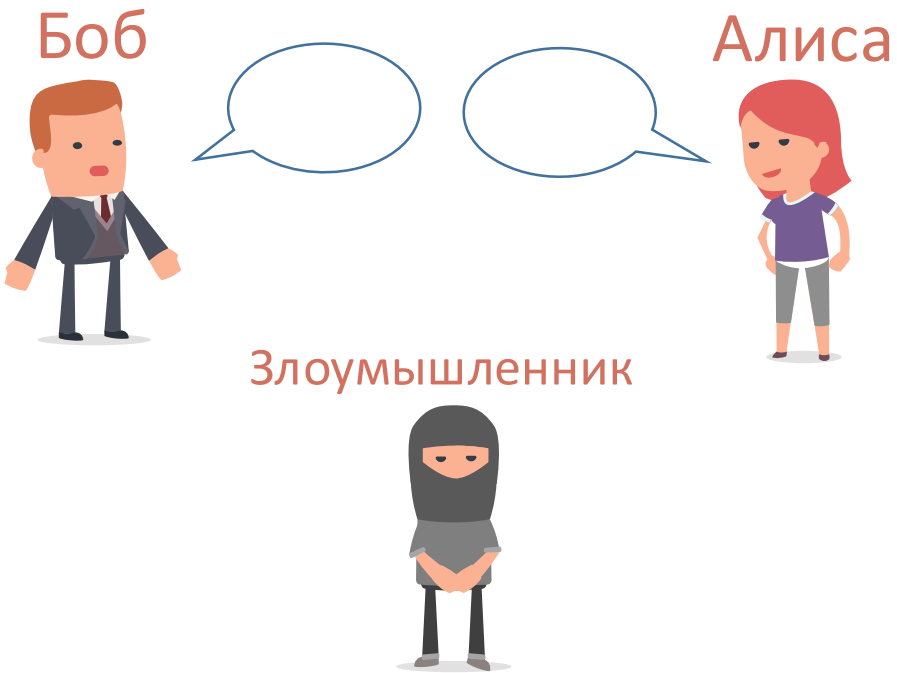
Обзор продуктов квантового направления

Александр Поздняков

Приз за Лучший вопрос

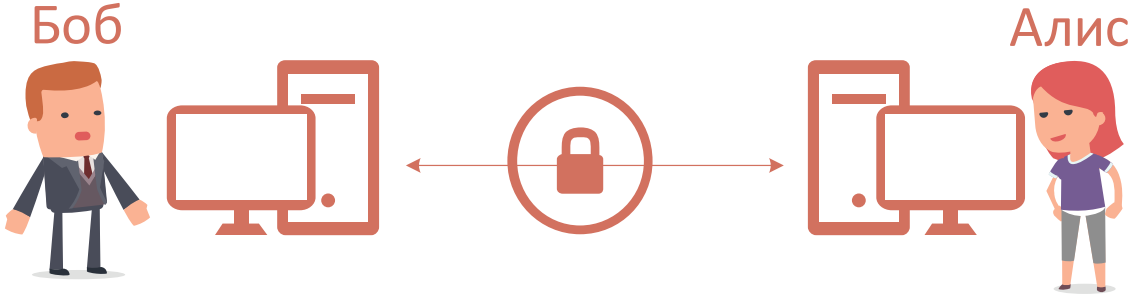
Карманный набор отверток

Квантовые технологии в информационной безопасности



Основные действующие лица

- Легитимные участники информационного взаимодействия
- Потенциальный злоумышленник



Криптографическая защита информации

- Для защиты информации часто применяются криптографические способы
- Легитимные участники используют Средства Криптографической защиты Информации (СКЗИ)
- СКЗИ – специальные вычислительные устройства, выполненные с соблюдением требований ФСБ России
- Согласование ТЗ, проведение ТИ, Сертификация ФСБ

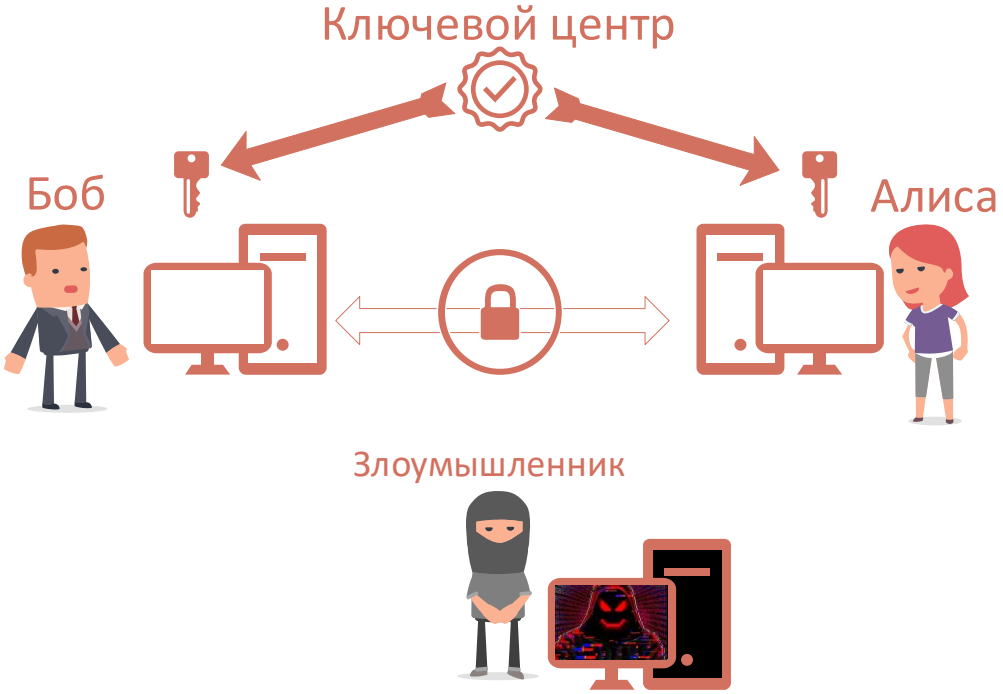
Основа криптостойкости

Базовый принцип проектирования средств криптографической защиты информации:

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

Остается главный вопрос:

Откуда взять ключ?



Доставка ключей

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

или

- Ключи **вычисляют** при условии двусторонней аутентификации (ассиметричные алгоритмы)

Особенности всех классических механизмов распределения ключей

- Достаточно дорогостоящие организационно-технические меры, причем, чем больше людей, участвующих в процессе, тем сложнее обеспечить секретность
- **Не обеспечивается** доказуемая секретность ключей. Доверие к ключам основано лишь на предположении, что у злоумышленника нет достаточного количества вычислительных ресурсов и предположении о том, что злоумышленнику не известен эффективный алгоритм взлома. (**Доказать**, что такого алгоритма нет, **невозможно**)
- Большое влияние «человеческого фактора»
- Создание квантового компьютера приведет к компрометации всех ассиметричных криптографических алгоритмов и протоколов на их основе (DH, RSA, ECDSA TLS/SSL, HTTPS, IPsec, X.509) и снижению стойкости симметричных протоколов
- Не обеспечивают быструю смену ключей автоматически, без участия администратора

Квантовая криптографическая система выработки и распределения ключей (ККС ВРК) – еще один способ доставки ключей

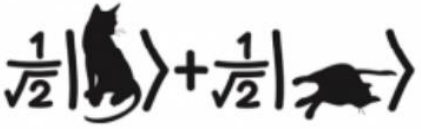
СКЗИ с использованием технологии КРК. В сем суть?

Преимущества технологии квантового распределения ключей

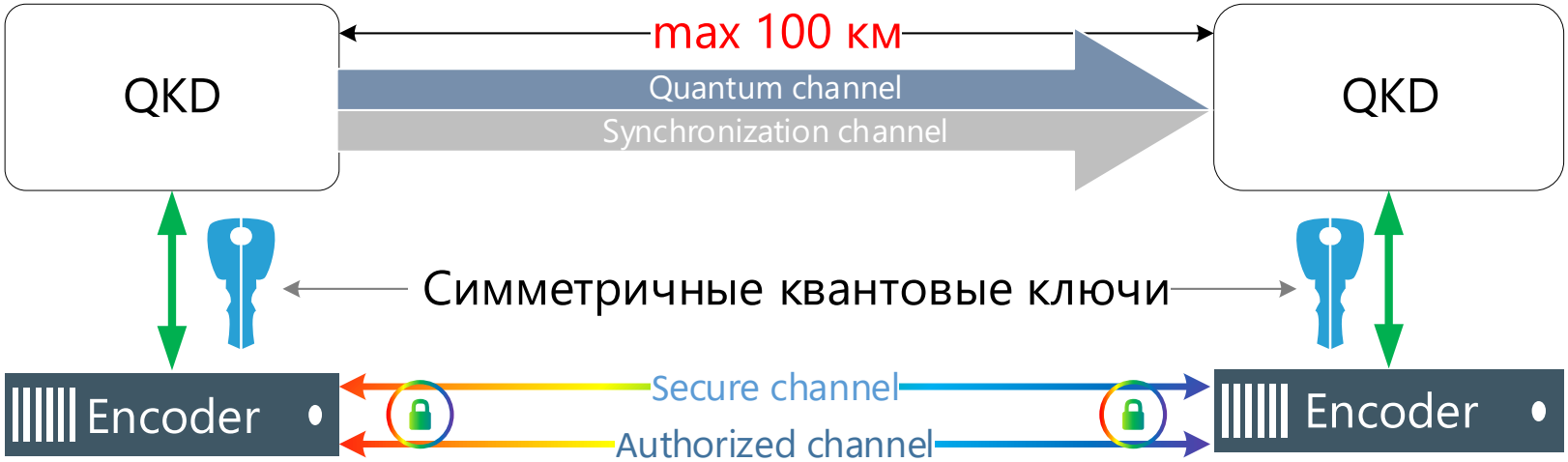
1. Безусловная **секретность** квантовых ключей **доказанная** математически
2. Выработка ключей и загрузка в СКЗИ происходит автоматически – **без** участия администратора
3. Обеспечивается стойкость к криптографическим атакам при помощи квантового компьютера
4. Высокая скорость смены ключей позволяет на практике достичь высокой степени защиты от чтения вперед и защиты от чтения назад.

Секретность выработки квантовых ключей основана на следующих принципах:

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



Базовые элементы квантовой криптографической системы



Жизненный цикл квантовых ключей

I

Настройка квантового канала

Создание и передача квантовых состояний

Измерение квантовых состояний

SQKD

CQKD

II

Процедуры выработки секретной согласованной последовательности и процедуры усиления секретности

III

Управление квантовыми ключами

Manager QKD

IV

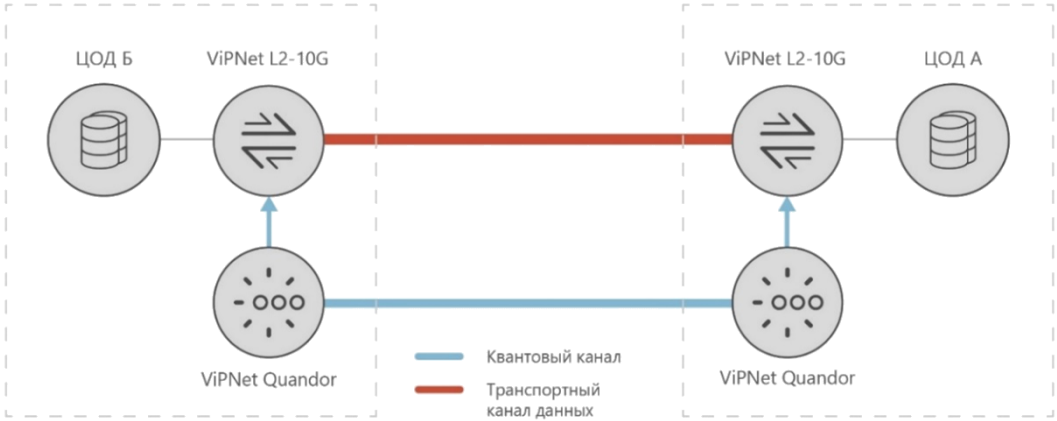
Защищенное взаимодействие с использованием квантовых ключей

ViPNet Quandor

Комплекс автоматической доверенной доставки криптографических ключей

Комплекс автоматической доверенной доставки криптографических ключей

Совместный проект АО ИнфоТеКС
и МГУ им. М.В. Ломоносова

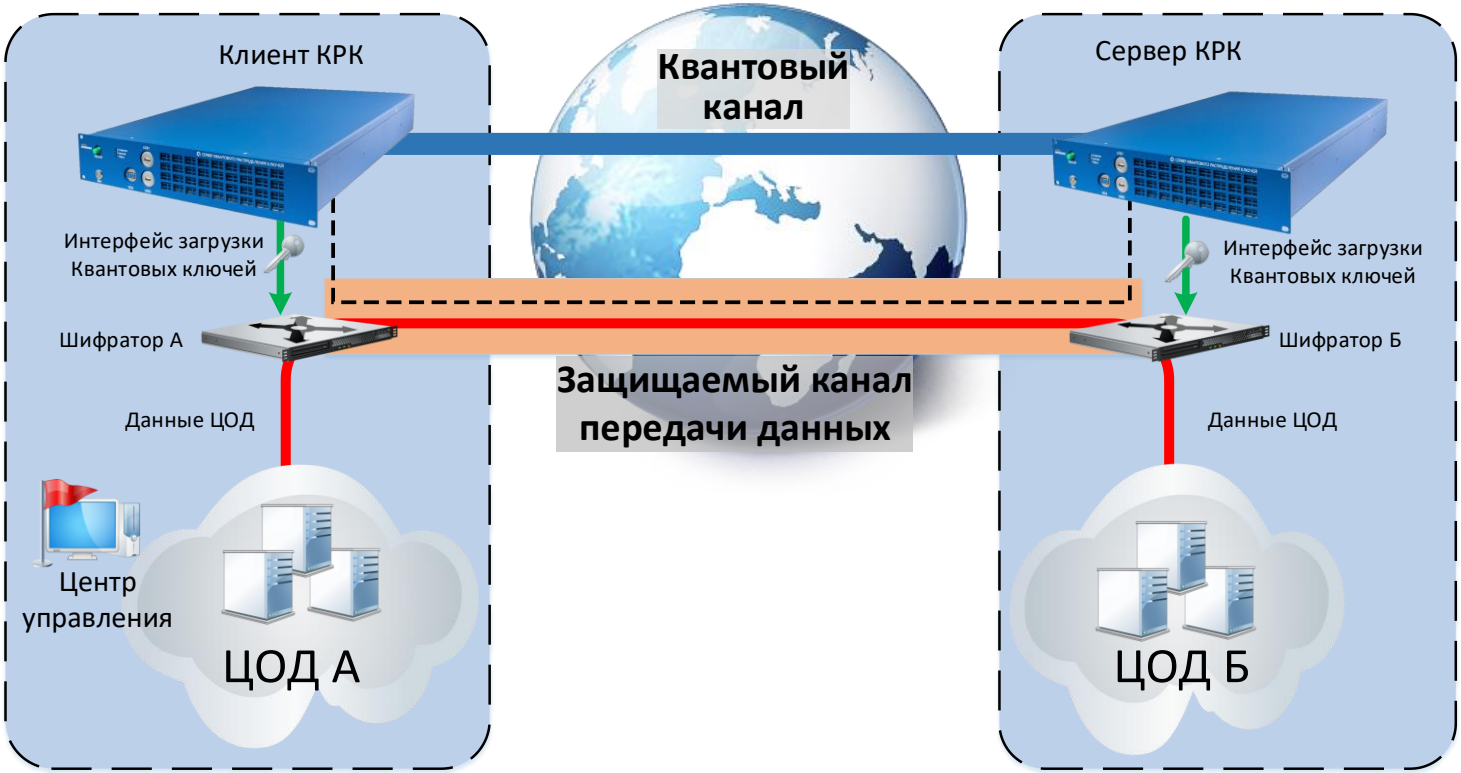


ViPNet Quandor

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

Каналы данных

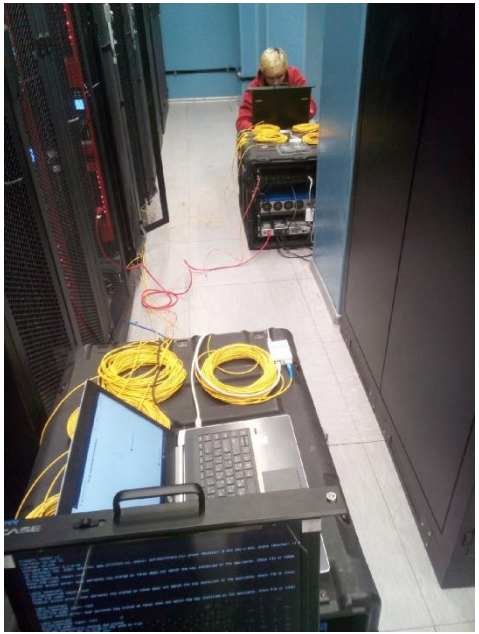


Особенности решения ViPNet Quandor

- Длина квантового канала 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
- Математически доказанная стойкость протокола КРК

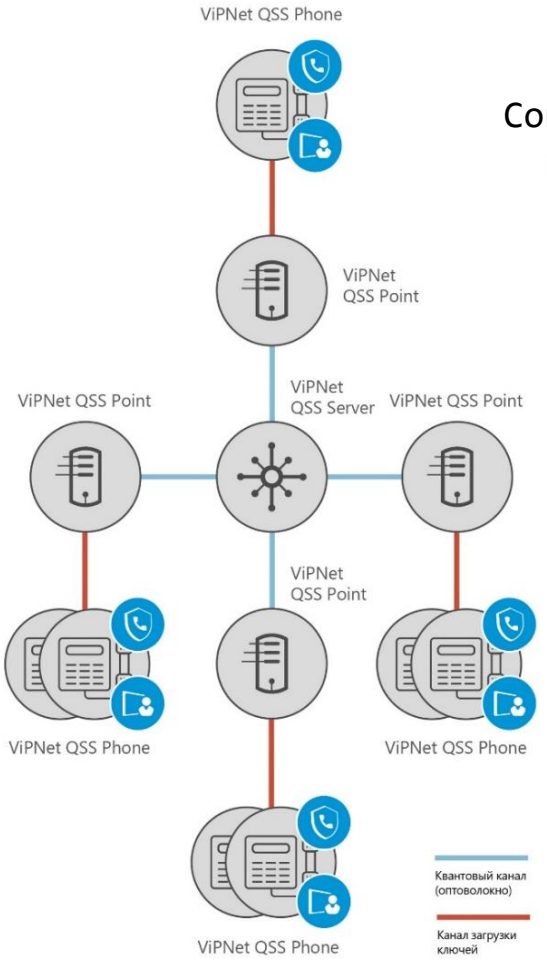
Завершены тематические исследования.
Проводится экспертиза 8 центром ФСБ России

Защита городской инфраструктуры СПБ (НИР). Испытания на в боевых условиях



Для Санкт-Петербургского информационно-аналитического центра, подведомственного Комитету по информатизации и связи Санкт-Петербурга, успешно выполнена НИР «Исследование характеристик комплекса квантово-криптографической аппаратуры защиты информации в инфраструктуре городской волоконно-оптической сети передачи данных».

ViPNet
Quantum Security System



Совместный проект АО ИнфоТеКС
и МГУ им. М.В. Ломоносова

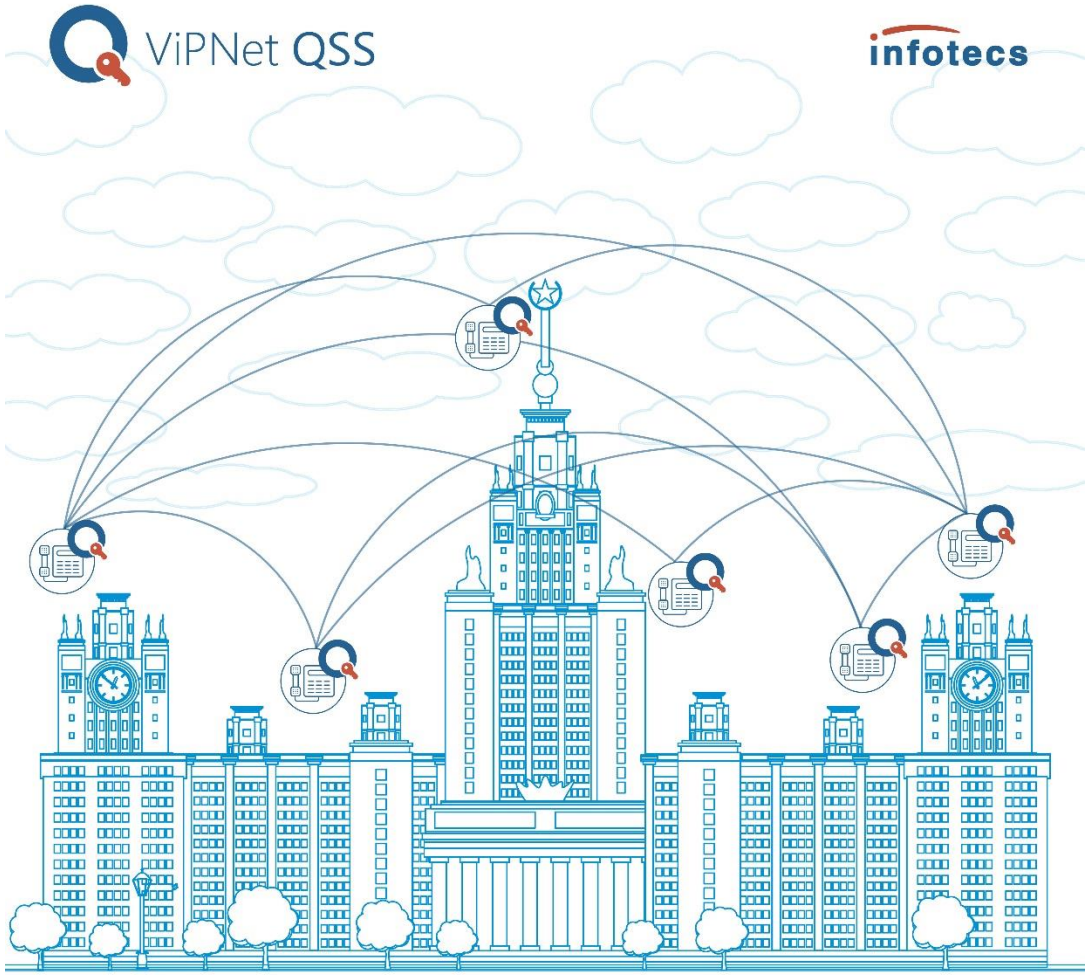
Особенности ViPNet QSS

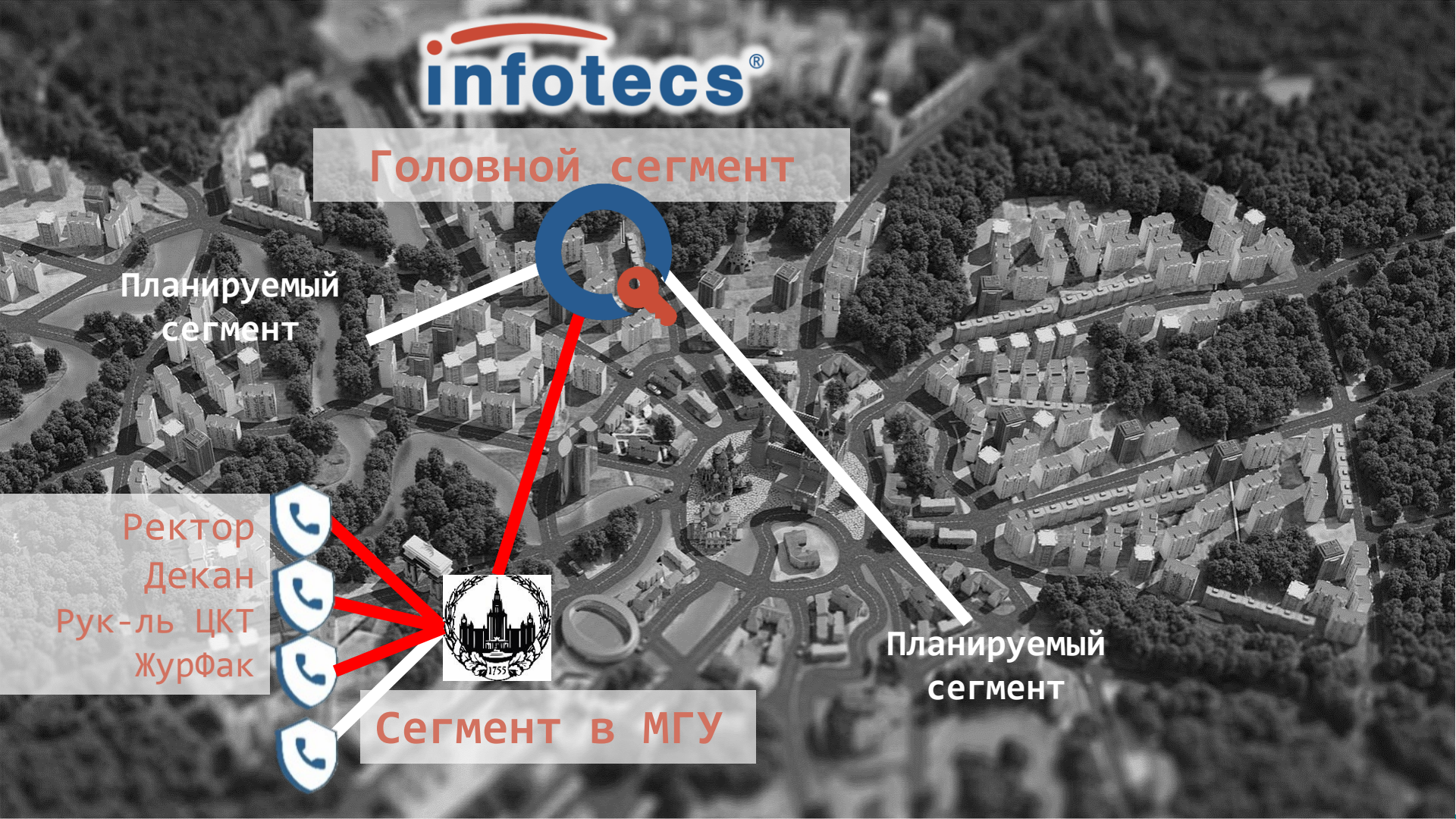
- Распределяет квантовые ключи по сетевой топологии «Звезда» для практически неограниченного количества абонентов
- Не подвержен атакам, которые станут возможными при реализации эффективного квантового компьютера
- Стойкость квантового протокола математически доказана
- Защита от Администратора. Шифрование на ключах, не известных даже администратору сети
- Возможность выработки на одном Клиенте квантовозащищенных ключей для нескольких абонентов
- Полностью автоматическая регулярная смена ключей шифрования

В процессе сертификации ФСБ России

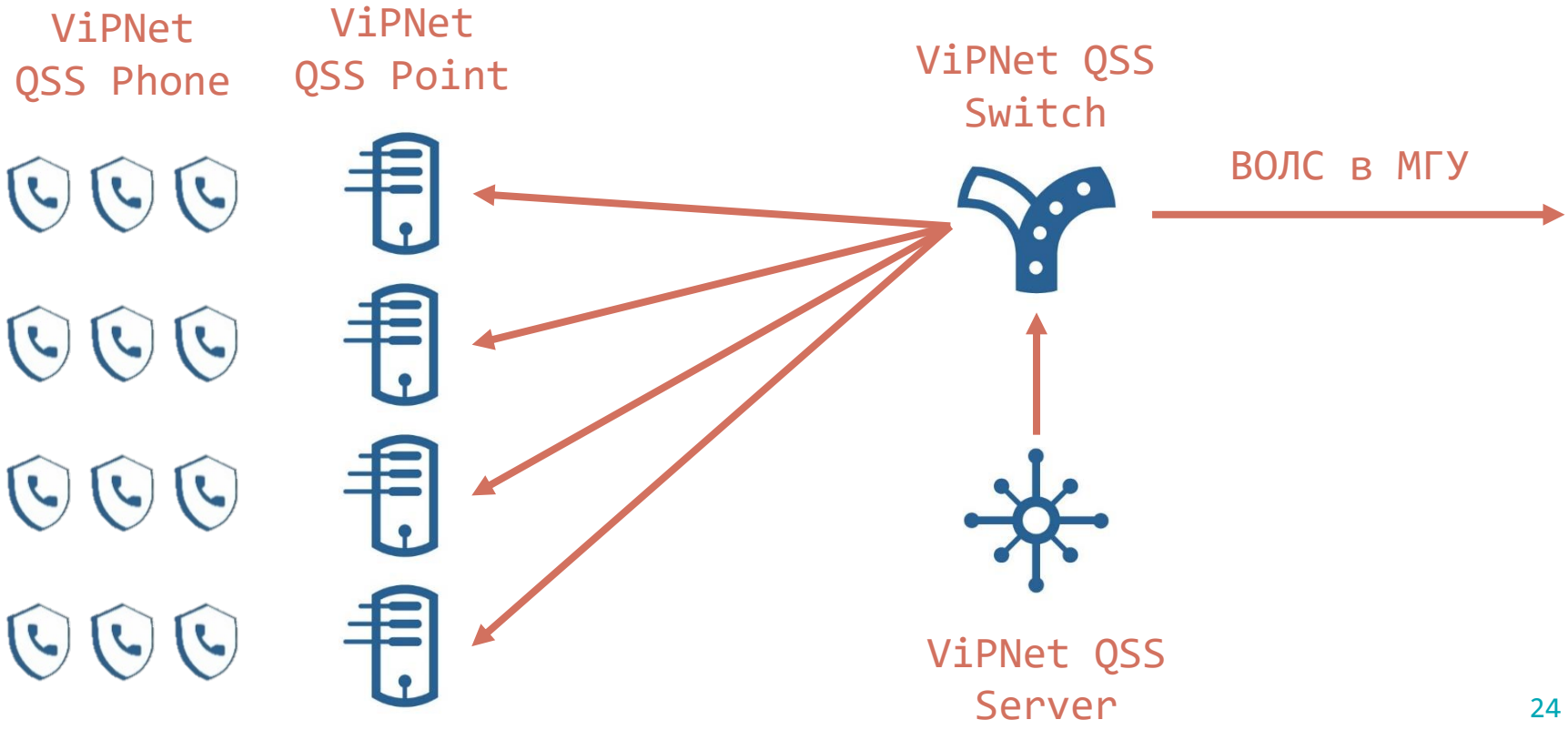
Университетская Квантовая Сеть

- В офисе ИнфоТеКС развернута сеть опытной эксплуатации
- К сети компании подключен сегмент квантовой сети МГУ
- Осуществляется автоматическая непрерывная эксплуатация «квантовых» СКЗИ




infotecs®
Головной сегмент
Планируемый сегмент
Ректор
Декан
Рук-ль ЦКТ
ЖурФак
Сегмент в МГУ
Планируемый сегмент

УКС
Сегмент ИнфоТеКС



УКС. Сегмент МГУ

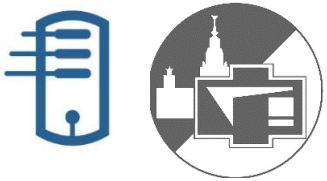
ЖурФак

ВОЛС от ИнфоТеКС

ViPNet QSS Point
ЦКТ, Кабинет руководителя

ViPNet QSS Point
Главное здание
Кабинет Ректора

ViPNet QSS Phone



ViPNet QSS Point
Здание ФизФака
Кабинет Декана

ViPNet QSS Phone

Сердце УКС
Сервер квантового распределения ключей – ViPNet QSS Server

Отечественное серийное производство ViPNet QSS Point