РКЦ | Российский Квантовый Центр

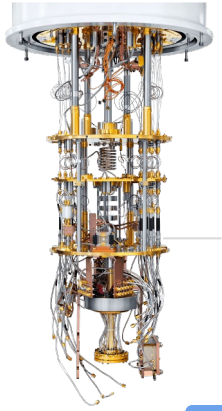
ГАЗПРОМБАНК

СИНЕРГИЯ КВАНТОВОЙ И ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

Алексей Федоров,
Руководитель научной группы
«Квантовые информационные технологии»

РКЦ Российский Квантовый Центр

КВАНТОВАЯ УГРОЗА ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Квантовые компьютеры активно развиваются год от года

Уже доступны через облако

С помощью квантовых компьютеров злоумышленники могут атаковать данные, защищенные традиционными методами шифрования. Распространенные сегодня алгоритмы криптографии неустойчивы к квантовой угрозе:

Распределение ключей	Асимметричное шифрование	Электронная подпись

Квантовая угроза усиливает ключевые риски ИБ

- Сетевая инфраструктура
- Стандартное программное обеспечение

- Финансовые риски при судебных издержках при обнаружении кражи данных
- Упущенная коммерческая выгода
- Репутационные риски, включая шантаж организации расшифрованным трафиком
- Фрод по платежам, подмена реквизитов…

РКЦ Российский Квантовый Центр

ЦЕННЫЕ ПОЛЬЗОВАТЕЛЬСКИЕ И КОРПОРАТИВНЫЕ ДАННЫЕ ТРЕБУЮТ ЗАЩИТЫ НОВЫМИ ИНСТРУМЕНТАМИ

- Пользовательские данные
- Внутренние и внешние коммуникации
- Хранение данных
- Электронный документооборот
- Аутентификация

Технологии квантовых коммуникаций и постквантовая криптография
могут обеспечить информационную безопасность на принципиально новом уровне

Квантовые коммуникации
Аппаратные решения квантового распределения ключей. Безопасность обеспечивается законами физики

Постквантовая криптография
Программные решения защиты данных. Безопасность обеспечивается новыми математическими подходами

РКЦ Российский Квантовый Центр

ОСНОВНЫЕ ИГРОКИ РЫНКА

В мире

Квантовые коммуникации

IDQ, TOSHIBA, KETS, QuantLR, MagiQ, 国盾量子 QuantumCTek, QUANTUMXCHANGE, Quintessence Labs, InfiniQuant, QUANTUM DICE

Постквантовая криптография

PQSHIELD, CRYPTONEXT SECURITY, PQSecure, INFOSEC GLOBAL, cyph, ISARA, QuantiCor, Post-Quantum, AGILEPQ, AMBIT

В России

Квантовые коммуникации

QRATE QUANTUM SOLUTIONS, infotecs, СМАРТС КВАНТТЕЛЕКОМ

Постквантовая криптография

QApp, КРИПТОНИТ, с•терра®, infotecs

РКЦ Российский Квантовый Центр

СИНЕРГИЯ ТЕХНОЛОГИЙ — КВАНТОВО-УСТОЙЧИВАЯ КИБЕРБЕЗОПАСНОСТЬ НА ВСЕХ УРОВНЯХ РАБОТЫ С ДАННЫМИ

УРОВНИ ЗАЩИТЫ ДАННЫХ		КВАНТОВАЯ КРИПТОГРАФИЯ	ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ
ПЛАТФОРМЫ	Комплексные IT-системы	✓	✓
ДАТА-ЦЕНТРЫ	Критическая инфраструктура	✓	✓
ИНФРАСТРУКТУРА	Каналы коммуникации, VPN, 5G	✓	✓
ПРИЛОЖЕНИЯ	Мобайл, Веб, Интернет вещей		✓

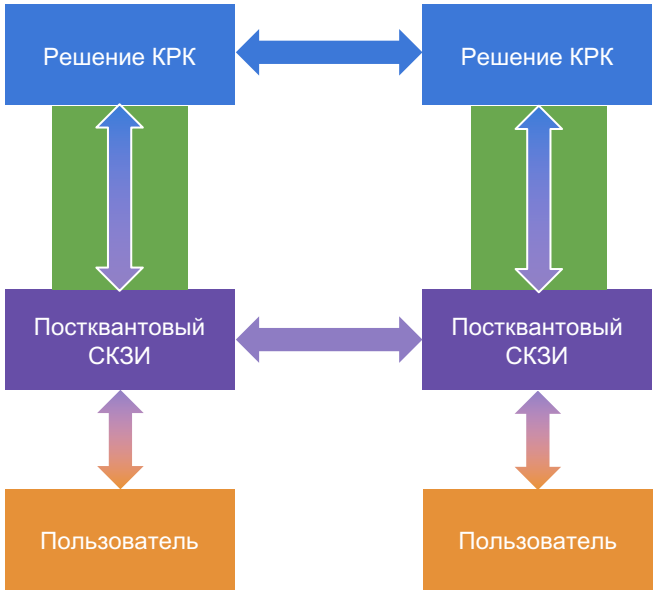
РКЦ Российский Квантовый Центр

ПРИМЕРЫ ИНТЕГРАЦИОННЫХ СЦЕНАРИЕВ ТЕХНОЛОГИИ ПОСТКВАНТОВОЙ И КВАНТОВОЙ КРИПТОГРАФИИ

- **Последняя миля**
  защита канала доставки ключей до потребителей не включенных непосредственно в квантовую сеть, подключение новых устройств в квантовую сеть

- **PKI (инфраструктура открытых ключей)**
  поддержка аутентификации между различными сегментами квантовых сетей или организация доступа к ключам

- **Защита вспомогательных соединений от MITM атак**
  в результате MITM не получится скомпрометировать ключ, но можно вызвать более сложно отлаживаемый отказ в обслуживании



РКЦ Российский Квантовый Центр

ВОЗМОЖНОСТЬ СИНЕРГИИ ТЕХНОЛОГИЙ В ОТКРЫТЫХ КВАНТОВЫХ СЕТЯХ

РКЦ | Российский Квантовый Центр

ГАЗПРОМБАНК

Алексей Федоров

Руководитель научной группы
«Квантовые информационные технологии»

Email: akf@rqc.ru

Телефон: +7 916 297-09-77

Telegram: @alekseyfedorov

rqc.ru

РКЦ Российский Квантовый Центр

ОТЛИЧИЕ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ ОТ КВАНТОВОЙ КРИПТОГРАФИИ

	Постквантовая криптография	Квантовое распределение ключей
Область применения	Асимметричное шифрование, схемы цифровой подписи, механизмы инкапсуляции ключа	Распределение симметричного ключа
Безопасность	Основана на математических предположениях, проверенных временем	Основана на законах квантовой механики
Реализация	Программная, но может быть ускорена аппаратно	Аппаратная
Стоимость	Невысокая, так как основные решения являются программными	Высокая цена из-за использования специализированного оборудования
Сертификация	Технический комитет 26 и конкурсы NIST, CACR	Проекты ETSI, ISO, ITU-T
Коммуникация	Может использоваться в любых цифровых типах коммуникации (беспроводные сети, оптические каналы и т.д.) на любом расстоянии	В основном используются волоконно-оптические линии связи (ВОЛС). На данный момент соединение между двумя точками ограничено 100 км при использовании оптоволоконных линий связи и практически не ограничено при использовании атмосферных оптических линий связи (АОЛС)

РКЦ Российский Квантовый Центр

СЦЕНАРИЙ ПОДКЛЮЧЕНИЯ НОВОГО УЗЛА В КВАНТОВУЮ СЕТЬ