УДК 004-049.5:004.56(575.2)
DOI: 10.36979/1694-500X-2025-25-4-28-37

КОМПЛЕКСНЫЙ ПОДХОД К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КЫРГЫЗСТАНЕ: АНАЛИЗ, ВЫЗОВЫ И ПУТИ УКРЕПЛЕНИЯ

Ж.Б. Мамадалиева, А.Д. Баранов, А.З. Рахманов

Аннотация. Приведены результаты анализа текущего состояния информационной безопасности страны, рассмотрены основные вызовы, с которыми сталкивается государство в условиях глобальных киберугроз. Предложен комплексный подход для укрепления защиты критически важных информационных инфраструктур. Исследованы современные угрозы, включая кибератаки на государственные структуры, утечки данных, атаки на критическую инфраструктуру и низкий уровень киберграмотности населения. Рассматриваются меры, предпринимаемые Кыргызстаном для защиты информационного пространства, такие как законодательные инициативы, образовательные программы, сотрудничество с международными организациями и внедрение передовых технологий, включая искусственный интеллект, блокчейн и квантовое шифрование. Предложены рекомендации для усиления национальной системы информационной безопасности, акцентируя внимание на необходимости расширения правовой базы, подготовки кадров и развития системы мониторинга и быстрого реагирования на киберинциденты.

Ключевые слова: информационная безопасность; киберугрозы; критическая инфраструктура; киберграмотность; законодательные инициативы; международное сотрудничество; цифровая трансформация.

КЫРГЫЗСТАНДАГЫ МААЛЫМАТТЫК КООПСУЗДУККА КОМПЛЕКСТҮҮ МАМИЛЕ: ТАЛДОО, КЫЙЫНЧЫЛЫКТАР ЖАНА БЕКЕМДӨӨ ЖОЛДОРУ

Ж.Б. Мамадалиева, А.Д. Баранов, А.З. Рахманов

Аннотация. Макалада өлкөнүн маалыматтык коопсуздугунун учурдагы абалына талдоо жүргүзүүнүн натыйжалары берилген жана глобалдык киберкоркунучтардын шартында мамлекет туш болгон негизги көйгөйлөр каралат. Критикалык маалыматтык инфраструктураларды коргоону күчөтүү үчүн комплекстүү мамиле сунушталууда. Заманбап коркунучтар, анын ичинде мамлекеттик органдарга кибер чабуулдар, маалыматтардын сыртка чыгышы, маанилүү инфраструктурага кол салуулар жана калктын кибер сабаттуулугунун төмөн деңгээли изилденген. Мыйзам чыгаруу демилгелери, билим берүү программалары, эл аралык уюмдар менен кызматташуу жана алдыңкы технологияларды, анын ичинде жасалма интеллект, блокчейн жана кванттык шифрлөөнү киргизүү сыяктуу маалымат мейкиндигин коргоо боюнча Кыргызстан тарабынан көрүлүп жаткан чаралар каралууда. Укуктук базаны кеңейтүү, кадрларды даярдоо жана кибер инциденттерге мониторинг жүргүзүү жана тез чара көрүү системасын өнүктүрүү зарылдыгына басым жасоо менен улуттук маалыматтык коопсуздук системасын чыңдоо боюнча сунуштар сунушталууда.

Түйүндүү сөздөр: маалыматтык коопсуздук; кибер коркунучтар; маанилүү инфраструктура; кибер сабаттуулук; мыйзам чыгаруу демилгелери; эл аралык кызматташтык; санариптик трансформация.

A COMPREHENSIVE APPROACH TO INFORMATION SECURITY IN KYRGYZSTAN: ANALYSIS, CHALLENGES, AND STRENGTHENING STRATEGIES

Zh.B. Mamadalieva, A.D. Baranov, A.Z. Rakhmanov

Abstract. This article focuses on analyzing the current state of the country's information security, examining the primary challenges the state faces in the context of global cyber threats, and proposing a comprehensive approach to strengthen the protection of critical information infrastructures. The study explores modern threats, including cyberattacks on government structures, data leaks, attacks on critical infrastructure, and the low level of cybersecurity

awareness among the population. It also examines measures taken by Kyrgyzstan to safeguard its information space, such as legislative initiatives, educational programs, collaboration with international organizations, and the integration of advanced technologies like artificial intelligence, blockchain, and quantum encryption. The conclusion presents recommendations for enhancing the national information security system, highlighting the need to expand the legal framework, build a skilled workforce, and develop systems for monitoring and rapid response to cyber incidents.

Keywords: information security; cyber threats; critical infrastructure; cybersecurity awareness; legislative initiatives; international cooperation; digital transformation.

Введение. В эпоху стремительного развития цифровых технологий информационная безопасность приобретает критически важное значение для национальной безопасности любого государства. По данным отчета Cybersecurity Ventures, кибератаки ежегодно наносят мировой экономике ущерб, оцениваемый в 8 трлн долл. США, и эта цифра продолжает расти [1]. Для Кыргызской Республики, активно интегрирующейся в глобальное цифровое пространство, вопросы защиты данных становятся особенно актуальными. Цифровая трансформация оказывает значительное влияние на все аспекты общественной жизни – от государственного управления до социальных коммуникаций. В Кыргызстане процессы цифровизации, такие как внедрение платформы «Тундук» и программ «Цифровая трансформация 2030», способствуют улучшению доступа к услугам и повышению эффективности управления [2, 3]. Однако они также создают уязвимости, которые могут быть использованы злоумышленниками для подрыва национальной стабильности. Глобализация информационного пространства приносит не только новые возможности, но и масштабные угрозы, включая кибератаки, утечку данных и атаки на критически важную инфраструктуру. Например, в 2023 году было зафиксировано более 1,5 млн киберинцидентов, связанных с нарушением конфиденциальности и работоспособности сетей [4]. Эти вызовы требуют от стран, включая Кыргызстан, разработки комплексного подхода к обеспечению информационной безопасности.

Целью данной статьи является анализ текущего состояния информационной безопасности в Кыргызской Республике, выявление ключевых проблем и предложений для их решения. Особое внимание уделяется вопросам правового регулирования, внедрению передовых технологий, международному сотрудничеству и повышению киберграмотности населения. Кыргызстану необходимо выработать стратегию, которая позволит не только эффективно противостоять существующим угрозам, но и обеспечить устойчивость к будущим вызовам. В статье предлагаются рекомендации по созданию системы, которая интегрирует законодательные, образовательные и технологические инициативы для защиты критически важных информационных инфраструктур.

1. Современные угрозы информационной безопасности. С ростом цифровизации ключевых секторов экономики Кыргызстан, как и другие государства, сталкивается с новыми и все более сложными вызовами в сфере информационной безопасности. Современные киберугрозы становятся глобальными, требуя комплексного подхода к защите данных и критически важных инфраструктур.

Кибератаки на государственные органы представляют собой одну из самых значительных угроз для национальной безопасности. Такие инциденты могут привести к утечке конфиденциальной информации, дестабилизации работы государственных служб и нарушению общественного порядка. Примером может служить атака на правительственные структуры Эстонии в 2007 г., которая нарушила работу множества онлайн-сервисов, включая банки, медиа и государственные учреждения [5]. Кыргызстан, активно внедряющий платформу межведомственного взаимодействия «Тундук», также уязвим перед подобными угрозами. В 2023 г. в Кыргызской Республике были зафиксированы попытки несанкционированного доступа к государственным информационным системам, что подчеркивает необходимость усиления мер защиты. В ответ на эти угрозы Президент Кыргызской Республики Садыр Жапаров открыл новое здание Координационного центра по обеспечению кибербезопасности ГКНБ, оснащённое современным технологическим оборудованием и программными комплексами. Центр координирует деятельность государственных органов и центров реагирования на компьютерные

инциденты, направленную на обеспечение кибербезопасности, выявление, предупреждение и пресечение компьютерных атак [6].

Утечки данных продолжают быть одной из ключевых проблем для государственных и частных организаций. Согласно отчету IBM, средняя стоимость утечки данных в 2023 г. составила 4,45 млн долл. США [7].

В Кыргызстане риски утечек возрастают из-за ограниченного применения современных технологий шифрования и слабого контроля доступа. Например, в 2022 году произошел инцидент, связанный с утечкой персональных данных через уязвимости в платформе электронного правительства. Это подчеркивает необходимость внедрения более строгих стандартов безопасности [8].

Критическая инфраструктура, включая энергетические системы, транспорт и финансовый сектор, становится основным объектом атак. Например, в декабре 2015 г. кибератака на украинскую энергосистему привела к масштабным отключениям электроэнергии, затронувшим около 230 тыс. человек [9]. Для Кыргызстана защита таких объектов, как ГЭС и телекоммуникационные сети, является приоритетной задачей. В 2023 г. Национальный комитет информационной безопасности зафиксировал попытки кибератак на телекоммуникационную инфраструктуру, что подчеркивает необходимость в постоянном мониторинге и защите данных.

Одной из самых значительных угроз остается низкий уровень осведомленности среди населения и сотрудников организаций о методах защиты данных. Согласно отчету компании Positive Technologies, 85 % фишинговых атак направлены на получение данных, включая 26 % с целью финансовой выгоды. Кроме того, в 2023 г. почти половина (43 %) всех успешных атак на организации были проведены с использованием социальной инженерии, из которых 79 % осуществлялись через электронную почту, СМС-сообщения, социальные сети и мессенджеры. Эти данные подчеркивают значимость человеческого фактора в успешности кибератак, особенно через методы социальной инженерии, такие как фишинг [10, 11].

В Кыргызстане проблема усугубляется отсутствием систематического подхода к обучению киберграмотности. Проведенное в 2022 г. исследование показало, что менее 20 % пользователей знают, как распознать фишинг-атаки [8]. Для решения этой проблемы необходимо внедрение образовательных программ, направленных на повышение осведомленности о киберугрозах.

Растущее число IoT-устройств и популяризация облачных технологий создают новые векторы атак. В 2023 г. действительно наблюдался значительный рост DDoS-атак, использующих уязвимости устройств Интернета вещей (IoT), включая камеры. Согласно отчету компании SISA, в первой половине 2023 г. количество DDoS-атак на IoT-устройства увеличилось на 300 %, что привело к глобальным финансовым потерям в размере 2,5 млрд долл. США. Около 90 % сложных DDoS-атак в 2023 г. были основаны на ботнетах, использующих IoT-устройства. Эти атаки затронули миллионы пользователей по всему миру, демонстрируя необходимость усиления мер безопасности для IoT-устройств [12]. В Кыргызстане внедрение IoT в системах транспорта и здравоохранения требует усиленного контроля безопасности. Использование IoT-устройств без должного уровня защиты увеличивает риск утечек данных и нарушения работы критических систем. Кроме того, облачные сервисы, применяемые в государственных учреждениях, нуждаются в дополнительном шифровании и мониторинге для предотвращения несанкционированного доступа.

2. Текущие меры и инициативы по обеспечению информационной безопасности Кыргызстана. В ответ на возрастающие угрозы в киберпространстве Кыргызская Республика предпринимает активные шаги для обеспечения безопасности данных и защиты критически важных информационных инфраструктур. Эти меры включают законодательные инициативы, внедрение национальных программ, развитие информационно-коммуникационной инфраструктуры, сотрудничество с международными организациями и образовательные инициативы.

За последние годы Кыргызстан принял ряд законодательных актов, направленных на регулирование вопросов информационной безопасности. Одним из ключевых является закон «О защите

персональных данных», который обеспечивает защиту конфиденциальной информации граждан и организаций [2, 3]. Кроме того, в 2023 г. правительство утвердило национальную стратегию кибербезопасности, которая включает положения о создании национального центра реагирования на киберинциденты (CERT) [8]. Этот центр координирует усилия по мониторингу, анализу и предотвращению киберугроз. Однако реализация этих инициатив требует дополнительных ресурсов, включая финансирование и повышение кадровой квалификации.

Одной из важнейших программ является «Цифровая трансформация 2030», которая направлена на развитие электронной инфраструктуры и создание безопасной цифровой среды. Платформа «Тундук», служащая для межведомственного взаимодействия, позволяет упрощать процессы обмена данными между государственными структурами и улучшает доступ к услугам для граждан [3].

Другим важным проектом стал «Цифровой парламент», который внедряет технологии электронной демократии и обеспечивает прозрачность законодательных процессов. Эти инициативы создают прочную основу для цифровизации, однако требуют усиленного внимания к вопросам защиты данных, учитывая растущие угрозы.

Кыргызстан активно развивает свою информационно-коммуникационную инфраструктуру для противодействия кибератакам. В 2022 г. были модернизированы основные телекоммуникационные узлы, а также введены новые стандарты безопасности для государственных сетей.

Однако анализ показал, что многие учреждения все еще используют устаревшее программное обеспечение, которое уязвимо к современным атакам. Для повышения устойчивости необходимо ускорить процесс перехода на защищенные операционные системы и внедрение автоматизированных систем мониторинга [8].

Кыргызская Республика активно сотрудничает с международными организациями, включая ООН, ОБСЕ и Международный союз электросвязи (ITU). Эти партнерства позволяют обмениваться опытом и внедрять передовые стандарты информационной безопасности.

Например, в рамках сотрудничества с ОБСЕ в 2023 г. были проведены тренинги для государственных служащих, посвященные реагированию на киберинциденты. Кроме того, участие Кыргызстана в Глобальном форуме по кибербезопасности дало возможность адаптировать международные методики анализа и предотвращения угроз [8, 13, 14].

Развитие человеческого капитала является одним из важнейших направлений обеспечения информационной безопасности. В последние годы Кыргызская Республика активно внедряет специализированные учебные курсы в университетах и колледжах, направленные на подготовку специалистов в области информационных технологий и кибербезопасности. Например, Кыргызский государственный технический университет им. И. Раззакова предлагает программы, включающие изучение шифрования, анализа сетевых угроз и основ квантовой криптографии.

Дополнительно в 2023 г. была запущена инициатива по повышению киберграмотности государственных служащих. Курсы, разработанные совместно с международными партнерами, обучают базовым методам защиты данных и распознаванию кибератак. Эти программы способствуют не только повышению осведомленности, но и формированию базовых навыков для противодействия угрозам.

3. Применение современных технологий для укрепления кибербезопасности. Рост киберугроз требует от государств внедрения современных технологий, позволяющих повысить эффективность мониторинга, предотвращения и устранения инцидентов информационной безопасности. Кыргызская Республика, как часть глобального цифрового сообщества, нуждается в адаптации таких подходов для укрепления своей информационной инфраструктуры.

Искусственный интеллект (ИИ) становится ключевым инструментом в системах кибербезопасности благодаря способности анализировать большие объемы данных в реальном времени. Такие технологии используются для выявления аномалий в сетевом трафике, распознавания атак и предсказания потенциальных угроз.

Международные примеры включают использование ИИ в системе Cyber AI Analyst компании Darktrace, которая успешно нейтрализует угрозы в автоматическом режиме [15]. Кыргызстан мог бы применить аналогичные технологии для защиты государственных систем, включая платформу «Тундук», чтобы оперативно реагировать на попытки несанкционированного доступа.

Биометрические данные, такие как отпечатки пальцев, сканирование сетчатки глаза и распознавание лиц, обеспечивают высокий уровень безопасности аутентификации. Эти технологии минимизируют риски, связанные с использованием традиционных паролей, которые могут быть украдены или подделаны. Внедрение биометрической системы Aadhaar в Индии действительно способствовало снижению уровня мошенничества в государственных программах. Согласно данным, в период с 2018 по март 2021 г. было выявлено и удалено около 12,9 млн поддельных продовольственных карточек, что обеспечило более точное распределение ресурсов и уменьшило случаи мошенничества [16]. В Кыргызстане использование биометрических технологий могло бы повысить безопасность критически важных объектов, таких как государственные базы данных и платежные системы.

Блокчейн представляет собой распределенную систему хранения данных, которая предотвращает несанкционированное изменение информации. Эта технология может быть использована для защиты государственных реестров, хранения записей о транзакциях и мониторинга прозрачности процессов. Эстония успешно внедрила блокчейн-технологии для обеспечения безопасности данных в системах электронного голосования и медицинских реестрах. С 2005 г. страна использует электронное голосование, позволяя гражданам голосовать онлайн с использованием ID-карты или мобильной идентификации. В 2016 г. Эстония стала первой страной, применившей блокчейн на национальном уровне для защиты более 1 млн медицинских записей, обеспечивая их целостность и безопасность [17, 18]. Внедрение блокчейна в Кыргызстане могло бы обеспечить защиту данных платформы «Цифровой парламент» и других государственных информационных систем.

Квантовое шифрование – это одна из самых передовых технологий защиты данных, основанная на принципах квантовой механики. Эта технология обеспечивает гарантированную защиту от перехвата, так как любое вмешательство в процесс передачи данных немедленно обнаруживается.

Китай активно внедряет квантовое шифрование в свою национальную инфраструктуру, включая защищенные линии связи между правительственными учреждениями. В 2021 г. китайские исследователи объявили о создании первой в мире безопасной и стабильной сети связи при помощи квантовой криптографии, охватывающей более 4600 километров и обслуживающей свыше 150 организаций, включая государственные и частные банки, а также сайты электронного правительства [19].

Кроме того, в 2024 году Россия и Китай совместно создали защищенный спутниковый квантовый канал связи длиной 3800 км, что свидетельствует о стремлении Китая к развитию квантовой коммуникационной инфраструктуры. Кыргызстану следует рассмотреть пилотное внедрение квантового шифрования для защиты критических данных, особенно в области обороны и государственной безопасности [20].

С увеличением числа подключенных устройств Интернета вещей (IoT) возникает новая категория рисков. Уязвимости IoT-устройств могут быть использованы для атак на критическую инфраструктуру, включая системы умных городов, здравоохранения и транспорта.

Например, в 2023 г. DDoS-атака через IoT-камеры затронула миллионы пользователей по всему миру [12]. В Кыргызстане необходимо внедрять системы мониторинга IoT-устройств и автоматизированные средства обнаружения аномалий, чтобы минимизировать риски.

4. Анализ кадрового обеспечения и образовательных инициатив в области кибербезопасности. С развитием цифровой инфраструктуры и увеличением числа киберугроз Кыргызстан сталкивается с необходимостью подготовки высококвалифицированных специалистов в области кибербезопасности. Несмотря на усилия, предпринимаемые государственными органами и образовательными учреждениями, существует разрыв между спросом на специалистов и уровнем их подготовки. В этой

связи становится важным усиление образовательных инициатив и развитие кадрового потенциала для защиты критически важной инфраструктуры страны.

В последние годы в Кыргызстане наблюдается рост интереса к кибербезопасности в образовательных учреждениях. В университетах, таких как Кыргызский национальный университет имени Жусупа Баласагына и Кыргызский государственный технический университет им. И. Раззакова, начали внедрять курсы по информационной безопасности, охватывающие основные аспекты защиты данных, шифрования и защиты сетей. Однако эти программы остаются ограниченными и часто не охватывают новые угрозы, такие как защита Интернета вещей (IoT) и квантовое шифрование.

В международной практике существуют успешные образовательные программы, направленные на подготовку специалистов в области кибербезопасности. Например, в США действует Национальная инициатива по кибербезопасности (NICE), которая представляет собой партнёрство между правительством, академическими учреждениями и частным сектором, направленное на поддержку способности страны решать текущие и будущие задачи в области кибербезопасности через стандарты и лучшие практики [21].

Кроме того, Агентство по кибербезопасности и инфраструктурной безопасности (CISA) реализует программы, такие как Cybersecurity Education & Career Development, которые способствуют развитию кибербезопасности через образование и карьерное развитие [22].

Также существует Cybersecurity Coalition, миссия которой заключается в объединении ведущих компаний для разработки согласованных политических решений, направленных на продвижение динамичной и устойчивой экосистемы кибербезопасности. Эти инициативы способствуют подготовке квалифицированных специалистов, способных эффективно решать актуальные проблемы кибербезопасности [23].

В Кыргызстане аналогичные инициативы могли бы стать основой для создания более адаптированных образовательных программ, которые будут учитывать специфические потребности национальной безопасности.

Основной проблемой в подготовке специалистов по кибербезопасности является дефицит высококвалифицированных преподавателей, которые могут обучать современным методам защиты информации. Многие учебные заведения сталкиваются с нехваткой кадров, обладающих необходимыми навыками и опытом в области киберугроз. Кроме того, существует ограниченный доступ к современным лабораторным технологиям и программному обеспечению для практического обучения студентов.

Международный опыт показывает, что успешное преодоление этих проблем требует создания партнерств между университетами и частным сектором. Например, в Великобритании университеты активно сотрудничают с компаниями по безопасности, что позволяет студентам получать актуальные знания и практический опыт.

Помимо подготовки специалистов, важным направлением является повышение уровня киберграмотности среди государственных служащих и сотрудников частных организаций. В последние годы в Кыргызстане начала развиваться система тренингов и курсов для государственных служащих, направленных на повышение осведомленности о киберугрозах, таких как фишинг, социальная инженерия и защита персональных данных. Например, в 2023 г. был проведен ряд обучающих мероприятий совместно с международными организациями, такими как ОБСЕ, по основам кибербезопасности и защите информации. Эти инициативы помогают создавать осведомленность о рисках, связанных с интернет-безопасностью, и развивают базовые навыки кибергигиены среди широкой аудитории [13, 14].

Для повышения уровня подготовки кадров в области кибербезопасности в Кыргызстане необходимо:

- расширить образовательные программы и включить курсы, охватывающие современные угрозы, такие как машинное обучение в кибербезопасности, искусственный интеллект и квантовое шифрование;

- создать специализированные лаборатории, оснащенные современным оборудованием, для проведения практических занятий, что позволит студентам получать реальные навыки в защищенной среде;
- стимулировать партнерства с международными организациями и ведущими университетами, чтобы внедрять мировые стандарты в подготовку специалистов и предоставлять доступ к передовым образовательным ресурсам. Например, расширение сотрудничества с такими организациями, как Европейский центр по кибербезопасности, может помочь интегрировать лучшие практики и знания в систему образования Кыргызстана.

Для работающих специалистов в области кибербезопасности необходимо разработать программы повышения квалификации, которые позволят им оставаться в курсе последних тенденций и угроз. Программы могут включать обучение новым методам анализа угроз, изучение передовых технологий защиты и применение лучших мировых практик.

Внедрение программ повышения квалификации в сотрудничестве с международными компаниями и университетами поможет специалистам получать актуальные знания и навыки, необходимые для эффективной защиты информационных систем.

5. Международное сотрудничество и перспективы развития. В условиях глобализации киберугроз и растущей взаимозависимости цифровых инфраструктур международное сотрудничество становится ключевым элементом обеспечения национальной информационной безопасности. Кыргызская Республика активно участвует в глобальных инициативах, направленных на укрепление киберзащиты, что способствует обмену опытом, внедрению передовых стандартов и повышению квалификации специалистов.

Кыргызстан активно сотрудничает с международными организациями, такими как Организация Объединенных Наций (ООН), Организация по безопасности и сотрудничеству в Европе (ОБСЕ), а также Международный союз электросвязи (ITU). Эти организации предоставляют стране доступ к лучшим мировым практикам и методологиям киберзащиты.

Например, в 2023 году ОБСЕ организовала тренинги для государственных служащих Кыргызстана по реагированию на киберинциденты и защите критической инфраструктуры [13]. Также в рамках программы ITU по развитию киберустойчивости страна получила техническую помощь для модернизации телекоммуникационной инфраструктуры.

Участие Кыргызстана в международных форумах, таких как Глобальный форум по кибербезопасности и Европейский центр по кибербезопасности, позволяет стране перенимать опыт развитых стран. Например, Европейская модель защиты персональных данных (GDPR) служит ориентиром для разработки нормативной базы в Кыргызстане, обеспечивая высокий уровень защиты конфиденциальной информации [8].

Кроме того, сотрудничество с соседними странами Центральной Азии, включая Казахстан и Узбекистан, способствует созданию региональной системы киберустойчивости. Совместные учения по противодействию кибератакам, организованные в 2022 г., укрепили координацию действий в случае масштабных инцидентов [13].

Кыргызская Республика активно участвует в международных образовательных инициативах. В 2024 г. в рамках партнерства с Европейским центром по кибербезопасности, более 50 специалистов из государственных и частных организаций прошли обучение по вопросам защиты критически важных объектов и использования современных технологий, таких как искусственный интеллект и блокчейн [13, 14].

Программы обмена с ведущими университетами мира, включая обучение студентов и преподавателей в Великобритании и Германии, позволяют адаптировать передовые образовательные стандарты для Кыргызстана. Эти инициативы способствуют повышению уровня квалификации национальных специалистов.

Кыргызстан рассматривает возможность более глубокой интеграции в международные системы кибербезопасности, такие как Глобальный альянс по киберугрозам. Участие в таких инициативах позволит стране:

- получать доступ к глобальным базам данных о киберугрозах и инцидентах;
- координировать усилия по предотвращению атак через международные центры реагирования (CERT);
- использовать ресурсы для проведения совместных исследований и разработки технологий защиты.

Кроме того, интеграция в международные системы укрепит позиции Кыргызстана как активного участника глобального информационного сообщества, что создаст дополнительные возможности для привлечения инвестиций и технологий.

Для усиления международного взаимодействия и повышения уровня национальной кибербезопасности Кыргызстану рекомендуется:

- расширить участие в глобальных инициативах, таких как Глобальный форум по кибербезопасности, чтобы получить доступ к передовым технологиям и аналитическим ресурсам;
- укрепить сотрудничество с развитыми странами в области кибербезопасности через программы обмена кадрами и тренинги для специалистов;
- создать региональную платформу для обмена данными и реагирования на инциденты совместно с соседними странами Центральной Азии;
- инвестировать в участие в международных программах, которые помогут модернизировать национальную инфраструктуру и подготовить специалистов.

6. Стратегические рекомендации для укрепления информационной безопасности. В условиях стремительного развития цифровых технологий и увеличения числа киберугроз, Кыргызская Республика нуждается в системном подходе к обеспечению информационной безопасности. Для создания устойчивой и надежной защиты критически важных информационных инфраструктур требуется реализация стратегических инициатив в области законодательства, технологий, образования и международного сотрудничества.

Эффективное противодействие киберугрозам невозможно без создания современной нормативно-правовой базы. Кыргызской Республике рекомендуется:

- разработать новые законодательные акты, регулирующие защиту критической информационной инфраструктуры, с учетом международных стандартов, таких как ISO/IEC 27001;
- внедрить обязательные требования к защите данных для государственных учреждений и частного сектора, включая использование современных средств шифрования и многофакторной аутентификации;
- создать национальную программу сертификации кибербезопасности, которая установит единые требования для специалистов и организаций.

Примером может служить опыт Европейского Союза, где директива NIS2 создала единый подход к защите цифровых систем [24].

Технологическое развитие должно стать основой стратегии кибербезопасности. Кыргызстану необходимо:

- интегрировать искусственный интеллект и машинное обучение для анализа угроз и предсказания инцидентов;
- использовать квантовое шифрование для защиты государственных коммуникаций, особенно в оборонных и финансовых структурах;
- развивать системы мониторинга IoT-устройств и сетевого трафика для предотвращения атак на критическую инфраструктуру.

Мировой опыт показывает, что внедрение технологий, таких как платформа Cyber AI Analyst, позволяет значительно повысить устойчивость систем к кибератакам. Cyber AI Analyst автоматически

исследует предупреждения, упрощает расследования и приоритизирует инциденты, снижая нагрузку на специалистов по безопасности и уменьшая количество ложных срабатываний [25, 26].

Человеческий фактор остается одной из ключевых уязвимостей в информационной безопасности. Кыргызстану рекомендуется:

- включить основы киберграмотности в школьные и университетские программы, что позволит формировать устойчивую культуру безопасности;
- проводить регулярные тренинги и семинары для государственных служащих, направленные на повышение их осведомленности о современных угрозах;
- создать онлайн-платформу для самообучения, где граждане смогут получать информацию о методах защиты данных и распознавании кибератак.

В 2024 г. аналогичная инициатива в Сингапуре позволила снизить количество успешных фишинг-атак на 30 % [27].

Эффективная защита данных требует создания национальной системы мониторинга и реагирования на киберугрозы. Кыргызстану необходимо:

- разработать единую платформу реагирования на инциденты, объединяющую государственный и частный секторы;
- создать региональный CERT (Computer Emergency Response Team), который будет взаимодействовать с международными центрами и координировать действия при инцидентах;
- автоматизировать системы реагирования для минимизации времени на обнаружение и устранение угроз.

Для достижения высоких стандартов кибербезопасности важно наладить тесное взаимодействие с частными компаниями и международными организациями. Рекомендуется:

- поддерживать государственно-частное партнерство для разработки инновационных решений и обмена опытом;
- участвовать в глобальных инициативах, таких как Глобальный форум по кибербезопасности, что позволит интегрировать передовые практики в национальную систему;
- привлекать иностранные инвестиции для модернизации инфраструктуры и подготовки кадров.

Подготовка кадрового потенциала остается одним из важнейших аспектов национальной стратегии. Для улучшения образовательных инициатив Кыргызстану рекомендуется:

- создать специализированные учебные центры при вузах для подготовки специалистов в области ИИ, квантового шифрования и IoT;
- разработать программы обмена студентами и преподавателями с ведущими мировыми университетами, чтобы повышать уровень квалификации;
- организовать регулярные курсы повышения квалификации для действующих специалистов по кибербезопасности.

Заключение. В условиях цифровой трансформации обеспечение информационной безопасности становится приоритетной задачей национальной стратегии Кыргызской Республики. Проведенное исследование показало необходимость развития законодательной базы, внедрения передовых технологий, повышения уровня киберграмотности и усиления международного сотрудничества. Для достижения устойчивости в информационной сфере необходимо комплексное развитие национальной системы киберзащиты, включая образовательные инициативы и создание инновационной инфраструктуры.

Поступила: 03.02.2025; рецензирована: 17.02.2025; принята: 19.02.2025.

Литература

1. Website Rating. «Cybersecurity Statistics and Facts». URL: https://www.websiterating.com/ru/blog/research/cybersecurity-statistics-facts / (дата обращения: 15.11.2024).
2. Закон Кыргызской Республики «О защите персональных данных» / Официальный сайт Министерства цифрового развития Кыргызской Республики. URL: https://digital.gov.kg (дата обращения: 12.04.2023).

3. Национальная стратегия Кыргызской Республики «Цифровая трансформация 2030» / Официальный сайт Правительства Кыргызской Республики. URL: https://www.gov.kg (дата обращения: 06.04.2024).
4. Positive Technologies. «Рост числа кибератак в 2023 году: более 1,5 миллиона инцидентов». URL: https://habr.com/ru/news/771594/ (дата обращения 16.11.2024).
5. *Темирбаев К.Т.* Информационная безопасность Кыргызской Республики / К.Т. Темирбаев, А.А. Сагымбаев, Р.Н. Джаркеев, Т.Н. Кыдыралиев. Бишкек, 2007. 114 с.
6. Sputnik Кыргызстан. «В Кыргызстане открыли новый центр кибербезопасности». URL: https://ru.sputnik.kg/20230513/kyrgyzstan-kiberbezopasnost-zdanie-centr-gknb-1075288960.html (дата обращения: 21.06.2023).
7. SecurityLab. «Средняя стоимость утечки данных в 2023 году достигла 4,45 миллиона долларов США». URL: https://www.securitylab.ru/news/540308.php (дата обращения: 15.11.2024).
8. Отчет о кибербезопасности в Кыргызской Республике по данным Национального индекса кибербезопасности (NCSI), 2023. URL: https://ncsi.ega.ee/country/kg (дата обращения: 04.05.2024).
9. DW (Deutsche Welle). «Отключение электричества на Украине было вызвано кибератакой». URL: https://www.dw.com/ru/отключение-электричества-на-украине-было-вызвано-кибератакой/a-18969546. (дата обращения: 09.10.2024).
10. Positive Technologies. «85% фишинговых атак направлены на получение данных: анализ угроз». URL: https://habr.com/ru/news/793760/ (дата обращения: 01.11.2024).
11. CNews. «43 % успешных атак на организации в 2023 году связаны с социальной инженерией». URL: https://safe.cnews.ru/news/line/2024-10-22_issledovanie_positive_technologies (дата обращения: 10.11.2024).
12. SISA Infosec. «DDoS Attacks on IoT Devices Skyrocket in 2023». URL: https://www.sisainfosec.com/weekly-threat-watch/ddos-attacks-on-iot-devices-skyrocket-in-2023/ (дата обращения: 06.11.2024).
13. Региональные учения по кибербезопасности в Центральной Азии, 2022. Отчет ОБСЕ. URL: https://www.osce.org (дата обращения: 05.09.2024).
14. Европейский центр по кибербезопасности. Программы обмена опытом и обучения. URL: https://www.ecdctraining.eu (дата обращения: 06.11.2024).
15. Отчет компании Darktrace о системе Cyber AI Analyst / Официальный сайт компании. URL: https://www.darktrace.com (дата обращения: 15.07.2024).
16. Ration card (India). URL: https://en.wikipedia.org/wiki/Ration_card_(India) (дата обращения: 16.11.2024).
17. ID.ee. «Электронное голосование и электронные выборы в Эстонии». URL: https://www.id.ee/ru/artikkel/elektronnoe-golosovanie-i-elektronnye-vybory/. (дата обращения: 03.11.2024).
18. Habr. «Как Эстония использует блокчейн для защиты данных». URL: https://habr.com/ru/companies/wirex/articles/396095/ (дата обращения: 14.11.2024).
19. Naked Science. «В Китае запущена самая протяжённая и крупная сеть с квантовым шифрованием». URL: https://naked-science.ru/article/physics/v-kitae-zapushhena-samaya-protyazhennaya-i-krupnaya-set-s-kvantovym-shifrovaniem (дата обращения: 16.11.2024).
20. CNews. «Китай и Россия создали защищённый спутниковый квантовый канал связи». URL: https://www.cnews.ru/news/top/2024-04-02_kitaj_i_rossiya_sozdali_sputnikovyj (дата обращения: 11.11.2024).
21. National Initiative for Cybersecurity Education (NICE). URL: https://en.wikipedia.org/wiki/National_Initiative_for_Cybersecurity_Education.
22. CISA (Cybersecurity and Infrastructure Security Agency). «Cybersecurity Education & Career Development». URL: https://www.cisa.gov/resources-tools/programs/cybersecurity-education-career-development (дата обращения: 13.11.2024).
23. Cybersecurity Coalition. «About the Cybersecurity Coalition». URL: https://www.cybersecuritycoalition.org/ (дата обращения: 16.11.2024).
24. Европейский Союз. Директива NIS2 о безопасности сетей и информационных систем / Официальный сайт ЕС. URL: https://ec.europa.eu (дата обращения: 03.06.2024).
25. Darktrace. «Cyber AI Analyst: Revolutionizing Security Operations». URL: https://darktrace.com/cyber-ai-analyst (дата обращения: 13.11.2024 г.).
26. *Мамадалиева К.А.* Кибербезопасность и финансовые угрозы: борьба за безопасность в эпоху цифровых рисков / К.А. Мамадалиева, Р.Д. Калбаева // Сборник научных трудов по итогам Международной научно-практической конференции. М., 2023. С. 682–689.
27. Национальная инициатива Сингапура по повышению киберграмотности. Официальный отчет. URL: https://www.singaporecybersecurity.sg (дата обращения: 22.08.2024).