

Квантовое распределение ключей на практике

Смирнов Николай
Директор по продуктам, Инфотекс

День сегодняшний



Структура продуктов и решений КРК (и их аббревиатуры) Инфотекс 2023

ViPNet Quantum Cryptographic System ViPNet QCS

ViPNet Quantum Trusted System ViPNet QTS

ViPNet QTS Lite ViPNet QTS



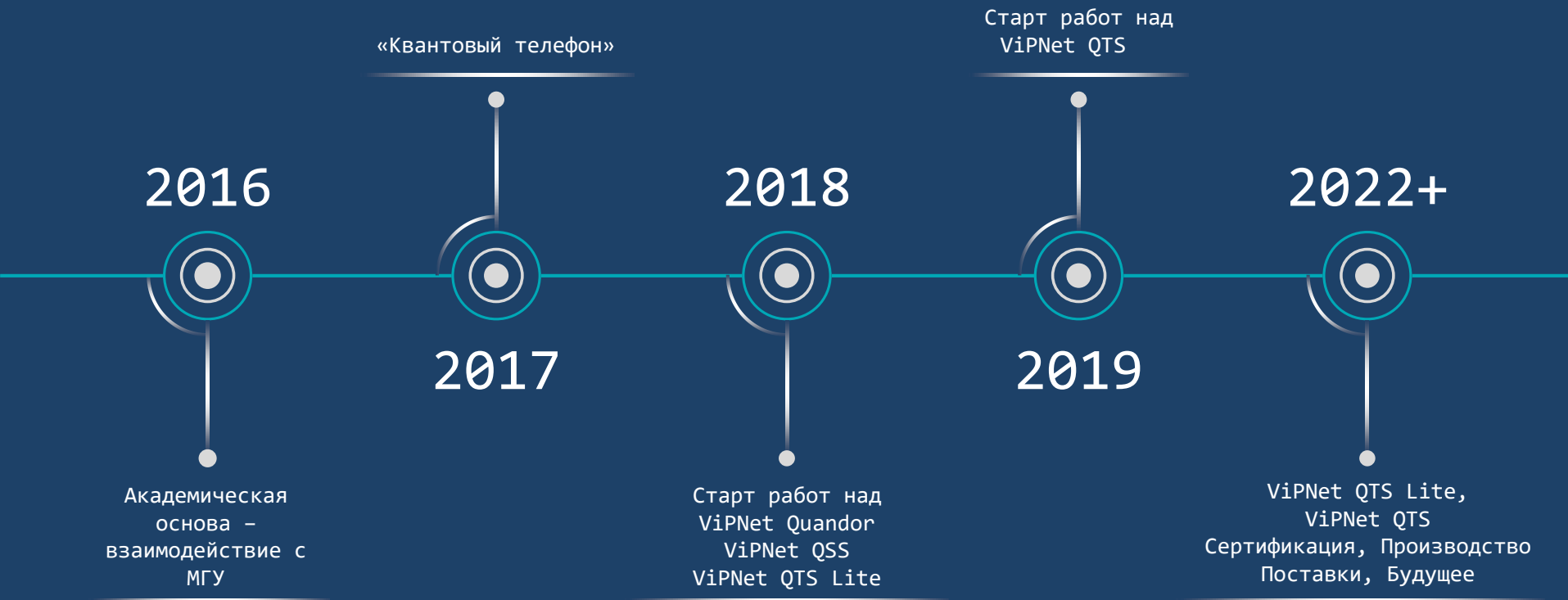
ViPNet Quandor



Этапы большого пути



Ретроспектива событий





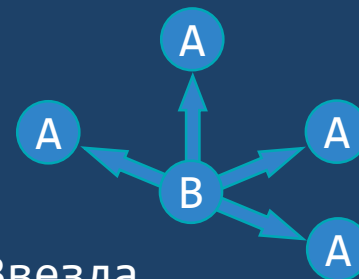
«Квантовый телефон»

2017:

- Быстрый старт и предметное начало сотрудничества
- Демонстрация ключевых преимуществ технологии
- Интеграция с системой ViPNet VPN и ViPNet CSS Connect
- Это еще не Продукт!

VIPNet QTS Lite (VIPNet QSS)

- VIPNet РУКС Лайт (QSS Server)



Топология Звезда

- VIPNet QSS Switch



- VIPNet КУКС Лайт (QSS Point)



- Распределение ключей по топологии «Звезда» для практически неограниченного количества абонентов
- Бесшовная интеграция с существующими сетями на базе технологии VIPNet
- Шифрование трафика на ключах, не известных администратору сети
- Возможность выработки на одном Клиенте квантовозащищенных ключей для нескольких абонентов
- Протяженность оптического канала до 44—км 100 км
- А вот это уже продукт!

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



Академические и собственные пилоты и проекты

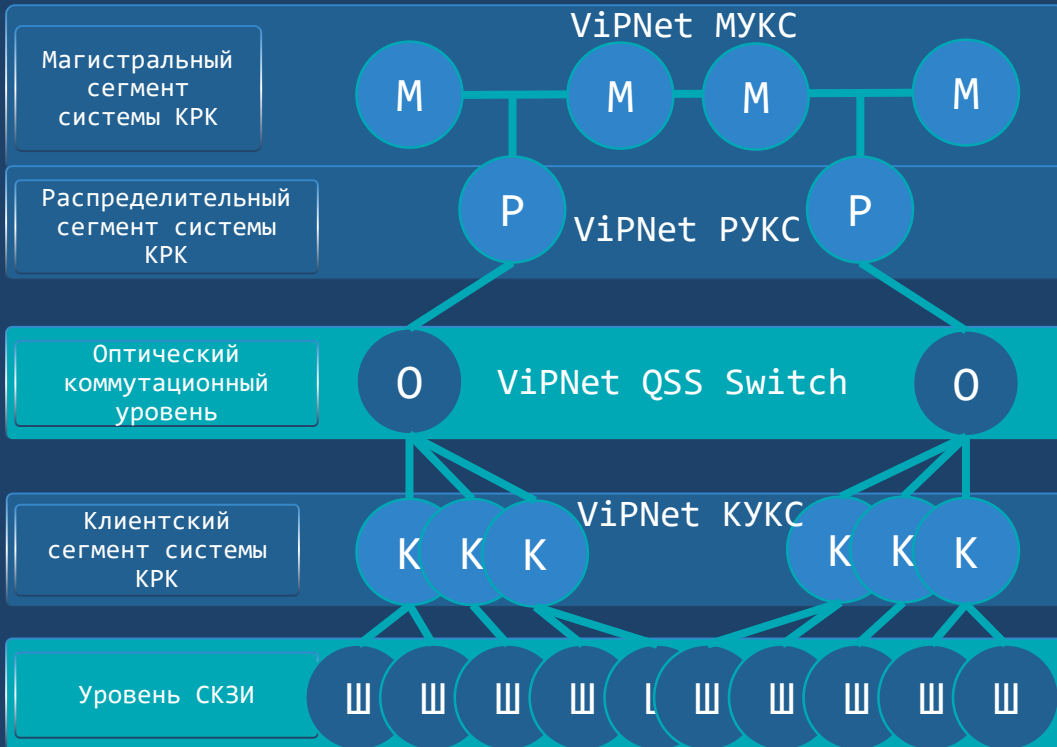
ТУСУР
TUSUR UNIVERSITY

Собственные
ПИЛОТЫ

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

 - 1 РУКС Лайт
 - 2 КУКС Лайт
 - 1 QSS Switch
 - 15 Абонентских пункта
- 2 МУКС
 - 1 РУКС
 - 2 КУКС
 - 80 км

ViPNet QTS (ДПУ)



- Расстояние $100 \text{ км} * N$
- Произвольная топология
- Стандартный интерфейс подключения СКЗИ ProtoQa
- Произвольные СКЗИ - потребители

ViPNet QTS продукты

ViPNet МУКС и ViPNet РУКС



- Два квантовых оптических модуля в одном корпусе
- 4U защищенный корпус
- Масса ~ 40 кг

ViPNet КУКС

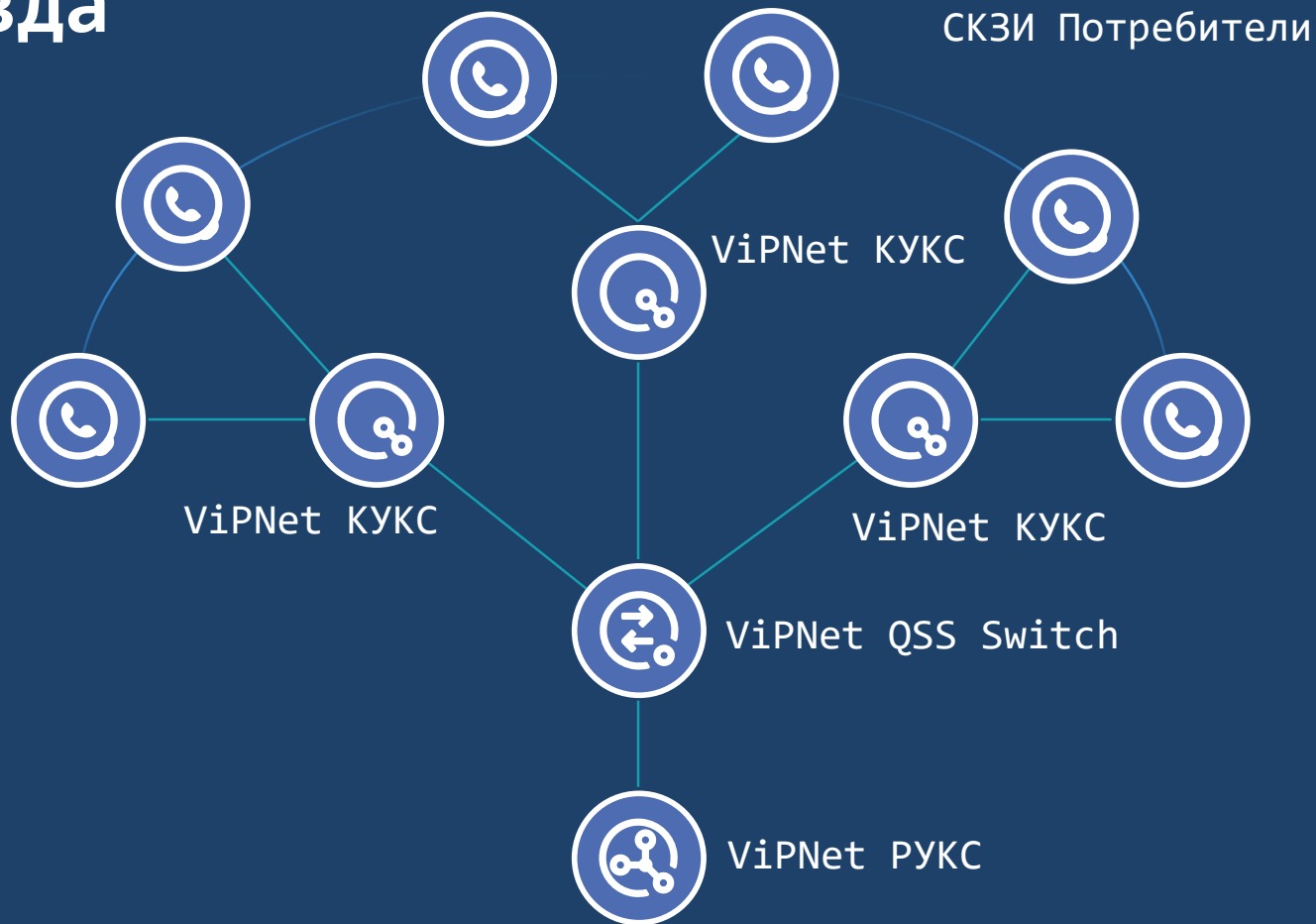


- Один квантовый оптический модуль в корпусе
- 2U защищенный корпус
- Масса ~ 20 кг

Магистраль



Звезда



Опыт



Подготовительный этап

- Рефлектометрия линии
- Определение длины и потерь

Сеть ViPNet VPN

- Квантовые узлы
- Классические узлы
- Служебный канал
- Абонентские пункты (шифраторы, телефоны)

Сеть КРК

- Монтаж оборудования
- Ввод ключевой и справочной информации

Пилот подготовка

Линия

- Темное волокно
- Одномодовое волокно
- FC/UPC (переходники допускаются)
- Потери не более 0.2 дБ на км (на длине волны 1550нм)
- 100 км для QTS
- 44 (100!) км для QTS Lite

Размещение

- ПКЗ 2005
- Телекоммуникационная сеть для служебных каналов
- Температура +10 - +40

Неприятности

Монтаж

- Дефекты линии
- Грязные разъемы
- Ошибки подключения
- Подрядчик заменил участок оптоволокна медью через конверторы (😊)

Линия

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

Эксплуатация

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

Главное

- Мы говорим о серийном оборудовании
- В ГК Инфотекс собран уникальный опыт испытаний и измерений оборудования КРК
- Мы уже перешли на 3-ю ревизию оптического оборудования, в которой учтен весь полученный опыт
- Магистраль QTS (ДПУ) с ответвлениями – можно рассматривать как пример взаимодействия оператора квантовой сети федерального и регионального уровней

Спасибо за внимание!

Электронная почта:
smirnovnv@infotecs.ru