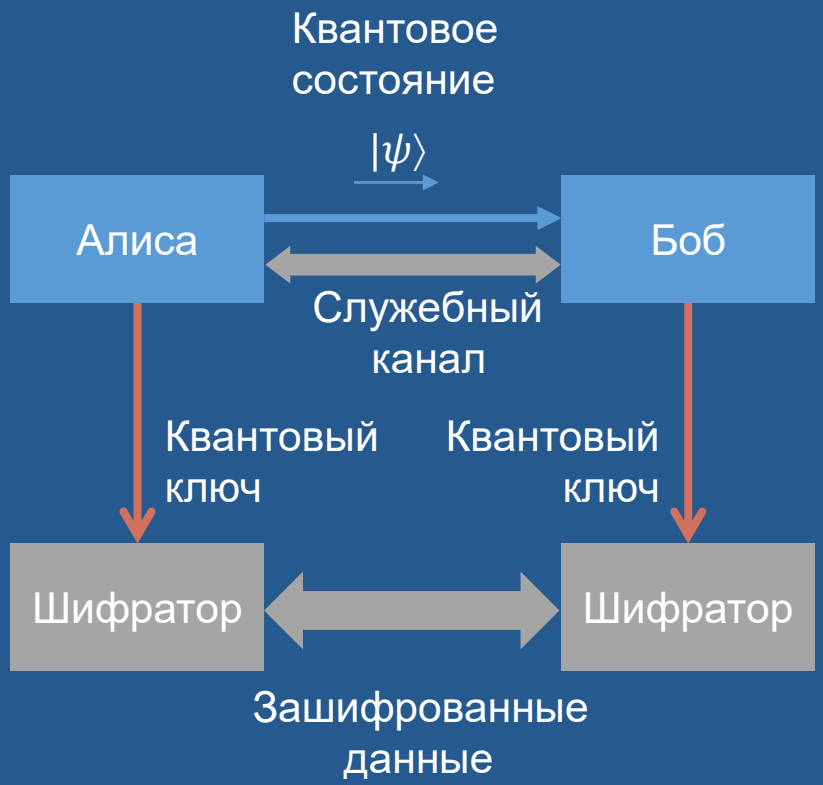
infotecs

Перспективные исследования технологии квантового распределения ключей для защиты информации

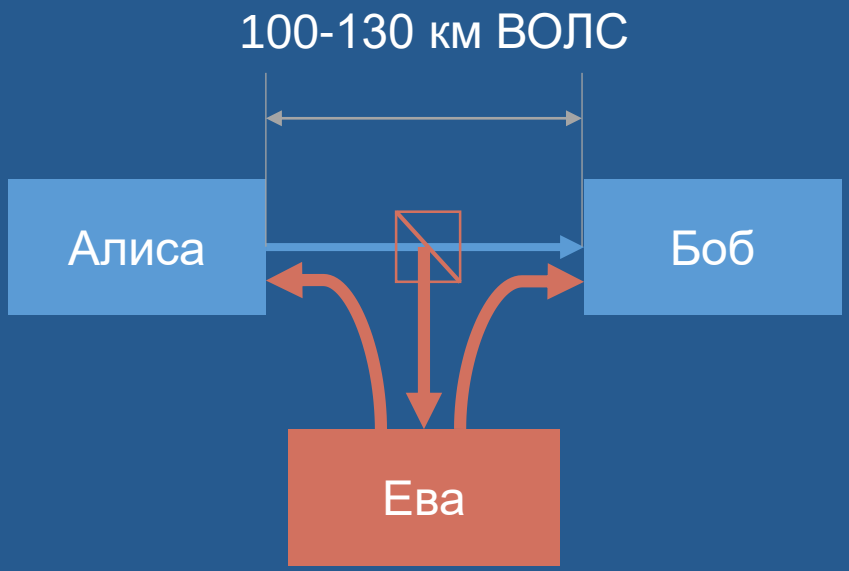
Владимир Елисеев

Что такое квантовое распределение ключей?

- Цель квантового распределения ключей (КРК) – получить общий секретный ключ у двух абонентов, не передавая его
- КРК – это квантово-механический конкурент протокола Диффи-Хеллмана
- Наиболее удобным и надежным является формирование квантовых состояний фотонов, передаваемых по оптоволокну или по открытому пространству
- Квантовое состояние получается путем задания поляризации или сдвига фазы одиночного фотона
- Квантовые состояния невозможно скопировать или усилить, поэтому их невозможно «подслушать» в традиционном смысле этого слова



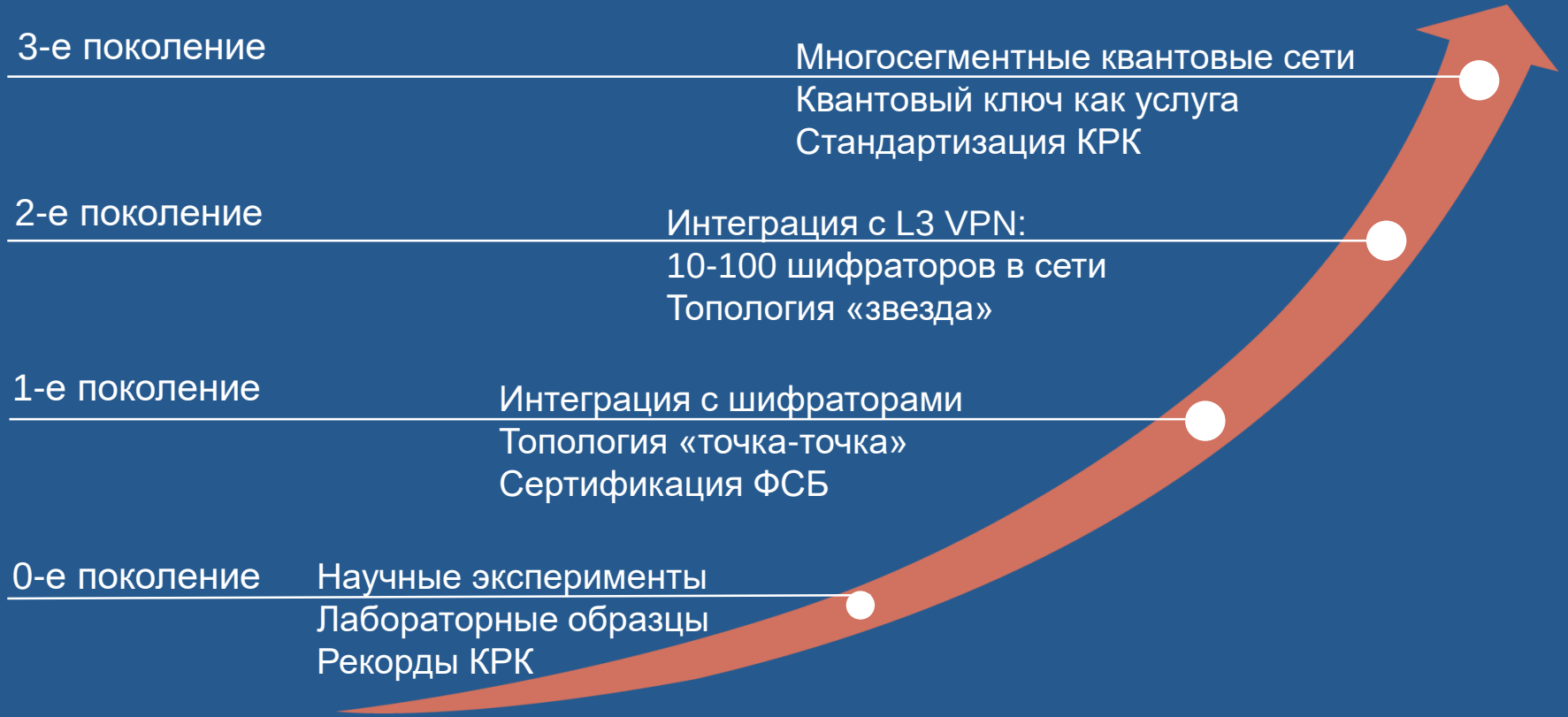
Свойства и ограничения КРК



- Принципиально топология «точка-точка» – не подходит напрямую для сети Интернет с адресацией «каждый с каждым»
- Ограничение по дальности одного сегмента ВОЛС
- Секретный квантовый ключ – только на одном сегменте ВОЛС
- КРК на околоземный спутник позволит кардинально решить вопрос ограничения расстояний
- Аппаратура КРК является частным случаем системы криптографической защиты информации (СКЗИ)
- Необходима сертификация ФСБ
- На протоколы и аппаратуру КРК тоже есть атаки, от которых необходимо защищаться

Развитие систем КРК

infotecs



Исследование точности и надежности аппаратуры КРК

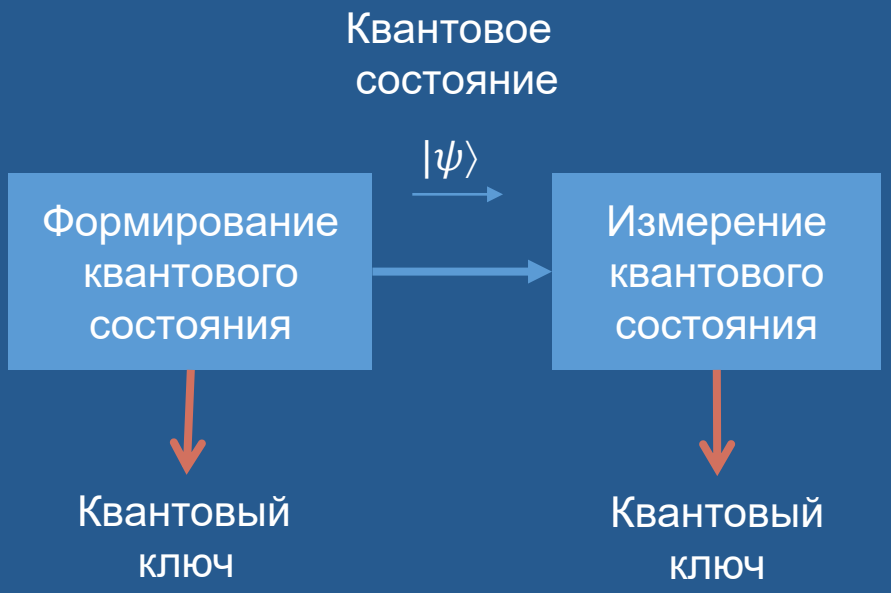
infotecs

Многие системы КРК можно представить в виде:

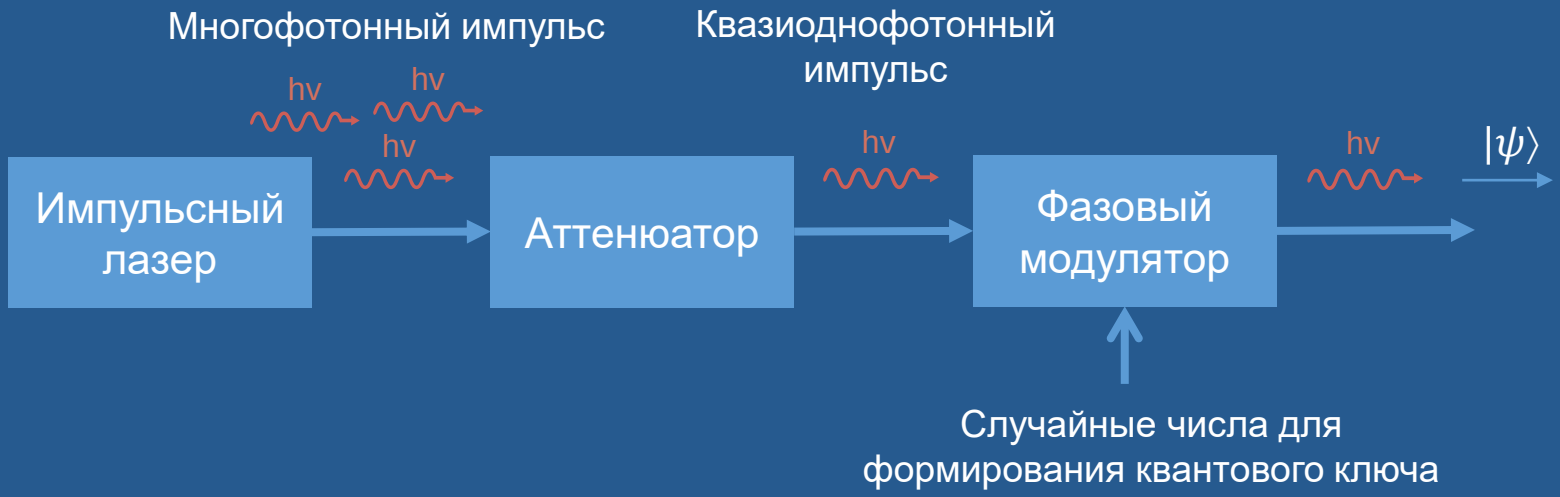
- Алиса – формирование квантового состояния
- Боб – измерение квантового состояния

Требования сертификации и эксплуатации:

- Точность реализации протокола КРК с учетом характеристик элементов
- Влияние надежности элементов на корректность и эффективность реализации протокола КРК
- Оценка реализованных мер защиты с учетом характеристик элементов

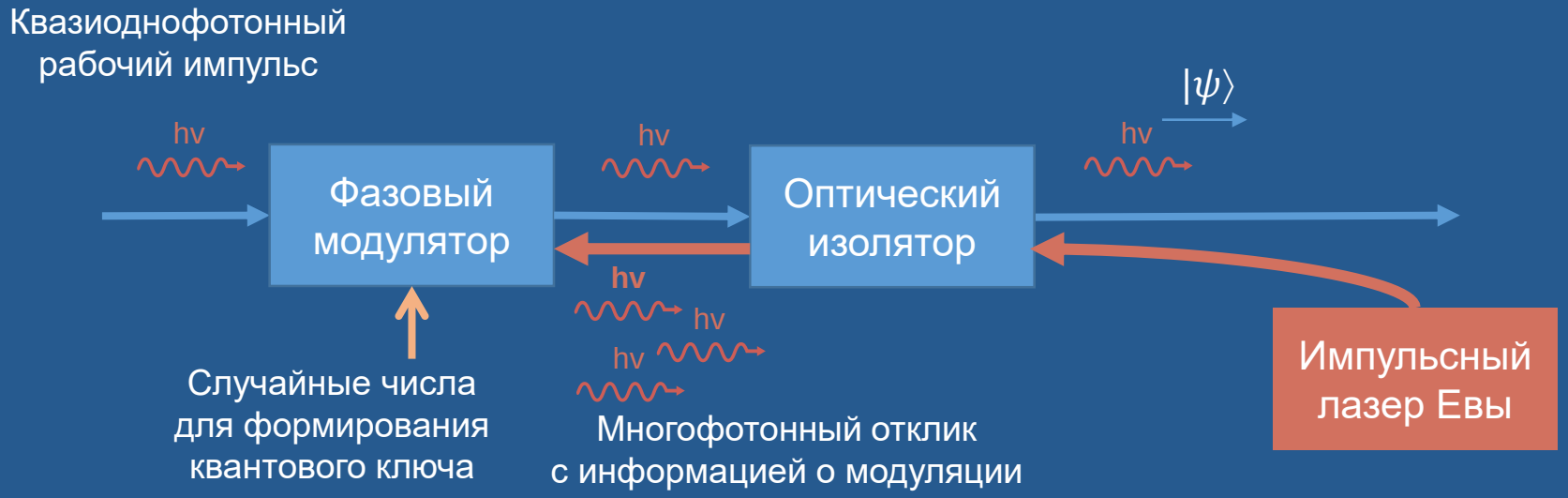


Точность и надежность переменного аттенюатора



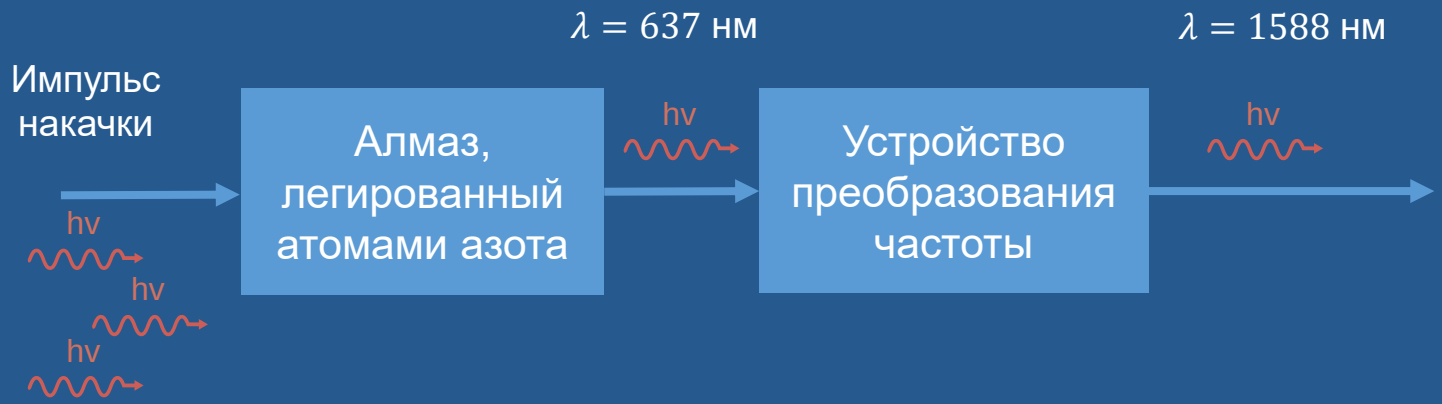
- Секретность систем КРК основана на формировании квантовых состояний на одиночных фотонах
- Реальные многофотонные импульсы делаются путем ослабления до почти однофотонного уровня
- Точность и надежность переменного аттенюатора – залог секретности формирования квантового ключа

Спектральные характеристики оптического изолятора



- В атаке активного зондирования Ева узнаёт случайные числа на фазовом модуляторе по отклику и нарушает секретность формируемого квантового ключа
- Для защиты от зондирования нужен оптический изолятор, пропускающий фотоны в одном направлении
- Необходимо исследовать спектральные характеристики оптического изолятора для предотвращения зондирования на нештатных для изолятора длинах волн, где его изолирующие свойства становятся хуже

Формирование истинно однофотонного импульса *



- Вероятность излучения двух и более фотонов существенно ниже, чем при ослаблении аттенюатором
- По этой причине у Евы значительно меньше возможностей для эффективной PNS атаки
- Большой потенциал не только для КРК, но и для оптических квантовых вычислителей

* Работа поддержана Минобрнауки России и ведется совместно с ВНИИОФИ

Выход за рамки одного сегмента волоконно-оптической сети

Основные ограничения базовой технологии КРК:

- Ограниченная дальность выработки квантового ключа в ВОЛС на уровне 100-130 км
- Квантовый ключ всегда вырабатывается в топологии «точка-точка»

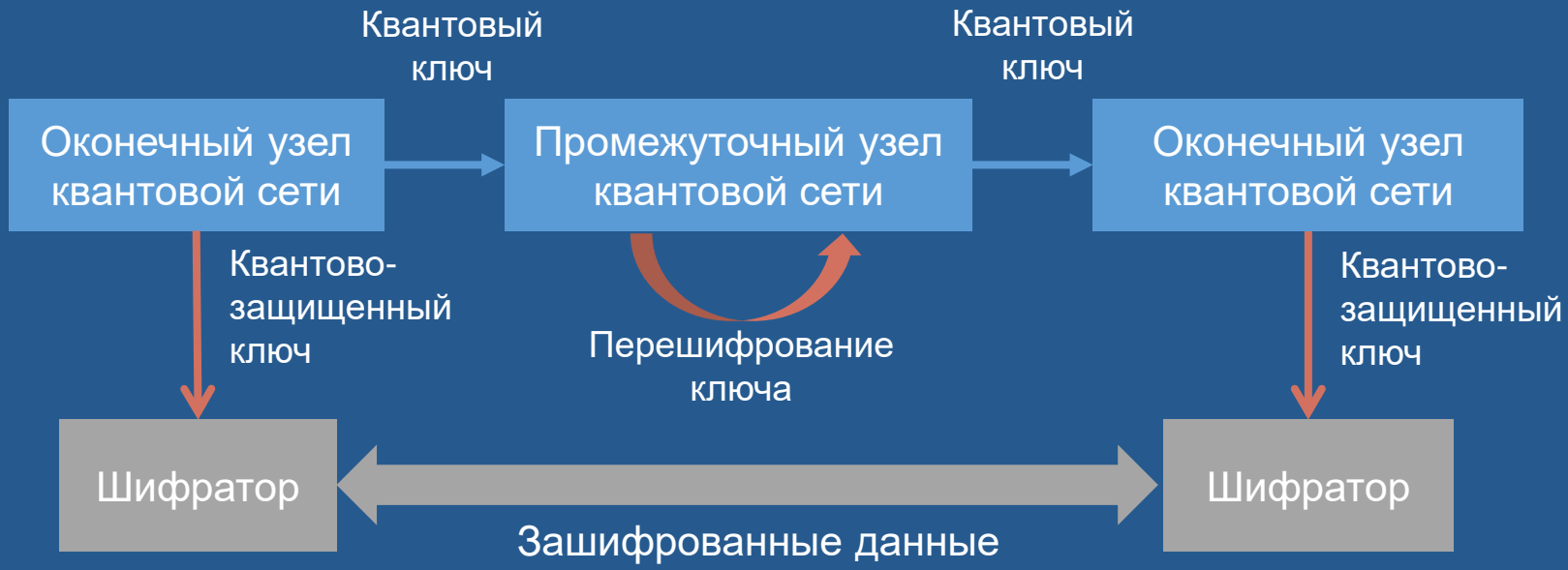
Современные потребности:

- Сети передачи данных реализуют логическую топологию «каждый с каждым»
- Протяженность телекоммуникационных линий может достигать тысяч километров

Многосегментные сети КРК с доверенными узлами:

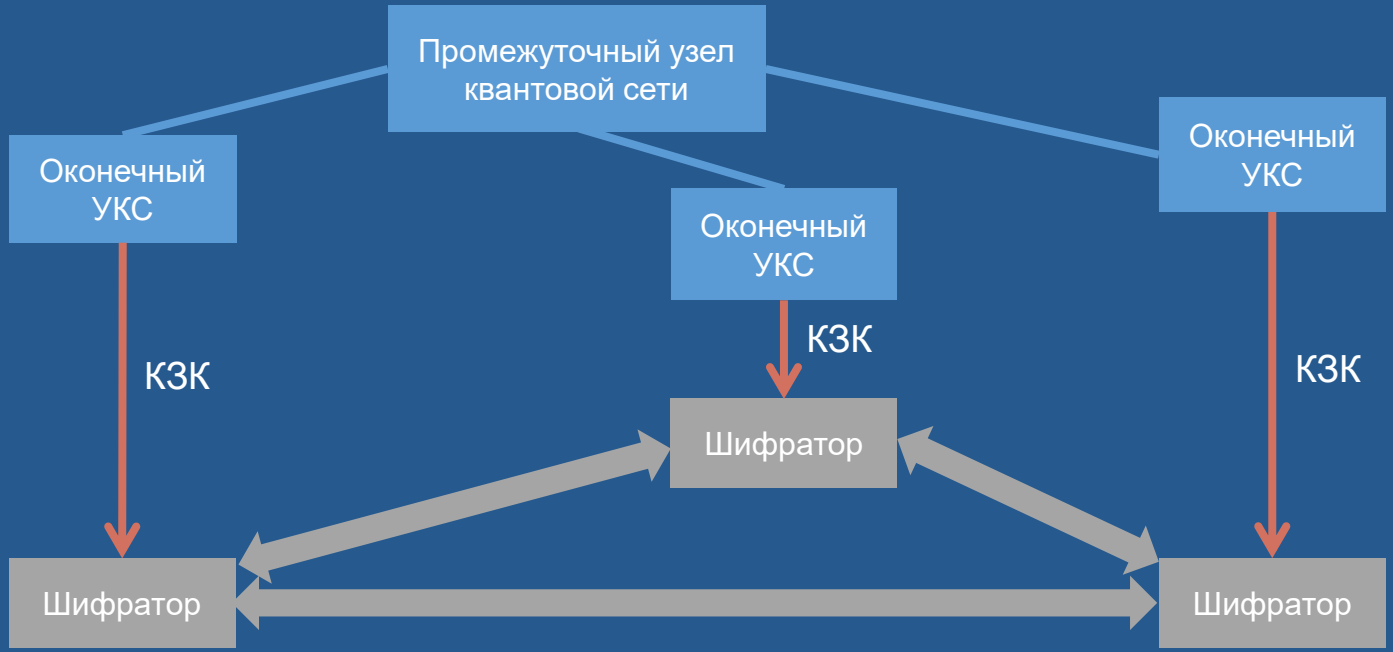
- На основе ВОЛС
- С сегментами открытого пространства
- С сегментами на космические спутники

Многосегментная сеть КРК с доверенными узлами



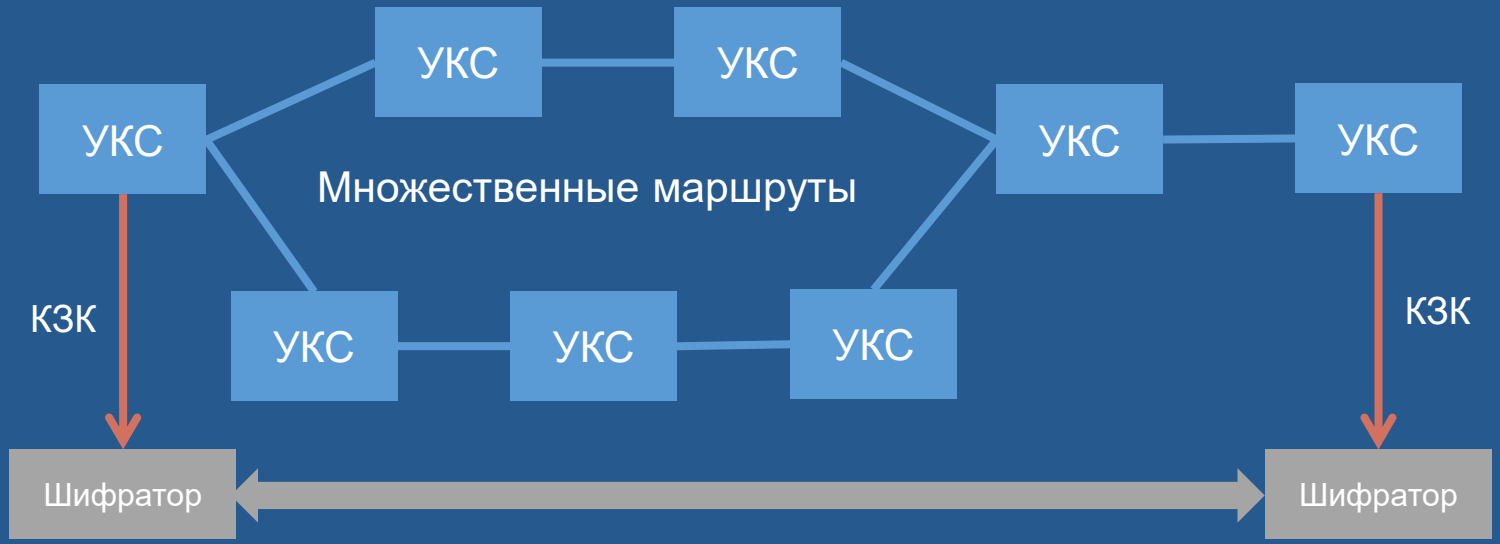
- Квантово-защищенный ключ (КЗК) передается по сети под защитой квантовых ключей на сегментах
- КЗК используется шифраторами как аналог квантового ключа

Многосегментная сеть КРК масштаба мегаполиса/региона



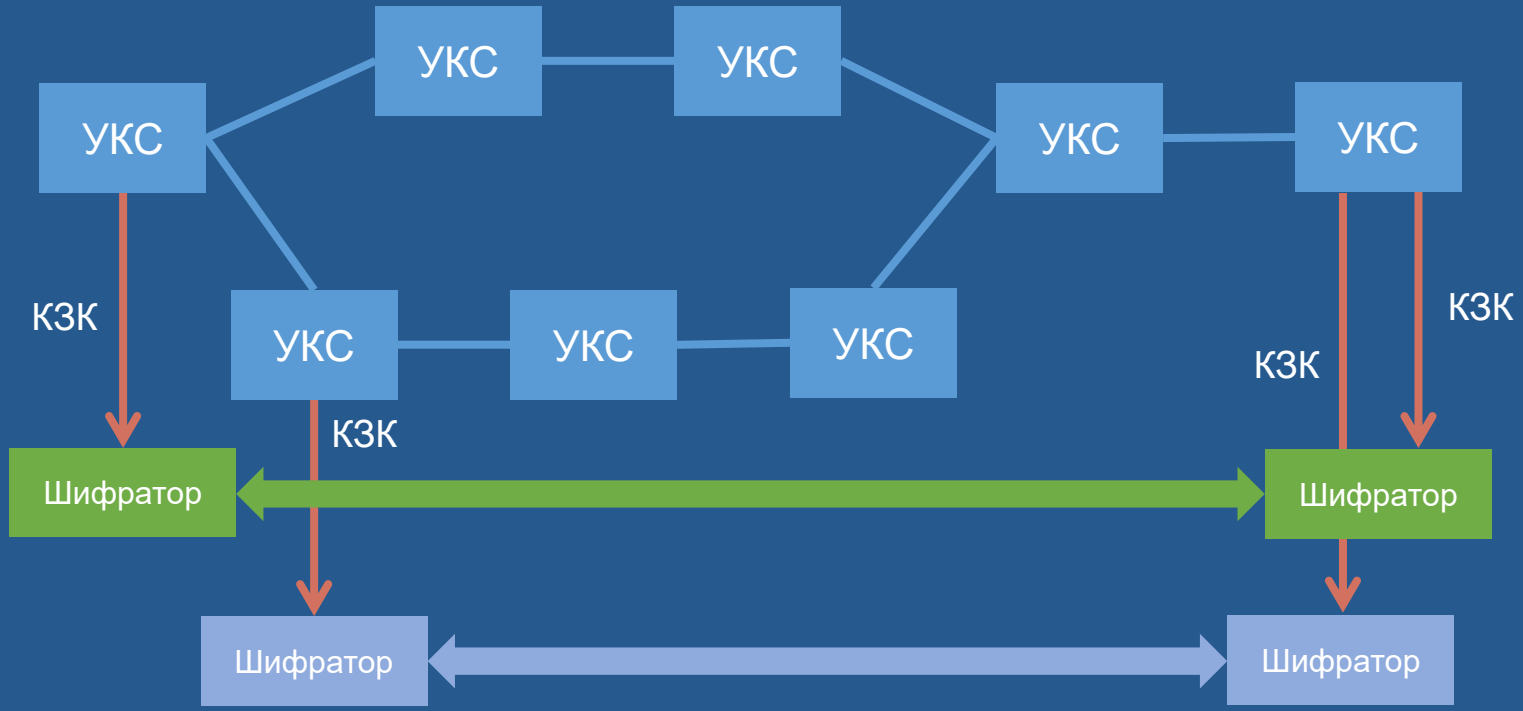
- Топология «звезда» сети КРК с помощью доверенного промежуточного узла в центре превращается в топологию «каждый с каждым» для шифраторов
- Технология отработана в проекте «Квантовый телефон» и реализуется в проекте ViPNet Quantum Security System (QSS)

Многосегментная сеть КРК масштаба страны



- Дублирование маршрутов для повышения производительности и отказоустойчивости
- Сочетание преимуществ топологии «магистраль» и «звезда»
- Подключение шифраторов различных производителей к узлам квантовой сети
- Технология построения квантовых сетей востребована лидерами рынка телекоммуникаций

Квантово-защищенный ключ как услуга квантовой сети



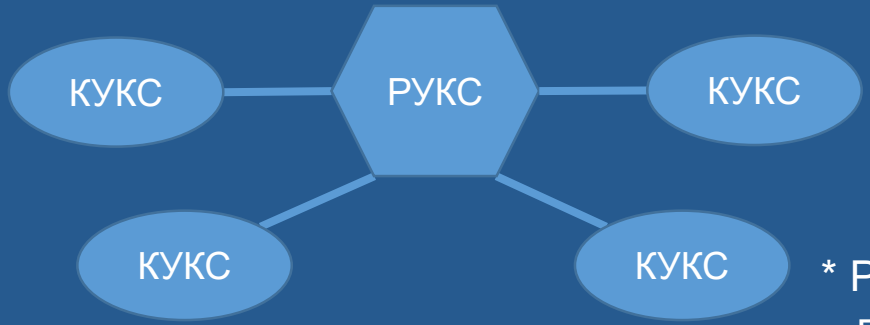
- Подключение шифраторов различных владельцев к узлам квантовой сети
- Необходимо стандартизовать протокол подключения шифраторов к узлам сети

Разработка технологии и аппаратуры квантовых сетей *

Базовые элементы квантовых сетей:

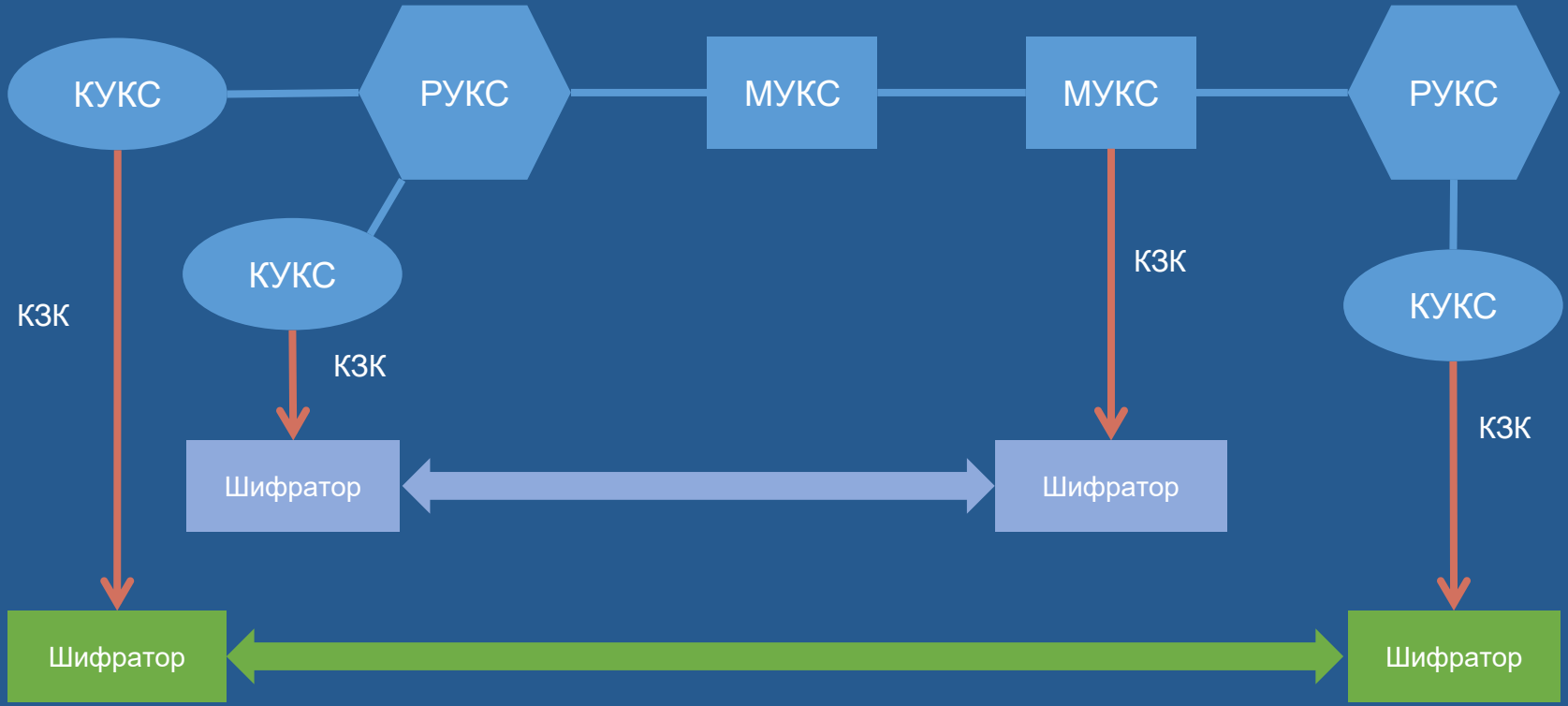
- Магистральный узел квантовой сети (МУКС)

- Распределительный узел квантовой сети (РУКС)
- Клиентский узел квантовой сети (КУКС)

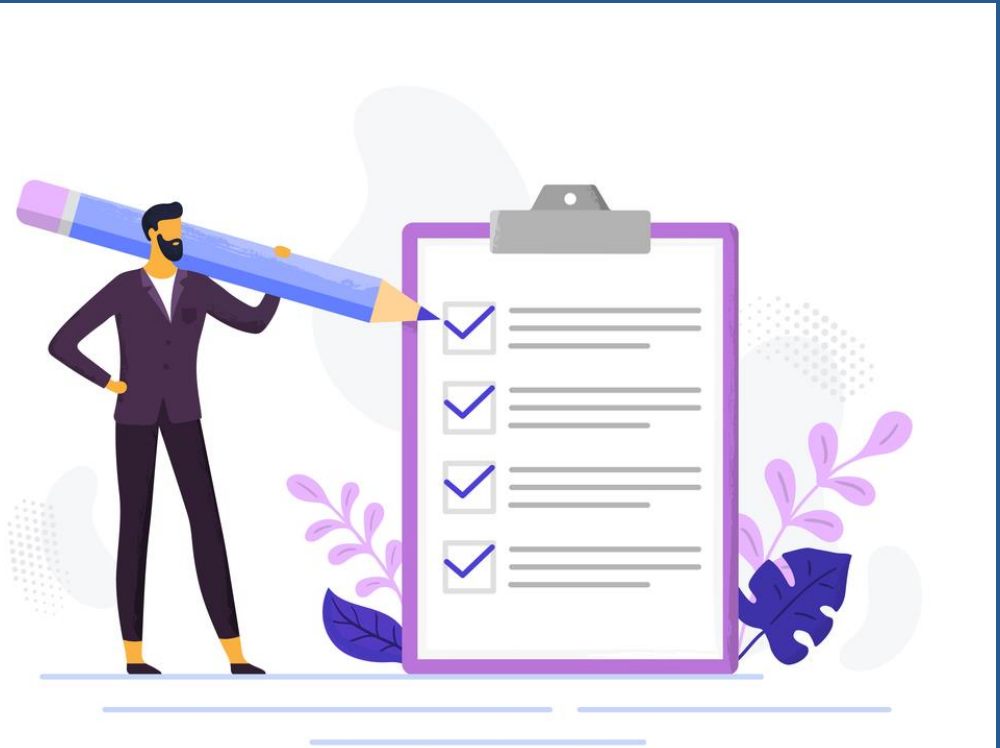


* Работа поддержана Министерством промышленности и торговли России

Пример квантовой сети на основе разрабатываемых узлов



План разработки технологии и аппаратуры квантовых сетей



2020

- Эскизное проектирование
- Техническое проектирование

2021

- Подготовка конструкторской документации
- Разработка опытных образцов
- Макет квантовой сети

2022

- Производство
- Сертификация

infotecs

Спасибо
за внимание!