ОБЩИЙ ПОДХОД К СНИЖЕНИЮ РИСКОВ ПРИ ВНЕДРЕНИИ КВАНТОВЫХ ТЕХНОЛОГИЙ

В.К. Снежко, *канд. техн. наук, доцент*
С.А. Якушенко, *канд. техн. наук, доцент*
А.В. Лукашев, *канд. воен. наук*
В.Е. Егрушев, *канд. техн. наук*
С.С. Веркин, *канд. техн. наук*
В.В. Антонов, *преподаватель*
Е.В. Чеканова, *преподаватель*
Военная академия связи им. Маршала Советского Союза С.М. Буденного (Россия, г. Санкт-Петербург)

DOI:10.24412/2500-1000-2023-6-3-151-155

Аннотация. *В статье рассмотрены угрозы информационной безопасности со стороны квантовых компьютеров, а также некоторые подходы к снижению таких угроз при плановом переходе на новый технологический уровень. Результаты исследований могут быт использованы при планирование государственного заказа в рамках планового перехода на квантовые технологии.*

Ключевые слова: *информационная безопасность, квантовые технологии, квантовые коммуникации, способы защиты от угроз.*

Бурное развитие и внедрение квантовых технологий определяет основное содержание современного научно-технического прогресса в сфере информационных технологий. При этом между участниками этого процесса сформировались отношения не столько международной кооперации, сколько соревнования за достижения квантового превосходства или, как недавно принято, квантового преимущества. С этой целью группой западных стран 31 января 2023 года учреждён Международный совет ассоциаций квантовой промышленности, объединивший передовые национальные ассоциации Канады – Quantum Industry Canada, QIC, США – Консорциум квантового экономического развития QED-C, Японии Quantum Strategic Industry Alliance for Revolution, Q-STAR и Европейского Союза – Европейский консорциум квантовой промышленности, QuIC. Выступая на заключительном заседании этого совета, его председатель, в частности, заявил о начале глобальной технологической революции [1].

Большинство развитых стран имеют национальные программы создания и внедрения квантовых технологий в сферы информационного обеспечения экономической и оборонной деятельности. Признанным лидером квантовой гонки является Китай, вложивший в 2021 году в эту сферу 10 млрд. долларов США, что составило около 40 процентов мировых инвестиций [2].

Американская программа предусматривает создание и использование квантового интернета в интересах силовых ведомств [3]. Дорожная карта создания и развития интегрированной квантовой информационной сети с космическим сегментом Евросоюза рассчитана на период с 2020 по 2036 год [4]. Подобная дорожная карта существует и в России [5]. Таким образом, переход на новый технологический уровень в сфере развития информационных технологий и систем коммуникаций постепенно набирает обороты.

Следует отметить, что переход на новый технологический уклад в данной сфере попутно создает угрозы существующим системам криптографии, а следовательно, и национальной информационной безопасности. Поэтому ниже такие угрозы рассмотрены в аспекте обоснования подходов к их снижению.

Вероятные угрозы информационной безопасности со стороны квантовых технологий

Для оценки реальности угроз информационной безопасности рассмотрим некоторые факты, имеющиеся в доступных источниках. До недавнего времени считалось, что квантовые компьютеры, способные взламывать современные криптографические системы появятся через 5-10 лет [6]. Но действительность начала опровергать эти расчеты. Об этом свидетельствует целый ряд свершившихся успешных экспериментов.

4 мая 2023 года российское электронное периодическое издание «3DNews», со ссылкой на американское агентство Semiconductor Digest, сообщило о начале проектирования квантовых процессоров для квантовых компьютеров емкостью миллион кубитов [7]. Ранее, 4 января 2023 года, китайские исследователи опубликовали [8] результат успешного эксперимента по взлому криптографического ключа RSA-48 с помощью разработанного ими протокола QAOA (Quantum Approximation Optimization Algorithm) на 10-ти кубитном квантовом компьютере применительно к алгоритму Шнорра [9]. Авторы эксперимента предоставили аналитические расчеты по характеристикам квантового компьютера, способного взломать криптографические ключи различной длины одной из основных систем шифрования (табл. 1).

Таблица 1. Расчетные характеристики квантового компьютера для взлома криптосистем RSA

RSA number\ параметры	Qubits	Kn-depth	2DSL-depth	LNN-depth
RSA-128	37	113	121	150
RSA-256	64	194	204	258
RSA-512	114	344	357	458
RSA-1024	205	617	633	822
RSA-2048	372	1118	1139	1490

В описании эксперимента авторы представили экспериментальную установку и разработанный ими алгоритм взлома ключа шифрования. Ценность опубликованного эксперимента состоит в декларации угрозы со стороны квантовых компьютеров в ближайшем будущем.

К этому следует добавить, что еще в ноябре прошлого года компания IBM ввела в эксплуатацию квантовый компьютер Orsey емкостью 433 кубита, а к концу текущего года запустит систему Quantum System Two емкостью 1127 кубитов. Сопоставляя эти сообщения, приходится сделать вывод о наличии реальных угроз информационной безопасности в критически важных областях, в том числе, в системах управления войсками и оружием. И уже не в отдаленном, как считалось до недавнего времени, а в ближайшем будущем.

Общий подход к безопасному переходу на новый технологический уровень

Существуют различные подходы к решению возникшей проблемы безопасности. Если отбросить позицию, что ничего не надо делать, так как угроза мнимая, то есть три основных варианта. Один из них – разработка и внедрение постквантовых (квантовобезопасных) алгоритмов шифрования. Другой – создание и освоение квантовых технологий, в первую очередь, квантового распределения ключей [10]. Разумный подход заключается в оптимизации соотношения этих вариантов, когда на наиболее важных информационных направлениях используются квантовые, а на менее важных – постквантовые системы криптографии.

Здесь мы формулируем подход к детализации сосуществования двух различных подходов. На рисунке 1 этот подход представлен в динамике.

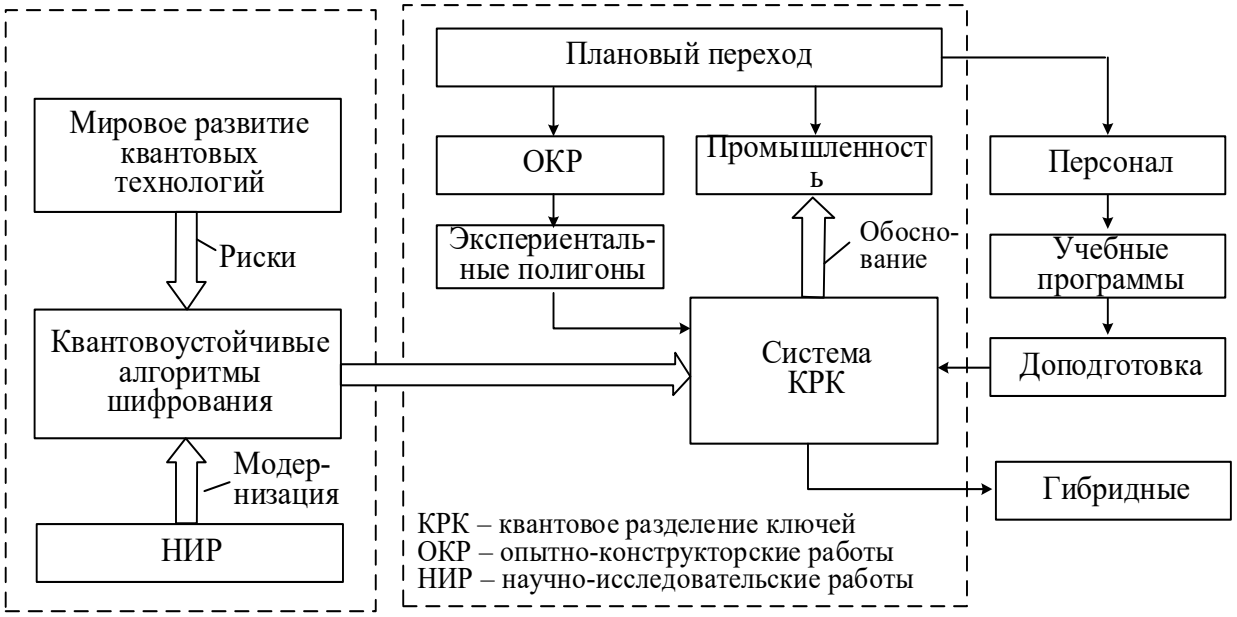

Рис. 1. Плановый переход на новый технологический уровень при внедрении квантовых технологий

Суть нашего подхода состоит в следующих основных положениях:

- квантовые технологии создают риски взлома существующим системам криптографии, однако нет гарантий того, что в будущем такой же угрозе не могут подвергнуться и постквантовые системы;

- постквантовые системы могут и должны модернизироваться с целью повышения устойчивости к взлому;

- на первом этапе внедрения квантовых технологий в системы связи специального назначения целесообразно применять квантовое распределение ключей на наиболее важных информационных направлениях. При этом необходимо уделять внимание важности исследований в создании систем связи на принципах нелокальности [11];

- на менее важных направлениях могут использоваться постквантовые (квантовоустойчивые) алгоритмы шифрования;

- по мере роста угроз со стороны квантовых компьютеров, следует постепенно переводить направления с постквантовых на квантовые системы. Для упорядоченной организации такого перехода необходимо всесторонне анализировать зарубежные эксперименты и отечественные достижения в сфере развития квантовых систем вычислений с целью обоснованной оценки рисков, а также планового создания резервов квантовых систем и оборудования, подготовки кадров для их эксплуатации;

- поскольку сами квантовые системы коммуникации подвержены квантовым атакам, следует развивать методы защиты от них, в том числе создание гибридных систем, например, развитием стеганографии [12] внутри квантовых систем коммуникаций;

- с учетом аналитических оценок рисков для существующих и постквантовых систем криптографии, целесообразно создавать планы перехода на квантовые системы коммуникаций информационных направлений в соответствии с их ранжированием по важности. В свою очередь, такие планы позволяют своевременно организовать закупки оборудования для квантовых систем в промышленности.

На рисунке дополнительно показаны блоки доподготовки научных и преподавательских кадров, в том числе с использованием экспериментальных полигонов, районов и лабораторий для симуляции, либо натуральных систем для квантовых атак и разработки методов защиты от них. В этом аспекте целесообразно установить требование к защите диссертационных и дипломных работ по темам квантовых коммуникаций по результатам успешного эксперимента. Такое требование создаст условия для более оперативного решения

задач, развития и укрепления информационной безопасности и в полной мере обеспечит загрузку развернутых экспериментальных полигонов.

Заключение

Таким образом, в статье в общем виде предложен подход к обоснованию рациональной организации перехода на новый технологический уровень путем снижения рисков в различных сферах управления, в первую очередь, в критически важных отраслях. Его суть сводится к объективной оценке угроз со стороны квантовых компьютеров и, на этой основе, планирования процесса перехода, управления финансовыми ресурсами и промышленными возможностями, начиная с научно-исследовательских работ и заканчивая организацией государственных закупок.

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. Krebs, Gunter D. «Jinan 1 (Diguidao Lianzi Miyao Fenfao)». Gunter's Space Page. Retrieved February 04, 2023. – [Электронный ресурс]. – Режим доступа: https://space.skyrocket.de/doc_sdat/jinan-1.htm.

3. Quantum Communications and Networks. – [Электронный ресурс]. – Режим доступа: https://www.nist.gov/programs-projects/quantum-communications-and-networks/.

4. Laurent de Forges de Parny et.al. Satellite-based quantum information net-works: use cases, architecture, and roadmap. – [Электронный ресурс]. – Режим доступа: https://www.nature.com/articles/s42005-022-01123-7.

5. Дорожная карта развития высокотехнологичной области «Квантовые коммуникации» на период до 2030 года. Министерство цифрового развития РФ, №17 от 27.08.2020 г.

6. Квантовые компьютеры и конец безопасности/ Блог Касперского. – [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/kvantovye-kmpyutery-i-konec-bezopasnosti/1989/.

7. Детинич Г. Процессоры для квантового компьютера на 1 млн кубитов будут выпускать в США на заводе прошлого века, 04.05.2023, Сетевое агентство 3DNews, Daily Digital Digest/10-86179. – [Электронный ресурс]. – Режим доступа: https:///protsessri-dlya-rvantovogo-kompyutera-na-million-kubitov-budut-razrabativat-i-vipuskat-v-ssha-na-zavjde-proshlogo-veka.

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

9. Schnorr C.P. Fast factoring integers by SVP algorithms, corrected, Cryptology ePrint Archive (2).

10. 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.

11. Einstein A., Podolsky B., Rosen N. (1935). «Can Quantum-Mechanical Description of Physical Realty Be Considered Complete?». Phys. Rev. 47 (10): 777-780/ DOI: 10.1103/PhysRev./47.777.

12. Что такое стеганография? – [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/recource-centere/definitions/what-is-steganography.

GENERAL APPROACH TO RISK REDUCTION DURING IMPLEMENTATION TO QUANTUM TECHNOLOGY

V.C. Snezhko, *Candidate of Technical Sciences, Associate Professor*
S.A. Yakushenko, *Candidate of Technical Sciences, Associate Professor*
A.V. Lukashev, *Candidate of Military Sciences*
V.E. Egrushev, *Candidate of Technical Sciences*
S.S. Verkin, *Candidate of Technical Sciences*
V.V. Antonov, *Lecturer*
E.V. Chekanova, *Lecturer*
Military Academy of Communications. Marshal of the Soviet Union S.M. Budyonny (Russia, St. Petersburg)

Abstract. *New threats to information security from quantum technologies, being introduced into field of management, and some threat protection methods are considered in the article. The results of the research can be used in the planning of the state order as part of the planned transition to quantum technologies.*

Keywords: *Information security, quantum technologies, quantum communications, threat protection methods.*