УДК 004.056.5:004.032.26

Ларин Александр Иванович, кандидат технических наук, доцент, Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», г. Москва

Назаров Михаил Владимирович, магистрант, Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», г. Москва

ИССЛЕДОВАНИЕ КВАНТОВОЙ УГРОЗЫ ДЛЯ СИСТЕМ ЭЛЕКТРОННОЙ ПОДПИСИ, ПРИМЕНЯЕМЫХ ВО ВНУТРЕННЕМ ДОКУМЕНТООБОРОТЕ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Аннотация

Статья посвящена исследованию угроз системам электронной подписи внутреннего документооборота финансовых организаций со стороны квантовых вычислений. Доказана уязвимость современных криптографических алгоритмов (RSA, DSA ECDSA, ГОСТ Р 34.10-2012) перед квантовым алгоритмом Шора. Особое внимание уделено анализу стремительного прогресса в этой области: если в 2019 году для взлома RSA-2048 требовалось 20 млн кубитов, то по данным 2025 года достаточно уже менее 1 млн. Обоснована необходимость срочного перехода на квантово-устойчивые криптографические стандарты для противодействия угрозе HNDL ("собери сейчас, расшифруй позже") и обеспечения долгосрочной безопасности систем электронного документооборота организаций финансового сектора.

Annotation

The article is devoted to the study of threats to the electronic signature systems of internal document management of financial organizations from quantum computing.

The vulnerability of modern cryptographic algorithms (RSA, DSA ECDSA, GOST R 34.10-2012) to the Shor quantum algorithm is proved. Special attention is paid to the analysis of rapid progress in this area: if in 2019 20 million qubits were needed to crack RSA-2048, then according to 2025 data, less than 1 million is enough. The necessity of an urgent transition to quantum-resistant cryptographic standards to counteract the threat of HNDL ("assemble now, decrypt later") and ensure the long-term security of electronic document management systems of financial sector organizations is substantiated.

Ключевые слова: ассиметричная криптография, квантово-уязвимые алгоритмы, квантовое превосходство, квантовый алгоритм Шора, квантовый кубит, квантовая факторизация больших чисел.

Keywords: asymmetric cryptography, quantum vulnerable algorithms, quantum supremacy, Shor's quantum algorithm, quantum qubit, quantum factorization of large numbers.

Электронный документооборот (ЭДО) и связанное с ним использование электронной подписи (ЭП) с каждым годом все сильнее охватывают различные сферы деятельности человека в современном обществе. ЭП является основным инструментом обеспечения юридической значимости ЭДО. ЭП представляет собой цифровой аналог собственноручной подписи, который обеспечивает аутентификацию, целостность и неотказуемость электронных документов в ЭДО организаций различных форм собственности. То же касается и применения ЭП во внутреннем ЭДО финансовых организаций. Технически, ЭП - это информация в электронной форме, присоединенная к другим данным в электронной форме, которая используется для удостоверения личности подписавшего и подтверждения целостности подписанных данных.

В Российской Федерации основным регулирующим документом в этой сфере является Федеральный закон № 63-ФЗ «Об электронной подписи», который четко устанавливает классификацию электронных подписей и их

юридическую силу. В зависимости от уровня защиты и целей использования, выделяются простая, неквалифицированная и квалифицированная электронные подписи (рис. 1), каждая из которых обладает определенной степенью доверия со стороны государственных органов и бизнеса [7, с. 88].

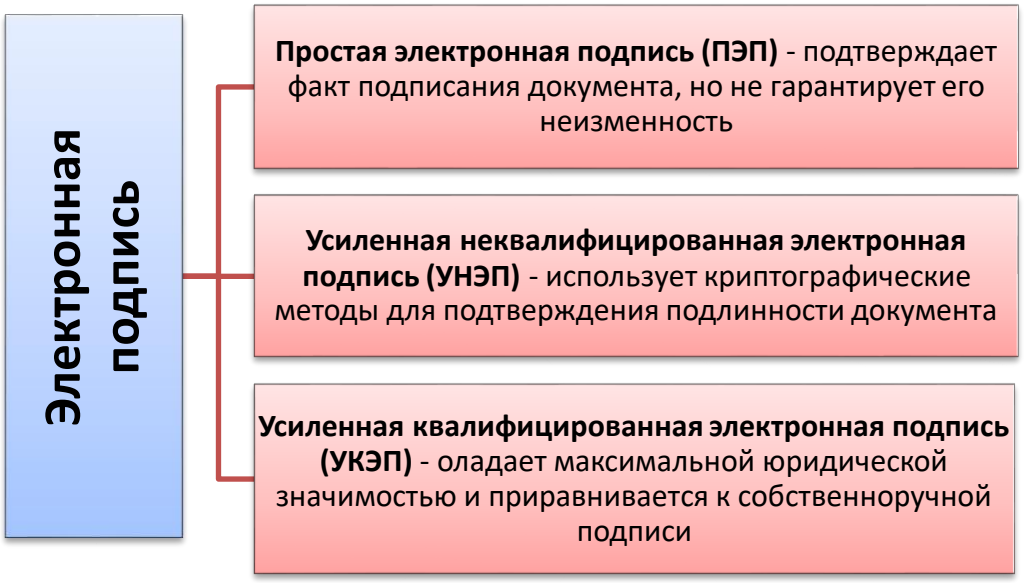

Рис. 1. Классификация ЭП по степени юридической значимости

Касаемо внутреннего ЭДО финорганизаций на примере Российской Федерации: согласно требований Банка России финансовые учреждения при установлении типа ЭП (ПЭП, УНЭП или УКЭП) для тех или иных документов (операций) в соответствующих внутренних регламентах должны действовать риск-ориентированно: чем выше потенциальный риск от компрометации документа (операции), тем строже требования к его подписанию.

Так, документом Банка России «Основные направления цифровизации финансового рынка на 2022–2024 годы» было предусмотрено внедрение инструментов и механизмов для борьбы с киберугрозами и мошенничеством. Головные пункты предусматривали:

- внедрение облачной УКЭП,
- обеспечение поднадзорных организаций УКЭП [3, с. 50].

Очевидно, что во внутреннем ЭДО финансовых организаций к УКЭП устанавливается наибольшее доверие, а это означает, что и риски, связанные с компрометацией УКЭП, самые высокие.

Современные российские и зарубежные системы обеспечения безопасного функционирования усиленной ЭП построены на нескольких криптографических алгоритмах, основанных на значительной вычислительной сложности решения ряда математических задач.

Наиболее популярные классические алгоритмы шифрования, применяемые в мировых системах ЭП, представлены на рис. 2.

Рис. 2. Классические криптографические алгоритмы ЭП

Безопасность современных классических алгоритмов ЭП с точки зрения криптографической стойкости основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш–функции.

На сегодняшний день наиболее распространенными алгоритмами ЭП на основе архитектуры открытых ключей (PKI) являются: устаревший **RSA** (Rivest-Shamir-Adleman), устаревающий **DSA** (Digital Signature Algorithm) и современные **ECC-алгоритмы**: **ECDSA** (Elliptic Curve Digital Signature Algorithm), **SM2** (китайский аналог ECDSA), а также отечественный **ГОСТ Р 34.10-2012** (российский аналог ECDSA).

Взлом каждого из перечисленных алгоритмов для классического компьютера (даже для самого быстродействующего суперкомпьютера в мире) является вычислительно сложным и требующим экспоненциального времени. Так, для взлома ЭП, реализованной на **«RSA-2048»**, потребуется около 100 миллионов лет,

а в том случае, если ЭП защищена криптоалгоритмом **«ECC P-256»** - не менее 6 триллионов лет. Время, требуемое для совершения успешной «атаки» **методом исчерпывающего поиска** с применением классических (не квантовых) компьютеров, является экспоненциальным, то есть увеличение длины ключа приводит к экспоненциальному увеличению требуемого на его «взлом» времени [8, 9]. Тем самым обеспечивается безопасность современных, основанных на классической ассиметричной криптографии алгоритмов ЭП, в том числе используемых в отечественных и зарубежных системах внутреннего ЭДО финансовых организаций.

В последнее десятилетие в мире наблюдается активное развитие квантовых вычислений. Фактически, набирает обороты «квантовая гонка»: ряд крупнейших IT – компаний работает над созданием полномасштабных квантовых компьютеров – вычислительных устройств, которые используют явления квантовой механики (суперпозицию, запутанность, интерференцию) для обработки информации. В 2019 году компания Google объявила о достижении квантового превосходства, когда их процессор за 200 секунд выполнил расчёт, который классическому суперкомпьютеру потребовал бы 10 тысяч лет [2, с. 35]. Ключевой особенностью квантовой ЭВМ является ее способность находиться в квантовой суперпозиции и использовать квантовую запутанность для выполнения вычислений. Основным логическим элементом квантового компьютера является кубит. В табл. 1 приведена сравнительная характеристика классического бита и квантового кубита.

Таблица 1. Сравнение бита и кубита

Критерий сравнения	**Классический бит**	**Квантовый кубит**
Основное состояние	Находится только в одном из двух возможных состояний: **«0» или «1»**	Может находиться в **суперпозиции** состояний: одновременно **«0» и «1»**, с определенной вероятностью
Количество состояний	1 бит кодирует 1 состояние: **«0» или «1»**	1 кубит кодирует 2 вероятностных состояния: **«0» и «1»**
Масштабирование	N бит кодирует **1 состояние из 2^N** возможных	N кубит кодируют **сразу все 2^N** состояний одновременно (в суперпозиции)
Принцип работы	Основан на законах **классической физики** (ток есть	Основан на законах **квантовой механики** (суперпозиция, запутанность, интерференция)

	или нет, напряжение высокое или низкое)	
Обработка информации	Вычисления производятся **последовательно**, перебирая варианты	Возможность квантового параллелизма – вычисления над множеством состояний производятся **одновременно**
Считывание (измерение)	При измерении значение бита **не изменяется**	При измерении суперпозиция **разрушается (коллапсирует)** в одно конкретное состояние. Вся промежуточная информация утрачивается
Взаимосвязь	Бит **не зависит** от состояния других битов	Кубиты находятся в состоянии **квантовой запутанности**. Состояние одного кубита мгновенно коррелирует с состоянием другого даже на расстоянии
Основное преимущество	Надежность, предсказуемость, относительная простота создания и управления	Экспоненциальная вычислительная мощность для специфических задач, невозможных для классических компьютеров
Физическая реализация	Транзисторы, конденсаторы, ячейки памяти	Ионы, сверхпроводящие цепи, квантовые точки, фотоны и др.

Таким образом, наиважнейшим вычислительным преимуществом квантовых компьютеров является **масштабирование**:

- **100 классических бит** могут хранить лишь какое-то одно значение длиною в 100 бит, представляющее собой **одно из 2^{100}** возможных значений;

- тогда как **100 квантовых кубит** могут находиться в суперпозиции, которая представляет **сразу все 2^{100}** возможных состояний.

Одно из важнейших свойств квантовых вычислений заключается в возможности факторизации больших чисел с применением квантового алгоритма Шора за полиноминальное время [6, с. 59]. Квантовый алгоритм Шора предназначен для решения задачи факторизации большого числа $N = 2^n$ и имеет полиномиальную вычислительную сложность $O(n^3)$, где n – количество бит числа. Это делает алгоритм ECDSA, основанный на сложности решения проблемы дискретного логарифмирования, неустойчивым при наличии достаточного количества логических кубитов [1, с. 74].

Сегодня злоумышленники используют машинное обучение и искусственный интеллект для совершения кибератак, но с квантовыми вычислениями находить уязвимости в программном обеспечении и ИТ-инфраструктурах будет намного проще. Многие субъекты угроз занимаются поиском конфиденциальных данных и сохранением защищенной информации

до тех пор, пока квантовые вычисления не станут готовым инструментом для применения. Как только это произойдет, накопленная конфиденциальная информация может быть расшифрована и использована по усмотрению хакера [4, с. 13]. Этот распространенный метод атаки на зашифрованные конфиденциальные данные, ориентированный на появление в будущем квантовых вычислений, называется HNDL (Harvest Now, Decrypt Later – «Собери сейчас, расшифруй позже»). При этом, эксперты международной консалтинговой компании McKinsey предполагают, что **к 2030 г. появятся квантовые компьютеры** достаточной мощности для успешного криптоанализа («взлома») реально применяемых сегодня во всем мире классических асимметричных криптоалгоритмов [5, с. 29].

Квантовые вычисления также представляют серьезную угрозу для ЭП, которые основаны на тех же криптографических принципах, что и шифрование конфиденциальных данных. **Теоретическая уязвимость** современных алгоритмов ЭП, таких как RSA и ECDSA, перед атакой с использованием квантового компьютера была математически доказана Питером Шором еще в 1994 году [12]. ЭП служат для проверки источника и целостности сообщений, предотвращая таким образом несанкционированные изменения. **Квантовый алгоритм Шора ставит под угрозу подлинность и неотказуемость**, предоставляемые ЭП. При наличии квантового компьютера позволит злоумышленникам извлекать закрытые ключи и подделывать ЭП, аннулируя юридическую значимость последних.

Мировое криптографическое сообщество регулярно проводит теоретические исследования для оценки необходимой мощности квантового вычислителя и требуемого времени для «взлома» квантово-уязвимых алгоритмов шифрования. Одно из последних исследований показывает, что за счет постоянного процесса усовершенствования математических подходов, например - алгоритмов факторизации больших чисел, снижаются требования к минимальной требуемой вычислительной мощности квантовой ЭВМ для успешной реализации алгоритма Шора против RSA -, DSA - и ECC -

алгоритмов. Так, если в 2019 году исследователи опубликовали оценку, согласно которой 2048-битные числа RSA могут быть разложены на множители **за восемь часов с помощью квантового компьютера с 20 миллионами** зашумлённых кубит [11], то в недавнем исследовании 2025 года ожидаемое количество кубит, необходимых для взлома RSA-2048 **менее чем за неделю**, сокращено с 20 миллионов **до 1 миллиона** (рис. 3) [10].

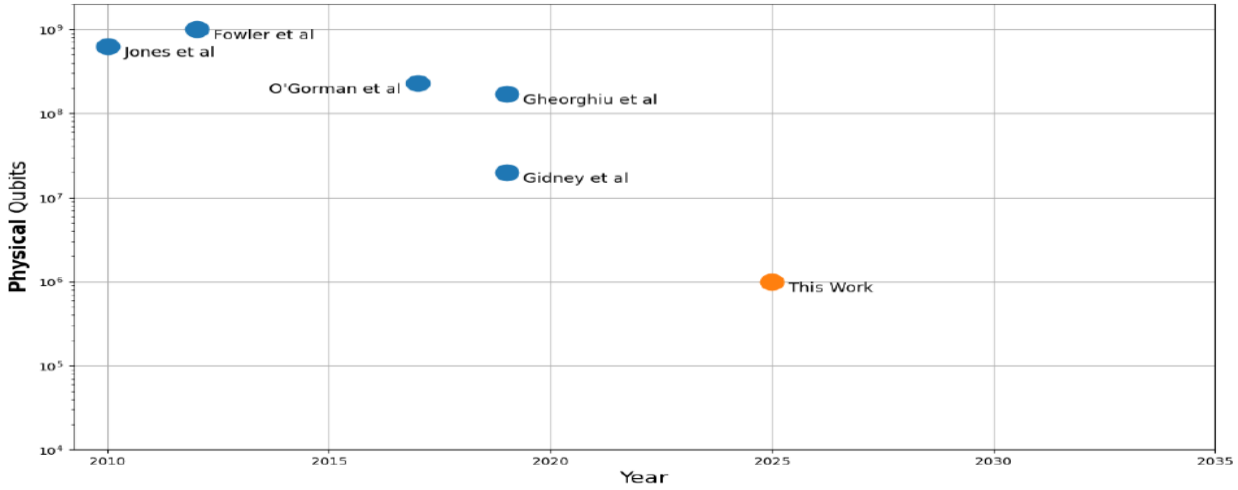

Рис. 3. Историческая оценка необходимого количества кубит в квантовом процессоре для факторизации RSA-2048 [10]

Приведенные оценки исследователей теоретически доказывают возможность взлома RSA -, DSA - и ECC - алгоритмов за практически приемлемое время (часы, дни) при наличии достаточно мощного квантового процессора и подтверждают актуальность квантовой угрозы для современной ассиметричной криптографии в общем, и для широко используемых сегодня в мире алгоритмов ЭП, в частности.

Развитие квантовых вычислений создает экзистенциальную угрозу для основанных на асимметричной криптографии систем электронной подписи, являющихся основой и гарантом юридической значимости внутреннего документооборота финансовых организаций.

Квантовый алгоритм Шора, теоретически позволяющий взломать такие криптоалгоритмы, как RSA, ECDSA и ГОСТ Р 34.10-2012, за приемлемое время, перестает быть сугубо теоретической проблемой, о чем

свидетельствует стремительное сокращение в научных оценках количества кубит, необходимых для успешной атаки.

Угроза стратегии «Harvest Now, Decrypt Later» и высокая концентрация рисков в финансовом секторе требуют безотлагательных превентивных мер уже сегодня, в частности: разработки и скорейшего перехода на квантово-устойчивые криптографические алгоритмы для обеспечения долгосрочной безопасности и юридической значимости систем ЭДО.

Литература

1. Балябин Артём Алексеевич, Петренко Сергей Анатольевич Модель блокчейн-платформы с кибериммунитетом в условиях квантовых атак // Вопросы кибербезопасности. 2025. №3 (67). DOI: 10.21681/2311-3456-2025-3-72-82.
2. Белослудцев Н. В., Гаев Л. В. Основы квантовых компьютеров и их потенциальное применение // Инновационная наука. 2025. №4-2. URL: https://cyberleninka.ru/article/n/osnovy-kvantovyh-kompyuterov-i-ih-potentsialnoe-primenenie (дата обращения: 05.10.2025).
3. Буевич А.П. Киберугрозы как современный вызов безопасности банковского сектора в России // Национальная безопасность / nota bene. 2025. № 4. DOI: 10.7256/2454-0668.2025.4.74921 URL: https://nbpublish.com/ library_read_article.php?id=74921 (дата обращения: 05.10.2025).
4. Булатова Алина Рустемовна Квантовая криптография и квантовые вычисления // Вестник ПензГУ. 2025. №1 (49). URL: https://cyberleninka.ru/article/n/kvantovaya-kriptografiya-i-kvantovye-vychisleniya (дата обращения: 05.10.2025).
5. Панасенко С. П. О применимости постквантового стандарта электронной подписи SLH-DSA в смарт-картах // Вопросы кибербезопасности. – 2025. – №. 3 (67). – С. 29-37. DOI: 10.21681/2311-3456-2025-3-29-37.

6. 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.
7. Сапаров Д. К. Правовое регулирование электронного документооборота и цифровых подписей //Холодная наука. – 2025. – №. 14. – С. 86-107.
8. Bernstein, D.J., Lange, T. Post-quantum cryptography. Nature 549, 2017. – С. 188–194. DOI: 10.1038/nature23461.
9. Focardi R., Luccio F. L., Wahsheh H. A. M. Security threats and solutions for two-dimensional barcodes: a comparative study //Computer and network security essentials. – Cham : Springer International Publishing, 2017. – С. 207-219. DOI: 10.1007/978-3-319-58424-9_12.
10. Gidney C. How to factor 2048 bit RSA integers with less than a million noisy qubits //arXiv preprint arXiv:2505.15917. – 2025. DOI: 10.48550/arXiv.2505.15917.
11. Gidney C., Ekerå M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits //Quantum. – 2021. – Т. 5. – С. 433. DOI: 10.48550/arXiv.1905.09749.
12. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer //SIAM review. – 1999. – Т. 41. – №. 2. – С. 303-332.

Literature

1. Balyabin Artem Alekseevich, Petrenko Sergey Anatolyevich A model of a blockchain platform with cyberimmunity in the context of quantum attacks // Cybersecurity issues. 2025. No. 3 (67). DOI: 10.21681/2311-3456-2025-3-72-82.
2. Belosludtsev N. V., Gaev L. V. Fundamentals of quantum computers and their potential applications // Innovative Science. 2025. No. 4-2. URL: https://cyberleninka.ru/article/n/osnovy-kvantovyh-kompyuterov-i-ih-potentsialnoe-primenenie (date of request: 05.10.2025).

3. Buevich A.P. Cyber threats as a modern challenge to the security of the banking sector in Russia // National security / nota bene. 2025. № 4. DOI: 10.7256/2454-0668.2025.4.74921 URL: https://nbpublish.com / library_read_article.php?id=74921 (accessed 05.10.2025).
4. Bulatova Alina Rustemovna Quantum cryptography and quantum Computing // Bulletin of Penza State University. 2025. No. 1 (49). URL: https://cyberleninka.ru/article/n/kvantovaya-kriptografiya-i-kvantovye-vychisleniya (date of request: 05.10.2025).
5. Panasenko S. P. On the applicability of the SLH-DSA post-quantum electronic signature standard in smart cards // Cybersecurity issues. – 2025. – №. 3 (67). – Pp. 29-37. DOI: 10.21681/2311-3456-2025-3-29-37.
6. 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.
7. Saparov D. K. Legal regulation of electronic document management and digital signatures //Cold Science. – 2025. – №. 14. – Pp. 86-107.
8. Bernstein, D.J., Lange, T. Post-quantum cryptography. Nature 549, 2017. – pp. 188-194. DOI: 10.1038/nature23461.
9. Focardi R., Luccio F. L., Wahsheh H. A. M. Security threats and solutions for two-dimensional barcodes: a comparative study //Computer and network security essentials. – Cham : Springer International Publishing, 2017. pp. 207-219. DOI: 10.1007/978-3-319-58424-9_12.
10. Gidney C. How to factor 2048 bit RSA integers with less than a million noisy qubits //arXiv preprint arXiv:2505.15917. – 2025. DOI: 10.48550/arXiv.2505.15917.
11. Gidney C., Ekerå M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits //Quantum. – 2021. – Vol. 5. – p. 433. DOI:10.48550/arXiv.1905.09749.

12. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer //SIAM review. – 1999. – Vol. 41. – No. 2. – pp. 303-332.