ViPNet QTS Lite квантовое распределение ключей в топологии «Звезда» на практике



Иванов Олег Менеджер



Ретроспектива событий





Академическая основа — взаимодействие с МГУ



Старт работ над ViPNet Quandor, ViPNet QSS



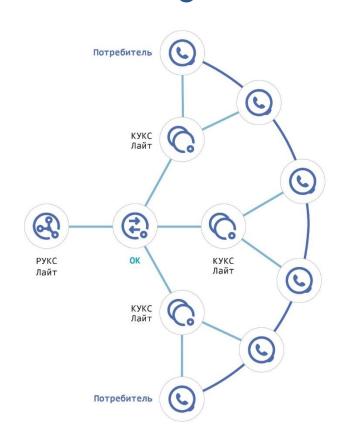




ViPNet QTS Lite,
ViPNet QTS:
Сертификация,
Производство
Поставки, Будущее

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
- о Возможность выработки на одном Клиенте КРК квантовозащищенных ключей для нескольких абонентов
- Полностью автоматическая регулярная смена ключей шифрования





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 ключейне 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





Оптический коммутатор квантовых сетей

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

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







Клиентский узел квантовой сети

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

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





ViPNet CSS Connect HW



Защищенный ІР-телефон

Предназначен для защиты информации с использованием квантовых ключей



Исполнение на базе аппаратной платформы GrandStream

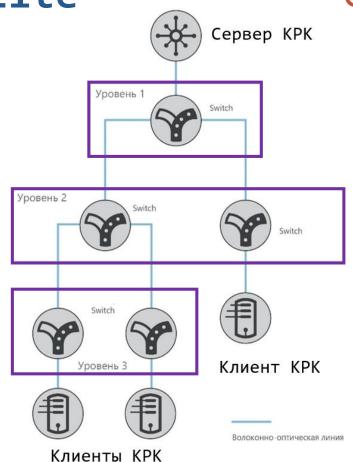


Исполнение на базе аппаратной платформы Aquarius

Комплекс ViPNet QTS Lite

TEXH@infotecs
2023 DECT

- 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







ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

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

от "05 " мая 2023 г.

Выдви Акционерному обществу «Информационные технологии и коммуникационные системы», Настоящий сертификат удостоверяет, что программию-аппаратный комплек-«ViPNet Клиентский узел квантовой сети Лайт» на состава квантовой криптограф

системы выработки и распределения ключей ViPNet Quantum Trusted Syste в комплектации согласно формуляру ФРКЕ 465636.005-01ФО еоответствует Требованиям к средствам кринтографической дашиты киф предназначенным для запиты информации, не содержащей сведений, соста государственную тайну, класса КСЗ, Воеменным требованиям к квантовым криптограсистемам выработки и распределения ключей для средств криптографической информации, предназначенным для защиты информации, не содержащей составляющих государственную тайну, класса КС и может использоват криптографической запиты (создание и управление ключевой информанией, в то

квантовозащищённой, шифрование файлов и данных, содержащихся в областих опе памети, вычисление имитовствики для файлов и данных, содержащихся в областях опе паняти, начисление значения хэш-функции для файлов и данных, содержащихся в оперативной памяти) информации, не содержащей сведений, составляющих государ

Сертификат выдан на основании результатов проведенных Обществом с огран ответственностью «СФБ Лаборатория». сертификационных непытаний образцов продукции ______ № № 1075Б-000501, 1075Б-000

Везопасность информации обеспечивается при использовании комплекса, изготова соответствии с техническими условиями ФРКЕ 465636.005-01ТУ, и выполнения тре эксплуатационной документации согласно формудиру ФРКЕ 465636.005-01ФО.

Заместитель, пуковолителя Научно-технической службы - пачальник Центра защиты информации и специальной связи ФСБ России





ФЕЛЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер <u>СФ /124-4509</u> Лействителен до " 05 " мая 2026 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы». Настоящий сертификат удостоверяет, что программно-аппаратилий комплекс «ViPNet Распределительный умед квантовой сети Лайт» из состава квантовой пригтографической системы выработки и распределения ключей ViPNet Quantum Trusted System Lite в комплектации согласно формулиру ФРКЕ 463636.004-01ФО

соответствует Тоебованиям к средствам кринтографической запиты информ предназначенным для запиты информации, не содержащей сведений, составляющих государственную тайну, класса КСЗ. Временным требованиям к квантовым принтографическия системам выработки и распределения ключей для средств криптографической заприза информации, предпазначенным для защиты информации, не содержащей сведений составляющих государственную тайну, класса КС и может использоваться для приглографической защиты (соклание и управление иличеной информацией, в том числе свантовозанившённой, шифрование файлов и дажных, содержащихся в облистях оперативно намети, вычисление воитовстанки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хош-функции для фойлов и данных, содержащихся в областях оперативной намити) виформации, не содержащей спедений, составляющих государственную

Сертификат выдан на основании результатов вроведенимх Обществом с ограниченной ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов продукции 2626 1075А-000501, 1075А-000502 Везопасность информации обеспечивается при использовании вомплекса, инготовленного в соответствии с техническими условиями ФРКЕ 455636 004-01ТУ, и выполнении требований эксплуатационной документации согласно формулиру ФРКЕ 465636.004-01ФО.

Заместитель руководителя Научно-технической и специальной связи ФСБ России



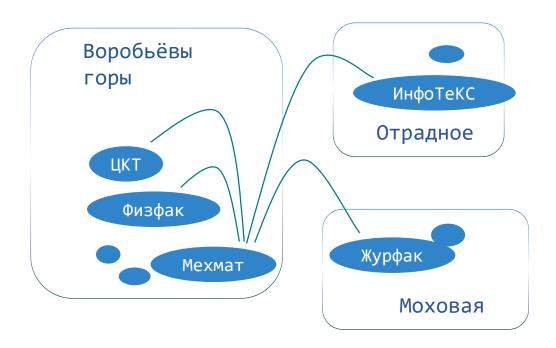
- ViPNet Клиентский узел квантовой сети Лайт (КУКС Лайт)
- ViPNet Распределительный узел квантовой сети Лайт (РУКС Лайт)
- соответствуют требованиям к СКЗИ и временным требованиям к квантовым криптографическим системам выработки и распространения ключей для СКЗИ







- 1 РУКС Лайт
- о 5 КУКС Лайт
- 22 абонентских пунктов
- о 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
- o 1 QSS Switch
- 26 абонентских пунктов



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

Подготовка



Линия

- Темное волокно
- Одномодовое волокно
- Допускаются переходники FC/UPC
- На длине полны 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





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



Собственное производство





Возможности

Полный технологический цикл опытного и мелкосерийного производства Поддержка максимально возможного уровня локализации производства

Собственное производствов Томске





Этапы строительства:

Начало строительства: июнь 2022 года

Ввод в эксплуатацию 1 очереди: в 2023

Ввод в эксплуатацию 2 очереди: к 2025 году



QTS Lite 2.0



- Увеличение расстояния между сервером КРК и клиентом КРК до 100 км.
- Реализация протокола защищенного взаимодействия между узлом квантовой сети и потребителем ключей ProtoQa.
- Поддержка большего количества и типов потребителей.
- Разработка клиента КРК в форм-факторе 2U для телеком-стоек.



Спасибо за внимание!

Подписывайтесь на наши соцсети





vk.com/infotecs news





https://t.me/infotecs official





rutube.ru/channel/24686363