конференция РусКрипто

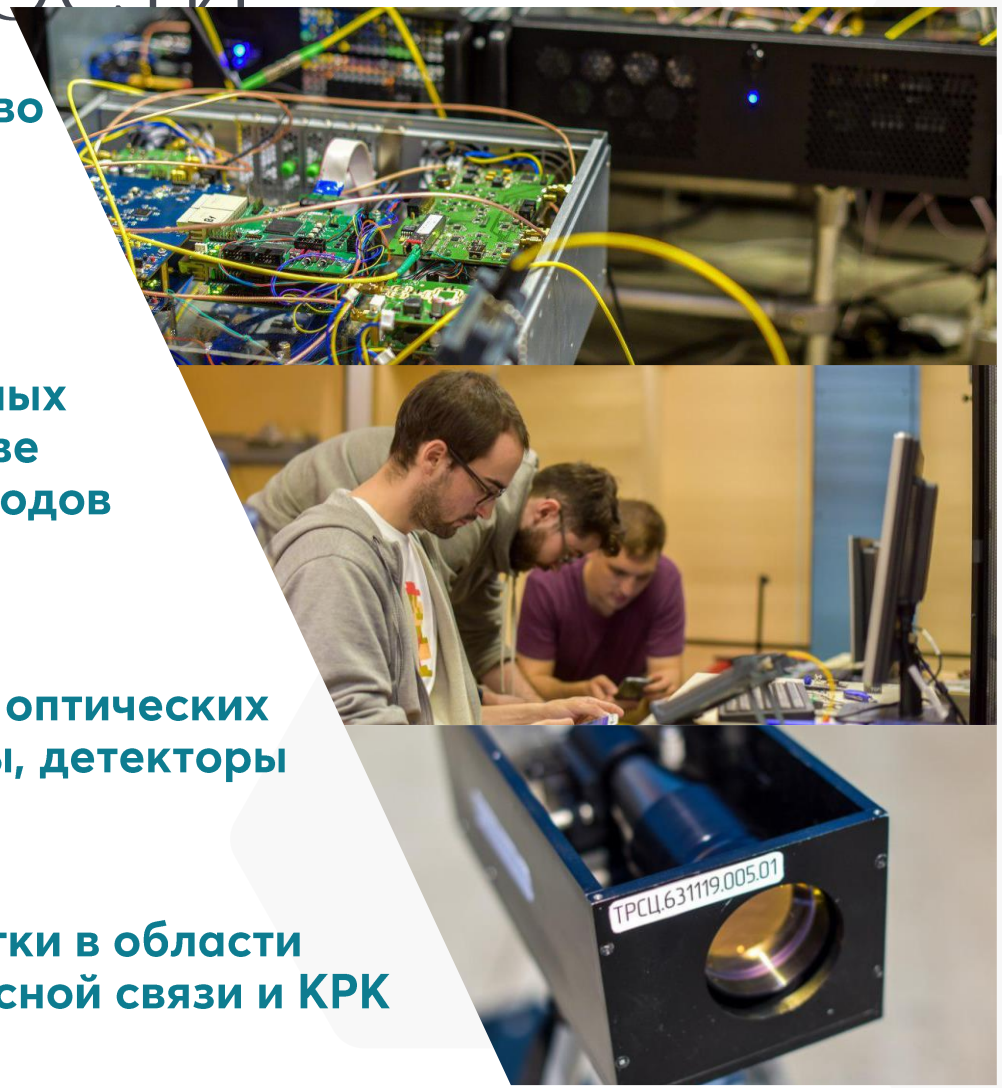
КВАНТОВЫЕ СИСТЕМЫ И СЕТИ:

ЗАДАЧИ И ПЕРСПЕКТИВЫ

Верещагина Елена Валентиновна,
генеральный директор, ООО «СМАРТС-Кванттелеком»

ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ

- **Разработка и производство систем квантового распределения ключей (КРК)**
- **Предоставление безопасных сетевых решений на основе КРК и «классических» методов шифрования**
- **Производство и продажа оптических компонентов (модуляторы, детекторы одиночных фотонов)**
- **Исследования и разработки в области оптических сетей, безопасной связи и КРК**



КВАНТОВЫЕ

сенсоры

вычисления

коммуникации

РЕШЕНИЯ ДЛЯ ИНТЕГРАЦИИ

Система ККС ВРК

Проведены испытания, проверки, показаны положительные результаты:

- Запуск всех интерфейсов, в т.ч. высокоскоростных (1 GB Eth, Jesd204b, MiG7) , работоспособность подтверждена
- Подтверждено функционирование СКЗИ
- Выпущен эмулятор КРК на основе отладочной платы (для стационарного тестирования у соисполнителя) и проведены испытания функционала системы KC705 EVALUATION PLATFORM HW-K7-KC705.
- Доработан прокол обмена данными между СКЗИ и КРК, верифицированы прошивки ПЛИС КРК и СКЗИ

Квантовая криптографическая система выработки и распределения ключей (ККС ВРК). Образец изготовлен на собственной производственной базе, на данный момент проходит сертификацию в ФСБ России.

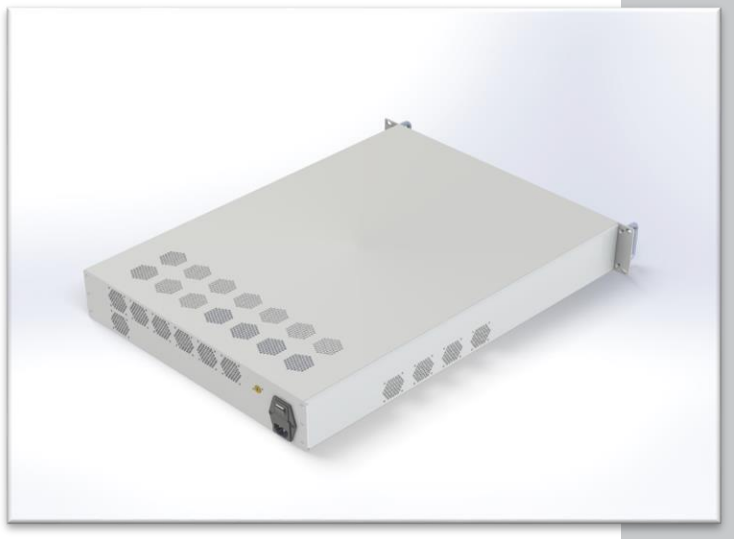
РЕШЕНИЯ ДЛЯ ИНТЕГРАЦИИ

Основные параметры и характеристики ККС ВРК :

- Клиентские интерфейсы (Клиент): 10 Gbit Ethernet или 8 Gbit FC, модуль SFP+
- Линейные интерфейсы (Канал): 2xOTU2e, модуль SFP+
- Линейные интерфейсы КРК: КК-1 Gbit Ethernet, тип FC, СК-1 Gbit Ethernet, модуль SFP+
- Производительность при передаче: 10 Gbit/s Ethernet или 6, 8 Gbit/s FC
- Скорость генерации КвК не менее 1 кбит/с (для линии связи с потерями 10 дБ (эквивалент 50 км)
- Латенсия (Latency), мс 0,044
- Резервирование Автоматическое переключение между линиями за время не более 50 мс
- Коррекция ошибок (FEC): ITU-T G.709/ITU-T G.975.1

Система ККС ВРК

РЕШЕНИЯ ДЛЯ ИНТЕГРАЦИИ



Клиентский модуль ККС BPK

Основные параметры и характеристики

КРК:

- Энергопотребление: не более 450 Вт
- Расстояние: до 80 км (между КМ КРК-А и КРК-Б)
- Режимы выработки ключей: "точка-точка"
- Возможность шифрования ключей и передачи их по каналам общего пользования (для клиентов, не имеющих квантовой аппаратуры).
- Криптоалгоритм: ГОСТ Р 34.12-2015
- Режим шифрования: ГОСТ Р 34.13-2015 (режим гаммирования)
- Реализация шифрования: аппаратная (ПЛИС)
- Алгоритм исправления ошибок в квантовом канале: LDPC
- Исправляемый QBER: до 7%
- Локальное управление/мониторинг: да (ПК, разъем подключения 1Гбит/сек, RJ45)
- Габариты: 19" 2U 600x175x436 (без учета ручек на фронтальной панели)

ПАРАМЕТРЫ МОДЕЛИ СИСТЕМЫ КРК «КВАНТТЕЛЕКОМ»

- μ_0 = 4 – среднее число фотонов на центральной моде до модуляции
- μ = 0.1 – среднее число фотонов во всем спектре боковых частот
- $\triangle m$ = 0.03 – несовпадение индексов модуляции
- $\Delta\varphi = 5°$ – дрожание фазы
- FL = 27 dB – доля пропускания фильтром на центральной моде
- η = 100 Hz – частота темновых срабатываний детектора
- QE = 20% – квантовая эффективность детектора
- η_{Bob} = 8 dB – потери в модуле получателя
- F = 100 MHz – частота смены кодирующей фазы
- $n = 10^7$ – необходимое количество бит в сырой битовой последовательности
- $\varepsilon_s = 10^{-10}$ – параметр гладкости мин-энтропии
- $\varepsilon_{PA} = 10^{-10}$ – параметр усиления секретности
- $\varepsilon_{EC} = 10^{-10}$ – вероятность несовпадения битовых последовательностей после
- исправления ошибок
- $\varepsilon_{EC}^{c} = 10^{-10}$ – вероятность неисправления всех ошибок в битовых последовательностях отправителя и получателя

В качестве рабочих параметров системы выбраны следующие значения

УСТОЙЧИВОСТЬ РЕАЛИЗАЦИИ К АТАКАМ НА ТЕХНИЧЕСКУЮ РЕАЛИЗАЦИЮ

Атака	Краткое описание	Возможные контрмеры
Навязывание ключа (ослепление детектора)	Ослепление детектора фотонов сильным излучением (перевод из гейгеровского режима в линейный) и управление срабатываниями с помощью оптических импульсов	• Контроль силы тока в цепи гашения лавины МДФ • Мониторинг излучения засветки • Спектральное ограничение излучения нарушителя
Троянский конь	Отправка нарушителем сильного импульса в блок СКК и измерение фазового сдвига, внесённого модулятором в отражённое излучение	Отправитель: •Добавление оптического изолятора •Установка высоких потерь на аттенюаторах. Получатель: •Спектральное ограничение излучения нарушителя •Изоляция отражённого излучения •Регистрация отражённого излучения •Учёт в мат. модели
Переизлучение детектора	Излучение лавинным фотодиодом в блоке получателя СКК вторичного фотона после регистрации сигнального.	Установка циркулятора в СКК получателя, вторичный фотон не возвращается нарушителю в канал.

Испытания системы КРК на боковых частотах, посвящённые исследованию устойчивости её текущей реализации к атакам на квантовый протокол и техническую реализацию, известным из открытых источников.

ОБОРУДОВАНИЕ

Детектор одиночных фотонов

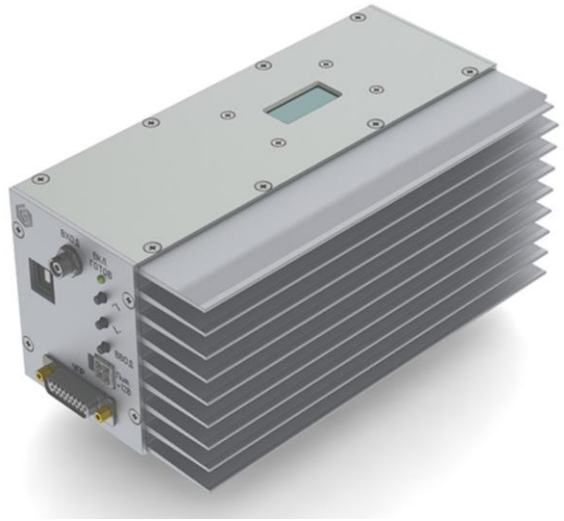
- Экспериментальная квантовая оптика - исследование связанных (перепутанных) состояний
- Лазерная локация - LIDAR/LADAR.
- Квантовая криптография
- Фотолюминисценция
- Спектроскопия

Характеристики:

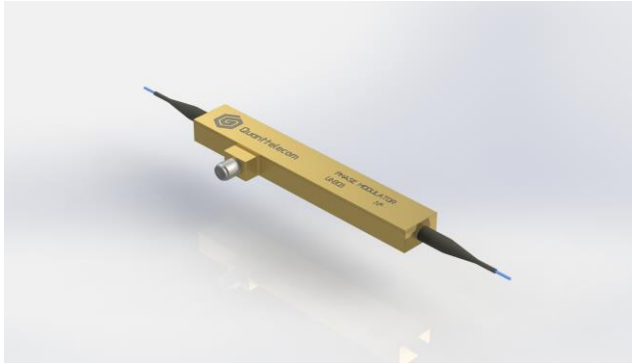
Квантовая эффективность:
не менее 10% (настраиваемое значение, до 20% с шагом 2,5%).

Вероятность темнового отсчета :
$5 \cdot 10^{-7}$ (при квантовой эффективности 10% и длительности стробирующего импульса 1 нс).

Максимальная частота повторения импульсов запуска :
300 МГц.



СВЧ интегрально-оптические модуляторы



- Телекоммуникация
- Квантовое распределение ключей

Характеристики:

- Рабочая длина волны (тип.): 1520-1560 нм
- Электрооптическая полоса пропускания: до 40 ГГц
- Вносимые потери (тип.): 4 дБ
- Возвратная потеря (макс): 50 дБ
- Оптическая входная мощность (макс.): 100 мВт
- Vp напряжение RF: <5 В
- Оптический разъем: FC/APC, с сохранением поляризации

ЭТАПЫ РАЗВИТИЯ КВАНТОВЫХ КОММУНИКАЦИЙ

1

ТЕКУЩИЙ ПЕРИОД

Квантовая рассылка ключа «точка– точка»

- ТЕМНОЕ ВОЛОКНО
- ПЕРЕХОД НА СТАНДАРТНОЕ ВОЛОКНО
- ИНТЕГРАЦИЯ КРК И СКЗИ
- СЕРТИФИКАЦИЯ ФСБ

2

1 -7 ЛЕТ

Квантовые сетевые технологии

- Интеграция с существующими телекоммуникационными сетями
- Обеспечение физической безопасности сети
- Снижение стоимости

- ГИБРИДНЫЕ СЕТИ (МУЛЬТИПЛЕКСИРОВАНИЕ КВАНТОВЫХ И ИНФОРМАЦИОННЫХ КАНАЛОВ)
- КВАНТОВЫЕ МАРШРУТИЗАТОРЫ
- ИНТЕГРАЦИЯ С СЕТЯМИ 5G
- КВАНТОВЫЙ КЛЮЧ КАК УСЛУГА

3

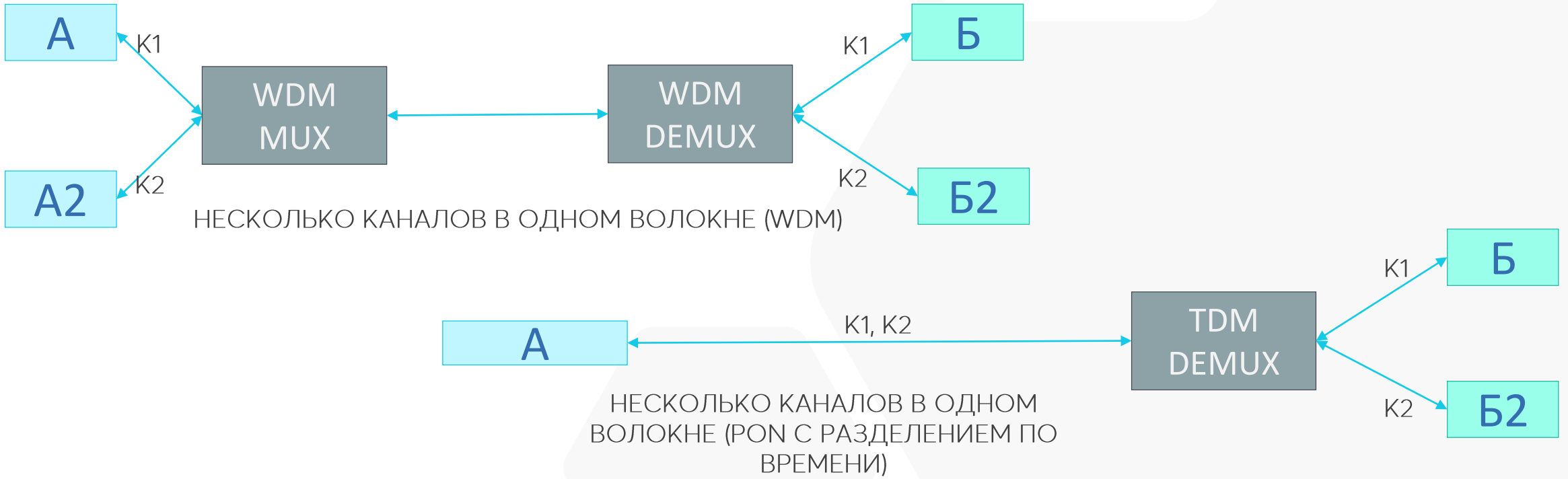
10+ ЛЕТ

Глобальные квантовые сети

- Недоверенные квантовые сети
- Распределенные квантовые вычисления
- Устойчиво работающие крупномасштабные квантовые системы

- КВАНТОВЫЕ ПОВТОРИТЕЛИ
- КВАНТОВЫЕ ВЫЧИСЛЕНИЯ
- МОБИЛЬНЫЕ И КОНЕЧНЫЕ УСТРОЙСТВА
- СПУТНИКОВЫЕ КВАНТОВЫЕ СЕТИ

АРХИТЕКТУРА КВАНТОВЫХ СЕТЕЙ МУЛЬТИПЛЕКСИРОВАНИЕ

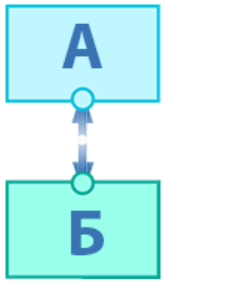


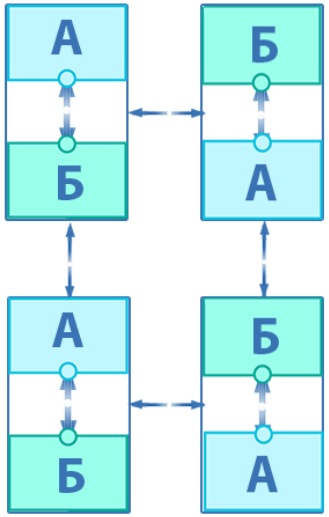
А = модуль отправителя системы КРК

Б = модуль получателя системы КРК

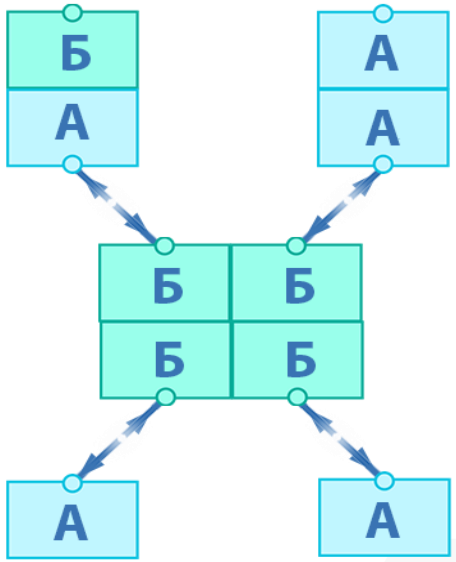
Между каждой парой А и Б генерируется уникальный ключ (свойство КРК)

АРХИТЕКТУРА КВАНТОВЫХ КОММУНИКАЦИОННЫХ СЕТЕЙ



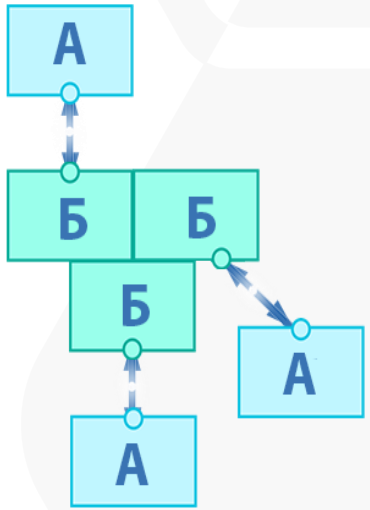


«КОЛЬЦО»



«ПРОИЗВОЛЬНАЯ»

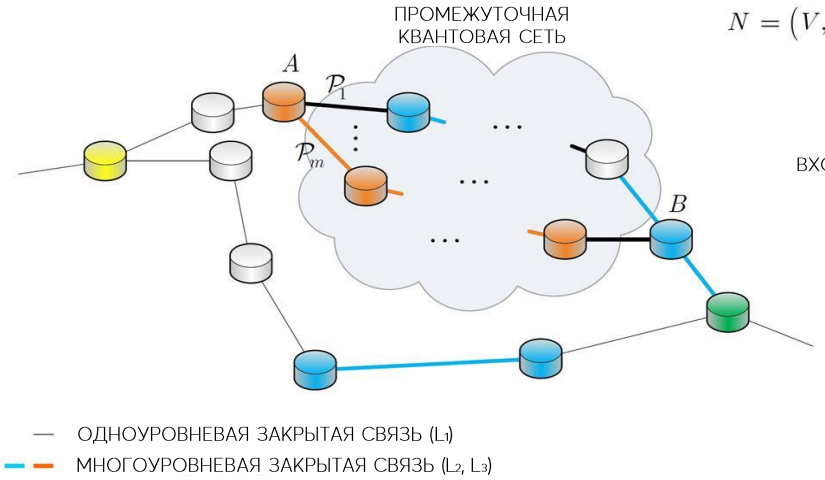
Нужна пара модулей КРК для каждой связи



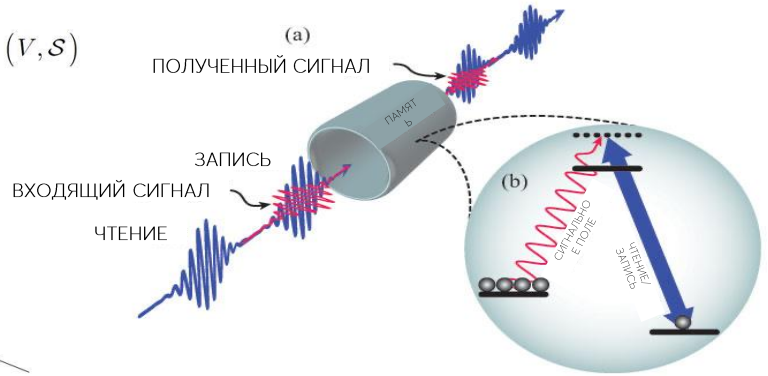
«ЗВЕЗДА»

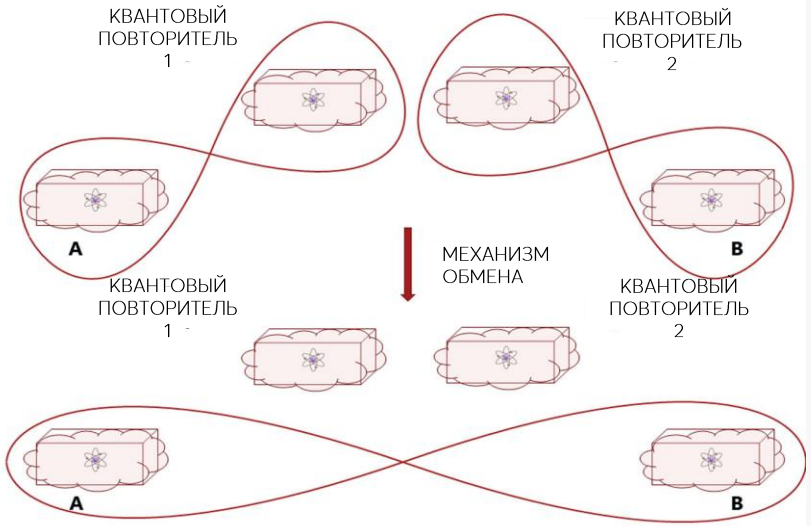
Задача магистральных систем КРК поддерживать одновременную передачу ключевой информации множества пользователей. Необходимость построения квантовых сетей произвольной топологии: не только «точка-точка», но и «звезда», «кольцо», «смешанная».

КВАНТОВЫЕ ПОВТОРИТЕЛИ И КВАНТОВАЯ ПАМЯТЬ



$N = (V, \mathcal{S})$



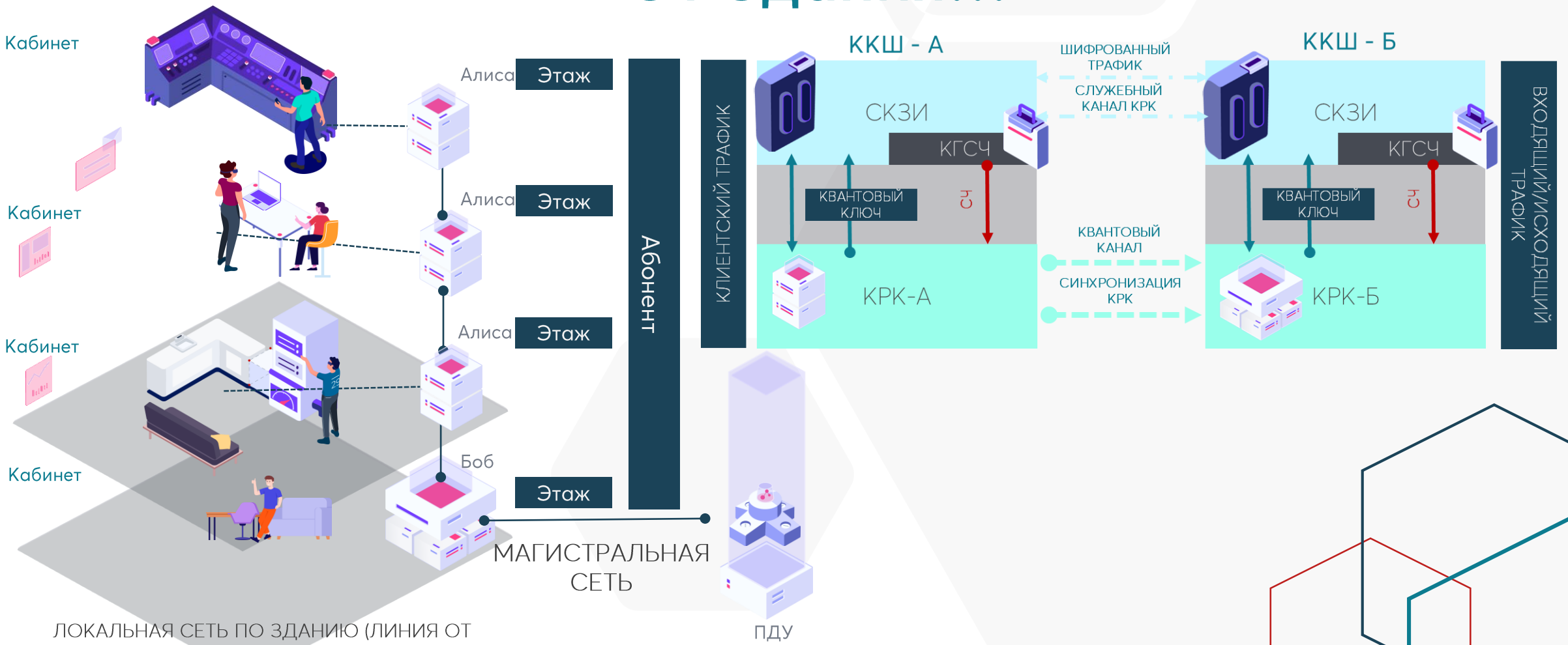


Отсутствие на сегодняшний день эффективных и надежных реализаций квантовых повторителей с квантовой памятью

BRIEGEL, H.-J., AND R. RAUSSENDORF, PHYS. REV. LETT. 86, 910 (1998)
GYONGYOSI, L., IMRE, S. ENTANGLEMENT-GRADIENT ROUTING FOR QUANTUM NETWORKS. SCI REP 7, 14255 (2017). HTTPS://DOI.ORG/10.1038/S41598-017-14394-W
IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS, VOL. 21, NO. 3, MAY/JUNE 2015
HTTPS://PHYS.ORG/NEWS/2018-11-IMPORTANT-QUANTUM-NETWORK.HTML
HTTPS://WWW.SCIENTIFICAMERICAN.COM/ARTICLE/THE-QUANTUM-INTERNET-IS-EMERGING-ONE-EXPERIMENT-AT-A-TIME/
HTTPS://PHYSICSWORLD.COM/A/QUANTUM-MEMORY-WORKS-AT-ROOM-TEMPERATURE/

ИНТЕГРАЦИЯ И РАСПРЕДЕЛЕНИЕ

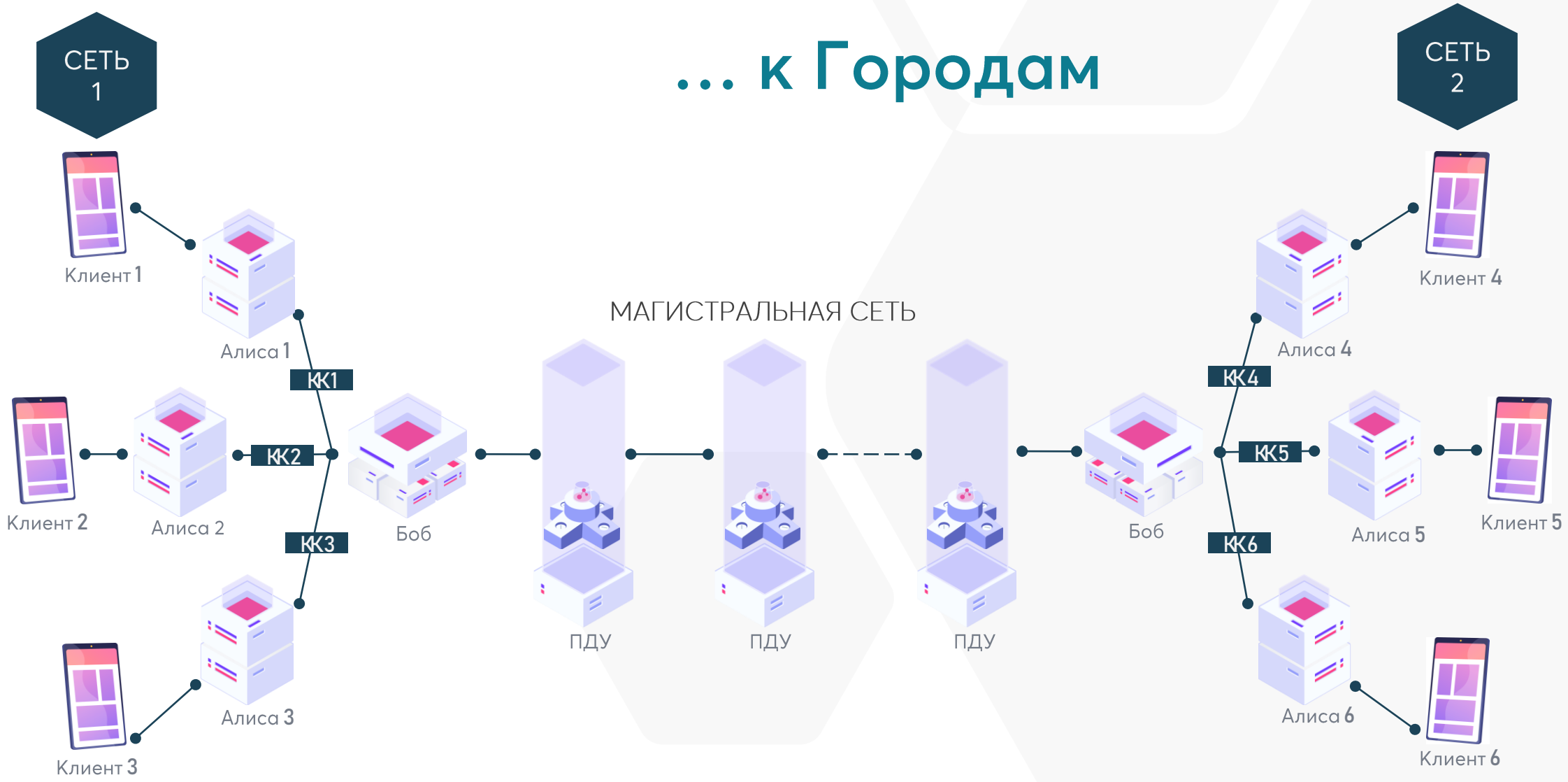
От Здания...



ЛОКАЛЬНАЯ СЕТЬ ПО ЗДАНИЮ (ЛИНИЯ ОТ ЦЕНТРАЛЬНОГО УЗЛА ЗДАНИЯ ДО АБОНЕНТА БОЛЕЕ 100 М.)

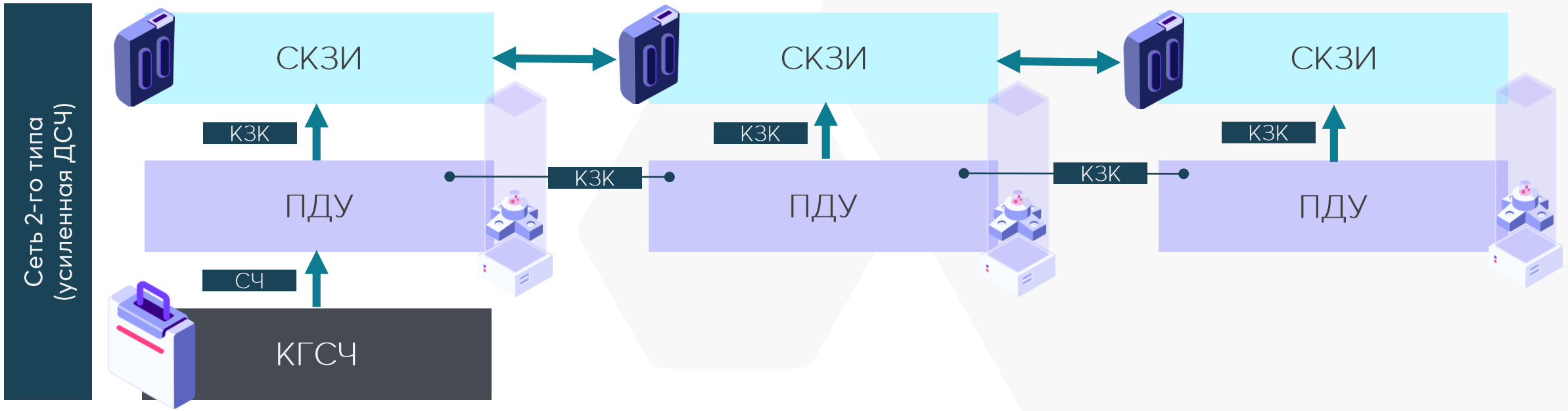
ИНТЕГРАЦИЯ И РАСПРЕДЕЛЕНИЕ

… к Городам



ТИПЫ СЕТЕЙ

Свойства/тип сети	Сеть 1-го типа («классическая»)	Сеть 2-го типа (усиленная ДСЧ)	Сеть 3-го типа («квантовая»)
Необходимость предварительной доставки ключей на узлы сети	Да	Да	Нет
Трудоемкость распределения ключей по узлам сети	Высокая	Средняя	Минимальная
Время актуального действия ключа	Определено формуляром СКЗИ	Определено формуляром СКЗИ	Не ограничено
Трудоемкость замены ключа при компрометации	Высокая (новое распределение ключей)	Средняя (определена запасом предварительно выработанной матрицы)	Минимальная (автоматическая смена)



СЕРВИСНАЯ МОДЕЛЬ – КВАНТОВЫЙ КЛЮЧ КАК УСЛУГА

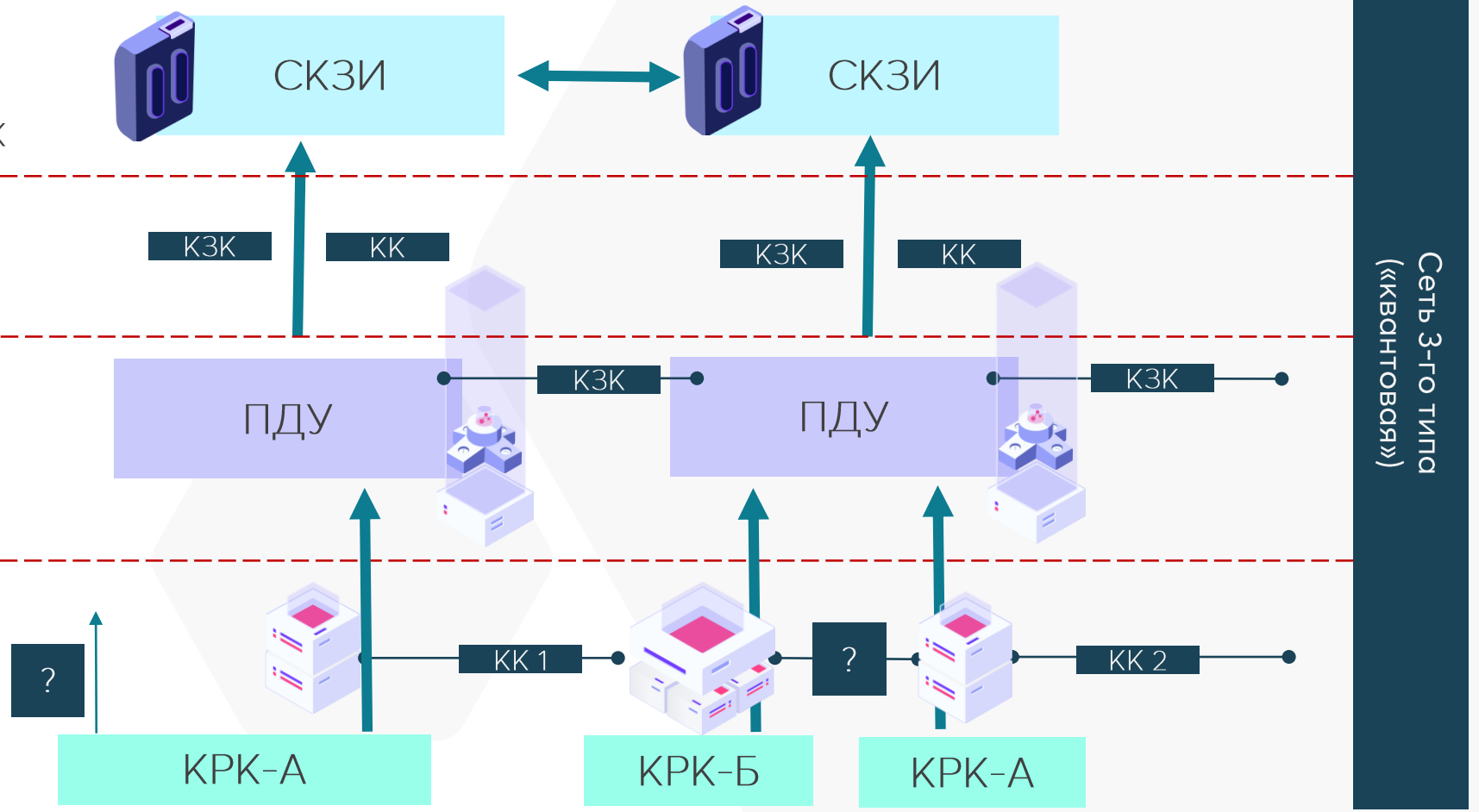
Уровни

4 ИСПОЛЬЗОВАНИЕ КЛЮЧЕЙ КОНЕЧНЫМИ ПОТРЕБИТЕЛЯМИ МАГИСТРАЛЬНОЙ СЕТИ (МС) КК

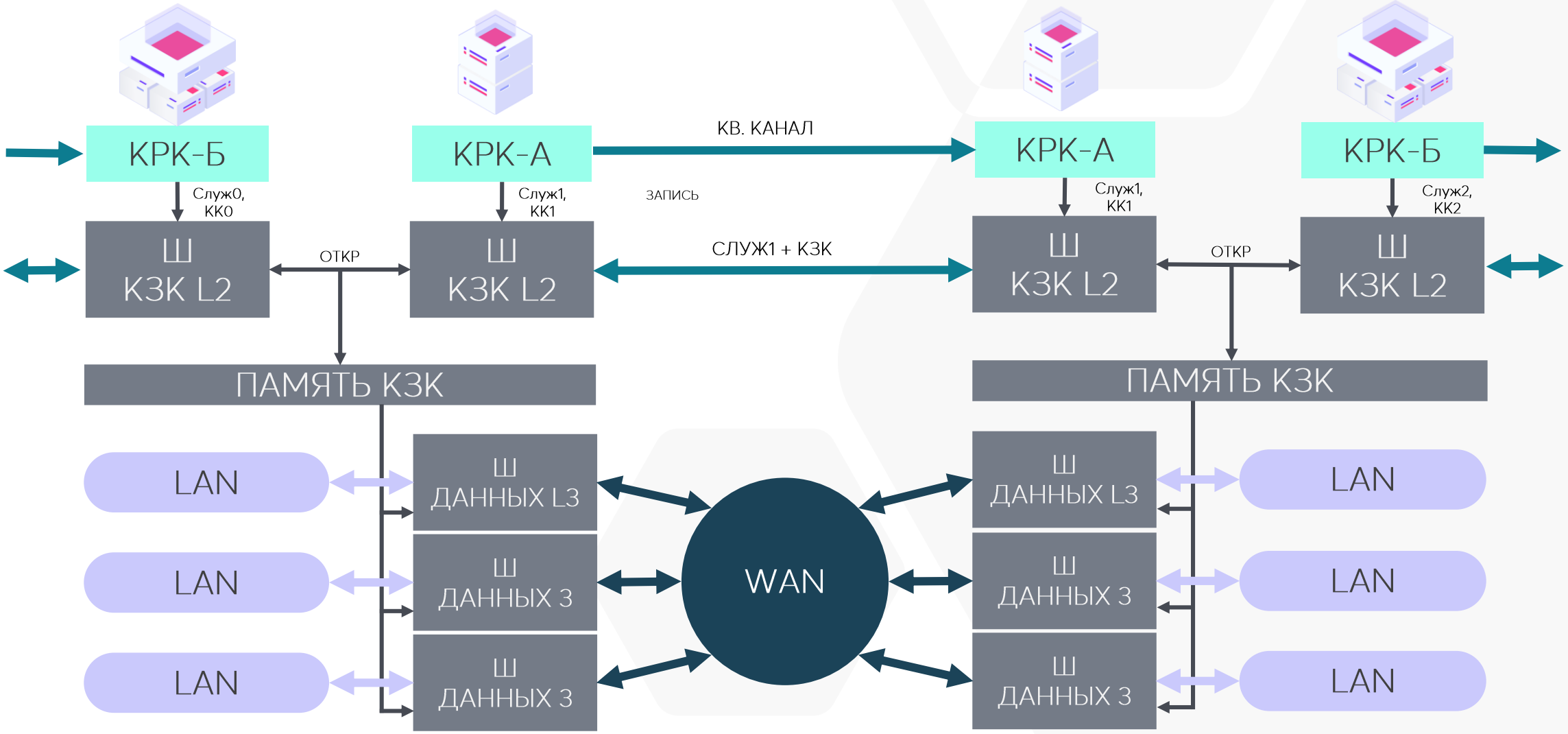
3 ИНТЕРФЕЙС. ПЕРЕДАЧА КВАНТОВЫХ КЛЮЧЕЙ ПОТРЕБИТЕЛЯМ МС ОТ ПДУ

2 АДМИНИСТРАТОР КК. ХРАНЕНИЕ КВАНТОВЫХ КЛЮЧЕЙ В ПДУ

1 ВЫДАЧА КК. ПОЛУЧЕНИЕ КЛЮЧЕЙ ОТ УСТРОЙСТВ КРК



ПРИМЕР СХЕМЫ ПКСПК



СИСТЕМА УПРАВЛЕНИЯ КЛЮЧАМИ И СИСТЕМА УПРАВЛЕНИЯ СЕТЬЮ

Задачи, решаемые системой управления ключами:

- генерация, распределение между пользователями сети,
- хранение и управление циклом жизни квантово-защищенных ключей.

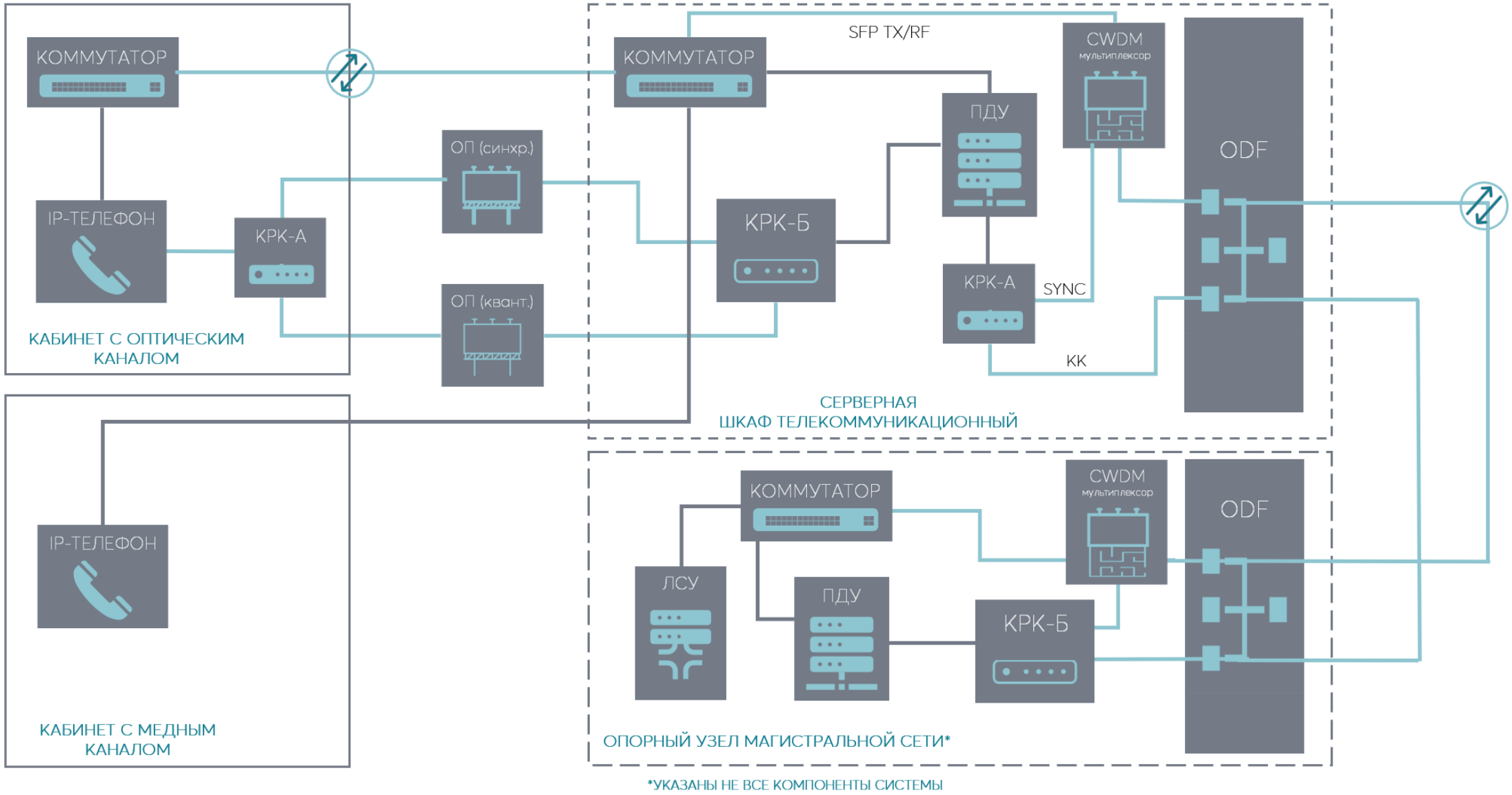
Смена ключей шифрования должна производиться в полностью автоматическом режиме на регулярной основе.

Задачи управления и мониторинга протяженных квантовых сетей:

- управление сервисами,
- ресурсное планирование,
- контроль параметров качества оказания услуг.

Контроль скорости генерации квантовых ключей, контроль значений квантового коэффициента ошибок (QBER) для различных участков сети. Выдача предупреждений о превышении порога QBER, так как данная ситуация может быть вызвана попыткой НСД к квантовому каналу.

ОДНО ИЗ РЕАЛЬНЫХ РЕШЕНИЙ



КВАНТОВЫЕ СИСТЕМЫ И СЕТИ:

ЗАДАЧИ И ПЕРСПЕКТИВЫ

Верещагина Елена Валентиновна,
генеральный директор, ООО «СМАРТС-Кванттелеком»

Электронная почта:
vereschagina@qcphotonics.com

Телефон:
+7 981 803-79-11

Сайт:
www.quanttelecom.ru