УДК 004.056.53
DOI: 10.26102/2310-6018/2025.49.2.019

Квантовые алгоритмы и угрозы кибербезопасности

А.В. Козачок[1], С.С. Тарасенко[2]✉, А.В. Козачок[1]

[1]МИРЭА – Российский технологический университет, Москва, Российская Федерация
[2]Академия Федеральной службы охраны Российской Федерации, Орёл, Российская Федерация

Резюме. Целью написания данной статьи является оценка потенциальных угроз для кибербезопасности, вызванных развитием квантовых алгоритмов. В тексте работы осуществляется анализ существующих квантовых алгоритмов, таких как алгоритм Шора и алгоритм Гровера, и исследуется возможность их потенциального применения в контексте взлома существующих криптографических систем. Методология проводимого исследования заключается в анализе литературы, а также рассмотрении основных принципов функционирования квантовых вычислителей и потенциала реализации квантовых алгоритмов, способных влиять на безопасность как симметричных, так и асимметричных криптографических схем. Кроме того, в исследовании анализируются перспективы создания криптографических алгоритмов, способных противостоять атакам с применением квантовых технологий. На основе анализа существующих квантовых алгоритмов и их потенциального воздействия на широко распространенные в настоящее время криптографические системы, авторы исследования приходят к выводу, что на текущий момент отсутствуют убедительные основания для констатации реальной возможности взлома ассиметричных или симметричных криптографических алгоритмов в ближайшее время в контексте квантовых вычислений. Однако, учитывая постоянное развитие квантовых технологий, а также необходимость сохранения конфиденциальности сведений, актуальность которых с течением времени не будет претерпевать значительное снижение, и необходимость обеспечения защиты конфиденциальной информации в будущем, требуется разработка и активное внедрение квантово-устойчивых криптографических методов для обеспечения конфиденциальности информации в долгосрочной перспективе.

Ключевые слова: постквантовая криптография, алгоритм Шора, алгоритм Гровера, асимметричная криптография, симметричная криптография, квантовые вычислители, сохранение конфиденциальности информации.

Для цитирования: Козачок А.В., Тарасенко С.С., Козачок А.В. Квантовые алгоритмы и угрозы кибербезопасности. *Моделирование, оптимизация и информационные технологии.* 2025;13(2). URL: https://moitvivt.ru/ru/journal/pdf?id=1878 DOI: 10.26102/2310-6018/2025.49.2.019.

Quantum algorithms and cybersecurity threats

A.V. Kozachok[1], S.S. Tarasenko[2]✉, A.V. Kozachok[1]

[1]MIREA – Russian Technological University, Moscow, the Russian Federation
[2]Academy of Federal Guard Service of the Russian Federation, Oryol, the Russian Federation

Abstract. The purpose of this article is to assess potential threats to cybersecurity arising from the development of quantum algorithms. The text analyzes existing quantum algorithms, such as Shor's algorithm and Grover's algorithm, and explores the possibility of their potential application in the context of compromising existing cryptographic systems. The research approach includes a literature review and examination of core mechanisms underlying quantum computers, along with assessment of their capability to perform algorithms potentially affecting various cryptographic systems, both symmetric and asymmetric. Additionally, the paper discusses the prospects for developing quantum-resistant cryptographic algorithms aimed at protecting against cryptanalysis using quantum

computations. Based on the analysis of existing quantum algorithms and their potential impact on widely used cryptographic systems, the authors of the study conclude that, at present, there is no compelling evidence to assert the real possibility of compromising asymmetric or symmetric cryptographic algorithms in the near future within the context of quantum computations. However, considering the ongoing development of quantum technologies and the necessity of maintaining the confidentiality of information, the relevance of which will not significantly diminish over time, as well as the need to ensure the protection of confidential information in the future, there is a requirement for the development and active implementation of quantum-resistant cryptographic methods to ensure information confidentiality in the long term.

Keywords: post-quantum cryptography, Shor's algorithm, Grover's algorithm, asymmetric cryptography, symmetric cryptography, quantum computers, confidentiality preservation of information.

For citation: Kozachok A.V., Tarasenko S.S., Kozachok A.V. Quantum algorithms and cybersecurity threats. *Modeling, Optimization and Information Technology*. 2025;13(2). (In Russ.). URL: https://moitvivt.ru/ru/journal/pdf?id=1878 DOI: 10.26102/2310-6018/2025.49.2.019

Введение

В контексте стремительного развития квантовых вычислений в последние десятилетия вопросы кибербезопасности приобретают новый уровень значимости. Наступление эпохи квантовых компьютеров несет с собой потенциальные вызовы для традиционных методов криптографии, в частности для ассиметричных и симметричных криптографических алгоритмов. В связи с этим вопрос рассмотрения и анализа существующих на данный момент квантовых алгоритмов и их влиянии на стойкость современных криптографических систем является актуальным.

Целью написания данной статьи является оценка потенциальных угроз для кибербезопасности, вызванных развитием квантовых алгоритмов. Для осуществления данной оценки на основе обзора и анализа различных литературных источников необходимо решить ряд задач: произвести обзор фундаментальных принципов, лежащих в основе квантовых вычислений; провести анализ различий между физическими и логическими кубитами, а также анализ последних практических достижений в области квантовых вычислителей; исследовать новые актуальные квантовые алгоритмы и их влияние на современные криптографические примитивы; осуществить обзор текущих разработок в области криптографических алгоритмов, устойчивых к квантовым атакам.

Таким образом, статья призвана рассмотреть и проанализировать проблемы, которые могут возникнуть в связи с использованием квантовых вычислителей для взлома классической криптографии, а также дать оценку степени уязвимости существующих криптографических систем перед квантовыми алгоритмами в краткосрочной и долгосрочных перспективах.

Материалы и методы

Квантовый вычислитель. Квантовый компьютер представляет собой вычислительную машину, базирующуюся на принципах квантовой механики и использующую при обработке и транспортировке данных принципы квантовой суперпозиции и квантовой запутанности. Единицей информации, которой оперирует вычислительное устройство, построенное на принципах квантовой физики, является кубит, способный иметь значение одновременно и нуля, и единицы, в то время как бит – единица хранимой информации, используемая на классических электронно-вычислительных машинах (ЭВМ), способен в один момент времени иметь либо только значение единицы, либо только нуля.

Одновременное нахождения кубита в состоянии нуля $|0\rangle$ и в состоянии единицы $|1\rangle$ называется суперпозицией. Состояние суперпозиции кубита описывается волновой функцией, представленной формулой:

$$\psi = F_1 \cdot |0\rangle + F_2 \cdot |1\rangle, \quad (1)$$

где F_1, F_2 – амплитудные вероятности, представленные комплексными числами, которые удовлетворяют условию:

$$|F_1|^2 + |F_2|^2 = 1. \quad (2)$$

На Рисунке 1 представлено графическое изображение кубита в виде сферы Блоха[1].

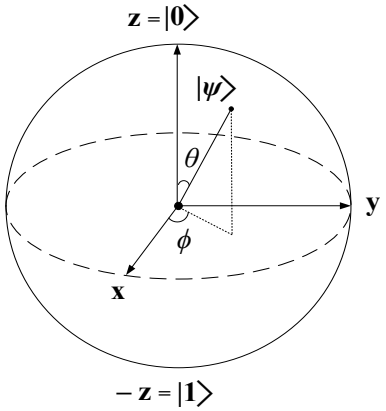

Рисунок 1 – Графическое представление кубита
Figure 1 – Graphical representation of a qubit

Амплитудные вероятности вычисляются следующим образом:

$$F_1 = cos(\frac{\theta}{2}),\ F_2 = e^{i\phi}\, sin(\frac{\theta}{2}). \quad (3)$$

При измерении состояния кубита (путем проведения физического эксперимента) его суперпозиция коллапсирует к одному из состояний: либо $|0\rangle$, либо $|1\rangle$. Вероятность $P_{|0\rangle}$ получить при измерении $|0\rangle$ равна:

$$P_{|0\rangle} = |F_1|^2, \quad (4)$$

а вероятность $P_{|1\rangle}$ получить при измерении $|1\rangle$ равна:

$$P_{|1\rangle} = |F_2|^2. \quad (5)$$

Принцип квантовой запутанности заключается в наличии корреляции между состояниями двух или более кубитов. Состояние Белла[2] $|\Phi^+\rangle$ иллюстрирует явление запутанности состояний двух кубитов следующим образом:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle). \quad (6)$$

Обозначение $|00\rangle$ указывает на то, что оба кубита находятся в состоянии $|0\rangle$, обозначение $|11\rangle$ на то, что оба кубита находятся в состоянии $|1\rangle$.

[1] Нильсен М., Чанг И. *Квантовые вычисления и квантовая информация.* Москва: Мир; 2006. 824 с.
[2] Кайе Ф., Лафламм Р., Моска М. *Введение в квантовые вычисления.* Москва–Ижевск: НИЦ «Регулярная и хаотическая динамика», Институт компьютерных исследований; 2009. 360 с.

Измерение состояния 1-го кубита может дать результат 0 с вероятностью 50 % и итоговым состоянием двух кубитов $|00\rangle$, либо результат 1 с вероятностью 50 % и итоговым состоянием двух кибитов $|11\rangle$. Это позволяет сделать вывод, что измерение состояния 2-го кубита всегда даст результат аналогичный результату, полученному при измерении 1-го кубита, а, следовательно, сделать вывод о том, что состояния 1-го и 2-го кубитов взаимосвязаны. Состояние Белла можно получить, подав на вход квантовой схемы[3], представленной на Рисунке 2, два кубита с заведомо известным состоянием $|0\rangle$.

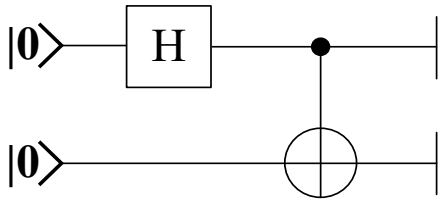

Рисунок 2 – Квантовая схема для запутывания кубитов в состояние Белла
Figure 2 – A quantum circuit for entangling quibits into a Bell state

Большинство классических ЭВМ устроены по следующему принципу: в n_q битах оперативной памяти (англ. *Random-access memory, RAM*) хранятся n_q состояний, модифицируемых центральным процессором (англ. *central processing unit*, *CPU*) за один такт времени.

Квантовый компьютер, имеющий n_q кубит в квантовой памяти (англ. *Quantum random-access memory, QRAM*) хранит 2^{n_q} состояний (вследствие действия принципа суперпозиции состояний в квантовых системах), которые также периодически изменяются за один такт времени.

Таким образом, теоретически, квантовый компьютер может обеспечить экспоненциальный прирост вычислительной мощности относительно классических вычислений.

Квантовые алгоритмы. Наибольшую угрозу для безопасности использования существующих криптографических систем представляют два алгоритма.

Первый – алгоритм Гровера. Данный квантовый алгоритм применяется для решения задачи перебора, формально сводящейся к решению следующего уравнения:

$$f_b(x) = 1, \tag{7}$$

где $f_b(x)$ – булева функция от N_v переменных величин.

Функция $f_b(x)$ – оракул[4]. Алгоритм Гровера заключается в многократном вызове данной функции при различных значениях x и использовании полученных значений для осуществления последующих вычислений. Таким образом, вычисление функции $f_b(x)$ – решение задачи перебора. На классической ЭВМ для решения данной задачи необходимо осуществить 2^{n_q} обращений к функции-оракулу $f_b(x)$, в то время как на квантовом компьютере, имеющем n_q кубитов, согласно [1] необходимо осуществить $\frac{\pi}{4}\sqrt{N_v}$ обращений к $f_b(x)$. Таким образом, решение задачи перебора с применением квантового алгоритма Гровера дает квадратичное ускорение в поиске решения

[3] Williams C.P. Quantum Gates. In: *Explorations in Quantum Computing.* London: Springer; 2011. P. 51–122. https://doi.org/10.1007/978-1-84628-887-6_2

[4] Bellare M., Rogaway Ph. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In: *CCS '93: Proceedings of the 1st ACM Conference on Computer and Communications Security, 03–05 November 1993, Fairfax, Virginia, USA.* New York: Association for Computing Machinery; 1993 P. 62–73. https://doi.org/10.1145/168588.168596

относительно классической ЭВМ. Данный факт позволяет сделать вывод о том, что алгоритм Гровера может быть использован для ускоренного решения *NP*-полных задач, однако без достижения полиномиального ускорения, необходимого для перевода решаемой задачи в разряд *P*-задач (англ. *Polynomial*).

Из этого следует, что алгоритм Гровера [2] может быть использован для ускоренного перебора ключей шифрования, применяемых в симметричных и асимметричных криптосистемах [3, 4]. Для сохранения имеющийся стойкости криптографических систем при переборе ключей с помощью квантового алгоритма Гровера размеры ключей шифрования необходимо увеличить в 2 раза, так как прирост длины ключа вдвое компенсирует квадратичное ускорение решения задачи перебора [5].

Второй квантовый алгоритм, представляющий угрозу безопасности современных криптосистем, – алгоритм Шора [6]. Данный квантовый алгоритм применяется для решения задачи факторизации целых чисел, лежащей в основе асимметричного алгоритма шифрования *RSA*. При условии, что квантовый компьютер имеет $log(M_q)$ логических кубитов, алгоритм Шора реализует разложение числа M_q с вычислительной сложностью $O(log^3 M_q)$, за полиномиальное время, в отличие от вычислительной сложности решения задачи факторизации методом перебора возможных делителей числа M_q на классической ЭВМ равной $O(\sqrt{n_q}\, log^2 n_q)$[5].

Полное описание квантового алгоритма Шора приведено в [7].

Задача дискретного логарифмирования, лежащая в основе другого алгоритма асимметричной криптографии – Диффи-Хэллмана, также решается с помощью алгоритма Шора за полиномиальное время.

Среди последних достижений в данной области следует выделить алгоритм факторизации, предложенный О. Регевым, который демонстрирует более высокую эффективность по сравнению с алгоритмом Шора [8]. Кроме того, за последние полтора десятилетия разработан широкий спектр методов, сокращающих время криптоанализа симметричных алгоритмов, включая: квантовые атаки на криптографические конструкции с закрытым ключом [9]; эффективные распределенные квантовые вычисления [10]; ускоренный поиск коллизий для режимов работы шифров, предназначенных для проверки целостности и подлинности [11], с использованием алгоритма Саймона [12]; квантовые атаки на основе знания криптоаналитиком открытого текста [13]; квантовые линейный и дифференциальный криптоанализ [14]; квантовые атаки со связанными ключами [15]; квантовые атаки на блочные шифры Фейстеля [16]; квантовая атака *Meet-in-the-Middle* [17]; квантовая атака с восстановлением ключа с более чем квадратичным сокращением по времени в сравнении с лучшей классической атакой подобного типа [18]; использование квантовых алгоритмов для улучшения невозможных дифференциальных атак на симметричные шифры [19]; увеличение точности восстановления ключей в симметричных шифрах при использовании квантовой нейронной сети Хопфилда (англ. *Quantum Hopfield Neural Network, QHopNN*) [20], поиск ключа для квантовой версии шифра *Even-Mansour* за полиномиальное время [21], расширенная скользящая атака на криптосистему *Even-Mansour* [22], квантовое восстановление ключа в полном *AEZ* [23] и др. [24, 25].

Обзор достижений в области создания квантовых вычислителей. На данном этапе необходимо пояснить принципиальную разницу между логическими и физическими кубитами. Логический кубит – это абстракция, предоставляющая средства для разработки и понимания алгоритмов квантовых вычислений независимо от

[5] Нестеренко А.Ю. *Теоретико-числовые методы в криптографии.* Москва: Московский государственный институт электроники и математики; 2012. 224 с.

технических деталей, а физический кубит – представляет собой конкретную физическую систему, способную реализовать квантовые свойства. Это может быть, например, квантовый бит в квантовом компьютере, реализованный через квантовые системы, такие как кубиты на основе квантовых точек или сверхпроводящие кубиты. В отличие от логических кубитов, физические кубиты чувствительны к внешнему воздействию, такому, например, как тепловые флуктуации и шум, что требует разработки методов коррекции ошибок. В зависимости от используемой схемы исправления ошибок и частоты ошибок каждого физического кубита, один логический кубит может состоять из множества физических кубитов.

Одной из последних значимых разработок в области квантовых вычислителей общего назначения является создание инженерами компании *IBM* квантового процессора «*Kondor*» с 1121 кубитом. Необходимо отметить, что простое количество кубитов не является «универсальной» мерой качества и применимости квантовых вычислителей для выполнения различных типов задач. Учитывается также частота ошибок при вычислениях – компания *IBM* также выпустила квантовый процессор «*Heron*» со 133 кубитами, но с очень низкой частотой ошибок вычислений[6].

Также учитывается применимость квантового вычислителя для «общего назначения». Так, например, компания *D-Wave Systems* заявляет о создании квантового компьютера с 5000 кубитами[7], однако данный вычислитель может быть использован только для решения узкого класса задач[8].

Оценки времени взлома разнятся в различных работах в зависимости от используемого подхода. Согласно исследованию [26] для взлома *RSA* с 2048-битным ключом за 8 часов необходимо 20 миллионов физических кубитов (в которых уже учтена коррекция ошибок). В другой работе [27] заявляется, что достаточно лишь 13436 кубитов и 177 дней, но с условием, что будут использоваться миллионы единиц квантовой памяти *QRAM*, что также еще не реализовано на практике.

Постквантовые криптографические алгоритмы. На данный момент существует большое количество квантовых алгоритмов [28, 29], имеющих потенциальное применение в различных областях, например, таких как решение дифференциальных уравнений [30]. Доказано, что любой алгоритм, реализуемый на классической ЭВМ, возможно реализовать на квантовом компьютере [31]. Однако не любой классический алгоритм можно реализовать с использованием квантовых вычислений, получив при этом увеличение скорости выполнения алгоритма [32].

Научное сообщество осознало, что как только квантовые компьютеры достигнут необходимых вычислительных мощностей, асимметричная криптография в том виде, в котором она существует на данный момент, станет неэффективной или вовсе будет неспособна обеспечить необходимый уровень стойкости шифрования для защиты передаваемых данных. Привлечение внимания общественности к этой проблеме началось с серии конференций *Post-quantum cryptography* (*PQCrypto*)[9] с начала 2006 года. На конференции *PQCrypto* 2016 было объявлено о конкурсе на постквантовый (устойчивый к криптоанализу с помощью квантовых вычислений [33]) стандарт

[6] IBM Quantum System Two: the era of quantum utility is here | IBM Quantum Computing Blog. IBM. URL: https://www.ibm.com/quantum/blog/quantum-roadmap-2033/ (дата обращения: 30.01.2024).
[7] TechRepublic: D-Wave Announces 5,000-Qubit Fifth Generation Quantum Annealer. D-Wave Quantum. URL: https://www.dwavesys.com/company/newsroom/media-coverage/techrepublic-d-wave-announces-5-000-qubit-fifth-generation-quantum-annealer/ (дата обращения: 30.01.2024).
[8] Russell J. D-Wave Embraces Gate-Based Quantum Computing; Charts Path Forward. HPCwire. URL: https://www.hpcwire.com/2021/10/21/d-wave-embraces-gate-based-quantum-computing-charts-path-forward/ (дата обращения: 30.01.2024).
[9] Computer Security Resource Center. Post-Quantum Cryptography. National Institute of Standards and Technology. URL: https://www.nist.gov/pqcrypto (дата обращения: 30.01.2024).

асимметричной криптографии, включая и новый стандарт электронно-цифровой подписи.

На данный момент разработано большое количество постквантовых алгоритмов криптографии, позволяющих осуществлять защищенную коммуникацию в условиях применения криптоаналитиками квантовых вычислений для криптоанализа.

Наиболее известными устойчивыми к квантовым вычислениям криптографическими алгоритмами являются (Рисунок 3):

1) Криптографические алгоритмы, основанные на хеш-функциях [34];
2) Криптографические алгоритмы, основанные на кодах исправления ошибок [35, 36];
3) Криптографические алгоритмы, основанные на решётках [37, 38];
4) Криптографические алгоритмы, основанные на многомерных квадратичных системах [39];
5) Криптографические алгоритмы с секретным ключом [40];
6) Криптографические алгоритмы, основанные на использовании суперсингулярных изогений [41, 42], в том числе с использованием суперсингулярных изогенических графов [43];
7) Криптографические алгоритмы, основанные на искусственных нейронных сетях [44, 45], в том числе применяемые для выработки общих ключей шифрования [46].

5 июля 2022 года был завершен 3-й раунд конкурса и *NIST* объявил первую группу победителей, которыми являются криптографические алгоритмы, основанные на решетках и на основе хеш-функций[9].

Представителем отечественных постквантовых криптографических алгоритмов является алгоритм электронной подписи «Шиповник»[10], открытая реализация которого представлена в публичном *GitHub*-репозитории[11].

Обсуждение

Несмотря на то, что с математической точки зрения асимметричные криптографические алгоритмы, сложность вскрытия которых основана на задачах факторизации больших целых чисел и дискретного логарифмирования, можно считать взломанными (при условии использования квантовых вычислителей для проведения криптоаналитических атак), на практике осуществление данной атаки в ближайшее время не представляется возможным в связи со сложностью инженерной задачи, заключающейся в технической реализации квантового вычислителя, способного одновременно удерживать в связанном состоянии достаточное количество кубитов для взлома современных асимметричных шифров с принятыми для них на данный момент длинами ключей.

Таким образом, основываясь на последних исследованиях, доступных в открытом доступе, а также известном мировому сообществу уровне развития квантовых вычислителей, существующему на сегодняшний день, можно прийти к выводу, что вероятность появления квантового компьютера, способного существенно ослабить защиту современных симметричных и асимметричных шифров, оценивается как низкая в ближайшем будущем.

Несмотря на то, что в ближайшей перспективе квантовые технологии не несут значительной угрозы приватности данных, в будущем такая угроза становится реальной

[10] От Штерна до «Шиповника»: как изменится ЭЦП в постквантовую эру. Криптонит. URL: https://kryptonite.ru/articles/how-eds-will-change-in-the-post-quantum-era/ (дата обращения: 30.01.2024).
[11] QAPP-tech/shipovnik_tc26: Открытая реализация алгоритма ЭЦП Шиповник для ТК26. GitHub. URL: https://github.com/QAPP-tech/shipovnik_tc26/ (дата обращения: 30.01.2024).

и требует своевременного реагирования. В области асимметричной криптографии рекомендуется переходить на использование стандартизированных решений в области постквантовой криптографии, а в области симметричной – учитывать период актуальности зашифровываемой информации и выбирать алгоритмы и параметры шифрования, способные обеспечить требуемый уровень криптографической стойкости в течение данного периода с учетом роста вычислительных мощностей квантовых вычислителей и существующих на сегодняшний день методов квантового криптоанализа симметричных криптопримитивов.

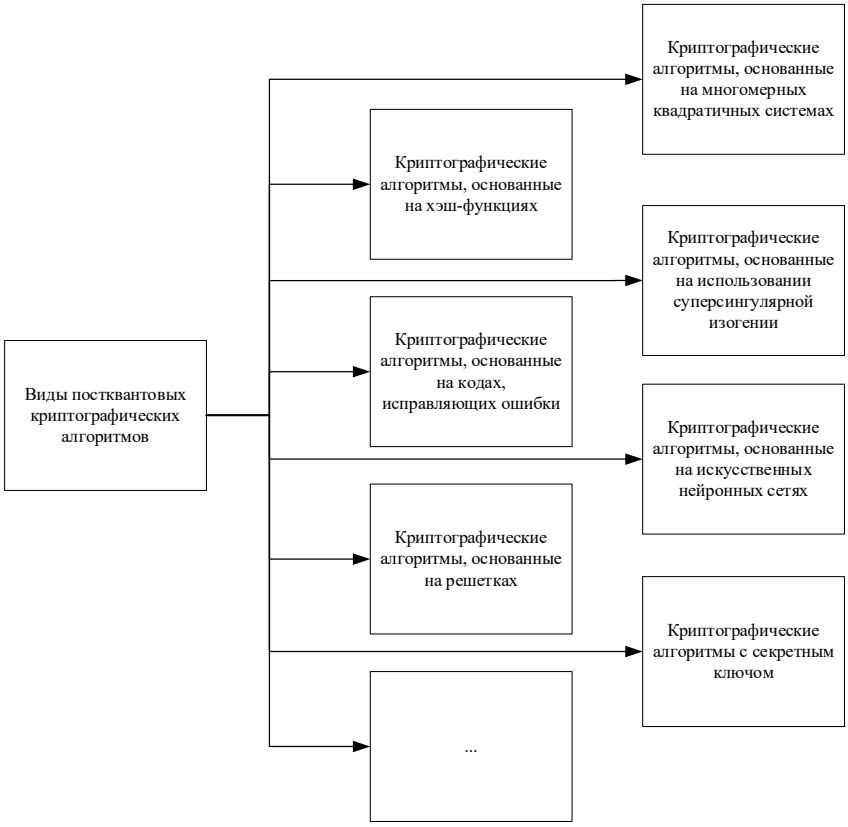

Рисунок 3 – Постквантовые алгоритмы криптографии
Figure 3 – Post-quantum cryptography algorithms

Заключение

Обобщая все представленные выше сведения, можно выдвинуть ряд тезисов.

Несмотря на существование математических моделей квантовых алгоритмов, способных выполнить успешную атаку на широко использующиеся на текущий момент асимметричные криптоалгоритмы, не было представлено ни одной реализации квантового компьютера, способного реализовать данные атаки на практике. Кроме того, разработка и внедрение постквантовых криптографических алгоритмов (поддержка которых уже есть в некоторых браузерах: например, браузер *Google Chrome* поддерживает алгоритм «*X25519Kyber768*»[12]) также не позволит в дальнейшем вскрывать защищенные *TLS* соединения.

[12] O'Brien D. Protecting Chrome Traffic with Hybrid Kyber KEM. Chromium. URL: https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html (дата обращения: 30.01.2024).

Реальной проблемой является атака «*Harvest Now, Decrypt Later*»[13], которая заключается в предварительном массовом сборе данных, зашифрованных с использованием асимметричных алгоритмов, основанных на задачах, допускающих ускоренное решение на квантовом вычислителе, или с использованием симметричных алгоритмов с длиной ключа, допускающей осуществление за обозримое время перебора ключевого пространства с учетом квадратичного ускорения, с целью их дешифрования в будущем.

Также атака типа «*Harvest Now, Decrypt Later*» в долгосрочной перспективе теоретически может быть применена к информации, зашифрованной с использованием симметричных криптопримитивов, для которых были найдены эффективные квантовые алгоритмы.

Однако, как известно, актуальность информации с течением времени имеет тенденцию снижаться, в связи с чем проведение данной атаки будет целесообразным только для незначительной части зашифрованных данных [47], для которых уже на данный момент рекомендуется использовать более стойкие криптографические методы и алгоритмы [48, 49].

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Bennett Ch.H., Bernstein E., Brassard G., Vazirani U. Strengths and Weaknesses of Quantum Computing. *SIAM Journal on Computing*. 1997;26(5):1510–1523. https://doi.org/10.1137/s0097539796300933
2. Anand R., Maitra A., Mukhopadhyay S. Grover on *SIMON*. *Quantum Information Processing*. 2020;19(9). https://doi.org/10.1007/S11128-020-02844-W
3. Jaques S., Naehrig M., Roetteler M., Virdia F. Implementing Grover Oracles for Quantum Key Search on AES and LowMC. In: *Advances in Cryptology – EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques: Proceedings: Part II, 10–14 May 2020, Zagreb, Croatia.* Cham: Springer; 2020. P. 280–310. https://doi.org/10.1007/978-3-030-45724-2_10
4. Song G., Jang K., Kim H., Lee W.-K., Seo H. Grover on Caesar and Vigenère Ciphers. Cryptology ePrint Archive. URL: https://eprint.iacr.org/2021/554 [Accessed 30th January 2024].
5. Kochan R., Yevseiev S., Korolyov R., et al. Development of Methods for Improving Crypto Transformations in the Block-Symmetric Code. In: *2020 IEEE 5th International Symposium on Smart and Wireless Systems Within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), 17–18 September 2020, Dortmund, Germany.* IEEE; 2020. P. 1–9. https://doi.org/10.1109/IDAACS-SWS50031.2020.9297102
6. Jing Z., Gu C., Ge C., Shi P. Cryptanalysis of a Public Key Cryptosystem Based on Data Complexity Under Quantum Environment. In: *Security and Privacy in New Computing Environments, Second EAI International Conference, SPNCE 2019: Proceedings, 13–14 April 2019, Tianjin, China.* Cham: Springer; 2019. P. 411–420. https://doi.org/10.1007/978-3-030-21373-2_32
7. Grover L.K. A Fast Quantum Mechanical Algorithm for Database Search. In: *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing, 22–24 May 1996, Philadelphia, PA, USA.* New York: Association for Computing Machinery; 1996. P. 212–219. https://doi.org/10.1145/237814.237866

[13] Townsend K. Solving the Quantum Decryption 'Harvest Now, Decrypt Later' Problem. SecurityWeek. URL: https://www.securityweek.com/solving-quantum-decryption-harvest-now-decrypt-later-problem/ (дата обращения: 30.01.2024).

8. Regev O. An Efficient Quantum Factoring Algorithm. arXiv. URL: https://arxiv.org/abs/2308.06572 [Accessed 30th January 2024].
9. Kuwakado H., Morii M. Quantum Distinguisher Between the 3-Round Feistel Cipher and the Random Permutation. In: *2010 IEEE International Symposium on Information Theory (ISIT 2010), 13–18 June 2010, Austin, TX, USA*. IEEE; 2010. P. 2682–2685. https://doi.org/10.1109/ISIT.2010.5513654
10. Beals R., Brierley S., Gray O., et al. Efficient Distributed Quantum Computing. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*. 2013;469(2153). https://doi.org/10.1098/rspa.2012.0686
11. Kaplan M., Leurent G., Leverrier A., Naya-Plasencia M. Breaking Symmetric Cryptosystems Using Quantum Period Finding. In: *Advances in Cryptology – CRYPTO 2016: 36th Annual International Cryptology Conference: Proceedings: Part II, 14–18 August 2016, Santa Barbara, CA, USA*. Berlin, Heidelberg: Springer; 2016. P. 207–237. https://doi.org/10.1007/978-3-662-53008-5_8
12. Simon D.R. On the Power of Quantum Computation. *SIAM Journal on Computing*. 1997;26(5):1474–1483. https://doi.org/10.1137/S0097539796298637
13. Alagic G., Russell A. Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts. In: *Advances in Cryptology – EUROCRYPT 2017: 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques: Proceedings: Part III, 30 April – 04 May 2017, Paris, France*. Cham: Springer; 2017. P. 65–93. https://doi.org/10.1007/978-3-319-56617-7_3
14. Kaplan M., Leurent G., Leverrier A., Naya-Plasencia M. Quantum Differential and Linear Cryptanalysis. *IACR Transactions on Symmetric Cryptology*. 2016;2016(1):71–94. https://doi.org/10.13154/tosc.v2016.i1.71-94
15. Hosoyamada A., Aoki K. On Quantum Related-Key Attacks on Iterated Even-Mansour Ciphers. In: *Advances in Information and Computer Security: 12th International Workshop on Security, IWSEC 2017: Proceedings, 30 August – 01 September 2017, Hiroshima, Japan*. Cham: Springer; 2017. P. 3–18. https://doi.org/10.1007/978-3-319-64200-0_1
16. Dong X., Dong B., Wang X. Quantum Attacks on Some Feistel Block Ciphers. *Designs, Codes and Cryptography*. 2020;88(6):1179–1203. https://doi.org/10.1007/s10623-020-00741-y
17. Xu Yi., Yuan Zh. Quantum Meet-in-the-Middle Attack on Feistel Construction. arXiv. URL: https://arxiv.org/abs/2107.12724 [Accessed 30th January 2024].
18. Bonnetain X., Schrottenloher A., Sibleyras F. Beyond Quadratic Speedups in Quantum Attacks on Symmetric Schemes. In: *Advances in Cryptology – EUROCRYPT 2022: 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques: Proceedings: Part III, 30 May – 03 June 2022, Trondheim, Norway*. Cham: Springer; 2022. P. 315–344. https://doi.org/10.1007/978-3-031-07082-2_12
19. Xie H., Xia Q., Wang K., Li Ya., Yang L. Quantum Automated Tools for Finding Impossible Differentials. *Mathematics*. 2024;12(16). https://doi.org/10.3390/math12162598
20. S H., Mishra N., D V. QHopNN: Investigating Quantum Advantage in Cryptanalysis Using a Quantum Hopfield Neural Network. *Physica Scripta*. 2024;99(8). https://doi.org/10.1088/1402-4896/ad5ed1
21. Kuwakado H., Morii M. Security on the Quantum-Type Even-Mansour Cipher. In: *2012 International Symposium on Information Theory and its Applications, 28–31 October 2012, Honolulu, HI, USA*. IEEE; 2012. P. 312–316.

22. Dunkelman O., Keller N., Shamir A. Slidex Attacks on the Even-Mansour Encryption Scheme. *Journal of Cryptology*. 2015;28(1):1–28. https://doi.org/10.1007/s00145-013-9164-7
23. Bonnetain X. Quantum Key-Recovery on Full AEZ. In: *Selected Areas in Cryptography – SAC 2017: 24th International Conference: Revised Selected Papers, 16–18 August 2017, Ottawa, ON, Canada.* Cham: Springer; 2018. P. 394–406. https://doi.org/10.1007/978-3-319-72565-9_20
24. Kuperberg G. A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem. *SIAM Journal on Computing*. 2005;35(1):170–188. https://doi.org/10.1137/S0097539703436345
25. Chailloux A., Naya-Plasencia M., Schrottenloher A. An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography. In: *Advances in Cryptology – ASIACRYPT 2017: 23rd International Conference on the Theory and Application of Cryptology and Information Security: Proceedings: Part II, 03–07 December 2017, Hong Kong, China.* Cham: Springer; 2017. P. 211–240. https://doi.org/10.1007/978-3-319-70697-9_8
26. Gidney C., Ekerå M. How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits. arXiv. URL: https://arxiv.org/abs/1905.09749 [Accessed 30th January 2024].
27. Gouzien E., Sangouard N. Factoring 2048-bit RSA Integers in 177 Days with 13436 Qubits and a Multimode Memory. arXiv. URL: https://arxiv.org/abs/2103.06159 [Accessed 30th January 2024].
28. Deutsch D., Jozsa R. Rapid Solution of Problems by Quantum Computation. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*. 1992;439(1907):553–558. https://doi.org/10.1098/rspa.1992.0167
29. Cleve R., Ekert A., Macchiavello C., Mosca M. Quantum Algorithms Revisited. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*. 1998;454(1969):339–354. https://doi.org/10.1098/rspa.1998.0164
30. Childs A.M., Liu J.-P. Quantum Spectral Methods for Differential Equations. *Communications in Mathematical Physics*. 2019;375(2):1427–1457. https://doi.org/10.1007/s00220-020-03699-z
31. Nielsen M.A., Chuang I.L. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge: Cambridge University Press; 2010. 702 p. https://doi.org/10.1017/cbo9780511976667
32. Ozhigov Yu. Quantum Computers Speed Up Classical with Probability Zero. *Chaos Solitons Fractals*. 1999;10(10):1707–1714. https://doi.org/10.1016/S0960-0779(98)00226-4
33. Петренко А.С., Петренко С.А. Основные алгоритмы квантового криптоанализа. *Вопросы кибербезопасности.* 2023;(1):100–115. (На англ.).
Petrenko A., Petrenko S. Basic Algorithms Quantum Cryptanalysis. *Voprosy kiberbezopasnosti*. 2023;(1):100–115.
34. Buchmann J., García L.C.C., Dahmen E., Döring M., Klintsevich E. CMSS – An Improved Merkle Signature Scheme. In: *Progress in Cryptology – INDOCRYPT 2006: 7th International Conference on Cryptology in India: Proceedings, 11–13 December 2006, Kolkata, India.* Berlin, Heidelberg: Springer; 2006. P. 349–363. https://doi.org/10.1007/11941378_25
35. Dinh H., Moore C., Russell A. McEliece and Niederreiter Cryptosystems That Resist Quantum Fourier Sampling Attacks. In: *Advances in Cryptology – CRYPTO 2011: 31st Annual Cryptology Conference: Proceedings, 14–18 August 2011, Santa Barbara, CA,*

USA. Berlin, Heidelberg: Springer; 2011. P. 761–779. https://doi.org/10.1007/978-3-642-22792-9_43

36. Овчинников А.А. Вариант постквантовой системы на основе кодов, исправляющих пакеты ошибок, и задачи полного декодирования. *Информационно-управляющие системы.* 2022;(3):45–54. (На англ.). https://doi.org/10.31799/1684-8853-2022-3-45-54
Ovchinnikov A. The Variant of Post-Quantum Cryptosystem Based on Burst-Correcting Codes and on the Complete Decoding Problem. *Information and Control Systems*. 2022;(3):45–54. https://doi.org/10.31799/1684-8853-2022-3-45-54
37. Goldreich O., Goldwasser Sh., Halevi Sh. Public-Key Cryptosystems from Lattice Reduction Problems. In: *Advances in Cryptology – CRYPTO '97: 17th Annual International Cryptology Conference: Proceedings, 17–21 August 1997, Santa Barbara, California, USA*. Berlin, Heidelberg: Springer; 1997. P. 112–131. https://doi.org/10.1007/BFb0052231
38. Yu Yu. Preface to Special Topic on Lattice-Based Cryptography. *National Science Review*. 2021;8(9). https://doi.org/10.1093/nsr/nwab154
39. Courtois N.T. The Security of Hidden Field Equations (HFE). In: *Topics in Cryptology – CT-RSA 2001: The Cryptographer's Track at RSA Conference: Proceedings, 08–12 April 2001, San Francisco, CA, USA.* Berlin, Heidelberg: Springer; 2001. P. 266–281. https://doi.org/10.1007/3-540-45353-9_20
40. Bogomolec X., Underhill J.G., Kovac S.A. Towards Post-Quantum Secure Symmetric Cryptography: A Mathematical Perspective. Cryptology ePrint Archive. URL: https://eprint.iacr.org/2019/1208 [Accessed 30th January 2024].
41. Jao D., De Feo L. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. In: *Post-Quantum Cryptography: 4th International Workshop, PQCrypto 2011: Proceedings, 29 November – 02 December 2011, Taipei, Taiwan.* Berlin, Heidelberg: Springer; 2011. P. 19–34. https://doi.org/10.1007/978-3-642-25405-5_2
42. Stratil Ph., Hasegawa Sh., Shizuya H. Supersingular Isogeny-Based Cryptography: A Survey. *Interdisciplinary Information Sciences*. 2021;27(1):1–23. https://doi.org/10.4036/iis.2020.r.02
43. Lauter K.E., Petit Ch. Supersingular Isogeny Graphs in Cryptography. In: *Surveys in Combinatorics: Chapter 5*. Cambridge University Press; 2019. P. 143–166. https://doi.org/10.1017/9781108649094.006
44. Tenorio R.H.V., Sham Ch.W., Vargas D.V. Preliminary Study of Applied Binary Neural Networks for Neural Cryptography. In: *GECCO '20: Proceedings of the 2020 Genetic and Evolutionary Computation Conference Companion, 08–12 July 2020, Cancún, Mexico*. New York: Association for Computing Machinery; 2020. P. 291–292. https://doi.org/10.1145/3377929.3389933
45. Tarasenko S.S., Andriyanov N.A., Gladkikh A.A. Analysis of the Applicability of Artificial Neural Networks for the Post-Quantum Cryptography Algorithms Development. In: *Journal of Physics: Conference Series: Volume 2032: International Conference on IT in Business and Industry (ITBI 2021), 12–14 May 2021, Novosibirsk, Russia.* IOP Publishing Ltd; 2021. https://doi.org/10.1088/1742-6596/2032/1/012026
46. Singh A., Nandal A. Neural Cryptography for Secret Key Exchange and Encryption with AES. *International Journal of Advanced Research in Computer Science and Software Engineering*. 2013;3(5):376–381.
47. Тарасенко С.С., Чубуткин И.А. Модель угроз и нарушителя безопасности информации в симметричных криптосистемах. В сборнике: *Юность и Знания – Гарантия Успеха – 2023: сборник научных статей 10-й Международной*

молодежной научной конференции: Том 2, 19–20 сентября 2023 года, Курск, Россия. Курск: Университетская книга; 2023. С. 180–184.

48. Tarasenko S., Ivanov Yu. Approach to Constructing Symmetric Cryptographic Systems Ensuring Specified Resilience to Cryptoanalysis over the Long-Term Time Horizon. *Journal of Science and Technology on Information Security*. 2023;3(20):88–94. https://doi.org/10.54654/isj.v3i20.1016
49. Тарасенко С.С. Алгоритм криптографического преобразования полезной нагрузки и ключевой информации на основе шифра Вернама и композиционного шифра. *Современная наука: актуальные проблемы теории и практики. Серия Естественные и технические науки*. 2023;(6/2):147–152.
Tarasenko S.S. Algorithm of Cryptographic Transformation of Payload and Key Information Based on Vernam Cipher and Composite Cipher. *Sovremennaya nauka: aktualnye problemy teorii i praktiki. Seriya estestvennye i tekhnicheskie nauki*. 2023;(6/2):147–152. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Козачок Александр Васильевич, доктор технических наук, доцент, профессор кафедры КБ-4 института кибербезопасности и цифровых технологий, МИРЭА – Российский технологический университет, Москва, Российская Федерация.
e-mail: kozachok_a@mirea.ru
ORCID: 0000-0002-6501-2008

Aleksandr V. Kozachok, Doctor of Engineering Sciences, Docent, Professor at the Department KB-4 of the Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University, Moscow, the Russian Federation.

Тарасенко Сергей Сергеевич, кандидат технических наук, сотрудник, Академия Федеральной службы охраны Российской Федерации, Орёл, Российская Федерация.
e-mail: dor7la96@mail.ru
ORCID: 0000-0001-7473-1971

Sergey S. Tarasenko, Candidate of Engineering Sciences, Employee, Academy of Federal Guard Service of the Russian Federation, Oryol, the Russian Federation.

Козачок Андрей Васильевич, кандидат технических наук, доцент кафедры КБ-4 института кибербезопасности и цифровых технологий, МИРЭА – Российский технологический университет, Москва, Российская Федерация.
e-mail: kozachok@mirea.ru
ORCID: 0000-0001-6191-8614

Andrey V. Kozachok, Candidate of Engineering Sciences, Associate Professor at the Department KB-4 of the Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University, Moscow, the Russian Federation.

Статья поступила в редакцию 06.04.2025; одобрена после рецензирования 26.04.2025; принята к публикации 05.05.2025.

The article was submitted 06.04.2025; approved after reviewing 26.04.2025; accepted for publication 05.05.2025.