УДК 004.056.5

П.Н. Наседкин[1], В.А. Сверкунов[1]

[1] Иркутский государственный университет путей сообщений, г. Иркутск, Российская Федерация

КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ НА ПУТИ К ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

Аннотация. В работе выполнен анализ уязвимости криптографических алгоритмов, которые обеспечивают одну или несколько из следующих услуг: создание и обмен ключами шифрования, зашифрованные соединения или создание и проверка цифровых подписей к атакам типа «собери сейчас, расшифруй позже», которая может быть реализована со стороны квантовых компьютеров. Отражены уязвимые криптографические алгоритмы в разрезе сетевых моделей, сертифицированных ФСТЭК средств защиты информации. Проведено исследование эксплуатируемого в Российской Федерации сертифицированных средств защиты информации, использующих уязвимые криптографические алгоритмы. Выявлен диапазон времени по возможности проведения атак, связанных с прекращением срока действия сертификата на модельный ряд сетевых средств защиты информации отечественных и иностранных производителей.

Представленный в настоящей работе анализ уязвимых криптографических алгоритмов не является окончательным, а требует более детальной инвентаризации всей ИТ-инфраструктуры Российской Федерации, которая может содержать криптографические системы, уязвимые для квантовых вычислений.

Ключевые слова: информационная безопасность, квантовые вычисления, криптографические алгоритмы, постквантовая криптография, уязвимость алгоритмов.

P.N. Nasedkin [1], V.A. Sverkunov[1]

[1] Irkutsk State Transport University, Irkutsk, Russian Federation

CRYPTOGRAPHIC ALGORITHMS ON THE WAY TO POST-QUANTUM CRYPTOGRAPHY

Abstract. This paper analyzes the vulnerability of cryptographic algorithms that provide one or more of the following services: creation and exchange of encryption keys, encrypted connections, or creation and verification of digital signatures to "build now, decrypt later" attacks, which can be implemented by quantum computers. Vulnerable cryptographic algorithms in the context of network models, certified by FSTEC means of information protection. A study in the context of the operated in the Russian Federation certified means of protection of information, which use vulnerable cryptographic algorithms, has been carried out. A time range for the possibility of attacks, related to termination of the certificate on the model range of network information security devices of domestic and foreign manufacturers has been revealed.

The analysis of vulnerable cryptographic algorithms presented in this paper is not final, but requires a more detailed inventory of the entire IT infrastructure of the Russian Federation, which may contain cryptographic systems vulnerable to QC quantum computing.

Keywords: information security, quantum computing, cryptographic algorithms, post-quantum cryptography, algorithm vulnerability.

Введение. Как известно, криптография и криптоанализ изучают способы шифрования и дешифрования информации в основе которой рассматриваются методы защиты и нарушения конфиденциальности, как свойства информации. [1]

Все многообразие существующих в настоящее время алгоритмов шифрования может быть сгруппировано, как представлено на рисунке 1.

Однако, с дальнейшим развитием науки и техники начались исследования в области квантовой криптографии, которая в настоящее время являет собой новый виток в развитии информационной защиты. История развития самой идеи использовать квантовые объекты для защиты информации от модификации и несанкционированного доступа впервые была озвучена Стефаном Вейснером в 1970 г. и далее, через 10 лет со стороны ученых Беннет и Брассард было предложено использовать квантовые объекты для передачи секретного ключа.

Рис. 1. Группировка алгоритмов шифрования.

В последствии, разработанный алгоритм Шора [2] дал импульс для развития квантовых компьютеров (КК) в 1990-х годах. В условиях рыночной экономики идея применения КК даст квантовое превосходство в вычислениях по сравнению с вычислениями, производимыми с применением классических компьютеров и которые между тем не обладают вычислительной способностью для разрушения криптографических алгоритмов в разумные сроки.

В ответ на потенциальные возможности КК и опасность, которую они могут нанести установленным методам шифрования проводятся разработки асимметричных алгоритмов, способных производить, шифровать и расшифровывать ключи. В связи с чем появился термин постквантовая криптография (PQC), которая является областью исследований, специализирующихся на создании криптографических алгоритмов, достаточно устойчивых, чтобы противостоять атакам КК [3]. Предполагается, что после стандартизации квантово-устойчивые алгоритмы должны будут заменить используемые в настоящее время криптосистемы с открытым ключом [3].

Из представленной на рисунке 1 группировки алгоритмов шифрования выделим те из них, алгоритм шифрования которых может быть уязвим к атакам в результате квантовых вычислений. Перечень уязвимых алгоритмов приведен в таблице 1 согласно опубликованному в США от 18.11.2022 меморандуму M-23-02 Migrating to Post-Quantum Cryptography [4] для руководителей исполнительных департаментов и агентств.

Таблица 1

Список уязвимых криптографических алгоритмов для квантовых компьютеров

Криптографический алгоритм	**Выполняемая функция**	**Спецификация**
Обмен ключами Диффи-Хеллмана на эллиптических кривых (ECDH)	Асимметричный алгоритм используется для создания ключей	НИСТ СП 800-56А/Б/С
Менезес-Ку-Ванстон (MQV). Обмен ключами	Асимметричный алгоритм используется для создания ключей	НИСТ СП 800-56А/Б/С
Алгоритм цифровой подписи на основе эллиптических кривых (ECDSA)	Асимметричные алгоритмы используется для цифровых подписей	ФИПС ПАБ 186-4
Диффи-Хеллман (DH). Обмен ключами	Асимметричный алгоритм используется для создания ключей	IETF RFC3526
Алгоритм подписи RSA	Асимметричный алгоритм используется для создания ключей	ФИПС СП 800-56Б Ред.1

Алгоритм цифровой подписи	Асимметричный алгоритм используется для цифровых подписей	ФИПС ПАБ 186-4
Другие не-PQC Асимметричный алгоритм	Оставшиеся асимметричные алгоритмы, не перечисленные в списке выше	Не применима

На основании изложенного, необходимо отметить, что необходимым условием для преодоления проблемы внедрения PQC (сложность миграции данных, риск неправильного внедрения, длительные сроки) является применение для оценки и управления рисками в ИТ-системах модели «Куб МакКамбера» [5], которая была создана Джоном МакКамбером в 1991 году. Модель «Куб МакКамбера» представлена на рисунке 2. Данная модель хорошо себя зарекомендовала при разработке программного обеспечения, оценки продуктов, создании программы безопасности.

Рис. 2. Модель «Куб МакКамбера»

Криптография являясь одним из основных механизмов защиты информации поддерживает различные свойства информации, а именно: обеспечивает конфиденциальность преобразуя данные в шифротекст, поддерживает целостность информации через сервисы цифровой подписи. В связи с чем, возникает потребность в доступе к актуальной базе знаний в области изменения криптографических алгоритмов

Уязвимые алгоритмы шифрования для квантовых компьютеров (КК) и сертифицированные средств защиты информации (СЗИ) использующие их в разрезе моделей сетевых устройств в отечественной ИТ-инфраструктуре.

Квантовые компьютеры, используя принципы квантовой физики, в основе которых лежит уравнение Шрёдингера [6], превышают вычислительную мощность самых производительных суперкомпьютеров, что уже представляет повышенную угрозу безопасности от брутфорса (перебора всевозможных комбинаций) для перечня шифров в разрезе симметричного и ассиметричного криптографических алгоритмов, а также алгоритмов хэш-функций, представленных в таблице 2.

Таблица 2

Список уязвимых криптографических алгоритмов для квантовых компьютеров

Наименование криптографического алгоритма	Способ шифрования	Перечень шифров
Симметричные алгоритмы: - блочные; - поточные	Симметричное шифрование предусматривает использование одного и того же ключа и для зашифрования, и для расшифрования. К симметричным алгоритмам	• ГОСТ 28147-89 — отечественный стандарт шифрования; • 3DES (Triple-DES, тройной DES); • RC6 (Шифр Ривеста); • Twofish; • SEED - корейский стандарт шифрования;

	применяются два основных требования: полная утрата всех статистических закономерностей в объекте шифрования и отсутствие линейности.	• Camellia – японский стандарт шифрования; • CAST (по инициалам разработчиков Carlisle Adams и Stafford Tavares); • IDEA; • XTEA - наиболее простой в реализации алгоритм; • AES – американский стандарт шифрования; • DES – стандарт шифрования данных в США до AES.
Ассиметричные алгоритмы	Ассиметричные системы также называют криптосистемами с открытым ключом. Это такой способ преобразования данных, при котором открытый ключ передается по открытому каналу (не скрывается) и используется для проверки электронной подписи и для шифрования данных. Для расшифрования и создания электронной подписи используется второй ключ, закрытый.	• RSA (Rivest-Shamir-Adleman, Ривест — Шамир — Адлеман); • DSA (Digital Signature Algorithm); • Elgamal (Шифросистема Эль-Гамаля); • Diffie-Hellman (Обмен ключами Диффи — Хелмана); • ECC (Elliptic Curve Cryptography, криптография эллиптической кривой); • ГОСТ Р 34.10-2001; • Rabin; • Luc; • McEliece
Алгоритмы хэш-функций	Хешированием (от англ. hash) называется преобразование исходного информационного массива произвольной длины в битовую строку фиксированной длины. Алгоритмов хеш-функций немало, а различаются они своими характеристиками – криптостойкостью, разрядностью, вычислительной сложностью и т.д.	• Adler-32 • CRC • SHA-1 • SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512) • HAVAL • MD2 • MD4 • MD5 • N-Hash • RIPEMD-160 • RIPEMD-256 • RIPEMD-320 • Skein • Snefru • Tiger (TTH) • Whirlpool • ГОСТ Р34.11-94 (ГОСТ 34.311-95) • IP Internet Checksum (RFC 1071)

В целях исследования на предмет уязвимых алгоритмов шифрования к квантовым вычислениям был проведён анализ реестра, представленного на сайте ФСТЭК [7] сертифицированных средств защиты информации как в разрезе моделей сетевых устройств, представленных на рисунке 3, так и по датам окончания срока действия их сертификатов, представленных на рисунке 4.

В результате анализа сертифицированных средств защиты информации установлено, что вся исследуемая выборка в количестве 81 позиции по оборудованию и программных средств содержат уязвимые алгоритмы шифрования (DH, RSA, DSS) к атакам с использованием квантовых вычислений.

Из представленной на рисунке 3 и рисунке 4 информации следует, что весь сегмент отечественной ИТ-инфраструктуры в разрезе сертифицированных ФСТЭК сетевых программно-аппаратных средств содержит:

– в большей степени программно-аппаратные средства (ПАС) защиты информации иностранного производства, среди которых имеется оборудование не дружественных стран;

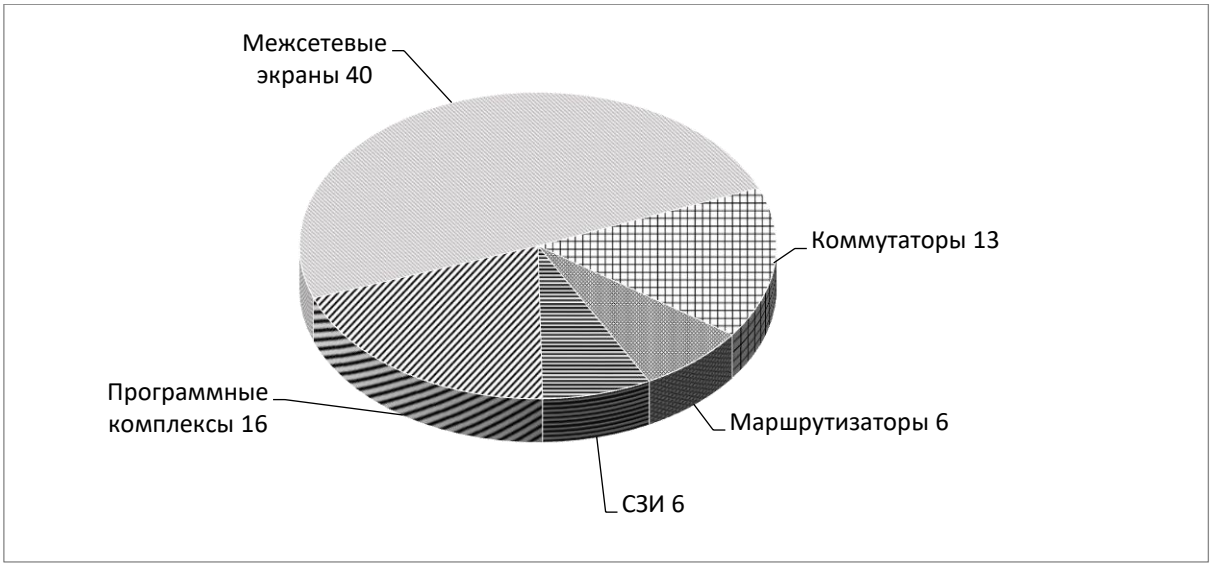

Рис. 3. Модели сертифицированных ФСТЭК сетевых устройств, применяемых на территории Российской Федерации для защиты информации.

Рис. 4. Год окончания действия сертификата ФСТЭК на уязвимые модели сетевых устройств, применяемых на территории Российской Федерации для защиты информации.

– оборудование и программные средства, использующие уязвимые криптографические алгоритмы для квантовых вычислений;

– горизонт использования ПАС по сроку эксплуатации уязвимых алгоритмов шифрования до 2026 г. для отечественных и до 2027 года для иностранных производителей средств защиты информации.

Вместе с тем, необходимо отметить, что в соответствие с указом Президента РФ от 01.05.2022г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [8] предписано с 1 января 2025 г. запретить органам (организациям) использовать средства защиты информации иностранных государств, совершающие в отношении Российской Федерации недружественные действия.

Заключение. В работе выполнен анализ уязвимости криптографических алгоритмов к атакам типа «собери сейчас, расшифруй позже», которая может быть реализована со стороны квантовых компьютеров. Выявлены уязвимые криптографические алгоритмы DH, RSA, DSS

в разрезе сетевых моделей, сертифицированных ФСТЭК средств защиты информации (СЗИ). В соответствие с большим количеством эксплуатируемого в Российской Федерации сертифицированных ПАС, использующих уязвимые криптографические алгоритмы с планируемым горизонтом срока прекращения действия их сертификата до 2026 – 2027гг. установлен риск возможных атак со стороны КК.

Также хотелось бы отметить, что представленный в настоящей работе анализ уязвимых криптографических алгоритмов не является окончательным, а требует более детальной инвентаризации всей ИТ-инфраструктуры Российской Федерации, которая может содержать криптографические системы, уязвимые для квантовых вычислений КК.

С увеличением вычислительных мощностей квантовых компьютеров появляются как квантовое превосходство, так и новые риски ИБ, влияние которых на ИТ-инфраструктуру предприятий необходимо учитывать при будущей оценке уровня защищённости предприятий. В настоящее время для моделирования сценариев атак используются следующие инструменты для моделирования:

- база знаний ATT&CK (Adversarial Tactics, Techniques & Common Knowledge – тактики, техники и известные факты о противнике) компании MITRE, которая содержит 14 фаз тактик и 224 техники;
- база данных угроз и уязвимостей ФСТЭК, которая содержит 222 угрозы и 43856 уязвимостей.

Однако, к существенным недостаткам в части вычислительных способностей квантовых сопроцессоров в настоящее время можно отнести ошибки в вычислении по причине которых они не доступны для массового пользования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Криптография [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Статья:Криптография, свободный (дата обращения: 02.12.2022).

2. Nannicini, Giacomo. An Introduction to Quantum Computing, without the Physics // SIAM Review 2020. Vol. 62. Number 4, 2020, pp. 936–981.

3. Logan O. Mailloux, Charlton D. Lewis II, Casey Riggs, Michael R. Grimaila. Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals // IT Professional. 2016. Vol. 18(5), pp. 42-47.

4. M-23-02 Migrating to Post-Quantum Cryptography [Электронный ресурс]. Режим доступа: https://www.whitehouse.gov/, свободный (дата обращения: 02.12.2022).

5. John McCumber. Assessing and Managing Security Risk in IT Systems // Auerbach Publications. 2004. P. 35

6. Уравнение Шрёдингера [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/, свободный (дата обращения: 29.11.2022).

7. Государственный реестр сертифицированных средств защиты информации [Электронный ресурс]. – Режим доступа: https://fstec.ru/, свободный (дата обращения: 27.11.2022).

8. Указ Президента РФ от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [Электронный ресурс]. – Режим доступа: http://pravo.gov.ru/, свободный (дата обращения: 02.12.2022).

REFERENCES

1. *Kriptografia*. [Cryptography]. Available at: https://www.tadviser.ru/index.php/ (Accessed: December 02, 2022) (in Russ.).

2. Nannicini, Giacomo. An Introduction to Quantum Computing, without the Physics // SIAM Review 2020. Vol. 62. Number 4, 2020, pp. 936–981.

3. Logan O. Mailloux, Charlton D. Lewis II, Casey Riggs, Michael R. Grimaila. Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals // IT Professional. 2016. Vol. 18(5), pp. 42-47.

4. M-23-02 Migrating to Post-Quantum Cryptography. Available at: https://www.whitehouse.gov/ (Accessed: December 02, 2022).

5. John McCumber. Assessing and Managing Security Risk in IT Systems // Auerbach Publications. 2004. P. 35.

6. *Uravnenie SHryodingera.* [Schrodinger equation]. Available at: https://ru.wikipedia.org / (Accessed: December 02, 2022) (in Russ.).

7. *Gosudarstvennyj reestr sertificirovannyh sredstv zashchity informacii.* [State Register of Certified Information Security Tools]. Available at: https://fstec.ru / (Accessed: December 02, 2022) (in Russ.).

8. *Ukaz Prezidenta RF ot 01.05.2022 g. № 250 «O dopolnitel'nyh merah po obespecheniyu informacionnoj bezopasnosti Rossijskoj Federacii».* [Decree of the President of the Russian Federation No. 250 dated 01.05.2022 «On additional measures to ensure information security of the Russian Federation»]. Available at: http://pravo.gov.ru/ (Accessed: December 02, 2022) (in Russ.).

Информация об авторах

Павел Николаевич Наседкин – аспирант кафедры «Информационные системы и защита информации», Иркутский государственный университет путей ний, г. Иркутск, e-mail: nasedkin_pn@irgups.ru

Владимир Александрович Сверкунов – студент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщений, г. Иркутск, e-mail: dyvv3@mail.ru

Authors

Pavel Nikolaevich Nasedkin – Postgraduate student, Department of Information Systems and Information Protection, Irkutsk State Transport University (ISTU), Irkutsk, e-mail: nasedkin_pn@irgups.ru.

Vladimir Aleksandrovich Sverkunov – student, Department of Information Systems and Information Protection, Irkutsk State Transport University (ISTU), Irkutsk, e-mail: dyvv3@mail.ru

Для цитирования

Наседкин, П. Н., Сверкунов В.А. Криптографические алгоритмы на пути к постквантовой криптографии // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2022. – №4(16). – С. 67-73 – DOI: 10.26731/2658-3704.2022.4(16).67-73 – Режим доступа: http://ismm-irgups.ru/toma/416-2022, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 23.12.2022).

For citation

Nasedkin P.N., Sverkunov V.A. Cryptographic algorithms on the way to post-quantum cryptography // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2022. No. 4(16). P. 67-73. DOI: 10.26731/2658-3704.2022.4(16).67-73 [Accessed 23/12/22].