

Качаева Гюльханум Ибадулаховна

Дагестанский государственный технический университет

Султанов Нариман Гарунович

Дагестанский государственный технический университет

Чилаев Алаудин Шадитович

Чеченский государственный университет им. А. А. Кадырова

Интеграция искусственного интеллекта и кибербезопасности в системе обеспечения национальной экономической безопасности

Аннотация. В условиях усиления внешнего санкционного давления и необходимости достижения технологического суверенитета Российской Федерации особую актуальность приобретает исследование механизмов обеспечения национальной экономической безопасности в цифровой среде. Цель настоящего исследования состоит в систематизации теоретических подходов и разработке практических рекомендаций по интеграции искусственного интеллекта и средств кибербезопасности в систему обеспечения экономической безопасности государства. В работе использованы методы системного анализа, сравнительно-правового анализа, а также методы экономико-статистического моделирования. В результате исследования выявлены ключевые угрозы экономической безопасности, связанные с цифровизацией экономики, определены направления использования искусственного интеллекта как стратегического ресурса обеспечения безопасности, разработана концептуальная модель интеграции систем ИИ и кибербезопасности. Научная новизна исследования заключается в обосновании взаимосвязи между уровнем технологического суверенитета, развитием искусственного интеллекта и состоянием кибербезопасности как системообразующих факторов экономической безопасности. Практическая значимость результатов состоит в возможности их использования при разработке стратегических документов в области цифровой экономики и национальной безопасности.

Ключевые слова: цифровая экономика, технологический суверенитет, искусственный интеллект, кибербезопасность, экономическая безопасность, цифровая трансформация, национальная безопасность, стратегическое управление.

Kachaeva Gulhanum Ibadulakhovna

Dagestan State Technical University

Sultanov Nariman Harunovich

Dagestan State Technical University

Chilaev Alaudin Shaditovich

Kadyrov Chechen State University

Digital economy and technological sovereignty: integration of artificial intelligence and cybersecurity in the national economic security system

Abstract. In the context of increasing external sanctions pressure and the need to achieve technological sovereignty of the Russian Federation, the study of mechanisms for ensuring national economic security in the digital environment becomes particularly relevant. The purpose of this study is to systematize theoretical approaches and develop practical recommendations for the integration of artificial intelligence and cybersecurity tools into the economic security system. The research employs methods of system analysis, comparative legal analysis, as well as economic and statistical modeling. The study identifies key threats to economic security associated with digitalization, determines the directions for using artificial intelligence as a strategic security resource, and develops a conceptual model for integrating AI and cybersecurity systems. The scientific novelty lies in substantiating the relationship between the level of technological sovereignty, the development of artificial intelligence,

and the state of cybersecurity as system-forming factors of economic security. The practical significance of the results lies in their applicability for developing strategic documents in the field of digital economy and national security.

Keywords: digital economy, technological sovereignty, artificial intelligence, cybersecurity, economic security, digital transformation, national security, strategic management.

Введение

В последние годы цифровизация экономики и общества приобрела определяющее значение для достижения целей устойчивого развития национальной экономики. Параллельно с расширением цифровой инфраструктуры усилились и риски, связанные с киберугрозами: увеличилось число атак на информационные системы государственных и корпоративных объектов, участились случаи утечек конфиденциальных данных, возросла сложность и целенаправленность атак на цепочки поставок. Эти тенденции особенно явно проявились в 2024-2025 гг., когда специализированные аналитические центры зафиксировали значительный рост количества инцидентов, усиление коммерческой мотивации злоумышленников и широкое применение современных технологий, в том числе средств искусственного интеллекта (ИИ), для подготовки и реализации атак.

Для России совокупность перечисленных факторов представляет особую угрозу экономической безопасности и цифровому суверенитету. Критическая информационная инфраструктура, промышленный сектор, государственные учреждения и финансовые организации становятся основными мишенями кибератак, что наносит прямой экономический ущерб и подрывает доверие к цифровым институтам.

В 2024 г. объем российского ИТ-рынка превысил 3,1 трлн руб., показав рост почти на 19%. Однако одновременно с этим Россия опустилась в глобальном рейтинге кибербезопасности Международного союза электросвязи с пятой позиции в 2020 г. до 58-й в 2024 г..

Степень разработанности проблемы в отечественной науке характеризуется наличием отдельных исследований по вопросам кибербезопасности (Аветисян А.И. [1], Гоголева В.В., Мельник С.В. [4]), влияния искусственного интеллекта на экономическую безопасность (Татаринев К.А. [7], Дударев К.С. [5] и др.), а также проблем цифрового суверенитета (Алексеев Г.В. [2], Володенков С.В., Федорченко С.Н. [3]).

Однако комплексные исследования, объединяющие указанные направления в единую концепцию обеспечения национальной экономической безопасности, представлены недостаточно.

Научная проблема исследования заключается в противоречии между возрастающей зависимостью национальной экономики от цифровых технологий и недостаточной разработанностью механизмов интеграции искусственного интеллекта и кибербезопасности в систему обеспечения экономической безопасности в условиях формирования технологического суверенитета.

Цель исследования состоит в систематизации теоретических подходов и разработке практических рекомендаций по интеграции искусственного интеллекта и средств кибербезопасности в систему обеспечения экономической безопасности государства.

Теоретической основой исследования послужили работы отечественных и зарубежных ученых в области цифровой экономики, экономической безопасности, информационной безопасности и искусственного интеллекта. Методологическая база включает системный подход, позволяющий рассматривать экономическую безопасность как сложную многоуровневую систему; методы сравнительно-правового анализа для изучения нормативно-правовой базы в сфере цифровизации и кибербезопасности; а также методы экономико-статистического анализа для оценки масштабов киберугроз и экономического ущерба.

В работе использованы данные аналитических отчетов ведущих российских компаний в области кибербезопасности (RED Security SOC, Bi.Zone, Positive Technologies, Solar 4RAYS), статистические материалы Сбербанка, а также программные документы в сфере цифровой экономики и технологического суверенитета.

Основная часть

1. Теоретические аспекты взаимосвязи цифровой экономики, технологического

суверенитета и экономической безопасности

Технологический суверенитет в современной научной литературе описывается не как отраслевой проект, а как новая модель развития национальной экономики. Отправной точкой формирования технологического суверенитета стала политика импортозамещения. Так, с 2014 г. уровень локализации в нефтегазовом машиностроении вырос с 43 до 70%, а доля российских препаратов в аптечных продажах достигла 65%. Рынок беспилотных систем за 2024 г. увеличился в 2,7 раза, а число производителей выросло с 220 до более чем 600. Однако ключевая цель на современном этапе – перейти от количественных показателей замещения импорта к качественному скачку в создании собственных технологий.

В 2024 г. в России завершился национальный проект «Цифровая экономика». Уже в феврале 2025 г. заместитель председателя правительства РФ Дмитрий Григоренко презентовал новый нацпроект – «Экономика данных и цифровая трансформация государства», который будет реализован до конца 2030 г.

Следующий уровень технологического суверенитета – создание собственной цифровой инфраструктуры. Система быстрых платежей, которую авторы доклада АНО «Национальные приоритеты» называют мировым феноменом, обработала за 2024 г. 13,4 млрд операций на 69,5 трлн руб., а портал «Госуслуги» ежедневно обслуживает более 10 млн пользователей.

При этом авторы доклада указывают на сохранение системных проблем: зависимость от передовых чипов, фрагментация данных между ведомствами и компаниями, а также дефицит специалистов, способных одновременно работать с кодом и понимать отраслевую специфику. На следующее десятилетие фокус смещается с обеспечения внутреннего суверенитета на активную внешнюю экспансию. Россия стремится стать не только создателем собственных решений, но и источником международных стандартов в области цифровой этики, безопасности данных и интеграции платформ.

Экономический суверенитет государства в современных условиях напрямую связан со скоростью цифровизации национальной экономики, а также механизмами сглаживания цифрового неравенства регионов России. Технологический суверенитет приобретает приоритетное значение перед политикой импортозамещения, поскольку предполагает не просто замещение иностранных продуктов, а создание собственных технологических решений мирового уровня.

2. Роль искусственного интеллекта как стратегического ресурса обеспечения экономической безопасности

Искусственный интеллект в современных условиях рассматривается как стратегический ресурс экономической безопасности России. Как отмечают эксперты, разработка отечественных моделей ИИ и их внедрение, а также использование отечественных датасетов сегодня становятся вопросом национальной безопасности, так как зарубежные страны могут экспортировать искусственный интеллект, который будет им подконтролен.

Влияние ИИ на экономическую безопасность носит двойственный характер. С одной стороны, технологии ИИ открывают новые возможности для повышения конкурентоспособности национальной экономики, оптимизации производственных процессов и усиления комплаенс-контроля. С другой стороны, развитие ИИ создает новые угрозы, включая вопросы «профайлинга» и технологической безработицы. Особую озабоченность вызывает использование генеративных нейросетей для создания дипфейков, позволяющих обходить биометрическую защиту [13].

Минэкономразвития России подчёркивает, что безопасность и доверие к искусственному интеллекту являются ключевыми аспектами массового внедрения технологии. В России принят Кодекс этики в сфере искусственного интеллекта, который закладывает базовые стандарты и правила разработки и применения ИИ в нашей стране.

3. Кибербезопасность как системообразующий элемент защиты национальных экономических интересов в цифровой среде

Современное состояние кибербезопасности в России характеризуется беспрецедентным ростом угроз. По данным Сбербанка, в России каждые три минуты происходит кибератака на какую-либо компанию.

По итогам восьми месяцев 2025 года каждая вторая российская компания подверглась

кибератакам, а общий ущерб для экономики оценивается примерно в 1,5 трлн рублей. Количество атак на бизнес и госструктуры утроилось по сравнению с предыдущим периодом.

В 2025 году лидером по кибератакам стал госсектор. Причиной этого стало то, что финансовый сектор научился себя защищать и применять надежные технологии кибербезопасности [8]. Наблюдается смещение фокуса хакеров с финансового сектора на государственные структуры как на федеральном, так и на региональном уровне.

Ключевыми факторами риска выступают: кибератаки на критическую информационную инфраструктуру, утечки конфиденциальных данных, зависимость от иностранных технологий, экономический и промышленный шпионаж, а также угрозы цифровому суверенитету.

Особую тревогу вызывает резкое падение России в глобальном рейтинге кибербезопасности Международного союза электросвязи — с пятой позиции в 2020 году до 58-й в 2024.

Обобщённая характеристика основных угроз и вызовов приведена в таблице 1.

Таблица 1 – Ключевые угрозы и вызовы кибербезопасности в контексте обеспечения национальной экономической безопасности Российской Федерации

Вид угрозы / вызова	Характеристика	Влияние на экономическую безопасность	Основные меры противодействия
1. Кибератаки на критическую информационную инфраструктуру (КИИ)	Целенаправленные атаки на объекты энергетики, транспорта, связи, финансового сектора и оборонной промышленности. Рост числа атак: каждая вторая российская компания подверглась атакам в 2025 г.	Прямые финансовые потери (оцениваются в 1,5 трлн руб. за 2025 г.), сбои в работе стратегических предприятий, подрыв доверия к цифровым сервисам.	Внедрение отечественных СЗИ (средств защиты информации), использование ИИ для прогнозирования и обнаружения атак, переход на доверенные аппаратные платформы.
2. Утечки конфиденциальных данных и персональной информации	Участившиеся случаи компрометации баз данных государственных органов, банковской системы и коммерческих структур. Усиление коммерческой мотивации злоумышленников.	Репутационные и финансовые потери, снижение инвестиционной привлекательности, нарушение прав граждан, риск использования данных для промышленного шпионажа.	Применение технологий шифрования, поведенческий анализ пользователей, внедрение систем DLP (Data Loss Prevention) на основе ИИ.
3. Зависимость от иностранных технологий и ПО	Сохранение доли зарубежных решений в ключевых сегментах ИТ-инфраструктуры (СУБД, операционные системы, облачные платформы).	Уязвимость перед санкционными ограничениями, отключением от обновлений и техподдержки, риск внедрения «закладок» и недекларированных возможностей.	Импортозамещение и развитие реестра отечественного ПО, создание собственных облачных платформ, стимулирование перехода на российские продукты.
4. Экономический и промышленный шпионаж	Использование ИИ для проведения таргетированных атак, направленных на хищение интеллектуальной	Потеря конкурентных преимуществ, утрата технологического суверенитета, ослабление позиций на	Усиление защиты корпоративных сетей, обучение персонала, внедрение систем поведенческого анализа

Вид угрозы / вызова	Характеристика	Влияние на экономическую безопасность	Основные меры противодействия
	собственности, промышленных секретов и коммерческой информации.	международных рынках.	и классов защиты информации.
5. Использование ИИ злоумышленниками	Генеративные нейросети применяются для создания дипфейков, фишинговых писем, подбора паролей и обхода биометрической защиты.	Повышение сложности атак, снижение эффективности традиционных методов защиты, увеличение числа успешных инцидентов.	Разработка контр-ИИ-систем, создание методик идентификации дипфейков, совершенствование биометрической защиты с использованием собственных датасетов.
6. Падение России в международных рейтингах кибербезопасности	Снижение позиции в рейтинге Международного союза электросвязи с 5-го места (2020 г.) до 58-го (2024 г.).	Снижение международного авторитета, ухудшение условий для международного сотрудничества, отток инвестиций.	Разработка и реализация национальной программы повышения киберустойчивости, активизация международного продвижения российских решений.

Источник: составлено автором на основе анализа данных RED Security SOC, Bi.Zone, Positive Technologies, а также статистических материалов Сбербанка и отчёта Международного союза электросвязи.

Анализа представленных в таблице 1 данных позволил сделать вывод о том, что спектр угроз экономической безопасности в цифровой среде многогранен и охватывает не только прямые финансовые потери от кибератак, но и стратегические риски потери технологического суверенитета, утраты конкурентоспособности и ослабления позиций России на международной арене. Особую опасность представляет зависимость от иностранных технологий, поскольку она создаёт «порочный круг»: использование зарубежного ПО увеличивает уязвимость перед санкциями и одновременно замедляет развитие собственной технологической базы. Кроме того традиционных подходов к кибербезопасности становится недостаточно. Рост числа атак, их усложнение и активное использование злоумышленниками искусственного интеллекта требуют перехода от реактивной модели защиты к проактивной, основанной на прогнозировании угроз и автоматизированном реагировании. Это подтверждается данными о том, что финансовый сектор, активно внедряющий ИИ-решения, сумел снизить уязвимость, что привело к смещению фокуса атак на менее защищённые государственные структуры.

В этой связи комплексный характер угроз требует системных решений на уровне государства, включающих не только технологические меры, но и институциональные преобразования. Ключевым элементом такой системы должно стать создание единого уполномоченного органа по киберустойчивости, объединяющего усилия всех заинтересованных сторон – государства, бизнеса и науки. Только в этом случае возможно преодоление отставания в глобальных рейтингах и обеспечение надёжной защиты национальных экономических интересов в условиях цифровой трансформации.

Осенью 2025 года российский сектор кибербезопасности работает в условиях двойного давления: с одной стороны, продолжает набирать обороты эволюция угроз, использующих ИИ, с другой – происходит ужесточение регуляторных требований. Ключевым драйвером изменений стало Положение Банка России № 851-П, вступившее в силу весной 2025 года, устанавливающее более строгие стандарты защиты информации, особенно для финансового сектора. С 1 октября 2025 года кредитные организации обязаны регистрировать расширенный набор технических данных о действиях клиентов.

В ответ на нормативное давление и растущую изощренность атак российские банки и крупные компании массово внедряют системы на основе искусственного интеллекта [14]. Поведенческие антифрод-системы нового поколения анализируют в реальном времени тысячи параметров – от паттернов использования мыши и клавиатуры до типичного времени и маршрутов транзакций. Модули ИИ внедряются непосредственно в EDR-агенты, обеспечивая их автономность.

Однако, как отмечает заместитель председателя правления Сбербанка Станислав Кузнецов, традиционного понимания кибербезопасности уже недостаточно, требуется переход к концепции киберустойчивости – способности не только противостоять угрозам, но и оперативно восстанавливаться после атак [11]. Киберустойчивость является фундаментальным элементом цифрового суверенитета страны и бизнеса.

В связи с этим Сбербанк предложил масштабную инициативу – создание национальной программы повышения киберустойчивости «ОСНОВА». Аббревиатура расшифровывается как шесть ключевых элементов: Ответственный орган на уровне государства, Стратегия, Нормативно-правовая база, Отечественная технологическая база, Восстановление и Адаптивность. Ключевым звеном программы должно стать назначение единого уполномоченного государственного органа, который возьмет на себя стратегическое руководство и координацию всех усилий в этой сфере.

4. Концептуальная модель интеграции искусственного интеллекта и кибербезопасности в систему обеспечения национальной экономической безопасности

На основе проведенного анализа предлагается концептуальная модель интеграции искусственного интеллекта и кибербезопасности в систему обеспечения национальной экономической безопасности, включающая следующие взаимосвязанные элементы:

Технологический, который предполагает создание и развитие отечественных ИИ-решений для задач кибербезопасности, включая системы обнаружения и предотвращения атак, поведенческий анализ, прогнозирование угроз на основе больших данных. Как отмечается в исследовании, применение ИИ в кибербезопасности в России требует обобщения разрозненного опыта и определения ключевых преимуществ и трудностей этого процесса.

Институциональный, включающий формирование единого уполномоченного органа по киберустойчивости, развитие национальных стандартов и нормативно-правовой базы, а также механизмов государственно-частного партнерства в сфере ИИ и кибербезопасности.

Кадровый, предполагающий подготовку квалифицированных специалистов, способных работать с ИИ-системами и обеспечивать их безопасность. Как подчеркивается в экспертных публикациях, ИИ не заменяет специалистов по кибербезопасности, но кардинально меняет их роль. Вместо рутинного мониторинга в приоритете становится управление сложными системами и их аудит. Существующие кадровые позиции, такие как инженеры машинного обучения и MLOps, теперь включают в зону ответственности обеспечение безопасности AI-моделей и управление данными для их обучения.

Инфраструктурный, включающий развитие центров обработки данных для задач ИИ с обеспечением суверенитета данных, создание отечественных облачных платформ и программно-аппаратных комплексов, а также импортозамещение в сфере критической информационной инфраструктуры.

Международный, означающий активную внешнюю экспансию российских решений в области ИИ и кибербезопасности, продвижение концепции цифрового суверенитета среди стран-партнеров.

5. Практические рекомендации по укреплению технологического суверенитета России через развитие ИИ и кибербезопасности

На основе проведенного исследования сформулирован комплекс практических рекомендаций, направленных на укрепление технологического суверенитета России через развитие искусственного интеллекта и кибербезопасности.

В первую очередь, приоритетное внимание должно быть уделено развитию отечественных ИИ-решений. Необходимо ускорить разработку и внедрение российских моделей искусственного интеллекта, включая генеративные модели и большие языковые модели (LLM), с обязательным использованием отечественных датасетов. Это напрямую связано с обеспечением национальной

безопасности, поскольку зависимость от зарубежных платформ в данной сфере создаёт критическую уязвимость. Требуется активное развитие облачных ИИ-решений, размещаемых на отечественной инфраструктуре, что позволит гарантировать суверенитет данных и сохранность информации пользователей в контуре России [9].

В институциональной плоскости ключевой рекомендацией является создание национальной программы киберустойчивости. Предлагается реализовать инициативу «ОСНОВА», которая предусматривает назначение единого уполномоченного государственного органа по кибербезопасности, разработку комплексной стратегии, формирование нормативно-правовой базы и создание отечественной технологической базы. Такой подход позволит консолидировать усилия всех участников и обеспечить системное решение проблем кибербезопасности на государственном уровне.

Не менее важным направлением является усиление импортозамещения в сфере критической информационной инфраструктуры (КИИ). Необходимо ускорить переход на отечественное программное обеспечение и аппаратные платформы на объектах КИИ, которые являются основой функционирования экономики и государства. Особое внимание следует уделить средствам криптографической защиты информации, имеющим подтверждение соответствия от ФСБ России, поскольку именно они обеспечивают доверенную среду для обработки и передачи критических данных.

Кадровое обеспечение цифровой безопасности требует пересмотра образовательных программ в области информационной безопасности с включением модулей по машинному обучению, анализу больших данных и правовым аспектам регулирования искусственного интеллекта [12]. Сотрудникам, занятым в сфере кибербезопасности, необходимо осваивать основы машинного обучения, методы анализа больших данных и юридические тонкости новых редакций нормативных актов. Только такой междисциплинарный подход позволит подготовить специалистов, способных эффективно работать в условиях быстро меняющегося ландшафта угроз.

Правовое обеспечение также требует совершенствования: необходимо дальнейшее развитие нормативно-правового регулирования в сфере искусственного интеллекта и кибербезопасности. Особого внимания заслуживают вопросы ответственности за применение ИИ, защиты персональных данных и биометрической информации. Требуется устранение существующих пробелов в законодательстве и создание чётких правил, которые одновременно стимулировали бы инновации и гарантировали безопасность граждан и государства.

Реализация всех перечисленных мер невозможна без развития государственно-частного партнёрства. Требуется объединение усилий государства, бизнеса и науки для повышения устойчивости цифровой среды. Государство должно создавать условия и инфраструктуру, бизнес – внедрять передовые практики, а наука – обеспечивать методологическую базу и генерировать новые знания [6]. Такая синергия позволит наиболее эффективно использовать имеющиеся ресурсы и компетенции.

Наконец, важным направлением является международное продвижение российских решений. Россия обладает полным спектром технологий в области кибербезопасности и искусственного интеллекта и может продвигать концепцию цифрового суверенитета на международном уровне для стран-партнёров. Российские разработки в области кибербезопасности признаются одними из наиболее эффективных в мире, что открывает значительный экспортный потенциал. Активное позиционирование отечественных решений на глобальных рынках не только укрепит технологический суверенитет самой России, но и позволит сформировать альянс стран, разделяющих принципы независимого цифрового развития [10].

Обсуждение результатов

Проведённое исследование позволяет сделать вывод о том, что обеспечение национальной экономической безопасности в условиях цифровой трансформации требует комплексного подхода, объединяющего технологический, институциональный, кадровый и инфраструктурный аспекты. Полученные результаты согласуются с выводами других исследователей, в частности, с положениями работ Аветисяна А.И. о роли кибербезопасности в контексте искусственного интеллекта, Татаринова К.А. о влиянии ИИ на кибербезопасность, а также Володенкова С.В. и Федорченко С.Н. о новых социально-политических вызовах государственному суверенитету в

цифровую эпоху.

Вместе с тем, исследование имеет определённые ограничения. Во-первых, динамика развития технологий ИИ и киберугроз требует постоянного обновления эмпирической базы. Во-вторых, вопросы правового регулирования ИИ и кибербезопасности находятся в стадии активного развития, что затрудняет формирование окончательных выводов о эффективности тех или иных механизмов. В-третьих, международный аспект проблемы требует отдельного углублённого исследования с учётом различий в национальных подходах к регулированию цифровой сферы.

Направления дальнейших исследований могут включать: разработку методик оценки эффективности интеграции ИИ и кибербезопасности; анализ международного опыта и его адаптацию к российским условиям; исследование влияния ИИ на трансформацию рынка труда в сфере информационной безопасности; а также разработку конкретных механизмов государственно-частного партнёрства в сфере цифровой безопасности.

Заключение

Проведённое исследование позволяет сформулировать следующие основные выводы.

Во-первых, цифровая экономика и технологический суверенитет являются взаимосвязанными категориями, определяющими современное состояние и перспективы развития национальной экономической безопасности. Переход от импортозамещения к созданию собственных технологий мирового уровня составляет сущность современного этапа формирования технологического суверенитета России.

Во-вторых, искусственный интеллект выступает как стратегический ресурс обеспечения экономической безопасности, обладающий как значительным потенциалом для повышения конкурентоспособности и защищённости национальной экономики, так и создающий новые угрозы, требующие адекватного правового и институционального регулирования.

В-третьих, современное состояние кибербезопасности в России характеризуется беспрецедентным ростом угроз: ущерб от кибератак в 2025 году достиг 1,5 трлн рублей, а Россия опустилась с 5-го на 58-е место в глобальном рейтинге кибербезопасности. Требуется переход от традиционной кибербезопасности к концепции киберустойчивости, предполагающей способность не только противостоять атакам, но и оперативно восстанавливаться.

В-четвёртых, интеграция искусственного интеллекта и кибербезопасности в систему обеспечения национальной экономической безопасности должна осуществляться на основе комплексной модели, включающей технологический, институциональный, кадровый, инфраструктурный и международный элементы.

Научная новизна исследования заключается в обосновании взаимосвязи между уровнем технологического суверенитета, развитием искусственного интеллекта и состоянием кибербезопасности как системообразующих факторов экономической безопасности, а также в разработке концептуальной модели их интеграции.

Практическая значимость результатов состоит в возможности их использования при разработке стратегических документов в области цифровой экономики и национальной безопасности, в том числе при реализации национального проекта «Экономика данных и цифровая трансформация государства» до 2030 г., а также при формировании национальной программы повышения киберустойчивости.

Дальнейшие исследования в данной области должны быть направлены на разработку конкретных методик и механизмов реализации предложенной модели, а также на анализ эффективности интеграционных процессов в сфере ИИ и кибербезопасности в контексте обеспечения национальной экономической безопасности.

Список источников

1. Аветисян А.И. Кибербезопасность в контексте искусственного интеллекта // Вестник Российской академии наук. – 2022. – Т. 92. – № 12. – С. 1119–1123.
2. Алексеев Г.В. Цифровой суверенитет и защита прав человека в международном киберпространстве // Евразийский юридический журнал. – 2024. – № 6 (193). – С. 483–486.
3. Володенков С.В., Федорченко С.Н. Новые социально-политические вызовы государственному суверенитету в цифровую эпоху (по материалам международного экспертного

исследования) // Вестник Московского университета. Серия 12: Политические науки. – 2023. – Т. 1. – № 6. – С. 31–57.

4. Гоголева В.В., Мельник С.В. Проблемы кибербезопасности цифрового мира // Вестник связи. – 2022. – № 2. – С. 38–44.

5. Дударев К.С., Ерофеев О.Н., Иванов Н.А., Вертешев А.С. Искусственный интеллект в сфере кибербезопасности // Международный журнал прикладных наук и технологий Integral. – 2024. – № 1.

6. Колесова Д.А., Богушева К.О., Поначугин А.В. Передовые технологии: искусственный интеллект как щит и меч в кибербезопасности // Перспективы науки. – 2024. – № 12 (183). – С. 25–27.

7. Татаринов К.А. Влияние искусственного интеллекта на кибербезопасность // Вопросы российского и международного права. – 2025. – Т. 15. – № 5-1. – С. 197–205.

8. Хаджиева Л.К., Чадаев А.К. Кибербезопасность и искусственный интеллект: использование искусственного интеллекта для обнаружения и предотвращения кибератак // Экономика и управление: проблемы, решения. – 2025. – Т. 2. – № 12 (165). – С. 97–103.

9. Цифровой суверенитет и экономическая безопасность России в условиях современного роста киберугроз // naukaru.ru. – 2025. – С. 121–136. – URL: <https://naukaru.ru/ru/nauka/article/105251/view> (дата обращения: 06.06.2026).

10. Технологический суверенитет России: как ИТ, АПК, кадры и креатив формируют новую экономику // Эксперт. – 2025. – URL: <https://expert.ru/promishlennost/ano-natsionalnye-prioritety-otsenili-tekhnologicheskii-suverenitet> (дата обращения: 04.06.2026).

11. Сбер: ущерб от кибератак в России в 2025 году составил полтора триллиона рублей // NBJ. – 2025. – 5 сент. – URL: <https://nbj.ru/news/sber-ushcherb-ot-kiberatak-v-rossii-v-20/70290/> (дата обращения: 09.06.2026).

12. Защитная линия. В России появится программа национальной киберустойчивости // Аргументы и факты. – 2025. – URL: <https://aif.ru/society/safety/zashchitnaya-liniya-v-rossii-poyavitsya-programma-nacionalnoy-kiberustoychivosti> (дата обращения: 06.06.2026).

13. ИИ и нейросети. Как они меняют ландшафт кибербезопасности в России // PLUSworld. – 2025. – 24 нояб. – URL: <https://plusworld.ru/articles/68801/> (дата обращения: 08.06.2026).

14. Российские ИТ-компании меняют бизнес-модели // RUSSOFT. – 2025. – 21 июля. – URL: <https://russoft.org/> (дата обращения: 06.07.2026).

Сведения об авторах

Качаева Гюльханум Ибадулаховна, к.э.н., заведующая кафедрой информационной безопасности, Дагестанский государственный технический университет

Султанов Нариман Гарунович, студент специальности «Информационная безопасность», Дагестанский государственный технический университет

Чилаев Алаудин Шадитович, к.э.н., доцент кафедры «Экономическая теория и предпринимательство», Чеченский государственный университет им. А. А. Кадырова

Information about the authors

Kachaeva Gulhanum Ibadulakhovna, Ph.D. in Economics, Head of the Department of Information Security, Dagestan State Technical University

Sultanov Nariman Garunovich, student of the specialty «Information Security», Dagestan State Technical University

Chilaev Alaudin Shaditovich, PhD in Economics, Associate Professor of the Department of Economic Theory and Entrepreneurship, Kadyrov Chechen State University.