Вестник Национального исследовательского ядерного университета «МИФИ», 2025, т. 14, № 3, с. 240–248

ПРИКЛАДНАЯ МАТЕМАТИКА И ИНФОРМАТИКА

https://doi.org/10.26583/vestnik.2025.3.6 *Оригинальная статья* / *Original paper*

УДК 004.056.5

Квантовые киберугрозы и их воздействие на безопасность критической информационной инфраструктуры

И. А. Василенко

АНОО ВО «Университет «Сириус», федеральная территория «Сириус», 354349, Россия

Использование квантовых технологий в современном мире создает масштабные вызовы для сохранности критически значимой информационной инфраструктуры, на которой базируются такие основные отрасли, как медицина, энергетика, транспорт и связь. Криптографические алгоритмы RSA и ECC, долгое время считавшиеся надежными, утратили свою устойчивость перед мощью квантовых вычислений, что делает первостепенной задачей поиск современных решений для обеспечения защиты данных. Главные риски, которые несут квантовые компьютеры, включают возможность компрометации алгоритмов шифрования и возникающие вследствие этого угрозы целостности информации и устойчивости функционирования жизненно важных систем. Методологическая основа исследования основывается на анализе 318 источников из таких международных баз данных, как Scopus, Web of Science и др. Из этого количества были отобраны 24 публикаций, наиболее релевантных теме. Был проведен сравнительный метод анализа классических и квантовых угроз. Цель исследования – изучить влияние квантовых атак на безопасность критической информационной инфраструктуры (КИИ) на современном уровне и предложить пути перехода к квантово-устойчивым решениям. Результаты работы подчеркивают необходимость внедрения таких инновационных криптографических подходов, как алгоритмы на основе решеток и кодов, а также комбинированных (гибридных) технологий. Успешная защита инфраструктуры требует системного подхода, включающего комплексный аудит текущих систем, обучение специалистов и снятие технических и нормативных ограничений. Разработанный поэтапный план минимизирует риски и создает основу для безопасного внедрения новых стандартов.

Ключевые слова: квантовые киберугрозы, критическая информационная инфраструктура, защита информации, интернет, потенциальные атаки.

Введение

Инфраструктура критической значимости (КИИ) включает в себя совокупность информационных систем, телекоммуникационных сетей и автоматизированных управляющих комплексов, обеспечивающих стабильное функционирование ключевых отраслей, которые играют основополагающую роль для государства и общества. К таким сферам относятся здравоохранение, научные исследования, транспорт, связь, энергетика, финансовый сектор, топливно-энергетический комплекс, а также промышленность оборонного назначения, космическая, горнодобывающая, металлургическая и химическая отрасли. Ключевые риски, угрожающие КИИ, связаны с утратой конфиденциальности, искажением целостности и ограничением доступности информации. При этом конфиденциальность подразумевает предотвращение несанкционированного доступа к данным, целостность гарантирует их точность и полноту, а доступность – обеспечение своевременного доступа к информации для тех, кто обладает соответствующими правами [1]. Развитие квантовых вычислительных технологий представляет собой серьезный

✉ И.А. Василенко: iravas988@yandex.ru

Поступила в редакцию: 09.04.2025
После доработки: 03.06.2025
Принята к публикации: 03.06.2025

EDN PYGDET

вызов таким традиционным криптографическим механизмам, как RSA и ECC, которые рискуют утратить свою надежность, что открывает путь для потенциальной компрометации защищенных систем. Вдобавок к этому активное внедрение технологий Интернета вещей (IoT) и увеличение количества устройств, подключенных к сети, создают дополнительные точки уязвимости, что многократно усиливает угрозы для КИИ. В частности, согласно статистическим данным, за первую половину 2022 г. в России было зафиксировано увеличение числа атакованных IoT-устройств на 40 %, что подтверждает масштаб растущих рисков для информационной безопасности[1]. Таким образом, поддержание безопасности КИИ требует систематического наблюдения за технологическими изменениями, оперативной адаптации к новым угрозам, внедрения передовых защитных инструментов и постоянного повышения квалификации специалистов в области кибербезопасности. Основная цель исследования заключается в изучении влияния квантовых угроз на устойчивость КИИ и разработке практических рекомендаций для ее надежной защиты.

Методология исследования

В ходе исследования научных публикаций было обработано 318 источников, извлеченных из таких известных баз данных, как Elibrary, Scopus, Web of Science и SpringerLink. Из общего объема отобрано 24 наиболее значимых работ, посвященных вопросам квантовых вычислений, уязвимостям актуальных криптографических методов и подходам к их защите. Для уточнения поиска применялись запросы: «quantum computing», «post-quantum cryptography», «cybersecurity threats», «critical infrastructure», «RSA vulnerability», «ECC attacks». Результаты проведенного анализа позволили выделить ключевые векторы развития постквантовой криптографии, а также обозначить основные угрозы, касающиеся RSA и ECC. Кроме того, сравнительное изучение традиционных и квантовых киберугроз дало возможность упорядочить методы атак, их влияние на системы и последствия для криптографической инфраструктуры.

Определение угроз квантовых вычислений и защита информации

Опираясь на законы квантовой механики, квантовые вычисления открывают новые горизонты в информатике, полностью трансформируя подходы к обработке данных. Их ключевыми принципами являются суперпозиция, запутанность и интерференция – уникальные свойства, позволяющие квантовым машинам справляться с задачами, которые недостижимы для традиционных систем [2]. Вместо привычных битов, фиксированных в состояниях 0 или 1, в квантовых компьютерах используются кубиты, способные одновременно находиться в нескольких состояниях, что значительно повышает их вычислительные возможности за счет параллелизма. Однако, несмотря на значительный прогресс, данные технологии ставят под угрозу безопасность существующих криптографических систем, вызывая необходимость пересмотра методов защиты информации в условиях квантовой эпохи [3].

Квантовые вычисления несут три основные угрозы безопасности информационных систем.

1. Компрометация криптографических алгоритмов: квантовые компьютеры, используя алгоритм Шора, подрывают безопасность таких широко применяемых систем шифрования, как RSA, DSA и ECC. Эти механизмы, основанные на сложности математических задач (факторизации крупных чисел и вычислении дискретных логарифмов), утрачивают свою эффективность перед вычислительными возможностями квантовых технологий [4, 5].

2. Угроза искажения и подмены информации в результате компрометации криптографических механизмов. Кватновые атаки, получив доступ к ключам шифрования, могут открыть путь для вмешательства в передаваемые данные. Хотя сами по себе квантовые алгоритмы не искажают данные напрямую, уязвимости, возникающие после взлома, делают возможными вмешательста стороннего нарушителя. Это создает значительные риски для платформ, критически зависящих от достоверности информации, например, в области финансовых транзакций или управления стратегической инфраструктурой [6].

[1] Количество атак на IoT-устройства в России выросло на 40 % за первое полугодие 2022 г. [Электронный ресурс]. URL: https://www.kaspersky.ru/about/press-releases/kolichestvo-atak-na-iot-ustrojstva-v-rossii-vyroslo-na-40-za-pervoe-polugodie-2022-goda?utm_source=chatgpt.com (дата обращения: 02.12.2024).

3. Риск нарушения доступа к данным, обусловленный вторичными эффектами квантовой атаки. В случае успешного обхода защиты или блокировки систем может быть затруднен и невозможен доступ к информацилнным ресурсам. В результате возможна дестабилизация ключевых отраслей: основополагающие секторы, включая энергетику, транспорт, медицину и государственное управление, подвергаются опасности отказа в работе. Такие последствия опосредованно связаны с квантовыми возможностями, что несет угрозу устойчивости и функционированию систем жизненной важности.

Современные методы криптографической защиты, включая алгоритмы RSA, ECC и симметричные протоколы, теряют свою эффективность перед угрозами, возникающими из-за квантовых вычислений. Защита RSA (Rivest – Shamir – Adleman), базирующаяся на сложности разложения больших чисел на простые множители, ранее считалась практически неуязвимой, так как классическим компьютерам для выполнения подобных операций требуются миллионы лет [7]. Однако с появлением алгоритма Шора мощные квантовые компьютеры способны решать такие задачи за несколько часов, что обесценивает надежность RSA. Также криптография эллиптических кривых (ECC), использующая сложность дискретных логарифмов для обеспечения безопасности при меньших длинах ключей, оказывается неспособной противостоять вычислительным возможностям квантовых систем [8, 9].

Для всестороннего понимания проблемы требуется выполнить детальный сравнительный анализ угроз, создаваемых классическими и квантовыми кибератаками, включая их методы воздействия и последствия для систем безопасности. Этот анализ необходим для выявления различий между этими угрозами и выработки практических рекомендаций по защите критической инфраструктуры в условиях ускоряющегося развития квантовых технологий. Представленная ниже таблица служит инструментом для структурирования информации, подчеркивая основные различия, возможные риски и доступные способы защиты (табл. 1) [10 – 13].

Таблица 1. Сравнительный анализ классических и квантовых киберугроз

Категория	Классические киберугрозы	Квантовые киберугрозы
Типы угроз	Вирусы и черви. Фишинг. DDoS-атаки. Взлом паролей. Эксплойты уязвимостей ПО	Взлом асимметричных криптографических алгоритмов (RSA, ECC) с использованием квантовых компьютеров. Ускоренный перебор ключей симметричных алгоритмов (например, AES) с помощью алгоритма Гровера. Потенциальные атаки на квантовые коммуникационные каналы
Методы атаки	Использование известных уязвимостей. Социальная инженерия. Брутфорс. Малварь	Применение алгоритма Шора для факторизации больших чисел и взлома RSA. Использование алгоритма Гровера для ускоренного перебора ключей. Возможность подслушивания квантовых каналов связи при недостаточной защите.
Влияние на криптографию	Требуют увеличения длины ключей и улучшения алгоритмов шифрования. Необходимость регулярного обновления и патчей для устранения уязвимостей	Угроза полной компрометации текущих асимметричных алгоритмов шифрования. Необходимость разработки и внедрения постквантовых криптографических алгоритмов
Меры противодействия	Антивирусные программы. Фаерволы. Системы обнаружения вторжений (IDS). Обучение сотрудников кибергигиене. Регулярные обновления ПО	Разработка и внедрение квантово-устойчивых криптографических алгоритмов. Использование квантового распределения ключей (QKD) для обеспечения безопасной связи. Обновление инфраструктуры безопасности для противодействия квантовым атакам
Влияние на системы безопасности	Могут привести к утечке данных, финансовым потерям, нарушению работы систем. Требуют постоянного мониторинга и обновления систем безопасности	Потенциальная компрометация всей цифровой инфраструктуры, основанной на текущих криптографических стандартах. Необходимость глобального перехода на новые стандарты шифрования и обновления всех систем безопасности

Противопоставление традиционных и квантовых киберугроз позволяет выявить их принципиальные различия в механизмах воздействия, источниках угроз и степени риска для безопасности систем. Такие традиционные атаки, как вирусные программы, фишинг, DDoS-атаки и использование уязвимостей, опираются на эксплуатацию известных слабых мест в программном обеспечении и ошибках пользователей. Для защиты от таких угроз применяются проверенные методы, включая антивирусы, системы фильтрации трафика (фаерволы), инструменты обнаружения вторжений и регулярные обновления программного обеспечения. Однако, несмотря на наличие устоявшихся мер защиты, необходимость их усовершенствования и постоянного контроля остается актуальной [14].

В то же время меры противодействия квантовым угрозам требуют принципиально нового подхода. В отличие от классических атак, квантовые угрозы обусловлены вычислительными возможностями квантовых компьютеров, которые делают уязвимыми традиционные криптографические алгоритмы [15, 16]. Для минимизации рисков требуется внедрение таких технологий, как постквантовая криптография и квантовое распределение ключей (QKD). Однако их реализация сталкивается с масштабными трудностями, включая значительные технические ограничения, высокую стоимость и необходимость изменений в организационных процессах. Квантовые угрозы оказывают более разрушительное воздействие на системы безопасности, чем классические атаки. Если последствия традиционных угроз сводятся к утечкам данных и временным сбоям в работе систем, квантовые атаки способны поставить под угрозу устойчивость всей цифровой инфраструктуры, использующей современные криптографические стандарты. Таким образом, переход к технологиям, устойчивым к квантовым атакам, требует не только разработки инновационных решений, но и кардинального изменения подходов к планированию и распределению ресурсов на долгосрочную перспективу [17].

Постквантовая криптография (PQC) разрабатывает методы, которые способны эффективно противостоять угрозам, исходящим от квантовых компьютеров. Среди ключевых направлений выделяются три основные группы алгоритмов [18].

Первая категория включает такие решеточные схемы, как Learning With Errors (LWE) и NTRU. Они основываются на решении задач, связанных с векторными решетками, что обеспечивает их высокую устойчивость к квантовым атакам, и делает эти алгоритмы одними из наиболее перспективных для стандартизации. Вторая группа представлена кодовыми алгоритмами, в том числе схемой МакЭлиса, которые используют сложность декодирования случайных линейных кодов. Однако их внедрение затрудняется из-за значительных размеров ключей, необходимых для их работы. Третья категория – мультивариантные алгоритмы, построенные на решении нелинейных систем уравнений. Примером может служить схема Rainbow, особенно подходящая для реализации цифровых подписей. В августе 2024 г. Национальный институт стандартов и технологий США (NIST) утвердил глобальные стандарты постквантового шифрования – FIPS 203, FIPS 204 и FIPS 205. Это решение стало важным этапом в развитии информационной безопасности, отражая необходимость адаптации криптографических методов к вызовам квантовой эры [19].

Квантовая криптография, в частности технология квантового распределения ключей (QKD), представляет собой инновационный подход к защите данных, основанный на фундаментальных законах квантовой механики. QKD позволяет участникам безопасно обмениваться секретными ключами, а попытки несанкционированного доступа могут быть выявлены на этапе передачи. Однако процесс интеграции QKD в действующую инфраструктуру требует существенных финансовых вложений и решения ряда сложных инженерных задач. Эффективная защита ключевых инфраструктур от рисков, связанных с квантовыми угрозами, предполагает стратегическое использование комбинированных решений [20]. Такой гибридный подход, сочетающий традиционные и постквантовые криптографические алгоритмы, обеспечивает не только постепенный переход к новым стандартам безопасности, но и позволяет минимизировать риски, возникающие из-за потенциальных уязвимостей недавно разработанных технологий.

Во-вторых, важнейшим элементом перехода на постквантовые стандарты выступает детальное планирование. Оно начинается с комплексного анализа существующих систем, направленного на выявление применяемых криптографических методов и их слабых мест перед квантовыми атаками. Результаты этой работы становятся основой для разработки пошагового плана, определяющего последовательность внедрения постквантовых алгоритмов и сроки их реализации [21]. При этом ключевое

внимание уделяется профессиональной подготовке кадров: повышение компетенций специалистов в области новых криптографических технологий гарантирует правильное внедрение и эксплуатацию обновленных решений.

В-третьих, важным аспектом реализации постквантовой защиты является устранение препятствий, которые могут возникнуть в процессе адаптации. К числу технических задач относится обеспечение совместимости инновационных алгоритмов с действующими системами. С точки зрения экономики требуется проведение анализа затрат для оптимизации ресурсов, выделяемых на внедрение. Наряду с этим необходимо адаптировать нормативные документы, включая стандарты и регламенты, к требованиям постквантовой криптографии [22]. Только такой комплексный подход позволит минимизировать риски и создать надежную основу для устойчивой защиты критически важных объектов инфраструктуры [23].

Чтобы обеспечить эффективный переход к новым стандартам, процесс управления должен быть четко структурирован. Этапы анализа текущих систем, выбора наиболее подходящих мер защиты и их внедрения требуют строгой координации [24]. Схема, представленная в тексте, детализирует ключевые шаги, необходимые для нейтрализации угроз, связанных с развитием квантовых технологий.

На иллюстрированной схеме (рис. 1) подробно описан алгоритм последовательных действий, направленных на защиту КИИ от рисков, связанных с квантовыми угрозами. Первым шагом предусмо-

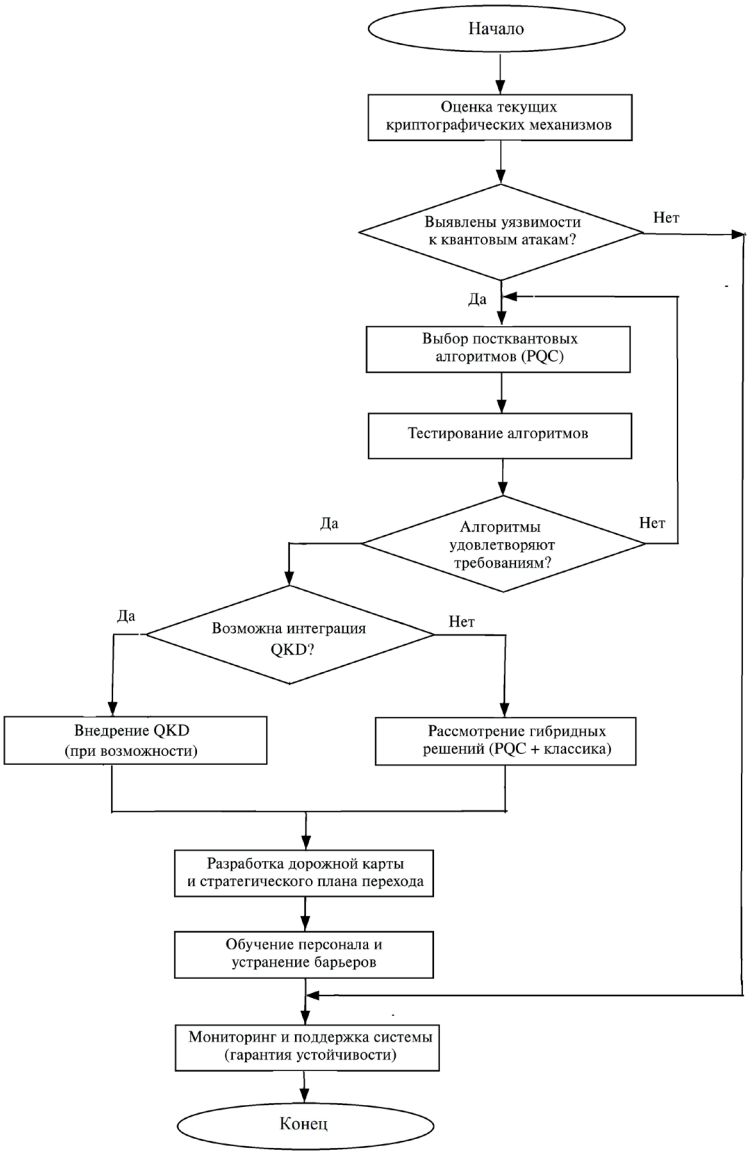

Рис. 1. Алгоритм защиты критической информационной инфраструктуры от квантовых угроз

трена глубокая оценка текущих криптографических механизмов для выявления их уязвимостей перед атаками с использованием квантовых технологий. Если анализ подтверждает наличие таких слабостей, следующим этапом становится выбор подходящих алгоритмов, после чего проводится их тщательное тестирование. Внедрение постквантовой криптографии (PQC) и квантового распределения ключей (QKD) могут использоваться параллельно, поэтапно или альтернативно, в зависимости от условий конкретной системы. В случае невозможности реализации QKD предлагается рассматривать гибридные подходы, где комбинируются классические и постквантовые решения.

Далее предусмотрен этап стратегического планирования, включающий разработку дорожной карты, которая определяет основные этапы перехода на постквантовые стандарты, сроки выполнения работ и ключевые задачи. Важным компонентом этого этапа является обучение специалистов новым криптографическим методам и устранение существующих барьеров технического, экономического и нормативного характера. Финальный шаг направлен на обеспечение постоянного мониторинга и технической поддержки системы, что гарантирует ее устойчивость перед потенциальными вызовами. Такая структурированная модель обеспечивает не только надежное управление процессом адаптации к новым стандартам безопасности, но и минимизирует риски, связанные с возможными недостатками внедряемых решений.

Заключение

Развитие квантовых технологий формирует беспрецедентные вызовы для безопасности КИИ, на основе которой функционируют ключевые отрасли. Криптографические алгоритмы RSA и ECC, которые на протяжении десятилетий служили опорой защиты данных, становятся уязвимыми перед вычислительными возможностями квантовых компьютеров. Атаки, основанные на таких технологиях, представляют угрозу не только конфиденциальности информации, но и ее целостности и доступности, ставя под удар устойчивость важнейших систем. Эффективное противодействие этим угрозам требует не только тактических решений, но и стратегического переосмысления подходов к защите КИИ. Переход на алгоритмы постквантовой криптографии, отличающиеся устойчивостью к квантовым атакам, становится одним из ключевых направлений. Однако их внедрение сопряжено с рядом серьезных вызовов: технологическими ограничениями, высокими финансовыми издержками и необходимостью пересмотра существующей нормативной базы. Вместе с тем использование гибридных методов, сочетающих традиционные и постквантовые подходы, позволяет минимизировать риски и обеспечить постепенный переход к обновленным стандартам кибербезопасности, что критически важно в условиях динамично развивающейся квантовой угрозы. Для надежного противодействия угрозам, связанным с квантовыми технологиями, необходимо скоординированное взаимодействие на уровнях организаций, государств и международных структур. Важнейшими шагами на этом пути являются внедрение стандартов постквантовой криптографии, повышение квалификации специалистов, всесторонний аудит текущих систем и тестирование новых решений. Только целостный и комплексный подход способен эффективно снизить риски, связанные с развитием квантовых вычислений, и обеспечить длительную защиту критической информационной инфраструктуры. Проведенное исследование подтверждает, что интеграция квантово-устойчивых технологий должна стать ключевым элементом стратегий кибербезопасности. Промедление с адаптацией к новым угрозам может привести к уязвимости значительной части цифровой инфраструктуры, что в свою очередь, может повлечь серьезные последствия как для отдельных организаций, так и для общества в целом.

Финансирование

Работа выполнена без привлечения внешних источников финансирования.

Конфликт интересов

Конфликт интересов отсутствует.

Список литературы

1. *Зудинов А.С.* Защита информации на объектах критической информационной инфраструктуры // StudNet, 2021. Т. 4. № 6. DOI: 10.24411/2658-4964-2021-10354.

2. *Гаврилов С.В., Клабукова И.С.* Квантовые компьютеры. Операционные системы для квантовых компьютеров // Материалы Международной научно-методической конференции « Интеграция науки и образования в вузах нефтегазового профиля, 2022. Передовые технологии и современные тенденции». Салават: УНПЦ «Издательство УГНТУ», 2022. С. 443 – 445.

3. *Ulyanov S.V., Ulyanov V.S.* Fast quantum search algorithm modelling on conventional computers: Information analysis of the halting problem // Software & Systems, 2023. № 3. P. 361 – 377. DOI: 10.15827/0236-235X.143.361-377.

4. *Бирюков А.А., Шлеенков М.А.* Моделирование процессов в элементах квантового компьютера на основе методов квантовой теории с целью совершенствования их эффективности / // Сборник трудов по материалам X Международной конференции и молодежной школы «Информационные технологии и нанотехнологии» (ИТНТ-2024). Самара: СНИУ им. академика С.П. Королева, 2024. Т. 1. С. 10462.

5. *Begmyradov M., Shohradova J.* The impact of quantum computers on cryptography: the Future of encryption technologies // EO IPSO, 2024. № 11. P. 46 – 48.

6. *La Cour B.* Advances in Quantum Computing // Entropy, 2023, V. 25(12), 1633. DOI: 10.3390/e25121633.

7. *Li Y., Bi R., Jiang N., Li F., Wang M., Jing X.* Methods and Challenges of Cryptography-Based Privacy-Protection Algorithms for Vehicular Networks // Electronics, 2024, V. 13, 2372. DOI: 10.3390/electronics13122372.

8. *Singh A., Sharma V.S., Basheer S., Chowdhary C.L.* A Deep Cryptographic Framework for Securing the Healthcare Network from Penetration // Sensors, 2024. V. 24. № 21, 7089. DOI: 10.3390/s24217089.

9. *Li S., Chen Y., Chen L., Liao J., Kuang C., Li K., Liang W., Xiong N.* Post-Quantum Security: Opportunities and Challenges // Sensors, 2023. V. 23. № 21. 8744. DOI: 10.3390/s23218744.

10. *Ning Y.-D., Chen Y.-H., Shih C.-S., Chu S.-I.* Lookup Table-Based Design of Scalar Multiplication for Elliptic Curve Cryptography // Cryptography. 2024. V.8(1), 11. DOI: 10.3390/cryptography8010011.

11. *Sebé F., Simón S.* E-Coin-Based Priced Oblivious Transfer with a Fast Item Retrieval // *Cryptography,* 2024, V.8 (1). 10. DOI: 10.3390/cryptography8010010.

12. *Raheman F.* The Future of Cybersecurity in the Age of Quantum Computers // Future Internet , 2022 V. 14 (11). 335. DOI: 10.3390/fi14110335.

13. *Tsantikidou K., Sklavos N.* Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures // *Cryptography,* 2024, V.8(1). 7. DOI: 10.3390/cryptography8010007.

14. *Wang Y., Li L., Zhou Y., Zhang H.* A Comprehensive Review of MI-HFE and IPHFE Cryptosystems: Advances in Internal Perturbations for Post-Quantum Security // Axioms, 2024 V.13, 741. DOI: 10.3390/axioms13110741.

15. *Li S., Chen Y., Chen L., Liao J., Kuang C., Li K., Liang W., Xiong N.* Post-Quantum Security: Opportunities and Challenges // *Sensors* 2023. V. 23, 8744. DOI:10.3390/s23218744.

16. *Токан К. О.* Квантовый компьютер как угроза информационной безопасности / К.О. Токан, В. И. Соловьев // Материалы национальной научно-практической конференции «Цифровые системы и модели: теория и практика проектирования, разработки и применения». Казань: КГЭУ, 2024. С. 1376 – 1380.

17. *Черепнев М. А., Грачева С.С.* Угрозы, связанные с применением квантовых эффектов в криптографии // Информационные технологии, 2024. Т. 30. № 8. С. 417–424. DOI: 10.17587/it.30.417 – 424.

18. *Петренко А.С., Петренко С.А., Ожиганова М.И.* Модель угроз безопасности по аналитике зарубежных национальных квантовых программ // Защита информации. Инсайд, 2021. № 4(100). С. 50 – 59.

19. *Гаврилова М.А., Козулина А.А., Новикова А.А.* Квантовый компьютер: человеческое благо или угроза всему миру? // Моя профессиональная карьера, 2021. Т. 1, № 25. С. 31 – 38.

20. *Петренко А.С., Петренко С.А., Костюков А.Д., Ожиганова М.И.* Модель квантовых угроз безопасности для современных блокчейн-платформ // Защита информации. Инсайд, 2022. № 3(105). С. 10 – 20.

21. *Ступин Д.Д., Петренко А.С., Петренко С.А.* Развитие технологий квантовых вычислений и связанные с ним угрозы для критической информационной инфраструктуры Российской Федерации // Материалы XVI Всероссийской мультиконференции по проблемам управления (МКПУ-2023). Волгоград: ВГТУ, 2023. Т. 2. С. 168 – 172.

22. *Овчинский В.С.* Об угрозах квантовых компьютерных вычислений // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции: Сборник материалов I Всероссийской научно-практической конференции. Москва: ФГКОУ ВО «Университет прокуратуры Российской Федерации», 2021. С. 54 – 60.

23. *Диамонд Д.М.* Насколько серьезна угроза квантовых вычислений для национальной криптовалюты Венесуэлы // Информационная безопасность в банковско-финансовой сфере. Москва: ООО «Издательство «КноРус», 2020. С. 61 – 67.

24. *Петренко А.С., Петренко. С.А.* Оценка квантовой угрозы для современных блокчейн-систем // Сборник трудов VII Международной научно-практической конференции. «Информационные системы и технологии в моделировании и управлении». Ялта, 24 – 25 мая 2023 г. Симферополь: ООО «Издательство Типография «Ариал», 2023. С. 171 – 173.

Vestnik Natsional'nogo Issledovatel'skogo Yadernogo Universiteta «MIFI», 2025, vol. 14, no. 3, pp. 240–248

Quantum cyber threats and their impact on the security of critical information infrastructure

I. A. Vasilenko ✉

Sirius University, Sirius Federal Territory, 354349, Russia
✉ iravas988@yandex.ru

Received April 09, 2025; revised June 03, 2025; accepted June 03, 2025

The use of quantum technologies in the modern world poses significant challenges to the security of critical information infrastructure, which underpins key sectors such as healthcare, energy, transportation, and communications. Cryptographic algorithms like RSA and ECC, long considered reliable, have lost their resilience in the face of quantum computing capabilities, making the search for modern solutions to ensure data protection a top priority. The main risks posed by quantum computers include the potential compromise of encryption algorithms, disruption of data integrity, and destabilization of critical system operations. The methodological foundation of this study is based on the analysis of 318 sources from international databases such as Scopus, Web of Science, and others. From this body of literature, 24 publications most relevant to the topic were selected. A comparative method was employed to analyze classical and quantum threats. The aim of the study is to examine the impact of quantum attacks on the security of critical information infrastructure (CII) at the current level and propose pathways for transitioning to quantum-resilient solutions. The results emphasize the necessity of implementing innovative cryptographic approaches, such as lattice-based and code-based algorithms, as well as combined (hybrid) technologies. Successful protection of the infrastructure requires a systematic approach, including a comprehensive audit of existing systems, training of specialists, and the removal of technical and regulatory barriers. The developed step-by-step plan minimizes risks and establishes a foundation for the secure implementation of new standards.

Keywords: quantum cyber threats, critical information infrastructure, information protection, internet, potential attacks.

Referenses

1. *Zudinov A.S.* Zashchita informatsii na ob»yektakh kriticheskoj informatsionnoj infrastruktury [Information security at critical information infrastructure facilities]. StudNet, 2021. Vol. 4. No. 6. DOI: 10.24411/2658-4964-2021-10354 (in Russian).

2. *Gavrilov S.V., Klaubukova I.S.* Kvantovye komp'yutery. Operatsionnye sistemy dlya kvantovykh komp'yuterov [Quantum computers. Operating systems for quantum computers]. Materialy Mezhdunarodnoj nauchno-metodicheskoj konferentsii « Integratsiya nauki i obrazovaniya v vuzakh neftegazovogo profilya, 2022. Peredovye tekhnologii i sovremennye tendentsii» [Proceedings of the International Scientific and Methodological Conference « Integration of Science and Education in Universities with Oil and Gas Profile, 2022. Advanced Technologies and Modern Trends»]. Salavat, UNPTS «Izdatel'stvo UGNPTU» Publ., 2022. Pp. 443–445 (in Russian).

3. *Ulyanov S.V., Ulyanov V.S.* Fast quantum search algorithm modelling on conventional computers: Information analysis of the halting problem. Software & Systems, 2023. No. 3. Pp. 361–377. DOI: 10.15827/0236-235X.143.361-377.

4. *Biryukov A.A., Shleenkov M.A.* Modelirovanie protsessov v elementakh kvantovogo komp'yutera na osnove metodov kvantovoj teorii s tsel'yu sovershenstvovaniya ikh effektivnosti [Modeling of processes in quantum computer elements based on quantum theory methods for improving efficiency]. Cbornik trudov po materialam X Mezhdunarodnoj konferencii i molodezhnoj shkoly «Informacionnye tekhnologii i nanotekhnologii» (ITNT-2024). [Collection of papers based on the materials of the X International Conference and Youth School «Information technologies and nanotechnologies (ITNT-2024)»]. Samara, SNRU Publ., 2024. Vol. 6. Pp. 10462 (in Russian).

5. *Begmyradov M., Shohradova J.* The impact of quantum computers on cryptography: the future of encryption technologies. EO IPSO, 2024. No. 11. Pp. 46–48.

6. *La Cour B.* Advances in quantum computing. Entropy, 2023. Vol. 25(12), art. 1633. DOI: 10.3390/e25121633.

7. *Li Y., Bi R., Jiang N., Li F., Wang M., Jing X.* Methods and challenges of cryptography-based privacy-protection algorithms for vehicular networks. Electronics, 2024, vol.13, art. 2372. DOI: 10.3390/electronics13122372.

8. *Singh A., Sharma V.S., Basheer S., Chowdhary C.L.* A deep cryptographic framework for securing the healthcare network from penetration. Sensors, 2024. Vol. 24. No. 21, art. 7089. DOI: 10.3390/s24217089.

9. *Li S., Chen Y., Chen L., Liao J., Kuang C., Li K., Liang W., Xiong N.* Post-quantum security: Opportunities and challenges. Sensors, 2023. Vol. 23. No. 21, art. 8744. DOI: 10.3390/s23218744.

10. *Ning Y.-D., Chen Y.-H., Shih C.-S., Chu S.-I.* Lookup table-based design of scalar multiplication for elliptic curve cryptography. Cryptography, 2024. Vol. 8. art. 11. DOI: 10.3390/cryptography8010011.

11. *Sebé F., Simón S.* E-coin-based priced oblivious transfer with a fast item retrieval. Cryptography, 2024. Vol. 8, art. 10. DOI: 10.3390/cryptography8010010.

12. *Raheman F.* The future of cybersecurity in the age of quantum computers. Future Internet, 2022. Vol. 14, art. 335. DOI: 10.3390/fi14110335.

13. *Tsantikidou K., Sklavos N.* Threats, attacks, and cryptography frameworks of cybersecurity in critical infrastructures. Cryptography, 2024. Vol. 8 (1), art.7. DOI: 10.3390/cryptography8010007.

14. *Wang Y., Li L., Zhou Y., Zhang H.* A comprehensive review of MI-HFE and IPHFE cryptosystems: Advances in internal perturbations for post-quantum security. Axioms, 2024. Vol. 13, art. 741. DOI: 10.3390/axioms13110741.

15. *Li S., Chen Y., Chen L., Liao J., Kuang C., Li K., Liang W., Xiong N.* Post-quantum security: Opportunities and challenges. Sensors, 2023. Vol. 23, art. 8744. DOI: 10.3390/s23218744.

16. *Tokan K.O., Soloviev V.I.* Kvantovyj komp'yuter kak ugroza informatsionnoj bezopasnosti [Quantum computer as a threat to information security]. Materialy nacional'noj nauchno-prakticheskoj konferencii «Cifrovye sistemy i modeli: teoriya i praktika proektirovaniya, razrabotki i primeneniya». [Proceedings of the national scientific and practical conference «Digital systems and models: theory and practice of design, development and application»]. Kazan, KSPEU Publ., 2024. Pp. 1376–1380 (in Russian).

17. *Cherepnev M.A., Gracheva S.S.* Ugrozy, svyazannye s primeneniem kvantovykh effektov v kriptografii [Threats associated with quantum effects in cryptography]. Informatsionnye tekhnologii, 2024. Vol. 30. No. 8, Pp. 417–424. DOI: 10.17587/it.30.417-424 (in Russian).

18. *Petrenko A.S., Petrenko S.A., Ozhiganova M.I.* Model' ugroz bezopasnosti po analitike zarubezhnykh natsional'nykh kvantovykh programm [Threat model analysis based on foreign national quantum programs]. Zashchita informatsii. Insaĭd, 2021. No. 4(100). Pp. 50–59 (in Russian).

19. *Gavrilova M.A., Kozulina A.A., Novikova A.A.* Kvantovyj komp'yuter: chelovecheskoe blago ili ugroza vsemu miru? [Quantum computer: human benefit or threat to the world?]. Moya professional'naya kar'era, 2021. Vol. 1. No. 25. Pp. 31 – 38 (in Russian).

20. *Petrenko A.S., Petrenko S.A., Kostyukov A.D., Ozhiganova M.I.* Model' kvantovykh ugroz bezopasnosti dlya sovremennykh blokcheĭn-platform [Quantum threat model for modern blockchain platforms]. Zashchita informatsii. Insaĭd, 2022. No. 3(105). Pp. 10 – 20 (in Russian).

21. *Stupin D.D., Petrenko A.S., Petrenko S.A.* Razvitie tekhnologij kvantovykh vychislenij i svyazannye s nim ugrozy dlya kriticheskoj informatsionnoj infrastruktury Rossiĭskoĭ Federatsii [Quantum computing technologies development and threats to Russian critical information infrastructure]. XVI Vserossiyskaya multikonferentsiya po problemam upravleniya (MKPU-2023). [Proceedings of the XVI All-Russian Multi-Conference on Management Problems (MKPU-2023)]. Volgograd, VSTU Publ., 2023. Vol. 2. Pp. 168 – 172 (in Russian).

22. *Ovchinskiy V.S.* Ob ugrozhakh kvantovykh komp'yuternykh vychislenij [On the threats of quantum computing]. Materials of 1st All-Russian Scientific-Practical Conf. «Tsifrovye tekhnologii v bor'be s prestupnost'yu: problemy, sostoyanie, tendentsii». [Collection of materials of the I All-Russian scientific and practical conference «Digital technologies in the fight against crime: problems, status, trends»]. Moscow, FGKOU VO «Universitet prokuratury Rossijskoj Federacii» Publ., 2021. Pp. 54 – 60 (in Russian).

23. *Diamond D.M.* Naskol'ko ser'yozna ugroza kvantovykh vychislenij dlya natsional'noj kriptovalyuty Venesuely [How serious is the quantum threat to Venezuela's national cryptocurrency]. Informatsionnaya bezopasnost' v bankovsko-finansovoy sfere. [Information security in the banking and financial sector]. Moscow, Knorus Publ., 2020. Pp. 61 – 67 (in Russian).

24. *Petrenko A.S., Petrenko S.A.* Otsenka kvantovoj ugrozy dlya sovremennykh blokcheĭn-sistem [Quantum threat assessment for modern blockchain systems]. Informatsionnye sistemy i tekhnologii v modelirovanii i upravlenii: Proc. of the 7th Int. Scientific-Practical Conf., Yalta, May 24–25, 2023. [Proceedings of the VII International Scientific and Practical Conference «Information Systems and Technologies in Modeling and Management». Yalta, May 24 – 25, 2023]. Simferopol, Arial Publ., 2023. Pp. 171 – 173 (in Russian).