


Квантовое распределение ключей: настоящее и будущее средств криптографической защиты информации

Владимир Елисеев, ОАО «ИнфоТеКС»

A decorative graphic in the bottom right corner consisting of two concentric orange arcs.

Тезисы презентации



- ✓ Рассмотрены основные тенденции в сфере криптографической защиты данных, передаваемых по телекоммуникационным каналам
- ✓ Отмечены риски, связанные как с известными, так и перспективными угрозами
- ✓ Изложены основные принципы квантового распределения ключей и практических систем криптографической защиты информации на основе этой технологии
- ✓ Сделан краткий обзор мирового и российского опыта в области разработки и применения систем квантовой криптографии
- ✓ Представлены продукты компании ИнфоТеКС, построенные на основе квантового распределения ключей
- ✓ Отмечены перспективы применения систем квантового распределения ключей в России.



Тенденции развития сетей связи и угрозы информационной безопасности

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

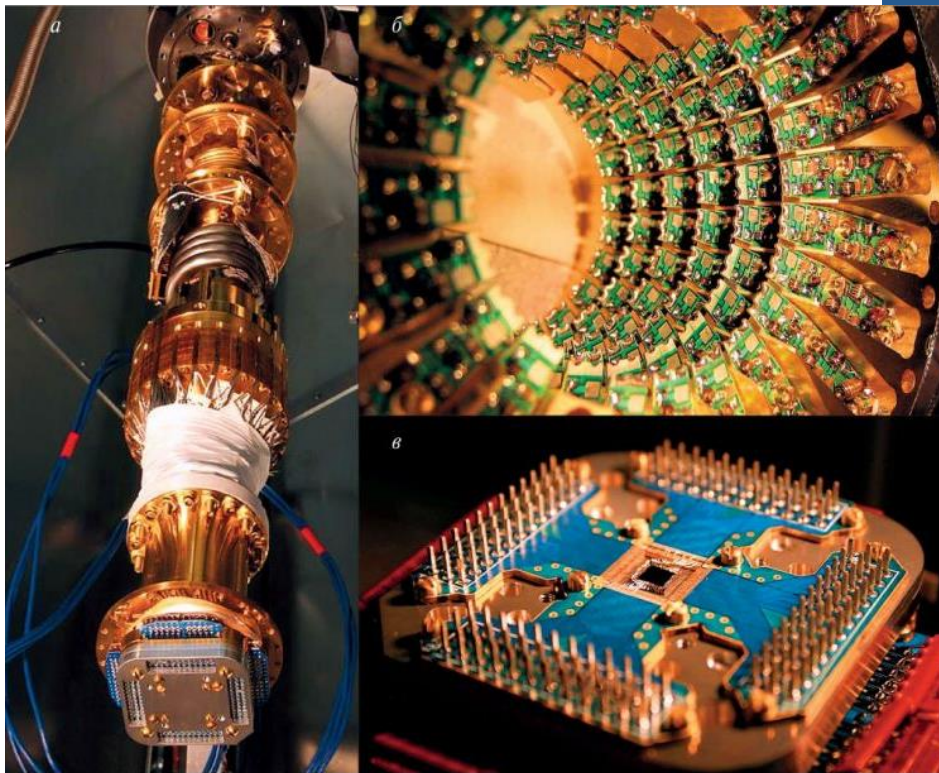
“Store now – decrypt later!”

 ethereum
golem



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 асимметричных 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)

Откуда брать секретные ключи?

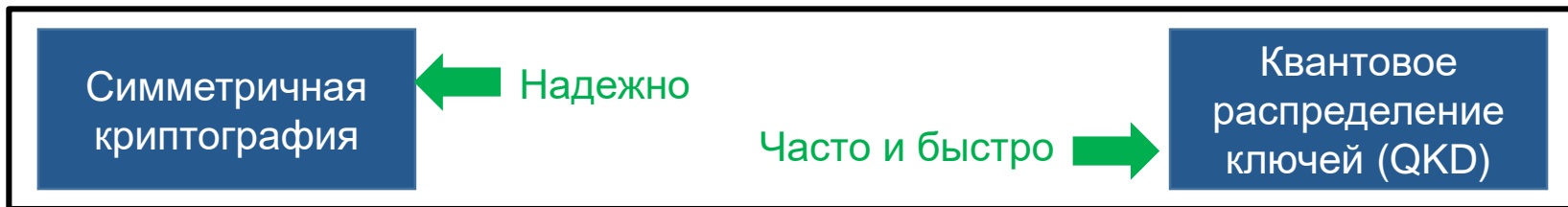
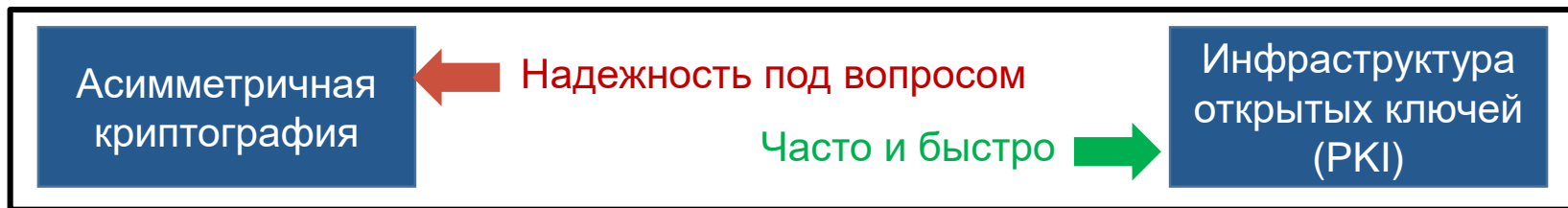
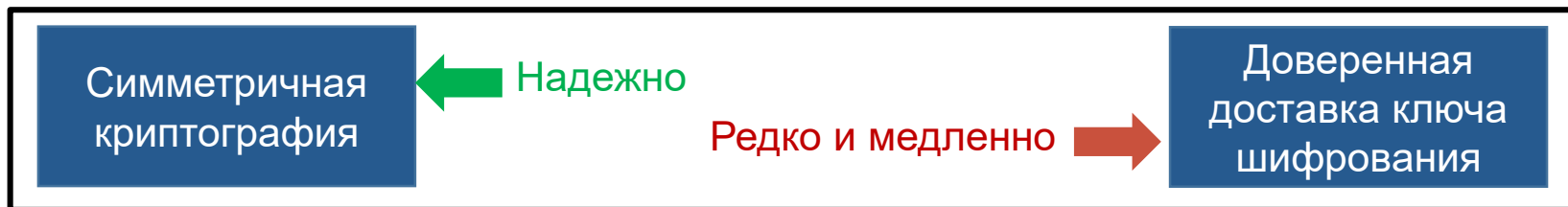
- ✓ Доверенный курьер **доставляет ключи** Алисе и Бобу из ключевого центра

или

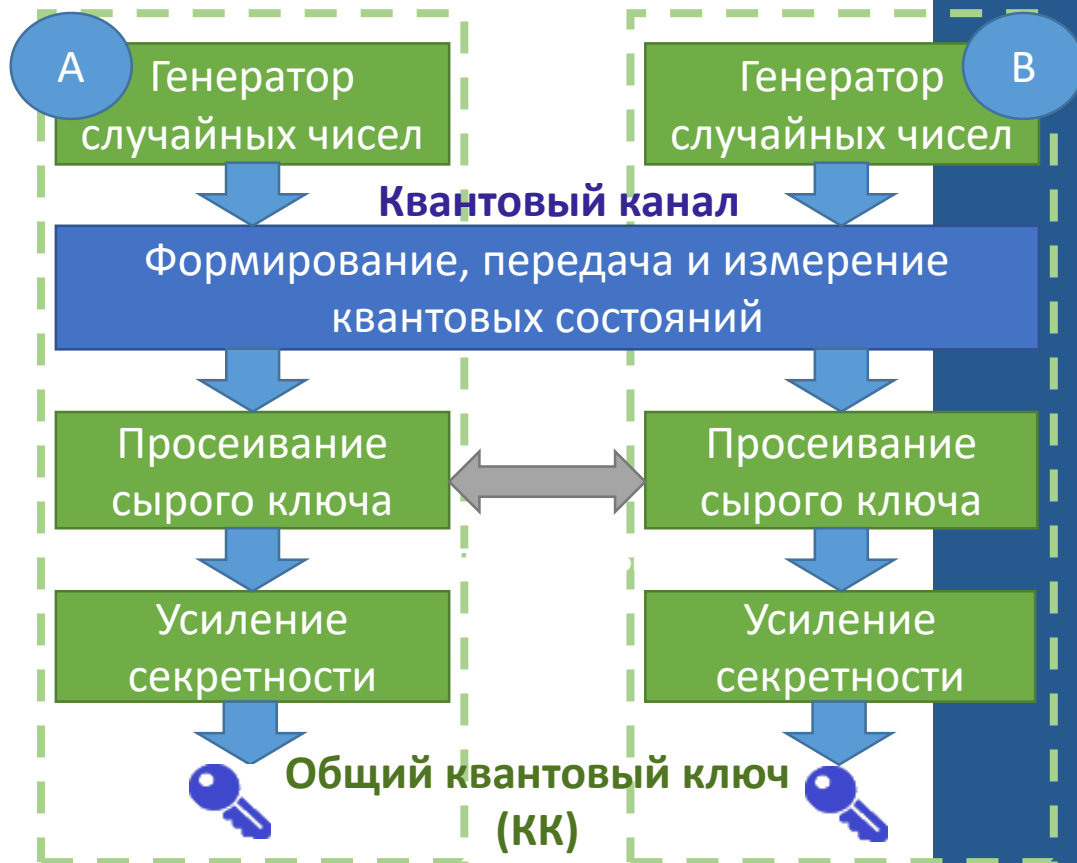
- ✓ Алиса и Боб **вычисляют ключ** при условии двусторонней аутентификации (DH)



Подходы к выработке общего секретного ключа



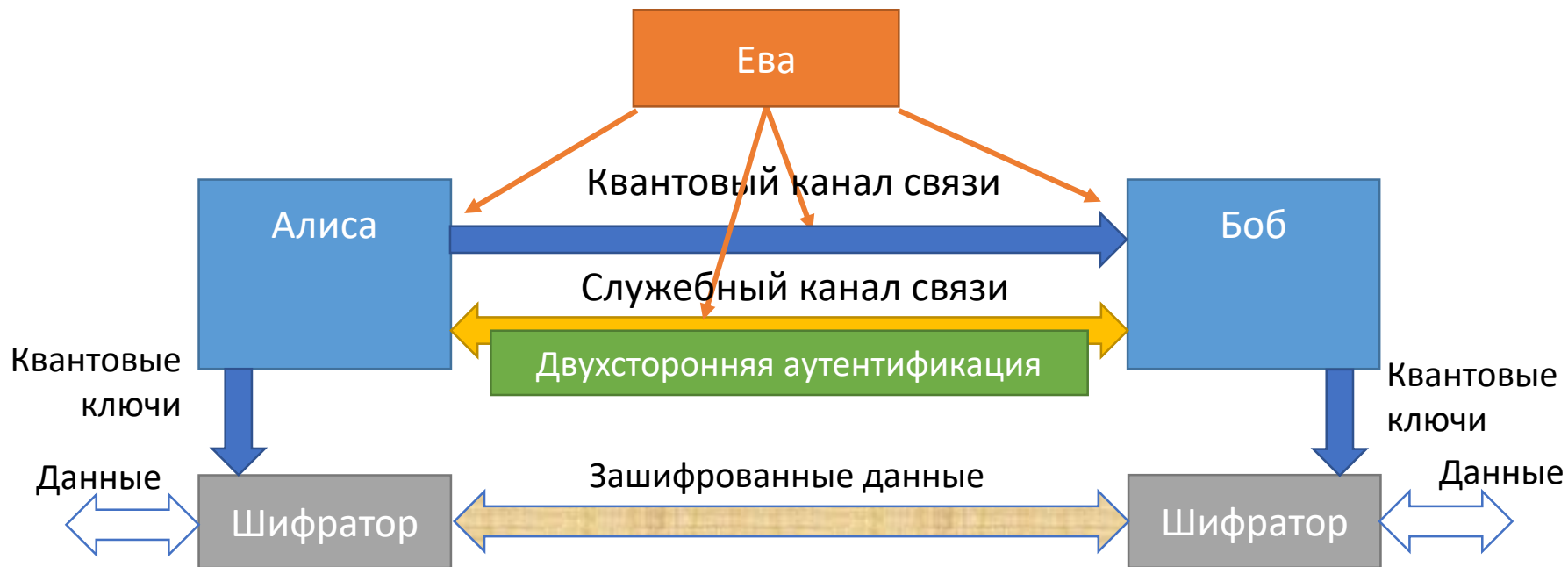
Принципы квантового
распределения
ключей для
практических систем
криптографической
защиты информации



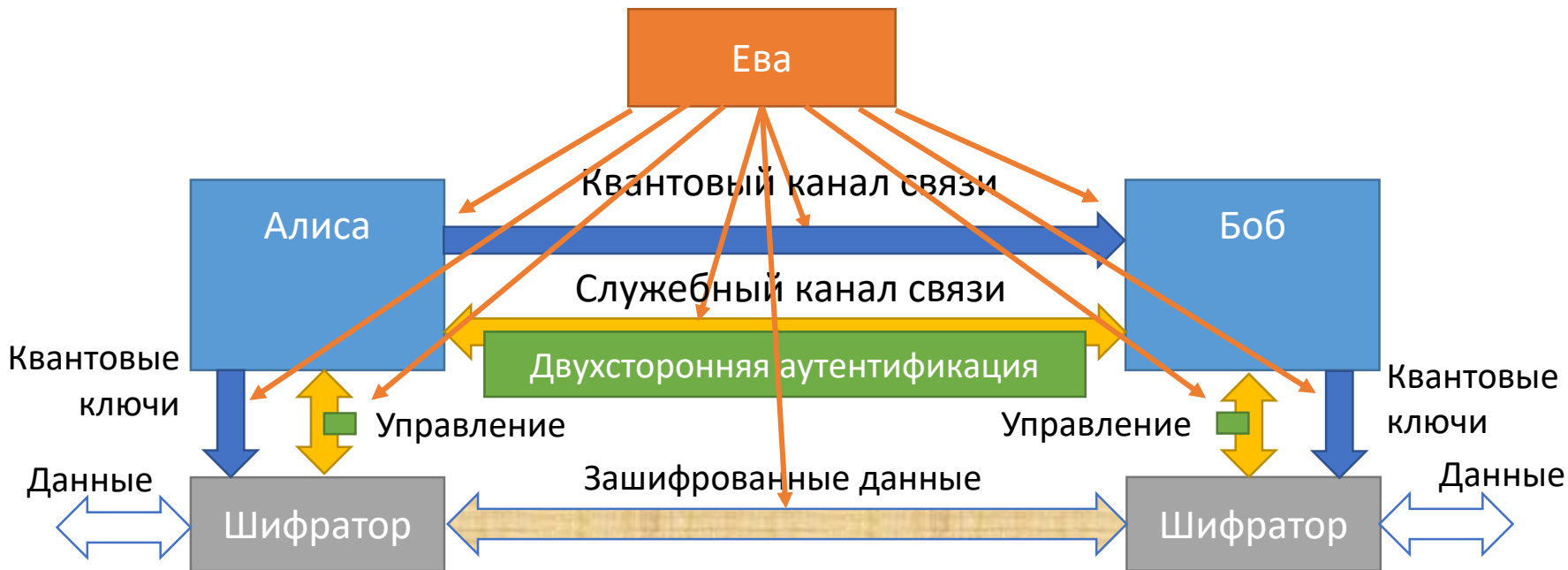
Обобщенный алгоритм квантового распределения ключей

- ✓ Передача информации производится с помощью квантовых состояний, обычно кодируемых на фотонах
- ✓ Определение совпадающих битов в независимых случайных последовательностях даёт сырой ключ
- ✓ Секретность обеспечивается за счет учёта уровня ошибок в квантовом канале
- ✓ Служебный канал аутентифицируется
- ✓ Квантовый ключ распределяется на концах квантового канала

Система квантового распределения ключей с точки зрения ученых



Система квантового распределения ключей для защиты информации



Необходимо рассмотреть весь комплекс вопросов защиты информации!

Квантовая криптография

Современный уровень развития технологии квантового распределения ключей позволяет переходить к практическому внедрению, но при условии, что обеспечиваются:

- ✓ Доказуемая стойкость квантового протокола
- ✓ Аппаратные методы генерации случайных чисел
- ✓ Системный подход к защите информации
- ✓ Передовые технологии шифрования

Квантовая
криптография



Секретность в
классической
криптографии



Квантовое
распределение
ключей (QKD)

Современный уровень
развития технологий и
продуктов квантового
распределения ключей



Волоконно-оптические линии связи для квантового распределения ключей

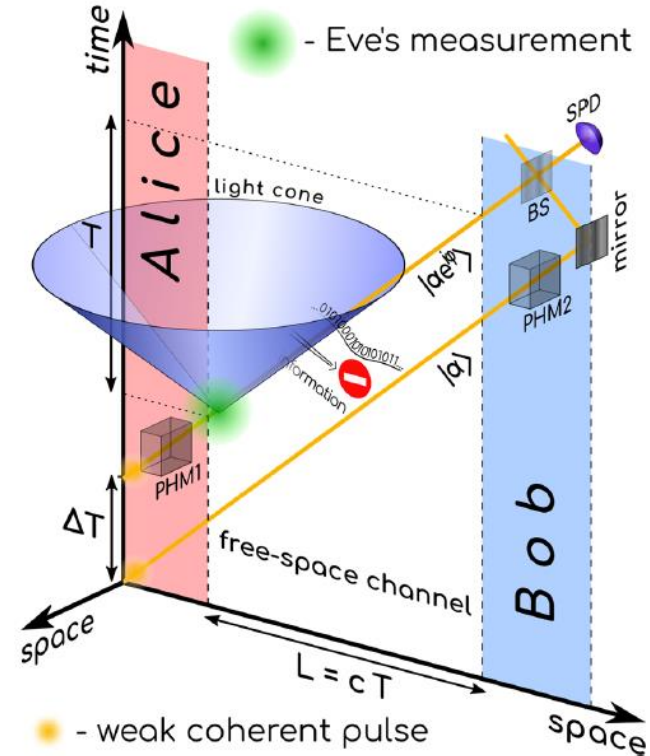


- ✓ Длины волн 1310-1550нм
- ✓ Затухание на одномодовом волокне от 0,18 дБ/км и выше
- ✓ Не сохраняет поляризацию (SM волокно)
- ✓ Недопустимо усиление оптических сигналов
- ✓ Использование спектрального уплотнения требует исследований

Атмосферные и космические перспективы

Особенности:

- Релятивистские протоколы КРК – проще обеспечить секретность, чем для ВОЛС
- Сохраняет поляризацию
- Сложно обеспечить точное наведение излучателя и приемника квантовых состояний за счет одномодового приема
- Квантовый и служебный каналы проще распределить по длине волны, чем для ВОЛС
- Приемная сторона квантового канала «орбита-поверхность» – телескоп.
- Малая производительность «орбита-поверхность» – 0,1-0,2 бит/мин



Прогресс в сфере квантового распределения ключей

- ✓ **1989** Первая экспериментальная установка КРК на расстояние 30 см
- ✓ **2004** США. DARPA 10 узлов КРК
- ✓ **2008** Евросоюз. Проект SECOQC, 5 узлов КРК, расстояния в сегментах ~25км
- ✓ **2009** Китай. Городская сеть КРК в Wuhu
- ✓ **2010** Япония. Сеть в районе Токио, 6 узлов, сегменты от 1 до 90 км
- ✓ **2014** Китай. Междугородная сеть КРК Hefei-Chaohu-Wuhu, 150 км,
- ✓ **2014** США. Проект сети КРК на всей континентальной территории США
- ✓ **2017** Китай. Сеть Пекин-Шанхай, 32 узла, магистраль на 2000 км
- ✓ **2018** Китай. Квантовое распределение ключей через спутник на 7600 км
- ✓ **2018** США. Коммерческая сеть КРК Quantum XС, Нью-Йорк – Нью-Джерси

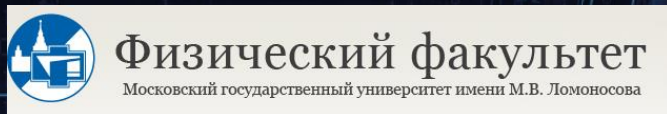
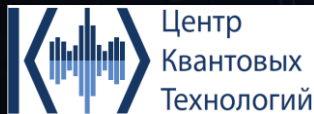


Образцы зарубежных систем квантового распределения ключей

- Использующие протоколы квантового распределения ключей не обладают доказуемой секретностью
- Отсутствуют стандартизированные протоколы взаимодействия с шифраторами

Разработки компании ИнфоТеКС и Центра квантовых технологий физического факультета МГУ имени М.В. Ломоносова

infotecs



Основные вехи:

2017

- ✓ «Квантовый телефон МГУ»
- ✓ Старт проекта ViPNet Quandor

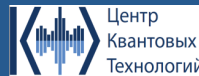
2018

- ✓ Старт проекта ViPNet QSS
- ✓ Согласовано ТЗ на ViPNet Quandor

2019

- ✓ Демонстрации ViPNet QSS и ViPNet Quandor на городской ВОЛС
- ✓ Согласовано ТЗ на ViPNet QSS

«Квантовый телефон МГУ» - опытная интеграция с ViPNet VPN



infotecs



Физический факультет
Московский государственный университет имени М.В. Ломоносова

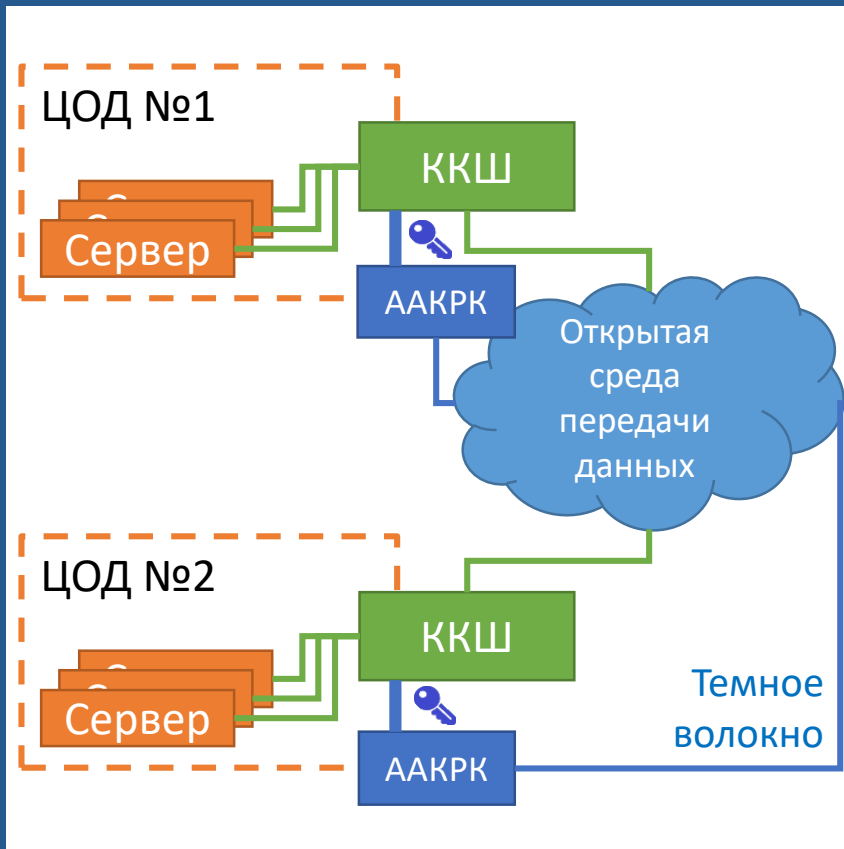




ViPNet Quandor Сценарий применения

ККШ (квантово-криптографический шифратор) – высокоскоростной шифратор канального уровня, в прозрачном для сети ЦОД режиме обеспечивающий защиту данных как на квантовых ключах, так и на классических

ААКРК (автоматическая аппаратура квантового распределения ключей) – инновационное оптоэлектронное устройство, обеспечивающее перехватываемое распределение ключей для шифраторов



ViPNet Quandor

Технические характеристики

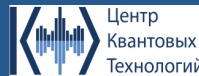


- ✓ Длина ВОЛС – до 100 км
- ✓ Выработка квантовых ключей – не менее 256 бит/мин
- ✓ Производительность ФДСЧ – 20 Мбит/с
- ✓ Автоматический режим работы

- ✓ Защищаемый протокол – Ethernet 10GBASE
- ✓ Шифрование – по ГОСТ Р 34.12-2015
- ✓ Задержка на шифраторе – не более 15 мкс
- ✓ Скорость передачи (полудуплекс) – 10 Гбит/с
- ✓ Скорость передачи (дуплекс) – 20 Гбит/с

ViPNet Quantum Security System

Сценарий применения



infotecs



Физический факультет
Московский государственный университет имени М.В. Ломоносова

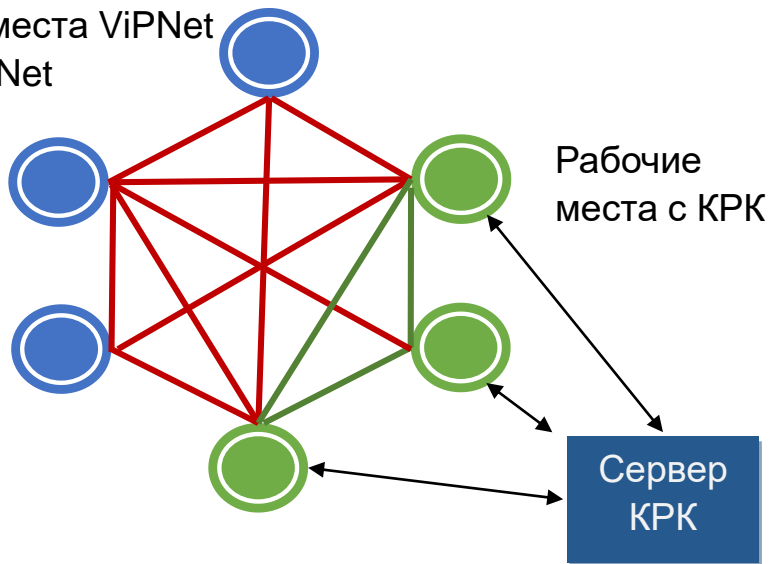
Обычные рабочие места ViPNet
и криптошлюзы ViPNet



ViPNet Client



ViPNet Connect



— Обычная защищенная сеть

— Сегмент некомпromетируемых коммуникаций

- ✓ Построение сети шифрованной связи End-to-End на основе квантовых ключей
- ✓ Гарантированный охват любого мегаполиса (Москва, Санкт-Петербург)
- ✓ Защита от компроматации администратором сети
- ✓ Бесшовная интеграция с VPN ViPNet

ViPNet Quantum Security System

Технические характеристики

Сервер КРК и коммутатор



Клиент КРК

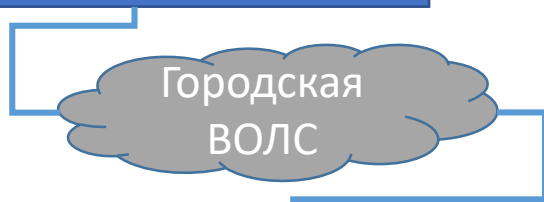


- ✓ Длина ВОЛС между сервером и клиентами КРК – 25-75 км
- ✓ Уровней коммутации – до 3-х
- ✓ Выработка квантовых ключей – не менее 256 бит/мин
- ✓ Автоматический режим работы
- ✓ Количество клиентов КРК – до 800

Офис ИнфоТеКС

Абоненты:

- Генеральный директор
- Шоу-рум
- Ведущие сотрудники



МГУ им. М.В. Ломоносова

Абоненты:

- Ректор
- Декан Физфака
- Центр Квантовых Технологий

Городская сеть ИнфоТеКС-МГУ

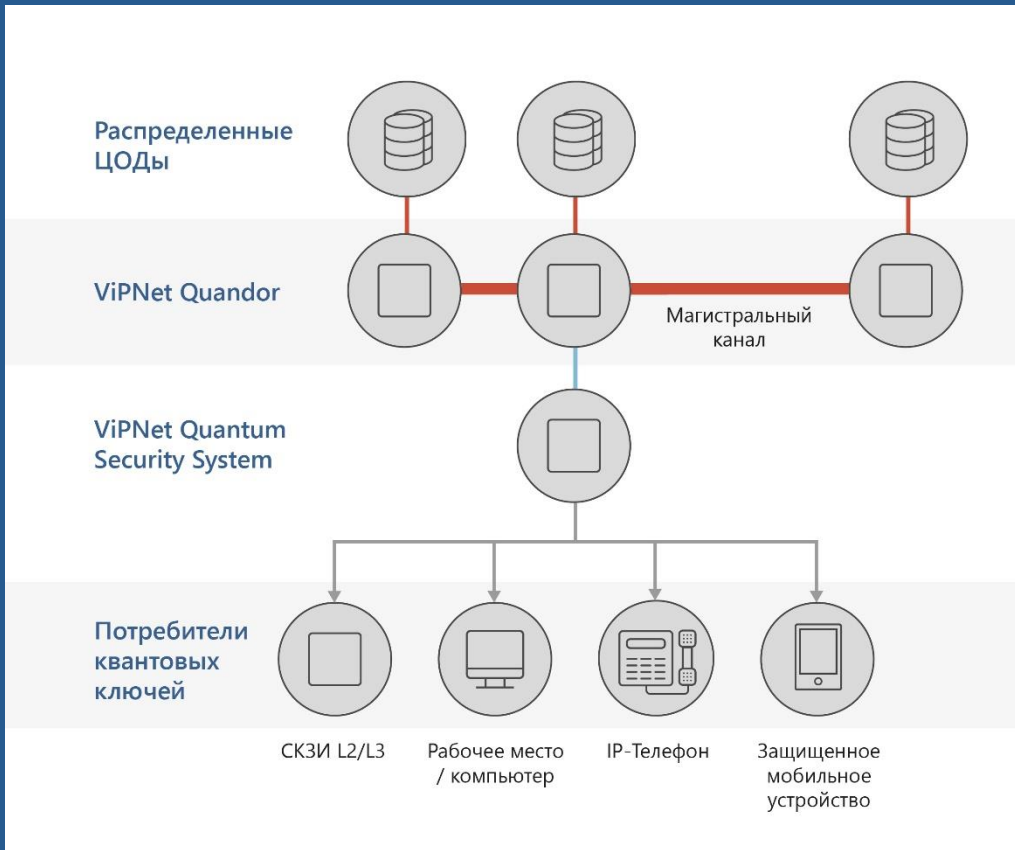
Длина (по ВОЛС) – 24,1 км

Оптические потери – 5,6 дБ

Реальная эксплуатация:

- ViPNet QSS
- ViPNet Quandor

Партнер – ЮЛком Медиа



Комплексное применение технологий КРК ViPNet

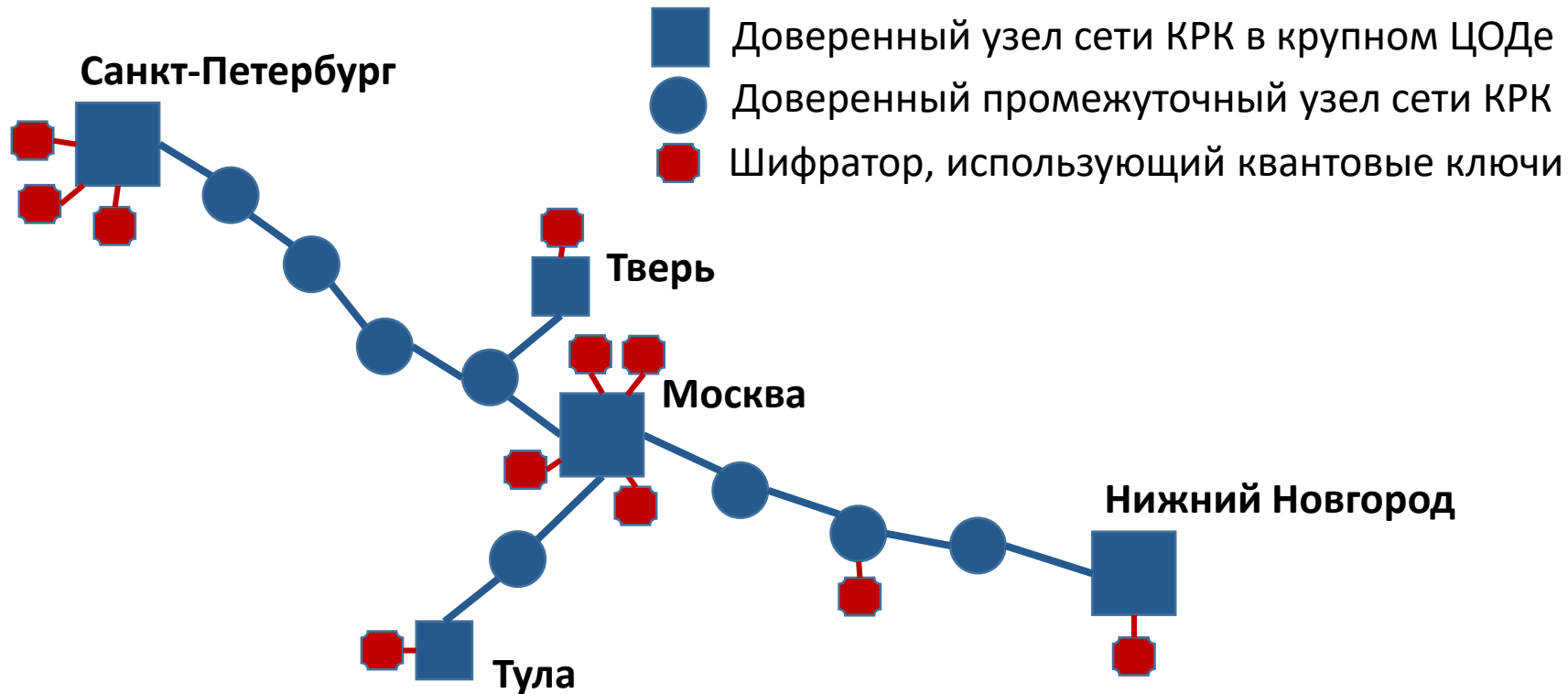
- ✓ Квантовая сеть произвольной топологии
- ✓ Секретность ключей доказана математически
- ✓ Не содержит ни одного асимметричного криптографического механизма
- ✓ Защита от компрометации ключей администратором сети
- ✓ Компрометация возможна только в период развертывания системы
- ✓ Автоматическая смена ключей шифрования, 1 раз в минуту
- ✓ СКЗИ класса КСЗ

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



The logo for 'infotecs' features a small orange dot above the letter 'i', followed by a curved orange line that arches over the letters 'f' and 'o'. The word 'infotecs' is written in a bold, white, lowercase sans-serif font.

infotecs

A vertical orange line that acts as a separator between the logo and the text.

Спасибо
за внимание!