Квантовые продукты ИнфоТеКС

Дмитрий Гусев

Квантовые технологии и безопасность

Квантовые технологии: различие 100 лет назад и сейчас

ТЕХНО infotecs 2021 ФЕСТ

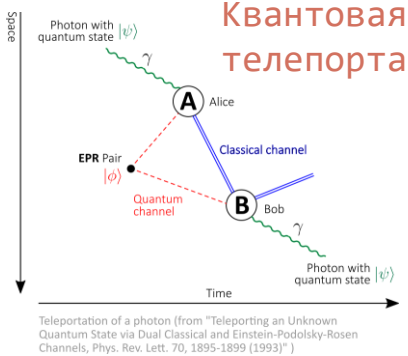
Коллективные квантовые эффекты

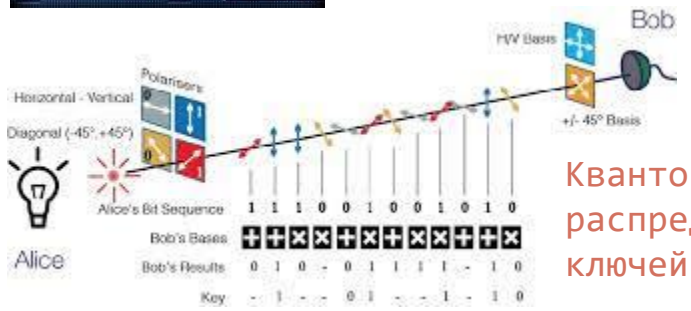
Ядерные реакции

Полупроводники

Индивидуальные квантовые эффекты

Квантовая телепортация

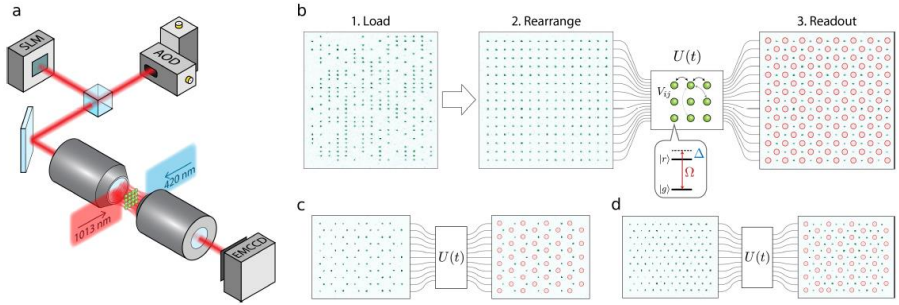


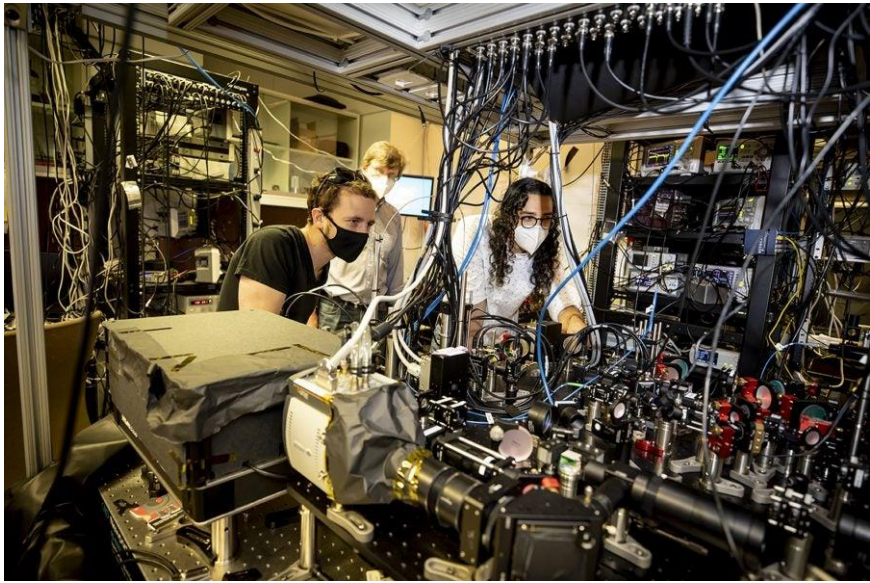


Квантовое распределение ключей

Достижения в области квантовых компьютеров

Июль 2021 года – программируемый квантовый компьютер с 256 кубитами на холодных атомах (Harvard-MIT Center for Ultracold Atoms)





Устойчивость к квантовому компьютеру? Зачем?

- Хэш-функции: **увеличение длины хэш-кода в 2-3 раза**
- Блочные шифры: **увеличение длины ключа в 2 раза**
- Асимметричная криптография (классическая): **экспоненциальное увеличение длины ключей**

Традиционные асимметричные криптографические схемы должны быть заменены. Для выработки общего ключа – квантовое распределение ключей.

КРК: Безопасное сегодня и завтра

Угрозы из будущего,
от которых защищает КРК:

- появление квантового компьютера;
- прогресс в вычислительных атаках на криптосистемы.

Борьба с **актуальными угрозами:**

- захват криптографического устройства (защита от чтения назад и вперед);
- вербовка администратора системы защиты (ключевого центра).

Серьезные намерения

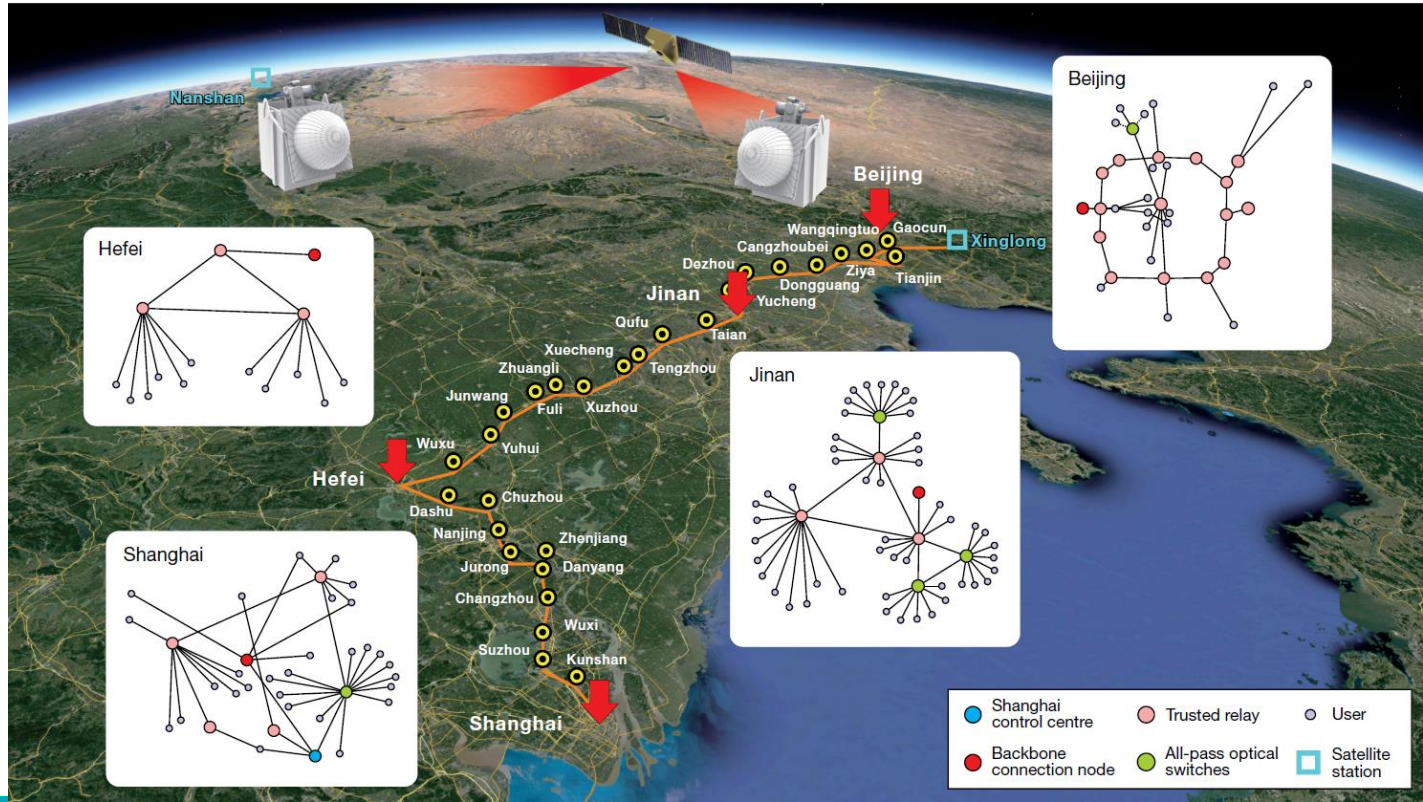
Великая китайская квантовая сеть с наземными и космическими сегментами

400
наземных сегментов

2 спутника

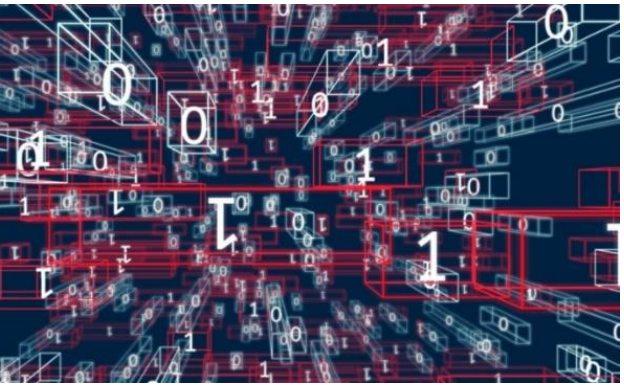
4600 км
общая протяженность

157
потребителей



Постквантовая криптография

Методы синтеза постквантовых механизмов



Синтез постквантовых асимметричных криптосхем – выбор математической задачи, для которой на текущий момент не известен эффективный алгоритм решения как на классическом, так и на квантовом компьютере.

Разделы математики, потенциально содержащие такие задачи:

- теория решеток
- теория кодирования
- криптографические хэш-функции
- многочлены от многих переменных
- изогении на эллиптических кривых
- прочее (алгебра октонионов, многочлены Чебышева, косы и т.д.)

Стандартизация постквантовых механизмов

ANSI: X9.98-2010: NTRU

IEEE: P1363.1-2008: NTRU

IETF

- RFC 8391 (2018): XMSS
- RFC 8554 (2019): LMS

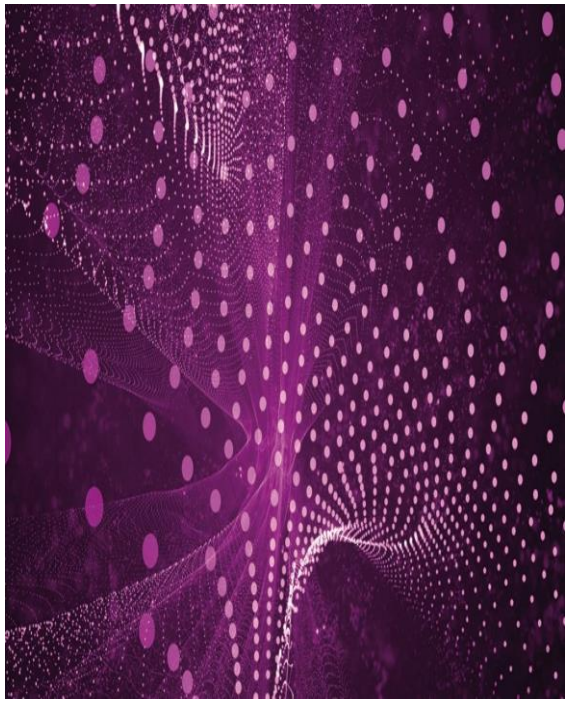
NIST: конкурс по выбору и стандартизации

ISO/IEC JTC1 SC27 WG2: SD8

ТК 26 РГ 2.5: подготовка предложений по стандартизации

Проблемы постквантовой криптографии

- Относительная молодость направления → недостаточные изученность и доверие
- Появления квантовых алгоритмов, эффективно решающих «новые» математические задачи → «новые» постквантовые схемы также перестанут быть стойкими
- Большое количество новых схем → возможность наличия закладок
- Меньшая эффективность постквантовых схем по сравнению с традиционными:
  - большие размеры ключей, шифртекстов и подписей
  - низкая производительность
- Практическая сложность массового перехода на постквантовые схемы и неясные сроки осуществления такого перехода



Как работает квантовое распределение ключей

Основы

КРК – **криптографический протокол,** позволяющий двум удаленным абонентам выработать общий случайный секрет (ключ)

Теорема о запрете клонирования (копирования) неизвестного квантового состояния позволяет **гарантированно детектировать** пассивного/активного злоумышленника.

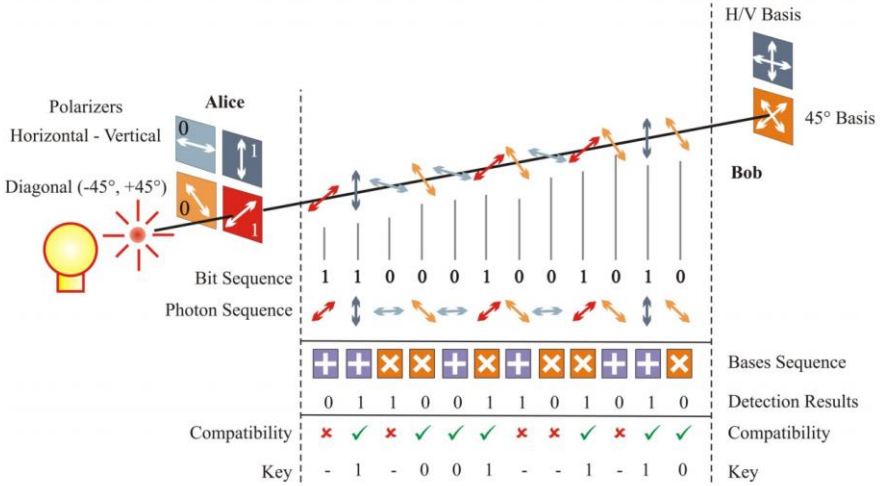
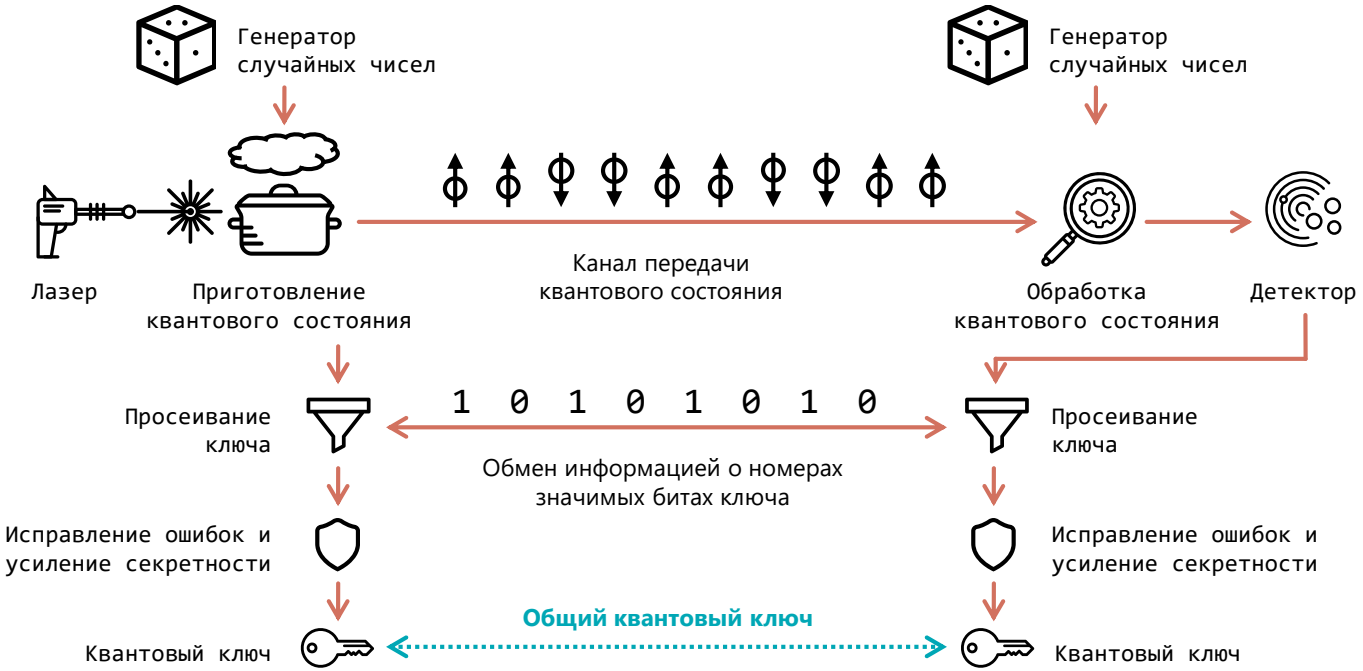


Fig. 1. Key exchange in the BB84 protocol implemented with polarization of photons (adapted from [56]).

Квантовое распределение ключей. Принцип действия



КРК: не все так просто

1. Проверенное качество генератора случайных чисел
2. Контролируемая псевдооднофотонность
3. Доказанная секретность квантового протокола с указанием ограничений
4. Поправка на псевдооднофотонность при усилении секретности
5. Поправка на потери в канале при усилении секретности
6. Реализация мер защиты аппаратуры от известных атак по требованиям Регулятора
7. Криптографическая подлинность коммуникаций между Алисой и Бобом
8. Эксплуатация с учетом ограничений и правил пользования

КРК: Текущий уровень и перспективы

ТехноИнфотекс Фест 2021

Расстояние

- до 100 км – типовое темное волокно, «сухой» детектор
- до 500 км – спец. волокно, сверхпроводящий детектор

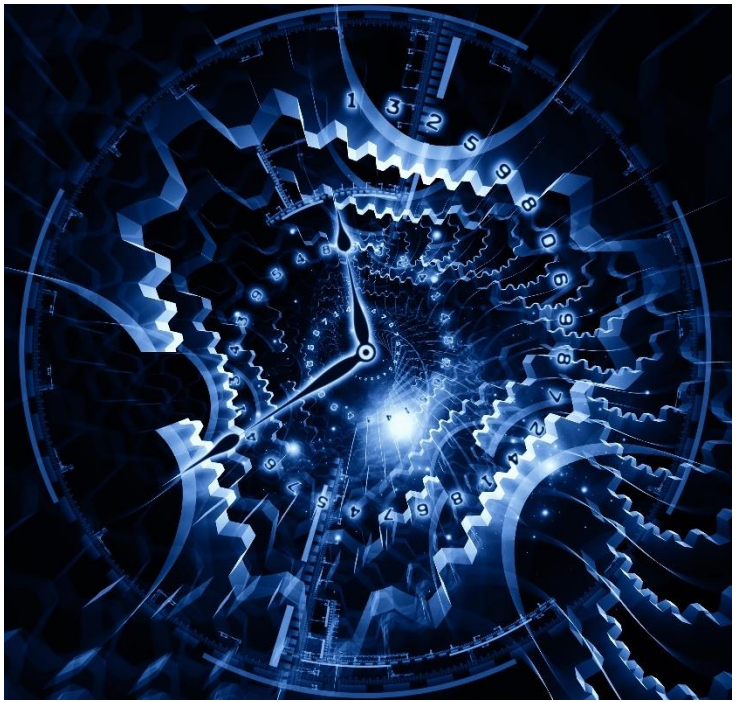
Скорость выработки ключа

типовая – килобиты/с на 50 км волокна;
достижимые:

- мегабиты/с в волокне
- килобиты/с на 1 км воздуха
- биты/сутки на низкоорбитальных спутниках

Массогабариты

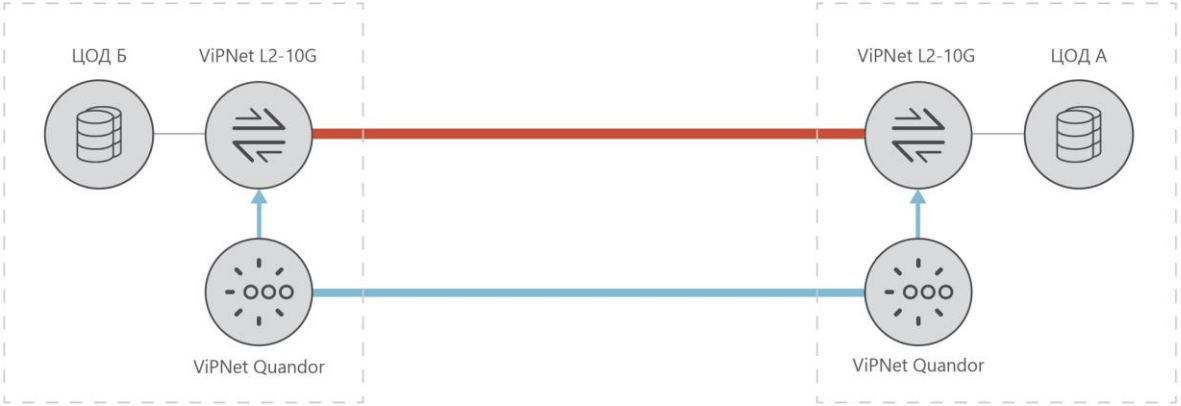
- типовые – сервер 1U-4U
- достижимые – 5’-CD-ROM
- перспектива – кредитная карта



Квантовые продукты и решения ViPNet

ViPNet Quandor

КРК для защиты каналов связи



ViPNet Quandor

Базовый сценарий – автоматическая доверенная доставка криптографических ключей для канальных шифраторов ViPNet L2.

Для использования квантовых ключей к шифратору по защищенному интерфейсу подключается аппаратура ViPNet Quandor, которая устанавливается в контролируемой зоне шифратора

Особенности решения ViPNet Quandor

- Длина квантового канала до 100 км
- Не требует дополнительного охлаждения
- Устанавливается в стандартную серверную стойку
- Автоматическая смена ключей не реже, чем 1 раз в минуту
- Гибридная ключевая система
- СКЗИ класса КС3
- Стойкость к атакам, возможным при реализации эффективного квантового компьютера

Находится на сертификации по требованиям ФСБ России

Комплект оборудования для пилотной эксплуатации ViPNet Quandor на сетях заказчика

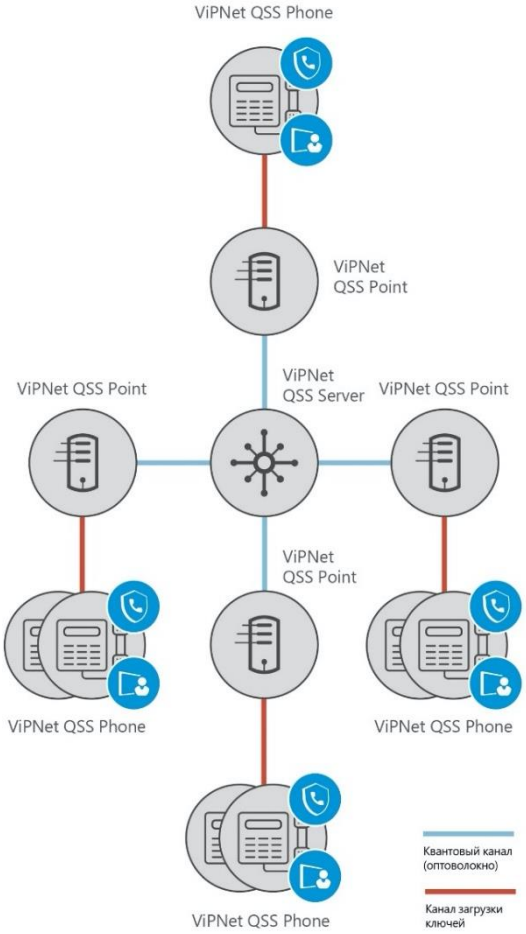
- Мобильный комплект для быстрого разворачивания на сетях заказчика
- Защита во время транспортировки
- Минимальные затраты времени на ввод в эксплуатацию
- Демонстрация рабочего решения, готового к поставкам

ViPNet QSS

КРК для абонентов

Особенности ViPNet QSS

- Распределяет квантовые ключи по сетевой топологии «Звезда» для практически неограниченного количества абонентов
- Бесшовная интеграция с существующими сетями на базе технологии ViPNet
- Не подвержен атакам, которые станут возможными при реализации эффективного квантового компьютера
- Стойкость квантового протокола математически доказана
- Шифрование трафика на ключах, неизвестных даже администратору сети
- Возможность выработки на одном Клиенте квантовозащищенных ключей для нескольких абонентов
- Полностью автоматическая регулярная смена ключей шифрования
- Пользователь сам может запросить выработку нового ключа в любой момент



ViPNet QSS: состав

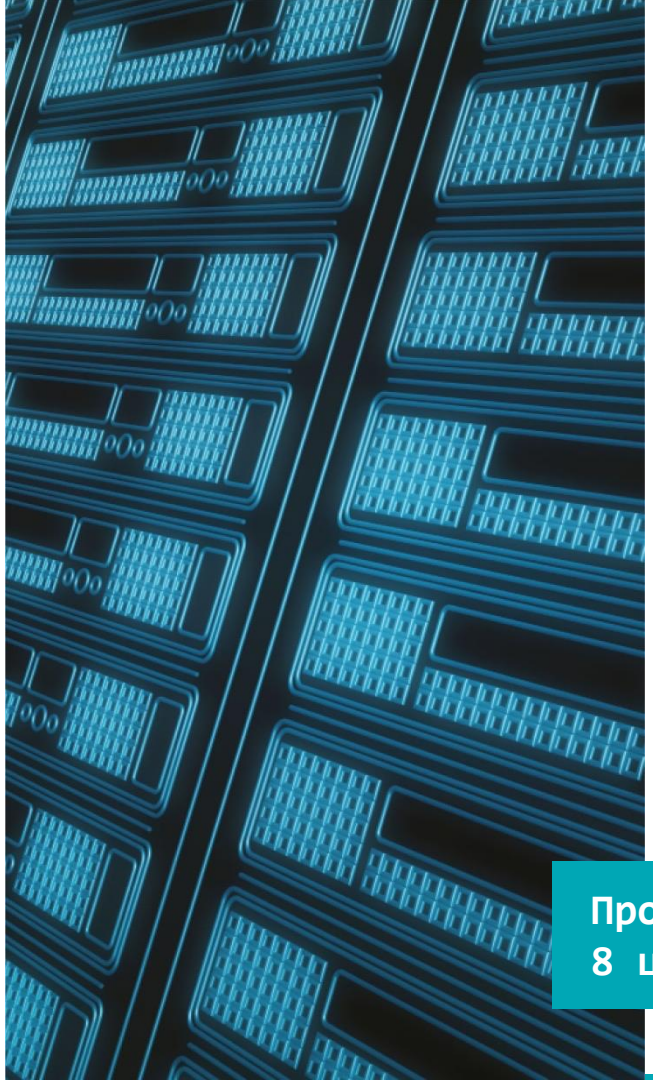
ViPNet
QSS Server

ViPNet
QSS Switch

ViPNet
QSS Point

Некоторые ТТХ ViPNet QSS

- Топология «Звезда»
- Расстояние между QSS Server и QSS Point до 44 км
- 3 уровня оптической коммутации с резервированием каналов
- До 1600 Клиентов КРК (ViPNet QSS Point, подключенных к серверу ViPNet QSS Server)
- К одному ViPNet QSS Point можно подключить много потребителей ключей (ViPNet QSS Phone) в пределах одной зоны доверия



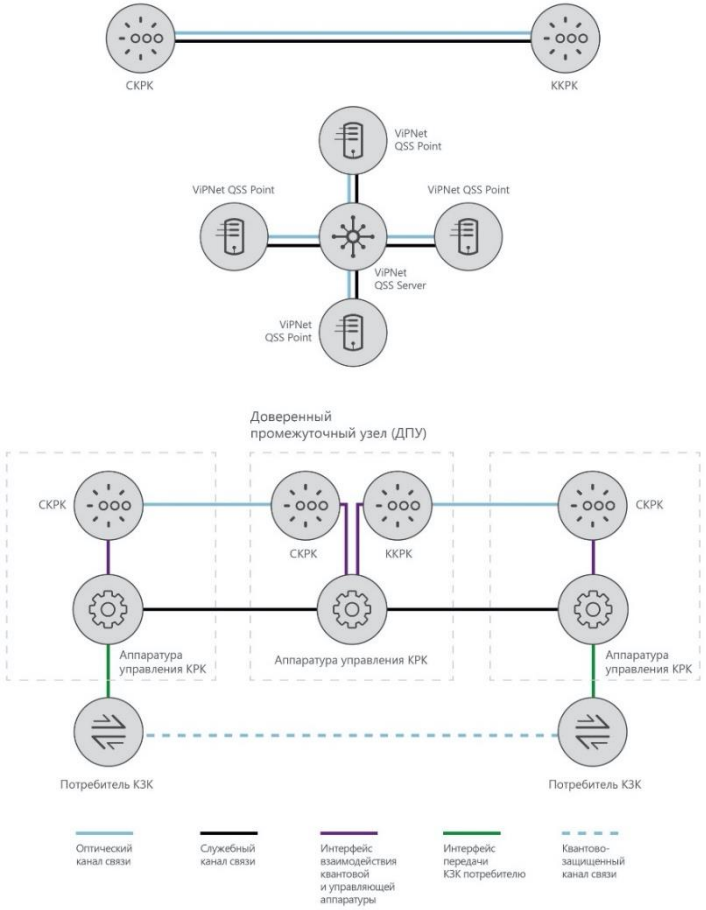
- Класс защиты ViPNet QSS Server и ViPNet QSS Point — КС3 (Все аппаратные решения соответствуют классу КВ, в планах весь комплекс «дотянуть» до КВ)
- ViPNet QSS Phone (Android) — КС1
- В планах создание телефона на OS Linux на класс КВ
- Возможно размещение в категорируемых помещениях

Проводятся исследования 8 центром ФСБ России

Что дальше?

Концепция развития технологии квантового распределения ключей ViPNet

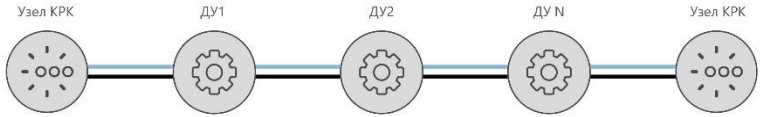
- Квантовая сеть произвольной топологии
- Криптографические ключи с доказательством секретности
- Без использования асимметричных криптографических механизмов
- Ключи неизвестны администратору сети
- Автоматическая смена ключей во всей сети
- Неявная компрометация одного узла (например, увольнение администратора ИБ) не приводит к необходимости переинициализации всей сети



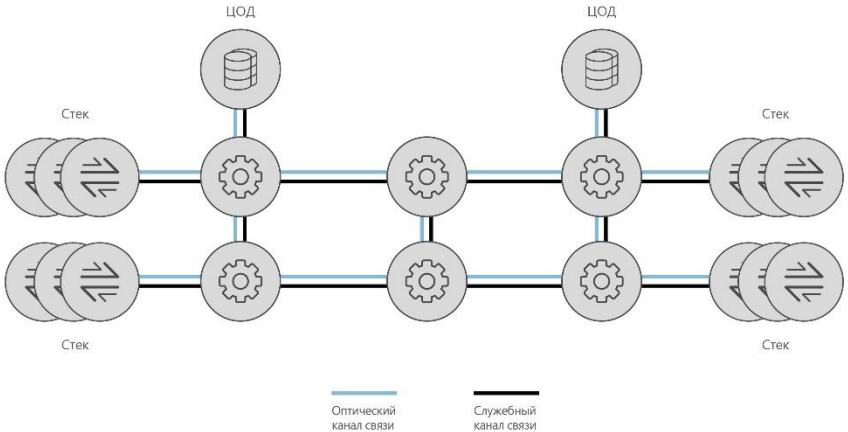
Пошаговое развитие топологии квантовых сетей

- Соединение топологии КРК «точка-точка» в любую конфигурацию
- В основе квантовой сети произвольной топологии — технология доверенного промежуточного узла
- Все «квантовые» продукты получают криптографические ключи от одной сети

Квантовая магистраль



Квантовая сеть произвольной топологии на базе доверенных промежуточных узлов



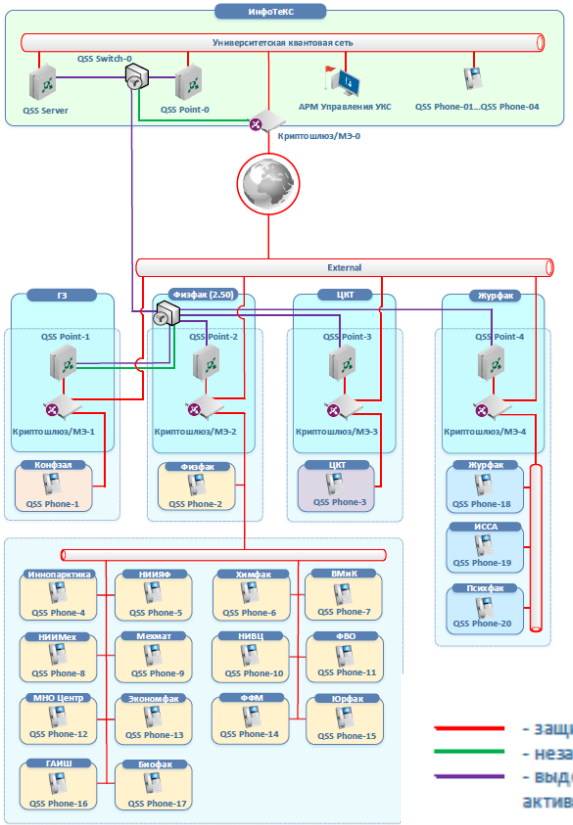
Пошаговое развитие топологии квантовых сетей

- Масштабируемая магистральная опорная сеть
- Подключение к квантовой сети любых СКЗИ
- Стандартизованные интерфейсы взаимодействия (протокол ProtoQa)

Практические шаги по реализации

Первые реальные проекты

Университетская квантовая сеть



Первое внедрение квантовой криптографии

- В офисе ИнфоТеКС развернута сеть опытной эксплуатации
- К сети компании подключен сегмент квантовой сети МГУ
- Планируется подключение новых сегментов в Москве
- Осуществляется автоматическая непрерывная эксплуатация «квантовых» СКЗИ

ТЕХНО 2021 infotecs Фест

Спасибо за внимание!

Дмитрий Гусев

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow