Сети квантового распределения ключей с доверенными промежуточными узлами

Руководитель Центра научных исследований и перспективных разработок АО «ИнфоТеКС»
Елисеев Владимир Леонидович

2022 год

Атаки на зашифрованную информацию

infotecs

ЧТО ГРОЗИТ ДАННЫМ:

- Расшифрование (в том числе, в будущем)
- Подмена

ИСТОЧНИКИ УГРОЗ:

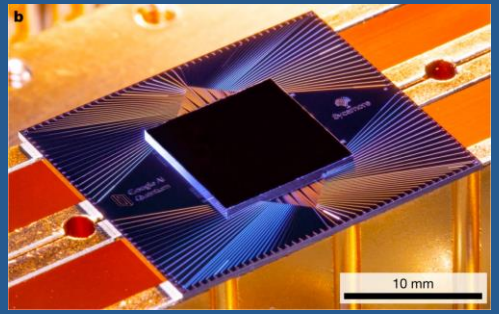
- Вычислительные ресурсы злоумышленника
  - Линейный и дифференциальный криптоанализ
  - Квантовые алгоритмы Шора и Гровера
- Побочные каналы утечки информации о ключах
- Разглашение секретных ключей

“Store now – decrypt later!”

Прогресс квантовых вычислений

infotecs

Квантовый компьютер Google Sycamore

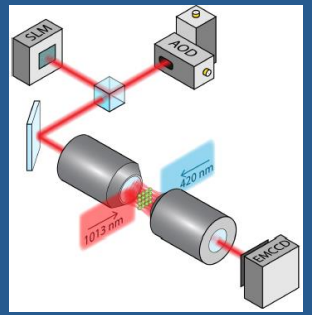


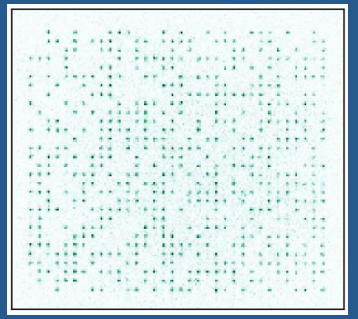
- 53 сверхпроводящих кубита
- Универсально программируется
- Формально показано квантовое превосходство в 2019 году

Квантовый компьютер Jiuzhang 九章算術

- 76 кубитов при комнатной температуре
- Решение узкоспециальной задачи
- Нет сомнений в квантовом превосходстве в 2020 году

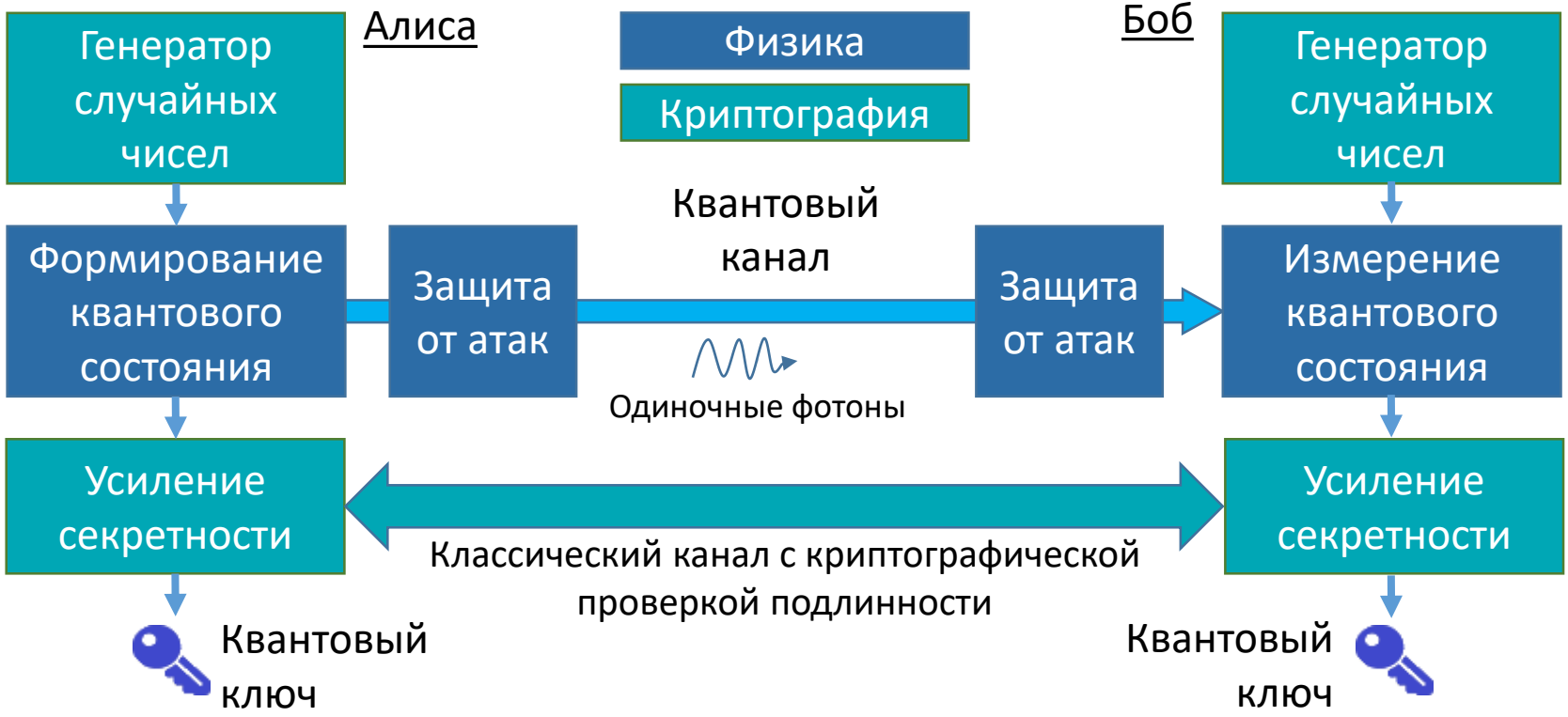
Квантовый симулятор из Гарварда



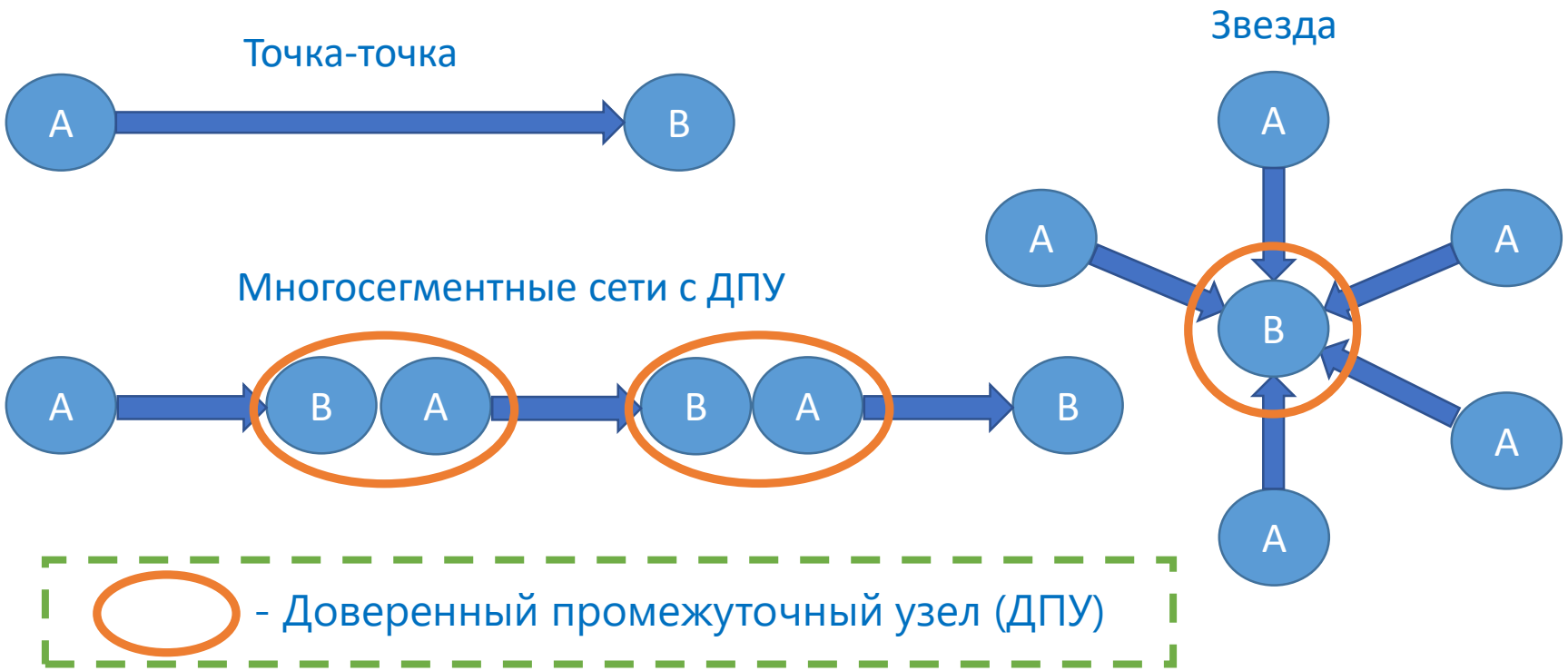


- >256 кубитов при комнатной температуре в 2021 году
- Универсально программируется

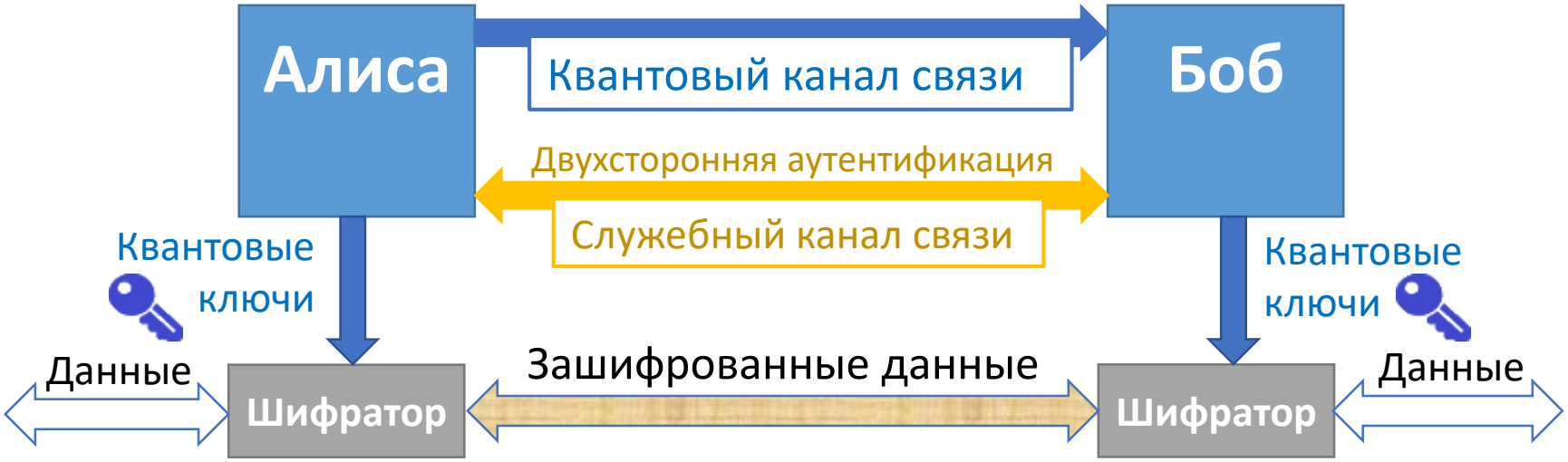
Основы квантового распределения ключей



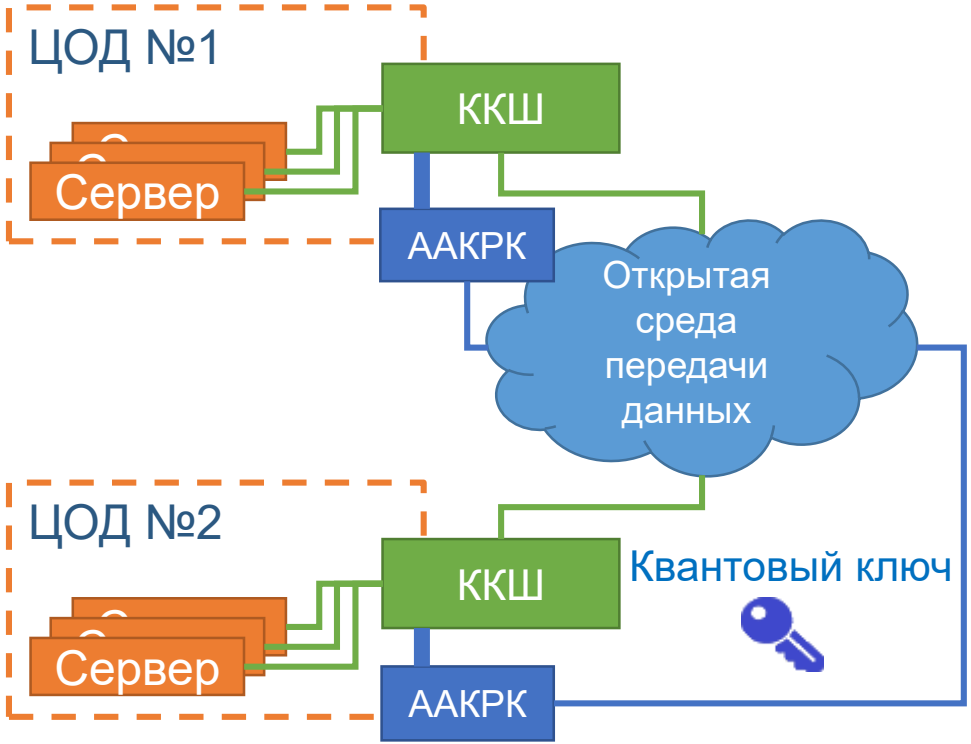
Базовые топологии сетей квантового распределения ключей



Защита канала связи «точка-точка» квантовыми ключами - идея



Защита канала связи «точка-точка» квантовыми ключами – сценарий



1. **ККШ (квантово-криптографический шифратор)** – шифратор канального уровня, доработанный для использования квантовых ключей

2. **ААКРК (автоматическая аппаратура квантового распределения ключей)** – инновационное оптоэлектронное устройство, обеспечивающее неперехватываемое распределение ключей для шифраторов

Защита канала связи «точка-точка» квантовыми ключами – продуктовое решение

ViPNet Quandor

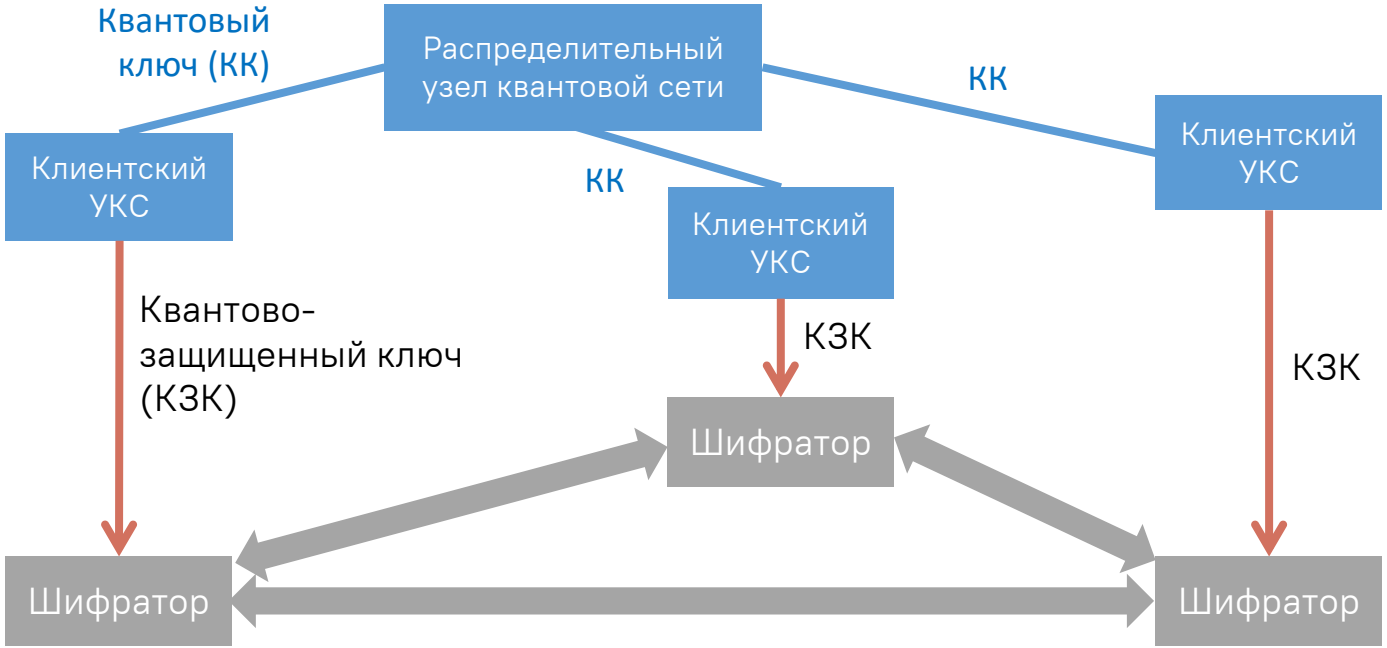
Два шифратора L2-10G (ККШ)

- 10Гбит/с, полный дуплекс
- ГОСТ 34.12-2018 «Кузнечик»
- Задержка <50 мкс

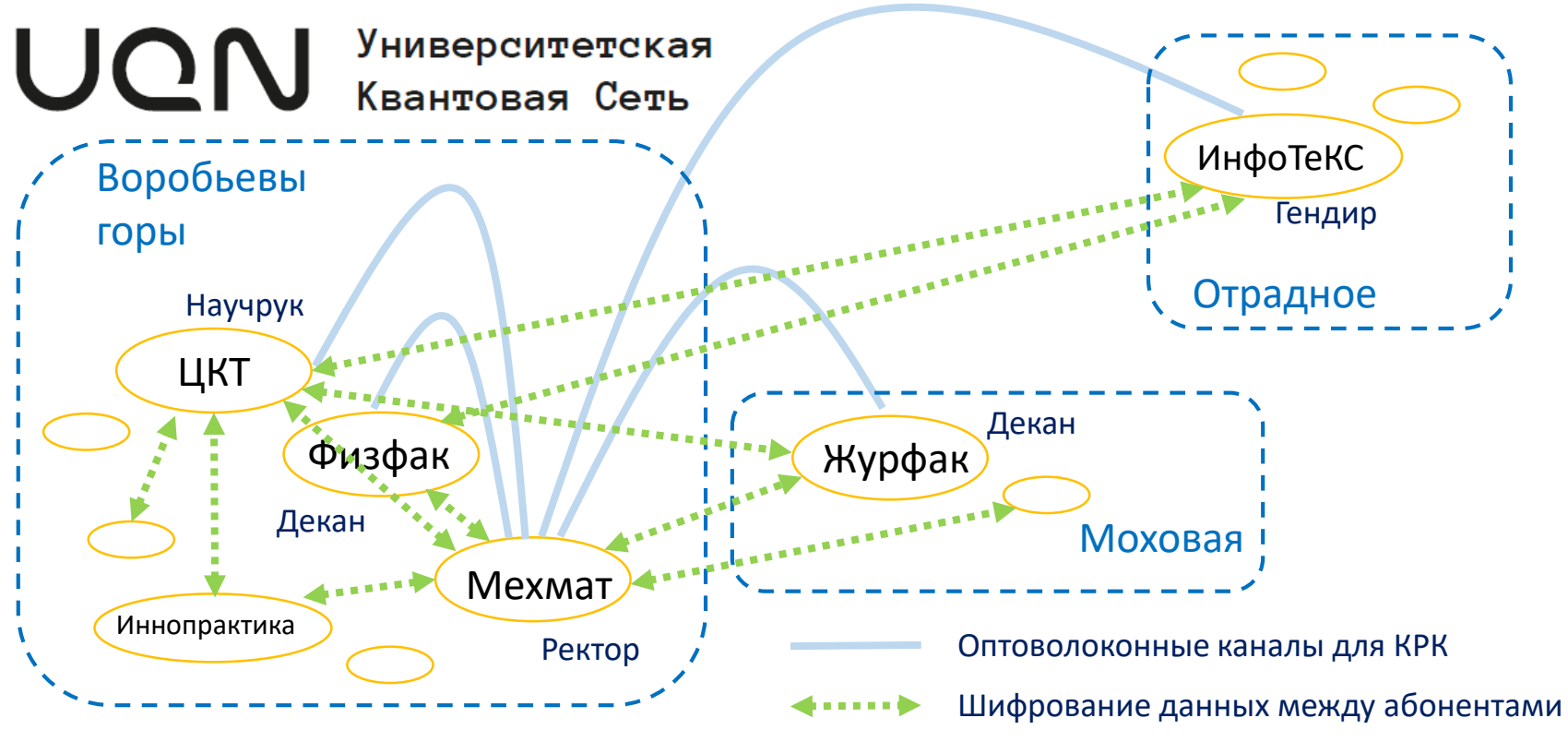
Алиса и Боб (ААКРК)

- Дальность >100 км (>20дБ)
- Скорость выработки квантовых ключей >256бит/мин
- Длина волны 1520 нм
- Прошла испытания:
  - ✓ Механические
  - ✓ Климатические
  - ✓ ЭМ-совместимость
  - ✓ Тематические

Защита городских каналов связи квантовыми ключами - идея



Защита городских каналов связи квантовыми ключами - сценарий



Защита городских каналов связи квантовыми ключами - продуктовое решение

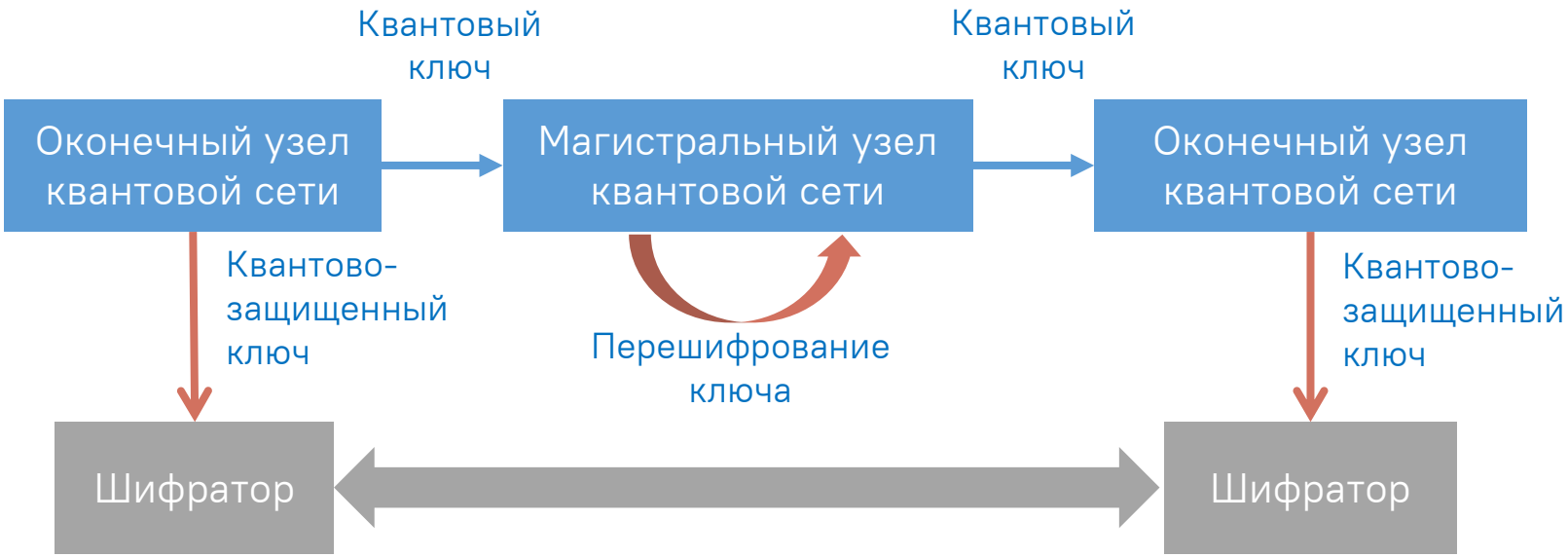
Оптический коммутатор – ViPNet QSS Switch

Распределительный узел квантовой сети – центр «звезды» ViPNet РУКС Лайт

Потребители ключей. IP-телефоны – ViPNet QSS Phone

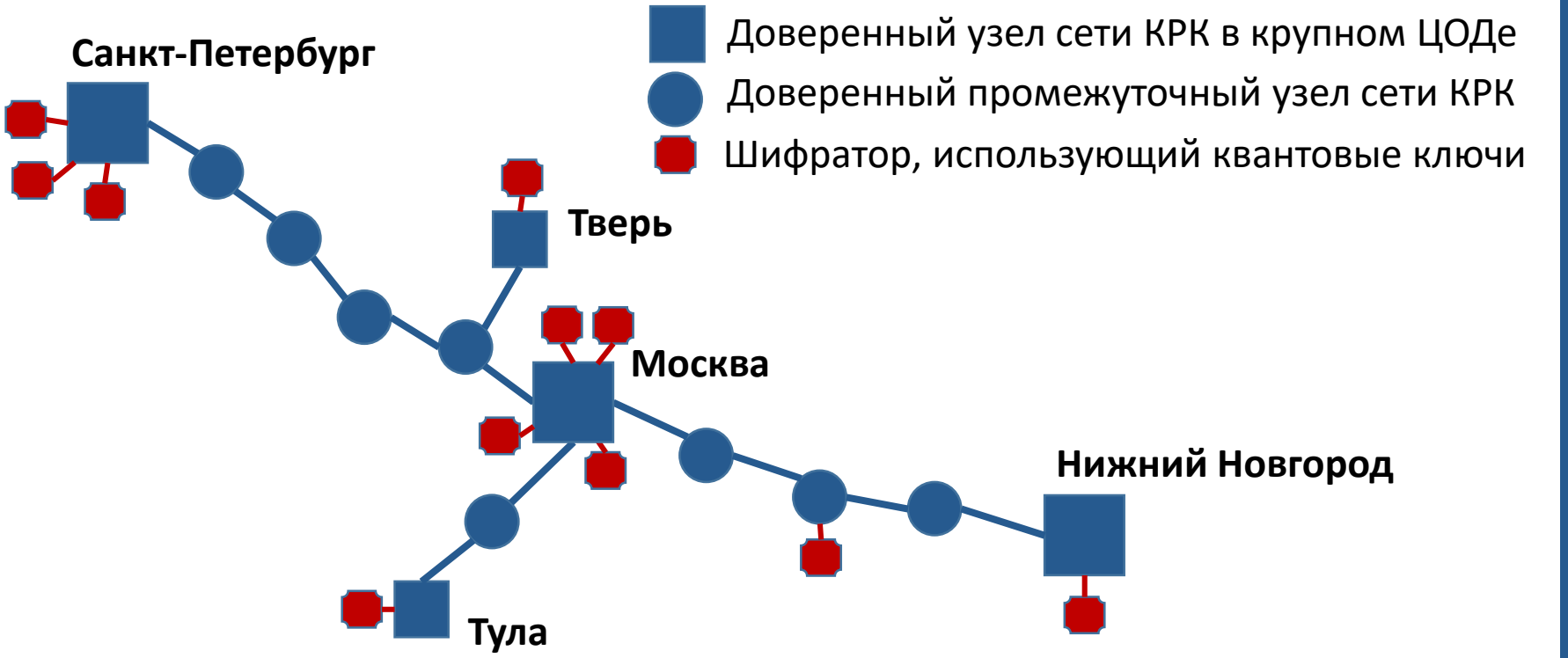
Клиентский узел квантовой сети – ViPNet КУКС Лайт (до 800 шт к одному)

Защита магистральных каналов связи квантовыми ключами - идея



- Квантово-защищенный ключ (КЗК) передается по сети под защитой квантовых ключей на сегментах
- КЗК используется шифраторами как аналог квантового ключа

Защита магистральных каналов связи квантовыми ключами - сценарий



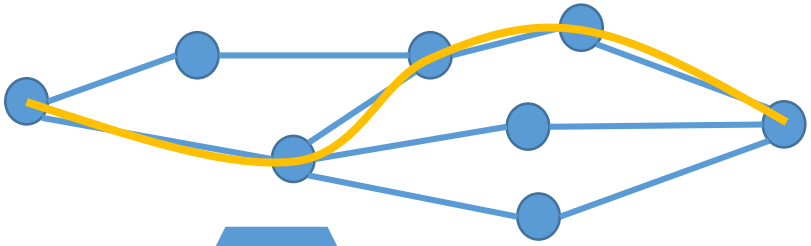
Защита магистральных каналов связи квантовыми ключами - продуктовое решение

Магистральный узел квантовой сети (МУКС)

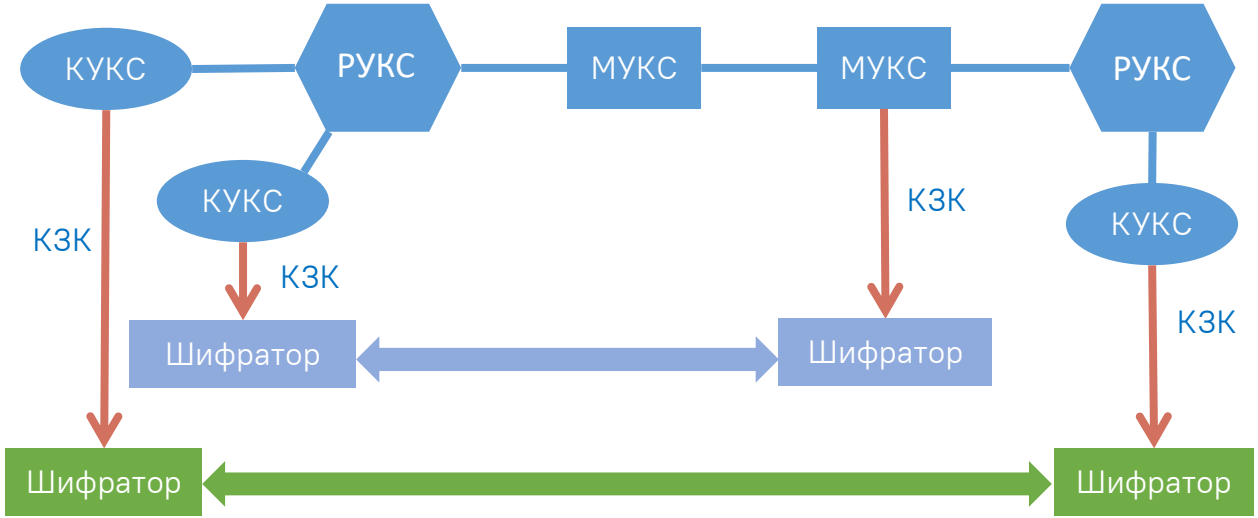
- Алиса и Боб в одном корпусе
- Длина сегмента – до 100 км
- Требуется только одно волокно
- Подключение шифраторов по интерфейсу ProtoQa (ТК-26)
- Интеграция с экосистемой продуктов ViPNet VPN

Защита распределенных сетей произвольной топологии квантовыми ключами - идея

Поиск оптимального пути в сети квантовых узлов



Сервисная модель сети КРК на основе доверенных промежуточных узлов



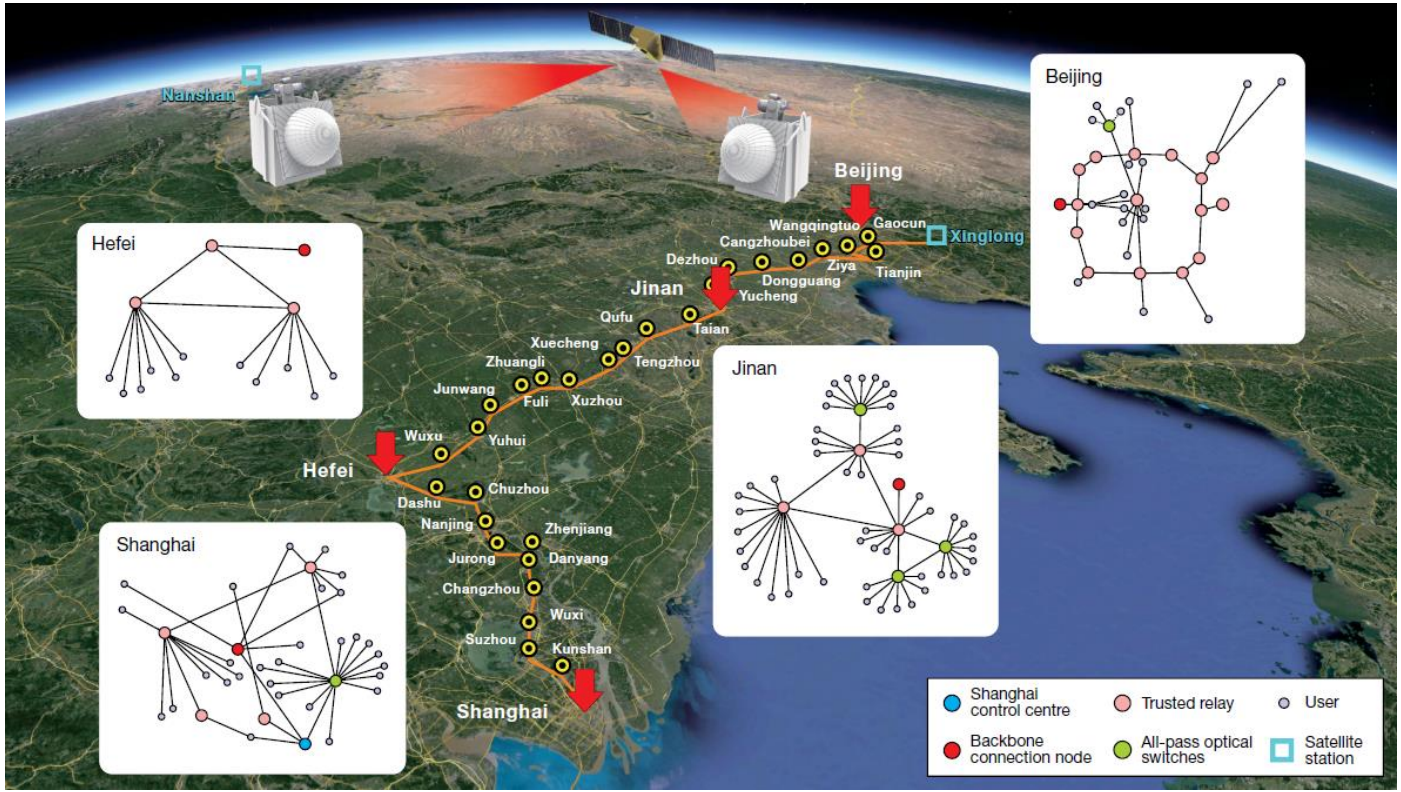
МУКС – Магистральный узел квантовой сети

РУКС – Распределительный узел квантовой сети

КУКС – Клиентский узел квантовой сети

КЗК – Квантово-защищенный ключ

Защита распределенных сетей произвольной топологии квантовыми ключами - сценарий



Квантовая сеть Китая

- 400 сегментов
- 2 спутника
- 4800 км общая протяженность
- 157 потребителей

Защита распределенных сетей произвольной топологии квантовыми ключами - продуктовое решение

Магистральный узел квантовой сети (ViPNet МУКС)

- Алиса и Боб в одном корпусе
- Подключение шифраторов

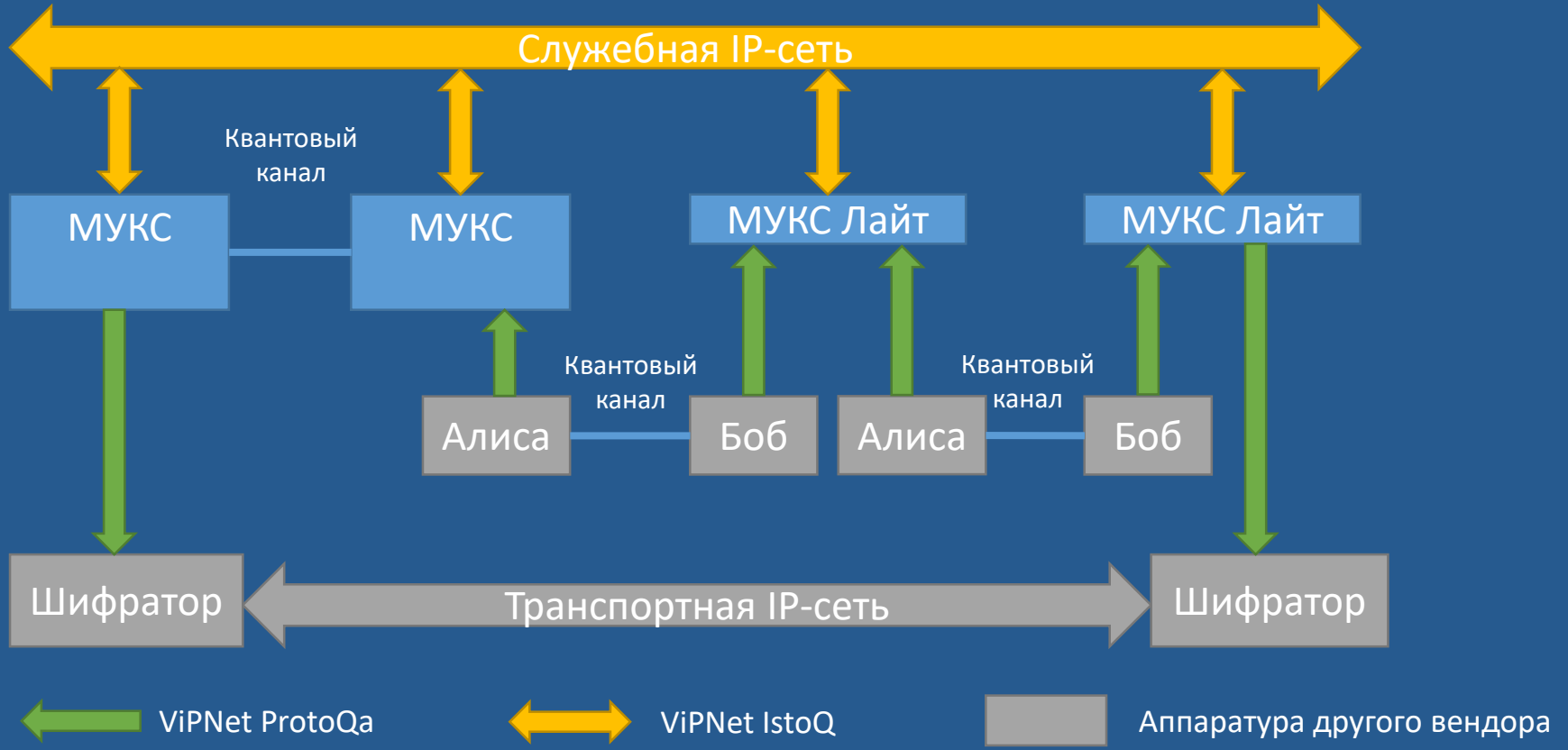
Распределительный узел квантовой сети (ViPNet РУКС) – центр «звезды»

- Управление оптическим коммутатором
- Подключение к ViPNet МУКС
- Подключение ViPNet КУКС

Клиентский узел квантовой сети (ViPNet КУКС)

- Подключение к ViPNet РУКС
- Подключение шифраторов

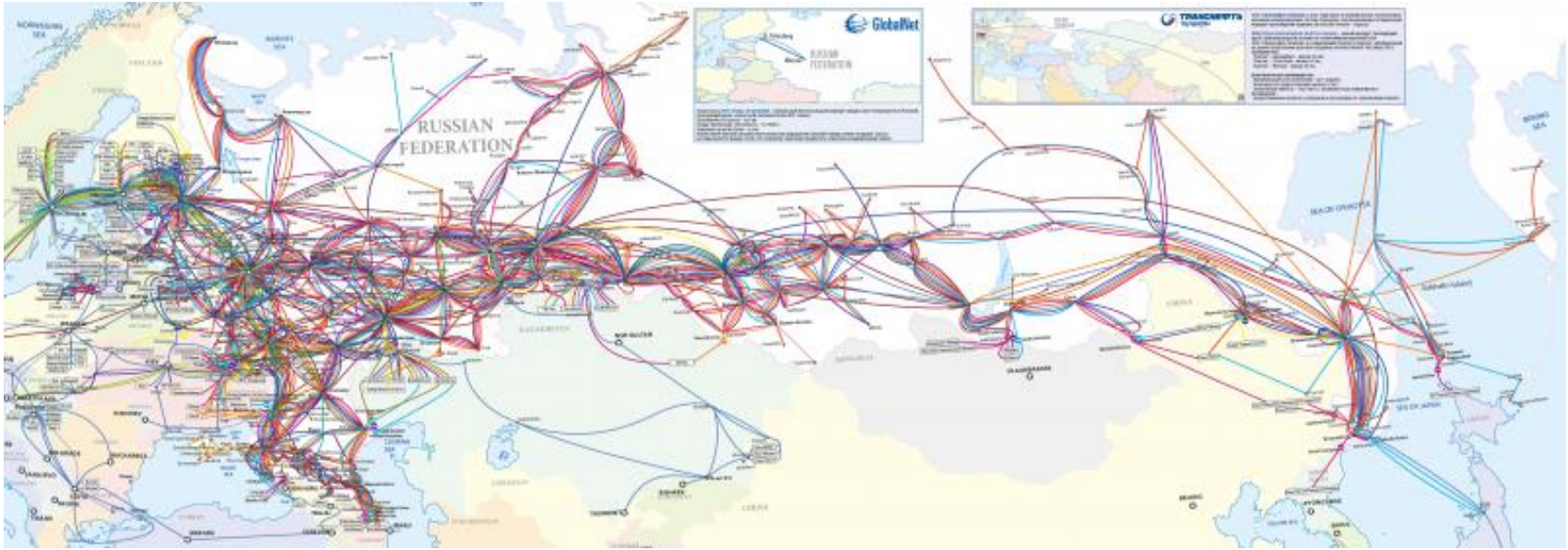
Возможная архитектура интеграции систем КРК различных вендоров



Перспективы развития сетей квантового распределения ключей в России

Магистральные сети связи в России (по материалам © ComNews 21.10.2020)

Разработка линейки доверенных промежуточных узлов (ViPNet МУКС, РУКС, КУКС) субсидирована МПТ России



infotecs

Спасибо
за внимание!