

Использование продуктов ViPNet для построение квантовых сетей

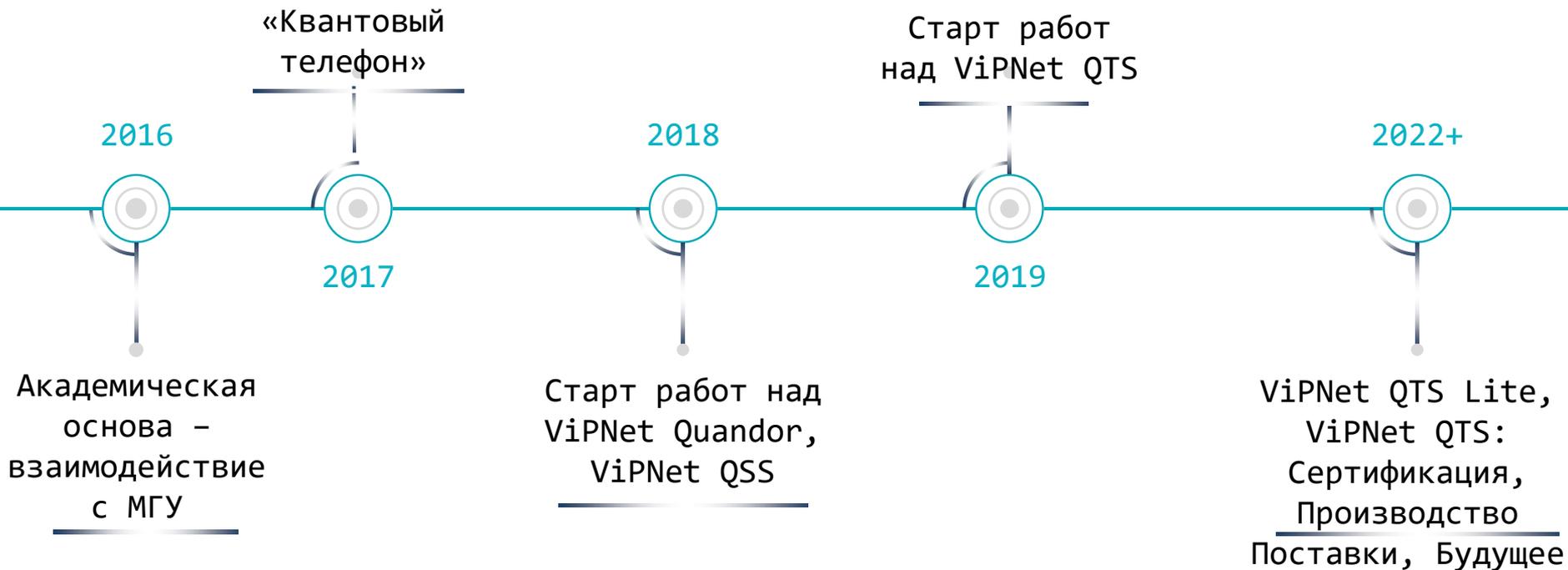


техно infotecs
2023 Фест
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

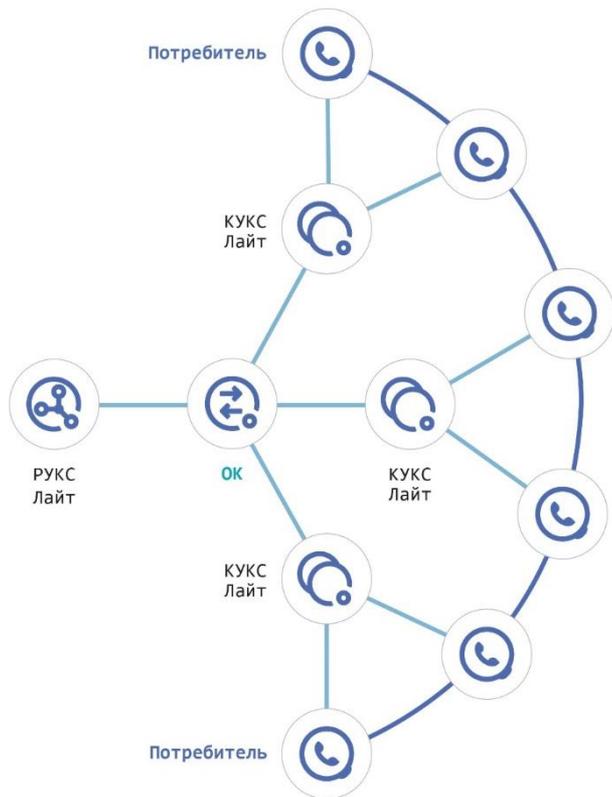
Иванов Олег
Менеджер

Этапы большого пути

Ретроспектива событий



VIPNet QTS Lite



- Распределяет квантовые ключи по сетевой топологии «Звезда» для большого числа абонентов
- Бесшовная интеграция с существующими сетями на базе технологии VIPNet
- Математически доказанная стойкость квантового протокола
- Шифрование телефонного трафика на ключах, не известных даже администратору сети
- Возможность выработки на одном Клиенте КРК квантовозащищенных ключей для нескольких абонентов
- Полностью автоматическая регулярная смена ключей шифрования



VIPNet РУКС Лайт

Распределительный узел квантовой сети

Предназначен для объединения различных сегментов квантовой сетей



- Один оптический модуль в корпусе
- Металлический корпус с датчиком несанкционированного доступа (ДНСД)
- Производительность генерации квантовых ключей – не менее 1 ключа в минуту
- Максимальная дальность квантового канала 44 км
- Размер 2U в 19” стойку глубиной не менее 800 мм. Масса – 14 кг
- Потребление не более 250 Вт, блоки питания с горячей заменой



VIPNet QSS Switch

Оптический коммутатор квантовых сетей

Предназначен для организации оптической сети для передачи квантовых состояний между квантовыми устройствами

- Габариты – 1U
- Масса – 4,6 кг
- Потребляемая мощность – до 15 Вт
- 12 оптических портов FC\UPC
- Вносимое затухание – не более 1,9 дБ





VIPNet KUKS Лайт

Клиентский узел квантовой сети

Предназначен для установки в доверенной зоне для снабжения ключами СКЗИ-потребителей

- Один оптический модуль в корпусе
- Корпус с датчиком несанкционированного доступа
- Производительность генерации квантовых ключей – не менее 1 ключа в минуту
- Максимальная дальность квантового канала 44 км
- Корпус формата Midi Tower
- Потребление не более 250 Вт, блоки питания с горячей заменой
- Масса – 20 кг





VIPNet CSS Connect HW

Защищенный IP-телефон

Предназначен для защиты информации с использованием квантовых ключей



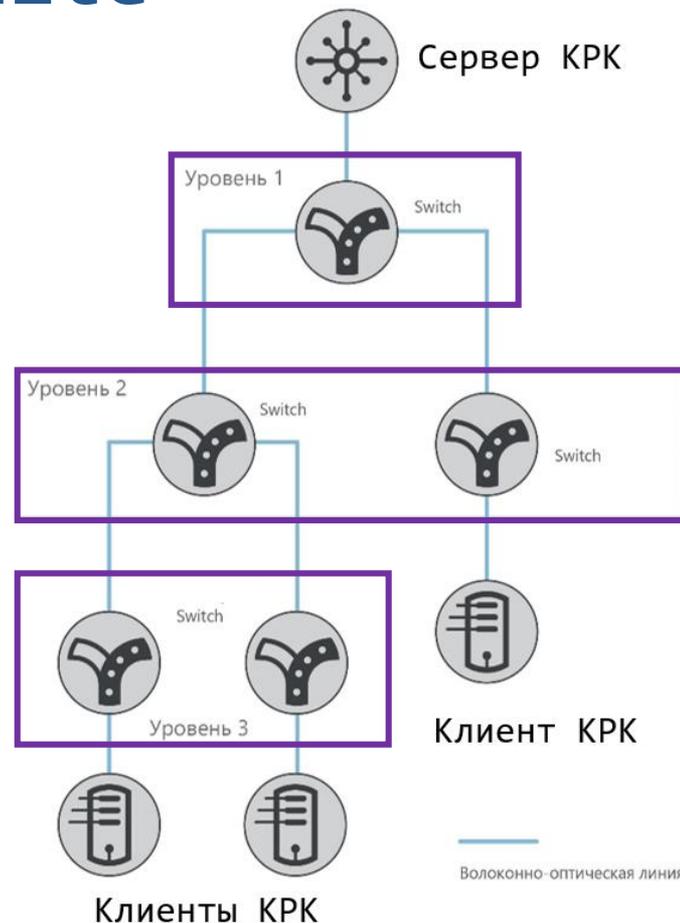
Исполнение на базе аппаратной платформы GrandStream



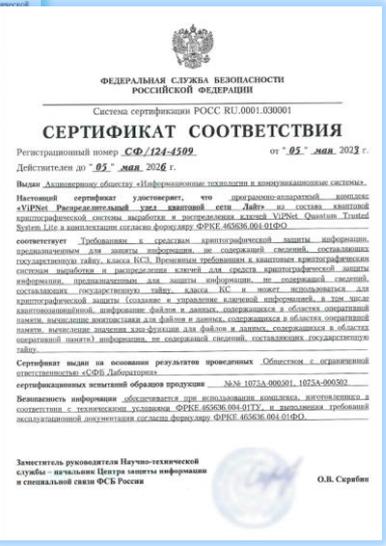
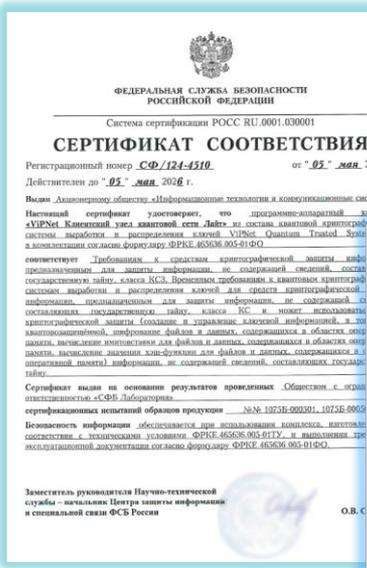
Исполнение на базе аппаратной платформы Aquarius

Комплекс ViPNet QTS Lite

- Три уровня оптической коммутации с резервированием каналов
- Более 1500 Клиентов КРК, подключенных к одному Серверу КРК
- К одному Клиенту КРК можно подключить более 100 потребителей ключей (IP-телефонов) в пределах одной зоны доверия
- Гибридная ключевая система:
 - квантовозащищенные ключи (КЗК) формируются из частей квантовых и классических предраспределенных ключей.



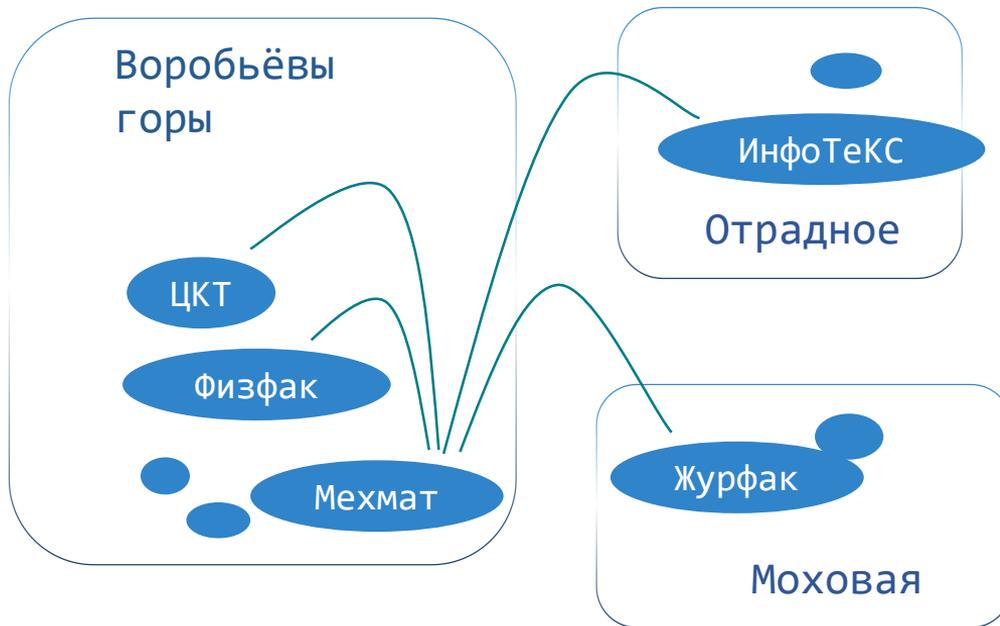
Сертификация



- ViPNet Клиентский узел квантовой сети Лайт (КУКС Лайт)
- ViPNet Распределительный узел квантовой сети Лайт (РУКС Лайт)
- соответствуют требованиям к СКЗИ и временным требованиям к квантовым криптографическим системам выработки и распространения ключей для СКЗИ

Университетская Квантовая Сеть

- 1 РУКС Лайт
- 5 КУКС Лайт
- 22 абонентских пунктов
- 40 км самый длинный луч
- Подключены подразделения МГУ и головной офис ИнфоТеКС



Пилоты и проекты

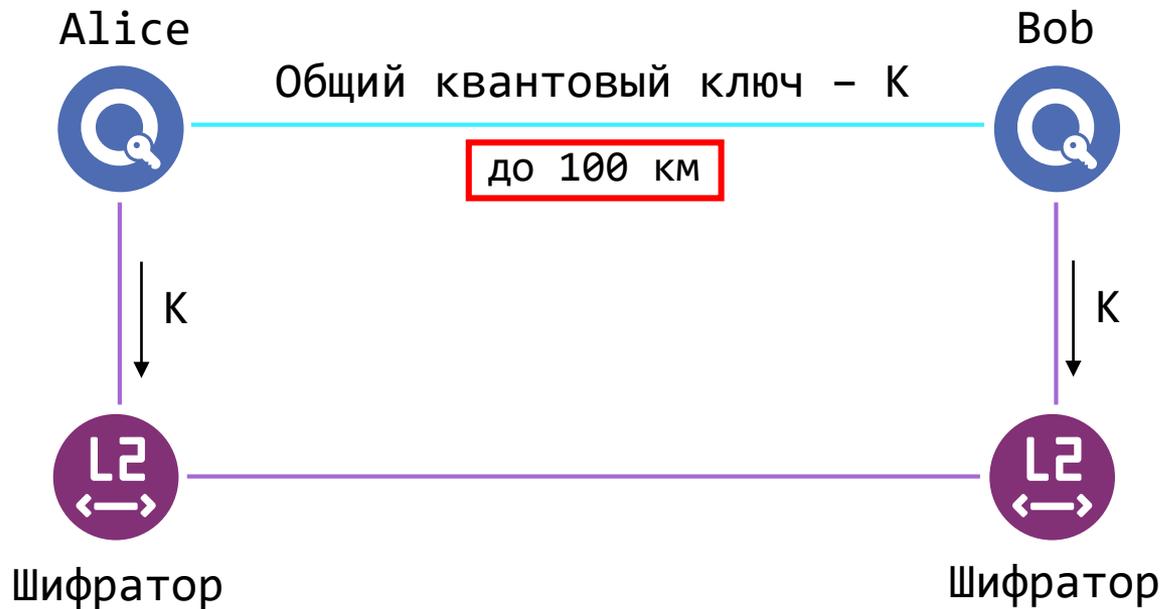


**Собственные пилоты –
внутренняя сеть
эксплуатации**

- 1 РУКС Лайт
 - 3 КУКС Лайт
 - 1 QSS Switch
 - 3 абонентских пункта
-
- 1 РУКС Лайт
 - 2 КУКС Лайт
 - 1 QSS Switch
 - 26 абонентских пунктов

ViPNet Quantum Trusted System

Простейшая квантовая сеть «точка-точка»



Проблема ограничения длины оптического канала

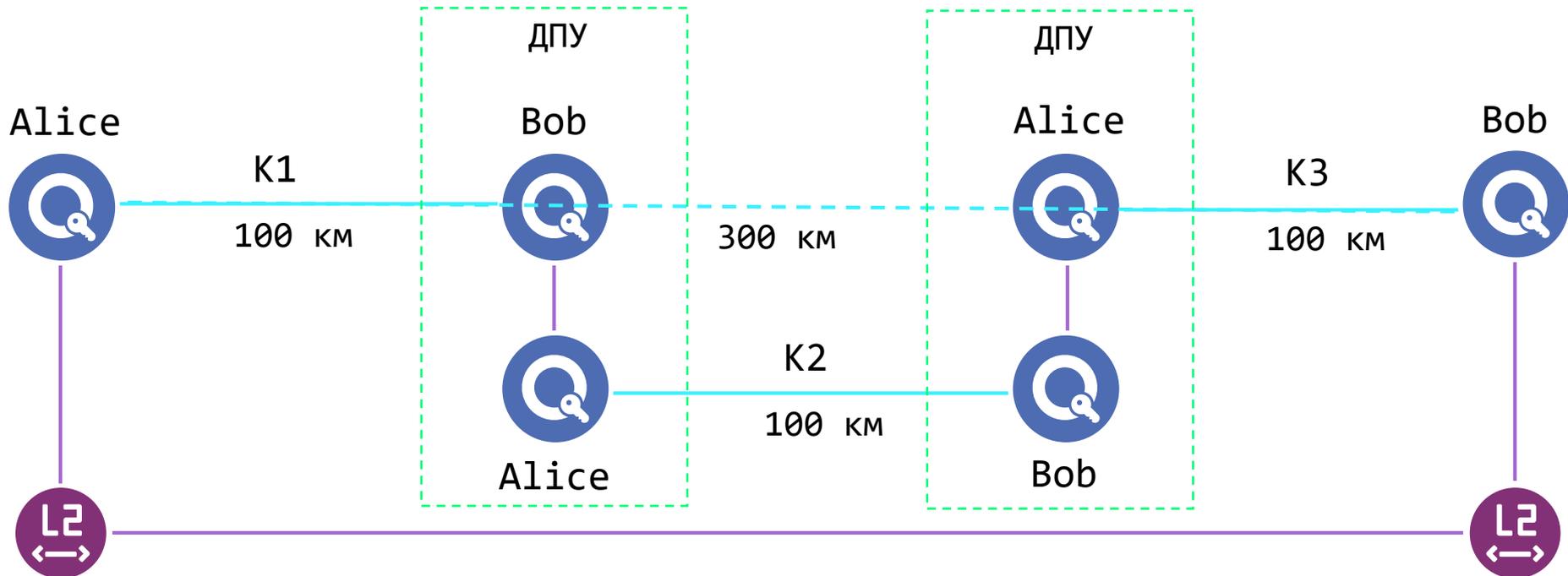


- Для продуктов ViPNet расстояние между квантовыми узлами – до 100 км
- Подобное ограничение есть у всех вендоров
- Причина:

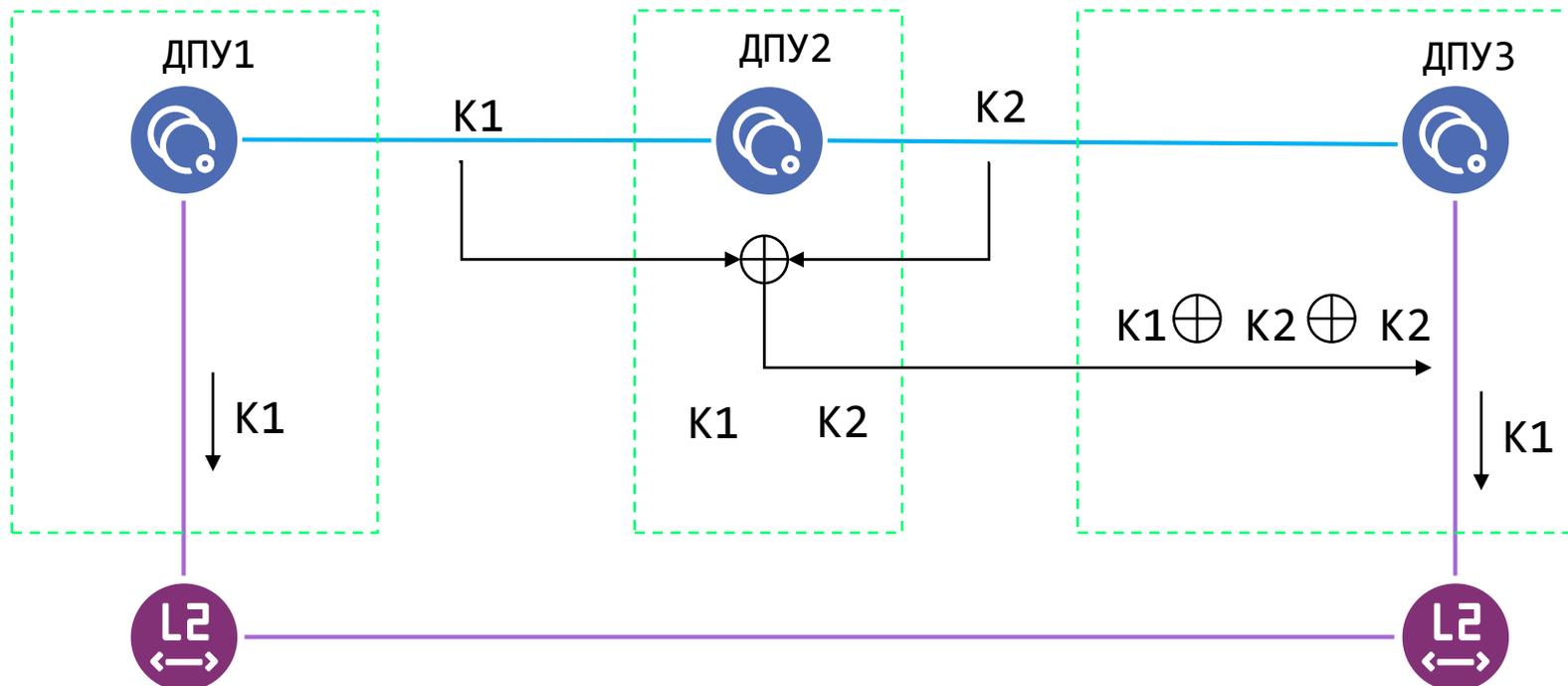


Решение проблемы – доверенный промежуточный узел

ДПУ – доверенный промежуточный узел

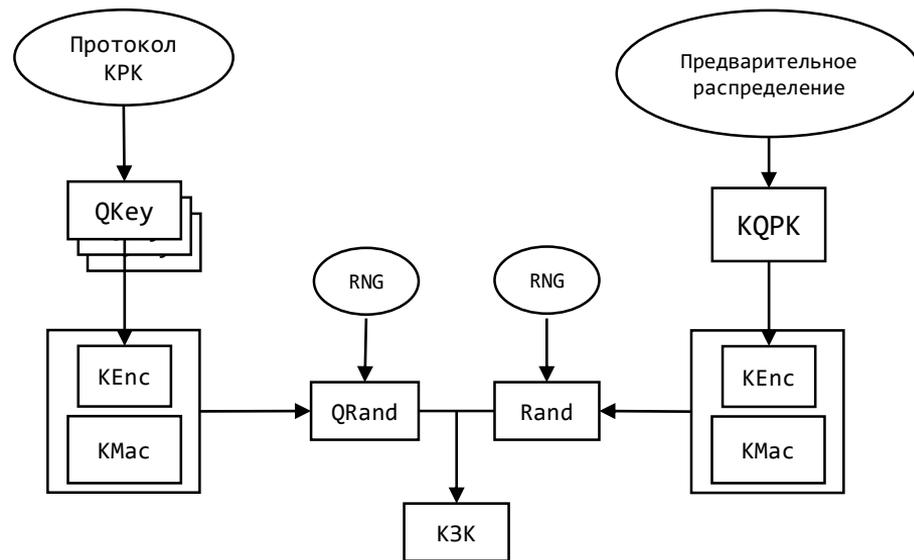


Простой пример выработки общего ключа



В реальности всё сложнее...

- КЗК – квантовозащищенный ключ
- КЗК создается из составляющих, каждая из которых суть ключевая информация
 - Часть составляющих передается с защитой на классических предраспределенных ключах
 - Часть составляющих передается с защитой на квантовых ключах
- Компрометация *отдельно* классических или квантовых ключей не приведет к компрометации КЗК



Система доверенных узлов

Комплексный проект по субсидии МПТ «Разработка технологии и аппаратуры сетей КРК с использованием доверенных узлов»

Результат разработки: доверенные промежуточные узлы квантовой сети



Клиентский
(КУКС)



Распределительный
(РУКС)



Магистральный
(МУКС)

Проведено пилотирование макетов

ViPNet МУКС/ПУКС



- Квантовый канал до 100 км
- Алиса и Боб в одном корпусе
- 4U защищенный корпус
- Масса ~ 40 кг
- До 8 потребителей

ViPNet КУКС



- Один квантовый оптический модуль в корпусе
- 2U защищенный корпус
- Масса ~ 20 кг
- До 8 потребителей

L2 ViPNet L2Q-10G

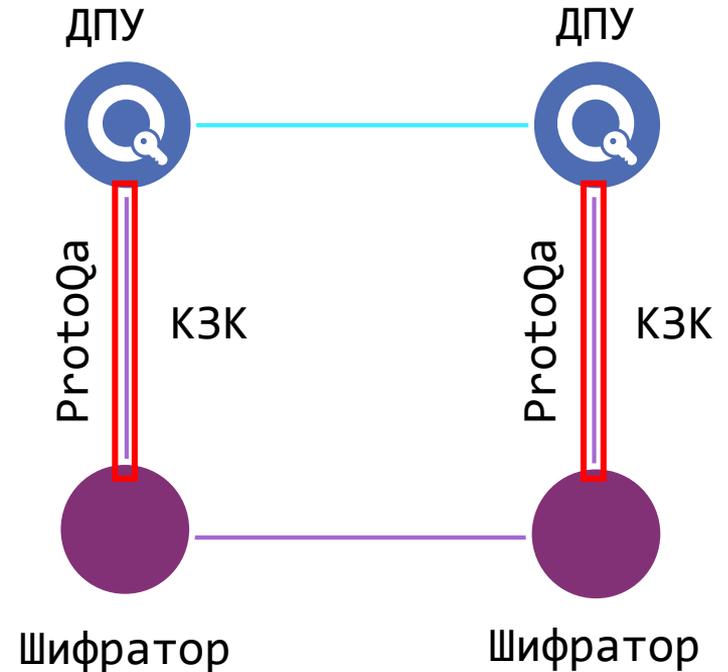
Шифратор канального уровня

- Производительность шифрования до 10 Гбит/с
- Металлический корпус с датчиком несанкционированного доступа (ДНСД)
- Размер 1U в 19” телеком-стойку



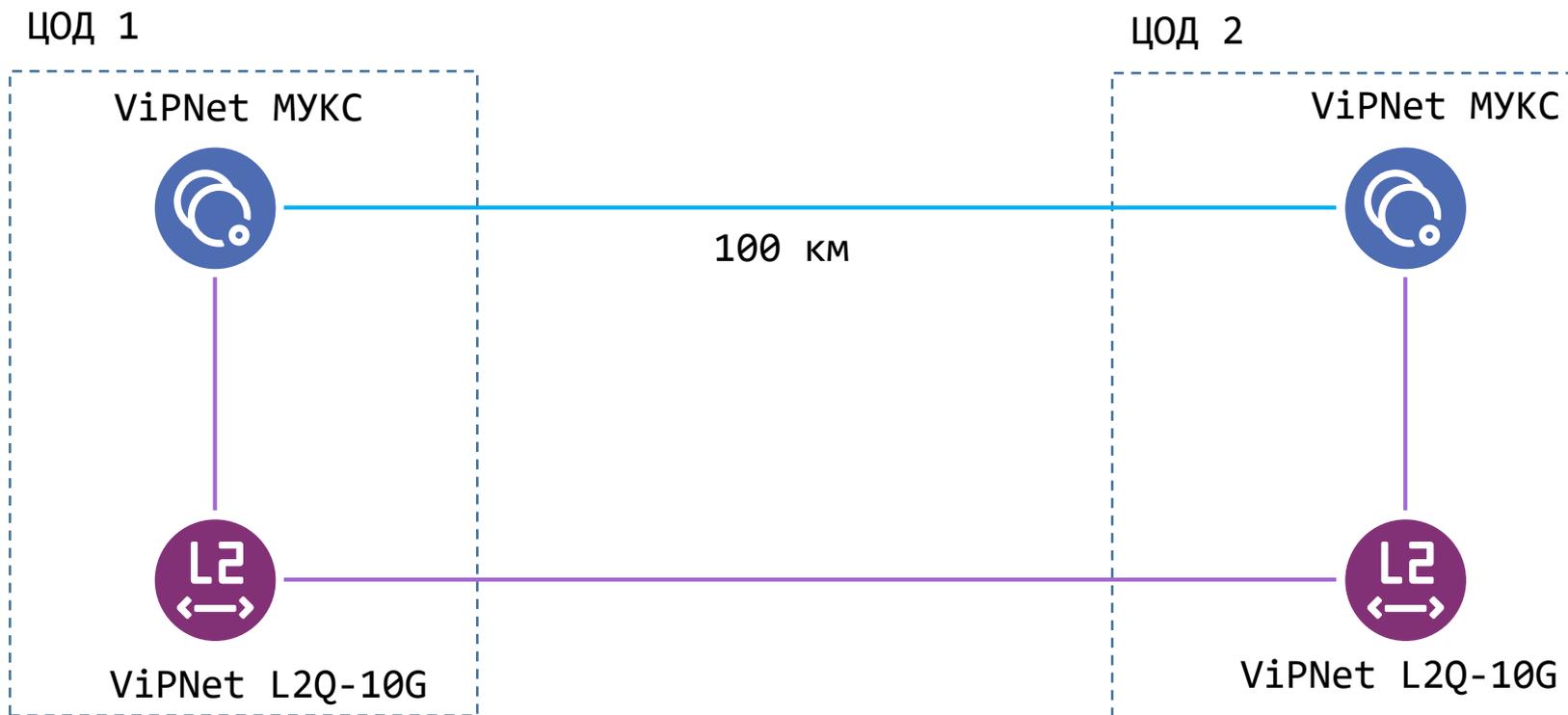
Потребитель ключей – любой шифратор с ProtoQa

- ProtoQa – протокол защищенного взаимодействия между узлом квантовой сети и потребителем ключей
- Построен по принципу запрос-ответ
- Защищен протоколом CRISP

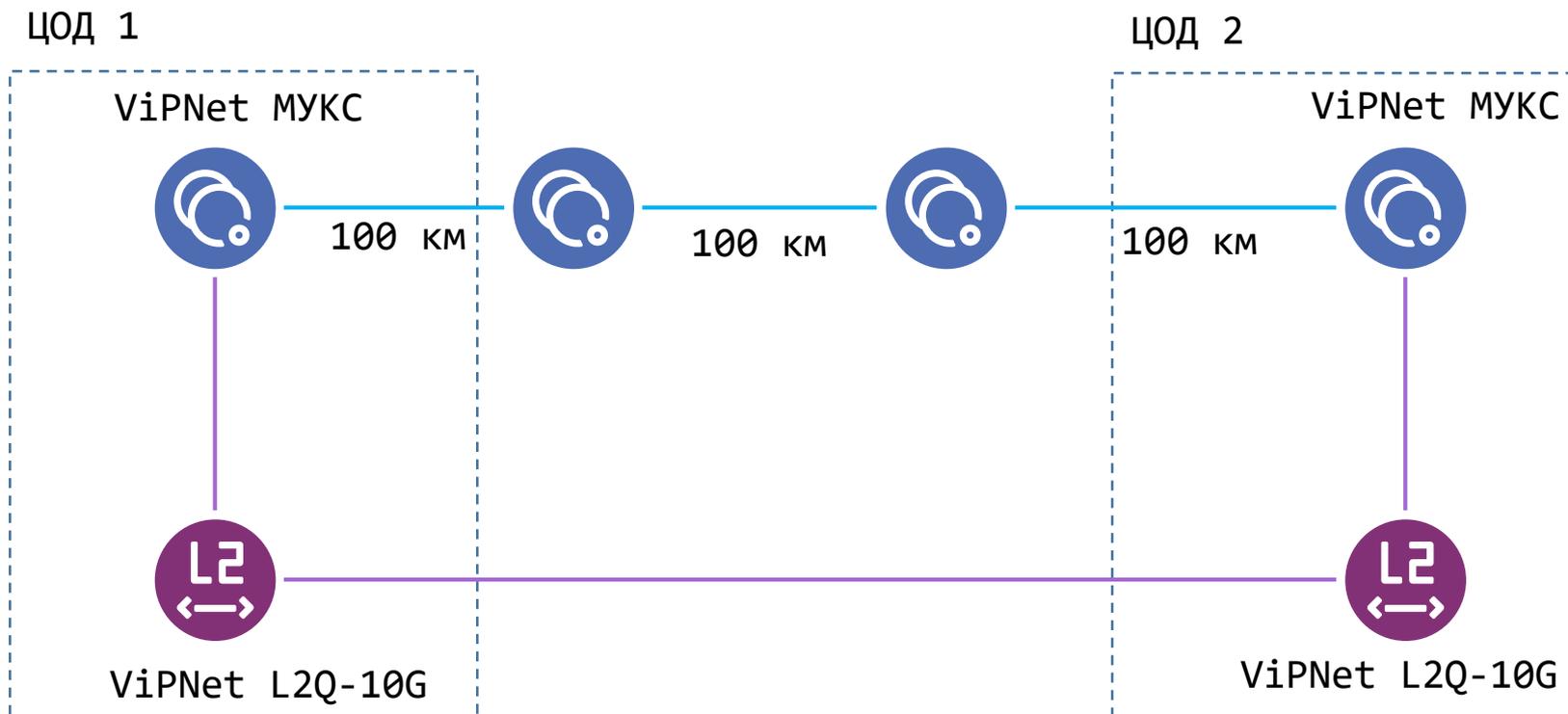


Возможные топологии квантовых сетей на базе ViPNet QTS

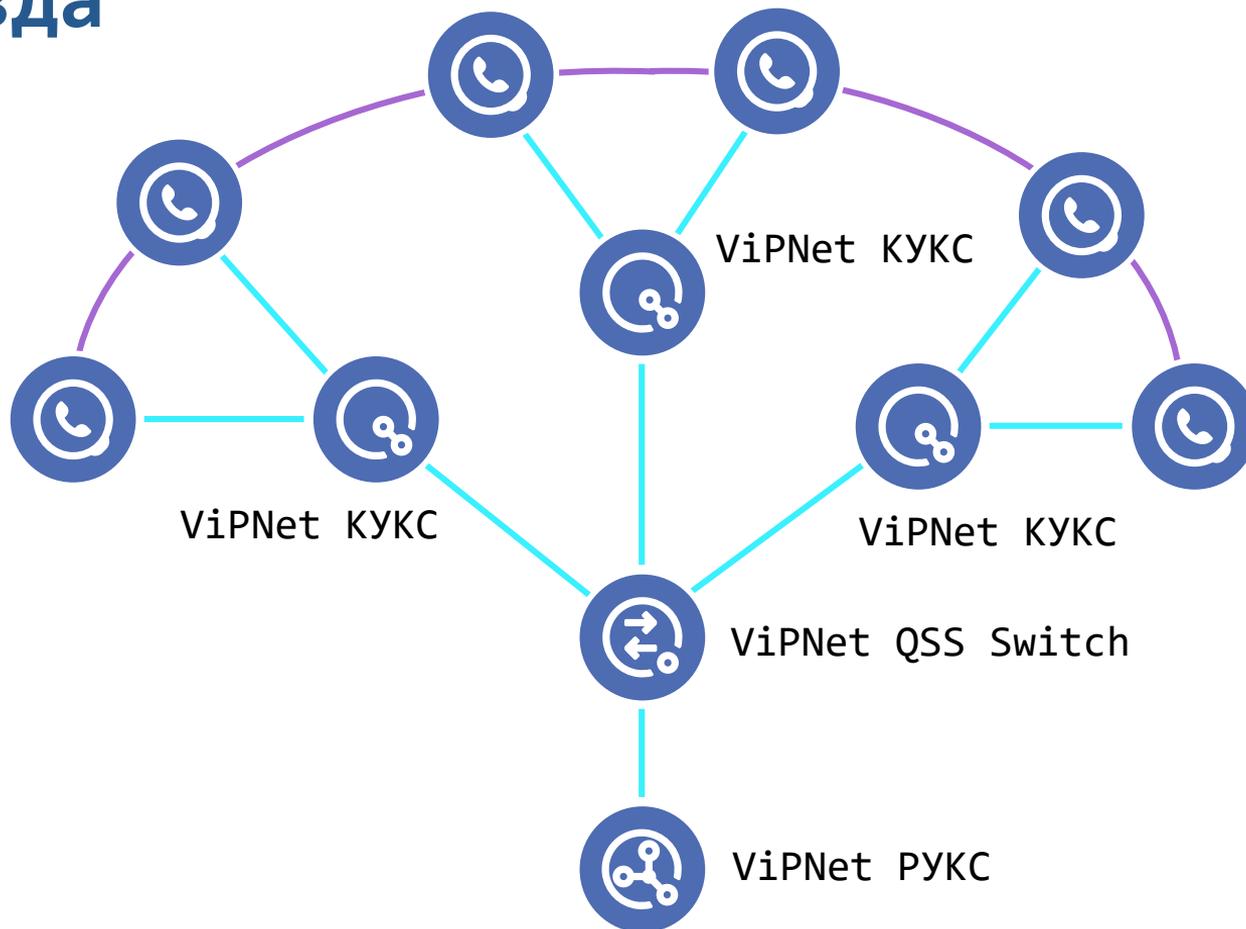
Точка-Точка



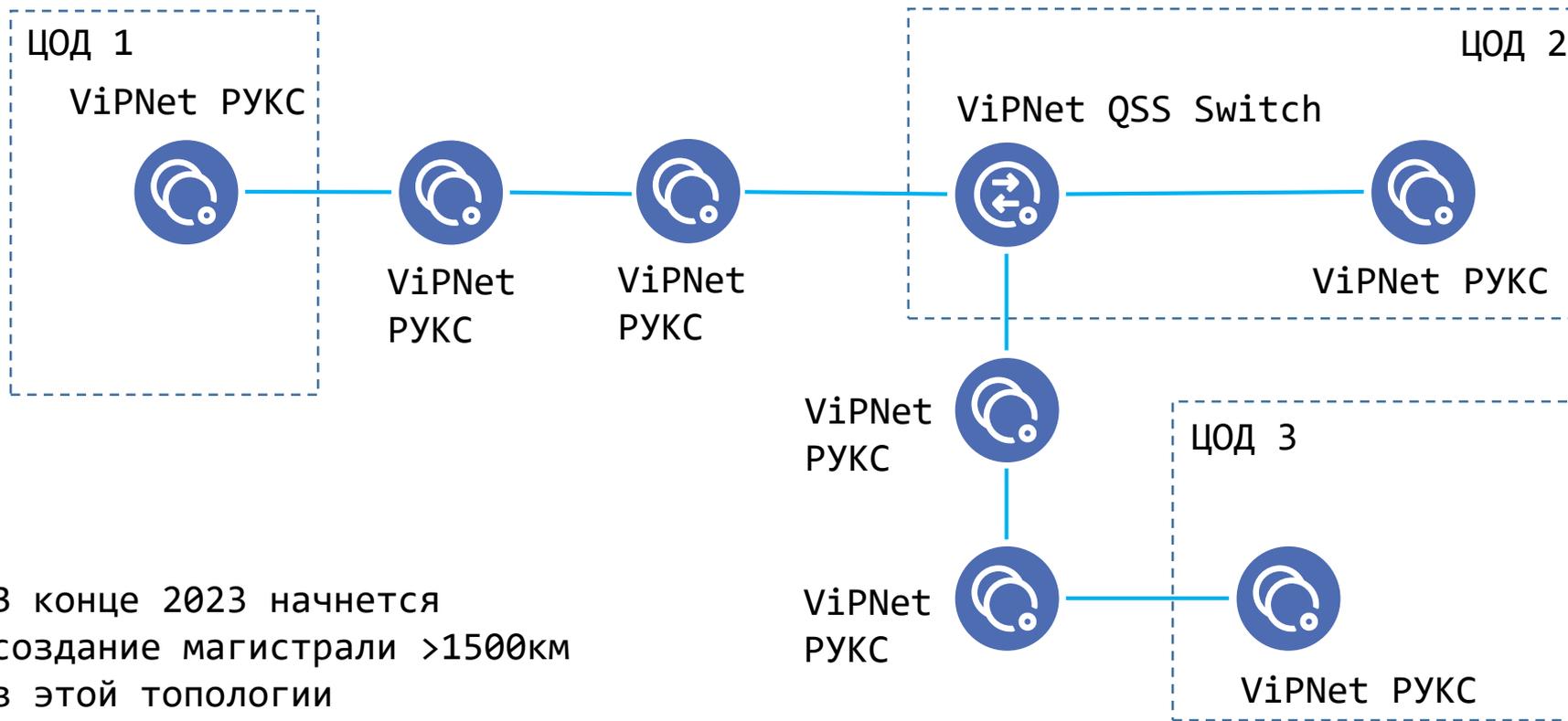
Магистраль



Звезда



Магистраль с ответвлением



В конце 2023 начнется
создание магистрали >1500км
в этой топологии

Опыт

Этапы пилотов

Подготовительный этап

Рефлектометрия линии

Определение длины
и потерь

Сеть ViPNet VPN

Квантовые узлы

Классические узлы

Служебный канал

Абонентские пункты

Сеть КРК

Монтаж оборудования

Ввод ключевой и
справочной информации

Линия

- Темное волокно
- Одномодовое волокно
- Допускаются переходники FC/UPC
- На длине волны 1550 нм потери не более 0,2 дБ на км

Размещение

- Согласно ПКЗ 2005
- Телекоммуникационная сеть для служебных каналов
- Рабочий температурный диапазон от +10 до +40 °C

Трудности запуска и эксплуатации

Монтаж

- Дефекты линии
- Грязные разъемы
- Ошибки подключения
- Подрядчик заменил участок оптоволокна медью через конверторы **(реальная история!)**

Линия

- Длина (19 км по прямой = 40 км волокна)
- Перегиб волокна
- Повреждение линии
- Низкое качество соединений

Эксплуатация

- Качество линии напрямую влияет на время выработки и распределения ключей
- Контроль и ответственность эксплуатирующих и смежных служб

Производство

Собственное производство в Томске



Возможности

Полный технологический цикл
опытного и мелкосерийного
производства

Поддержка максимально
возможного уровня
локализации производства

Собственное производство в Томске



Этапы строительства:

1

Начало строительства:
июнь 2022 года

2

Ввод в эксплуатацию
1 очереди: в 2023

3

Ввод в эксплуатацию
2 очереди: к 2025 году

техно infotecs
2023 Фест

Спасибо
за внимание!

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363