассматриваются как долгосрочная мера укрепления кибериммунитета общества [8].

Киберстрахование также становится важным инструментом управления рисками. Как показывает опыт США и Германии, наличие полисов стимулирует компании внедрять передовые системы защиты [12]. В России данный институт только начинает развиваться, но уже включён в стратегию «Цифровая экономика» как приоритетное направление [2].

Несмотря на обширную литературу, остаётся недостаток комплексных исследований, объединяющих актуальные статистические данные, технологические тренды и оценку эффективности государственной политики в области кибербезопасности. Данная статья призвана восполнить этот пробел.

Основная часть

Анализ данных за последние пять лет показывает неуклонный рост как количества, так и сложности кибератак. По отчёту IBM Cost of a Data Breach 2024, средняя стоимость утечки данных в мире составила 4,88 млн долларов – это исторический максимум [4]. В России этот показатель оценивается в 2,1 млн долларов, однако с учётом роста критичности инцидентов ожидается его увеличение в ближайшие годы [8].

Особую тревогу вызывает рост доли атак категории High. Если в 2021 году такие инциденты составляли менее 1% от общего числа, то в I квартале 2024 года – уже 9% [4]. Это свидетельствует о переходе злоумышленников от массовых спам-кампаний к целевым атакам на критически важные инфраструктуры: энергетику, здравоохранение, госуправление.

Таблица 1 – Динамика распределения киберинцидентов по категориям за 2021–2024 гг.

од	Вредоносное ПО (%)	Несанкционированный доступ (%)	Эксплуатация уязвимостей (%)	Социальная инженерия (%)
021	25	19	16	12
022	26	18	17	14
023	27	17	17	18
024*	27	11	14	22

* – данные за I квартал 2024 г. (источник: CERT.GOV.RU, RT-SOLAR)

По таблице 1 видно, что наблюдается стагнация в сегменте вредоносного ПО, но резкий рост атак, основанных на социальной инженерии (с 12% до 22%). Это подтверждает гипотезу о том, что современные киберпреступники всё чаще используют человеческий фактор как «точку входа» [9]. Одновременно снижается доля несанкционированного доступа – вероятно, благодаря усилению систем аутентификации и мониторинга.

Наиболее опасными остаются инциденты, связанные с несогласованным доступом к информационным системам. В I квартале 2024 года они составляли 49% от всех High-инцидентов, что на 8% больше, чем в предыдущем квартале [4].

Таблица 2 – Топ-3 киберинцидентов категории High (I квартал 2024 г.)

Тип инцидента	Доля (%)	Изменение по сравнению с Q4 2023
Несогласованный доступ к ИС	49	+8
Использование легитимного ПО в злонамеренных целях	28	-7
Эксплуатация нуледей-уязвимостей	23	+5

Таблица 2 показывает рост доли несогласованного доступа указывает на использование краденых учетных данных и compromised identities. Это требует перехода от традиционной модели «периметральной защиты» к концепции Zero Trust, где каждая операция верифицируется независимо от источника [5].

В рамках национальной программы «Цифровая экономика» на период 2021–2024 годов российское правительство выделило свыше 87 млрд рублей на реализацию мероприятий в рамках подраздела «Информационная безопасность» [2]. Эти средства направлены на формирование технологического суверенитета и повышение устойчивости киберпространства страны. Значительная часть финансирования была инвестирована в разработку и продвижение отечественного программного обеспечения, включая защищённые операционные системы, такие как Astra Linux, а также специализированные решения по защите данных и управления доступом, объединённые под общим брендом «Защита ОС».

Параллельно ведётся создание и укрепление инфраструктуры раннего предупреждения и реагирования на киберугрозы – в частности, через развитие центров мониторинга и анализа, таких как национальный CERT (Computer Emergency Response Team) и коммерческие платформы, например, Threat Intelligence от «Лаборатории Касперского». Эти центры обеспечивают сбор, анализ и распространение информации о новых векторах атак, уязвимостях и вредоносных кампаниях, что позволяет организациям оперативно адаптировать свои защитные меры.

Кроме того, в рамках программы активно внедряются современные национальные стандарты информационной безопасности, в первую очередь обновлённый ГОСТ Р ИСО/МЭК 27001–2023, гармонизированный с международным стандартом ISO/IEC 27001. Его применение способствует систематизации подходов к управлению информационной безопасностью, повышает доверие как со стороны регуляторов, так и деловых партнёров, а также формирует единые требования к защите данных в государственном и частном секторах. В совокупности эти меры свидетельствуют о переходе России от фрагментарной киберзащиты к комплексной, институционализированной системе обеспечения цифровой безопасности.

Особое внимание уделяется субъектам малого и среднего предпринимательства (МСП), которые из-за ограниченных ресурсов часто становятся «слабым звеном» в цепи поставок [4]. В 2023 году был запущен пилотный проект по субсидированию киберстрахования для МСП в Дагестане и Татарстане, что может стать моделью для других регионов [8].

Искусственный интеллект применяется как для защиты, так и для атак. С одной стороны, ИИ-системы (например, SIEM с ML-аналитикой) позволяют выявлять аномалии в реальном времени. С другой – злоумышленники используют deepfake и автоматизированные фишинговые кампании [9].

Блокчейн, несмотря на ограничения по масштабируемости, демонстрирует эффективность в аудите логов, цепочках поставок и цифровой идентификации [3]. Например, платформа «Цифровой рубль» в пилотной фазе использует гибридную архитектуру на основе распределённого реестра [6].

Россия активно участвует в инициативах ШОС и ЕАЭС по обмену данными об угрозах [8]. Однако из-за геополитической напряжённости сотрудничество с западными странами ограничено, что затрудняет доступ к передовым решениям и стандартам ENISA, NIST [11].

Обсуждение полученных результатов

Полученные данные подтверждают, что кибербезопасность перешла из разряда вспомогательных функций в категорию стратегических ресурсов национальной экономики. Рост доли High-инцидентов указывает на необходимость отказа от реактивной модели защиты в пользу предиктивной и адаптивной.

Устойчивость цифровой экономики в современных условиях обеспечивается не за счёт разрозненных усилий, а благодаря синергии трёх взаимодополняющих основ, которые можно назвать её «столпами». Первый из них – государственное регулирование – задаёт правовую и институциональную рамку, в которой развивается цифровая среда. Оно реализуется через принятие нормативных актов, направленных на защиту данных и критической инфраструктуры, целевое финансирование приоритетных направлений (таких как развитие отечественного ПО или киберрезилиентность), а также разработку и внедрение единых технических и организационных стандартов, обеспечивающих совместимость и безопасность цифровых систем на национальном уровне.

Второй столп – корпоративная ответственность – отражает зрелость бизнеса как субъекта цифровой экосистемы. Ведущие компании всё чаще отказываются от устаревшей модели «периметральной безопасности» в пользу архитектуры Zero Trust, предполагающей недоверие ко всем внутренним и внешним взаимодействиям без непрерывной верификации. Дополнительно усилия по обеспечению устойчивости подкрепляются практиками киберстрахования, которое не только компенсирует ущерб от инцидентов, но и стимулирует повышение уровня защиты, а также внедрением ИИ-систем мониторинга, способных в реальном времени выявлять аномалии, предсказывать угрозы и автоматизировать реагирование.

Третий, не менее важный элемент – образование и киберграмотность – формирует человеческий капитал, без которого даже самые передовые технологии теряют эффективность. Этот аспект охватывает как академическую подготовку специалистов в вузах, где обновляются учебные программы с акцентом на практические навыки в области кибербезопасности, управления данными и этики ИИ, так и регулярные корпоративные тренинги для всего персонала – от линейных сотрудников до топ-менеджмента. Именно уровень цифровой и киберграмотности определяет, насколько устойчивой будет «человеческая» составляющая цифровой экономики, ведь большинство инцидентов до сих пор начинаются с ошибки или недостаточной осведомлённости человека [1].

Только при равновесном развитии всех трёх столпов – государственного регулирования, корпоративной ответственности и образовательной базы – возможно построение цифровой экономики, способной выдерживать внешние шоки, противостоять киберугрозам и обеспечивать устойчивое развитие на основе доверия, инноваций и технологического суверенитета.

Важным выводом является то, что технологические решения сами по себе недостаточны. Эффективность систем защиты возрастает только при их интеграции в корпоративную культуру и стратегическое планирование [10].

Также подтверждается гипотеза о глобальном характере киберугроз. Локальные меры, даже самые передовые, не способны обеспечить полную защиту без международной координации. В этом контексте опыт ШОС может стать альтернативой западным моделям [8].

Наконец, необходимо признать, что киберстрахование в России находится на начальном этапе. Для его развития требуется:

– разработка единых методик оценки рисков;

– налоговые льготы для застрахованных компаний;
– создание пулов перестрахования на уровне государства.

Выводы и заключение

Кибербезопасность – неотъемлемая часть устойчивого развития цифровой экономики. Анализ показал, что современные угрозы носят комплексный, трансграничный и высокотехнологичный характер, что требует многоуровневого ответа.

Во-первых, необходимо переосмыслить архитектуру защиты: переход к модели Zero Trust, использование ИИ для прогнозирования атак, внедрение блокчейна для аудита – всё это повышает устойчивость цифровой инфраструктуры [5].

Во-вторых, государство должно играть активную роль не только как регулятор, но и как инвестор и координатор. Программа «Цифровая экономика» – важный шаг, но требует расширения на региональный уровень, особенно в субъектах с развитым МСП-сектором, таких как Республика Дагестан [8].

В-третьих, человеческий фактор остаётся главной уязвимостью. Повышение киберграмотности населения и сотрудников – не опциональная, а обязательная мера. В этой связи важно развивать как общие образовательные программы, так и специализированные курсы для ИТ-специалистов [9].

В-четвёртых, международное сотрудничество, даже в условиях ограничений, должно продолжаться на уровне нейтральных организаций и технических сообществ. Обмен угрозами, совместные учения и стандартизация – ключ к глобальной устойчивости [11].

В заключение, можно утверждать, что кибербезопасность – это не расход, а инвестиция в будущее. Только при условии системного подхода, объединяющего технологии, регулирование, образование и страхование, цифровая экономика сможет обеспечить устойчивый рост, конкурентоспособность и социальную стабильность.

Список источников

1. Абян В.М., Зурнаджиди С., Логинова В.О., Савинская Д.Н. Защита экономических данных: кибербезопасность в условиях современных угроз // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2025. – № 208. – С. 121–135.
2. Александрова Е.Н. Актуальные вопросы развития кибербезопасности в современной России // Экономика: теория и практика. – 2024. – № 2 (74). – С. 21–28.
3. Аничкина О.А., Руднева Ю.С., Цуй Ц. Цифровизация и угрозы кибербезопасности в экономике // Инновационное развитие экономики. – 2024. – № 2 (80). – С. 35–43.
4. Артемьев Н.В., Руднев С.Г., Тычков А.С., Золкин А.Л. Экономическое значение кибербезопасности для предприятий в условиях цифровой трансформации // Экономика и управление: проблемы, решения. – 2024. – Т. 2, № 11 (152). – С. 46–55.
5. Васильев А.В. Инновационные тренды в области обеспечения кибербезопасности // Инновации и инвестиции. – 2023. – № 9. – С. 191–195.
6. Верников В.А., Еремеев А.Н. Фактор устойчивого развития экономики России - инвестиции в кибербезопасность // Экономика и социум: современные модели развития. – 2024. – Т. 14, № 4. – С. 329–348.
7. Гоголева В.В., Мельник С.В. Проблемы кибербезопасности цифрового мира // Вестник связи. – 2022. – № 2. – С. 38–44.
8. Джамалова М.Р., Качаева Г.И., Абдулхаликов М.А. Развитие системы обеспечения кибербезопасности в рамках стратегии защиты от угроз безопасности // Региональные проблемы преобразования экономики. – 2024. – № 8 (166). – С. 316–323.
9. Исламгереева Я.С., Эдисултанова З.Р. Кибербезопасность в эпоху цифровой экономики: вызовы, угрозы и стратегии защиты // Научный бюллетень Чеченского государственного университета им. А.А. Кадырова. – 2025. – № 2 (6). – С. 21–26.

10. Корнеев М.Н., Черпаков И.В. Кибербезопасность и ее значение для защиты экономики от цифровых угроз // Вестник Тульского филиала Финуниверситета. – 2023. – № 1. – С. 342–343.

11. Криштаносов В.Б. Кибербезопасность. Опыт Республики Беларусь // Мир перемен. – 2022. – № 3. – С. 126–144.

12. Куценко С.М. Кибербезопасность в цифровой экономике // Экономика и предпринимательство. – 2025. – № 1 (174). – С. 130–132.

13. Пахомова А.И., Сайкинов В.Е., Ахмадуллин Ф.Р., Золкин А.Л. Влияние кибербезопасности на развитие цифровой экономики // Экономика и управление: проблемы, решения. – 2025. – Т. 2, № 6 (159). – С. 222–230.

14. Тасуева Х.З.А., Рахимова Г.С., Борисов А.Н. Роль кибербезопасности в обеспечении устойчивости экономических систем в условиях цифровизации // Экономика и управление: проблемы, решения. – 2024. – Т. 6, № 1 (142). – С. 4–9.

15. Чжао Л. Кибербезопасность как элемент национальной экономической стратегии в цифровую эпоху // Экономическое развитие России. – 2025. – Т. 32, № 6. – С. 241–246.

Сведения об авторах

Сулейманова Динара Абдулбасировна, к.э.н., доцент кафедры экономической безопасности, анализа и аудита, Дагестанский государственный университет,

Алиев Магомед Абдулхалимович, к.э.н., доцент кафедры мировой и региональной экономики**,** Дагестанский государственный университет

Магомедова Мадина Абдусаламовна, старший преподаватель кафедры бизнес-информатики и высшей математики, Дагестанский государственный университет

Information about the authors

Suleymanova Dinara Abdulbasirovna, PhD in Economics, Associate Professor of the Department of Economic Security, Analysis and Audit, Dagestan State University

Aliev Magomed Abdulkhalimovich, Ph. D., Associate Professor of the Department of World and Regional Economics**,** Dagestan State University

Magomedova Madina Abdusalamovna, Senior Lecturer of the Department of Business Informatics and Higher Mathematics, Dagestan State University.