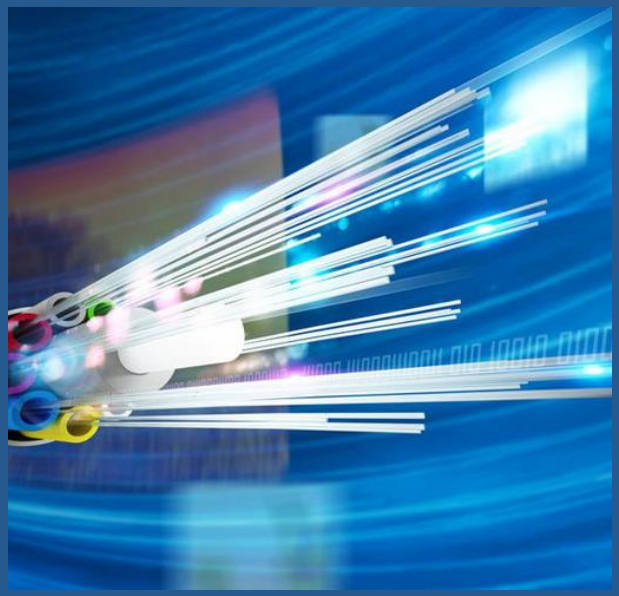
infotecs

Квантовая криптография в продуктах ИнфоТеКС

Александр Поздняков

Тенденции в развитии сетей связи и угрозы ИБ

Основные тенденции развития в сфере телекоммуникаций



- Увеличение скоростей магистральных каналов 10 Гбит/с → 100 Гбит/с → 400 Гбит/с
- Увеличение объемов передаваемой информации: на 20-25% ежегодно
- Вездесущая оптика, в том числе, на «последней миле»
- Необходимость криптографической защиты передаваемых данных

Современные и перспективные риски и угрозы для передаваемых зашифрованных данных

- ✓ Быстрая выработка нагрузки на ключ
- ✓ Отложенный взлом
- ✓ Создание эффективного квантового компьютера
- ✓ Компрометация ключей шифрования администратором

“Store now – decrypt later!”

ethereum
golem

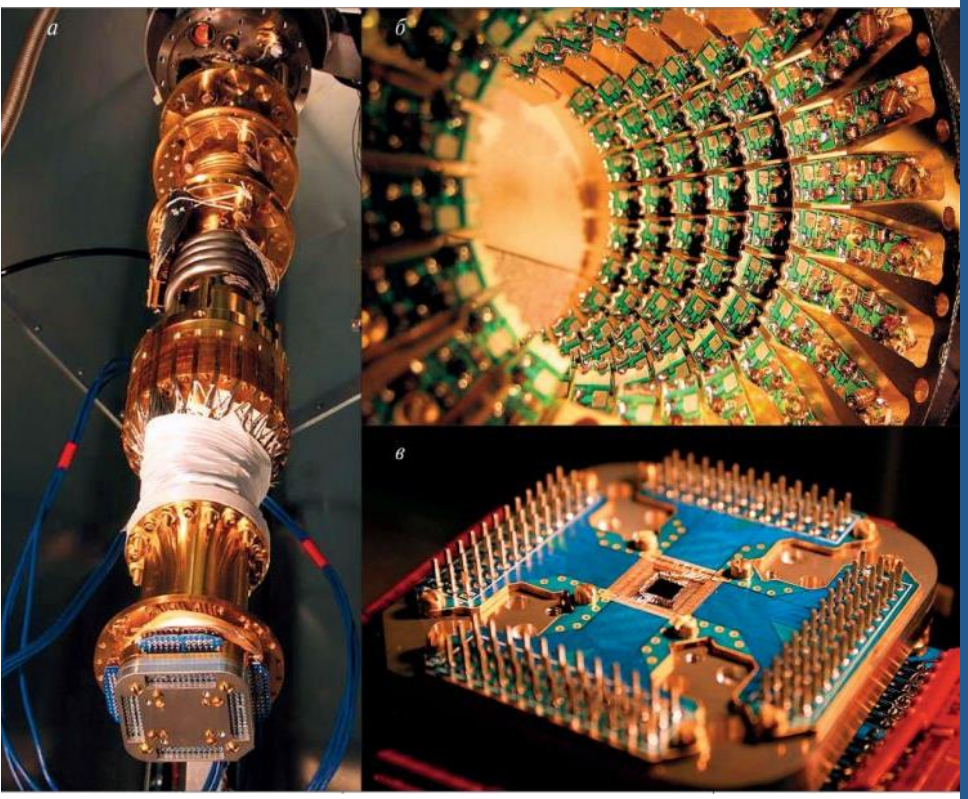
BITCOIN

Azure

EC2

Вычислительные ресурсы против зашифрованных данных

- ✓ Закон Мура
- ✓ Общедоступные средства распределенной обработки данных
- ✓ Готовая инфраструктура майнинга криптовалют
- ✓ Использование вычислительных ресурсов пользователей вредоносным программным обеспечением



Квантовые компьютеры

Коммерческие продукты:

- ✓ D-Wave Systems >1000 кубитов
- ✓ IBM Q System One 20 кубитов

Исследовательские системы:

- ✓ Intel Tangle Lake 49 кубитов
- ✓ IBM 50 кубитов
- ✓ Google Bristlecone 72 кубита

Квантовые алгоритмы Шора и Гровера

- Компрометация **всех** распространенных ассиметричных криптографических алгоритмов и протоколов на их основе (DH, RSA, ECDSA TLS/SSL, HTTPS, IPsec, X.509)
- Понижение стойкости симметричных криптоалгоритмов:

Криптоалгоритм	Атака	Стойкость в классике	Стойкость с учетом алгоритма Гровера
AES – 256 bit key	Подбор ключа	2^{256}	2^{128}
SHA2 или SHA3 – 384 bit hash	Поиск прообраза	2^{384}	2^{192}
	Поиск коллизии	2^{192}	2^{128} (с 2^{128} бит памяти)

Центральная задача в криптографии

Базовые практические задачи криптографии

1. Генерация качественных случайных чисел
2. Защищенные реализации криптографических алгоритмов
3. Управление ключами - совокупность процедур и процессов, сопровождающих жизненный цикл ключей в (крипто) системе:
   - Генерация
   - Установка или транспортировка
   - Архивирование или восстановление
   - Использование или хранение
   - Смена
   - Вывод из эксплуатации

infotecs

Ключи

«Враг знает систему» © Клод Шеннон

infotecs

То есть:

- Секретность алгоритмов шифрования и аппаратной реализации **не определяют** стойкость криптосистемы
- Стойкость криптосистемы определяется лишь **секретностью ключа**

Откуда взять ключ?

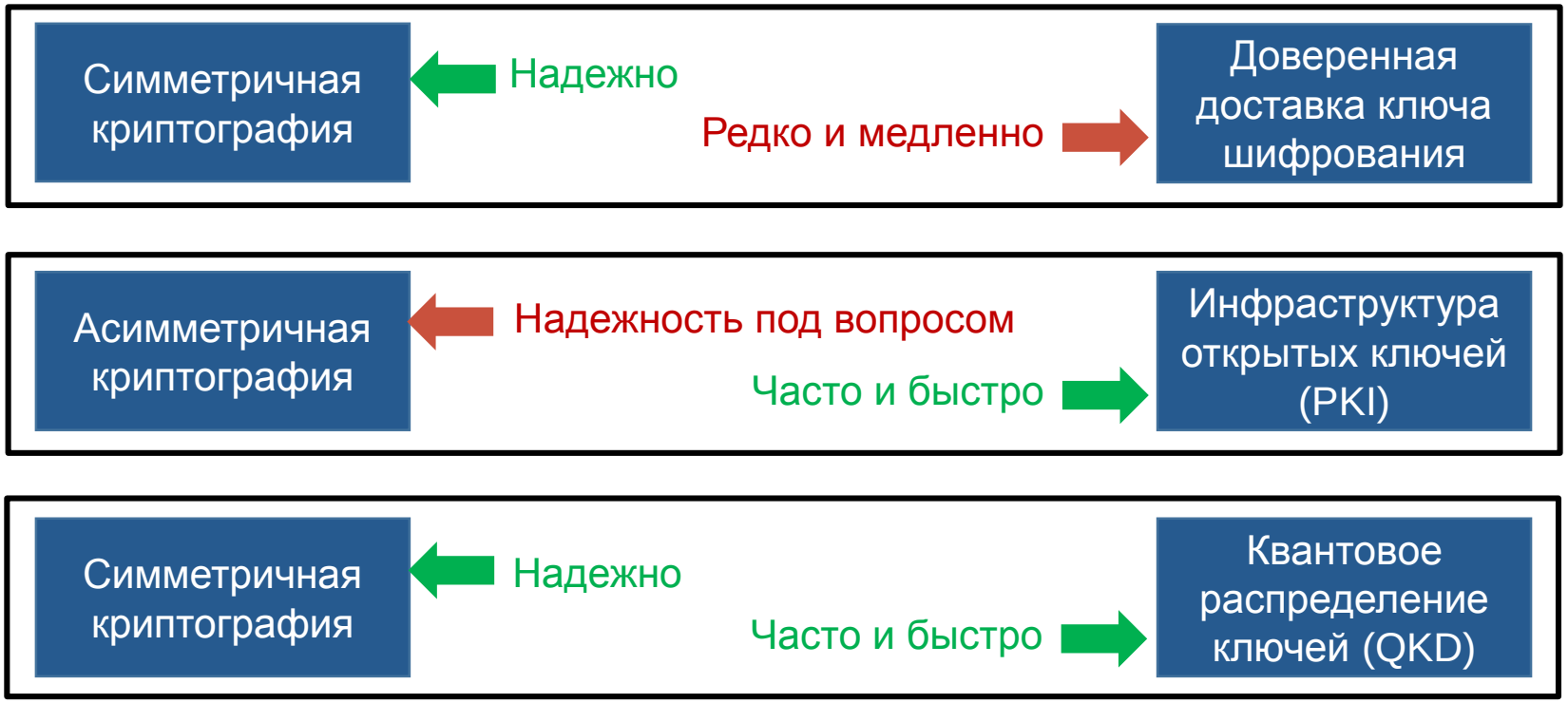
Откуда брать секретные ключи?

- Доверенный курьер **доставляет ключи** из ключевого центра

или

- Ключи **вычисляют** при условии двусторонней аутентификации (DH)

Подходы к выработке общего секретного ключа



Проблемы всех классических механизмов распределения ключей

- Не обеспечивается безусловная секретность ключей
- Дорогостоящие организационно-технические меры
- Всегда есть «человеческий фактор»
- Создание квантового компьютера приведет к компрометации всех ассиметричных криптографических алгоритмов и протоколов на их основе (DH, RSA, ECDSA TLS/SSL, HTTPS, IPsec, X.509)

Зачем нужна быстрая смена ключей?

Для
- конкретного алгоритма шифрования
- в конкретном режиме работы
- для конкретного варианта реализации СКЗИ

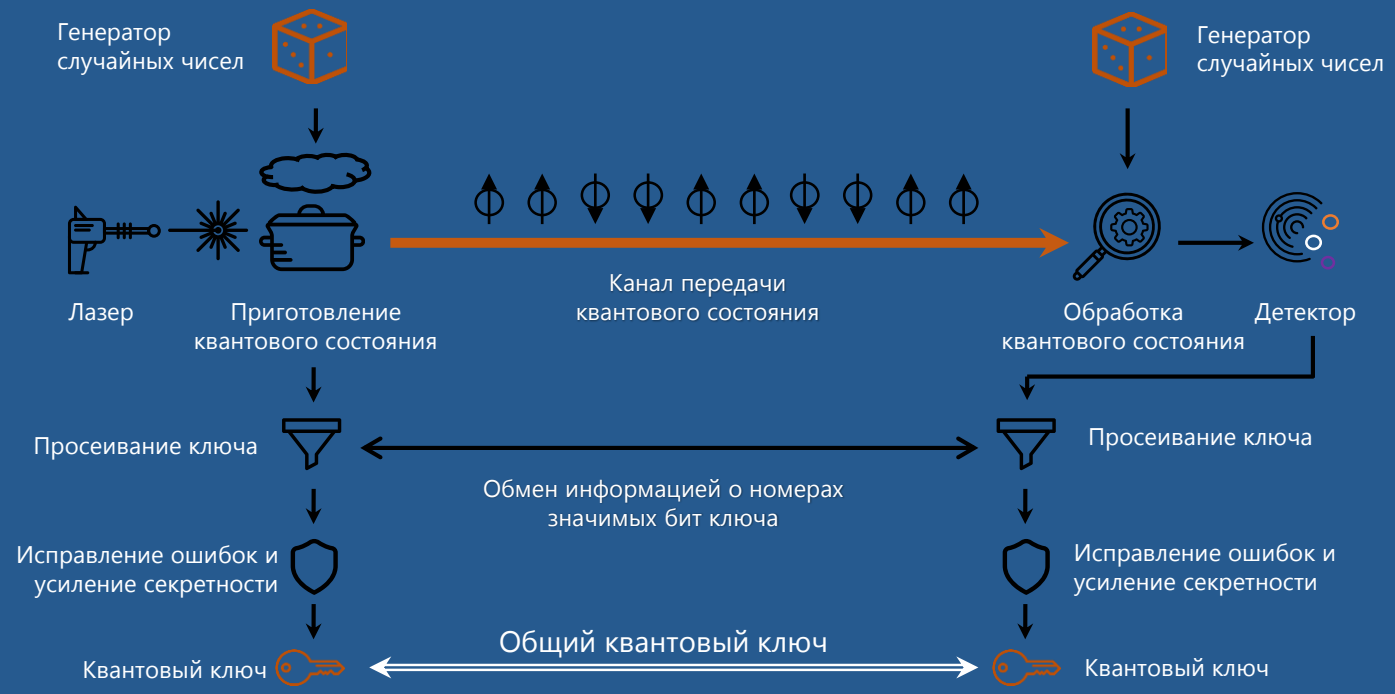
имеется предельное количество данных, которые допустимо зашифровать на одном ключе – **нагрузка на ключ**

Пример – Алгоритм блочного шифрования по ГОСТ 28147-89

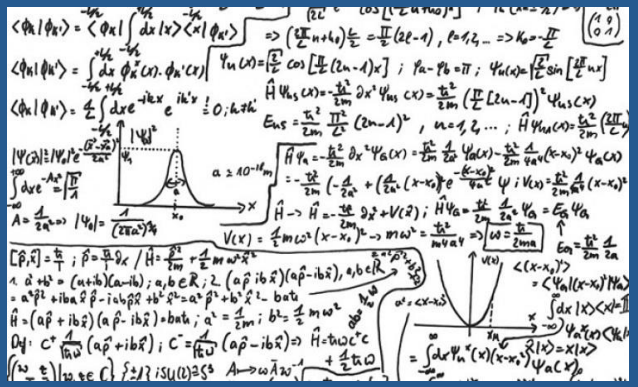
- Размер блока n = 64
- Предельная теоретическая нагрузка $2^{64/2} = 2^{32}$ блоков шифртекста, или 256 Гбит данных
- Шифратор на скорости 10 Гбит/с израсходует ключ за 25 секунд


infotecs
Технология
квантового
распределения
ключей

Квантовое распределение ключей
Принцип действия

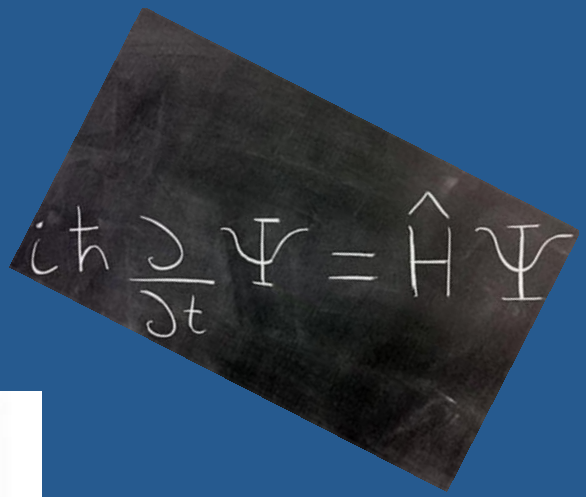


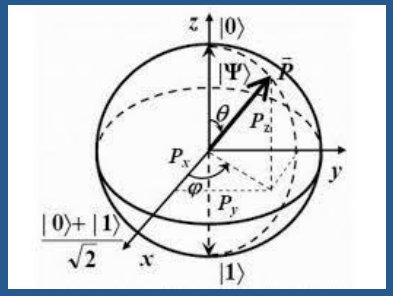
В чем «квантовость»?



Секретность выработки квантовых ключей основана на следующих квантовых принципах:

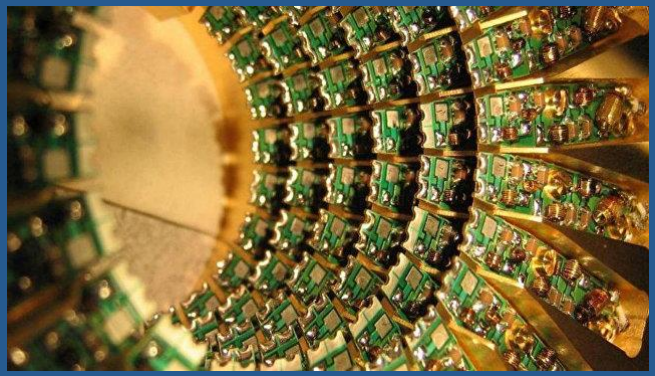
1. Фотон неделим
2. Невозможно клонировать неизвестное квантовое состояние
3. Невозможно измерить квантовое состояние без его изменения (редукция волновой функции)
4. Невозможно различить два неортогональных квантовых состояния



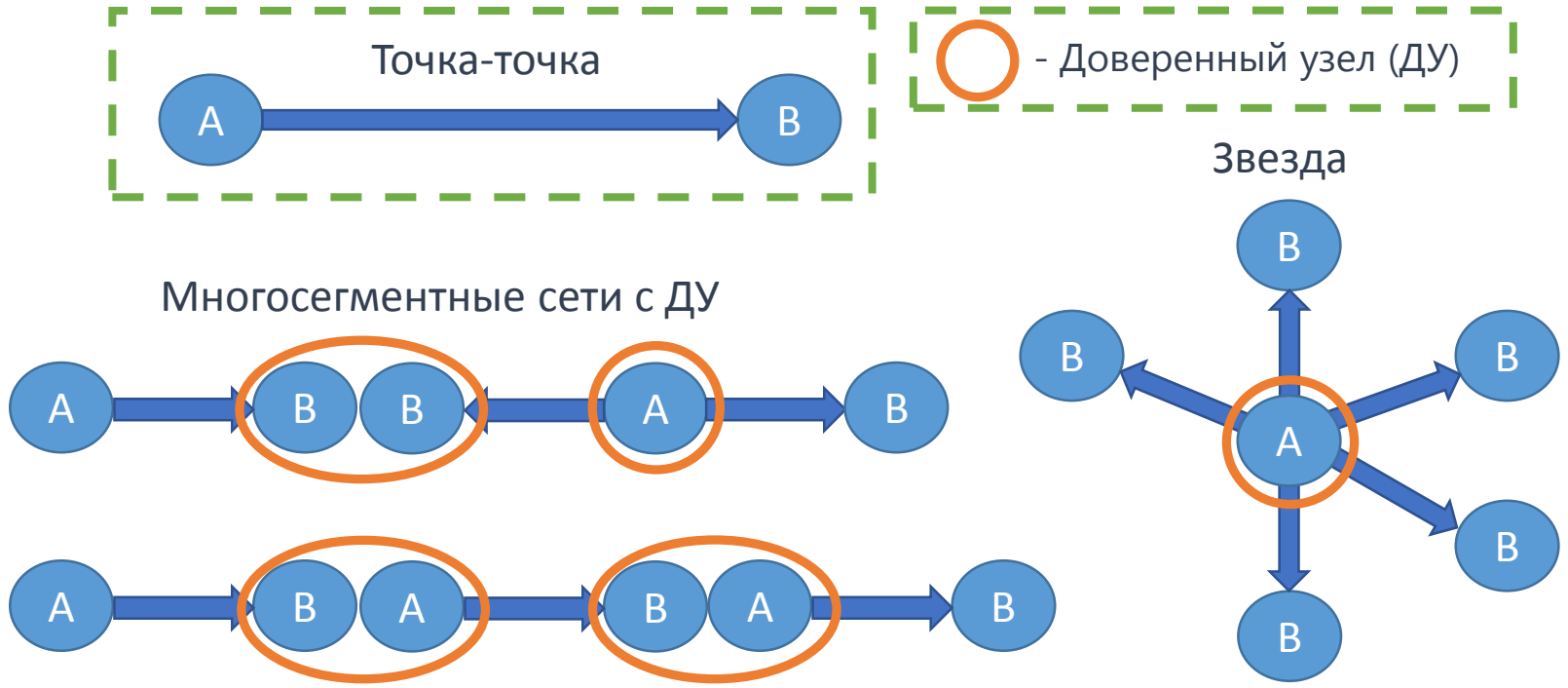


Преимущества технологии квантового распределения ключей

1. Секретность квантовых ключей доказана математически
2. Выработка ключей происходит автоматически без участия администратора
3. Устойчив к квантовому компьютеру
4. Высокая скорость смены ключей



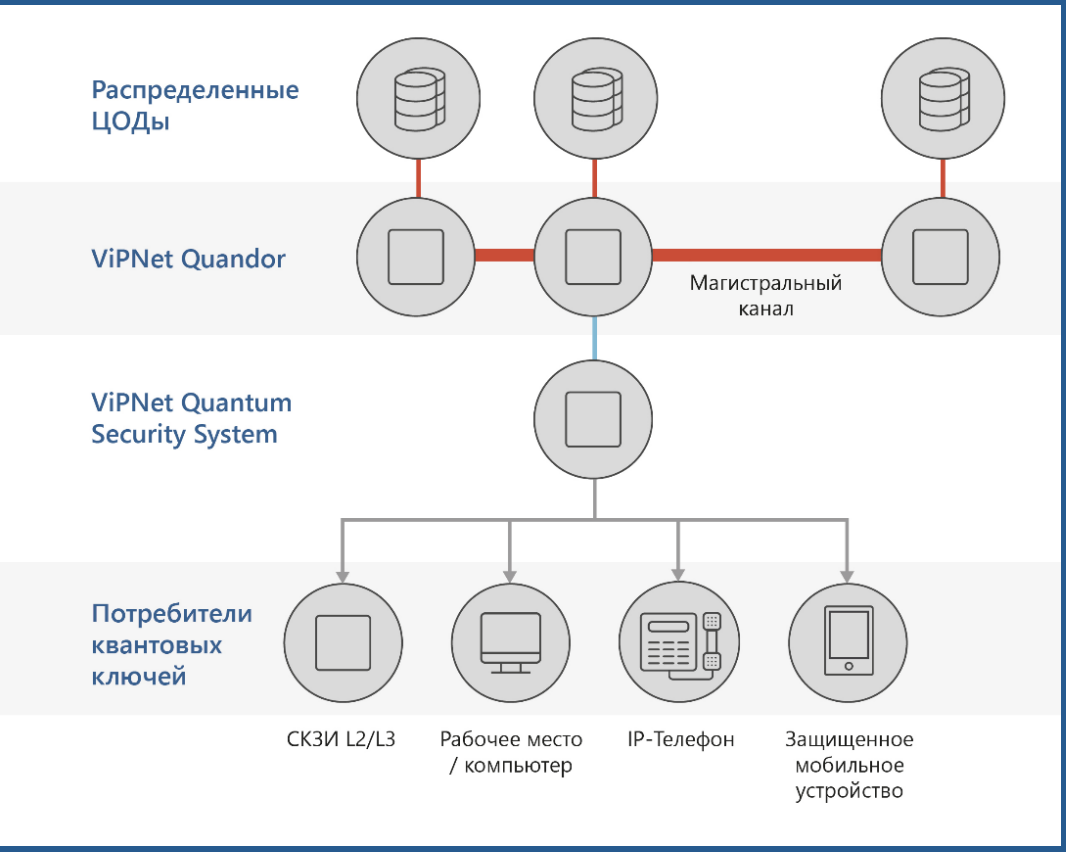
Топология сетей с технологией КРК



infotecs

Квантовые продукты ИнфоТеКС

Концепция развития технологии квантового распределения ключей в компании



- Квантовая сеть произвольной топологии
- Все ключи с гарантией секретности
- Не используется ни одного асимметричного криптографического механизма
- Ключи защищены от компрометации администратором сети
- Компрометация возможна только в период развертывания системы
- Автоматическая смена ключей шифрования 1 раз в минуту

Первые промышленные образцы

ViPNet Quantum Security System

ViPNet Quandor

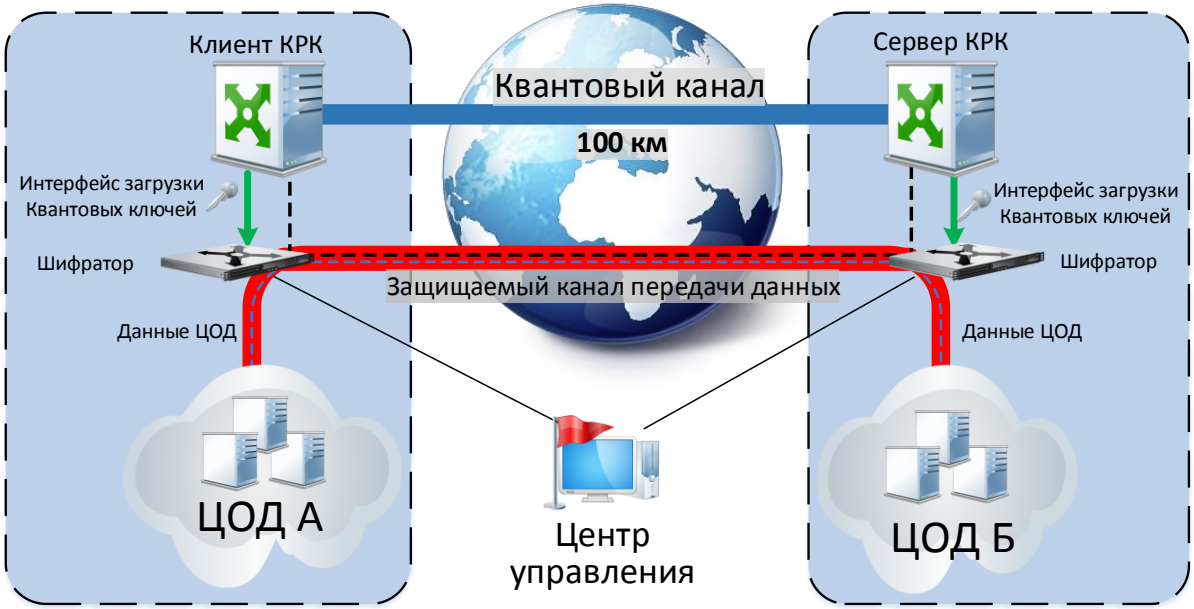
ViPNet QSS Phone

ViPNet QSS Server

ViPNet QSS Point

ViPNet QSS Switch

ViPNet Quandor



ViPNet Quandor

Комплекс квантово-криптографической аппаратуры защиты информации, состоящий из высокоскоростного шифратора канального уровня (L2) и оборудования квантового распределения ключей (КРК)

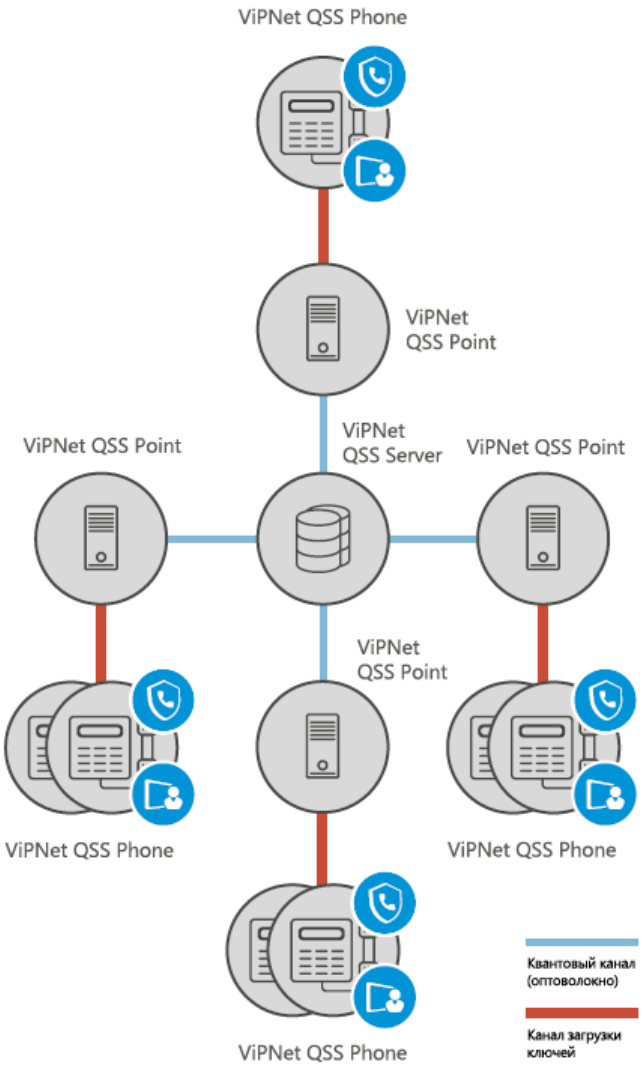
Стенд ViPNet Quandor в ИнфоТеКС

ТТХ решения ViPNet Quandor

- Длина квантового канала одного звена сети (СКРК-ККРК) до 100 км
- Скорость шифрования и имитозащиты 20 Гбит/с дуплекс
- Задержка не более 15 мкс
- Воздушное охлаждение
- Гибридная ключевая система на квантовых и предраспределённых ключах
- Скорость генерации КК – 1 ключ/мин.
- ФДСЧ на квантовых эффектах
- СКЗИ класса КС3 (КВ)

ТЗ согласовано с 8 центром ФСБ России


infotecs
ViPNet QSS



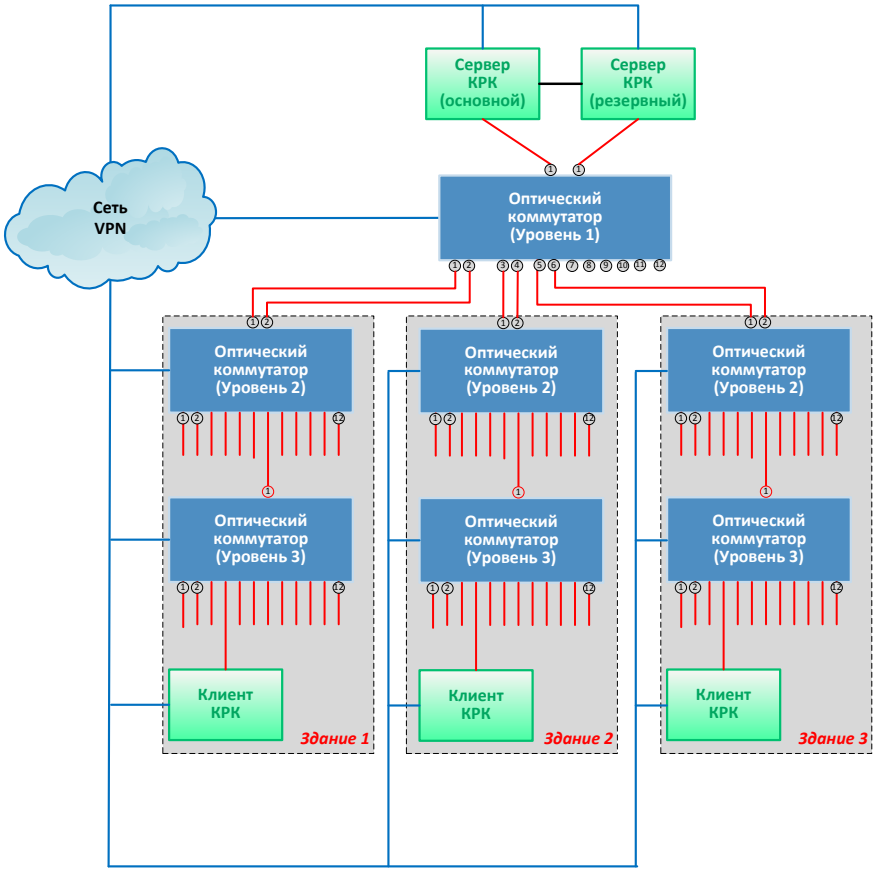
ViPNet VPN

ViPNet Client ViPNet Connect

infotecs

ViPNet Quantum Security System

Квантовая криптографическая система выработки и распределения ключей (ККС ВРК) сопряженная IP-телефонами

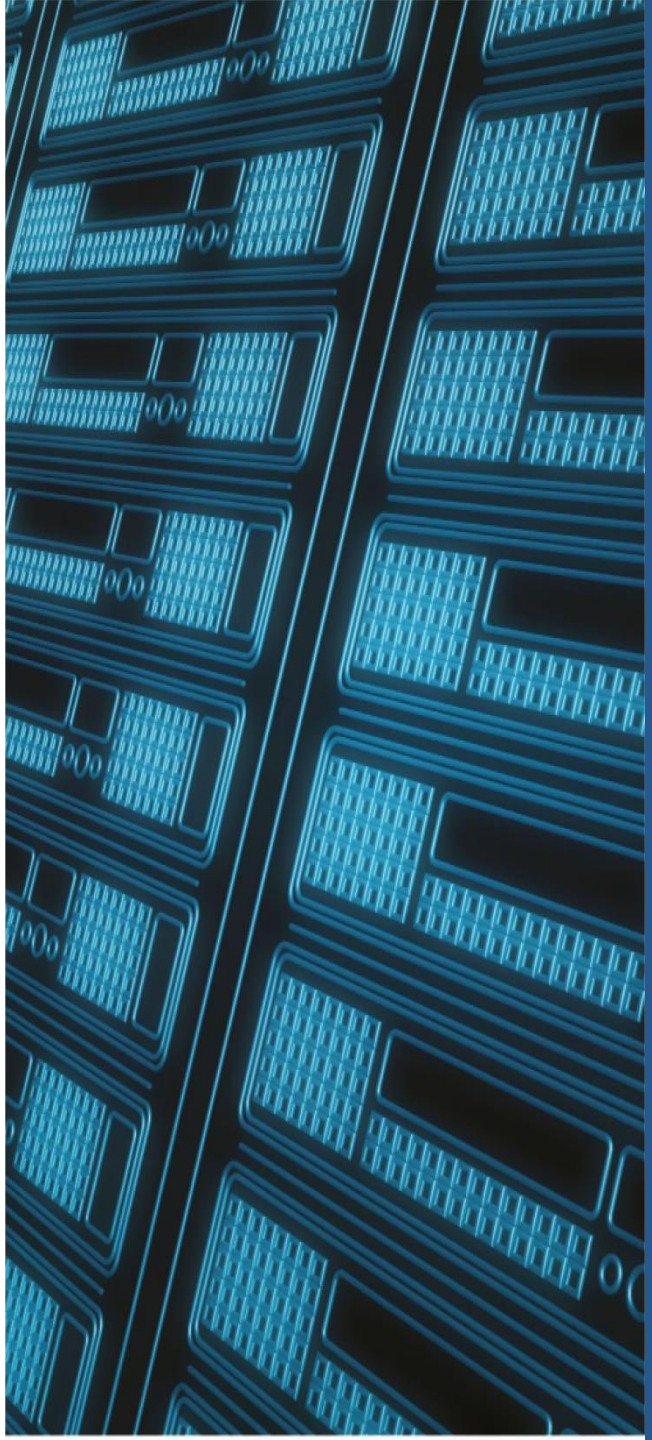


Иерархическая квантовая сеть

Стенд в ИнфоТеКС

ТТХ решения ViPNet QSS

- Расстояние СКРК-ККРК до 44 км
- 3 уровня оптической коммутации с резервированием каналов
- До 860 Клиентов КРК
- 1 Клиент – N Абонентов (в пределах КЗ)



- Сервер и Клиент КРК – КС3 (КВ)
- Абонент КРК (Android) – КС1
- Абонент КРК (Windows) – КС3
- Абонент КРК (Linux) – КВ

ТЗ согласовано с 8 центром ФСБ России

Особенности

- Не содержит ни одного асимметричного криптографического механизма
- Имеет 2 ключевые системы и обеспечивает защиту от компрометации ключей администраторами
- Скомпрометировать систему можно только путем одновременного подкупа двух администраторов (ViPNet и КРК) в период развертывания системы!

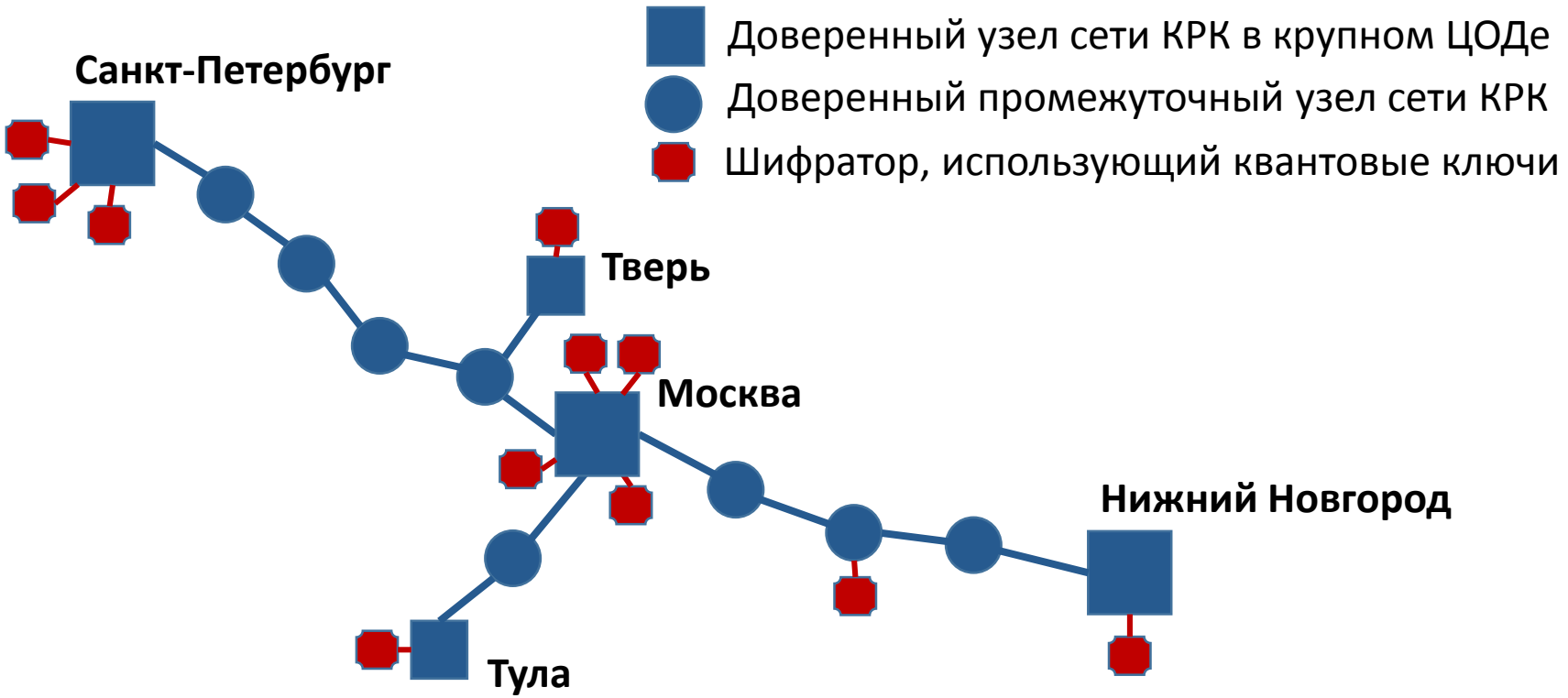
Особенности некоторых ТТХ ККС ВРК

- Скорость генерации секретного ключа:
  - топология и состав сети
  - скорость шифрования
  - МУиН
  - класс СКЗИ
- Топология КРК:
  - протокол КРК – всегда «точка-точка»
- Протокол КРК:
  - доказательство секретности
- QBER (ошибки):
  - разные протоколы КРК
  - разные ЛФД и т.д
- Поддержка стороннего СКЗИ:
  - РГ ККС ВРК в ТК 26 – разработка «ПЛИВ»
- Стоимость:
  - комплект ККС ВРК ~200 000$

Перспективы развития технологии квантового распределения ключей

- Сертификация систем КРК
- Разработка методических рекомендаций по интеграции СКЗИ и систем КРК (ТК-26)
- Построение распределенных сетей КРК на основе концепции доверенных промежуточных узлов
- Улучшение эксплуатационных характеристик

Мультисервисные сети квантового распределения ключей



Спасибо за внимание!

infotecs

Александр Поздняков
Менеджер продуктов
Aleksandr.Pozdnyakov@infotecs.ru