УДК 004.424
DOI 10.17513/snt.39855

ОСНОВНЫЕ ТЕНДЕНЦИИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ, СВЯЗАННЫЕ С КВАНТОВЫМ ПОВОРОТОМ

[1]Великанов В.В., [2]Ермолаев А.С.

[1]ФГБОУ ВО «Волгоградский государственный технический университет», Волгоград, e-mail: helen901@mail.ru;
[2]ООО «Интернет-агентство ИНТЕРВОЛГА», Волгоград, e-mail: alexey.0994@mail.ru

Данная статья посвящена рассмотрению проблемы квантового поворота и его влияния на тенденции в области кибербезопасности. Стремительный прогресс в области создания и использования квантовых компьютеров и квантовых вычислений, названный квантовым поворотом, а также быстроразвивающаяся квантовая криптография создают значительные угрозы в области кибербезопасности. Среди основных тенденций, создающих угрозы, необходимо отметить усиливающуюся американо-китайскую гонку за лидерство на рынке квантовых компьютеров и квантовых вычислений, которая увеличивает уровень неопределенности и рисков на рынке квантовых технологий. Также стоит отметить кратный рост успешных попыток проникновения в сети предприятий через домашние сети сотрудников, что связано, прежде всего, с ростом количества работников компаний, занятых удаленно, и значительным прогрессом в области совершенствования инструментов проникновения, используемых киберпреступниками. Третьей значимой тенденцией в области кибербезопасности станет рост опасности интернета вещей. В условиях квантового поворота возникают значительные угрозы безопасности пользователей так называемых умных вещей. С нашей точки зрения, основной проблемой интернета вещей (IoT) является отсутствие единых стандартов безопасности. В условиях квантового поворота IoT представляет собой значительные риски в области кибербезопасности, для предотвращения которых требуются совместные усилия производителей и пользователей по разработке единого стандарта безопасности.

Ключевые слова: квантовый поворот, кибербезопасность, методы квантовой криптографии, квантовый компьютер, интернет вещей

KEY CYBER SECURITY TRENDS RELATED TO THE QUANTUM EXCHANGE

[1]Velikanov V.V., [2]Ermolaev A.S.

[1]Volgograd State Technical University, Volgograd, e-mail: helen901@mail.ru;
[2]INTERVOLGA Internet Agency LLC, Volgograd, e-mail: alexey.0994@mail.ru

This article examines the problem of the quantum turn and its impact on trends in cybersecurity. Rapid advances in the creation and use of quantum computers and quantum computing, called the «Quantum exchange» as well as rapidly evolving quantum cryptography, pose significant cybersecurity threats. Among the main trends creating threats, it is necessary to note the intensifying US-China race for leadership in the market of quantum computers and quantum computing, which increases the level of uncertainty and risks in the market of quantum technologies. It is also worth noting the multiple increase in successful attempts to penetrate enterprise networks through the home networks of employees, which is primarily due to the increase in the number of company employees working remotely and significant progress in improving the penetration tools used by cybercriminals. The third significant trend in cybersecurity will be the growing threat of the Internet of Things. In the context of the quantum turn, significant threats to the security of users, the so-called «smart things», arise. From our point of view, the main problem of IoT is the lack of uniform security standards. In the context of the quantum turn, the Internet of Things (IoT) poses significant cybersecurity risks that require a collaborative effort between manufacturers and users to develop a common security standard.

Keywords: quantum turn, cybersecurity, quantum computer, quantum cryptography methods, Internet of things

Вместе с развитием квантовых информационных технологий и цифровой экономики происходит бурный рост рисков проведения кибератак и похищения конфиденциальных данных. Возникновение квантовых вычислений поставило новую задачу для служб, занимающихся кибербезопасностью. Эта технология и открывающиеся перед ней возможности могут значительно изменить подходы к криптографии и способам защиты данных.

На сегодняшний день происходят значимые изменения, получившие название «квантовый поворот», что вызвано потребностью во внедрении максимально проверенных технологий, обусловленном растущей угрозой со стороны квантовых компьютеров. Квантовые компьютеры способны с легкостью преодолеть устаревшие механизмы защиты информации. Именно поэтому многие компании начали пересмотр имеющихся систем безопасности и изучение новых. Это обусловлено внедрением квантовых ключей, гомоморфного шифрования и многосторонних вычислений. Кроме того, высокий уровень важности

на данный момент времени имеет обеспечение совместимости старых систем с новыми. Другую важную роль, кроме создания инновационных подходов к обеспечению безопасности, имеет обучение сотрудников новым методам защиты. Хотя этот процесс может быть трудным и затратным, он необходим для защиты данных и поддержания пользовательского доверия в условиях постоянно развивающихся угроз.

Цель исследования: создать структурированное представление об основных тенденциях в области кибербезопасности, связанных с так называемым квантовым поворотом, вызванным прогрессом в области квантовых компьютеров и квантовой криптографии.

Материалы и методы исследования

В работе использованы следующие методы исследования: теоретические (анализ научных источников по проблеме исследования, анализ результатов работы специалистов по кибербезопасности и преподавателей профильных дисциплин Волгоградского государственного технического университета) и эмпирические (наблюдение, беседа, метод экспертной оценки). Базой исследования выступил курс по информационной безопасности Центра защиты информации Волгоградского государственного технического университета.

Результаты исследования и их обсуждение

Внедрение квантовых информационных технологий изменит область информационной безопасности благодаря применению принципов квантовой механики. Используемые сегодня протоколы криптографии, такие как RSA и ECC, основаны на больших и сложных математических моделях, с трудом поддающихся расшифровке стандартными компьютерами. На данный момент защита более 95% всей информации в сети Интернет обеспечивается протоколом RSA, однако еще в 2022 году китайские исследователи опубликовали работу «Факторизация целых чисел с сублинейными ресурсами на сверхпроводящем квантовом процессоре» [1], в которой заявили, что разработали устойчиво работающий метод взлома алгоритма RSA с помощью квантовых вычислений. Таким образом, появление и внедрение в массовое использование квантовых компьютеров представляют серьезную угрозу, поскольку, обладая значительно большей вычислительной мощностью, они могут выполнять такие сложные операции, как, например, расчет дискретных логарифмов, гораздо быстрее, чем обычные компьютеры. Ответом на новые угрозы кибербезопасности может стать квантовая криптография. В частности, ответом на рост возможностей по взлому и проникновению может явиться алгоритм Шнорра, который сложно реализовать на современных классических компьютерах, но возможно на базе квантовых вычислительных систем. Возможно, что в ближайшее время возникнут смешанные, квантово-классические вычислительные системы, которые станут основой перехода к чистым квантовым системам криптографии.

Квантовая криптография – это быстро развивающаяся область, которая решает проблемы, возникающие в связи с развитием квантовых вычислений. Ее цель – обеспечить безопасную связь в условиях, когда злоумышленники могут использовать квантовые компьютеры для взлома существующих систем шифрования. Квантовая криптография построена на фундаментальном принципе использования уникальных физических свойств квантовых частиц для обеспечения информационной безопасности. Важнейшим аспектом этой области является использование квантовых ключей для шифрования данных. Процесс шифрования происходит следующим образом.

Для организации защищенной связи используется квантовый ключ. Отправитель генерирует квантовые биты (кубиты) и отправляет их получателю по квантовому каналу. Важно понимать, что любая попытка перехвата кубитов приведет к их изменению, которое отправитель может обнаружить. Получатель внимательно изучает кубиты и своевременно обнаруживает попытки вторжения или перехвата канала связи. В случае обнаружения аномалий отправитель и получатель немедленно выбрасывают ключи шифрования и получают уведомление о попытке атаки. После того как система обнаружит отсутствие атак, отправитель и получатель могут использовать сгенерированные квантовые ключи для безопасного шифрования и дешифрования данных.

Можно выделить ряд проблем и вызовов, связанных с квантовой криптографией.

1. Быстрый рост числа и мощности квантовых компьютеров может способствовать тому, что существующие методы квантовой криптографии устареют, что приведет к необходимости постоянного обновления систем квантовой безопасности.

2. Интеграция квантовых технологий в существующую информационную инфраструктуру сопряжена с определенными трудностями, особенно в части операционной совместимости и переходных решений.

Характерной чертой развития квантовой криптографии стала американо-китайская гонка за лидерство на рынке квантовых компьютеров и квантовых вычислений.

США и Китай ведут серьезную технологическую борьбу на мировой арене, в частности в области квантовых вычислений. Квантовые компьютеры способны произвести революцию в обработке информации, создав устойчивый тренд развития отрасли на следующие 50–75 лет, что делает это соревнование крайне важным для обеих стран, стремящихся к лидерству в данной области. Как США, так и Китай занимают лидирующие места в исследованиях квантовых технологий. В США такие компании, как IBM, Google и Microsoft, занимают лидирующие позиции в этой области, а согласно недавно принятым законам будут выделены значительные средства на дальнейшие разработки. Китай также активно инвестирует в квантовые вычисления, примером чему может служить запуск спутника Micius в 2018 году. Этот спутник продемонстрировал потенциал квантовых технологий, успешно передав квантовые состояния на большие расстояния. Квантовые вычисления обладают огромным потенциалом для различных областей, однако они также представляют значительную угрозу для криптографических систем, делая данные уязвимыми для взлома.

Специалисты из Hudson Quantum Alliance Initiative утверждают, что китайские специалисты сосредоточили свои усилия на двух базовых направлениях: создание собственных, независимых квантовых технологий, способных взламывать как симметричные, так и асимметрические системы шифрования, а также создание национальной системы безопасности, способной противостоять взлому и проникновению сил, использующих современные квантовые технологии, прежде всего США и их союзников.

Одновременно с этим Китай пытается догнать США в области создания квантово-фотонных схем передачи информации, используемых в сенсорных и вычислительных квантовых технологиях, шифровании и дешифровании данных. Отметим также, что китайское правительство объявило исследования в области квантовых технологий национальным приоритетом и способно национализировать любые новые технологии, алгоритмы или полученные данные. На данный момент самым мощным китайским квантовым компьютером является JiuZhang 3, который способен использовать 225 фотонов в качестве физического средства для выполнения расчетов [2].

В свою очередь, правительство США приняло закон о кибербезопасности квантовых вычислений, в котором прямо указано на необходимость активизировать разработку средств обеспечения безопасности так называемой постквантовой криптографии. Его главная задача – заставить сотрудничать частный и государственный сектора экономики для создания так называемых квантово готовых, а потом и квантово безопасных технологий шифрования и передачи данных. На Западе ключевым игроком рынка квантовой криптографии является американский Национальный институт стандартов и технологий (National Institute of Standards and Technology, NIST), в задачи которого входят отбор, проверка и тестирование новых стандартов шифрования. После длительного тестирования степени их уязвимости для квантовой дешифровки и взлома отобранные алгоритмы в будущем станут новыми стандартами безопасности.

Интенсивность общемировой квантовой гонки можно оценить по количеству патентов, полученных университетами и исследовательскими лабораториями этих стран в области квантовых вычислений. В США в течение 2020–2022 годов получено 1184 патентные заявки, в Китае – 684, в России – 21. Общее количество полученных патентных заявок неуклонно растет, отражая общую тенденцию роста инвестиций в сферу квантовых вычислений [3].

Одним из важных, но не очевидных последствий создания гибридных квантово-классических технологий станет рост проникновения в сети предприятий через домашние сети сотрудников.

Глобальная статистика показывает, что более 40% IT-специалистов работают удаленно, преимущественно дома, и это число будет расти. Так, по данным анализа активности киберпреступников, рост количества успешных кибератак на домашние сети сотрудников компаний в 2022–2023 годах составил более 300% [4].

Киберпреступники рассматривают проникновение в сети сотрудников, работающих удаленно, как легкий способ проникновения в корпоративные сети, поскольку традиционно вопросам поведения и защиты сотрудников предприятий в домашних и личных социальных сетях внимания уделяется гораздо меньше. Характерными особенностями здесь, как правило, являются «слабые» пароли, минимальные или вообще отсутствующие меры безопасности, низкие навыки обеспечения сетевой безопасности самих сотрудников компании.

В условиях «квантового поворота» и роста возможностей киберпреступников пред-

приятиям и их службам кибербезопасности придется значительно увеличить инвестиции для защиты своих сетей. Среди первоочередных мер, прежде всего, необходимо указать следующие.

1. Обязательное обучение всех сотрудников, работающих удаленно, правилам кибербезопасности.

2. Разработка новых инструментов, основанных на принципах квантового шифрования, для обеспечения безопасности домашних сетей сотрудников, включая новое антивирусное ПО и обеспечение регулярного обновления программ в автоматическом режиме, с минимальным участием сотрудников компании, работающих удаленно.

3. Постоянный мониторинг активности сотрудников, работающих удаленно, в корпоративной сети, выявление необычной активности и ее отслеживание и анализ.

4. Обеспечение регулярного обновления ПО на устройствах сотрудников, работающих удаленно.

Отметим, что наиболее перспективным способом решения проблемы проникновения в домашние сети сотрудников является корпоративное VPN-соединение, которое расширит корпоративную сеть компании, включив в нее домашние сети сотрудников. Такая схема позволит создать защищенное соединение между домашним компьютером и корпоративным сервером, направив весь сетевой трафик в корпоративную сеть, повысив тем самым его защищенность и обеспечив высокий уровень контроля. Одновременно с этим пользователям придется установить корпоративное ПО, необходимое для управления мобильными устройствами, поскольку оно позволяет широко применять правила корпоративной политики безопасности, проводить удаленную телеметрию интернет-трафика, отслеживать попытки несанкционированного доступа к сети. Вторым, но не менее важным последствием «квантового поворота» станет рост опасности интернета вещей с точки зрения кибербезопасности.

Технология интернета вещей (IoT) является одной из новых, ключевых технологий, которая позволяет «умным» устройствам обмениваться данными в режиме реального времени и эффективно выполнять задачи, поставленные пользователями. По статистике, в 2022 году 79% IT-фирм использовали технологии IoT, более 65% международных компаний используют или планируют использовать технологии IoT. В 2022 году к системе интернета вещей было подключено более 42 млрд устройств, однако в мире до сих пор не существует признанной безопасной экосистемы IoT [5].

При этом в условиях квантового поворота угрозы безопасности пользователей будут только расти. С нашей точки зрения, основной проблемой IoT является отсутствие единых стандартов безопасности и нежелание фирм – продавцов «умной» электроники обеспечивать послепродажную защиту устройств. Кроме того, спецификой рынка IoT является то, что по мере роста интернета вещей создаются новые точки доступа для киберпреступников. По данным статистики компании HP, более 70% устройств класса IoT не шифруют свой трафик, 30% устройств не позволяют изменить фабричный пароль, установленный по умолчанию, веб-интерфейс 60% устройств признан экспертами компании небезопасным, 90% устройств собирают информацию о пользователе без его разрешения [6].

Многие «умные» устройства недостаточно защищены или вообще не защищены, производители не уделяют приоритетного внимания защите от проникновения и перехвата контроля. Кроме того, программное обеспечение многих из этих устройств не обновляется регулярно или не обновляется вообще, что еще больше повышает их уязвимость.

Наиболее известный инцидент в области интернета вещей произошел 3 марта 2022 года, когда стало известно, что неисправленная DNS-уязвимость подвергла опасности миллионы умных устройств. Использование ошибки позволило провести атаки типа «человек посередине» (MITM) и повреждать кэш DNS, эффективно перенаправляя интернет-трафик на подконтрольный злоумышленникам сервер.

IoT-устройства подвержены различным атакам, основными из которых являются атаки, основанные на переборе паролей. Еще одной распространенной формой атак является распределенный отказ в обслуживании (DDoS), когда скомпрометированные IoT-устройства «зомбируются», а в дальнейшем используются для перегрузки и вывода из строя целевых сайтов или корпоративных сетей.

Кроме того, IoT-устройства могут стать мишенью для киберворов, которые стремятся похитить личную информацию пользователей; существуют значительные опасения по поводу недостаточных мер безопасности данных, передаваемых через носимые IoT-устройства, прежде всего устройства электронного банкинга. Отметим, что наибольший потенциал защиты тут имеет использование биометрических данных, что позволяет получить два преимущества – не позволить подобрать код доступа к устройству и ускорить обработку запро-

сов клиентов. Однако, как уже говорилось выше, современные, гибридные технологии позволяют обойти и биометрическую защиту устройства.

В условиях «квантового поворота» интернет вещей представляет собой значительный риск кибербезопасности, для предотвращения которого требуются совместные усилия производителей и пользователей по разработке единого стандарта безопасности. Это предполагает, прежде всего, внедрение надежных мер безопасности и разработку безопасной экосреды IoT-устройств, регулируемой государством. В России нормативно-правовое регулирование интернета вещей находится на начальном этапе развития. В федеральных законах интернет вещей не определен. Интернет вещей подчиняется общим нормам согласно Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федеральному закону от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», если то предприятие, где он используется, относится к КИИ.

Заключение

Квантовые вычисления – это новый, революционный подход к обработке информации, использующий принципы квантовой механики. Хотя квантовые компьютеры обладают огромным потенциалом с точки зрения вычислительной мощности, они также представляют собой значимую, серьезную проблему для существующих методов шифрования данных и мер кибербезопасности. Среди наиболее очевидных угроз, задающих новые тренды на рынке кибербезопасности, авторы отмечают рост проникновения в сети предприятий через домашние сети сотрудников и рост опасности интернета вещей с точки зрения кибербезопасности. Главным же фактором, определяющим будущее отрасли квантовых вычислений, станет американо-китайская гонка за лидерство на рынке квантовых компьютеров и квантовых вычислений.

Список литературы

1. Жмудь В.А., Ляпидевский А.В. Обзор активно финансируемых исследований зарубежной фотоники и электроники // Автоматика и программная инженерия. 2023. № 1 (43). С. 44-129.

2. Букашкин С.А., Черепнев М.А. Квантовые устройства в криптографии // International Journal of Open Information Technologies. 2023. № 1. С. 104-108.

3. Выходец Р.П. Стратегия Китая в области искусственного интеллекта // Евразийская интеграция: экономика, право, политика. 2022. № 2 (40). С. 140-147.

4. Назарова А.Д., Шведов В.В. Вызовы и решения в области кибербезопасности в эпоху цифровой трансформации // Столыпинский вестник. 2023. № 5. С. 2212-2220.

5. Накиев Р.Р., Ульянов В.В. Анализ уязвимостей интернет вещей (iot) и способы их предотвращения // Вестник науки. 2023. № 7 (64). С. 250-263.

6. Леонтьев С.М. Кибербезопасность в эпоху распределенных систем: защита данных и информации в условиях облачных технологий и интернета вещей // Вестник магистратуры. 2023. № 8 (143). С. 60-61.