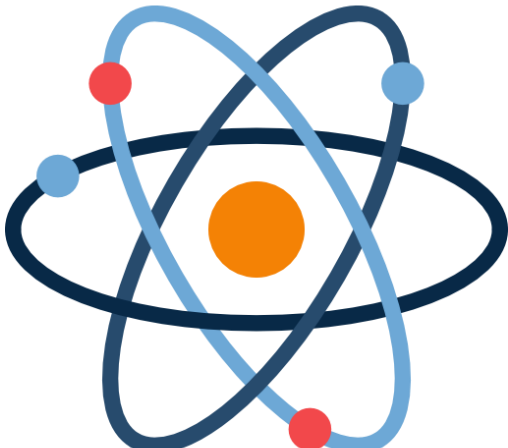


Проблема



- Развитие квантовых вычислений угрожает традиционным криптографическим механизмам.
- Полный переход на новые технологии требует времени и значительных ресурсов.

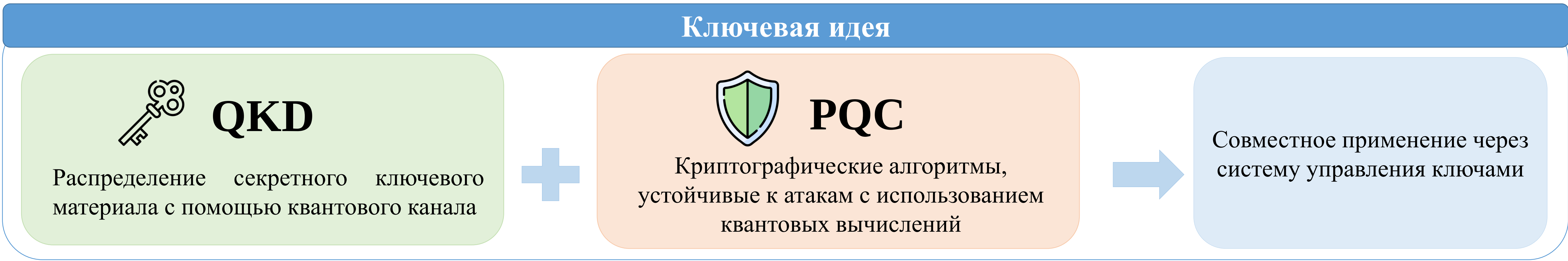
Необходим подход, который обеспечит квантово-устойчивую защиту с учётом существующей инфраструктуры.

Цель и задачи

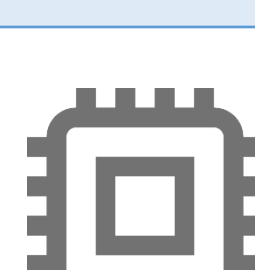
Цель: разработка принципов построения гибридной архитектуры криптографической защиты на основе QKD и постквантовых алгоритмов.

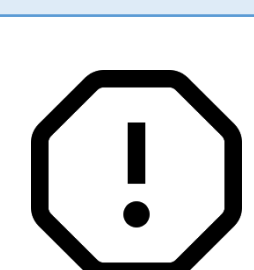
Основные задачи:

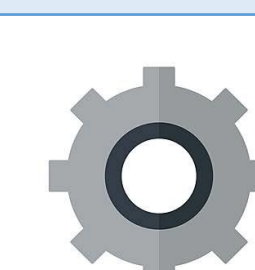
- Исследовать особенности QKD и PQC.
- Разработать архитектуру взаимодействия технологий.
- Определить принципы формирования ключевого материала.
- Разработать модель оценки стойкости.
- Определить требования к интеграции с существующими средствами защиты.

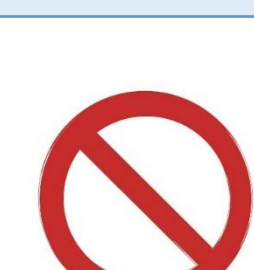


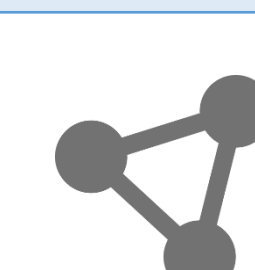
Модель угроз и сценарии оценки

Компрометация PQC

Нарушение QKD
(функционирования ПАК)

Компрометация системы управления ключами

Отказ квантового канала

Атаки на каналы взаимодействия

Оценка по ключевым характеристикам:

- криптографическая стойкость
- скорость формирования ключей
- доступность каналов
- время доставки ключа
- обновление ключей
- нагрузка и отказоустойчивость

Преимущества гибридного подхода

1 Постепенный переход без полной замены существующей инфраструктуры

2 Повышенная криптографическая устойчивость за счет независимых источников ключевого материала

3 Отказоустойчивость (резервный PQC-механизм при недоступности QKD)

4 Масштабируемость (поэтапное внедрение QKD-оборудование)

5 Совместимость с существующими средствами защиты

