УДК 004.056:341
DOI: 10.36979/1694-500X-2024-24-12-101-105

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ВЫЗОВЫ И ВОЗМОЖНОСТИ

Абдысамат А. Сагымбаев, Ж.Б. Мамадалиева, Амантур А. Сагымбаев, А.С. Курманкожоева

Аннотация. Рассмотрены современные угрозы и вызовы в области информационной безопасности, в том числе киберугрозы, связанные с быстрым развитием технологий, таких как искусственный интеллект и квантовые вычисления, и их влияние на национальные информационные системы. Подчёркнут рост числа кибератак на критическую инфраструктуру, включая банковские системы, здравоохранение и энергетику в Кыргызстане. Рассматриваются проблемы цифрового неравенства и зависимость от иностранных технологий, которые создают дополнительную уязвимость для развивающихся стран, таких как Кыргызская Республика. Предлагаются решения в виде разработки национальных стратегий по кибербезопасности и разработке локальных технологий.

Ключевые слова: киберугрозы; искусственный интеллект; квантовые вычисления; цифровая трансформация; кибератаки; кибербезопасность; цифровое неравенство; фишинг и ransomware-атаки.

ЭЛ АРАЛЫК МААЛЫМАТ КООПСУЗДУГУ: КЫЙЫНЧЫЛЫКТАР ЖАНА МҮМКҮНЧҮЛҮКТӨР

Абдысамат А. Сагымбаев, Ж.Б. Мамадалиева, Амантур А. Сагымбаев, А.С. Курманкожоева

Аннотация. Макалада маалыматтык коопсуздук чөйрөсүндөгү заманбап коркунучтар жана чакырыктар, анын ичинде жасалма интеллект жана кванттык эсептөө сыяктуу технологиялардын тез өнүгүшү менен байланышкан кибер коркунучтар жана алардын улуттук маалымат системаларына тийгизген таасири каралат. Кыргызстанда банк тутумдары, саламаттыкты сактоо жана энергетика сыяктуу маанилүү инфраструктурага киберчабуулдардын көбөйүшү баса белгиленет. Санариптик теңсиздик жана Кыргыз Республикасы сыяктуу өнүгүп келе жаткан өлкөлөр үчүн кошумча алсыздыктарды жараткан чет өлкөлүк технологияларга көз карандылык көйгөйлөрү каралат. Чечимдер киберкоопсуздуктун улуттук стратегияларын иштеп чыгуу жана жергиликтүү технологияларды өнүктүрүү түрүндө сунушталат.

Түйүндүү сөздөр: киберкоркунучтар; жасалма интеллект; кванттык эсептөө; санариптик трансформация; киберчабуулдар; кибер коопсуздук; санариптик теңсиздик; фишинг жана ransomware чабуулдары.

INTERNATIONAL INFORMATION SECURITY: CHALLENGES AND OPPORTUNITIES

Abdysamat A. Sagymbaev, Zh.B. Mamadalieva, Amantur A. Sagymbaev, A.S. Kurmankozhoeva

Abstract. The article analyzes modern threats and challenges in the field of information security, including cyber threats related to the rapid development of technologies such as artificial intelligence and quantum computing, and their impact on national information systems are considered. The growing number of cyber attacks on critical infrastructure, including banking systems, healthcare and energy in Kyrgyzstan, was highlighted. The problems of digital inequality and dependence on foreign technologies, which create additional vulnerability for developing countries such as the Kyrgyz Republic, are considered. Solutions are proposed in the form of developing national cybersecurity strategies and developing local technologies.

Keywords: cyber threats; artificial intelligence; quantum computing; digital transformation; cyber attacks; cybersecurity; digital inequality; phishing and ransomware attacks.

Введение. В последние годы международное сообщество столкнулось с серьезными проблемами, включая пандемию коронавирусной инфекции (COVID-19) и вооруженные конфликты в нескольких регионах мира, что нарушает стабильность существования человечества. Все эти факторы затормозили трансформационные процессы глобализации мира. Общеизвестно, что главным инструментом глобализации являются стремительно развивающиеся информационно-коммуникационные технологии (ИКТ), которые проникают во все сферы жизни общества, как на национальном, так и международном уровнях, тем самым создавая условия для успешной интеграции развивающих стран в глобальное информационное пространство [1].

1. Общие угрозы международной информационной безопасности

Международная информационная безопасность сталкивается с рядом серьезных вызовов, которые обусловлены быстрым развитием информационно-коммуникационных технологий (ИКТ) и цифровизации [2–6]. Одним из главных факторов риска является растущая уязвимость критической информационной инфраструктуры, которая охватывает такие сферы, как энергетика, транспорт, здравоохранение и финансовый сектор. В 2023 году было зарегистрировано значительное увеличение числа кибератак на ключевые объекты инфраструктуры. Например, атаки на системы здравоохранения и энергетики увеличились на 45 %, что подчеркивает критическую важность защиты данных и информационных систем для обеспечения национальной и международной безопасности. В Кыргызской Республике и других странах Центральной Азии остро стоит проблема информационной безопасности в связи с геополитическими факторами и сложной региональной ситуацией [2, 5, 6]. Примером этого может служить случай с кибератакой на финансовую инфраструктуру Кыргызской Республики в 2022 году, когда злоумышленники попытались взломать платежные системы, что вызвало временные перебои в банковской системе страны. Этот инцидент показал необходимость укрепления защиты национальных информационных ресурсов.

Киберугрозы продолжают эволюционировать, и злоумышленники всё чаще используют новые методы, такие как фишинг, атаки через программное обеспечение – вымогатель (ransomware), и сложные DDoS-атаки. Важным фактором является анонимность, которую предоставляет киберпространство, создавая благоприятные условия для незаконной деятельности, включая кибершпионаж и кибервойны.

Пропаганда через интернет также становится всё более опасным инструментом дестабилизации. Интернет-платформы часто используются террористическими организациями для вербовки сторонников, распространения идеологии насилия и создания дезинформационных кампаний. Это затрудняет поддержание информационной безопасности и требует усиления международного сотрудничества для противодействия данным угрозам.

Необходимо также отметить и ***разрыв в цифровом развитии***, или «цифровое неравенство», которое создает дополнительные сложности для развивающихся стран, таких как Кыргызстан. Страны с низким уровнем цифровой грамотности и слабой инфраструктурой становятся более уязвимыми к информационным угрозам и оказываются в положении зависимости от передовых держав, доминирующих на рынке ИКТ. Например, по данным Международного союза электросвязи (МСЭ) [7–9] и отчета Ассоциации GSM операторов связи [10], на 2022 год лишь 27 % населения стран с низким уровнем дохода имело доступ к интернету, что значительно отстает от показателей развитых стран, где уровень интернет-покрытия превышает 90 %.

Для обеспечения эффективной защиты в эпоху цифровизации необходимо принимать меры по повышению осведомленности населения, созданию более устойчивой информационной инфраструктуры, а также разрабатывать международные механизмы сотрудничества для противодействия киберугрозам.

В ответ на растущие киберугрозы Кыргызская Республика активно развивает своё сотрудничество с международными организациями, такими как ООН и Шанхайская организация сотрудничества (ШОС), в рамках которых реализуются программы по повышению уровня кибербезопасности. В 2021 году в рамках сотрудничества с ШОС были проведены учения по киберзащите, в которых приняли

участие специалисты из нескольких стран Центральной Азии [11]. Эти учения позволили нашей стране повысить свои навыки по отражению кибератак и наладить обмен информацией между странами-участниками. Кыргызская Республика также предпринимает шаги по улучшению внутреннего законодательства в области кибербезопасности. В 2022 г. был разработан законопроект, направленный на регулирование использования цифровых технологий в государственных органах, что должно снизить уязвимость к атакам на государственные информационные системы [12].

2. Новые технологии и их влияние на Кыргызскую Республику

Развитие технологий, таких как искусственный интеллект (ИИ) и квантовые вычисления, оказывает всё большее влияние на международную и национальную информационную безопасность. Кыргызская Республика, как часть глобального информационного сообщества, сталкивается с необходимостью адаптации к этим изменениям, что требует как возможностей, так и выработки стратегий по защите от новых рисков.

Чтобы противостоять таким вызовам, Кыргызстан начал разрабатывать стратегии по противодействию угрозам, связанным с ИИ. В 2023 году был запущен проект по созданию национальной системы киберзащиты с применением ИИ [13], которая позволит более эффективно мониторить и предотвращать атаки на государственные сети.

Искусственный интеллект становится важным инструментом для оптимизации государственных услуг и управления данными. Например, ИИ может улучшить процессы в таких областях, как здравоохранение, образование и сельское хозяйство, которые являются приоритетными сферами для нашей республики. Внедрение ИИ помогает ускорить анализ данных, снижая нагрузку на государственные ресурсы и улучшая предоставление услуг гражданам.

Однако значительные риски связаны и с использованием ИИ в кибератаках. В частности, системы ИИ могут использоваться злоумышленниками для автоматизации атак и манипуляции информацией. Например, модели генеративного ИИ способны создавать поддельные новости и видео (deepfake), что может нанести урон общественному доверию к политическим процессам в стране, особенно в периоды политической нестабильности. Слабая цифровая грамотность населения усугубляет эту проблему, делая его более уязвимым для дезинформации.

Кибершпионаж и целевые атаки на критические инфраструктуры, такие как государственные системы и финансовые учреждения, становятся более сложными из-за использования ИИ. Важным шагом для Кыргызской Республики является укрепление киберзащиты, чтобы минимизировать потенциальные угрозы, исходящие от таких атак.

Что касается ***квантовых вычислений***, то эта технология находится на стадии активного развития и имеет потенциал в ближайшие десятилетия изменить ландшафт информационной безопасности. Современные криптографические методы защиты данных могут быть легко взломаны квантовыми компьютерами, что создаёт значительный риск для государственных и финансовых систем. Для Кыргызской Республики, как и для многих стран с ограниченными ресурсами, переход на более устойчивые к квантовым атакам системы шифрования станет серьёзным вызовом.

Помимо этого, ***цифровое неравенство*** продолжает быть актуальной проблемой. По данным Международного союза электросвязи [9] на 2022 год, интернетом регулярно пользуется лишь 55 % населения Кыргызской Республики. Это ограничивает возможности страны по интеграции в глобальное цифровое пространство и увеличивает её уязвимость перед внешними угрозами, поскольку значительная часть населения остаётся без доступа к современным технологиям и средствам защиты от информационных атак.

Зависимость от иностранных технологий также влечёт за собой дополнительные риски. Критические элементы информационной инфраструктуры Кыргызской Республики – от финансовых систем до телекоммуникаций, зависят от зарубежных поставок технологий и программного обеспечения. Это увеличивает вероятность кибератак и возможных вмешательств извне. Поэтому нашей стране

необходимо выработать долгосрочную стратегию по снижению этой зависимости и укреплению собственной цифровой суверенности.

Для минимизации этих рисков государство должно активнее разрабатывать и внедрять меры по защите данных, а также повышать уровень кибербезопасности во всех сферах. Участие в международных инициативах по укреплению киберзащиты, таких как программы ООН и ШОС, а также развитие собственных технологий позволит Кыргызской Республике защитить свои интересы в условиях быстро меняющегося цифрового ландшафта.

3. Заключение, рекомендации и прогноз

Международная информационная безопасность становится всё более важной в условиях ускоряющейся цифровизации и роста глобальных киберугроз. Как было отмечено ранее, Кыргызская Республика сталкивается с рядом проблем, вызванных не только внутренними факторами, такими как цифровое неравенство и слабая инфраструктура, но и внешними угрозами, включая кибератаки и технологическую зависимость от зарубежных поставщиков.

Прогноз на будущее. С учётом текущих глобальных тенденций в области информационной безопасности можно выделить несколько ключевых направлений развития, которые окажут значительное влияние на будущее Кыргызской Республики и других стран:

1. Рост угроз со стороны искусственного интеллекта и автоматизации атак. В ближайшие годы ожидается увеличение числа кибератак с использованием ИИ. Технологии, позволяющие автоматизировать атаки и быстрее анализировать уязвимости, будут развиваться, что усложнит защиту информационных систем. Прогнозируется, что злоумышленники всё чаще будут использовать ИИ для создания более сложных видов фишинга, а также для кибершпионажа. Кыргызской Республике придётся адаптировать свои киберзащитные механизмы и обучать специалистов для противодействия этим угрозам.

2. Развитие квантовых вычислений и угроза для традиционной криптографии. В течение следующего десятилетия квантовые компьютеры могут стать реальностью, что поставит под угрозу существующие методы шифрования данных. Это означает, что Кыргызская Республика и другие страны должны будут начать переход на квантово-устойчивые системы шифрования для защиты своих критических данных. Прогнозируется, что страны, не подготовленные к этим изменениям, столкнутся с серьёзными рисками утечки информации и утратой конфиденциальных данных.

3. Усиление регулирования и глобального сотрудничества. В ответ на нарастающие киберугрозы международное сообщество будет усиливать законодательные меры и внедрять новые стандарты в области кибербезопасности. Кыргызская Республика может извлечь выгоду из активного участия в этих инициативах, что позволит адаптировать лучшие мировые практики для защиты собственной инфраструктуры. Международное сотрудничество в рамках ШОС, ООН и СНГ станет ключевым фактором успешного противостояния киберугрозам.

4. Повышение значения защиты персональных данных. В условиях расширяющегося применения ИКТ и увеличения количества подключенных устройств (IoT), защита персональных данных станет важнейшим направлением кибербезопасности. Ожидается, что международное сообщество будет разрабатывать и внедрять более жёсткие меры по защите конфиденциальности. Кыргызской Республике придётся интегрировать новые стандарты и законодательные нормы, чтобы обеспечить безопасность данных своих граждан и предприятий.

5. Цифровая трансформация и новые возможности для развивающихся стран. Несмотря на риски, цифровизация и развитие ИКТ открывают для стран, таких как Кыргызская Республика, новые возможности. Улучшение цифровой инфраструктуры, развитие местных технологий и повышение цифровой грамотности помогут сократить цифровое неравенство и укрепить позиции страны в глобальном информационном пространстве. Прогнозируется, что с правильными инвестициями в образование и инфраструктуру, Кыргызская Республика сможет воспользоваться преимуществами цифровой экономики, улучшив качество жизни своих граждан.

Рекомендации. В свете этих прогнозов, Кыргызская Республика должна уделять приоритетное внимание следующим шагам, это:

- усиление киберзащиты с учётом новых угроз, включая ИИ и квантовые вычисления;
- снижение зависимости от зарубежных технологий и развитие собственной технологической базы;
- активное участие в международных инициативах по кибербезопасности;
- повышение цифровой грамотности населения и развитие образовательных программ по информационной безопасности;
- усиление законодательства в области защиты персональных данных и конфиденциальной информации.

Эти меры помогут Кыргызской Республике адаптироваться к меняющимся условиям информационной безопасности и защитить свою инфраструктуру от новых вызовов.

Поступила: 28.10.24; рецензирована: 11.11.24; принята: 13.11.24.

Литература

1. Доклад Генерального секретаря ООН. Экономический и Социальный Совет: Прогресс, достигнутый в осуществлении решений и последующей деятельности по итогам Всемирной встречи на высшем уровне по вопросам информационного общества на региональном и международном уровнях. URL: https://undocs.org/ru/A/79/62 (дата обращения: 10.09.2024).
2. Указ Президента Кыргызской Республики. Концепция национальной безопасности Кыргызской Республики. URL: https://cbd.minjust.gov.kg/430810/edition/1118040/ru (дата обращения: 12.09.2024).
3. Указ Президента РФ. Основы государственной политики РФ в области международной информационной безопасности. URL: https://static.kremlin.ru (дата обращения: 15.09.2024).
4. *Бойко С.* Материалы конференции «Kuban CSC-2022». Международная информационная безопасность: новые вызовы и угрозы. URL: https://interaffairs.ru/jauthor/materia (дата обращения: 13.09.2024).
5. *Жайлообаев Н.* Проблема национальной безопасности: сб. статей. Бишкек: Ин-т социально-политических технологий, 2006.
6. *Алымбаева З.А.* Особенности и тенденции современного информационного пространства Кыргызстана / З.А. Алымбаева, А. Алимахунов // Бюллетень науки и практики. 2021. Т. 7. № 2. С. 271–275. URL: https://doi.org/10.33619/2414-2948/63/29 (дата обращения: 17.09.2024).
7. Пресс-релиз Международного союза электросвязи (МСЭ) от 12 сентября 2023 года. Достижение всеобщей и значимой цифровой связи. URL: https://www.itu.int/en/mediacentre/Pages/PR-2023-09-12.aspx (дата обращения: 10.10.2024).
8. Отчёт Международного союза электросвязи. «Измерение цифрового развития – факты и цифры 2023 года». URL: https://www.itu.int/hub/publication/d-ind-ict_mdd-2023-1 (дата обращения: 15.10.2024).
9. Пресс-релиз Международного союза электросвязи (МСЭ). Глобальная оценка цифрового разрыва. 2022 год. URL: https://www.itu.int/en/digital-gender-gap.
10. Отчёт Ассоциации GSM операторов связи. О состоянии мобильной интернет-связи за 2023 год. URL: https://www.gsma.com/r/somic (дата обращения: 18.10.2024).
11. ГКНБ: В Бишкеке проходят учения по кибербезопасности. URL: https://today.kg/news/145719 (дата обращения: 20.10.2024).
12. Министерство цифрового развития Кыргызской Республики разрабатывает Цифровой кодекс Кыргызстана. URL: https://economist.kg/novosti/2022/08/15/mincifry-razrabatyvaet-cifrovoj-kodeks-kyrgyzstana (дата обращения: 21.10.2024).
13. Риск или возможность. Власти Кыргызстана начинают внедрять искусственный интеллект в работу госсектора. URL: https://rus.azattyk.org/a/32802618.html (дата обращения: 22.10.2024).