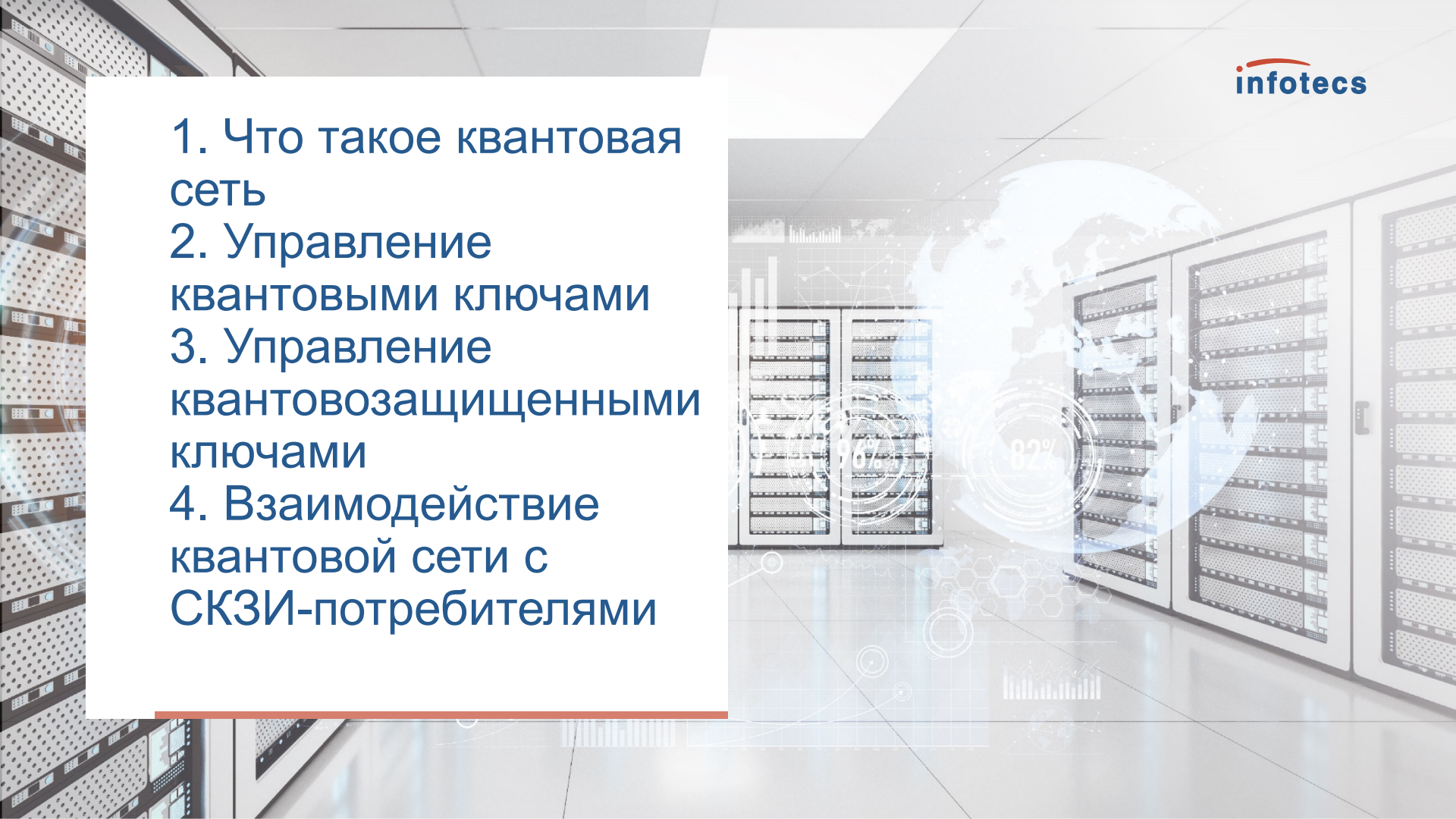
infotecs

Квантовая сеть и сервисы управления криптографическими ключами

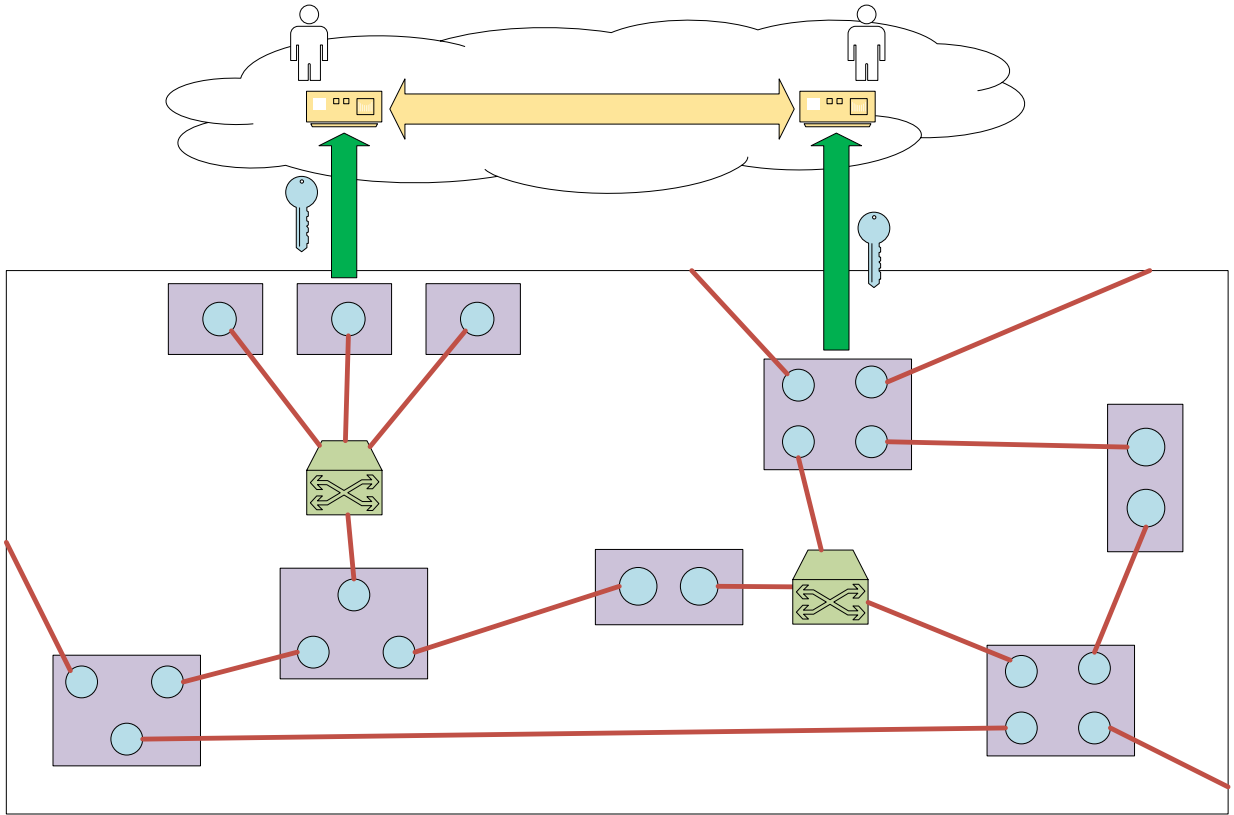
Андрей Жиляев



1. Что такое квантовая сеть
2. Управление квантовыми ключами
3. Управление квантовозащищенными ключами
4. Взаимодействие квантовой сети с СКЗИ-потребителями

Что такое квантовая сеть

Структура квантовой сети



СКЗИ

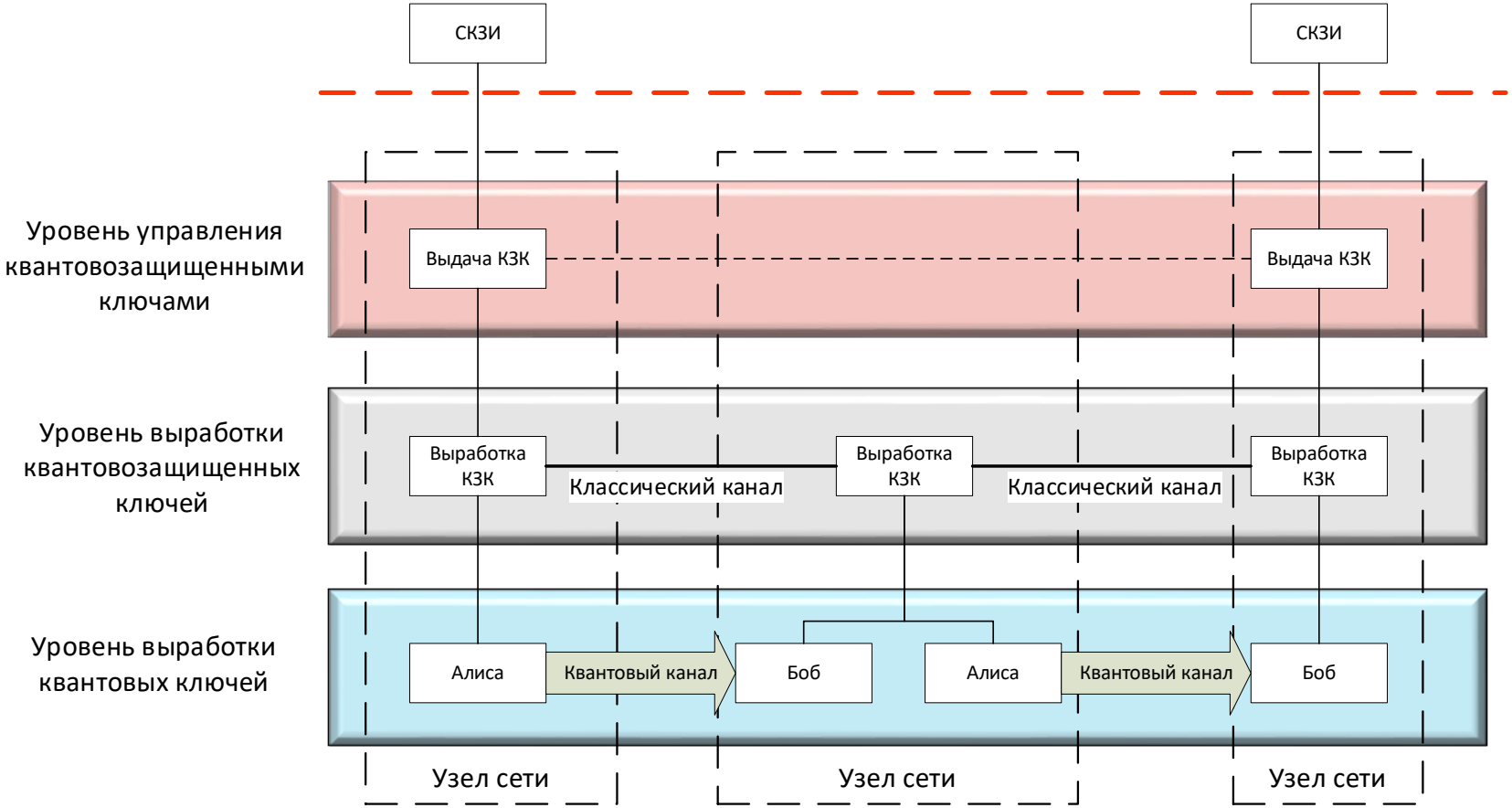
Узел квантовой Сети (УКС)

Аппаратура КРК

Оптический Коммутатор

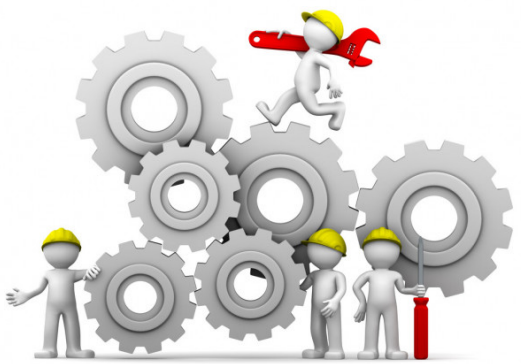
Квантовый Канал связи

Многоуровневая структура сети



Особенности развертывания квантовой сети

- Проблема предварительной генерации и доставки секретов на все узлы квантовой сети
- Адресация трафика в сети – топология классических связей повторяет топологию квантовых каналов или нет?
- Вычислительно стойкие алгоритмы – допустимы ли в квантовых сетях?
- Добавление нового узла в существующую сеть – только нового квантового канала не достаточно.



Управление выработкой квантовых ключей

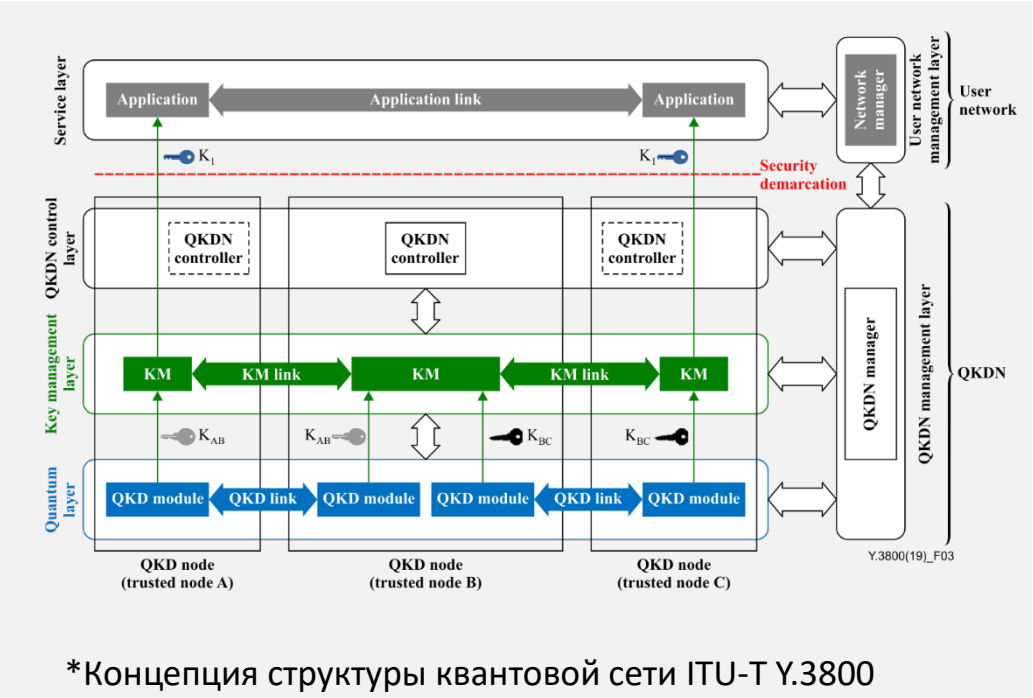
Централизованное управление выработкой квантовых ключей

Преимущества

- Согласованное переключение квантовых каналов
- Единый центр мониторинга состояний выработки квантовых ключей

Проблемы

- Контроллер – точка отказа сети
- Последовательное формирование запросов контроллером



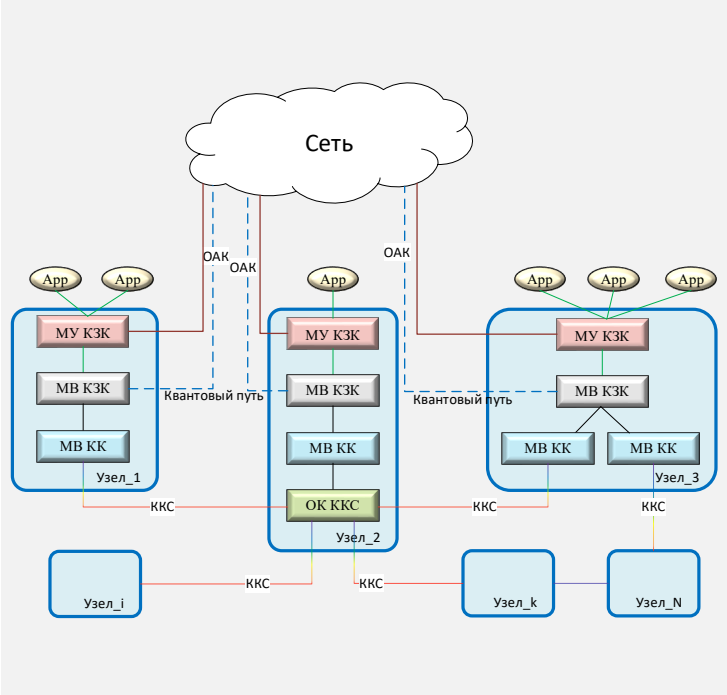
*Концепция структуры квантовой сети ITU-T Y.3800

Децентрализованное управление выработкой квантовых ключей

- Управление квантовым оборудованием локальными командами в рамках узла квантовой сети

Преимущества

- Выход из строя узла сети не приводит к отказу всей сети
- Генерация квантовых ключей не зависит от запросов сети (накопление квантовых ключей впрок независимо от необходимости генерировать КЗК)

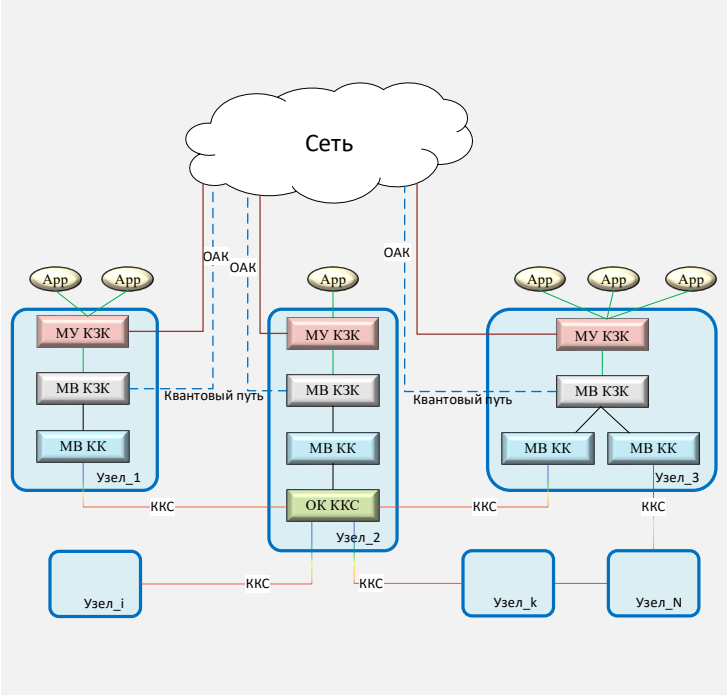


Децентрализованное управление выработкой квантовых ключей

- Управление квантовым оборудованием локальными командами в рамках узла квантовой сети

Проблемы

- С какой стороны квантового канала необходимо управлять квантовой аппаратурой?
- Переключение квантовых каналов (например через оптический коммутатор) не должно прерывать выработку квантового ключа



Управление выработкой квантовозащищенных ключей

Вопросы управления выработкой КЗК

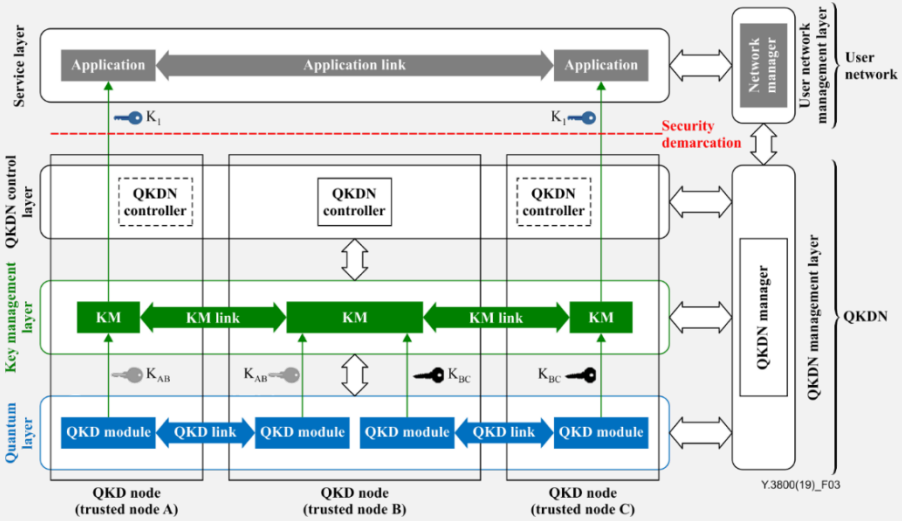
- Поддержание актуальной карты квантовой сети
- Выбор способа формирования КЗК
- Построение квантовых маршрутов для запроса КЗК
- Формирование очередности запросов КЗК
- Конкурирующие маршруты (надо вовремя сообщать о резерве маршрута для некоторого запроса КЗК)

Централизованное управление

- Единый контроллер собирает все запросы на КЗК, после чего рассчитывает оптимальные маршруты для совокупности запросов

Особенности:

- Концепция управления приближенная к концепции SDN-сетей для простоты интеграции
- Оптимальность расходование квантовых ключей для совокупности запросов
- Простота маршрутизации трафика в сети
- Высоконагруженная точка отказа всей сети



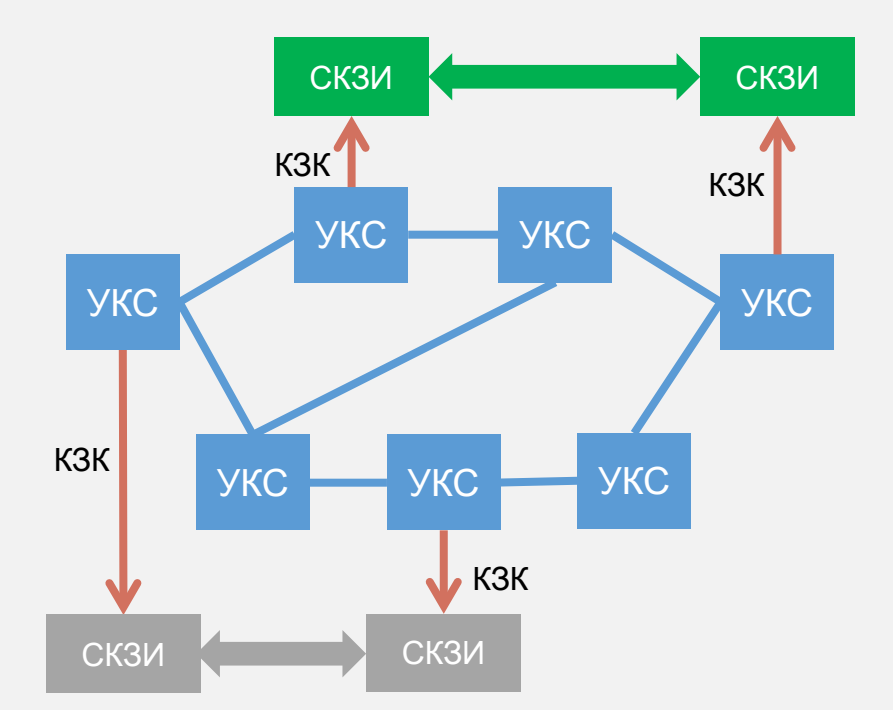
*Концепция структуры квантовой сети ITU-T Y.3800

Децентрализованное управление

- Запрос КЗК обрабатывает один узел сети

Особенности:

- Одновременная обработка запросов КЗК, поступивших в разные узлы сети
- Оптимизация выработки в случае непересекающихся маршрутов
- Необходимо поддерживать полную карту сети на каждом узле
- Необходимо учитывать возможность одновременного резервирования несколькими маршрутами одного сегмента

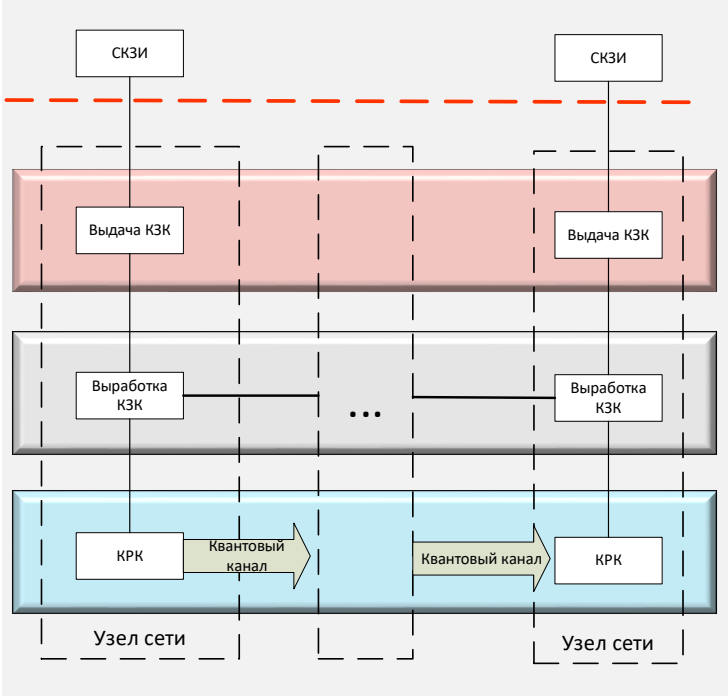


Взаимодействие квантовой сети с СКЗИ

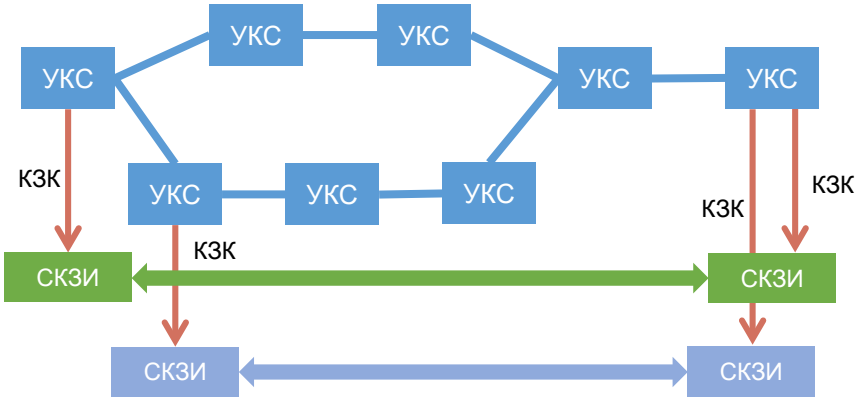
Взаимодействие квантовой сети с СКЗИ

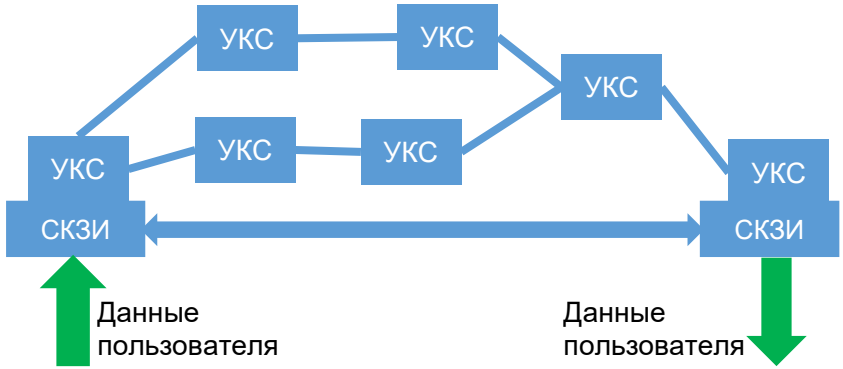
Проблемы:

- Взаимодействие с парой СКЗИ – какое из двух устройств инициирует запрос ключа от квантовой сети?
- Можно ли подключать СКЗИ к разным узлам квантовой сети (роуминг)
- Где контролируется легитимность запроса ключа с указанным СКЗИ
- Как контролировать доставку ключа в пару СКЗИ
- Защита передачи ключа на последней миле. Отсутствие квантовой аппаратуры в СКЗИ



Квантовая сеть как сервис





Сервис генерации ключей

- Контроль легитимности запроса КЗК
- Контроль доставки КЗК
- Контроль жизненного цикла ключей после передачи в СКЗИ перекладывается на сами СКЗИ

Сервис защиты информации на КЗК

- Полный контроль жизненного цикла КЗК
- Вопрос доверия владельца информации защите канала
- Предсказуемый расход КЗК

infotecs

Спасибо
за внимание!