DOI 10.37539/2949-1991.2023.9.9.003

**Федоров Алексей Алексеевич,** студент,
Донской Государственный Технический Университет,
г. Ростов-на-Дону

**Барашко Елена Николаевна,** старший преподаватель,
Донской Государственный Технический Университет,
г. Ростов-на-Дону

# ПРОБЛЕМЫ КВАНТОВОЙ КРИПТОГРАФИИ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

**Аннотация.** В статье рассматриваются и сравниваются квантовая и постквантовая криптографии и их актуальность в современном информационном обществе.

**Abstract.** The article discusses and compares quantum and post-quantum cryptography and their relevance in the modern information society.

**Ключевые слова:** квантовая криптография, постквантовая криптография, шифрование.

**Keywords:** quantum cryptography, post-quantum cryptography, encryption.

Информационная безопасность — важнейший элемент при формировании информационного общества и построении электронного государства. Большинство стран мира признали наличие квантовой угрозы и начали разработку новых методов защиты информации — постквантовой криптографии (Quantum-Safe Cryptography).

Есть два совершенно новых подхода: квантовая и постквантовая криптография. Квантовая строится на квантовом распределении ключей, когда биты информации кодируются в одиночные частицы (фотоны). Здесь можно найти вмешательство злоумышленников по количеству ошибок при передаче данных. Если оно не выше определенного уровня, можно сократить ключи так, чтобы информация мошенника о сокращенных ключах была неполной, – это называется «усиление секретности».[1] У этого метода есть недостатки: с увеличением длины квантового канала уменьшается скорость передачи; деполяризация фотонов в квантовом канале ведёт к высокому уровню помех; высокая стоимость оборудования.[5]

Постквантовая криптография основана на создании новых алгоритмов, в которых применяются более сложные математические задачи и хороша она тем, что её можно легко и быстро интегрировать.[2]

Недостатки постквантовой криптографии в том, что её секретность основывается на предположениях о сложности решения определённых классов математических задач. Вполне возможно, что скоро появится «постквантовый» компьютер, который разберётся с постквантовыми алгоритмами.

Специалисты считают, что переход всех технологий на квантово-устойчивые займёт около пяти лет. За период с 2021 г. по настоящее время технологии блокчейн и квантовой криптографии завоевали большую популярность. Много стандартов ИСО находятся в стадии разработки.[2]

Постквантовая криптография сегодня хорошо развита: уже есть коммерческие библиотеки, решения, продукты. Сейчас технология проходит процесс стандартизации. Преимущества этой технологии: простота и высокая скорость интеграции (поскольку речь идет о софте), регулярные обновления ПО. Эти решения применяются, чтобы усилить защиту информации.[1]

Эти две технологии можно успешно совместить. Например, каналы передачи данных между крупными компаниями можно защитить с помощью квантовой криптографии. А банковские транзакции или переписку с помощью постквантовой криптографии. Таким образом, квантовая – больше направлена на уровень стека, связанный с инфраструктурой; а постквантовая связана с пользователем.[1]

Стандарт квантовой криптографии пока формируется и сейчас он пока один – протокол BB84 с обманными состояниями. Но новые протоколы постоянно появляются.

Таблица 1

Сравнительный анализ особенностей постквантовой криптографии и квантового распределения ключей[4]

| Свойство | Постквантовая криптография | Квантовое распределение ключей | Вывод |
|---|---|---|---|
| Область применения | Асимметричное шифрование, схемы цифровой подписи, механизмы инкапсуляции ключа | Распределение симметричного ключа | ПКК обладает большим набором примитивов, которые не пересекаются с КРК |
| Безопасность | Основана на математических предположениях, проверенных временем | Основана на законах квантовой механики | КРК гарантирует обнаружение атаки |
| Реализация | Программная | Аппаратная | ПКК –в любой системе, КРК – спец. оборудование |
| Стоимость | Невысокая | Высокая | ПКК доступна, КРК скоро станет доступна |
| Сертификация | Технический комитет 26 и конкурсы NIST, CACR | Проекты ETSI, ISO, ITU-T | Скоро будут сертифицированы |
| Коммуникации | В любых цифровых типах коммуникации | ВОЛС и АОЛС. | КРК может выступать в синергии с ПКК |

Перед квантовой криптографией поставлена задача обеспечить абсолютную защиту шифрованных данных от взломов. Уже сейчас в России есть сети, защищённые квантово – критографическими методами, которые нельзя взломать.

Перед постквантовой криптографией стоит задача создать алгоритмы, устойчивые к кибератакам с помощью квантовых компьютеров. В этом направлении ведутся исследования. В 2023 году в России началось тестирование постквантовой защиты для видеоконференцсвязи, а учёные НИЯУ МИФИ предложили применять постквантовые криптографические алгоритмы для защиты обмена сообщениями в мессенджерах.[3]

Таким образом, в мире цифровых технологий появились новые методы защиты данных: квантовая и постквантовая криптографии и их развитие относится к вопросам национальной безопасности.

*Список литературы:*

1. Зачем нужны квантовые рельсы и как будут спасать данные в постквантовом мире // HIGHTECH URL: https://hightech.fm/2021/08/11/quantum-rails (дата обращения 18.05.2023)

2. Квантовый переход и безопасность блокчейнов // ITSEC URL: https://www.itsec.ru/articles/kvantovyj-perekhod-i-bezopasnost-blokchejnov (дата обращения 18.05.2023)

3. Постквантовая криптография. // TADVISER URL: https://www.tadviser.ru/index.php/Статья:Постквантовая_криптография (дата обращения 18.05.2023)

4. Сравнение квантовой и постквантовой криптографии // QAPP.TECH URL: https://qapp.tech/help/comparison-pqc-qkd (дата обращения 18.05.2023)

5. Филиппов М. А., Кротова Е. Л. Квантовая криптография. Преимущества и недостатки. Вестник УрФО №4 (26) 2017, с.25-27.