УДК 004.056.5:003.26

Кириленко Юлия Андреевна, магистрант Дальневосточный государственный университет путей сообщений, г. Хабаровск

ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ: ОТ ТЕОРЕТИЧЕСКИХ ОСНОВ К ГЛОБАЛЬНОМУ ПЕРЕХОДУ

Аннотация. Исследование посвящено постквантовой криптографии — направлению, разрабатывающему алгоритмы, устойчивые к атакам квантовых компьютеров. Рассмотрены ключевые угрозы, включая алгоритм Шора, способный взломать RSA и ECC. Проанализированы современные постквантовые методы: криптография на решётках (Kyber, Dilithium), кодовые системы (McEliece) и их сравнительная эффективность. Особое внимание уделено процессу стандартизации NIST и практическому внедрению в TLS, блокчейн и облачные технологии. Выявлены технические и организационные вызовы: высокая ресурсоёмкость, нехватка специалистов. Предложены стратегии перехода для организаций, включая гибридные решения и обучение кадров. Работа подчёркивает необходимость срочного перехода на квантово-безопасные стандарты для защиты данных в финансовой, государственной и ИТ-сферах.

Annotation. The research is devoted to post—quantum cryptography, a field that develops algorithms resistant to attacks by quantum computers. Key threats are considered, including Shor's algorithm, which can crack RSA and ECC. Modern post-quantum methods are analyzed: cryptography on lattices (Cyber, Dilithium), code systems (McEliece) and their comparative effectiveness. Special attention is paid to the NIST standardization process and practical implementation in TLS, blockchain and cloud technologies. Technical and organizational challenges have been identified: high resource intensity, lack of specialists. Transition strategies for organizations, including hybrid solutions and staff training, are proposed. The work highlights the need for an urgent transition to quantum-secure standards for data protection in the financial, government and IT fields.

Ключевые слова: Постквантовая криптография, квантовые вычисления, алгоритм Шора, NIST PQC, криптография на решётках, Kyber, Dilithium, McEliece, гибридное шифрование, стандартизация, TLS, квантовая безопасность, RSA, ECC, облачная безопасность, блокчейн.

Keywords: Post-quantum cryptography, quantum computing, Shor's algorithm, NIST PKI, lattice cryptography, Kyber, Dilithium, McEliece, hybrid encryption, standardization, TLS, quantum security, RSA, ECC, cloud security, blockchain.

В условиях стремительного технологического прогресса, характеризующего начало XXI века, перед специалистами по информационной безопасности встает принципиально новая и крайне актуальная задача - разработка и внедрение криптографических методов, устойчивых к потенциальным атакам с использованием квантовых компьютеров [1]. Эта проблема приобретает особую значимость в контексте глобальной цифровизации, когда безопасность практически всех сфер человеческой деятельности - от финансовых операций до государственного управления - зависит от надежности криптографических алгоритмов [2].

Угрозы квантовых вычислений для современных криптосистем

Современные научные исследования и технологические разработки убедительно демонстрируют, что появление полнофункциональных квантовых компьютеров способно кардинально изменить ландшафт информационной безопасности, поставив под угрозу защитные механизмы, десятилетиями считавшиеся надежными [3]. Особую опасность представляет алгоритм Шора, теоретическая модель которого была предложена в 1994 году и которая позволяет эффективно решать задачи факторизации больших чисел и вычисления дискретного логарифма - математические основы современных асимметричных криптосистем [4].

Эксперты в области квантовых вычислений и криптографии единодушно отмечают, что уже в ближайшие 10-15 лет квантовые компьютеры могут достичь уровня развития, достаточного для практической реализации атак на

существующие криптографические протоколы [5]. Это создает серьезные системные риски для различных сфер современного общества:

1. Финансовая сфера и электронные платежи [6]:

- Угроза безопасности банковских транзакций
- Риск компрометации систем цифровых подписей
- Потенциальная уязвимость криптовалютных систем

2. Государственная и коммерческая безопасность [7]:

- Опасность раскрытия защищенных государственных коммуникаций
- Угроза промышленному шпионажу
- Риски для систем управления критической инфраструктурой

3. Конфиденциальность персональных данных [8]:

- Возможность массового взлома баз данных
- Угроза приватности электронной переписки
- Риски для систем электронного здравоохранения

4. Блокчейн-технологии и распределенные системы [9]:

- Потенциальная уязвимость механизмов консенсуса
- Риск подделки транзакций
- Угроза безопасности смарт-контрактов

Описанные угрозы делают переход на квантово-устойчивые алгоритмы не просто желательным, а критически необходимым [10]. Однако этот процесс сталкивается с рядом фундаментальных сложностей:

1. Математическая сложность. В отличие от RSA и ECC, постквантовые алгоритмы основаны на новых математических задачах — решётках (LWE, NTRU), многомерных квадратичных системах или кодах исправления ошибок (McEliece). Их криптоанализ ещё не столь всесторонне изучен, как классические схемы [11].
2. Производительность и совместимость. Многие PQC-алгоритмы требуют [12]:

- Увеличенных размеров ключей (Dilithium-3: 1952 байта против 256 байт у RSA-2048).
- Изменений в сетевых протоколах (TLS, IKEv2, DNSSEC).

3. Гибридные решения. Для плавного перехода предлагается комбинировать классические и постквантовые алгоритмы, например:

- RSA + Kyber в TLS-рукопожатиях [6].
- ECDSA + Dilithium в электронных подписях [7].

4. Стандартизация. NIST уже выбрал первые алгоритмы (Kyber, Dilithium, SPHINCS+), но работы над оптимизацией и новыми подходами продолжаются.

Квантовая угроза — это не отдалённая гипотетическая возможность, а реальный вызов, требующий действий уже сегодня. Постквантовая криптография предлагает решения, но их внедрение потребует координации между разработчиками, регуляторами и бизнесом. Как отмечают в NIST, "переход займёт годы, но начинать нужно сейчас".

Преимущества постквантовой криптографии

1. Устойчивость к квантовым атакам [5]

Основное и наиболее значимое преимущество постквантовых криптографических алгоритмов заключается в их фундаментальной устойчивости к атакам с использованием квантовых компьютеров. В отличие от традиционных алгоритмов (RSA, ECC), которые могут быть взломаны с помощью алгоритма Шора и Гровера, постквантовые системы основаны на математических задачах, остающихся сложными даже для квантовых вычислителей:

- Доказанная сложность для квантовых атак на решетках
- Теоретическая устойчивость к будущим квантовым методам взлома

2. Долгосрочная безопасность данных [8]

Постквантовая криптография предлагает принципиально новый уровень защиты информации, обеспечивающий:

- Гарантированную защиту данных на десятилетия вперед
- Возможность безопасного шифрования уже сегодня
- Защиту от атак по накопленной информации
- Сохранение конфиденциальности исторических данных

3. Разнообразие математических подходов [11]

Широкий спектр математических основ обеспечивает гибкость и надежность:

- Множественность независимых математических задач (решётки, коды, многомерные системы)
- Возможность создания гибридных систем
- Альтернативные подходы на случай компрометации одного из методов
- Богатый теоретический фундамент для дальнейшего развития

4. Совместимость с существующей инфраструктурой

Современные постквантовые алгоритмы разрабатываются с учетом практических требований:

- Возможность постепенного перехода без полной замены инфраструктуры
- Поддержка гибридных режимов работы (классические и постквантовые алгоритмы)
- Адаптация к существующим криптографическим протоколам (TLS, IPSec)
- Оптимизация для различных аппаратных платформ

5. Эффективность и производительность

Несмотря на повышенную сложность, современные реализации демонстрируют:

- Приемлемую скорость работы на стандартном оборудовании
- Оптимизированные версии для IoT и мобильных устройств

- Эффективные схемы цифровых подписей
- Компактные реализации для встраиваемых систем

6. Стандартизация и международное признание

Процесс стандартизации NIST обеспечивает:

- Единые проверенные стандарты безопасности
- Международное признание и совместимость
- Прозрачность разработки и проверки алгоритмов
- Поддержку крупнейших технологических компаний

7. Стратегические преимущества для бизнеса и государства

Внедрение постквантовой криптографии дает:

- Конкурентное преимущество на рынке защищенных решений
- Соответствие будущим нормативным требованиям
- Защиту долгосрочных инвестиций в ИТ-инфраструктуру
- Уверенность в неизменности стандартов безопасности

8. Стимулирование научно-технического прогресса

Развитие направления способствует:

- Прогрессу в математике и теоретической информатике
- Развитию новых направлений в компьютерных науках
- Созданию междисциплинарных исследовательских центров
- Подготовке специалистов нового поколения

9. Гибкость и адаптивность

Архитектурные преимущества постквантовых систем:

- Модульность и возможность обновления
- Поддержка различных уровней безопасности
- Адаптация к конкретным требованиям приложений
- Масштабируемость для различных сценариев использования

10. Будущая устойчивость

Долгосрочные перспективы включают:

- Возможность эволюционного развития алгоритмов

- Защиту от пока неизвестных угроз
- Основу для следующих поколений криптографии
- Создание фундамента для квантово-безопасного будущего

Эти преимущества делают постквантовую криптографию не просто ответом на конкретную угрозу, а стратегическим направлением развития всей отрасли информационной безопасности, предлагающим комплексные решения для защиты данных в условиях стремительного технологического прогресса.

Перспективные направления постквантовой криптографии

В ответ на эти фундаментальные вызовы мировое научное сообщество активно разрабатывает и тестирует новые криптографические подходы, основанные на математических задачах, сохраняющих вычислительную сложность даже для квантовых компьютеров. Рассмотрим наиболее перспективные направления более детально:

1. Криптография на решетках (Lattice-based cryptography):

- Алгоритмы нового поколения: Kyber (KEM) и Dilithium (подписи)
- Теоретическая основа: сложность задач обучения с ошибками (LWE, RLWE)
- Преимущества: высокая устойчивость к квантовым атакам, относительная эффективность реализации
- Области применения: защищенные коммуникации, цифровые подписи

2. Кодовая криптография:

- Классическая система McEliece (с 1978 года)
- Теоретическая основа: сложность декодирования случайных линейных кодов
- Особенности: доказанная стойкость, но большие размеры ключей
- Современные модификации: алгоритмы на основе кодов Гоппы

3. Многомерные криптосистемы:

- Используют сложные алгебраические структуры (многомерные полиномиальные системы)

- Перспективны для схем цифровых подписей
- Примеры: алгоритмы Rainbow, GeMSS

4. Хэш-функции и их криптостойкость:

- Анализ устойчивости существующих хэш-функций
- Разработка квантово-устойчивых хэш-алгоритмов
- Применение в схемах доказательств с нулевым разглашением

Национальный институт стандартов и технологий (NIST) в настоящее время проводит масштабную работу по стандартизации постквантовых криптографических алгоритмов, что подчеркивает важность и актуальность данного направления. Процесс отбора включает несколько этапов:

- Теоретический анализ стойкости
- Практическая оценка производительности
- Тестирование на различных платформах
- Анализ возможных уязвимостей

Практические аспекты внедрения

Переход на новые криптографические стандарты представляет собой сложный многоаспектный процесс, сопряженный с рядом технических, организационных и экономических вызовов:

1. Проблемы совместимости и интеграции:

- Необходимость глубокой модификации существующих протоколов безопасности
- Обеспечение обратной совместимости с устаревшими системами
- Разработка переходных механизмов и гибридных схем

2. Ресурсные требования и производительность:

- Повышенные требования к вычислительным мощностям
- Увеличенные размеры ключей и служебных данных
- Оптимизация алгоритмов для различных платформ

3. Организационные и управленческие аспекты:

- Обучение и переподготовка специалистов по информационной безопасности
- Разработка стратегий поэтапного перехода
- Обновление нормативной базы и стандартов

4. Экономические факторы:

- Затраты на модернизацию инфраструктуры
- Оценка возврата инвестиций в безопасность
- Финансирование исследовательских программ

Для успешного внедрения эксперты рекомендуют использовать комплексные подходы:

- Разработка гибридных криптосистем, сочетающих традиционные и постквантовые алгоритмы
- Создание инструментов автоматизированного тестирования и оценки
- Формирование центров компетенций по постквантовой криптографии
- Международное сотрудничество в области стандартизации

Заключение

Развитие постквантовой криптографии представляет собой не просто техническую задачу, а стратегически важное направление обеспечения национальной и глобальной безопасности в цифровую эпоху. Своевременный и продуманный переход на новые алгоритмы шифрования требует:

1. Координации усилий научного сообщества, бизнеса и государства
2. Инвестиций в фундаментальные и прикладные исследования
3. Развития образовательных программ в области квантовой безопасности
4. Создания гибких нормативных рамок

Только комплексный подход позволит обеспечить устойчивую защиту данных в условиях неизбежного появления квантовых компьютеров и сохранить конфиденциальность информации в новой технологической реальности. Как показывает анализ, начать подготовку к этому переходу необходимо уже сегодня, чтобы избежать кризиса безопасности в будущем.

Список литературы

1. Бурмистров Н. В. Научные достижения 2024: гуманитарные и технические науки: сборник материалов LVII-ой международной очно-заочной научно-практической конференции, в 3 т., том 2 / Н. В. Бурмистров. — М.: Издательство НИЦ «Империя», 2024. — 257 с.
2. Вторая Всероссийская научно-техническая конференция «Кибернетика и информационная безопасность «КИБ-2024». Сборник научных трудов. 22-23 октября 2024 г., Москва. — М.: НИЯУ МИФИ, 2024. — 292 с.
3. https://cyberrus.info/wp-content/uploads/2024/08/vokib-2024-4-cc.pdf#page=67
4. Копылов А.Е. Экономические аспекты повышения конфиденциальности данных в блокчейне // Экономика: вчера, сегодня, завтра. — 2024. — Том 14. — № 11А. — С. 449-456. — DOI: 10.34670/AR.2024.52.75.050.
5. Молдовян А.А., Молдовян Д.Н., Молдовян Н.А. Новый подход к разработке алгоритмов многомерной криптографии // Вопросы кибербезопасности. — 2023. — № 2(54). — С. 52–64. DOI: 10.21681/2311-3456-2023-2-52-64.
6. Наседкин П.Н., Сверкунов В.А. Криптографические алгоритмы на пути к постквантовой криптографии // Иркутский государственный университет путей сообщений. — [б. г.]. — [б. м.]. — [б. и.].
7. Петренко А. С. Метод построения постквантовых алгоритмов ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. — 2025. — № 2 (66). — С. 52–63. — DOI: 10.21681/2311-3456-2025-2-52-63.
8. Рыбкин А., Моисеевский А. Квантовый компьютинг: мифы, реалии, прогнозы // CONNECT. — 2021. — № 9–10. — С. 110.
9. Современная наука: эксперимент и научная дискуссия. Сборник научных трудов по материалам XXX Международной научно-практической конференции (г.-к. Анапа, 27 января 2025 г.) / под ред. Скориковой Е.Н. — Анапа: НИЦ ЭСП в ЮФО, 2025. — 51 с.
10. Тельнов Ю. Ф. Инжиниринг предприятий и управление знаниями (ИП&УЗ-2022) : сборник научных трудов XXV Российской научной

конференции (молодежная секция). 6–7 декабря 2022 г. / под науч. ред. Ю. Ф. Тельнова. — Москва : ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2022. — Т. 2. — 328 с.

11. Цифровые технологии и право: сборник научных трудов III Международной научно-практической конференции (г. Казань, 20 сентября 2024 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. — Казань: Изд-во «Познание» Казанского инновационного университета, 2024. — 1 CD-ROM. — EDN: EIVHER. — URL: http://dx.doi.org/10.21202/978-5-8399-0846-8_6.
12. Шкоркина Е. Н. Криптографические наборы протокола аутентификации низкоресурсных устройств в граничной вычислительной архитектуре // Материалы 15-й мультиконференции по проблемам управления. — 2022. — С. 255–256.

literature

1. Burmistrov N. V. Scientific achievements in 2024: humanities and technical sciences: a collection of materials of the LVII international intramural scientific and practical conference, in 3 volumes, volume 2 / N. V. Burmistrov. - M.: Publishing House of SIC "Empire", 2024. - 257 p.
2. The second All-Russian Scientific and Technical Conference "Cybernetics and Information Security "CIB-2024". Collection of scientific papers. October 22-23, 2024, Moscow, Moscow: NRU MEPhI, 2024, 292 p.
3. https://cyberrus.info/wp-content/uploads/2024/08/vokib-2024-4-cc.pdf#page=67
4. Kopylov A.E. Economic aspects of increasing data privacy in the blockchain // Economics: yesterday, today, tomorrow. — 2024. — Volume 14. — No. 11A. — pp. 449-456. — DOI: 10.34670/AR.2024.52.75.050.
5. Moldovyan A.A., Moldovyan D.N., Moldovyan N.A. A new approach to the development of multidimensional cryptography algorithms // Cybersecurity issues. — 2023. — № 2(54). — Pp. 52-64. DOI: 10.21681/2311-3456-2023-2-52-64.

6. Nasedkin P.N., Sverkunov V.A. Cryptographic algorithms on the way to post-quantum cryptography // Irkutsk State University of Communications. — [B. G.]. — [B. M.]. — [B. I.].
7. Petrenko A. S. A method for constructing post-quantum EDS algorithms with two hidden groups // Cybersecurity issues. — 2025. — № 2 (66). — Pp. 52-63. — DOI: 10.21681/2311-3456-2025-2-52-63.
8. Rybkin A., Moiseevsky A. Quantum computing: myths, realities, forecasts // CONNECT. — 2021. — No. 9-10. — p. 110.
9. Modern science: experiment and scientific discussion. Collection of scientific papers based on the materials of the XXX International Scientific and Practical Conference (Anapa, January 27, 2025) / ed. Skorikova E.N. — Anapa: SIC ESP in the Southern Federal District, 2025. — 51 p.
10. Telnov Yu.F. Enterprise Engineering and Knowledge Management (IP&UZ-2022) : proceedings of the XXV Russian Scientific Conference (youth section). December 6-7, 2022 / edited by Yu. F. Telnov. Moscow : Plekhanov Russian University of Economics, 2022, vol. 2, 328 p.
11. Digital technologies and law: proceedings of the III International Scientific and Practical Conference (Kazan, September 20, 2024) / edited by I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova. — Kazan: Publishing house "Cognition" of Kazan Innovation University, 2024. — 1 CD-ROM. — EDN: EIVHER. — URL: http://dx.doi.org/10.21202/978-5-8399-0846-8_6.
12. Shkorkina E. N. Cryptographic authentication protocol sets for low-resource devices in edge computing architecture // Proceedings of the 15th multi-conference on management issues. - 2022. — pp. 255-256.