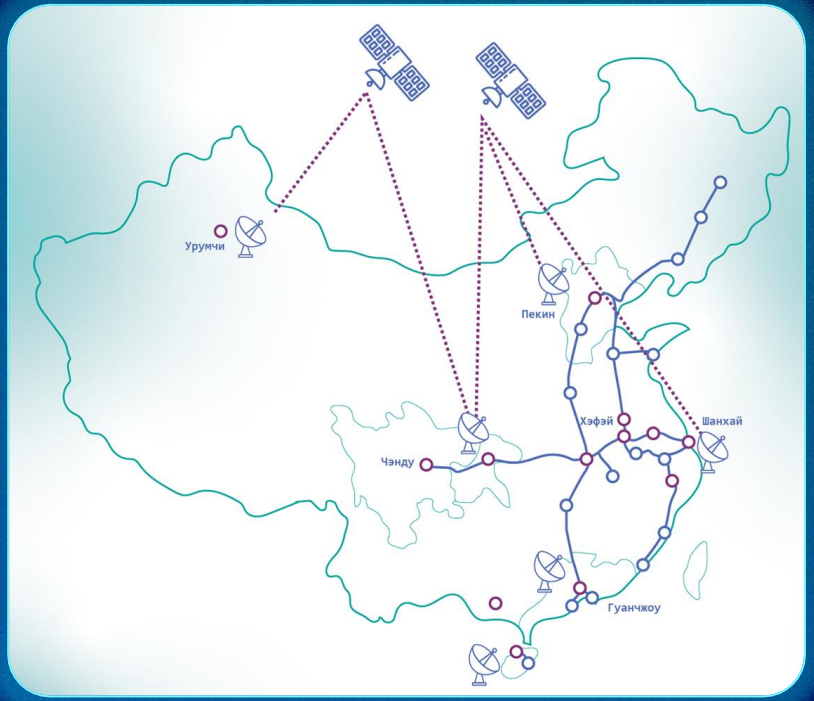
ViPNet QCS: от обучения до построения магистральных квантовых сетей

Олег Иванов
Менеджер продукта

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

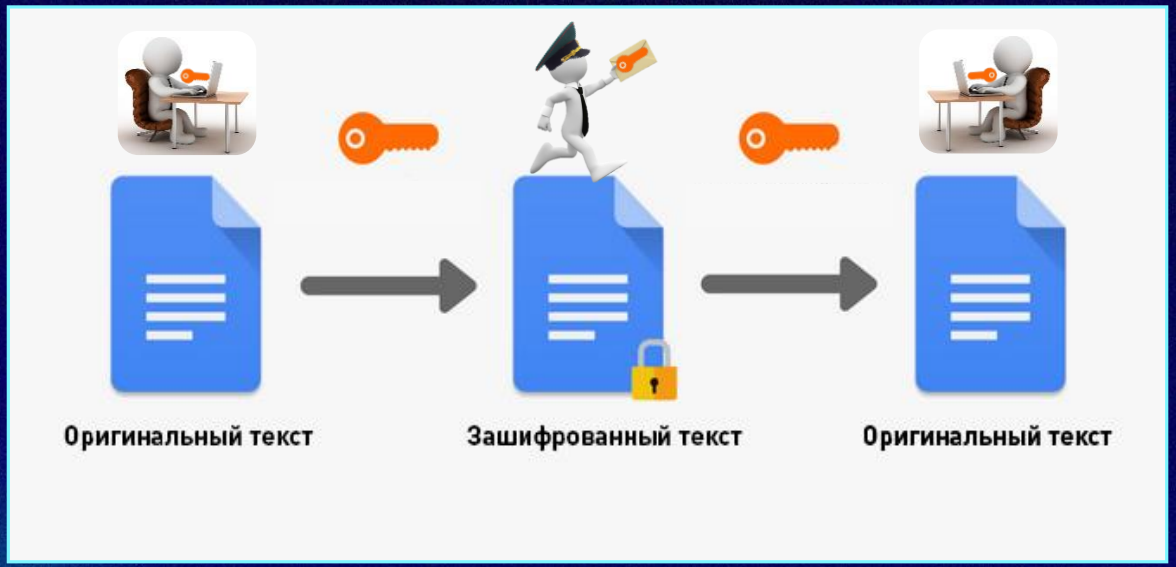
7 проектов по КРК

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

Сети КРК в России

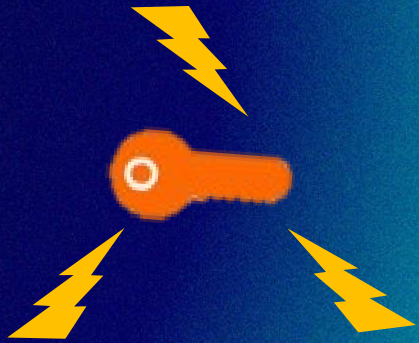
Для чего применяется криптография:

- 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)

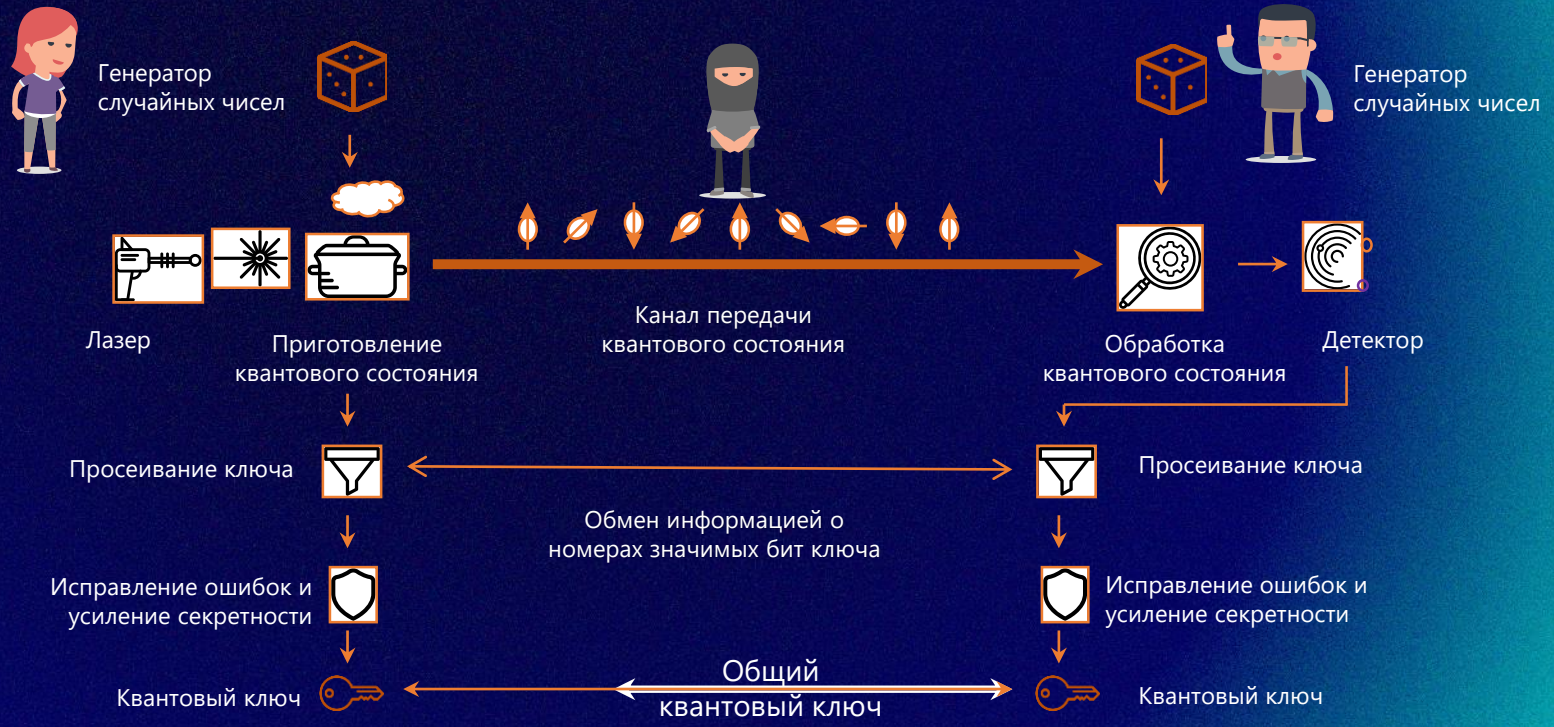
Принципы КРК

- 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

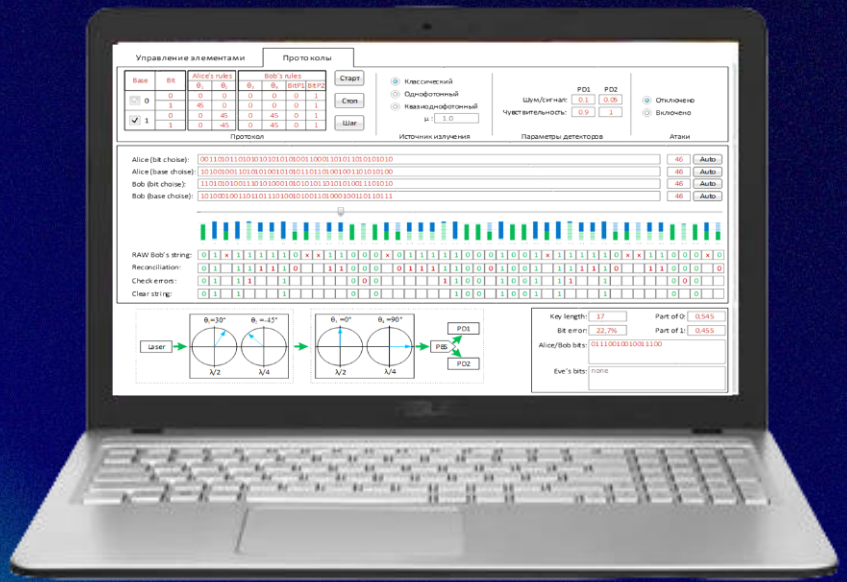


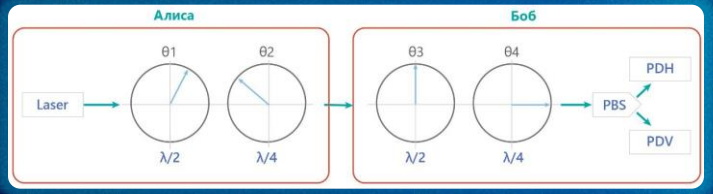
ViPNet Quantum Key Distribution Simulator

ViPNet QKDSim

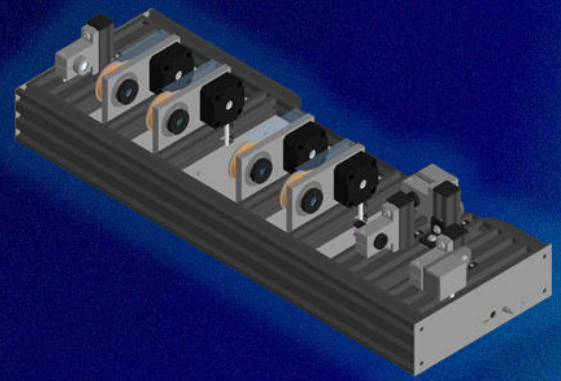
Компания «ИнфоТеКС»

- Программное обеспечение
- Эмулятор аппаратной платформы

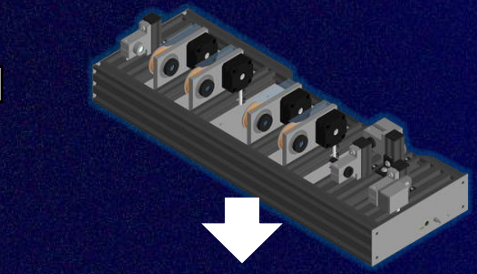


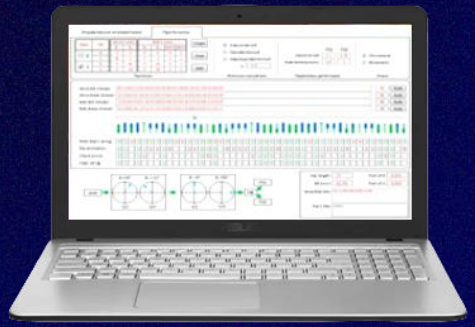


- Аппаратная платформа



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

Первое поколение

ViPNet Quandor

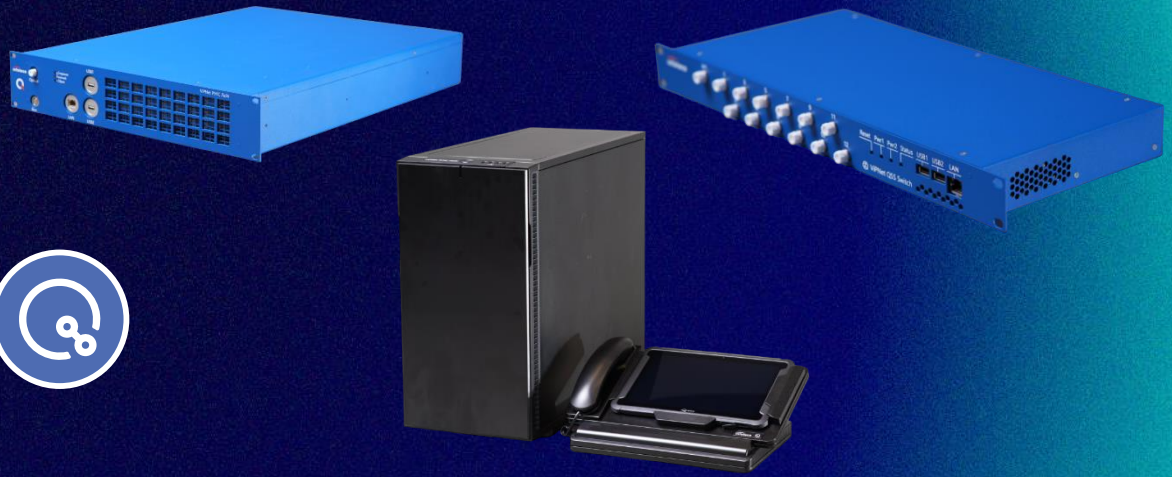
Точка - Точка

до 100 км

- Комплекс системы КРК и шифраторов уровня L2
- Автоматическая смена ключей не реже чем 1 раз в минуту
- Размер 2U и 1U
- Задержка не более 15 мкс

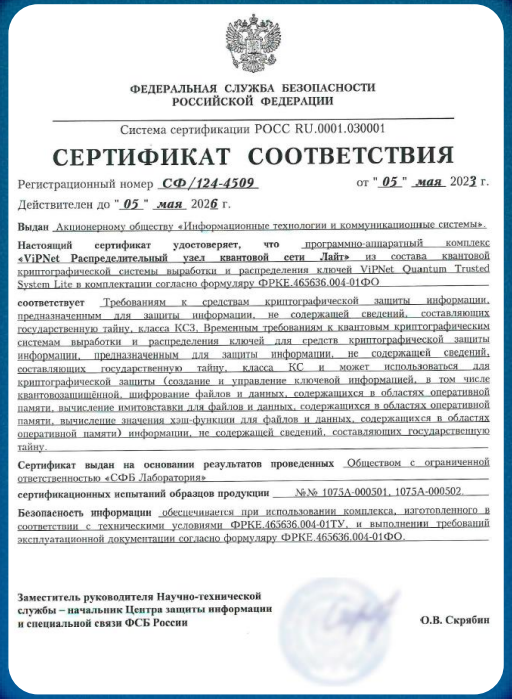
Комплекс обеспечивает скорость шифрования по алгоритму ГОСТ 34.12-2015 «Кузнечик» со скоростью до 20 Гбит/с в дуплексном режиме

ViPNet QTS Lite (ViPNet QSS)



- Распределение ключей по топологии «Звезда»
- Шифрование трафика на ключах, не известных администратору сети
- Возможность выработки на одном клиенте квантовозащищенных ключей для нескольких абонентов

Сертифицированное решение



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

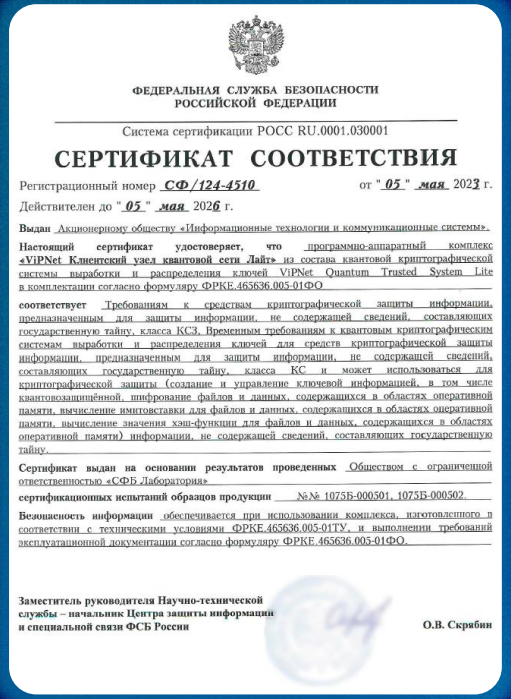
соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3. Временным требованиям к квантовым криптографическим системам выработки и распределения ключей для средств криптографической 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 №№ 1073А-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



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4510 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 Клиентский узел квантовой сети Лайт»** из состава квантовой криптографической системы выработки и распределения ключей ViPNet Quantum Trusted System Lite в комплектации согласно формуляру ФРКЕ.465636.005-01ФО

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 №№ 1075Б-000501, 1075Б-000502.

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

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

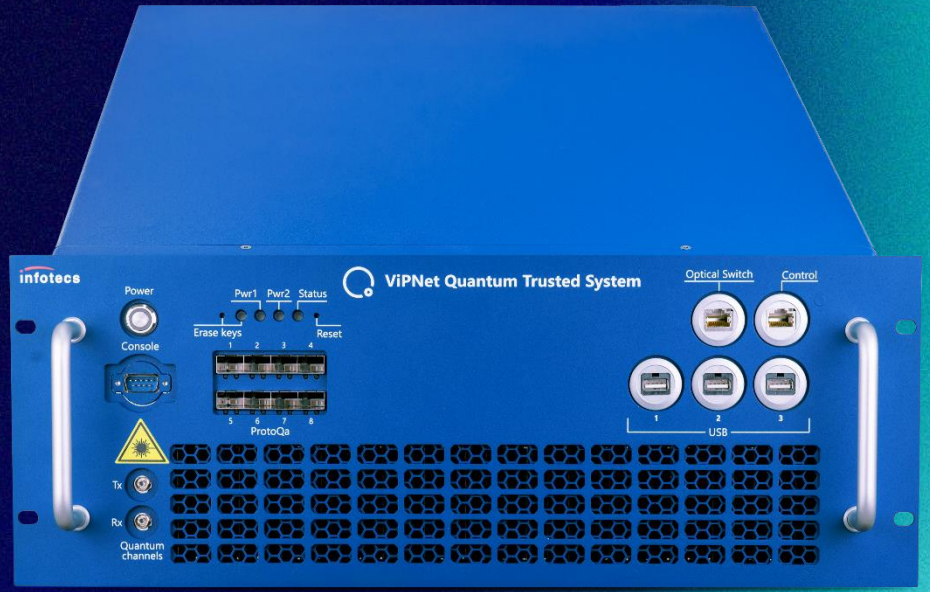
ViPNet Quantum Trusted System

ViPNet РУКС

Распределительный узел квантовой сети

Предназначен для объединения различных сегментов квантовой сети

- Квантовый канал до 100 км
- Доверенный промежуточный узел - приемник и передатчик квантовых импульсов в одном корпусе
- До 8 потребителей (шифраторов)



Сертификация

ViPNet Распределительный узел квантовой сети (ViPNet РУКС) соответствует требованиям к СКЗИ и временным требованиям к квантовым криптографическим системам выработки и распределения ключей для СКЗИ

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер ***СФ/124-5088*** от "***27***" ***декабря*** 2024 г.

Действителен до "***27***" ***декабря*** 2027 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программно-аппаратный комплекс «ViPNet Распределительный узел квантовой сети» (специальное программное обеспечение версии 1.0.1) из состава квантовой криптографической системы выработки и распределения ключей ViPNet Quantum Trusted System в комплектации согласно формуляру ФРКЕ.465636.004ФО

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 №№ 1108А-000501, 1108А-000502, 1108А-000503.

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

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

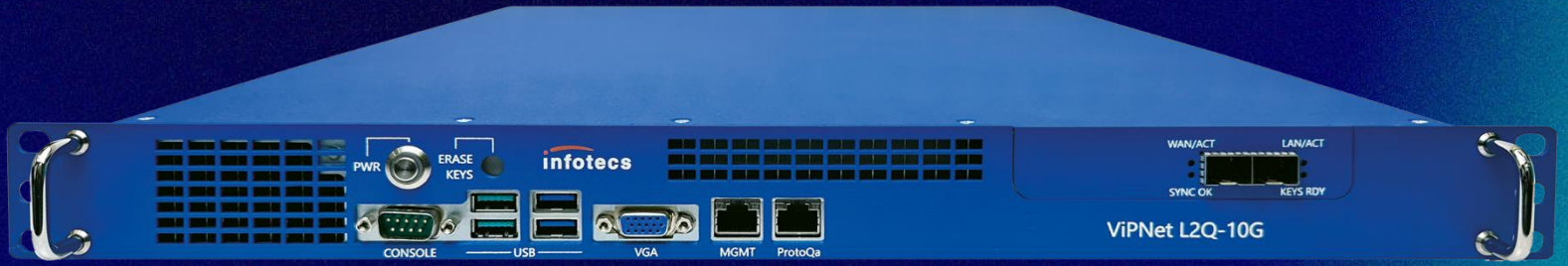
ViPNet КУКС

Клиентский узел квантовой сети

- Квантовый канал до 100 км
- 2U защищенный корпус
- Масса ~ 20 кг
- До 8 потребителей

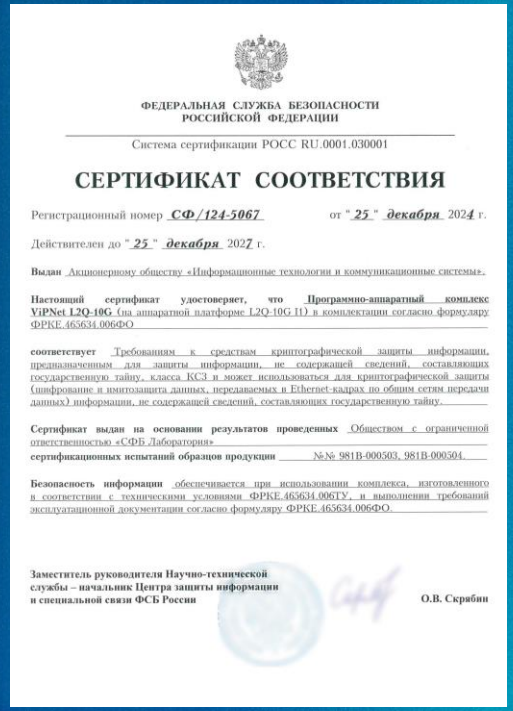
ViPNet L2Q-10G

- Шифратор канального уровня
- Производительность шифрования до 10 Гбит/с
- Металлический корпус с датчиком несанкционированного доступа (ДНСД)
- Размер 1U



Сертификация

ViPNet L2Q-10G (на аппаратной платформе L2Q-10G I1) соответствует требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-5067* от "*25*" *декабря* 2024 г.

Действителен до "*25*" *декабря* 2027 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программно-аппаратный комплекс ViPNet L2Q-10G (на аппаратной платформе L2Q-10G I1) в комплектации согласно формуляру ФРКЕ.465634.006ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3 и может использоваться для криптографической защиты (шифрование и имитозащита данных, передаваемых в Ethernet-кадрах по общим сетям передачи данных) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»
сертификационных испытаний образцов продукции №№ 981В-000503, 981В-000504.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.465634.006ТУ, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.465634.006ФО.

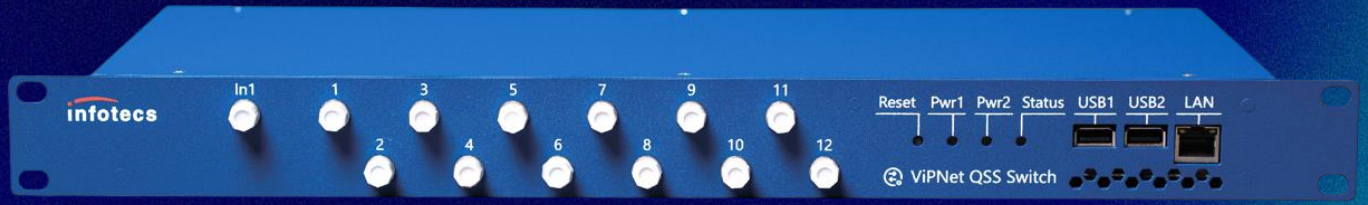
Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

ViPNet QSS Switch

Оптический коммутатор квантовых сетей

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

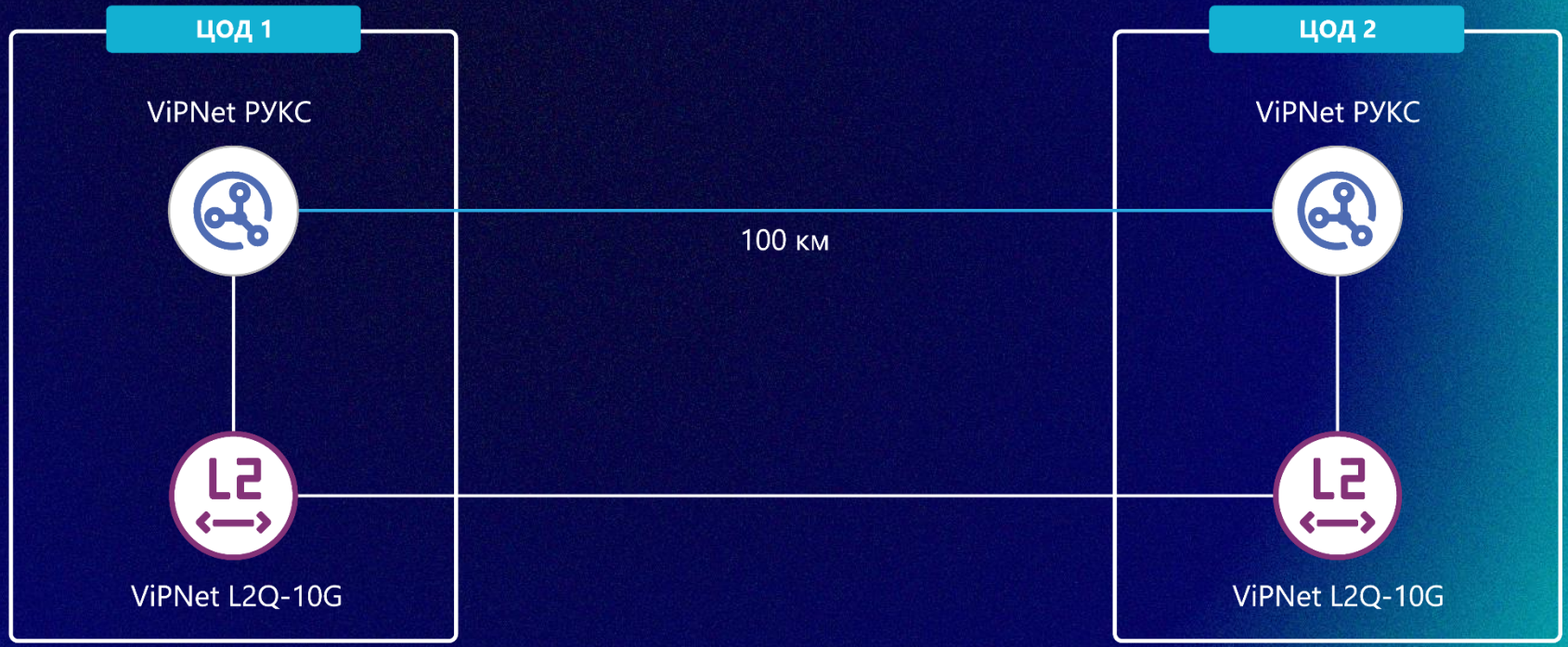
- Габариты – 1U
- Масса – 4,6 кг
- Потребляемая мощность – до 15 Вт
- 12 оптических портов FC\UPC
- Вносимое затухание – не более 1,9 дБ



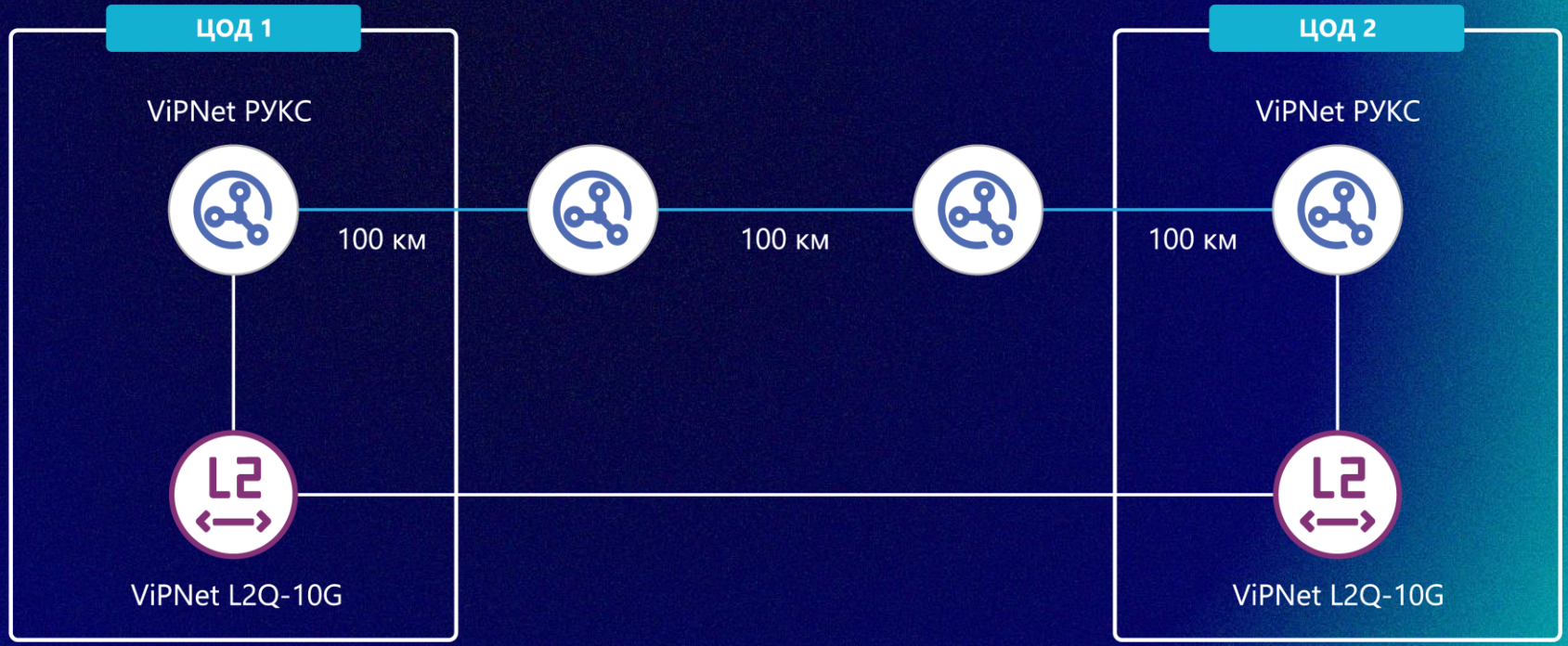
Возможные топологии квантовых сетей на базе ViPNet QTS

ТЕХНО infotecs Фест

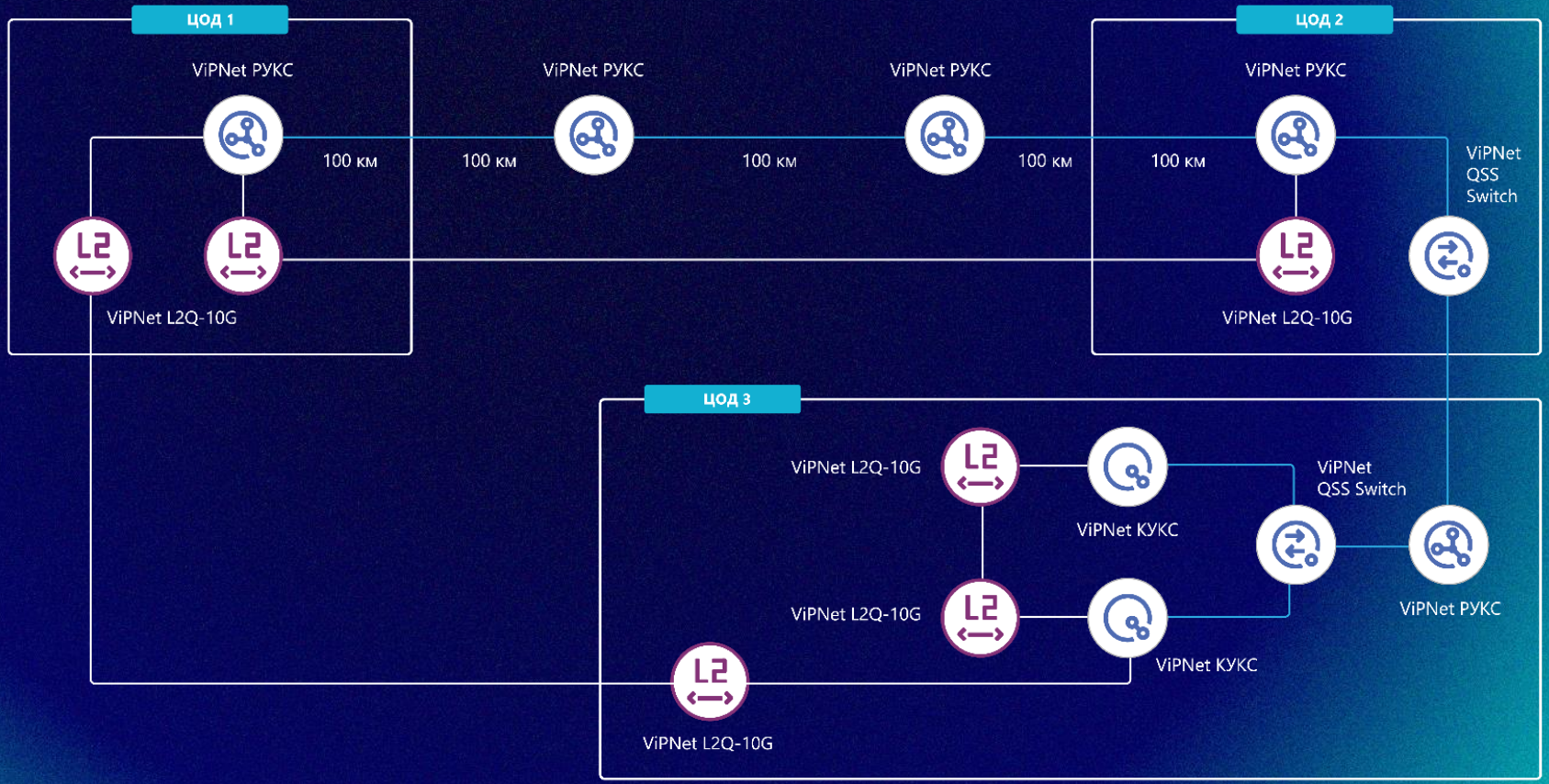
Точка-Точка


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

Магистраль


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

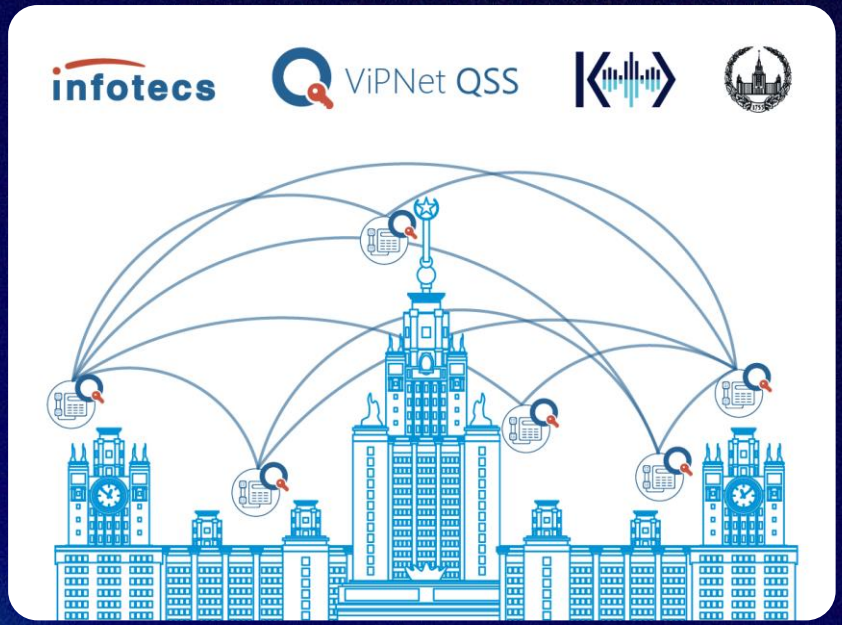
Магистраль с ответвлением



Реализованные проекты

Университетская квантовая сеть

UQN
Университетская
Квантовая Сеть



Университетская квантовая сеть (УКС МГУ) – совместная разработка ИнфоТеКС и Центра квантовых технологий Физического факультета МГУ имени М.В. Ломоносова

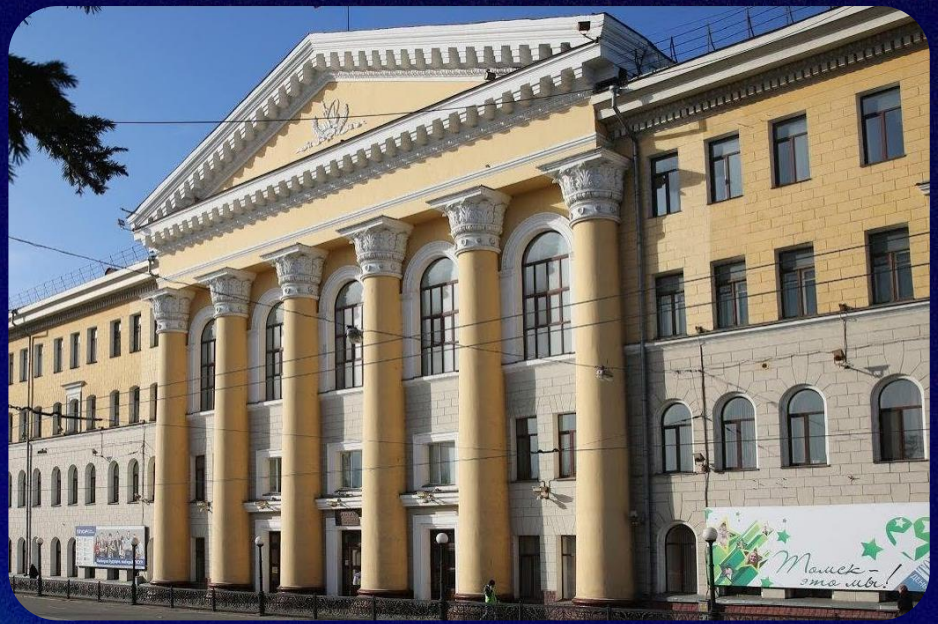
Эксплуатируется с 2021 года

6 квантовых устройств

20 абонентских терминалов

40 км длина канала квантово-защищенной связи

Квантовая сеть ТУСУР



Состав сети: ТУСУР

- ViPNet РУКС Лайт – **1 шт.**
- ViPNet КУКС Лайт – **3 шт.**
- ViPNet QSS Switch – **1 шт.**
- Абонентские устройства ViPNet CSS Connect HW – **3 шт.**

Магистральная квантовая сеть РЖД на участке Москва-Сочи

Состав сети:

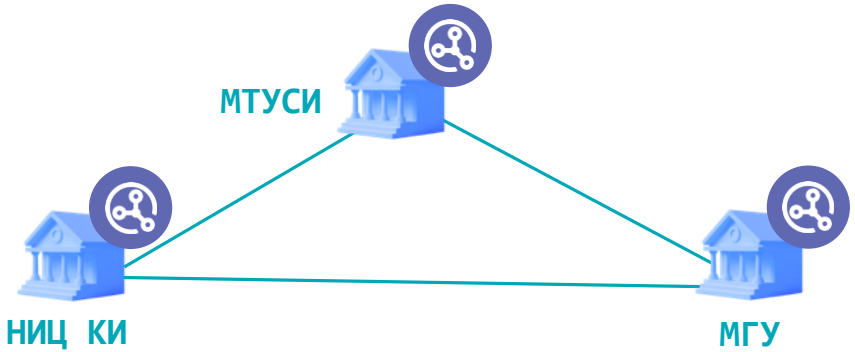
- Длина – более **1000** км
- Более **50** квантовых ПАК ViPNet РУКС
- Шифраторы L2Q-10G
- Сроки построения магистрали 2022-2023 гг.
- Проводятся ПНР

Конвергентная сеть

Состав сети:

- ViPNet РУКС Лайт – **1 шт.**
- ViPNet КУКС Лайт – **3 шт.**
- ViPNet QSS Switch – **1 шт.**
- Абонентские устройства ViPNet CSS Connect HW Special – **25 шт.**

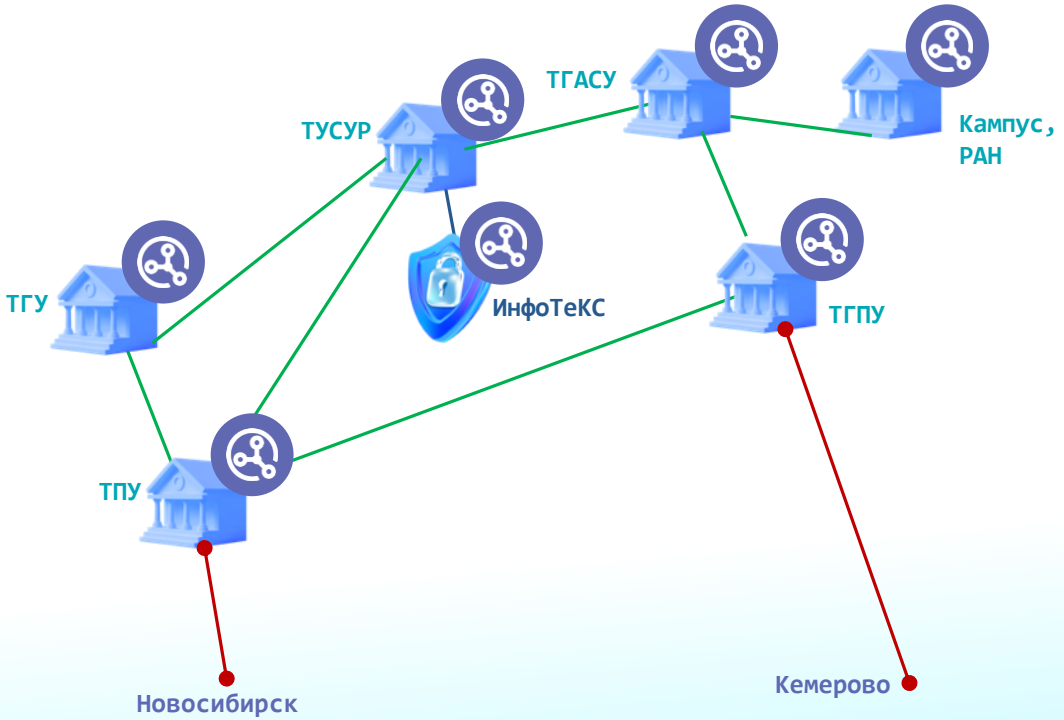
Межуниверситетская квантовая сеть



Этап 1:
Отказоустойчивое полносвязное ядро сети

Эксплуатируется с 2024 года

Межуниверситетская квантовая сеть Томска

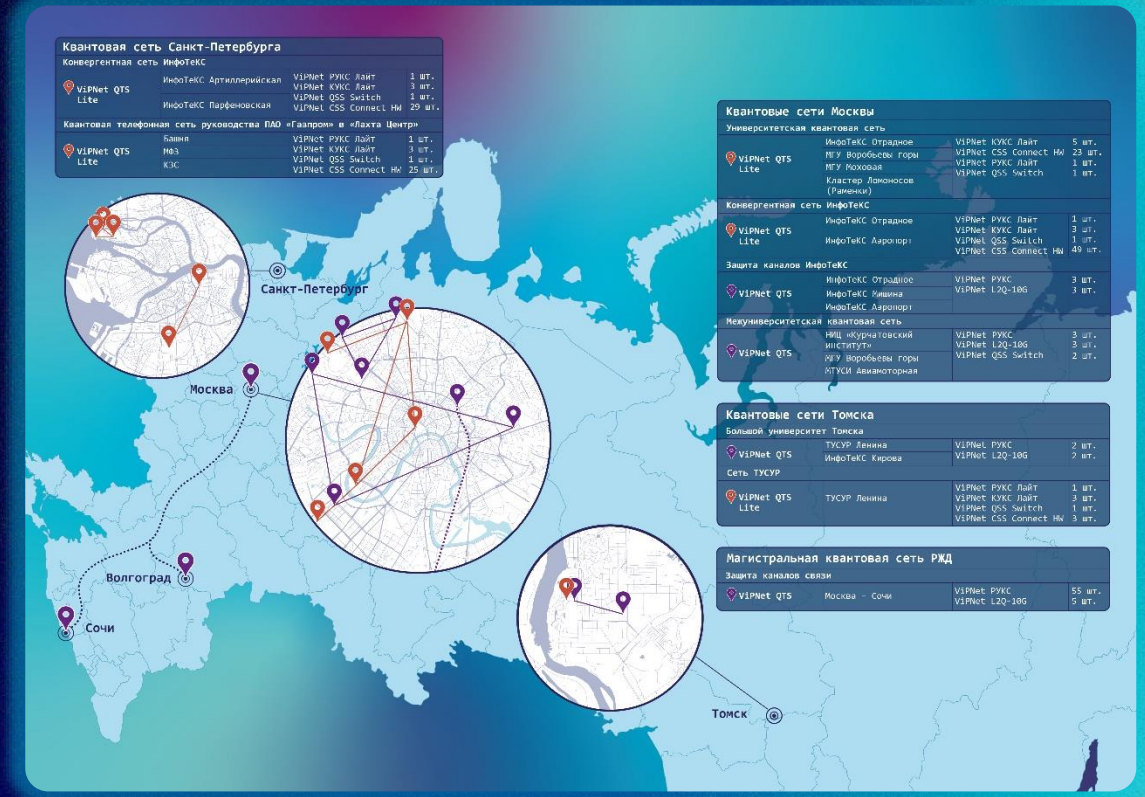


Этап 1:
Отказоустойчивое полносвязное ядро сети (проводятся пусконаладочные работы)

Этап 2:
Городская квантовая сеть (запуск в 2025 г.)

Этап 3:
МУКС национальной исследовательской компьютерной сети (НИКС); подключение к сети РЖД

Карта реализованных проектов



ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного