SCIENTIFIC CONFERENCE OPEN PROCEEDINGS
Global Academic Knowledge Repository

КВАНТОВЫЕ ВЫЧИСЛИТЕЛЬНЫЕ ТЕХНОЛОГИИ И ИХ ВЛИЯНИЕ НА КИБЕРБЕЗОПАСНОСТЬ

Курбонова Фируза Зариповна

Доктор философии по техническим наукам, доцент, Академия Министерства внутренних дел Республики Узбекистан, Ташкент, Узбекистан

https://doi.org/10.5281/zenodo.20957907

Аннотация. В данной статье рассматривается влияние технологий квантовых вычислений на современную кибербезопасность. Анализируются возможности квантовых компьютеров, их потенциальное воздействие на существующие криптографические алгоритмы и возникающие угрозы для защиты информации. Особое внимание уделяется проблеме устойчивости традиционных систем шифрования перед квантовыми атаками, развитию постквантовой криптографии, квантовому распределению ключей и новым методам обеспечения безопасности данных. Рассматриваются перспективы применения квантовых технологий как инструмента повышения уровня информационной безопасности.

Ключевые слова: квантовые вычисления, кибербезопасность, криптография, постквантовая криптография, квантовые атаки, защита информации.

Annotatsiya. Ushbu maqolada kvant hisoblash texnologiyalarining zamonaviy kiberxavfsizlik sohasiga ta’siri tahlil qilinadi. Kvant kompyuterlarining imkoniyatlari, ularning mavjud kriptografik algoritmlarga ta’siri va axborot xavfsizligiga yuzaga keltirishi mumkin bo‘lgan tahdidlar ko‘rib chiqiladi. An’anaviy shifrlash tizimlarining kvant hujumlariga nisbatan zaifligi, postkvant kriptografiya, kvant kalitlarni taqsimlash texnologiyalari va yangi himoya usullari yoritiladi.

Kalit so‘zlar: kvant hisoblash, kiberxavfsizlik, kriptografiya, postkvant

kriptografiya, kvant hujumlari, axborot xavfsizligi.

Abstract. This article examines the impact of quantum computing technologies on modern cybersecurity. The capabilities of quantum computers, their potential effects on existing cryptographic algorithms, and emerging threats to information protection are analyzed. The paper focuses on the vulnerability of traditional encryption systems against quantum attacks, the development of post-quantum cryptography, quantum key distribution, and future approaches to secure information systems.

Keywords: quantum computing, cybersecurity, cryptography, post-quantum cryptography, quantum attacks, information security.

Введение. В условиях активного развития цифровых технологий обеспечение информационной безопасности становится одной из главных задач современного общества. Государственные системы, финансовые организации, промышленные предприятия и частные пользователи ежедневно сталкиваются с различными киберугрозами.

Для защиты информации широко применяются криптографические алгоритмы, которые обеспечивают конфиденциальность, целостность и аутентификацию данных. Такие алгоритмы, как RSA, AES и ECC, являются основой современной цифровой инфраструктуры.

Однако развитие квантовых вычислений создаёт новые вызовы для существующих методов защиты. Квантовые компьютеры способны выполнять отдельные виды вычислений значительно быстрее традиционных систем, что в будущем может поставить под угрозу безопасность многих криптографических алгоритмов[3].

1. Основы квантовых вычислений

Квантовые вычисления — это направление информатики, основанное на принципах квантовой механики. В отличие от классических компьютеров, где

информация представлена в виде битов (0 или 1), квантовые компьютеры используют кубиты[1],[2].

Кубиты обладают свойством суперпозиции, позволяющей им находиться в нескольких состояниях одновременно. Это позволяет выполнять большое количество вычислений параллельно.

Другим важным свойством является квантовая запутанность, которая обеспечивает особую связь между квантовыми объектами[3].

Основными квантовыми алгоритмами являются:

- алгоритм Шора;
- алгоритм Гровера.

Алгоритм Шора представляет наибольшую опасность для современной криптографии, так как способен ускорить решение задач факторизации больших чисел.

2. Влияние квантовых вычислений на криптографию

Современные системы защиты используют криптографические методы, основанные на сложности математических задач.

Например:

- RSA основан на сложности факторизации больших чисел;
- ECC использует сложность вычисления дискретного логарифма.

Однако квантовые компьютеры с использованием алгоритма Шора могут значительно ускорить решение этих задач.

Это может привести к следующим угрозам:

- взлому зашифрованных сообщений[5];
- подделке цифровых подписей;
- компрометации банковских систем;
- нарушению государственных информационных систем[4].

Особую опасность представляет атака:

“Harvest Now, Decrypt Later” («Собрать сейчас — расшифровать потом»).

При такой атаке злоумышленники заранее сохраняют зашифрованные данные, рассчитывая расшифровать их после появления мощных квантовых компьютеров.

3. Постквантовая криптография

Для противодействия квантовым угрозам развивается направление постквантовой криптографии [3],[4].

Её задача — создание алгоритмов, устойчивых к атакам как обычных, так и квантовых компьютеров.

Решётчатая криптография

Использует сложные математические задачи на основе решёток. Считается одним из наиболее перспективных направлений [5].

Кодовая криптография

Основывается на сложности декодирования специальных кодов.

Хеш-основанные методы

Используют криптографические хеш-функции для создания цифровых подписей[6] .

Переход к таким алгоритмам является важным этапом подготовки к квантовой эпохе.

4. Квантовые технологии в защите информации

Несмотря на угрозы, квантовые технологии могут использоваться для усиления безопасности [7]. Одним из главных направлений является квантовое распределение ключей (**Quantum Key Distribution — QKD**).

Данная технология позволяет:

- безопасно передавать криптографические ключи;
- обнаруживать попытки перехвата информации;
- повышать уровень защиты каналов связи.

QKD может использоваться в:

- государственных сетях;
- банковской сфере;
- критической инфраструктуре.

5. Подготовка к квантовой угрозе

Организациям необходимо заранее подготовиться к распространению квантовых технологий.

Основные меры:

1. Анализ используемых криптографических систем.
2. Определение уязвимых алгоритмов.
3. Переход на постквантовые решения.
4. Подготовка специалистов.
5. Создание новых стандартов безопасности.

Использование гибридных систем, объединяющих традиционные и квантово-устойчивые алгоритмы, позволит обеспечить постепенный переход.

Заключение

Квантовые вычисления являются одной из наиболее перспективных технологий будущего. Они способны значительно изменить развитие науки, экономики и информационных систем. Однако вместе с преимуществами квантовые технологии создают новые риски для кибербезопасности.

Возможность взлома существующих криптографических алгоритмов требует заранее подготовить цифровую инфраструктуру к новым условиям. Развитие постквантовой криптографии, внедрение квантово-устойчивых алгоритмов и повышение квалификации специалистов являются основными направлениями защиты информации.

Таким образом, квантовые вычисления одновременно являются потенциальной угрозой и новым инструментом повышения уровня

безопасности.

REFERENCES

1. Nielsen M. A., Chuang I. L. **Quantum Computation and Quantum Information.** Cambridge University Press, 2010.
2. Shor P. W. **Algorithms for Quantum Computation: Discrete Logarithms and Factoring.** IEEE Symposium, 1994.
3. Grover L. K. **A Fast Quantum Mechanical Algorithm for Database Search.** ACM Symposium, 1996.
4. Bernstein D. J., Buchmann J., Dahmen E. **Post-Quantum Cryptography.** Springer, 2009.
5. National Institute of Standards and Technology (NIST). **Post-Quantum Cryptography Standardization.** https://csrc.nist.gov/projects/post-quantum-cryptography
6. Mosca M. **Cybersecurity in an Era with Quantum Computers: Will We Be Ready?** IEEE Security & Privacy, 2018.
7. Preskill J. **Quantum Computing in the NISQ Era and Beyond.** Quantum, 2018.
8. European Union Agency for Cybersecurity (ENISA). **Quantum Computing and Cybersecurity.** https://www.enisa.europa.eu/