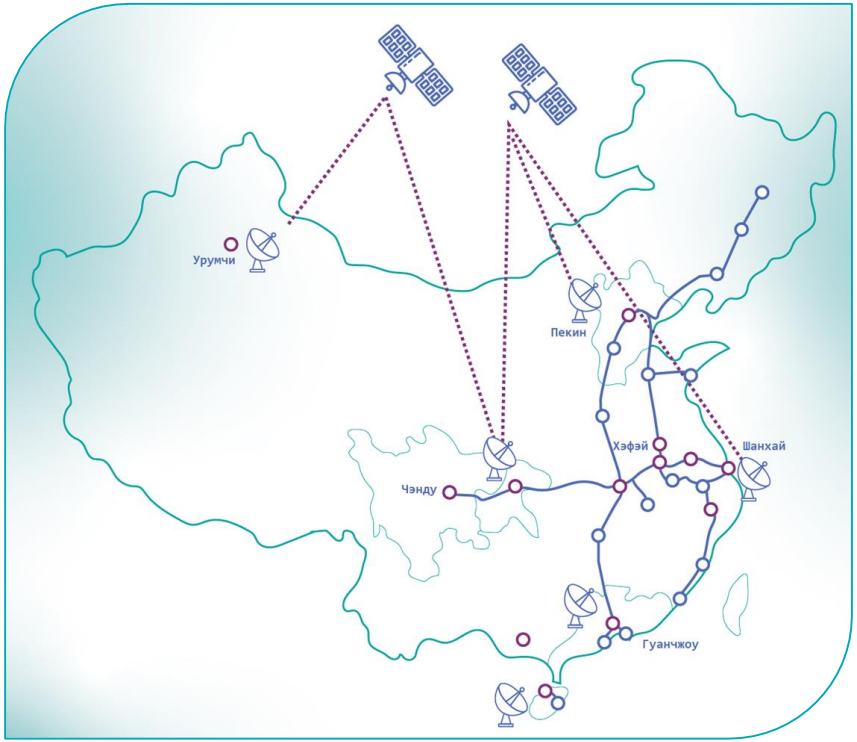
ViPNet QCS: от обучения до построения магистральных квантовых сетей

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)*

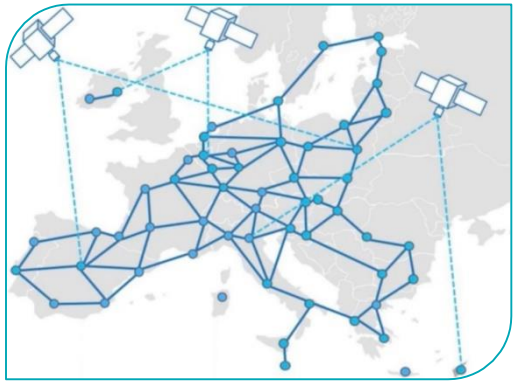
Сети КРК в Европе

Программа **Quantum Flagship**
с 2018 г.

Бюджет **€1000M**

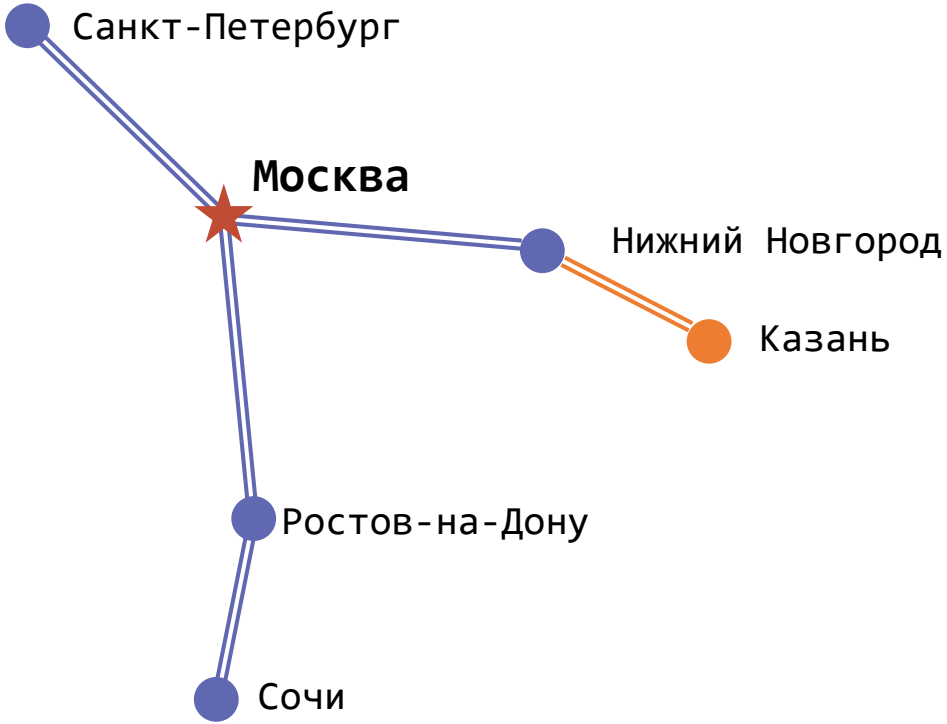
27 европейских стран

7 проектов по КРК



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

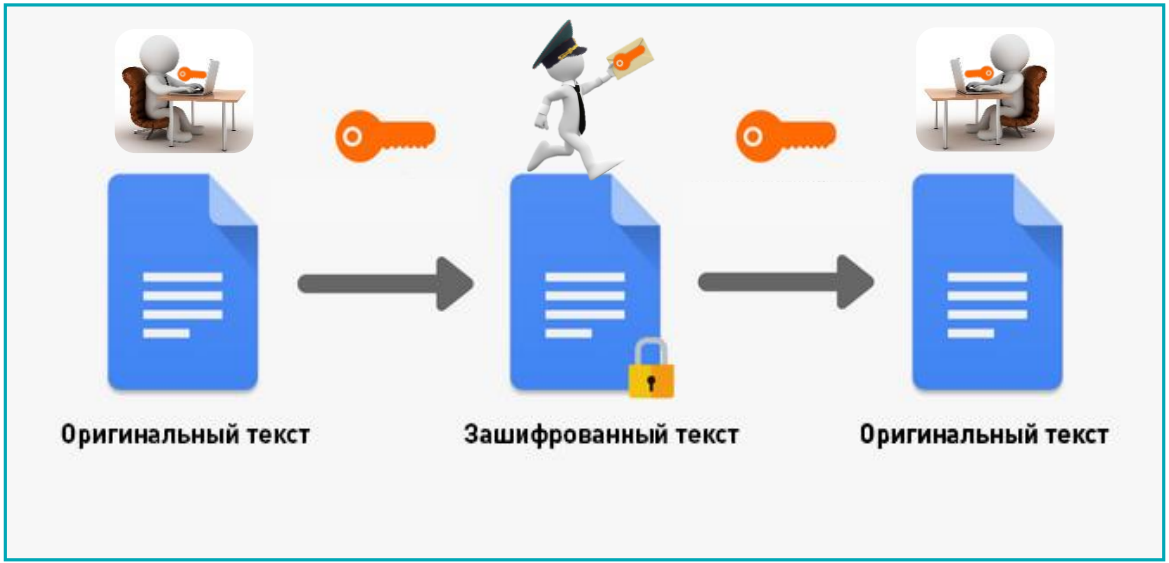
Сети КРК в России



Что такое квантовое распределение ключей

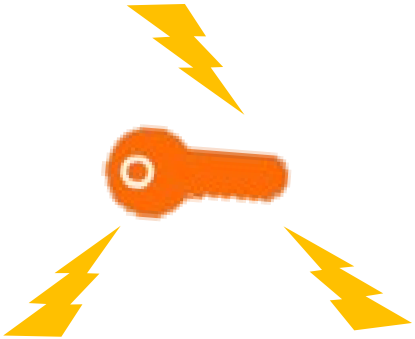
Для чего применяется криптография:

- 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).

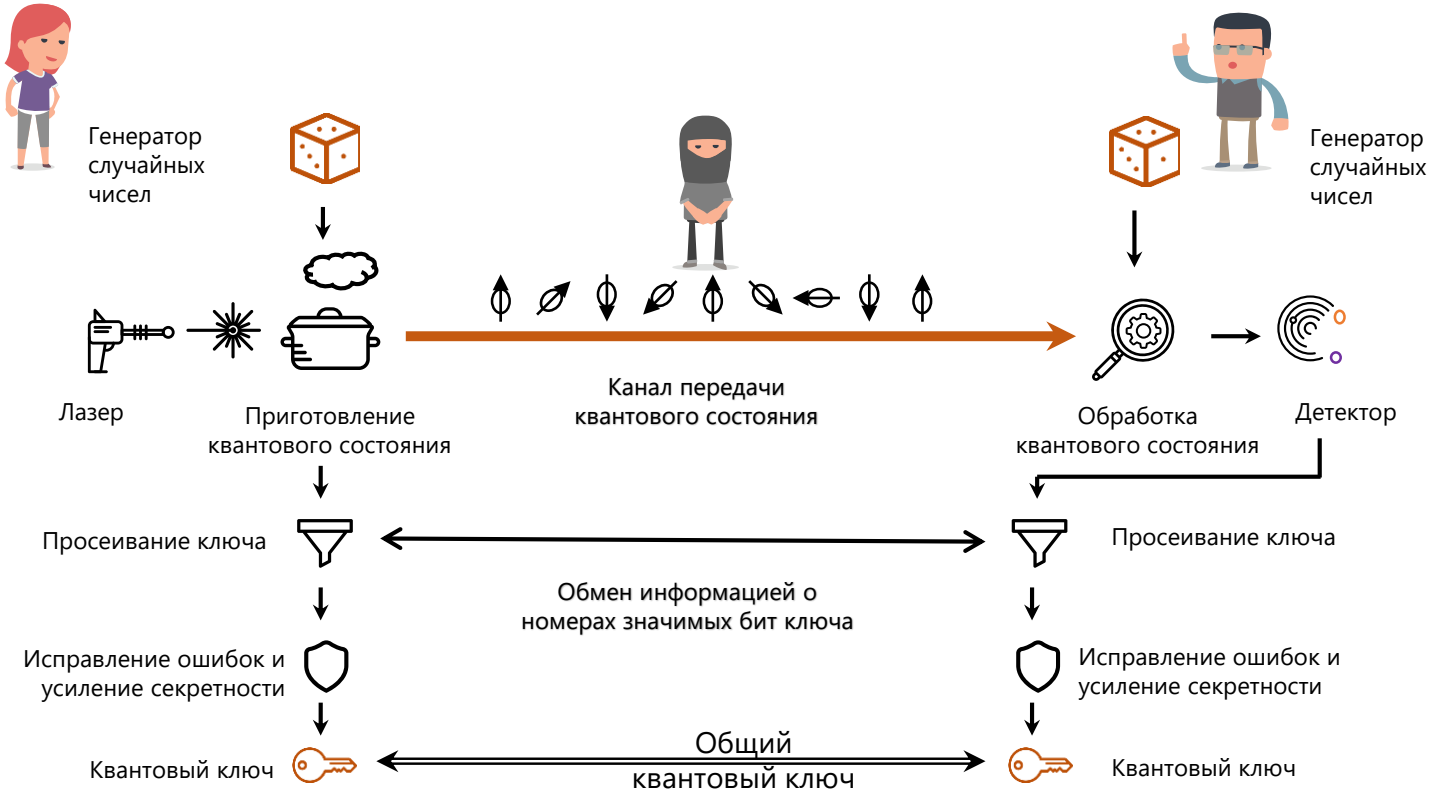
Принципы КРК

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

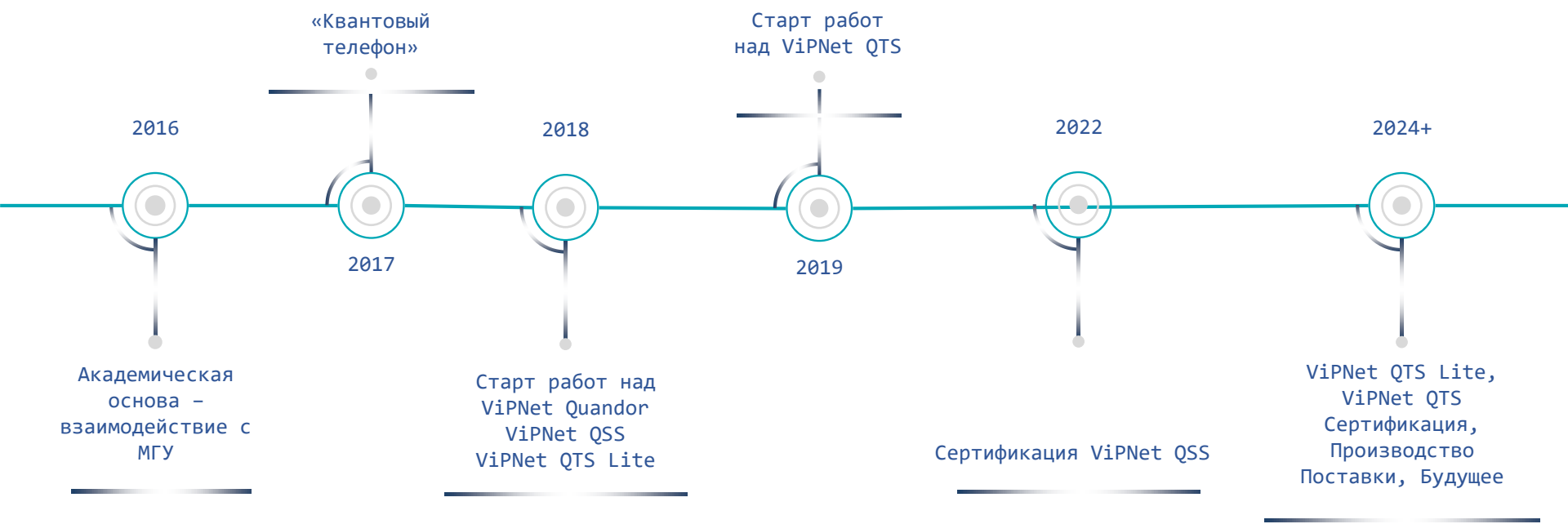
Кодирование через вектор поляризации магнитного поля

	0	1
Верт.-гор. базис		
Диагональный базис		

Используемые принципы



Ретроспектива событий

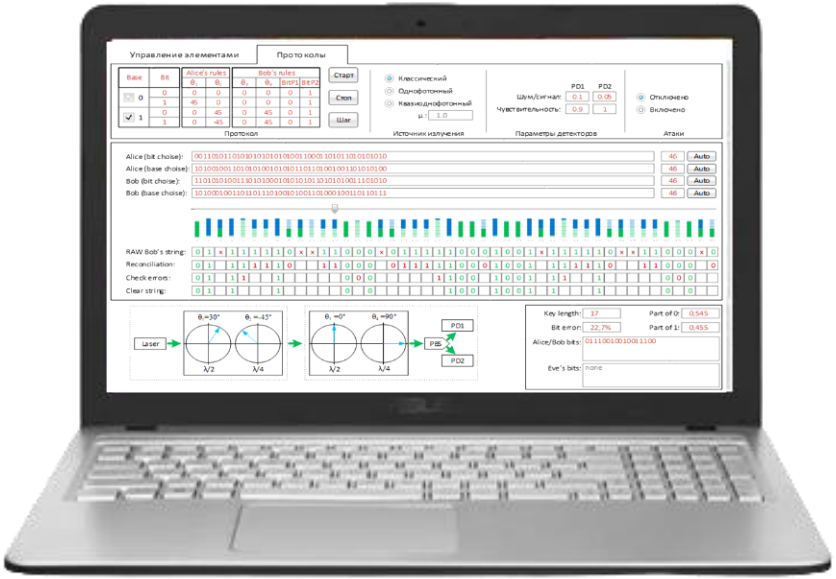


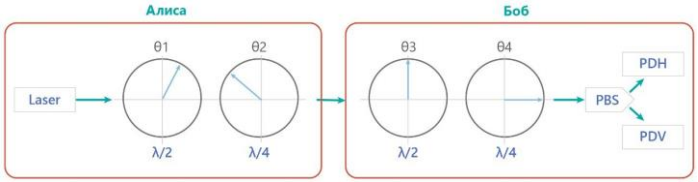
ViPNet Quantum Key Distribution Simulator

ViPNet QKDSim

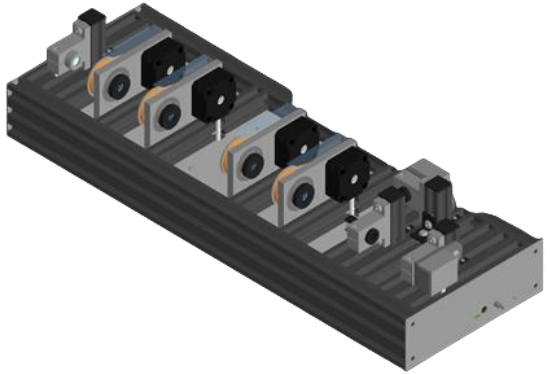
АО «ИнфоТеКС»

- Программное обеспечение
- Эмулятор аппаратной платформы

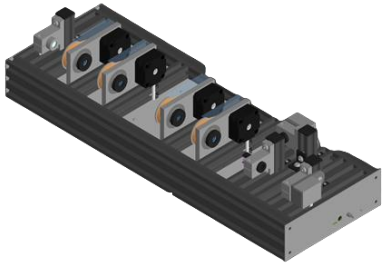


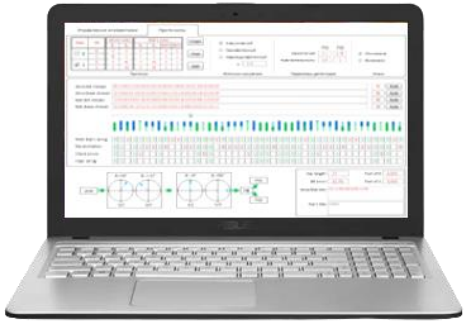


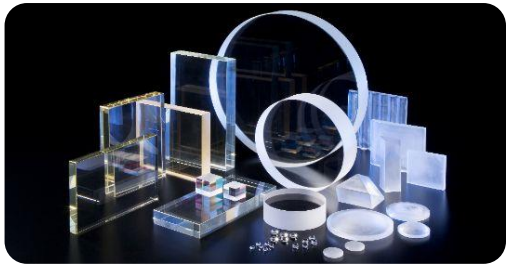
- Аппаратная платформа



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

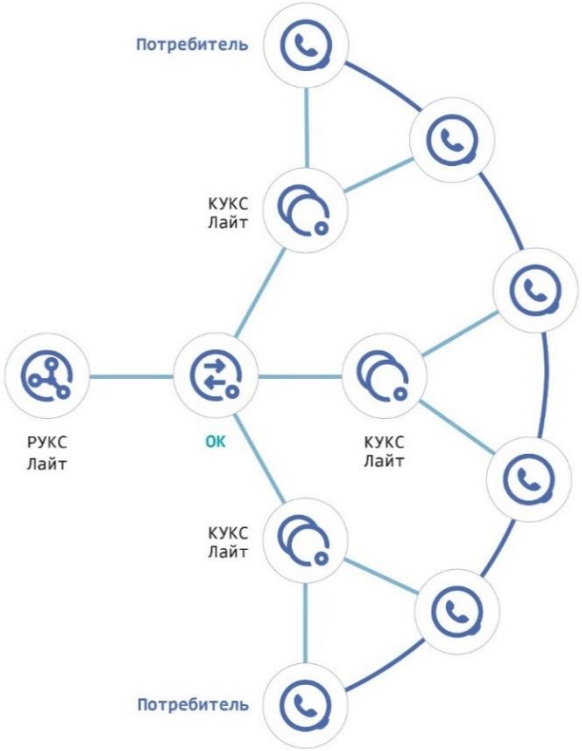
- Понятие о базисах кодирования
- Алгоритмы формирования и детектирования посылок
- Постобработка распределяемой последовательности

Безопасность передачи и распределения ключей

- Проведение атак на протоколы и системы КРК
- Связь ошибки распределения ключей с информацией, доступной нарушителю

ViPNet Quantum Trusted System

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

ТЕХНО infotecs 2024 ФЕСТ

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 РОСС 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 си

Настоящий сертификат удостоверяет, что программно-аппаратный «ViPNet Клиентский узел квантовой сети Лайт» из состава квантовой криптограф системы выработки и распределения ключей ViPNet Quantum Trusted Syst в комплектации согласно формуляру ФРКЕ.465636.005-01ФО

соответствует Требованиям к средствам криптографической защиты инф предназначенным для защиты информации, не содержащей сведений, состав государственную тайну, класса КС3, Временным требованиям к квантовым криптограф системам выработки и распределения ключей для средств криптографической информации, предназначенным для защиты информации, не содержащей с составляющих государственную тайну, класса КС и может использовать криптографической защиты (создание и управление ключевой информацией, в т квантовозащищённой, шифрование файлов и данных, содержащихся в областях опе памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в оперативной памяти) информации, не содержащей сведений, составляющих государ тайну.

Сертификат выдан на основании результатов проведенных Обществом с огра ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов продукции №№ 1075Б-000501, 1075Б-000

Безопасность информации обеспечивается при использовании комплекса, изготовл соответствии с техническими условиями ФРКЕ.465636.005-01ТУ, и выполнении тр эксплуатационной документации согласно формуляру ФРКЕ.465636.005-01ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России О.В.

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4509 от "05" мая 2023 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 Lite в комплектации согласно формуляру ФРКЕ.465636.004-01ФО

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 квантовозащищённой, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции 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 №№ 1075А-000501, 1075А-000502

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

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России О.В. Скрябин

- 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

Университетская Квантовая Сеть

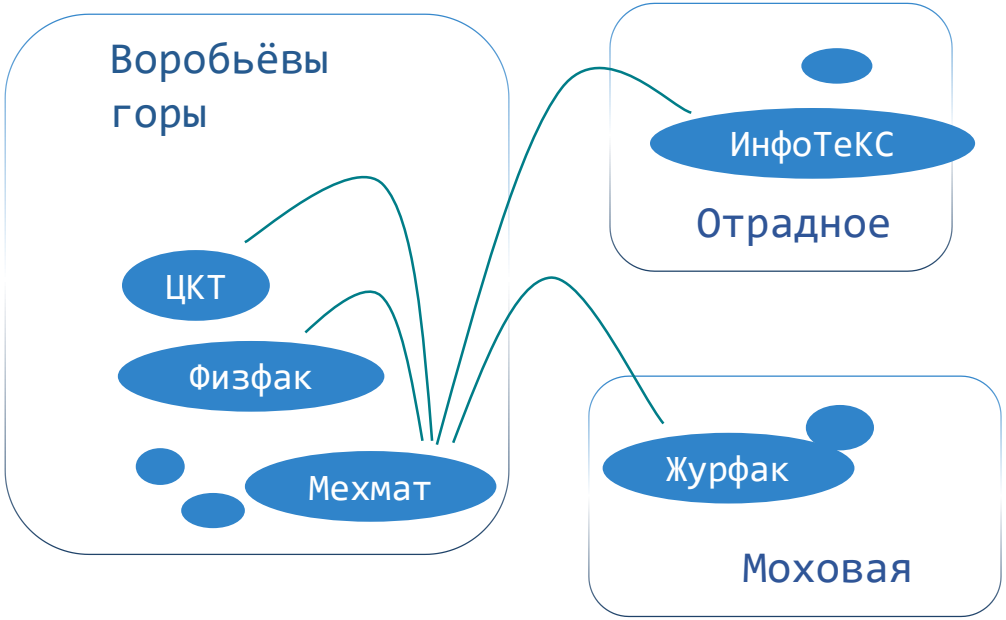
1 РУКС Лайт

5 КУКС Лайт

22 абонентских пунктов

40 км самый длинный луч

Подключены подразделения МГУ и головной офис ИнфоТеКС



Пилоты и проекты

ТУСУР
TUSUR UNIVERSITY

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

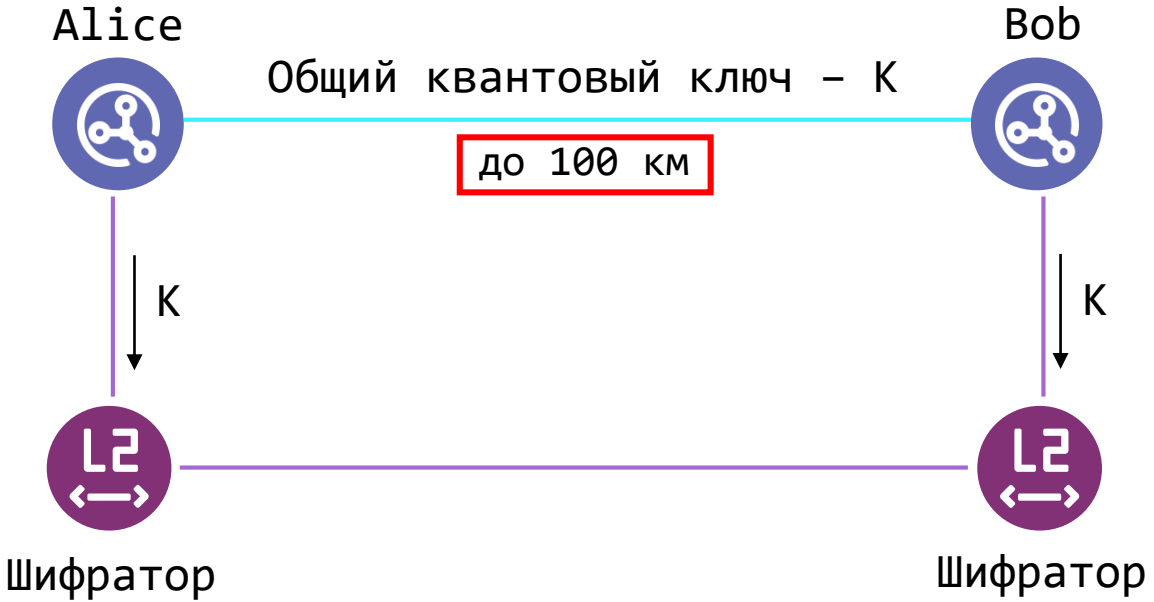
infotecs

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

ТЕХНО 2024 infotecs ФЕСТ

ViPNet Quantum Trusted

Простейшая квантовая сеть «точка-точка»

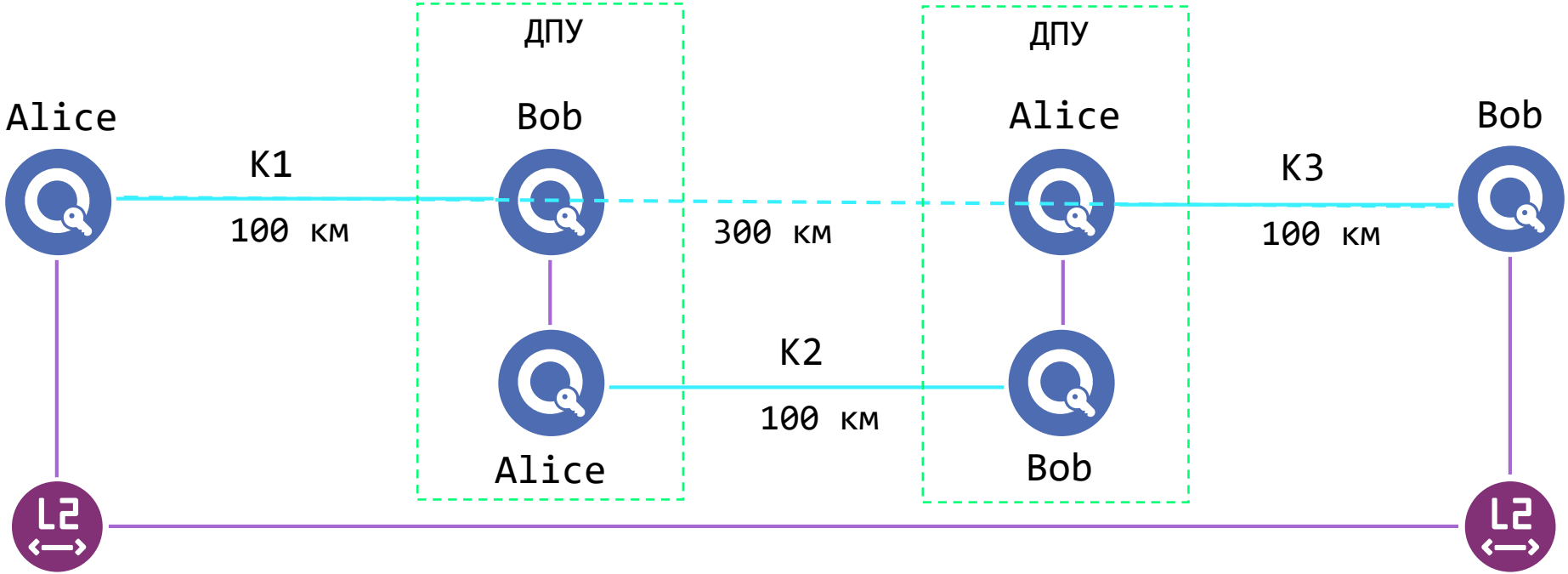


Проблема ограничения длины оптического канала

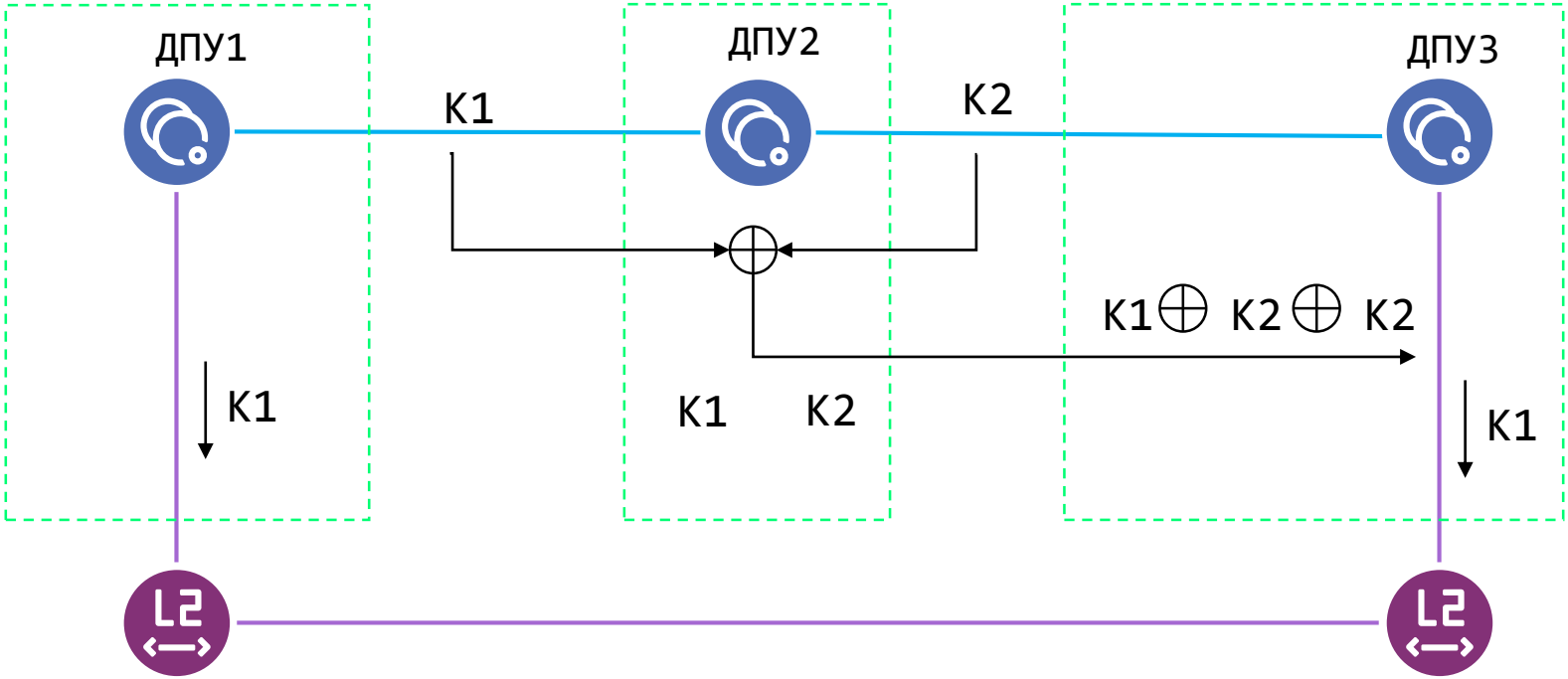
Затухание в волокне → Увеличение числа ошибок → Снижение скорости выработки ключа

Решение проблемы – доверенный промежуточный узел

ДПУ – доверенный промежуточный узел



Простой пример выработки общего ключа



ViPNet QTS

ViPNet МУКС/РУКС

- 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

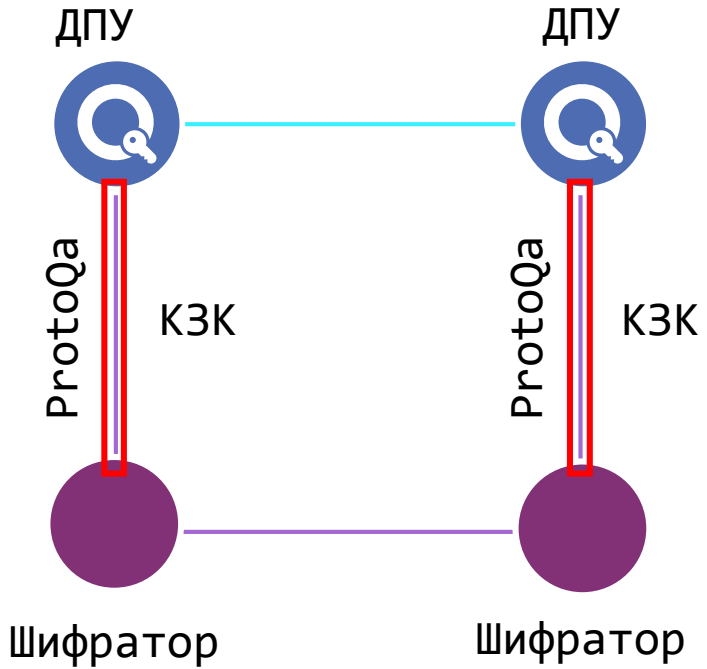
ViPNet L2Q-10G

Шифратор канального уровня

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

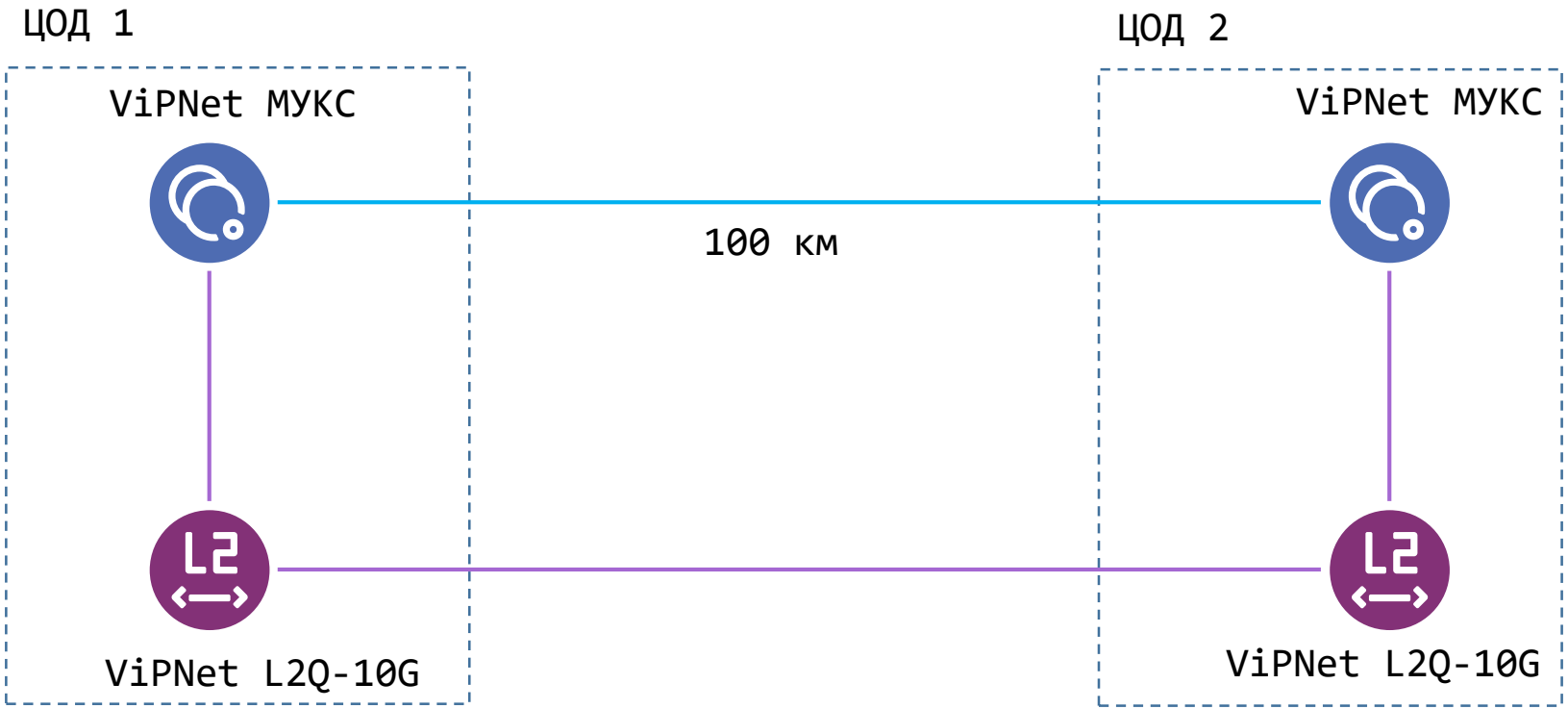
Потребитель ключей – любой шифратор с ProtoQa

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

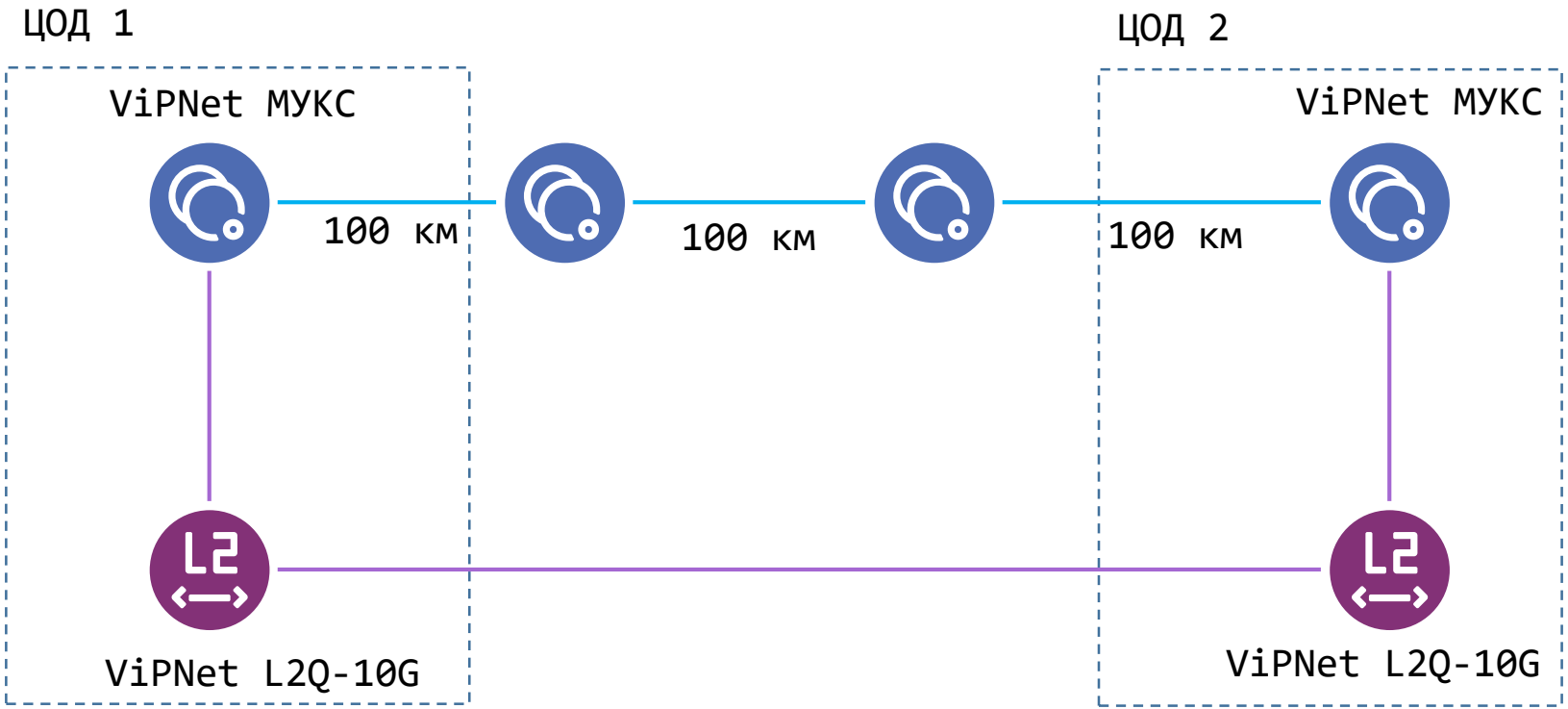


Возможные топологии квантовых сетей на базе ViPNet QTS

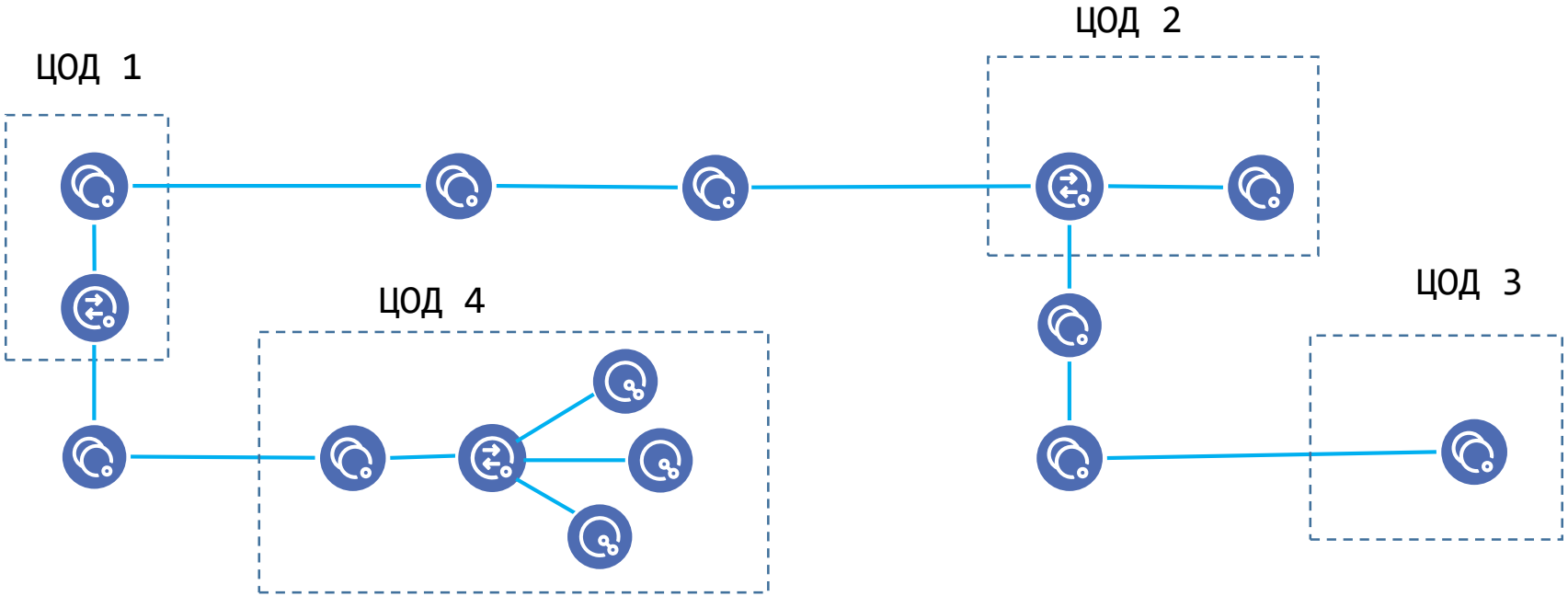
Точка-Точка


ЦОД 1
ЦОД 2
ViPNet МУКС
ViPNet МУКС
100 км
L2
L2
ViPNet L2Q-10G
ViPNet L2Q-10G

Магистраль


ЦОД 1
ЦОД 2
ViPNet МУКС
ViPNet МУКС
100 км
100 км
100 км
L2
L2
ViPNet L2Q-10G
ViPNet L2Q-10G

Магистраль с ответвлением

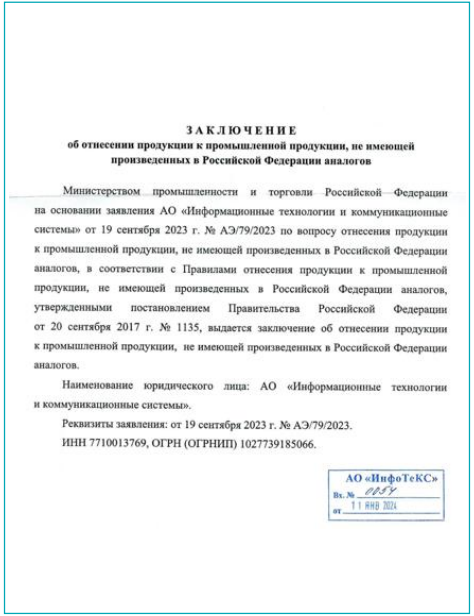


Отечественные реестры

Присутствие в реестрах

	Наименование	Тип	Реестровая запись
QTS Lite	ViPNet ПО МОС	Реестр ПО	№16924 от 21.03.2023
	ViPNet ПО МОК	Реестр ПО	№16921 от 21.03.2023
	ViPNet ПО РУКС Лайт	Реестр ПО	№16922 от 21.03.2023
	ViPNet ПО КУКС Лайт	Реестр ПО	№16923 от 21.03.2023
	ViPNet РУКС Лайт	Реестр ПАК	№18973 от 05.09.2023
	ViPNet КУКС Лайт	Реестр ПАК	№21053 от 29.12.2023
	ViPNet РУКС Лайт	РРЭП	№10535638 от 14.05.2024
	ViPNet КУКС Лайт	РРЭП	№10535637 от 14.05.2024
QTS	ViPNet МОС ДПУ	Реестр ПО	№20456 от 14.12.2023
	ViPNet УК ДПУ	Реестр ПО	№20455 от 14.12.2023
	ViPNet МОК ДПУ	Реестр ПО	№20454 от 14.12.2023
	ViPNet УК КУКС	Реестр ПО	№20453 от 14.12.2023

Российская продукция, не имеющая аналогов (Минпромторг России)



ЗАКЛЮЧЕНИЕ
об отнесении продукции к промышленной продукции, не имеющей произведенных в Российской Федерации аналогов

Министерством промышленности и торговли Российской Федерации на основании заявления АО «Информационные технологии и коммуникационные системы» от 19 сентября 2023 г. № АЭ/79/2023 по вопросу отнесения продукции к промышленной продукции, не имеющей произведенных в Российской Федерации аналогов, в соответствии с Правилами отнесения продукции к промышленной продукции, не имеющей произведенных в Российской Федерации аналогов, утвержденными постановлением Правительства Российской Федерации от 20 сентября 2017 г. № 1135, выдается заключение об отнесении продукции к промышленной продукции, не имеющей произведенных в Российской Федерации аналогов.

Наименование юридического лица: АО «Информационные технологии и коммуникационные системы».

Реквизиты заявления: от 19 сентября 2023 г. № АЭ/79/2023.

ИНН 7710013769, ОГРН (ОГРНИП) 1027739185066.

АО «ИнфоТеКС»
Вх. № 4869
от 11 ИЮЛ 2024

ТЕХНО 2024 infotecs ФЕСТ

Спасибо за внимание

Подписывайтесь на наши соцсети