

VIPNet QCS: от обучения до построения магистральных квантовых сетей

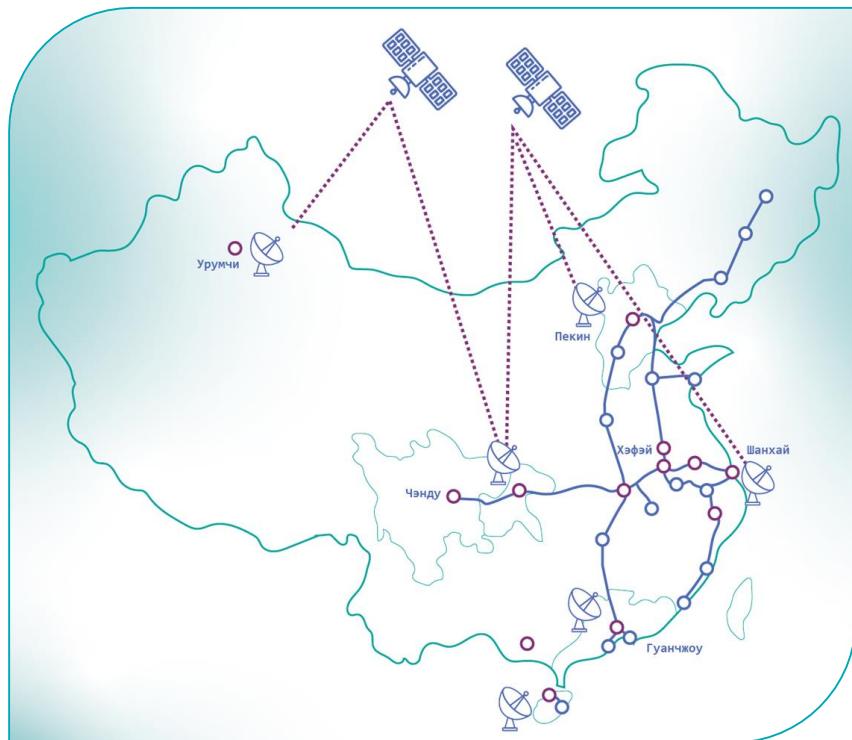
Иванов Олег
Менеджер продуктов



Стратегия государства в области развития квантовых коммуникаций:

- Распоряжением Правительства Российской Федерации от 11 июля 2023 г. № 1856-р утверждена [Концепция регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года](#)
- Осуществляется реализация "[дорожной карты](#)" развития высокотехнологичного направления "Квантовые коммуникации" в рамках национальной программы "Цифровая экономика Российской Федерации" и ее преемнице «Экономике данных»
- Распоряжением Правительства Российской Федерации от 24 ноября 2023 г. № 3339-р утверждена. [Стратегия развития отрасли связи Российской Федерации на период до 2035 года](#)
- [Перечень поручений Президента Российской Федерации](#) от 3 сентября 2023 г. № Пр-1734 по итогам встречи с учеными и пленарного заседания Форума будущих технологий «Вычисления и связь. Квантовый мир»
- [Комитет Совета Федерации по обороне и безопасности](#) 6 февраля 2024 [рассмотрел и взял на контроль](#) вопрос обеспечения ИБ с применением квантовых технологий в рамках национального проекта по формированию [Экономики Данных](#)

Сеть КРК в Китае



Создавалась с **2013** года

>10 000 км протяженность

40 сегментов **2** спутника

Оборудование нескольких производителей

>150 потребителей

- узлы в отделениях госбанка Китая
- коммерческие услуги в крупных городах (Пекин, Шанхай, Гуанчжоу)

Сети КРК в Европе

Программа Quantum Flagship
с 2018 г.

Бюджет €1000М

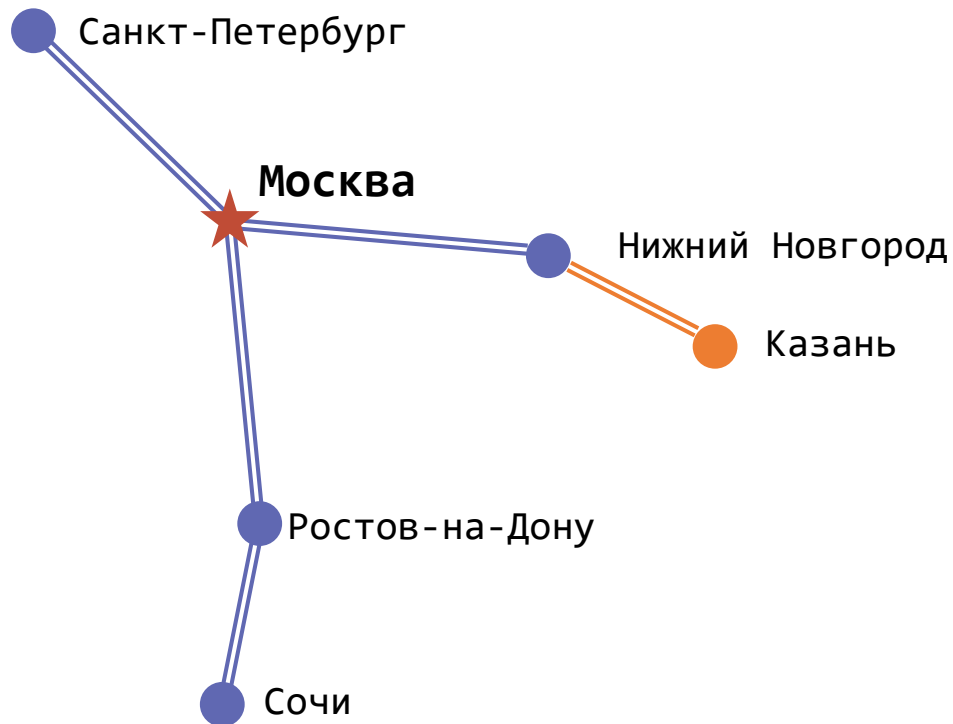
27 европейских стран

7 проектов по КРК



Единая магистральная и спутниковая
сеть КРК **European QCI**
(Quantum Communication Infrastructure)
2023-2030 гг.

Сети КРК в России

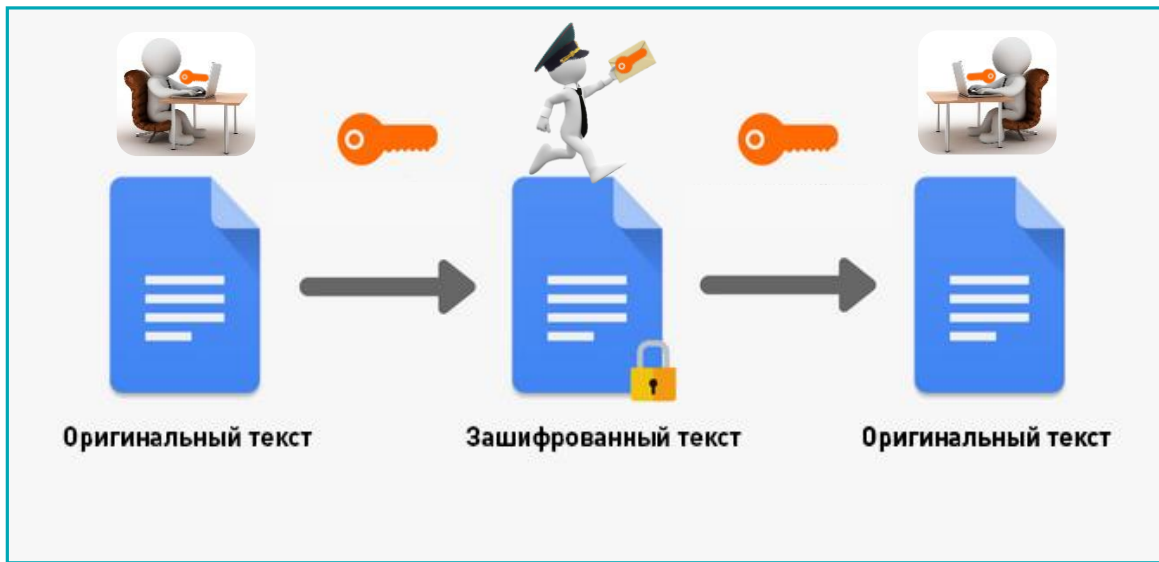


Что такое квантовое распределение ключей



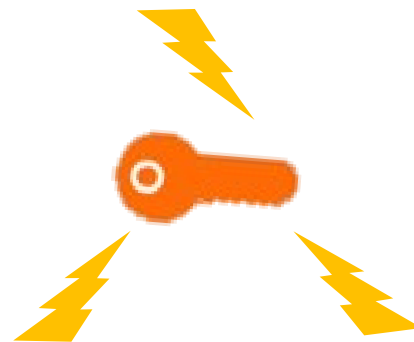
Для чего применяется криптография:

- Защита информации от несанкционированного доступа;
- Защита от подмены трафика;
- Подтверждение авторства.



Угрозы:

Растущие вычислительные мощности и новые алгоритмы взлома



Человеческий фактор

Быстрое расходование

Мотивация применения КРК

Квантовое распределение ключей – это процедура безопасной выработки и распределения симметричных ключей с использованием законов квантовой физики и специальных протоколов

А также:

- Защита от перспективных возможностей криптоанализа;
- Защита от внутреннего нарушителя;
- Шифрование очень больших потоков данных (снижение частой нагрузки на ключ, за счет частой смены ключей);
- Распределение ключей в недоступные иным образом объекты (например, на космические спутники).

Принципы КРК

- Случайный ключ кодируется через состояния фотонов
- Попытка перехвата ключа сразу становится известной
- Невозможно клонировать неизвестное квантовое состояние
- Невозможно измерить квантовое состояние без его изменения

Кодирование через вектор поляризации магнитного поля

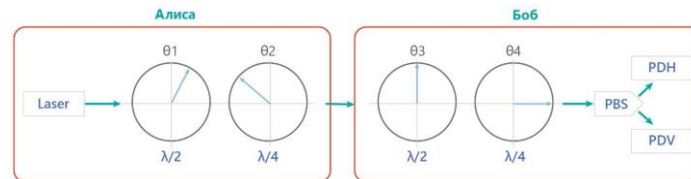
	0	1
Верт. - гор. базис		
Диагональный базис		

ViPNet Quantum Key Distribution Simulator

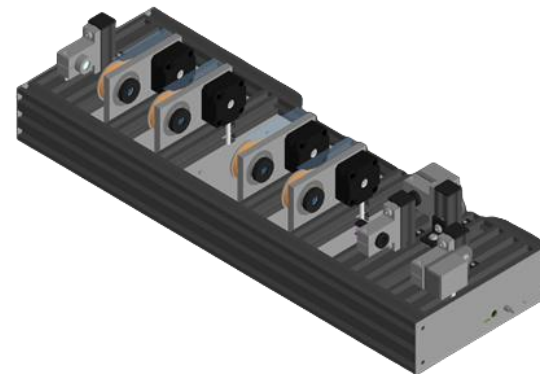
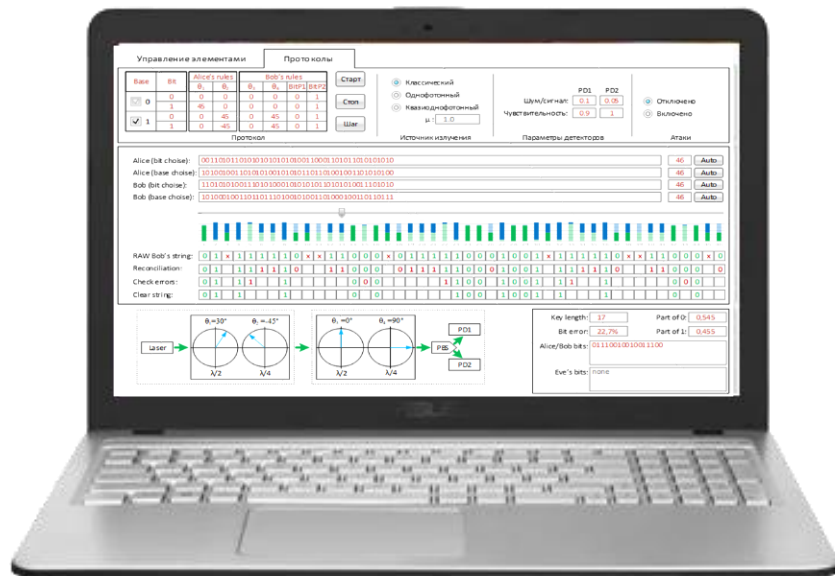
VIPNet QKDSim

АО «ИнфоТекС»

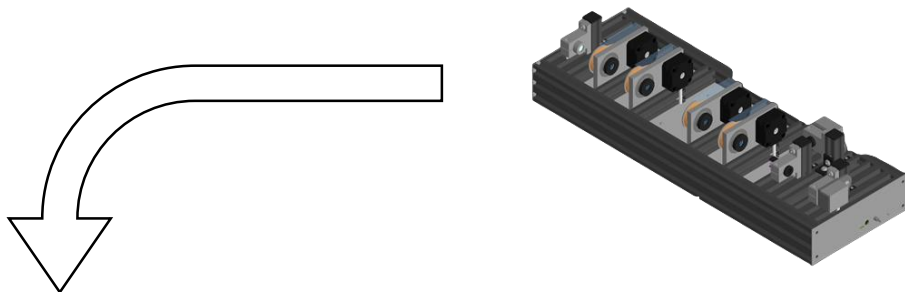
- Программное обеспечение
- Эмулятор аппаратной платформы



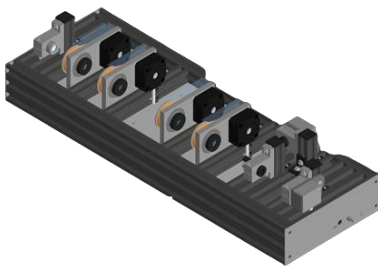
- Аппаратная платформа



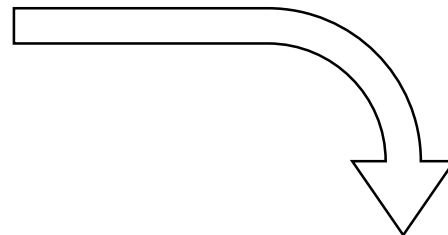
Аппаратная платформа



Улучшает восприятие
материала



Управляется с
ноутбука или ПК



Возможно устанавливать
дополнительное оборудование

Применение в образовательной сфере

Физические основы

Формирование поляризационных состояний

Регистрация поляризованного света

Классическая передача информационных бит

Принципы поляризационного кодирования бит

Принципы детектирования бит

Шумы в детекторах

Ошибки передачи

Квантовая передача информационных бит

Детектирование одиночных фотонов

Шумы в детекторах

Ошибки передачи

Квантовое распределение ключей

Понятие о базисах кодирования

Алгоритмы формирования и детектирования посылок

Постобработка распределяемой последовательности

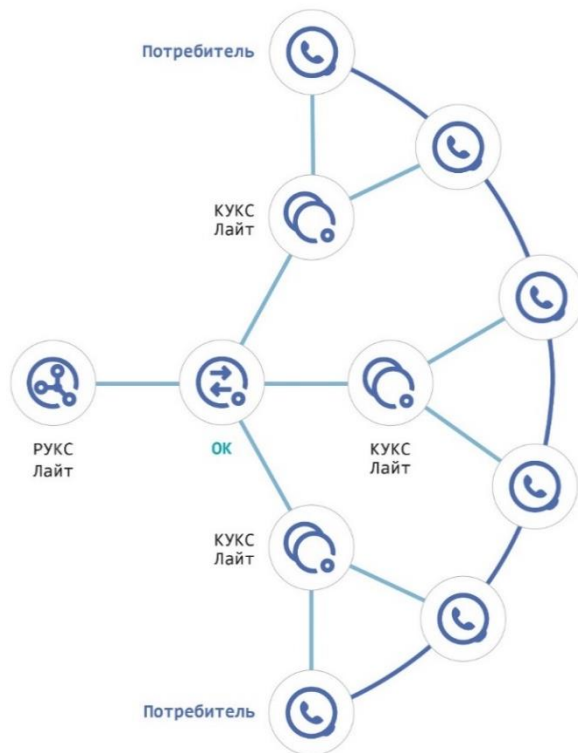
Безопасность передачи и распределения ключей

Проведение атак на протоколы и системы КРК

Связь ошибки распределения ключей с информацией, доступной нарушителю

VIPNet Quantum Trusted System Lite

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 КУКС 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

Сертификация


ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации POCC RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4510 от "05" мая
Действителен до "05" мая 2026 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы»


Настоящий сертификат удостоверяет, что программно-аппаратный комплекс «ViPNet Клиентский узел квантовой сети Лайт» из состава квантовой криптографической системы выработки и распределения ключей ViPNet Quantum Trusted System в соответствии со стандартом ФСТЭК России ФСТЭК.465636.004-01ДФ соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3. Временным требованиям к квантовым криптографическим системам выработки и распределения ключей для средств криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС, и может использоваться для криптографической защиты (создание и управление ключевой информацией, в том числе квантовозамкнутой, шифрование файлов и данных, содержащихся в областях оперативной памяти, выделение индикаторов для файлов и данных, содержащихся в областях оперативной памяти, выделение значений хэш-функций для файлов и данных, содержащихся в областях оперативной памяти) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ.Лаборатория» сертификационных испытаний образцов продукции №№ 1075B-000501, 1075B-000502

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФСТЭК.465636.005-01ТУ, и выполнении требований эксплуатационной документации согласно формуляру ФСТЭК.465636.004-01ДФ.

О.В. Скрюбин




ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации POCC RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4509 от "05" мая 2026 г.
Действителен до "05" мая 2026 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы»

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс «ViPNet Распределительный узел квантовой сети Лайт» из состава квантовой криптографической системы выработки и распределения ключей ViPNet Quantum Trusted System в соответствии со стандартом ФСТЭК России ФСТЭК.465636.004-01ДФ соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3. Временным требованиям к квантовым криптографическим системам выработки и распределения ключей для средств криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС, и может использоваться для криптографической защиты (создание и управление ключевой информацией, в том числе квантовозамкнутой, шифрование файлов и данных, содержащихся в областях оперативной памяти, выделение индикаторов для файлов и данных, содержащихся в областях оперативной памяти, выделение значений хэш-функций для файлов и данных, содержащихся в областях оперативной памяти) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ.Лаборатория» сертификационных испытаний образцов продукции №№ 1075A-000501, 1075A-000502

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФСТЭК.465636.004-01ТУ, и выполнении требований эксплуатационной документации согласно формуляру ФСТЭК.465636.004-01ДФ.

О.В. Скрюбин

- 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

UQN

Университетская
Квантовая Сеть

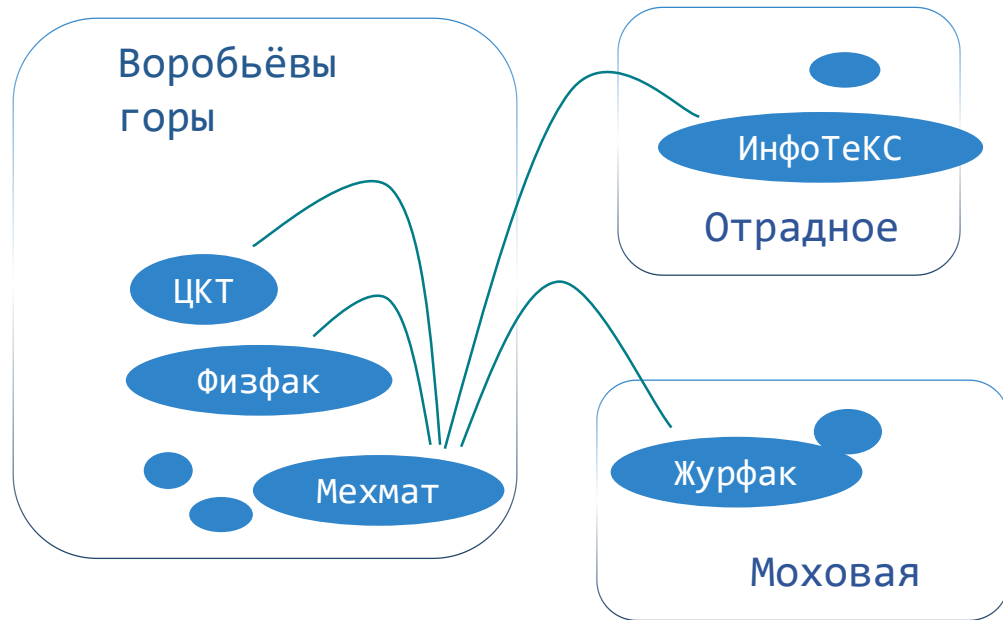
1 РУКС Лайт

5 КУКС Лайт

22 абонентских пунктов

40 км самый длинный луч

Подключены подразделения МГУ
и головной офис ИнфоТеКС



Пилоты и проекты



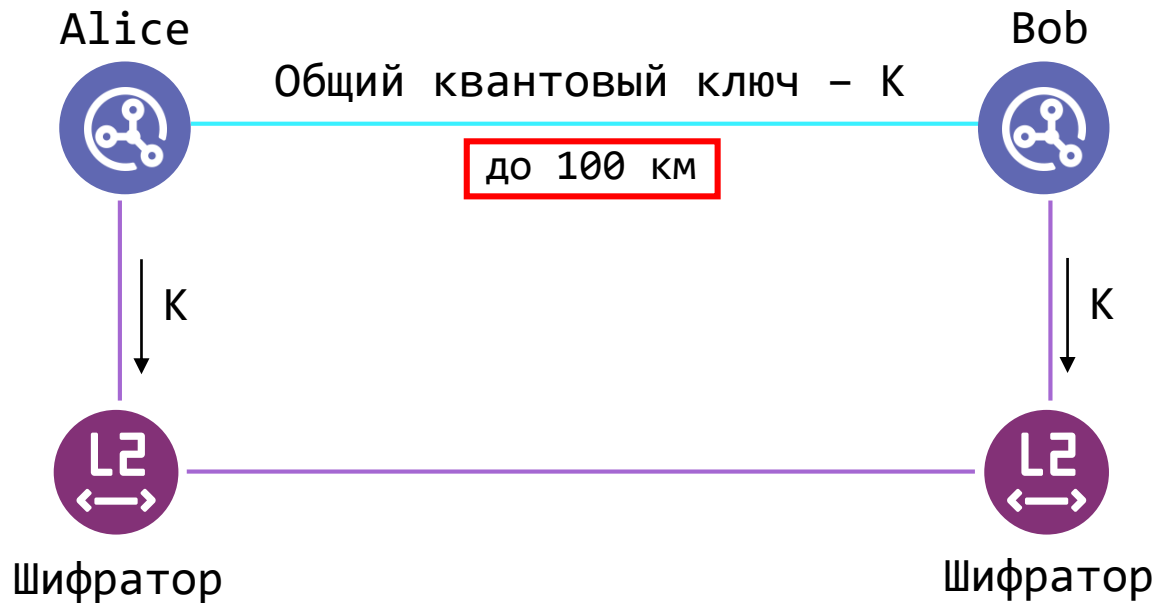
- 1 РУКС Лайт
- 3 КУКС Лайт
- 1 QSS Switch
- 3 абонентских пункта



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

VIPNet Quantum Trusted System

Простейшая квантовая сеть «точка-точка»

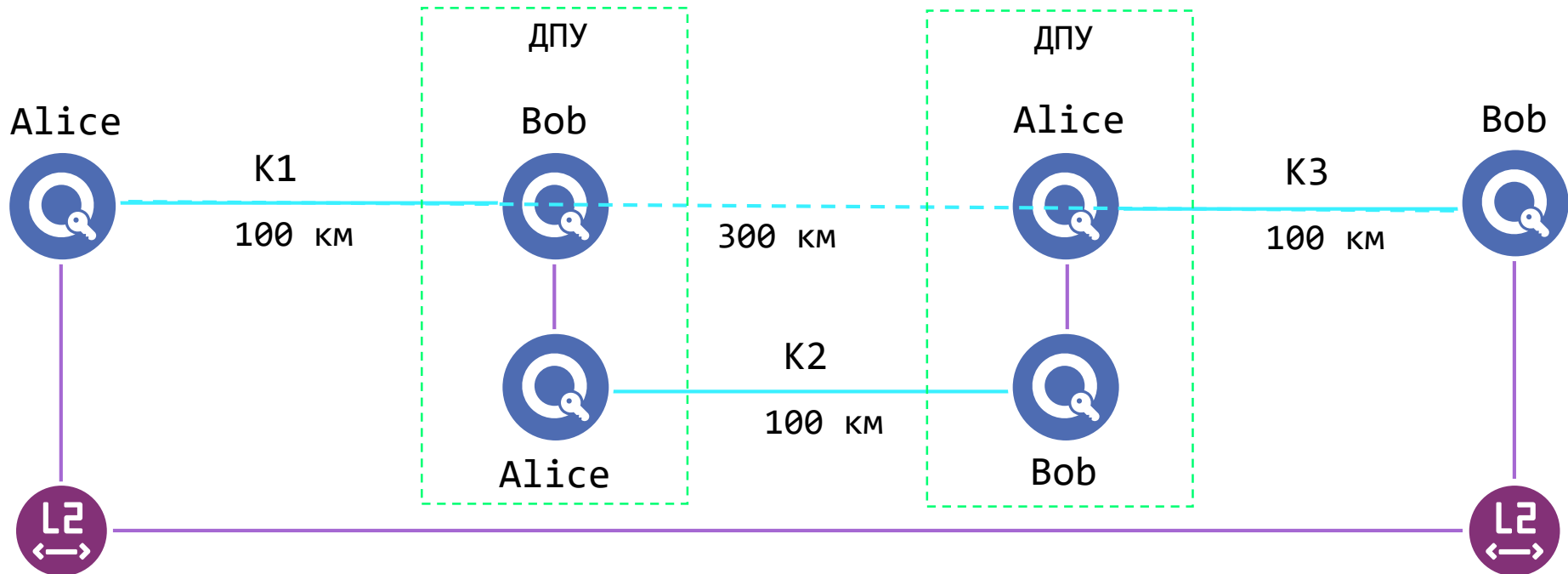


Проблема ограничения длины оптического канала

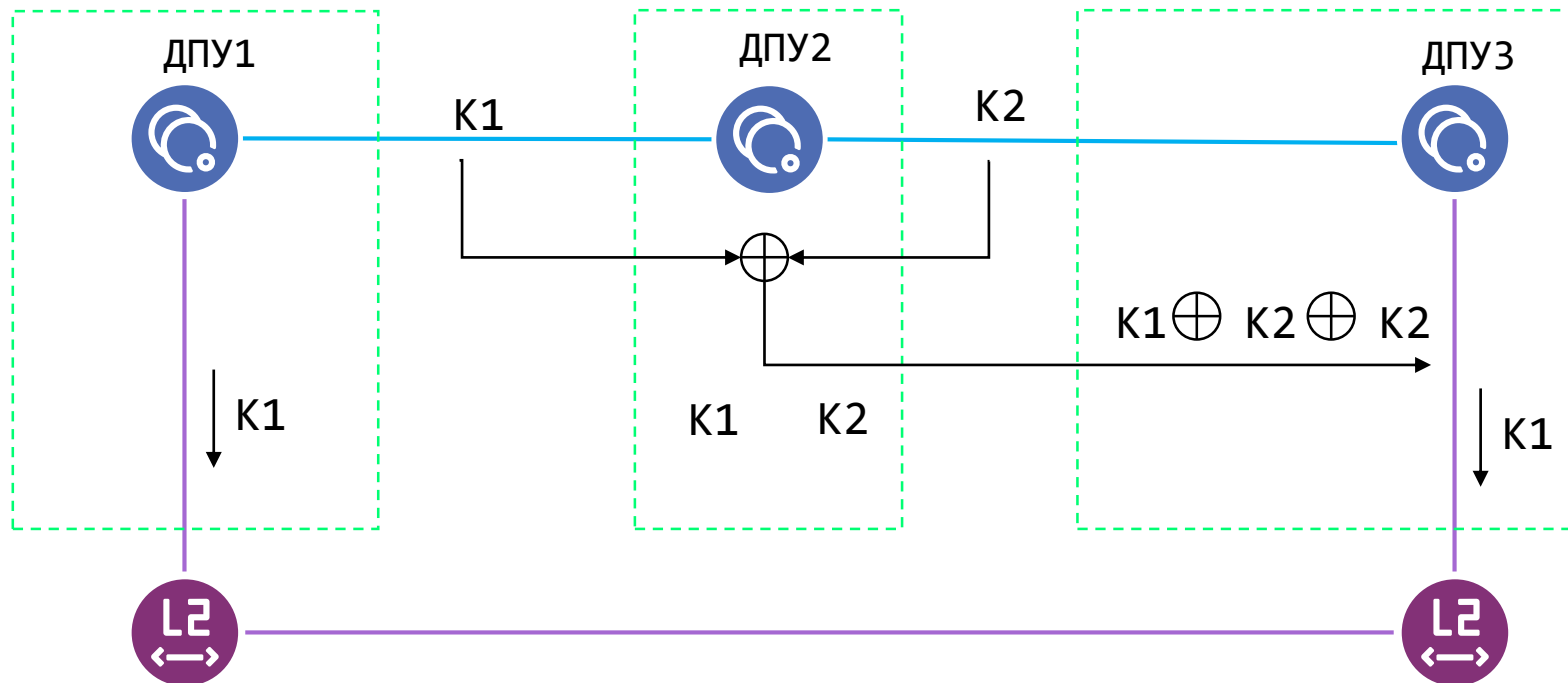


Решение проблемы – доверенный промежуточный узел

ДПУ – доверенный промежуточный узел



Простой пример выработки общего ключа





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

VIPNet QSS Switch



Оптический коммутатор

- 12 оптических портов FC\UPC
- Вносимое затухание – не более 1,9 дБ
- Габариты – 1U

VIPNet L2Q-10G

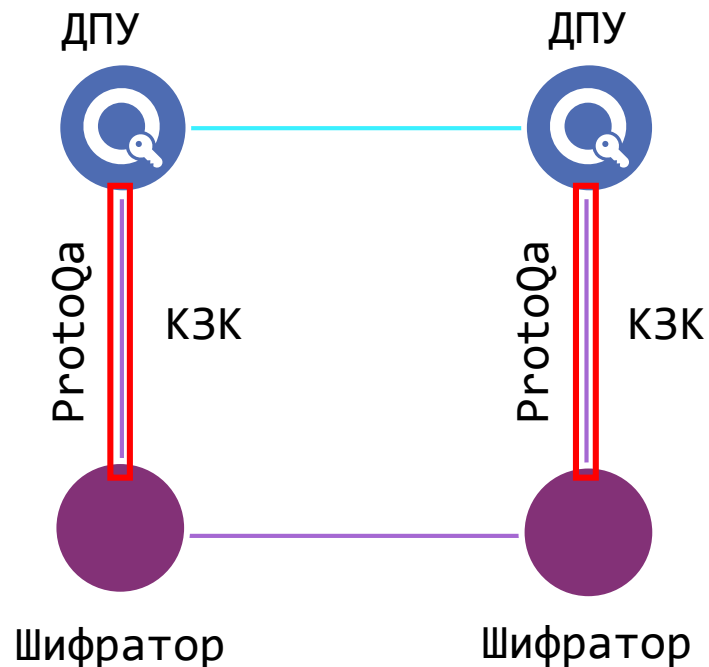


Шифратор канального уровня

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

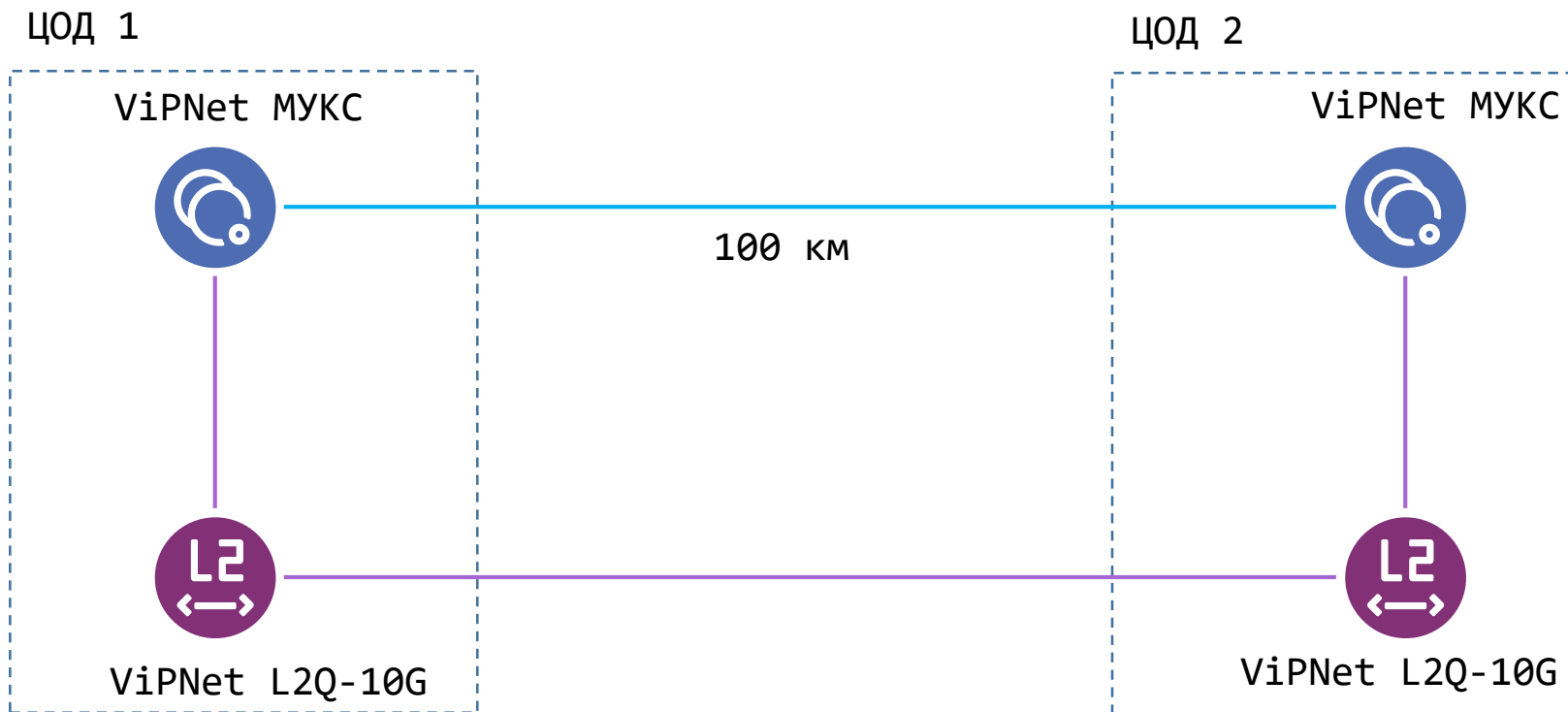
Потребитель ключей – любой шифратор с ProtoQa

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

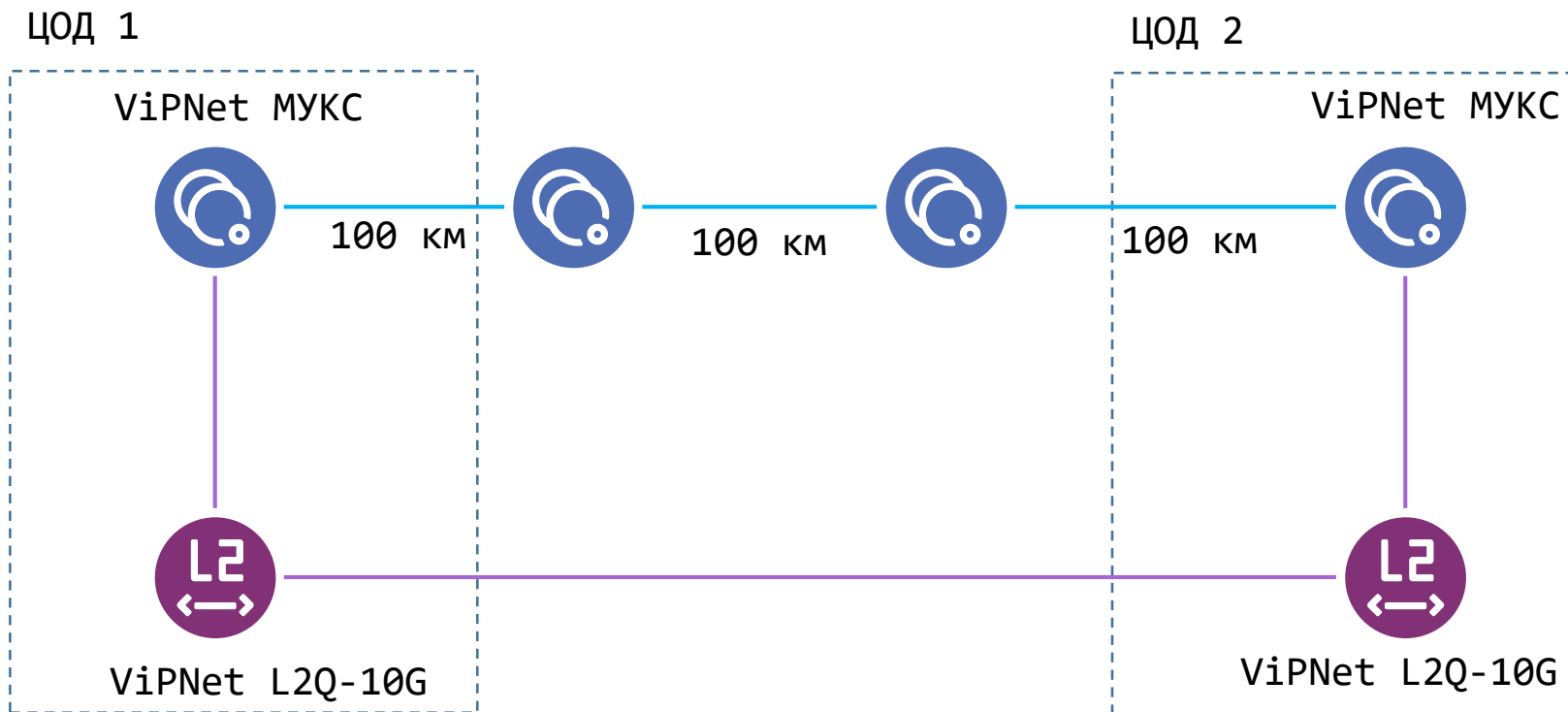


Возможные топологии квантовых сетей на базе ViPNet QTS

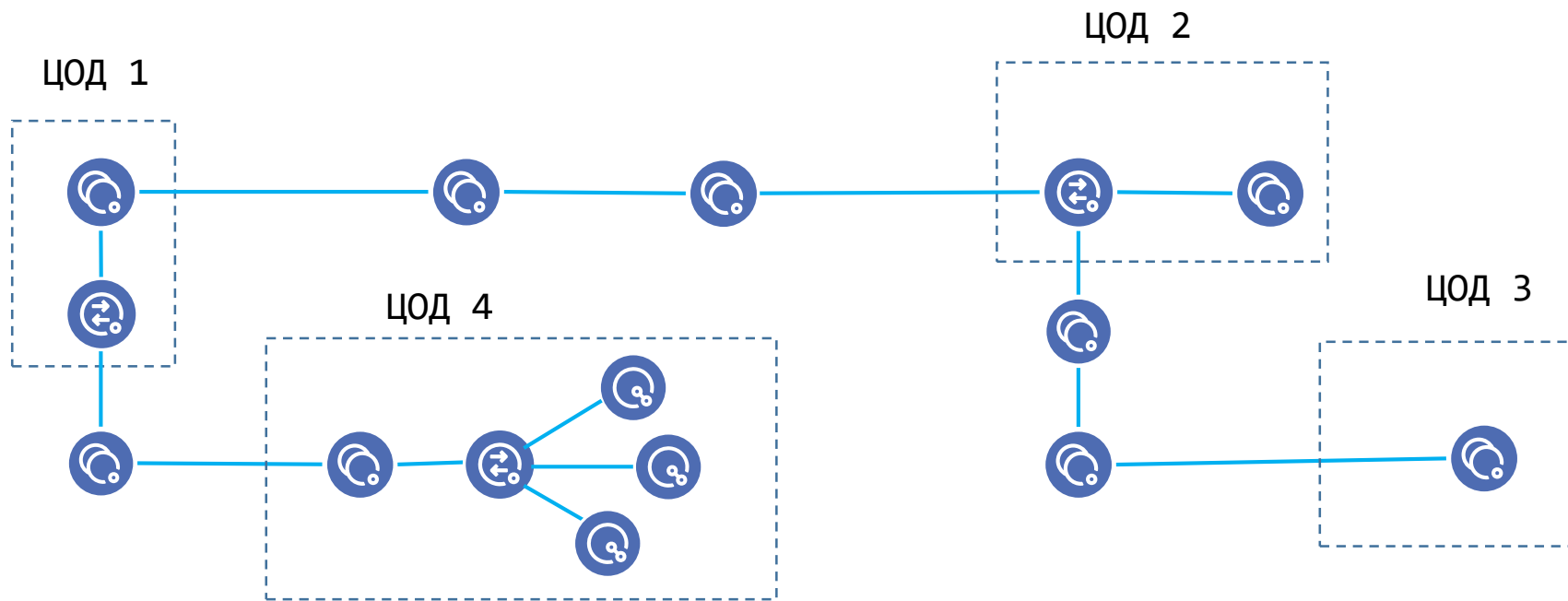
Точка-Точка



Магистраль



Магистраль с ответвлением



техно infotecs 2024 Фест

Иванов Олег

Менеджер продуктов
Oleg.Ivanov@infotecs.ru

Подписывайтесь на наши соцсети

