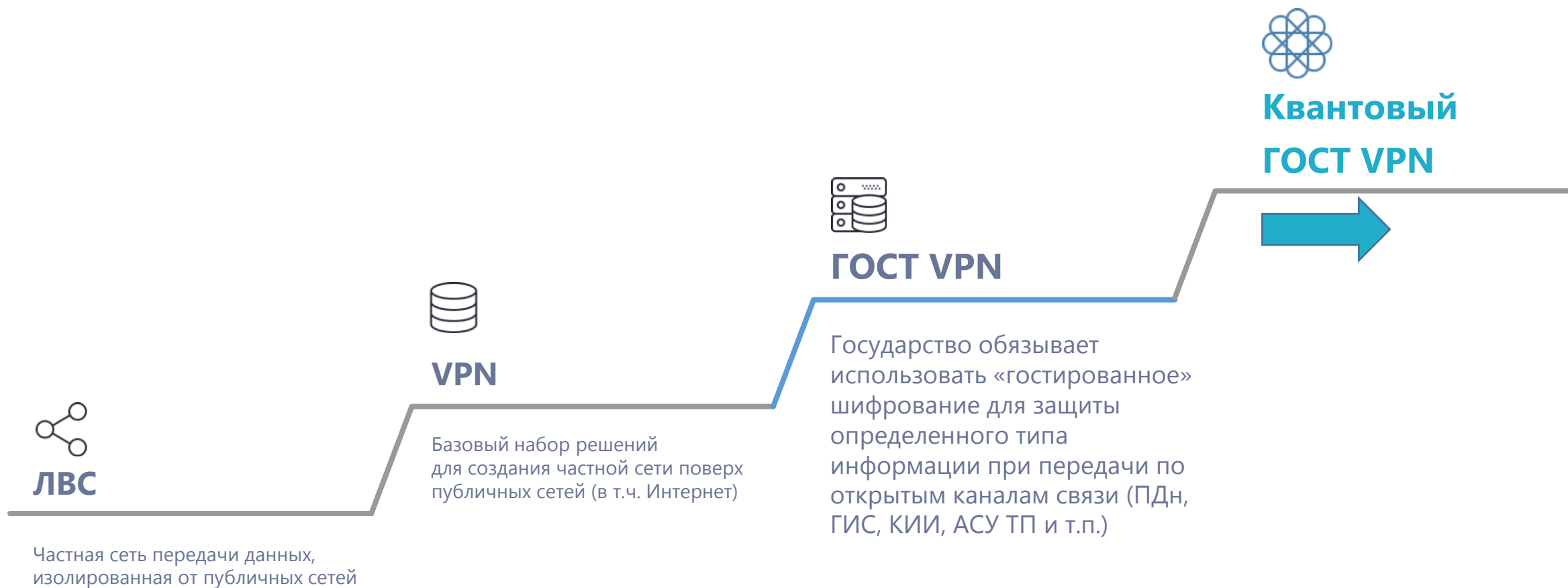


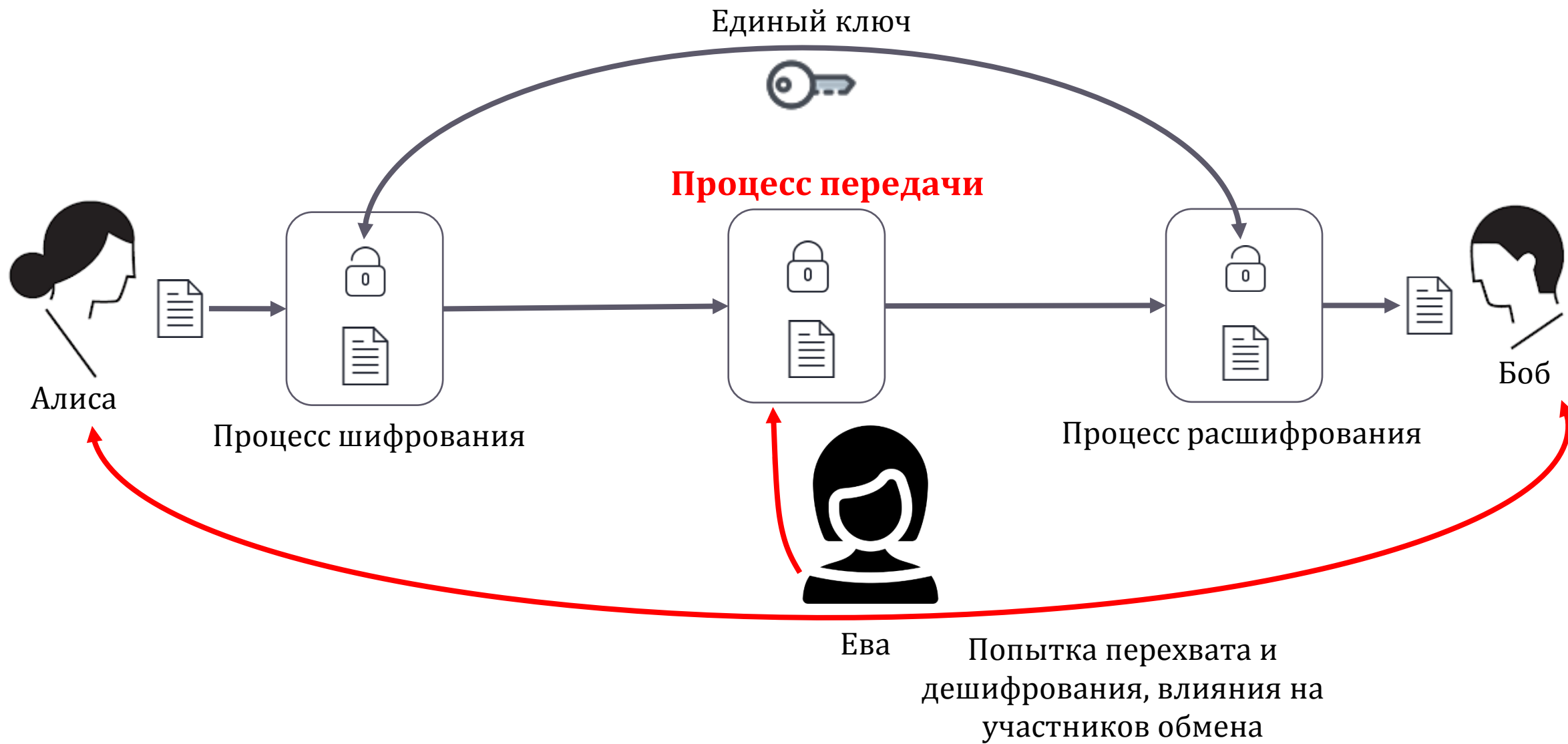
Квантовозащищённые каналы связи – время пришло

Объединённая конференция ИТ-служб. 2025
Энергетический сектор



Хронология реализации защиты данных в сетях связи







Квантовые вычисления

Появление квантовых компьютеров, а также высокая степень развития квантовых вычислений и технологий искусственного интеллекта создают риски и угрозы компрометации существующих способов защиты данных



Человеческий фактор

Риск компрометации криптографических ключей при процедуре их загрузки в СКЗИ.



Взломы из будущего

Данные копируются и хранятся злоумышленниками до появления возможности расшифровки

Агрессивная международная обстановка

кратно увеличивает все указанные факторы риска за счёт использования колоссальных финансовых и человеческих ресурсов

«Улучшение» традиционного ГОСТ VPN



Постквантовые алгоритмы

Существующие реализации подходят только для асимметричного шифрования.

Алгоритмы плохо изучены



Длина мастер-ключа

Потребуется внесение изменений в существующие ГОСТ, а так же внесение изменений в существующие ПАК СКЗИ



Частота смены ключа

Уменьшение регламентных норм по смене ключа потребует дополнительного ресурса



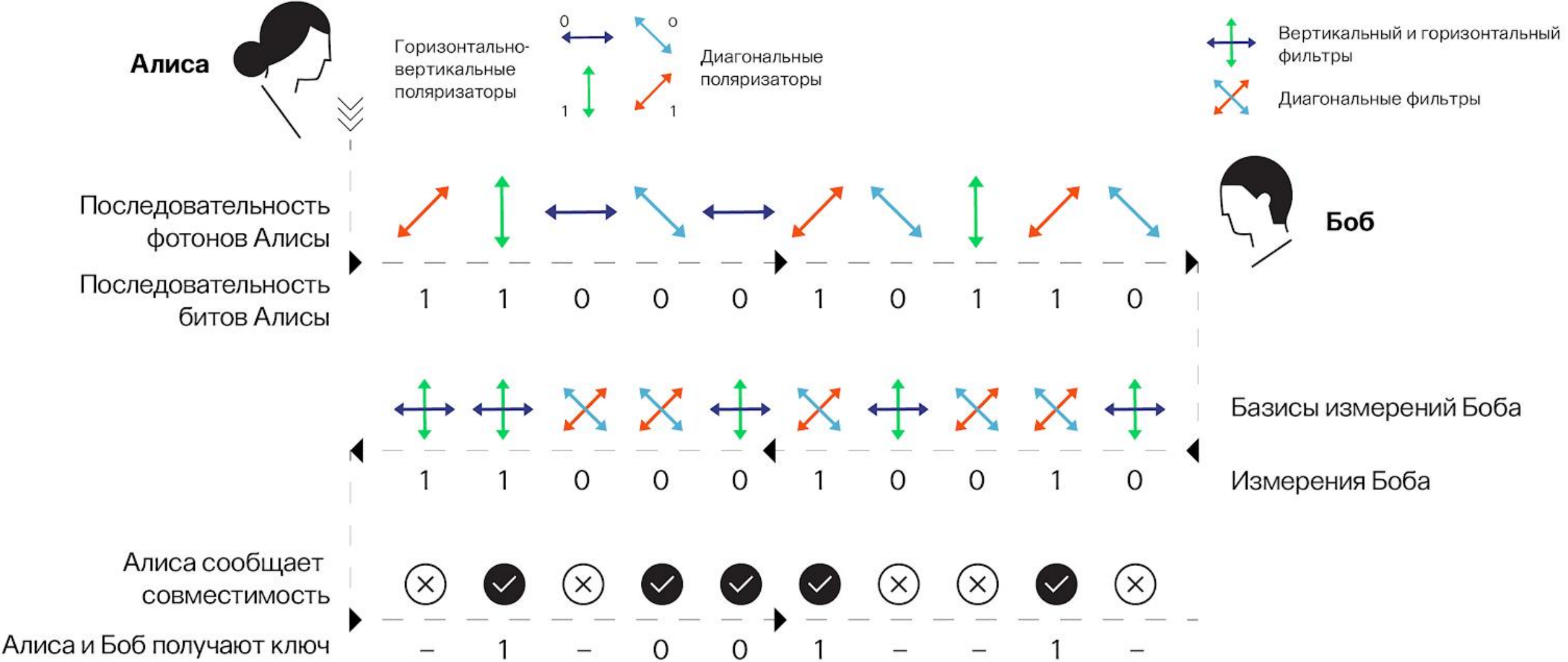
Автоматизация смены ключа

При классической реализации несёт дополнительные риски по компрометации ключа

Квантовое распределение ключей

- Технология КРК абсолютно устойчива к любой мощности вычислений*
- Технология КРК позволит автоматизировать процесс и увеличить частоту смены ключей не меняя длину ключей используемых в шифраторах
- Технология КРК существенно снизит, а со временем и вовсе сделает человеческий фактор ничтожным

Дорого и неэффективно



СТРОИТЕЛЬСТВО КВАНТОВОЙ МАГИСТРАЛИ (МКС)

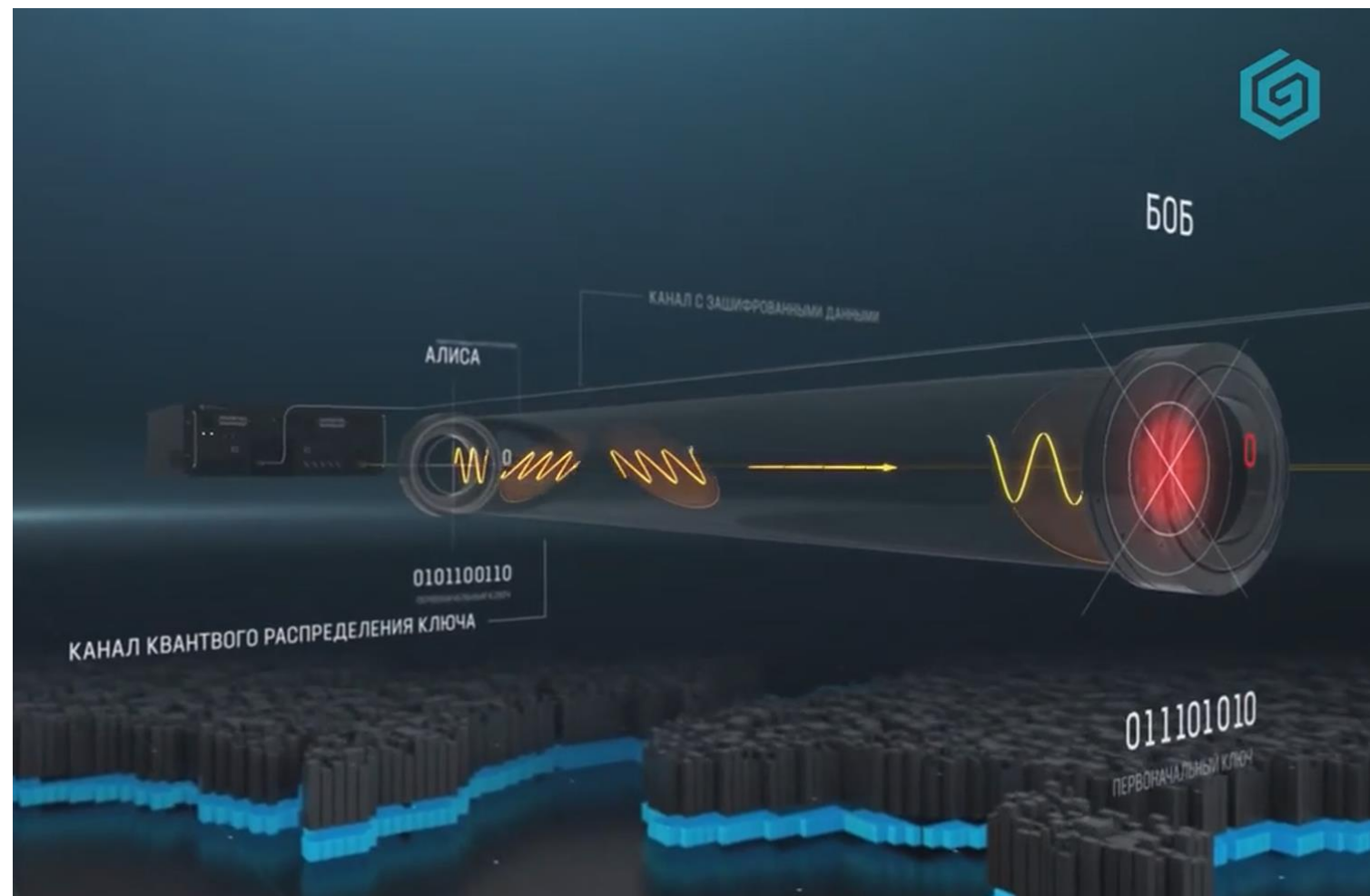
Распоряжение №1663р от 08.07.2024 г.

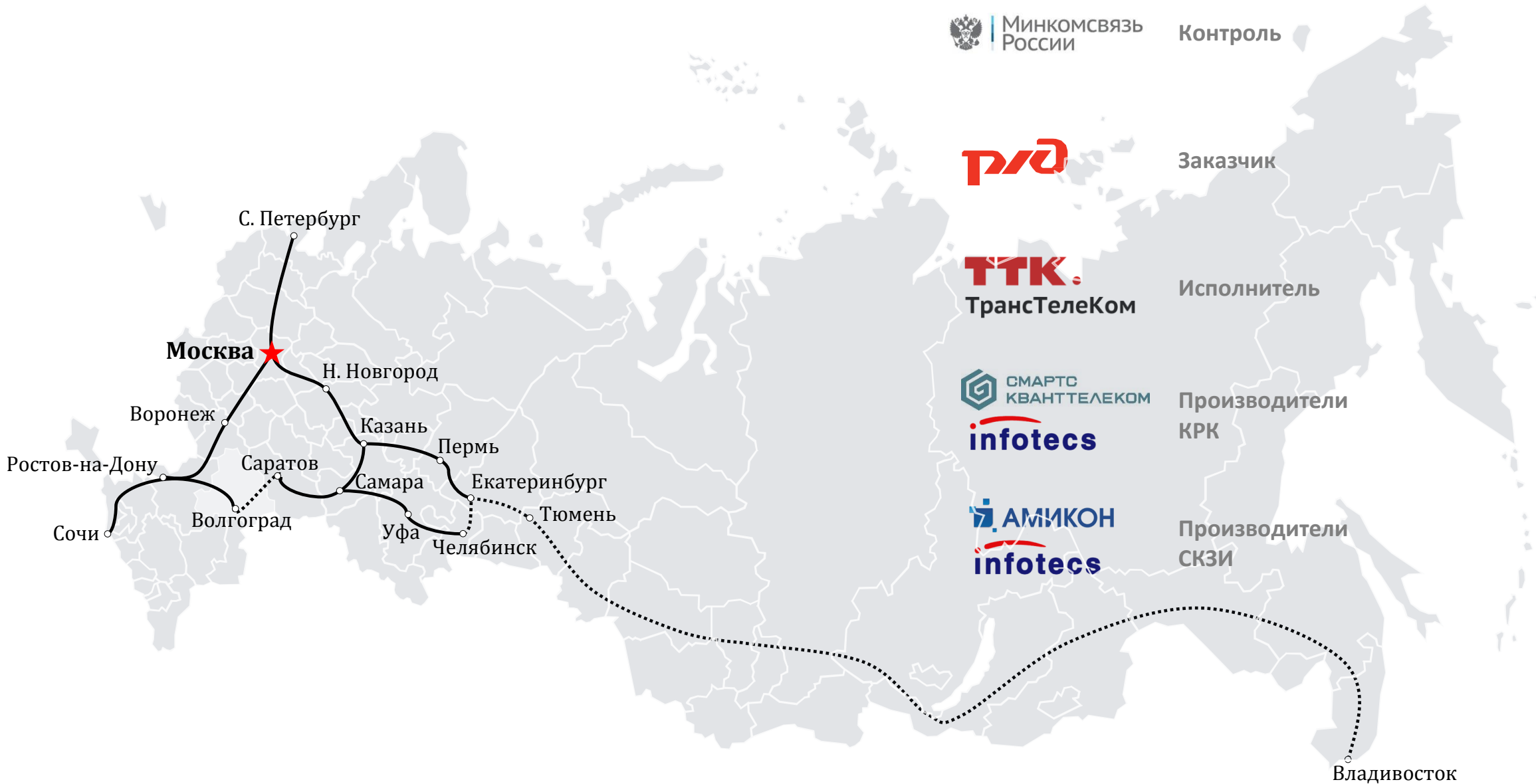
О развитии магистральной квантовой сети,
утвержденное Заместителем Генерального
директора-главным инженером
ОАО «РЖД» А.М. Храмцовым

ОКАЗАНИЕ УСЛУГ И СЕРВИСОВ НА БАЗЕ МКС

Распоряжение №3384р от 28.12.2024 г.

Об утверждении плана мероприятий
(«дорожной карты») по коммерциализации
магистральной квантовой сети ОАО «РЖД»,
утвержденное Генеральным директором
ОАО «РЖД» О.В. Белозеровым







КВАНТОВЫЙ VPN

Описание: комплексная услуга криптозащиты VPN трафика под ключ:

- Каналы связи необходимой пропускной способности;
- СКЗИ с поддержкой квантовозащищённого ключа;
- Оборудование для выработки и квантового распределения ключа (КРК).

Оборудование КРК и СКЗИ находятся на балансе оператора.

Тарификация:

- Разовый (инсталляционный) платеж (при необходимости);
- Ежемесячный платеж за аренду оборудования
- Ежемесячный платеж за аренду канала связи



КЛЮЧ КАК СЕРВИС

Описание: клиент сам приобретает необходимое оборудование.

Оператор осуществляет техническое присоединение к МКС и организацию служебного криптозащищенного) и квантового (темное волокно) каналов между КРК.

Оборудование КРК и СКЗИ находятся на балансе клиента.

Тарификация:

- Разовый платеж за техническое присоединение к МКС (при необходимости);
- Ежемесячные платеж за служебный канал.

Q&ATE

infotecs

СМАРТ
КВАНТТЕЛЕКОМ

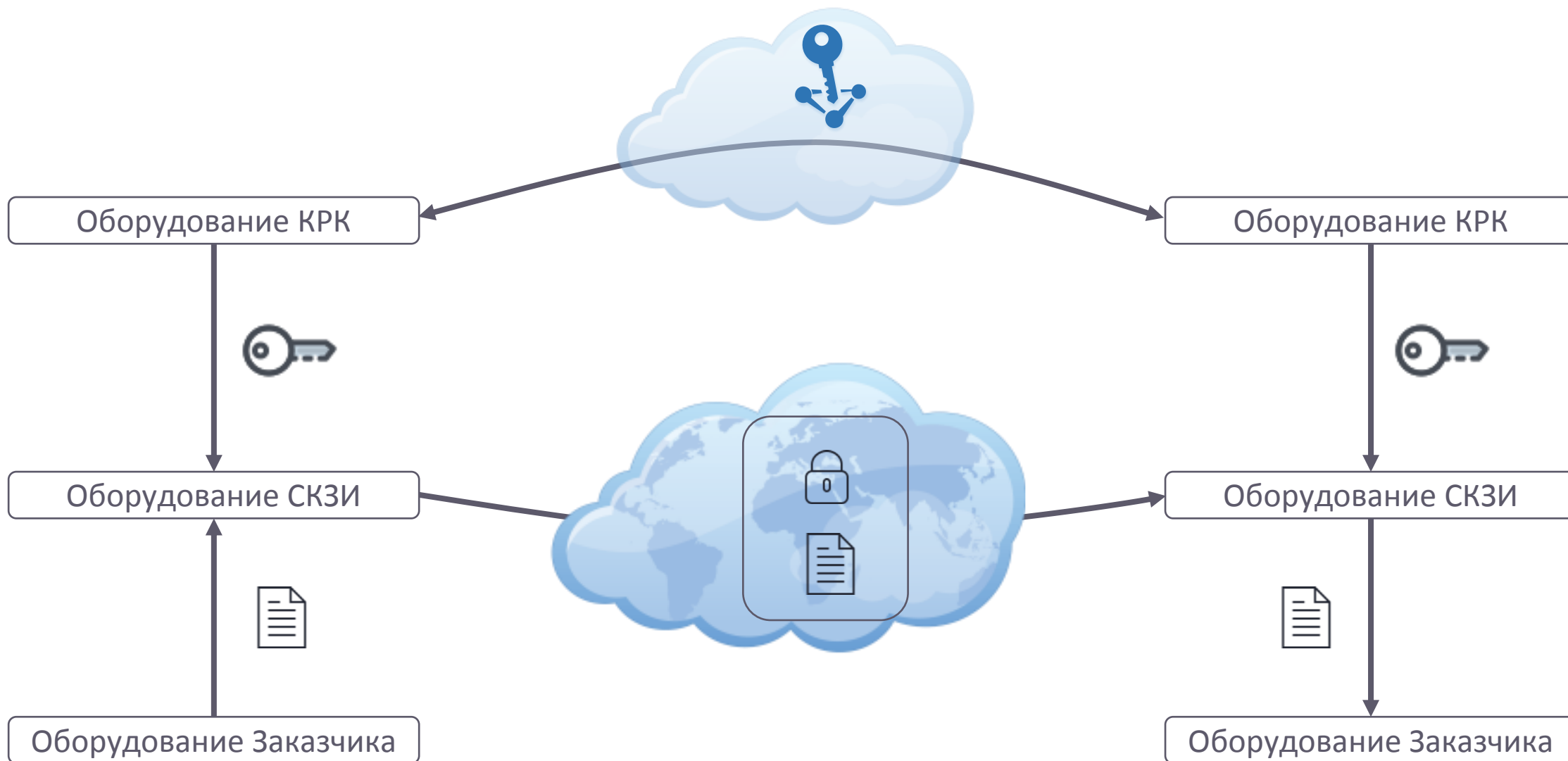


Схема 1. Прямое абонентское подключение

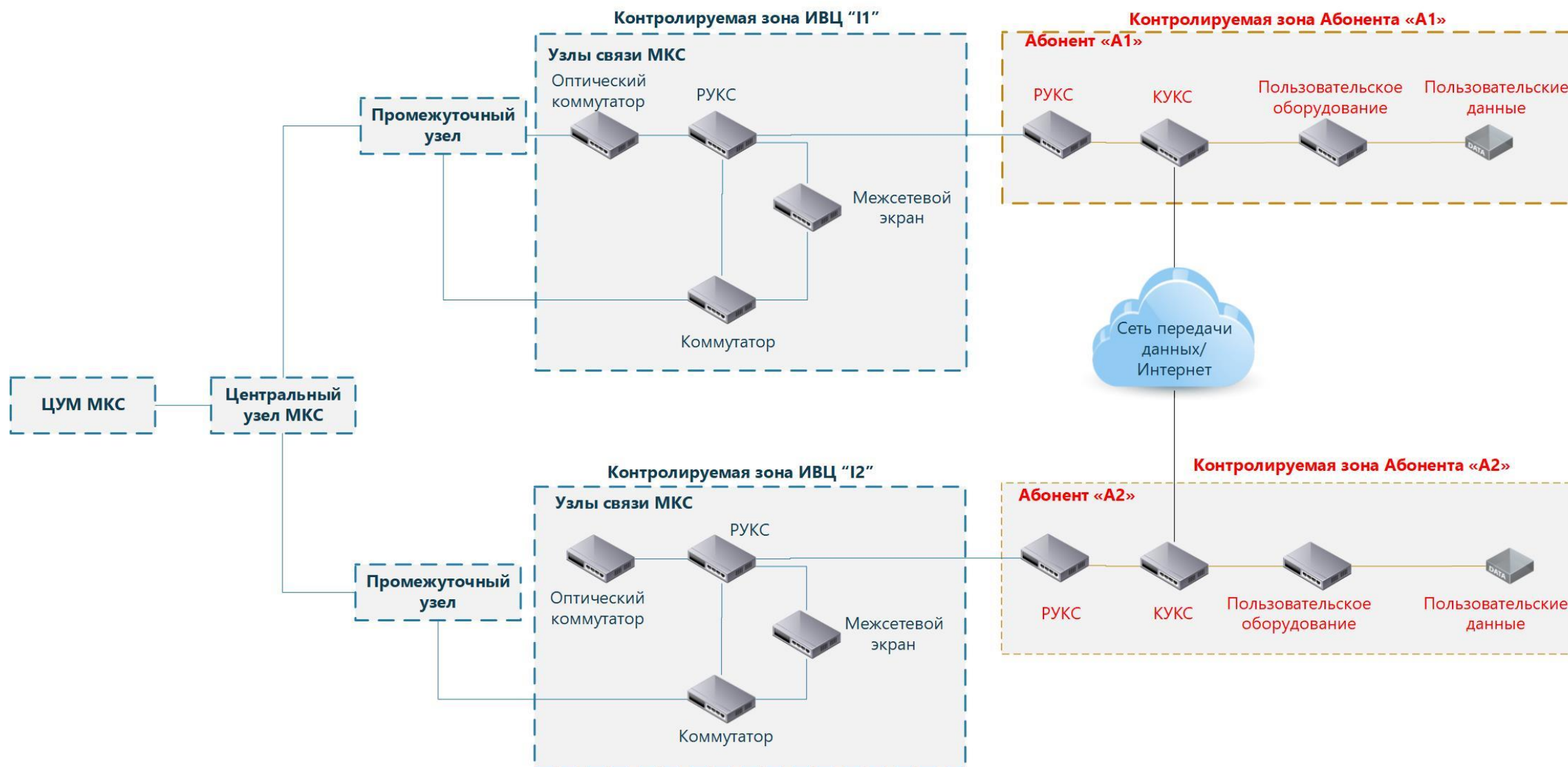
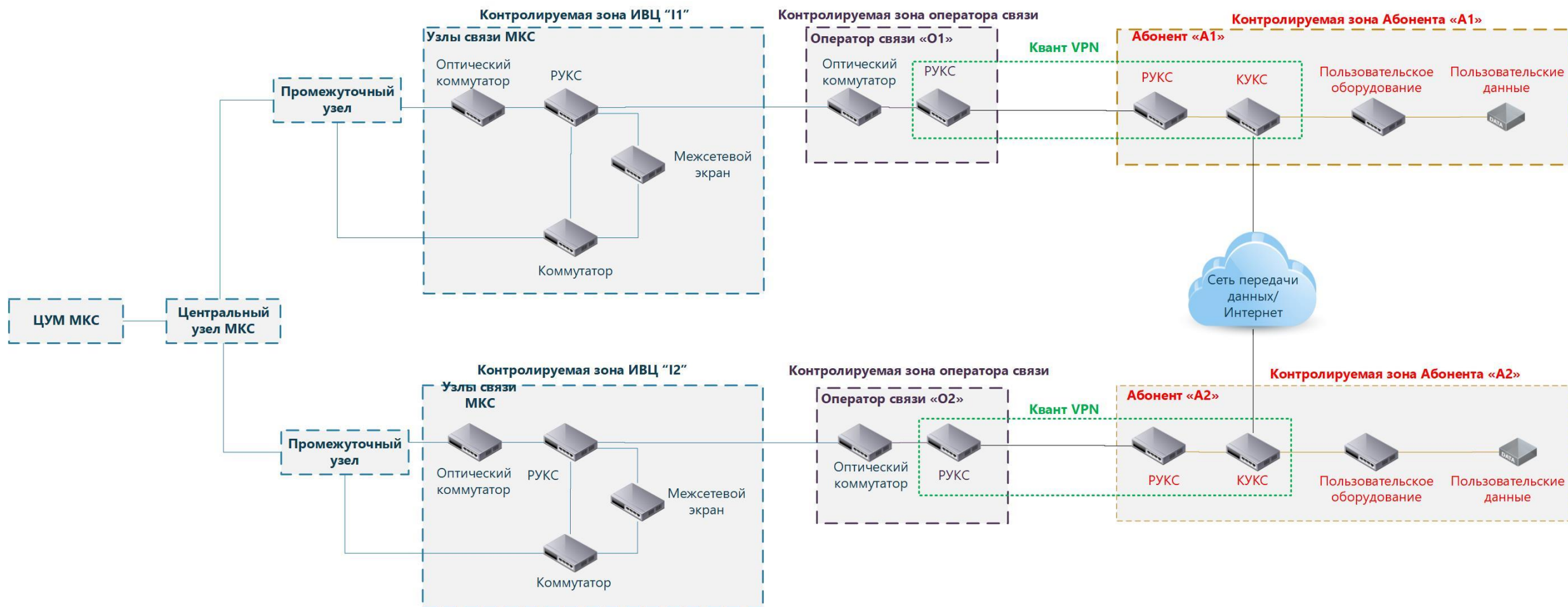


Схема 2. Подключение через оператора связи



Решение Комитета Совета Федерации по обороне и безопасности от 20.02.2024 г. «Обеспечение информационной безопасности с применением квантовых технологий в рамках национального проекта по формированию экономики данных на период до 2030 года»:

2.5. Федеральной службе безопасности Российской Федерации рассмотреть **необходимость уточнения требований по информационной безопасности с учетом использования технологий с квантовым распределением ключей.**

2.6. Государственным корпорациям «Ростех», «Росатом», «Роскосмос», ОАО «РЖД», ПАО «Ростелеком», ПАО «Газпром», ПАО «НК «Роснефть», ПАО «Транснефть», **ПАО «Россети», «ВЭБ.РФ», ПАО «Промсвязьбанк», ПАО «Сбербанк», ПАО «Интер РАО», ПАО «РусГидро», ПАО Банк «ВТБ», ПАО АФК «Система», АО «НСПК», другим заинтересованным структурам проработать вопросы использования в своей деятельности средств защиты информации на основе квантового распределения ключей в эксплуатируемых информационных системах и комплексах.**



Стратегия и план реализации стратегии развития отрасли связи до 2030 г.

обеспечить внедрение технологии квантового распределения ключей на основе российского оборудования в интересах государственного сектора и корпораций...

Отв. Минцифры России, ФСБ России



Россия в 2026 году примет международный форум по квантовым технологиям в рамках БРИКС

Участие в проекте по переходу на квантовозащищённые каналы связи может способствовать повышению имиджа Компании как инновационной и технологически продвинутой компании, а также привлечению внимания инвесторов, партнеров и клиентов



СОЗДАЕМ ЦИФРОВОЕ БУДУЩЕЕ **ВМЕСТЕ**

По вопросам подключения:
a.malyavkin@ttk.ru
info@ttk.ru