Квантовая устремленность как угроза информационной безопасности / Лукашев А.В., Шабуня В.В., Сарафанников В.С. и др.// Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 6(32) с. 97–101

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

КВАНТОВАЯ УСТРЕМЛЕННОСТЬ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

[1]Лукашев А.В., [2]Шабуня В.В., [3]Сарафанников В.С., [4]Билан В.В.
ФГКВОУ ВО "Военная Орденов Жукова и Ленина Краснознаменная Академия связи имени Маршала Советского Союза С.М.Буденного" МО РФ, Санкт-Петербург, Россия (194064, г.Санкт-Петербург, Тихорецкий просп., 3), e-mail: [1]lukasheff@mail.ru, [2]vvsch1970@mail.ru, [3]was16@mail.ru, [4]bilanvictoriya@yandex.ru.

В статье рассмотрены повсеместно и широко внедряемые в сферы управления квантовые технологии, представляющие новые угрозы информационной безопасности, а также некоторые подходы к их снижению.

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

QUANTUM ASPIRATION AS A THREAT INFORMATION SECURITY

[1]Lukashev A.V., [2]Shabunya V.V., [3]Sarafannikov V.S., [4]Bilan V.V.
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia (194064, St. Petersburg, Tikhoretsky prosp., 3), e-mail: [1]lukasheff@mail.ru, [2]vvsch1970@mail.ru, [3]was16@mail.ru, [4]bilanvictoriya@yandex.ru

The article discusses quantum technologies that are widely and widely implemented in the management sphere, which pose new threats to information security, as well as some approaches to their reduction.

Keywords: Theory Of constraints, system constraints, TOS implementation, implementation algorithm, cash flows, throughput.

Международным советом ассоциаций квантовой промышленности, который был учрежден 31 января 2023 года и объединил четыре ассоциации (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 заявлено: «Мы находимся в начале глобальной технологической революции» [1]. Из этой небольшой фразы можно сделать весьма определенный вывод: на текущий момент развитие квантовых технологий находится в ряду важнейших задач научно-технического прогресса.

Дорожная карта создания и развития интегрированной квантовой информационной сети с космическим сегментом Евросоюза предусматривает три этапа, рассчитанных на период с 2020 по 2036 год. Подобная дорожная карта существует и в России [2].

Таким образом, мы являемся свидетелями перехода на новый технологический уровень в сфере развития систем связи. Этому послужили многочисленные открытия, эксперименты и

разработки, в том числе в области коммуникаций. Особое значение приобретают не только вычисления и коммуникации с использованием квантовых технологий, но и попутно создаваемые угрозы существующим системам криптографии. Поэтому ниже рассмотрены такие угрозы и некоторые подходы к их снижению.

Новые угрозы информационной безопасности со стороны квантовых технологий

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 [3]. Ранее, 4 января 2023 года, китайские исследователи опубликовали [4] 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 [5]. Авторы эксперимента предоставили аналитические расчеты по характеристикам квантового компьютера, способного взломать криптографические ключи различной длины одной из основных систем шифрования (см. таблицу 1).

Таблица 1 – Расчетные характеристики квантового компьютера для взлома криптосистем RSA

RSA number	Qubits	K_n-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 статье представлены экспериментальная установка и алгоритм реализации 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.

Подходы к обеспечению информационной безопасности

Существуют различные подходы к решению возникшей проблемы безопасности. Если отбросить позицию, что ничего не надо делать, так как угроза мнимая, 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 [6]. 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.

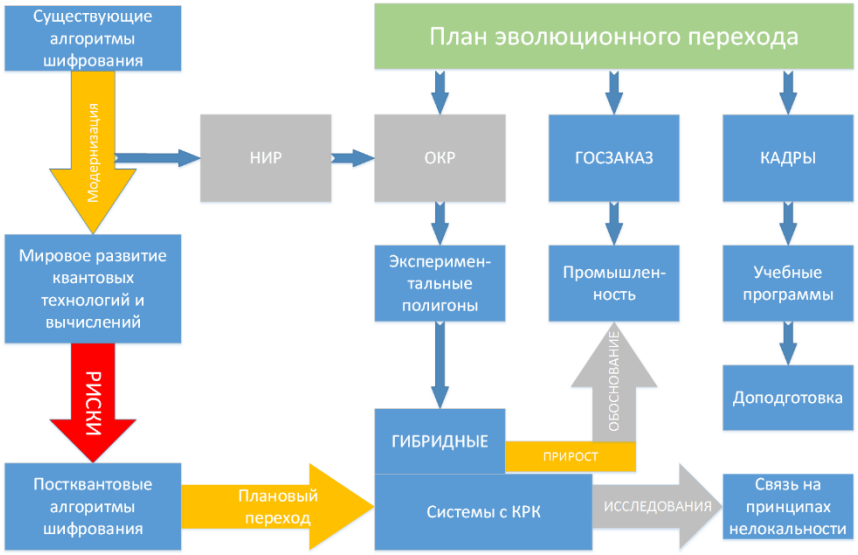

Рисунок 1 – Динамичное сосуществование существующих, квантовых и постквантовых систем криптографии (ОКР – опытно-конструкторские работы, НИР – научно-исследовательские работы, КРК – квантовое распределение ключей).

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 [7];
- 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 [8] 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.

Таким образом, суть подхода нивелирования рисков в различных сферах управления, в первую очередь, в критически важных отраслях, сводится к объективной оценке рисков и к планированию перехода систем управления на новый технологический уровень с использованием квантовых коммуникаций, что в статье представлено в общем виде. Основной этап может заключаться в создании квантовых систем на принципе нелокальности. Этот переход предполагает окончательное решение проблемы безопасности информационных систем, а квантовое распределение ключей предложено рассматривать как первый этап такого перехода.

Список литературы

1. International quantum industry councils formally joining forces for the development of quantum technologies, 02.02.2023, https://qt.eu/about-quantum-flagship/newsroom/international-quantum-industry-councils-formally-joining-forces-for-the-development-of-quantum-technologies/.
2. Дорожная карта развития высокотехнологичной области «Квантовые коммуникации» на период до 2030 года. Министерство цифрового развития РФ, №17 от 27.08.2020 г.
3. Детинич Г., – Процессоры для квантового компьютера на 1 млн кубитов будут выпускать в США на заводе прошлого века, 04.05.2023, Сетевое агентство 3ДНьюс, Daily Digital Digest/10-86179, https:///protsessri-dlya-rvantovogo-kompyutera-na-million-kubitov-budut-razrabativat-i-vipuskat-v-ssha-na-zavjde-proshlogo-veka.
4. Bao Yan et.al. Factoring integers with sublinear resources on a superconducting quantum processor, https://arxiv.org/pdf/2212.12372.pdf.
5. C. P. Schnorr, Fast factoring integers by SVP algorithms, corrected, Cryptology ePrint Archive (2).
6. 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.
7. 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; Bor N. “Can Quantum-Mechanical Description of Physical Realty Be Considered Complete?”. Phys. Rev. 48 (8): 696-702/ DOI: 10.1103/PhysRev./48.696.

8. Что такое стеганография? – https://www.kaspersky.ru/recource-centere/definitions/what-is-steganography.

References

1. International quantum industry councils formally joining forces for the development of quantum technologies, 02.02.2023, https://qt.eu/about-quantum-flagship/newsroom/international-quantum-industry-councils-formally-joining-forces- for-the-development-of-quantum-technologies/.
2. Roadmap for the development of the high-tech field "Quantum Communications" for the period up to 2030. Ministry of Digital Development of the Russian Federation, No. 17 dated August 27, 2020
3. Detinich G., - Processors for a quantum computer with 1 million qubits will be produced in the USA at a factory of the last century, 05/04/2023, 3DNews Network Agency, Daily Digital Digest/10-86179, https:///protsessri-dlya-rvantovogo -kompyutera-na-million-kubitov-budut-razrabativat-i-vipuskat-v-ssha-na-zavjde-proshlogo-veka.
4. Bao Yan et al. Factoring integers with sublinear resources on a superconducting quantum processor, https://arxiv.org/pdf/2212.12372.pdf.
5. C. P. Schnorr, Fast factoring integers by SVP algorithms, corrected, Cryptology ePrint Archive (2).
6. 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, India 10-12 December, New York: IEEE Press, 1984. V. 560. P. 175-179.
7. 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; Bor N. “Can Quantum-Mechanical Description of Physical Realty Be Considered Complete?”. Phys. Rev. 48 (8): 696-702/ DOI: 10.1103/PhysRev./48.696.
8. What is steganography? – https://www.kaspersky.ru/recourse-centere/definitions/what-is-steganography.