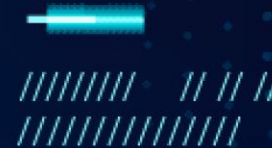




SMARTS
КВАНТТЕЛЕКОМ



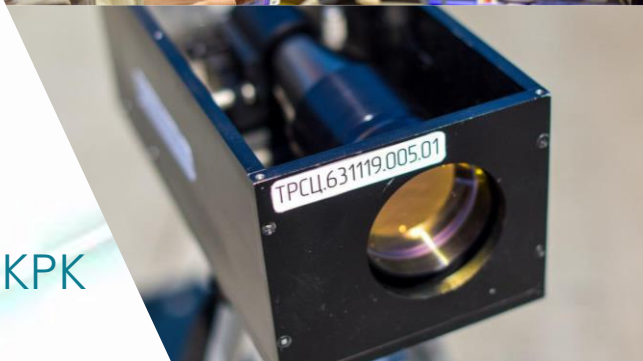
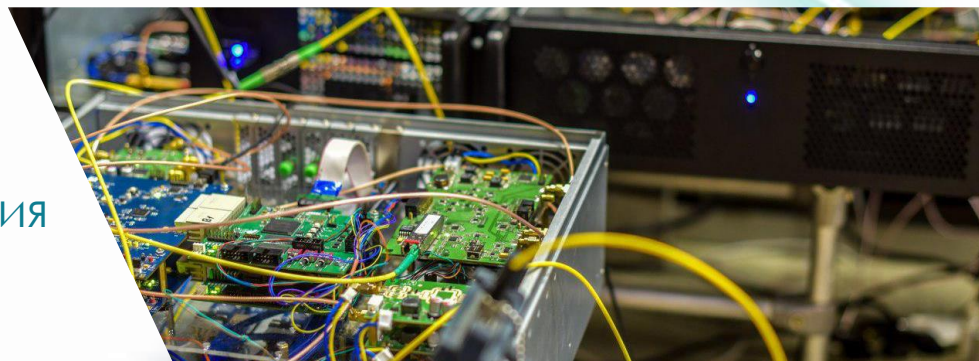
Разработки ООО «СМАРТС-Кванттелеком» в области квантовых коммуникаций



010010011011
011101010010



- 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



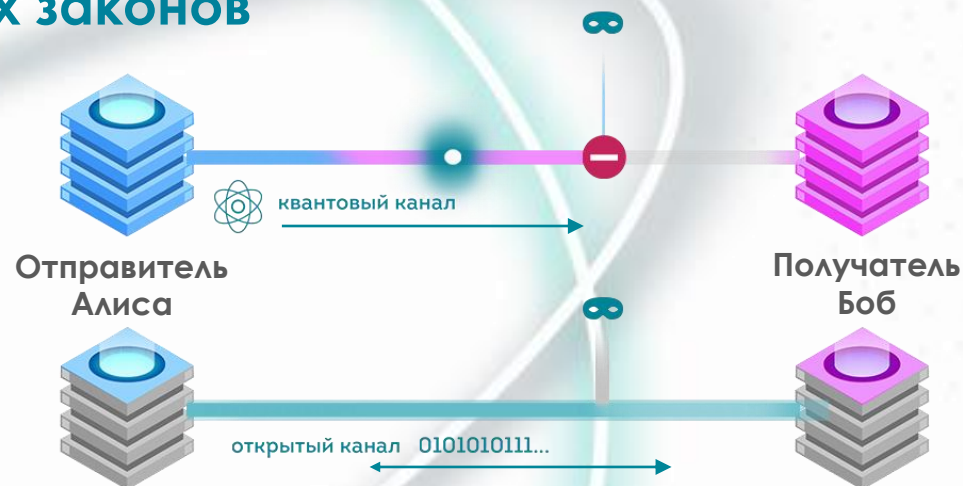
КВАНТОВЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ ВЫРАБОТКИ И РАСПРЕДЕЛЕНИЯ КЛЮЧА

Квантовый канал невозможно подслушать или «взломать» в силу физических законов

- Квантовое распределение ключа позволяет безопасно генерировать и передавать секретные ключи по методу одноразового блокнота на основе использования законов квантовой физики.
- Для создания ключа шифрования используются кванты света – фотоны
- В силу физических свойств фотоны:
 - разрушаются при измерении,
 - невозможно разделить
 - нельзя скопировать

Отправитель и получатель всегда будут знать, есть ли в канале нарушитель

- Путем измерения состояний фотонов получателем и сравнений их с данными отправителя формируется ключ необходимой длины, гарантированно известный только им.



Преимущества:

- Частая смена ключей. На одном сеансовом ключе шифруется гораздо меньше данных – даже при его «краже»;
- Автоматизация процесса управления ключами (снижается влияние человеческого фактора, высвобождаются человеко-часы и т.д.);
- Интегрируемость с существующими решениями в области безопасности;
- Регистрация попыток нарушения конфиденциальности передачи ключей;
- Защита от квантовых компьютеров.

ККС ВРК – СПОСОБ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ТЕОРЕТИЧЕСКОЙ СТОЙКОСТИ В СЕТЯХ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ



SMARTS
КВАНТТЕЛЕКОМ

Современные асимметричные криптоалгоритмы (RSA, протокол Диффи-Хеллмана, криптоалгоритмы на эллиптических кривых), и способные их заменить постквантовые асимметричные криптоалгоритмы имеют вычислительную стойкость.

Вычислительная стойкость – теоретический взлом криптоалгоритма возможен, но требует недостижимых вычислительных ресурсов или занимает длительное время, большее чем время актуальности информации.

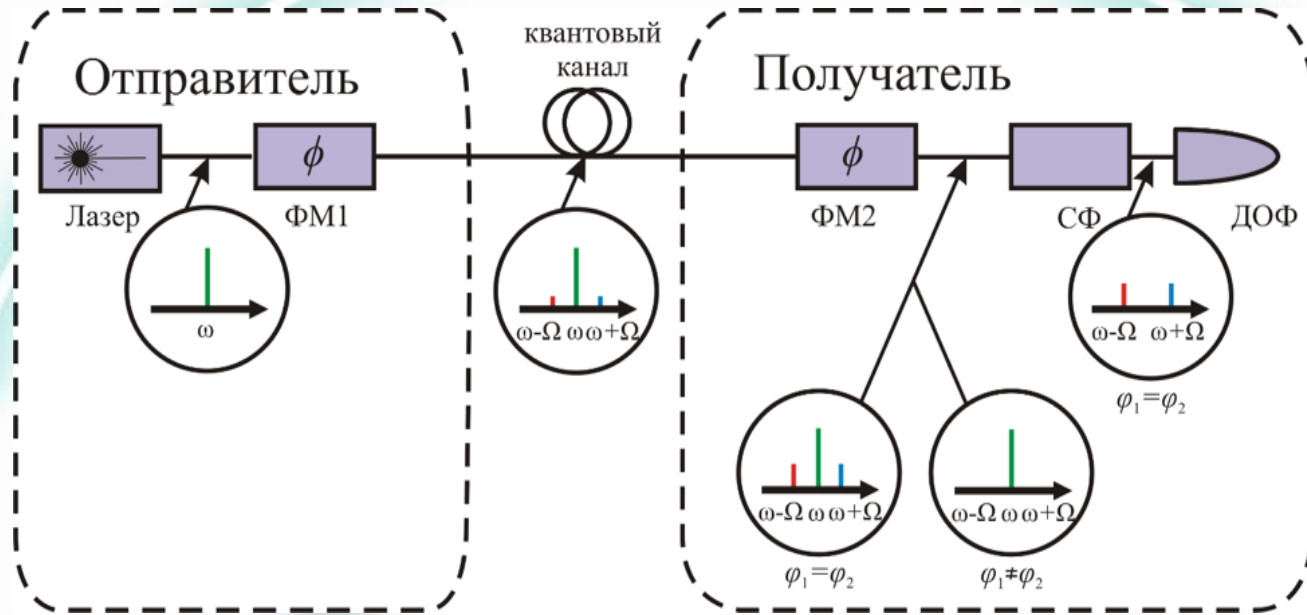
Постквантовые криптоалгоритмы также потенциально могут быть взломаны при появлении неизвестных ранее атак, не обязательно использующих квантовые методы. Например, в августе 2022 года было объявлено о взломе¹ алгоритма, который вошел в число победителей конкурса Национального института стандартов и технологий США на поиск криптоалгоритмов, устойчивым к квантовому компьютеру.

Для протоколов квантовой криптографии имеются доказательства информационно-теоретической стойкости, когда криптосистема не может быть раскрыта даже теоретически при неограниченных вычислительных возможностях.



Поскольку в специальных сетях связи риск утечки информации недопустим, необходимо использовать именно информационно-теоретически стойкие алгоритмы шифрования, в которых для обеспечения требований по частоте смены ключей необходимо использовать ККС ВРК.

СХЕМА ККБЧ И ФАЗОВЫЙ ПРОТОКОЛ BB84



Ю.Т. Мазуренко

Базис отправителя	[0;π]								[π/2;3π/2]							
	0				π				π/2				3π/2			
Фаза отправителя	0		π		0		π		π/2		3π/2		0		π	
Базис получателя	[0;π]		[π/2;3π/2]		[0;π]		[π/2;3π/2]		[0;π]		[π/2;3π/2]		[0;π]		[π/2;3π/2]	
Фаза получателя	0	π	π/2	3π/2	0	π	π/2	3π/2	0	π	π/2	3π/2	0	π	π/2	3π/2
Детектор получателя	+	-	+/-	+/-	-	+	+/-	+/-	+/-	+/-	+	-	+/-	+/-	-	+
Просеивание	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓
Сгенерированный бит	0				1				1				0			

ПРЕИМУЩЕСТВА СИСТЕМ НА БОКОВЫХ ЧАСТОТАХ (КБЧ)

Спектральная эффективность

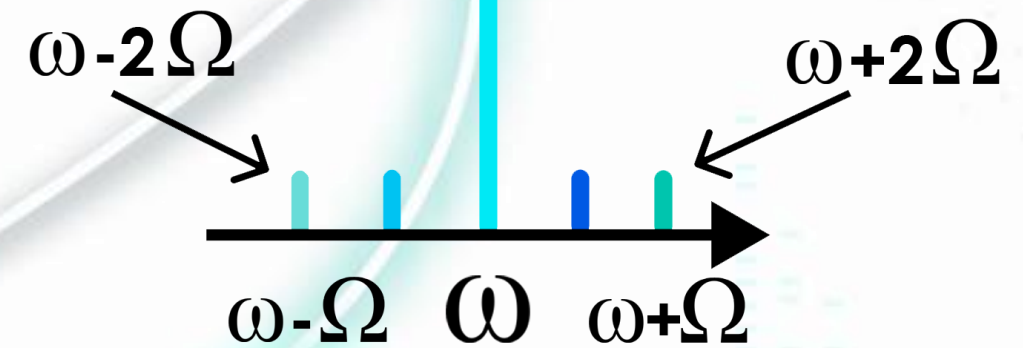
- Лучшие мировые системы КК: скорость 1-2 Мбит/с, 20 каналов DWDM = 40-80 Мбит/с, спектральная эффективность в канале с интерфейсом 1 Gbit Ethernet: 4-8%.
- Системы КБЧ позволят передавать до 10 независимых каналов [1] на каждой паре боковых частот (разнос каналов ~ 4 ГГц) внутри одного окна DWDM (разнос каналов ~ 100 ГГц)

Устойчивость к внешним воздействиям на канал

- Полная поляризационная независимость
- Работают в стандартных оптических волокнах
- Однонаправленная оптическая схема

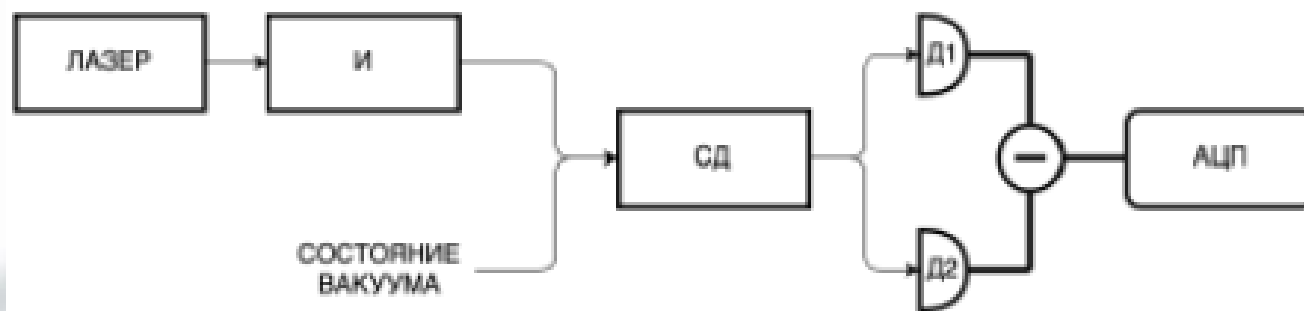
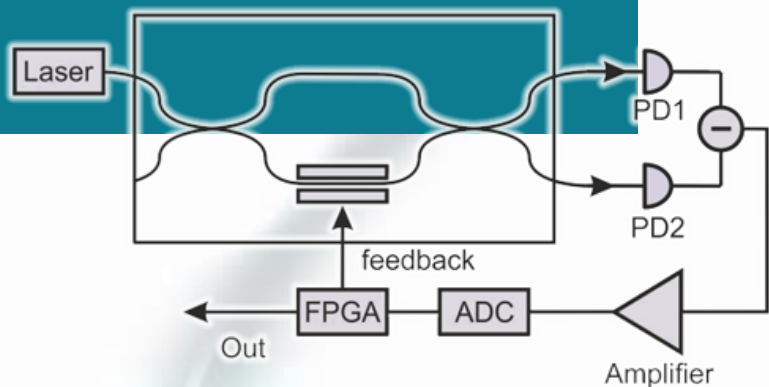
Гибкость

- На основе метода могут быть реализованы разные протоколы
- Технические параметры не ограничены архитектурой системы



Принцип работы:

В нашем решении мы используем в качестве источника энтропии флуктуации вакуума для достижения наиболее высоких скоростей и удобства использования. Процесс постобработки применяется для повышения случайности последовательности.



Л – лазер; И – изолятор; СД – светоделитель; Д1, Д2 – детекторы; АЦП – аналого-цифровой преобразователь.

Область применения

- Информационные системы, реализующие различные статистические методы и методы стохастического моделирования
- Электронные игровые платформы
- Системы информационной безопасности

Преимущества

- Высокая скорость генерации случайных чисел
- Интегрально-оптическая реализация
- Источник энтропии – вакуумные флуктуации
- Скорость генерации от 300 Мб/с до 3 Гб/с
- Рабочий диапазон температур от -25 до 70°C



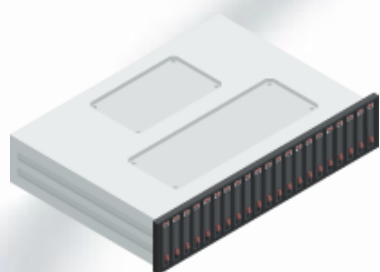
КРК



**ККС ВРК
«КВАКС»**



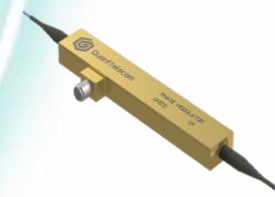
**Абонентский
модуль**



ПДУ



**Детектор
одиночных
фотонов**

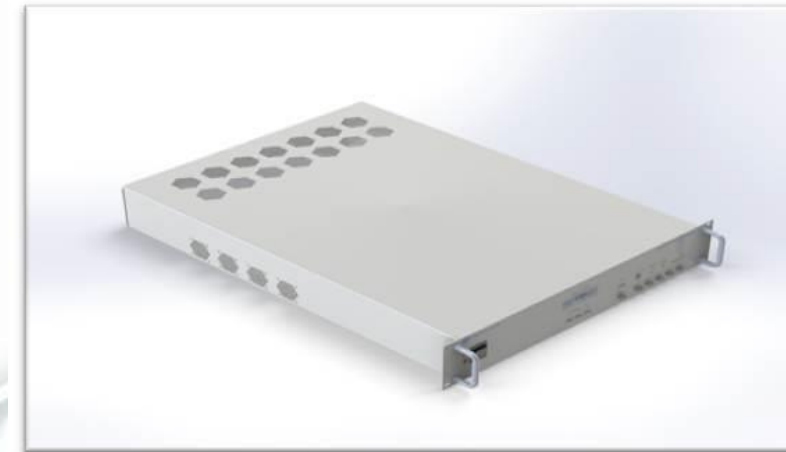
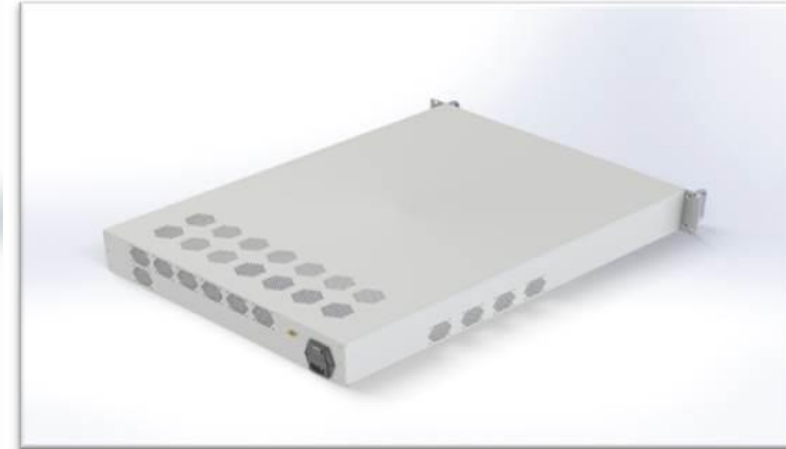


**СВЧ интегрально-
оптические
модуляторы**



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: 6%
- Локальное управление/мониторинг: да (ПК, разъем подключения 1Гбит/сек, RJ45)
- Габариты: 19" 2U 600x175x436 (без учета ручек на фронтальной панели)



ОБОРУДОВАНИЕ ДЛЯ КВАНТОВЫХ СЕТЕЙ

КВАНТОВАЯ КРИПТОГРАФИЧЕСКАЯ СИСТЕМА «МШ-ТР-КРК»



SMARTS
КВАНТТЕЛЕКОМ

Основные параметры и характеристики МШ-ТР-КРК

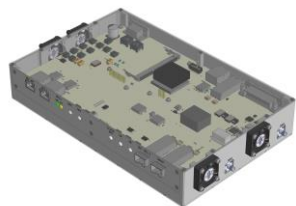
- Клиентские интерфейсы (Клиент): 10 Gbit Ethernet или 8 Gbit FC, модуль SFP+
- Линейные интерфейсы (Канал): 2xOTU2e, модуль SFP+
- Линейные интерфейсы КРК: КК-1 Gbit Ethernet, тип FC, СК-1 Gbit Ethernet, модуль SFP+
- Производительность при передаче: 10 Gbit/s Ethernet или 6, 8 Gbit/s FC
- Скорость генерации КК 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



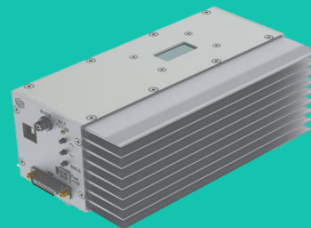
ОСНОВНЫЕ УЗЛЫ ККС



SMARTS
КВАНТТЕЛЕКОМ



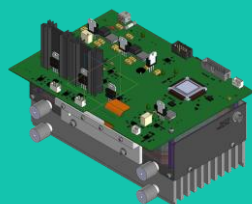
Блок управления



Детектор одиночных фотонов



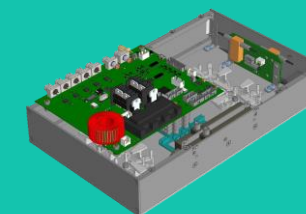
Корпус комплекса



Блок генерации излучения



СВЧ интегрально-оптические модуляторы



Оптический модуль и плата

РАЗРАБОТКИ «СМАРТС-КВАНТТЕЛЕКОМ»

Детектор одиночных фотонов



СМАРТС
КВАНТТЕЛЕКОМ

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

Характеристики:

Квантовая эффективность:

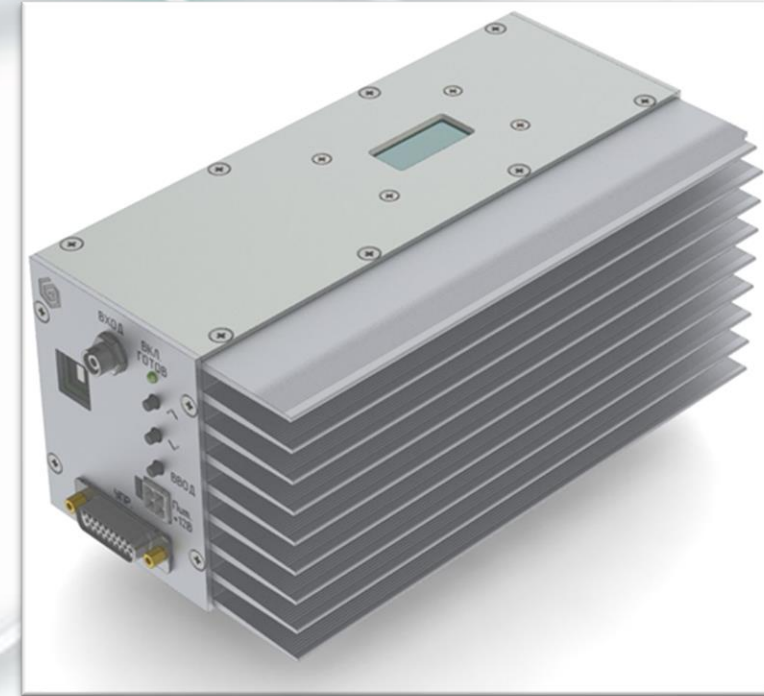
не менее 10% (настраиваемое значение, до 20% с шагом 2,5%).

Вероятность темнового отсчета :

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

Максимальная частота повторения импульсов запуска :

300 МГц.



Составная часть	Импортный образец	Отечественный аналог
Лазерный модуль	Neophotonics TTX1995Micro-ITLA-15.5 (США) Teraxion PS-LM-1550 (Канада)	Нолатех TLD-1550-14BF-10 (Москва) Нолатех DFB-1550-14BF-10 (Москва) Плата управления на основе МК Миландр
Волоконные фильтры на основе ВБР	Teraxion PWS-NLS-1550-0.05-99.9-CMS-P5-1 (Канада)	ВБР GTL-FBG-AD-810 НЦВО-Фотоника, Москва ВБР GTL-FBG-AD-820 НЦВО-Фотоника, Москва
Интегрально-оптические модуляторы	EOSPACE PM-0S5-10-PFA-PFAP (США) Thorlabs LN56S (США) iXBlue MX-LN-10-PD-P-P-FA-LIL (Франция)	Модулятор интенсивностей ИОМ-01-40 ПИКВ.433731.001 (Пермь, АО ПНППК) Фазовые и амплитудные модуляторы ГРТВ.433731.001 и ГРТВ.433733.001 (ООО «СМАРТС-Кванттелеком, СПб)
Микроконтроллеры	STM32F100	K1986BE92QI (АО Миландр, Зеленоград)
Лавинные фотодиоды	Wooririo SPAD with Internal TEC (Южная Корея)	Разрабатываются в кооперации: ООО «СМАРТС-Кванттелеком» ООО «Коннектор-Оптикс» (СПб), АО «ОКБ Планета» (Великий Новгород)

РАЗРАБОТКИ «СМАРТС-КВАНТТЕЛЕКОМ»

СВЧ интегрально-оптические модуляторы



СМАРТС
КВАНТТЕЛЕКОМ

- Телекоммуникация
- Квантовое распределение ключей

Характеристики:

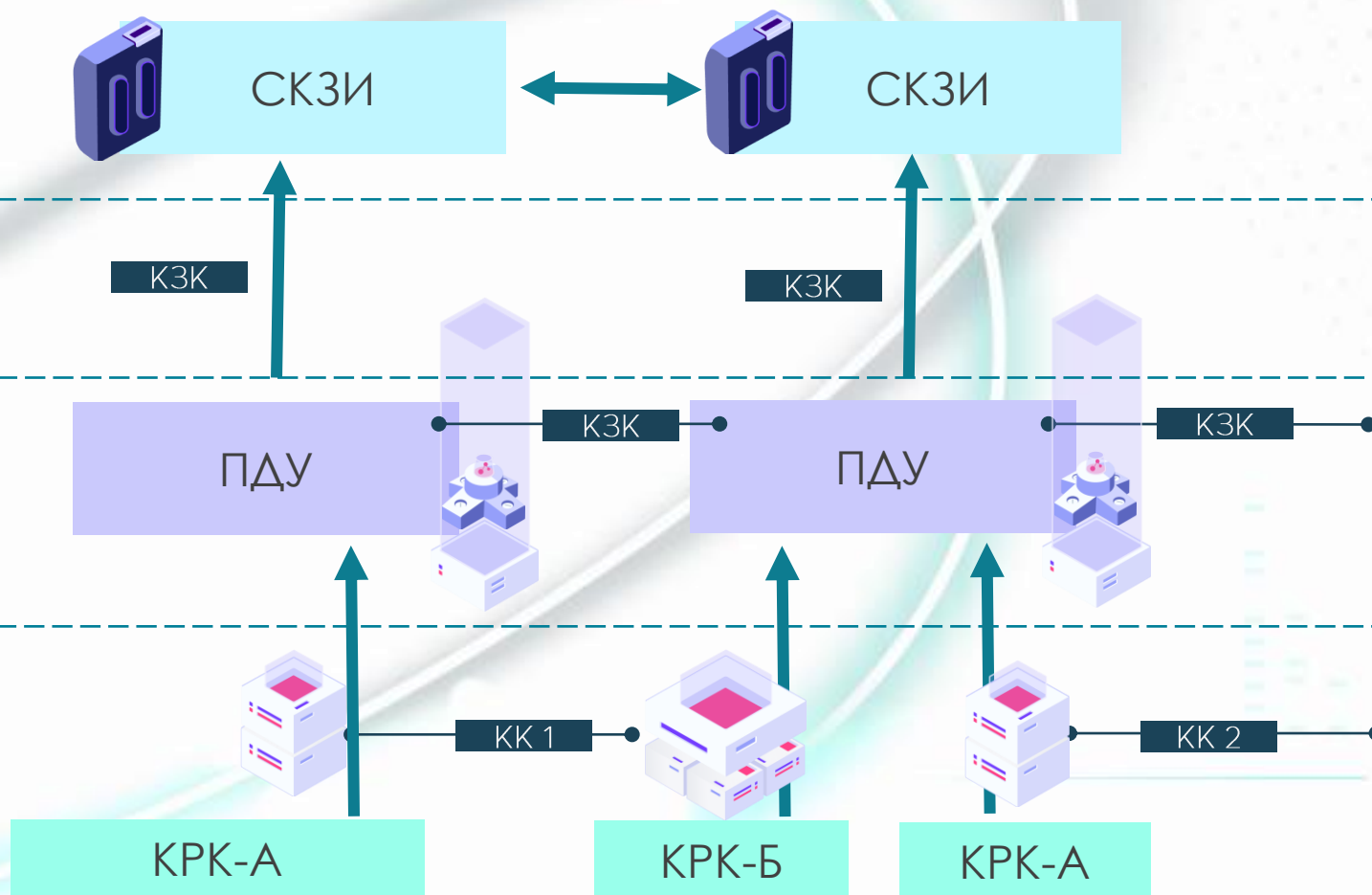
- Рабочая длина волны (тип.): 1520-1560 нм
- Электрооптическая полоса пропускания: до 40 ГГц
- Вносимые потери (тип.): 4 дБ
- Возвратные потери (макс): 50 дБ
- Оптическая входная мощность (макс.): 100 мВт
- V_p напряжение RF: <5 В
- Оптический разъем: FC/APC, с сохранением поляризации



Квантовый ключ, как услуга

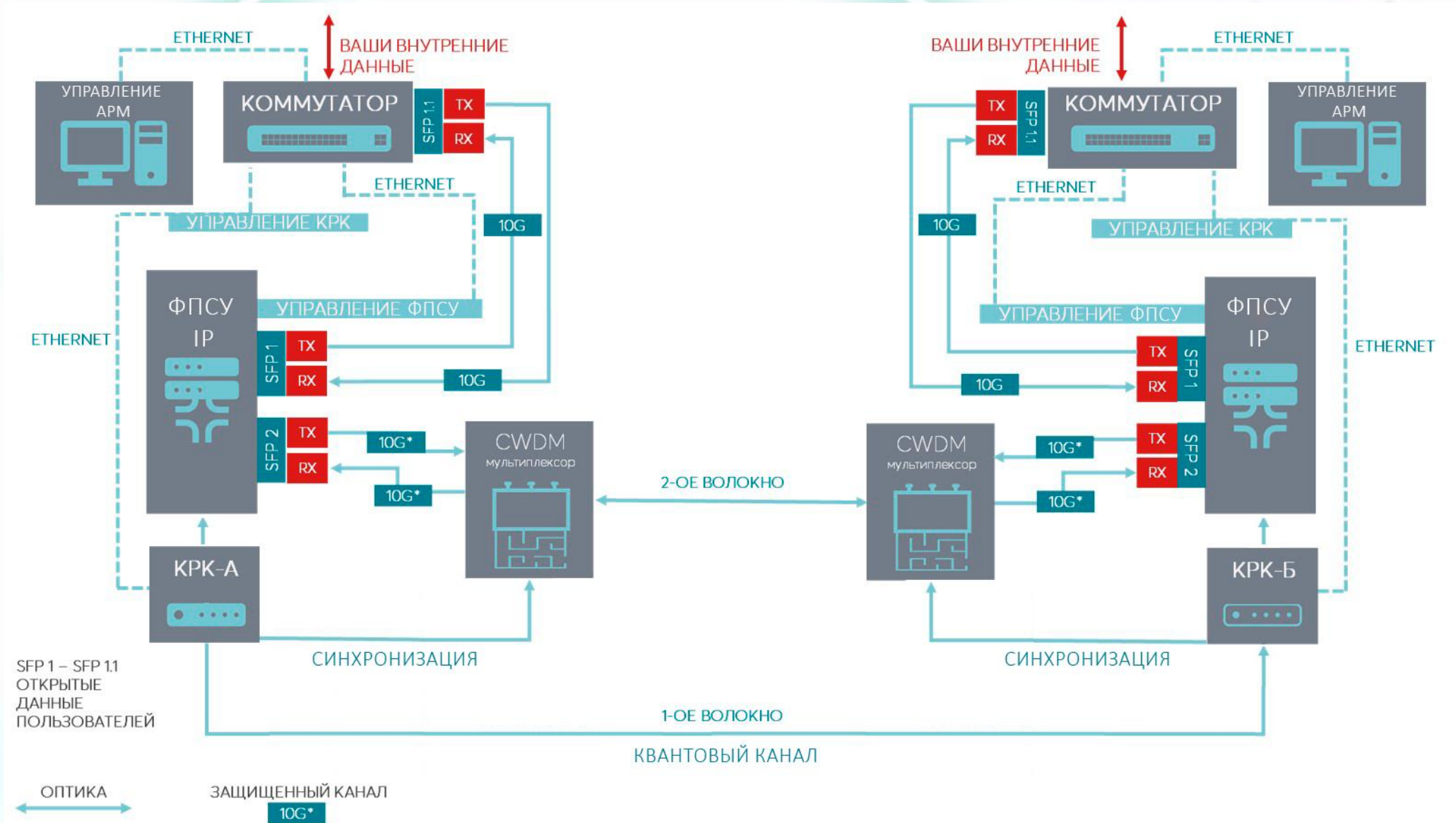
Уровни

- 1 ВЫДАЧА КК. ПОЛУЧЕНИЕ КЛЮЧЕЙ ОТ УСТРОЙСТВ КРК
- 2 АДМИНИСТРАТОР КК. ХРАНЕНИЕ КВАНТОВЫХ КЛЮЧЕЙ В ПДУ
- 3 ИНТЕРФЕЙС. ПЕРЕДАЧА КВАНТОВЫХ КЛЮЧЕЙ ПОТРЕБИТЕЛЯМ МС ОТ ПДУ
- 4 ИСПОЛЬЗОВАНИЕ КЛЮЧЕЙ КОНЕЧНЫМИ ПОТРЕБИТЕЛЯМИ МАГИСТРАЛЬНОЙ СЕТИ (МС) КК



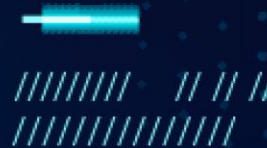
Сеть 3-го типа
(«Квантовый»)

ПОСТРОЕНИЕ КВАНТОВОЙ ПЕРЕДАЧИ ДАННЫХ





SMARTS
КВАНТТЕЛЕКОМ



Контактная информация

Генеральный директор ООО «СМАРТС-Кванттелеком»
Алексеев Алексей Леонидович

📍 199178, Санкт-Петербург, В.О., 6 линия д.59, корп. 1, лит. Б

📞 +7 (812) 244-29-23

✉ a.alekseev@quanttelecom.ru



quanttelecom.ru

010010011011
011101010010