НА ПОРОГЕ ГЛОБАЛЬНОГО ТЕХНОЛОГИЧЕСКОГО ПЕРЕХОДА. ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

А.В. Лукашев, *кандидат военных наук, старший научный сотрудник НИЦ*
В.С. Сарафанников, *старший научный сотрудник НИЦ*
Военная академия связи им. Маршала Советского Союза С.М. Будённого (Россия, г. Санкт-Петербург)

DOI:10.24412/2500-1000-2023-5-4-129-134

Аннотация. *В статье рассмотрены проблемы перехода страны на новый технологический уровень в свете появления квантовых компьютеров и угроз существующим системам криптографии. Исследованы некоторые подходы к решению проблем обеспечения информационной безопасности и преодоления отставания от лидеров мировой гонки внедрения квантовых технологий в различные сферы, в том числе, в системы связи специального назначения*

Ключевые слова: *квантовые технологии, квантовые коммуникации, квантовое распределение ключей, постквантовые алгоритмы криптографии.*

Объявление о начале глобальной технологической революции официально прозвучало по итогам учреждения 31 января 2023 года Международного совета ассоциаций квантовой промышленности развитых стран запада [1]. В совет вошли представители четырёх ассоциаций: Quantum Industry Canada, QIC – Канада, Консорциум квантового экономического развития, QED-C – США, Quantum Strategic Industry Alliance for Revolution, Q-STAR – Япония и Европейский консорциум квантовой промышленности, QuIC – Европа. В коммюнике по итогам первого заседания совета это объединения, в частности, было заявлено: «Мы находимся в начале глобальной технологической революции».

Основное содержание этой революции, будем пока называть этот процесс переходом, состоит в широком внедрении квантовых компьютеров в различные сферы научно-технического развития, а также критически важные отрасли управления и информационного обеспечения. В статье основное внимание будет уделено вопросам безопасного информационного обмена.

Но начать всё-таки следует с квантовых вычислений. Обычный компьютер, даже если это суперкомпьютер, вычисления осуществляет на основе математического аппарата. И даже если алгоритм вычислений предусматривает параллельные вычисления, где это возможно, на решение задач может уходить значительное время. Квантовый компьютер выполняет вычисления в тысячи, а порой и в миллионы раз быстрее. Например, в [2] сообщается, что китайским учёным удалось решить задачу распределения вероятностей прохождения фотонов через интерферометр с помощью квантового вычислителя (квантовым компьютером его пока назвать нельзя – он не приспособлен для программирования решений других задач) за 200 секунд, в то время как лучший китайский суперкомпьютер TaihuLight смог бы решить такую задачу за 2,5 млрд. лет.

В Сети можно найти множество подобных примеров, и их число постоянно растёт с всё новыми экспериментами с квантовыми компьютерами.

Другой пример, тоже китайский [3]. Исследователь Bao Yan (Бао Ян – *авт.*), вместе с 24-мя членами своего научного коллектива с помощью 10-кубитного квантового компьютера осуществил взлом криптографической системы RSA с длиной ключа 48 бит. Они также утверждают, что систему RSA-2048 с использованием разработанного ими протокола QAOA, встроенного в алгоритм К. П. Шнора, можно взломать с помощью 372-кубитного квантового компьютера.

Надо заметить, что введённый в ноябре 2022 года квантовый компьютер Osprey

компании IBM содержит 433 кубита [4]. К концу текущего года компания намерена параллельно ввести в эксплуатацию Quantum System Two, ёмкостью 1127 кубитов.

Продолжаем: отечественные исследователи из Российского квантового центра Сколково и Национального университета науки и технологий «МИСиС» в продолжение развития способов кодирования квантов осуществили успешный эксперимент по использованию кодирования кудитов [5]. Кудиты – кванты, в которых создаются не два уровня состояний, как в кубите, а более. Например, кутриты, квартиты, куквинты, имеют 3, 4 и 5 уровней соответственно. Тема использования кудитов для создания квантовых компьютеров в научном сообществе развивается давно. Авторы рассматриваемой статьи указывают более сорока предшествующих работ с обоснованием эффективности кудитов в квантовых схемах.

Для разложения вентиля Тоффоли были использованы пятиуровневые квантовые системы – куквинты, которые используют кодируемые уровни в качестве пространства двух кубитов с совместным вспомогательным состоянием. Этим самым, ёмкость 1000-кубитного квантового компьютера теоретически стало возможно заменить 88-куквинтовым квантовым компьютером. Одновременно упростилась и задача исправления ошибок за счёт использования этого вспомогательного состояния – в кубитном квантовом компьютере для этой цели вспомогательные кубиты создаются в дополнение к вычислительным.

Такое решение может существенно ускорить внедрение квантовых компьютеров, поскольку схема квантового процессора будет упрощена на порядки. Следовательно, сроки повышения рисков взлома существующих систем криптографии могут наступить ранее ожидаемых.

Таким образом, с лозунгом из выше упомянутого коммюнике [1] можно согласиться: квантовая революция действительно начинается. Это подтверждают и европейские агентства Atos и IQM [6]: «К концу 2023 года не менее 76 процентов центров обмена данными в мире будут использовать квантовые вычисления».

Выше изложенные факты служат аргументами наличия новой реальной угрозы существующим криптографическим системам с открытым ключом, создавая риски информационной безопасности систем управления в критических областях.

Существует два принципиальных подхода к решению проблемы информационной безопасности в свете угрозы со стороны квантовых компьютеров и алгоритмов.

Первый – квантовая криптография, то есть квантовое распределение ключей, которое изложено выше.

Таким способом мы решаем проблему распределения криптографических ключей при наличии у злоумышленников квантового компьютера, поскольку на сегодняшний день считается, что с помощью квантового компьютера нельзя взломать квантовую криптографию.

Преимущества: фундаментальная, основанная на физике защищённость.

Недостатки: ограничения по расстоянию в наземных оптических сетях без переприёма и скорости генерации ключей.

Второй подход – постквантовая криптография – идея создания новых асимметричных криптографических алгоритмов, построенных не на задачах разложения чисел на простые множители, а на других сложных математических задачах, при решении которых квантовый компьютер не будет иметь преимуществ. К таким решениям относят следующие:

- криптография, основанная на хеш-функциях.
- криптография, основанная на кодах исправления ошибок.
- криптография, основанная на решётках.
- криптография, основанная на многомерных квадратичных системах.
- шифрование с секретным ключом.

Постквантовая криптография сегодня достаточно хорошо развита: уже представлены коммерческие библиотеки, решения, продукты. Сейчас технология проходит стадию стандартизации: и в России, и в мире идёт процесс принятия решений, какие технологии будут стандартизированы. На горизонте 2024 года стандарты должны быть закреплены.

Преимущества технологии: простота и высокая скорость интеграции (поскольку речь идёт о программном обеспечении), регулярные обновления программ. Уже сегодня такие решения применяются, чтобы усилить защиту ценных данных широкого спектра сервисов и приложений корпоративных пользователей и физических лиц (веб, мобильные и десктопные приложения).

Основной недостаток – секретность постквантовой криптографии все ещё основывается на предположениях о сложности решения определённых классов математических задач. Всегда есть некоторая вероятность того, что появится квантовый компьютер, с помощью которого можно будет взламывать и постквантовые алгоритмы. В отличие от квантового распределения ключей здесь нет фундаментально доказуемой стойкости – такие алгоритмы продолжают изучаться на предмет устойчивости от взлома.

В настоящей статье задача анализа постквантовых алгоритмов не ставилась, поскольку сведения о них детально рассмотрены в многочисленных работах, а часть из таких алгоритмов уже принята к использованию некоторыми организациями и учреждениями.

Рассмотрим системы квантового шифрования. Основным протоколом, устойчивость к взлому которого считается доказанной, является протокол BB84 [8] и его многочисленные модернизации. В квантовых системах шифрования, как такового, нет. Основная суть сводится к получению одноразового секретного ключа с помощью квантового распределения ключей. До недавнего времени считалось, что безопасность таких ключей основана на законах квантовой механики – запрете клонирования неизвестных состояний.

Здесь вмешательство злоумышленника в квантовый канал, по которому стороны осуществляют процедуру формирования ключа, обнаруживается в результате разрушения состояний передаваемых кубитов при их измерении злоумышленником, а при превышении допустимого уровня искажений формирование ключа прекращается.

Однако попытки перехвата квантового ключа начались практически сразу после его создания. К настоящему времени известно около двадцати видов атак. И хотя виды квантовых атак описаны в учебниках вузов, а современные методы защиты от них достаточно надёжны [9], вопросы перехвата квантовых ключей находятся в плоскости технических решений. Важно отметить, что системы квантового распределения ключей представляют собой сложные программно-аппаратные комплексы. Несмотря на то, что защищённость квантово-сгенерированных ключей доказывается на основе аксиом квантовой механики, всегда остаётся опасность наличия уязвимостей при конкретной физической реализации.

Стоит отметить, что эти две технологии могут быть очень удачным образом скомбинированы. Так, высоконагруженные магистральные каналы передачи данных между, например, дата-центрами крупных компаний, каналы сетей связи специального назначения на основных, наиболее важных направлениях могут быть защищены с помощью квантовой криптографии.

Переписка или банковская транзакция на небольшие суммы, каналы сетей связи специального назначения на менее важных направлениях – с помощью постквантовой криптографии. То есть квантовую и постквантовую криптографию надо не противопоставлять, а использовать их как синергичные технологии.

С учётом того, что квантовые вычислительные системы быстро развиваются, см. приведённый пример с куквинтами, риски для постквантовых систем криптографии будут возрастать. И к этому следует готовиться уже сейчас.

На рисунке представлен вариант алгоритма организации использования рассмотренных квантовых и постквантовых систем на переходный период. По разным оценкам, такой период для разных стран может быть завершен на рубежах 2030-2035 годов (рис. 1).

Рис. 1. Обобщённый алгоритм перехода на новый технологический уровень сетей информационного обмена в критически важных отраслях

На рисунке показано: постквантовые (а с ними и существующие) алгоритмы шифрования подвергаются условному «давлению» со стороны развивающихся квантовых систем вычислений. Снизу показано, что научно-исследовательские разработки призваны повышать их стойкость к взлому. Также должны быть организованы исследования по оценке рисков взлома применительно к временно̀й шкале, для чего следует непрерывно вести мониторинг ведущихся исследований в зарубежных странах.

Квантовые системы криптографии, в частности, квантовое распределение ключей, уже создаются и внедряются в рассматриваемых нами системах коммуникаций. В таком случае, с приближением рисков к критическим отметкам, часть направлений следует переводить в область квантовой криптографии. Поэтому над блоком «Системы КРК» (квантового распределения ключей) обозначен ожидаемый прирост объёма этого блока. Разумеется, перевод каналов и сетей в квантовую сферу возможен при наличии резервов линий и каналов, пригодных по характеристикам, а также оборудования, которое должна подготовить электронная промышленность под госзаказ, который также необходимо планировать.

Подготовку кадров для эксплуатации квантовых систем следует начать с доподготовки научных сотрудников и преподавательского состава вузов, в том числе, силовых ведомств. Подготовленные научные сотрудники смогут вести компетентные научные исследования, а это невозможно без создания учебных стендов, лабораторий, полигонов, опытных районов, оборудованных программно-аппаратными комплексами симуляциями квантовых технологий, а где возможно, и реальным квантовым оборудованием.

На этих же полигонах и стендах должны учиться преподаватели, которые, в свою очередь, будут затем обучать студентов, слушателей и курсантов военных вузов.

Здесь сделаем ремарку: было бы полезным диссертационные и дипломные работы по теме квантовых коммуникаций завершать практическим экспериментом.

На рисунке обозначены ещё два блока пунктирными линиями. В зарубежных странах ведутся интенсивные поиски решений для организации квантовой связи на принципах нелокальности, например, [10]. Создание систем связи на принципах

нелокальности станет окончательной, закрывающей технологией. С её внедрением системы связи претерпят тектонические преобразования. Но об этом, как и о гибридных системах, поговорим в следующих работах.

К сказанному выше следует добавить несколько сентенций из реальной жизни. В процессе производства, монтажа и настройки оборудования возможны ошибки, неточности, технические дефекты по различным причинам. Имеет место и человеческий фактор. Разрабатываемые инструкции не могут предусмотреть всё. В результате теоретически надёжная система может оказаться уязвимой для атак. И такие риски также следует учитывать.

И ещё один тезис. Допустимо предположить, что в различных ведомствах, в том числе, силовых, разработки квантовых систем коммуникаций уже ведутся. Очень важно, чтобы такие системы сопрягались так же, как электрическая вилка с розеткой. Иными словами, стандартизация и сертификация должны быть унифицированными.

Выводы: 1. Криптостойкость существующих систем информационного обмена целесообразно усиливать уже сейчас.

2. Два рассмотренных пути и их синергичное сосуществование нуждаются в тщательном обосновании и планировании эволюционного перехода на новый технологический уровень. Такой переход неизбежен, а «своевременно» – значит «сейчас».

3. В работе не затронуты вопросы создания отечественного программного обеспечения для управления квантовыми системами. Но это критически важная отрасль, поскольку использование зарубежных программных систем означает бесполезность всех вышеперечисленных мероприятий – данные могут быть перехвачены ещё до их ввода в систему.

4. Исследования носят междисциплинарный характер, поэтому они требуют наличия специального надведомственного органа управления исследованиями, обладающего соответствующими полномочиями, в том числе, привлечения профильных (вновь подготовленных) специалистов различных организаций и учреждений, а также промышленности.

Таким образом, в статье сделана попытка систематизации проблем информационной безопасности вкупе с объективной необходимостью перехода на новый технологический уровень развития информационных систем. Возможно, статья окажется полезной для органов, принимающих решения, в том числе, осуществляющих выбор приоритетов в финансировании государственных программ развития технологий.

Библиографический список

1. International quantum industry councils formally joining forces for the development of quantum technologies, 02.02.2023. – [Электронный ресурс]. – Режим доступа: https://qt.eu/about-quantum-flagship/newsroom/international-quantum-industry-councils-formally-joining-forces-for-the-development-of-quantum-technologies/.

2. Han-Sen-Zhong et. al., Quantum computational advantage using photons, 03.12.2020. – [Электронный ресурс]. – Режим доступа: https://www.science.org/doi/10.1126/science.abe8770.

3. Bao Yan, et. al., Factoring integers with sublinear resources on a superconducting quantum processor, 23.12.2022. – [Электронный ресурс]. – Режим доступа: https://arxiv.org/pdf/2212.12372.pdf.

4. IBM launches its most powerful quantum computer with 433 qubits, 11.09.2022. – [Электронный ресурс]. – Режим доступа: https://www.reuters.com/technology/ibm-launches-its-most-powerful-quantum-computer-with-433-qubits-2022-11-09/.

5. Nikolaeva Anastasia S. et. al., Generalized Toffoli Gate Decomposition Using Ququints: Towards Realizing Grover's Algorithm with Qudits, – Entropy 2023, 25, 387, 20.02.2023. – [Электронный ресурс]. – Режим доступа: https://doi.org/10.3390/e25020387.

6. Литтке Удо, Исследование Atos и IQM, 12.10.2021. – [Электронный ресурс]. – Режим доступа: https://www.cnews.ru/news/line/2021-12-10_issledovanie_atos_-i_iqm_76_mirovyh.

7. Редакция ресурса “Habr.com”, Постквантовая криптография: основные подходы и причины использования. – [Электронный ресурс]. – Режим доступа: https://habr.com/ru/sandbox/163505/.

8. Bennett C.H., Brassard G. Quantum cryptography: public-key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, – Bangalore, India10-12 December, New York: IEEE Press, 1984. V. 560. P. 175-179.

9. Trushechkin A.S. et. al., Security of the decoy state method for quantum key distribution // Uspekhi Fizicheskikh Nauk. – 2021. – №191 (1). – P. 93-109. – DOI: https://doi.org/10.3367/UFNr.2020.11.038882.

10. Salekh S., From counterportation to local wormholes, 02.03.2023. – [Электронный ресурс]. – Режим доступа: https://iopscience.iop.org/article/10.1088/2058-9565/ac8ecd.

ON THE THRESHOLD OF A GLOBAL TECHNOLOGICAL TRANSITION. PROBLEMS AND SOLUTIONS

A.V. Lukashev, *Candidate of Military Sciences, Senior Researcher at SIC*
V.S. Sarafannikov, *Senior Researcher at SIC*
Marshal of the Soviet Union S.M. Budyonny Military Academy of Communications (Russia, St. Petersburg)

Abstract. *The article discusses the problems of the country's transition to a new technological level because of the advent of quantum computers and threats to existing cryptography systems. Some ways of solving the problems of ensuring information security and overcoming the lag behind the leaders of the world race for the introduction of quantum technologies in various fields, including special-purpose communication systems, are investigated.*

Keywords: *quantum technologies, quantum communications, quantum key distribution, post-quantum cryptography algorithms.*