



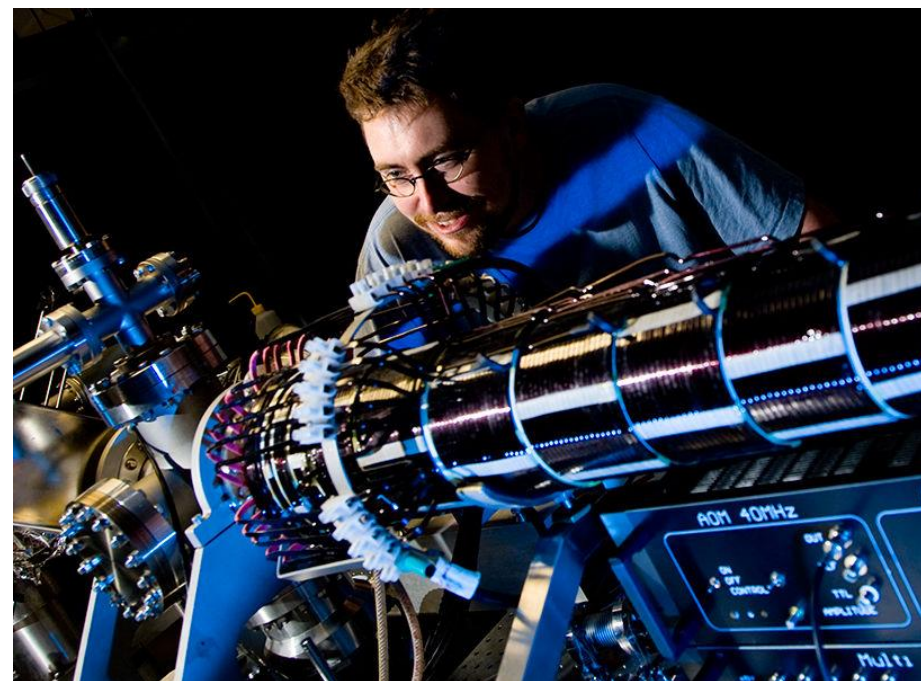
**SMARTS
КВАНТТЕЛЕКОМ**

Защищенная квантовая коммуникация в волоконно- оптических сетях

Глейм Артур Викторович
Генеральный директор, к.т.н.

Близкая угроза

"Защитный потенциал большинства современных систем обеспечения безопасности информации находится под угрозой в связи с потенциально возможным появлением в ближайшей и среднесрочной перспективе квантовых компьютеров. Их вычислительный ресурс должен быть несравнимо выше, чем у классических", — констатировал начальник Главного управления развития информационных и телекоммуникационных технологий Минобороны генерал-майор Олег Масленников в ходе форума "Инфофорум-2018".



В ожидании...

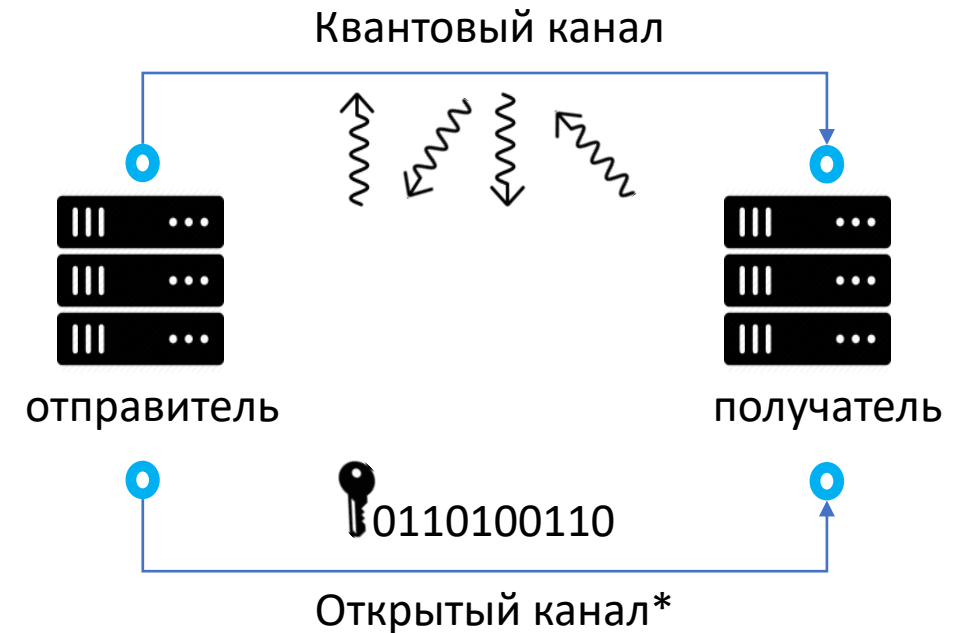
Если информацию нельзя взломать прямо сейчас, то ее можно расшифровать в будущем — например, с помощью квантовых компьютеров.



Дата-центр АНБ предназначен **для взлома** закодированных данных. Потенциальный объем информации, который может быть размещен в этом дата-центре, ошеломляет. По оценке экспертов, центр строится для обработки в будущем **йоттабайт(!)** данных.

Физика на страже

- Для генерации ключей шифрования используются кванты света - фотоны;
- В силу физических свойств фотонов (разрушаются при измерении, невозможно разделить и скопировать неизвестное состояние) – отправитель и получатель в процессе передачи всегда будут знать, есть ли в канале связи «нарушитель», который пытается украсть данные;
- Путем измерения состояний фотонов получателем и сравнений их с данными отправителя, формируется закрытый ключ шифрования необходимой длины (равной длине сообщения), известный только им.



Квантовые инфраструктуры в мире

Крупнейшие многоузловые квантовые сети созданы в США (разработка Управления перспективных исследовательских проектов Министерства обороны США (DARPA)), Европе (SEQOQC), Японии (Сеть Токио, разработчик – компания Toshiba), Китае

Американский

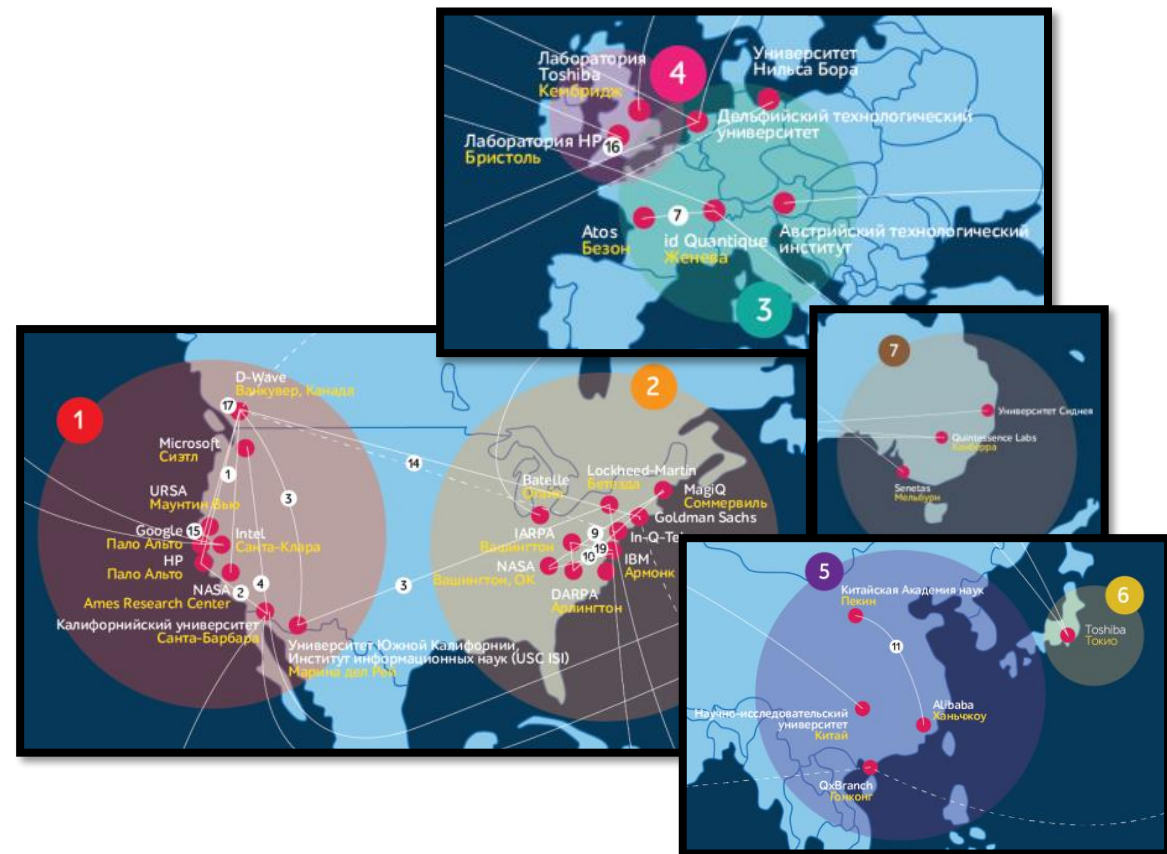
1 Европейский

2 Британский

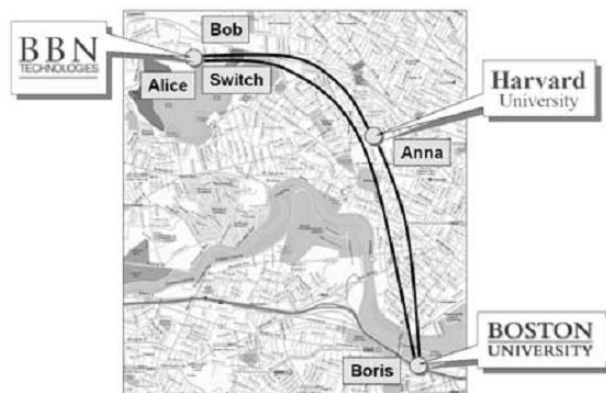
3 Китайский

4 Японский

5



Квантовые сети в мире



Darpa, США

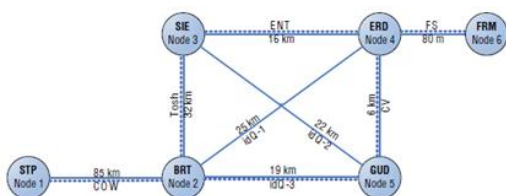
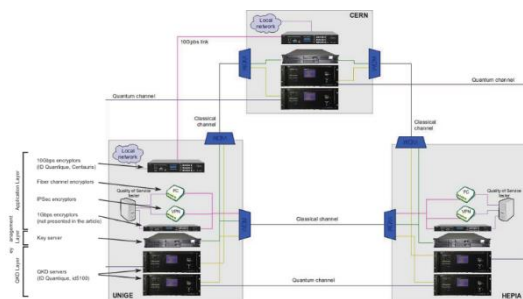


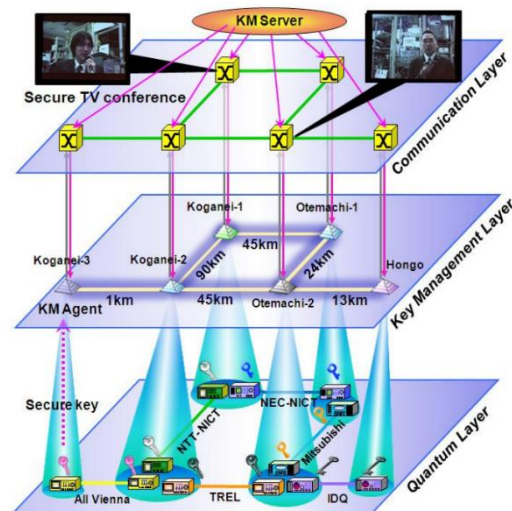
Figure 2. Network topology of the SECOQC KKD network prototype. Solid lines represent quantum communication channels, dotted lines denote classical communication channels.



SECOQC, ЕС



Swiss-quantum, Швейцария

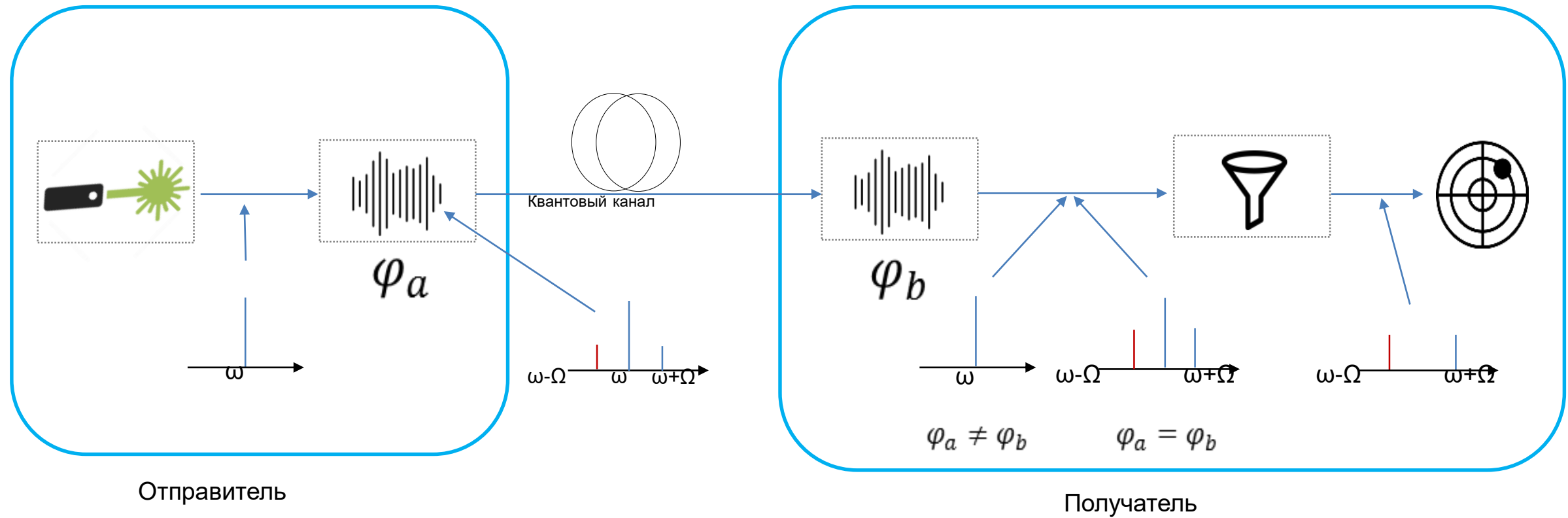


Токио QKD, Япония



Beijing-Shanghai, Китай

Квантовая коммуникация на боковых частотах

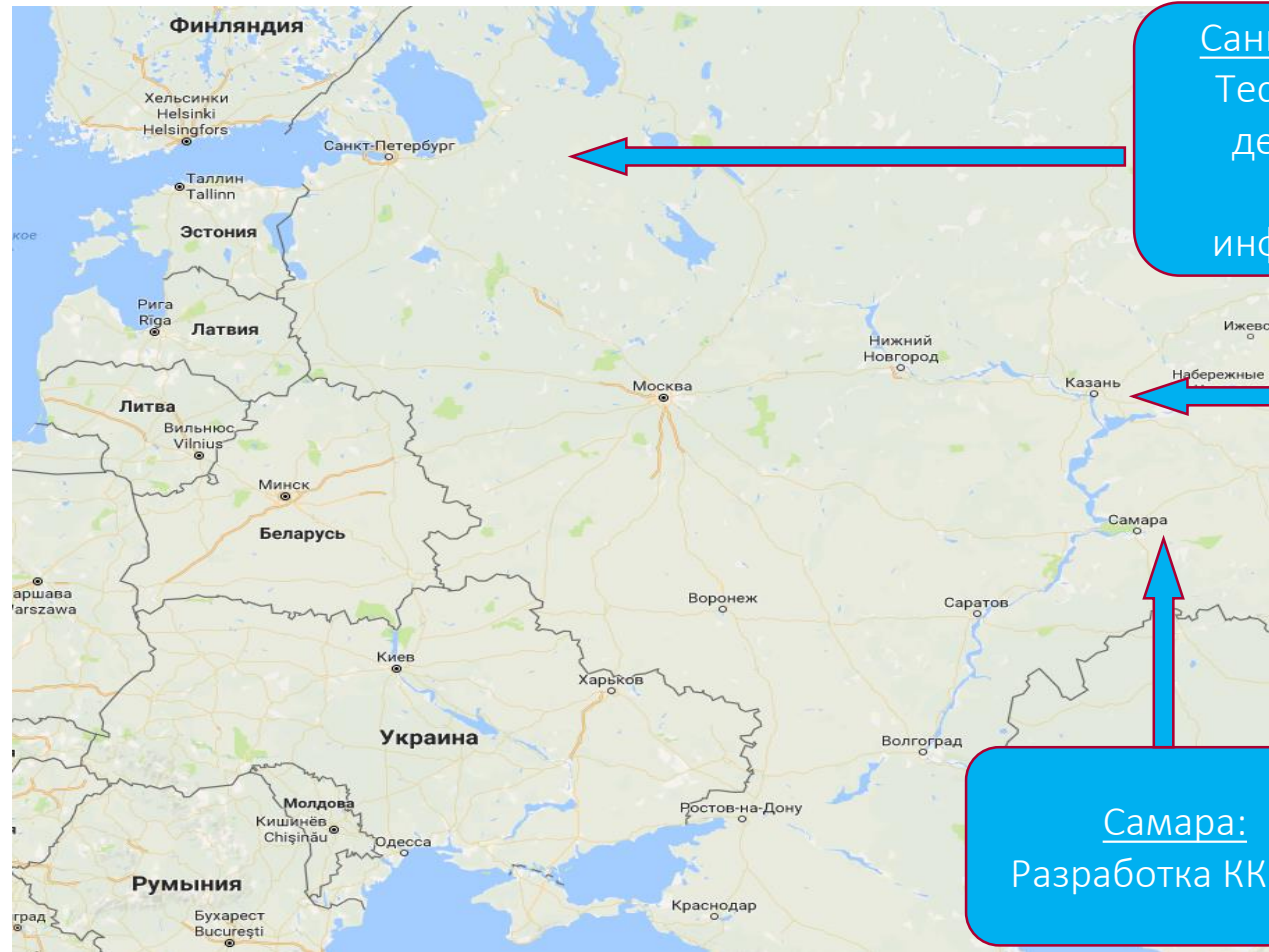


Шлюз защищенной передачи данных

- Скорость генерации квантового ключа: до 10 кбит/с
- Частота обновления ключа до 10 раз в секунду
- Скорость передачи данных 10 Гбит/с
- Поддержка протоколов OTN, TCP/IP, UDP
- Предельные потери в оптическом канале: 39 дБ (230 км)
- Спектральный диапазон C (1530 .. 1565 нм)
- Тип волокна: SMF-28e или аналогичное
- Интерфейс подключения: fc/арс
- Частота импульсов: 100 МГц
- Шифратор на основе системы КВАЗАР



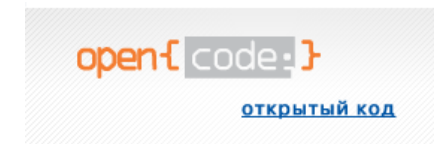
Испытательные полигоны квантовых сетей



Санкт-Петербург:
Тестирование в
действующей
телеком.
инфраструктуре

Казань:
Разработка
многоузловой сети

Самара:
Разработка ККПКС

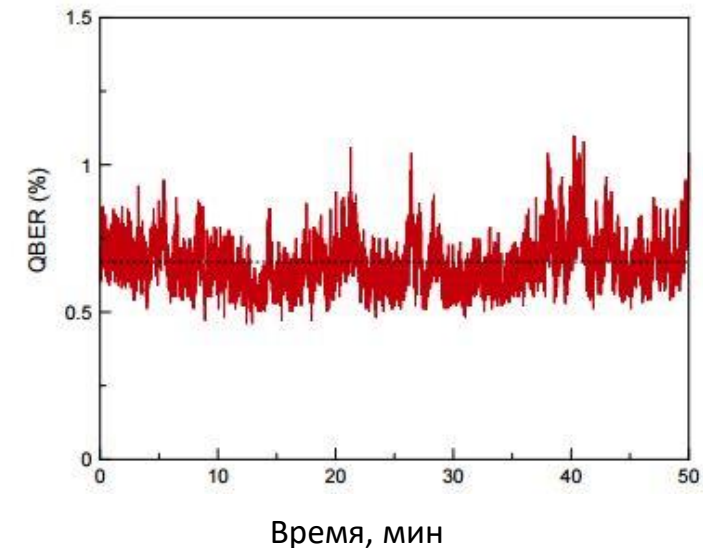


Местоположение ключевых проектов

Испытательный полигон системы ККБЧ



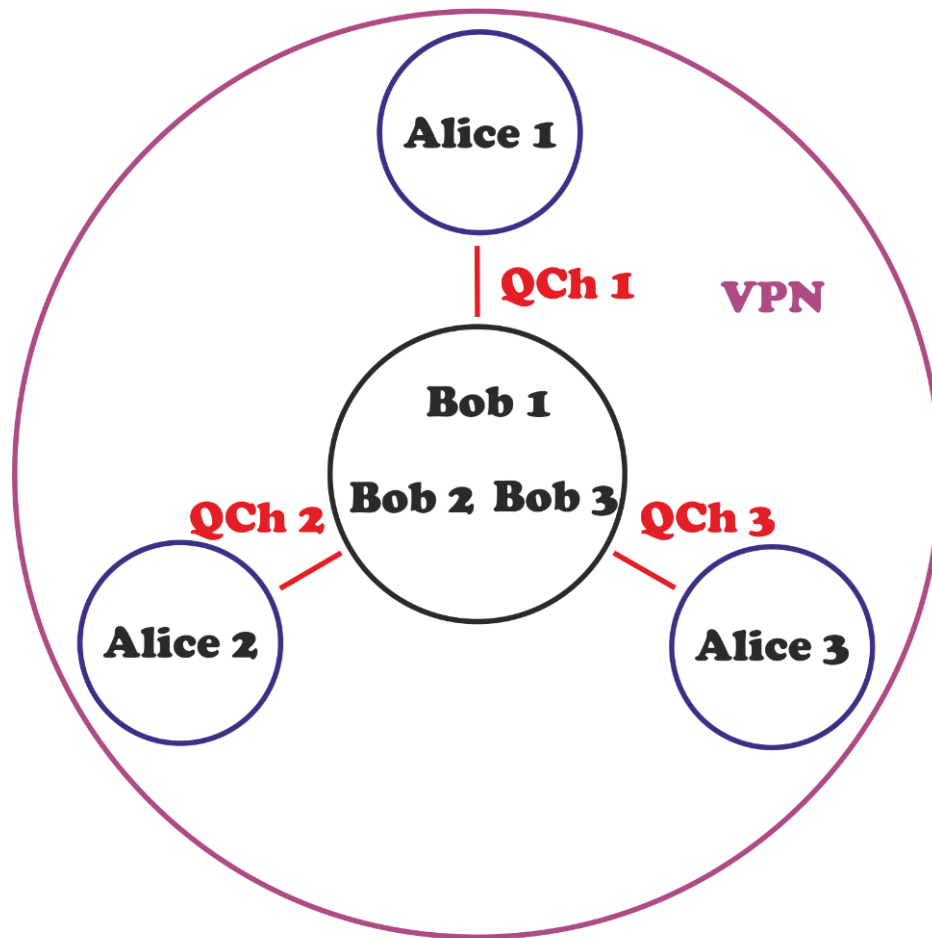
Схема участка сети между корпусами Университета ИТМО на Биржевой линии В.О., д.16 и Кадетской линии В.О., д.3Б



Технические параметры:

- Расстояние: 1 км
- Потери в линии: 1,6 дБ
- Скорость генерации просеянного ключа: 1 Мбит/с
- Скорость генерации секретного ключа: 100 кбит/с
- QBER: 1%
- Тип волокна – Smf-28e
- Длина волны излучения: 1550 нм

Архитектура сети и расположение узлов



***QCh - Quantum Channel**

***VPN - Virtual Private Network**

логическая схема сети в Казани



Расположение узлов сети

1 линия

- Длина волокна: 9,4 км
- Потери в линии: 7 дБ
- Скорость генерации секретного ключа: 0,6 кбит/с
- QBER: 3,7%

2 линия

- Длина волокна: 12,4 км
- Потери в линии: 7 дБ
- Скорость генерации секретного ключа: 0,5 кбит/с
- QBER: 4,5%

3 линия

- Длина волокна: 2,5 км
- Потери в линии: 1 дБ
- Скорость генерации секретного ключа: 6 кбит/с
- QBER: 3,5%

Детектор: APD

- Квантовая эффективность: 10 %
- Частота темновых срабатываний: 1 кГц
- Тип волокна: Smf-28e
- Длина волны: 1550 нм

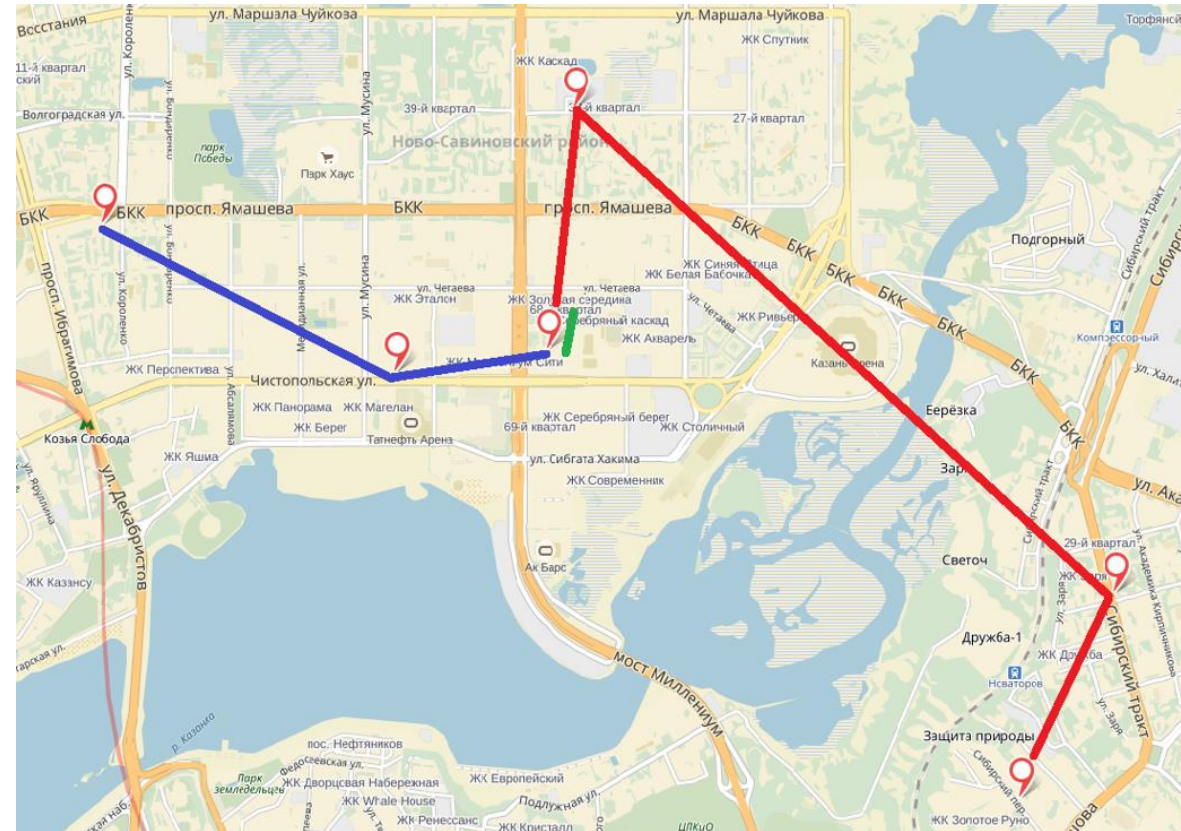


Схема многоузловой квантовой сети



ITMO UNIVERSITY



Kazan
Quantum
Center



Рефлектограммы сети

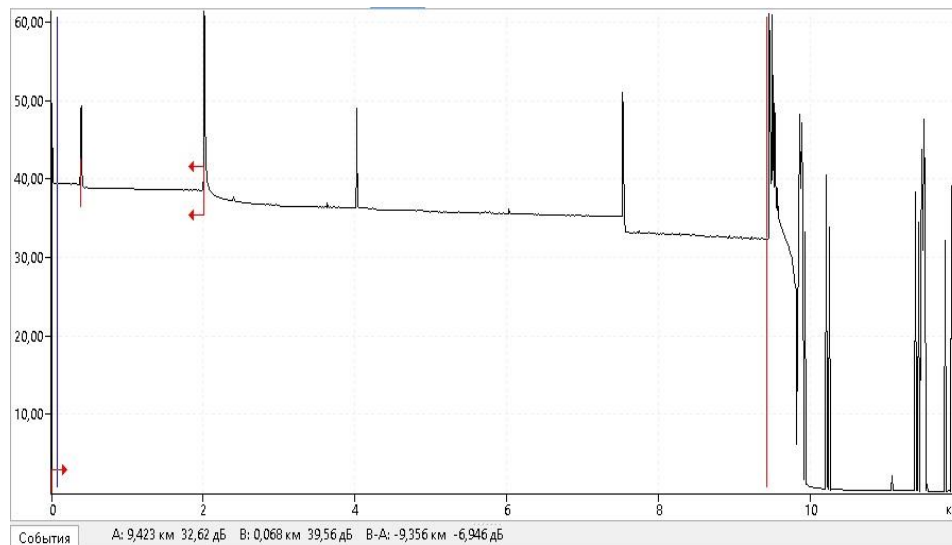


Рис.2. Участок Ершова 57В – Четаева 18А

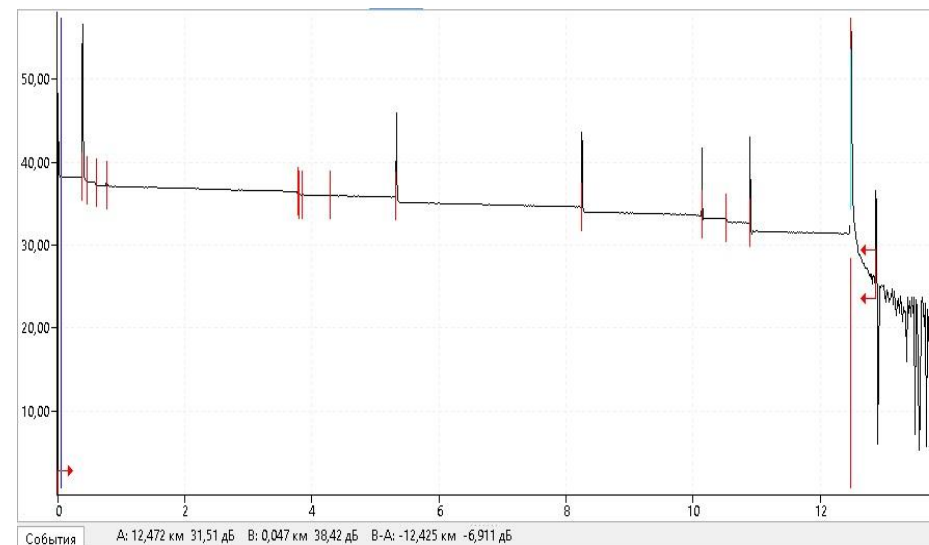


Рис.3. Участок Лаврентьева 3 - Четаева 18А

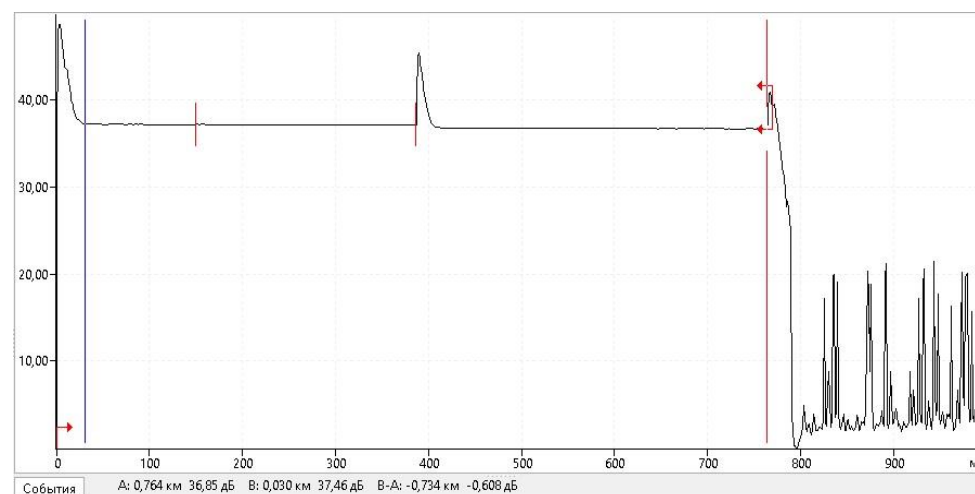
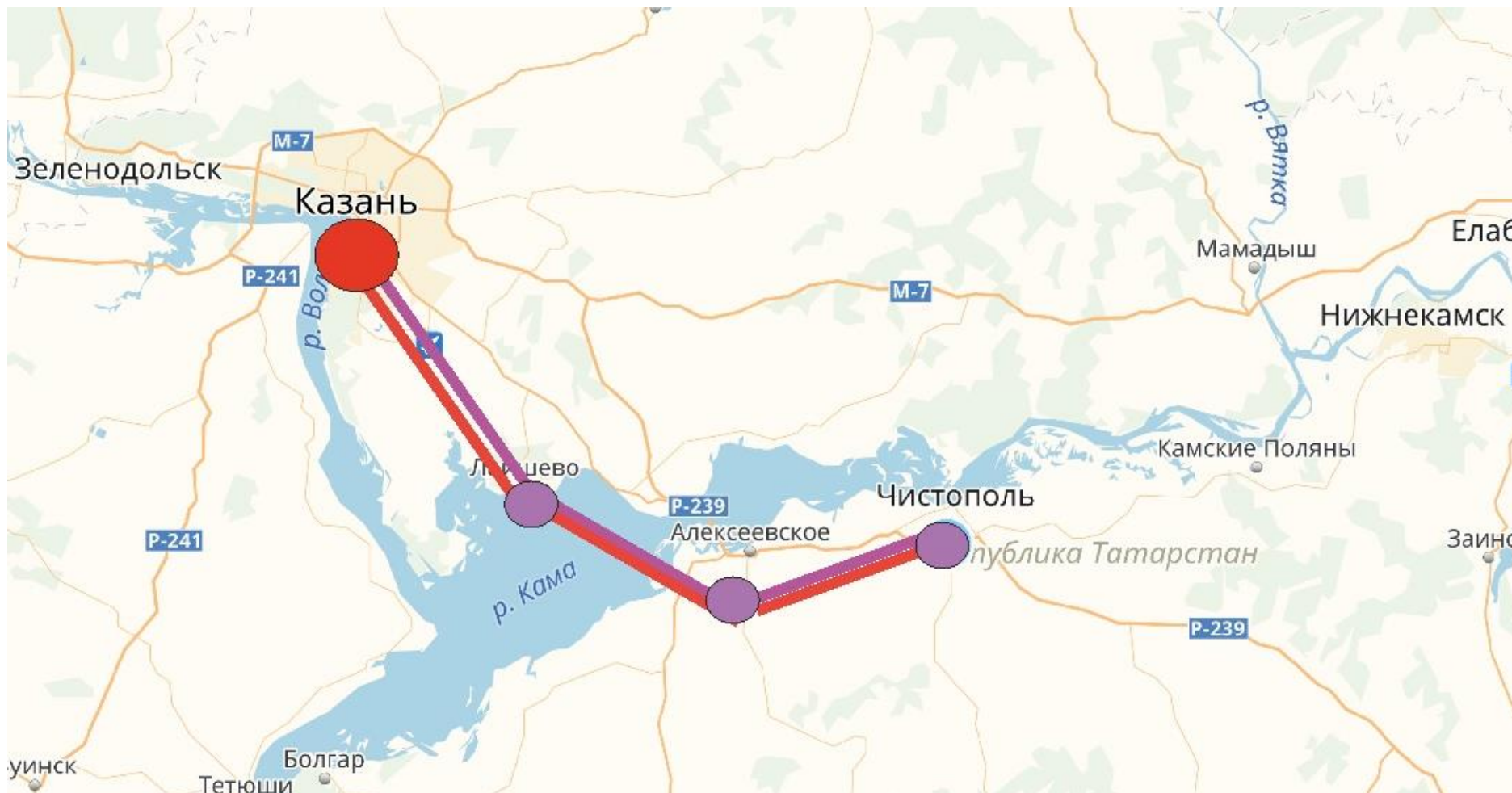


Рис.4. Участок Четаева 18 – Четаева 18А



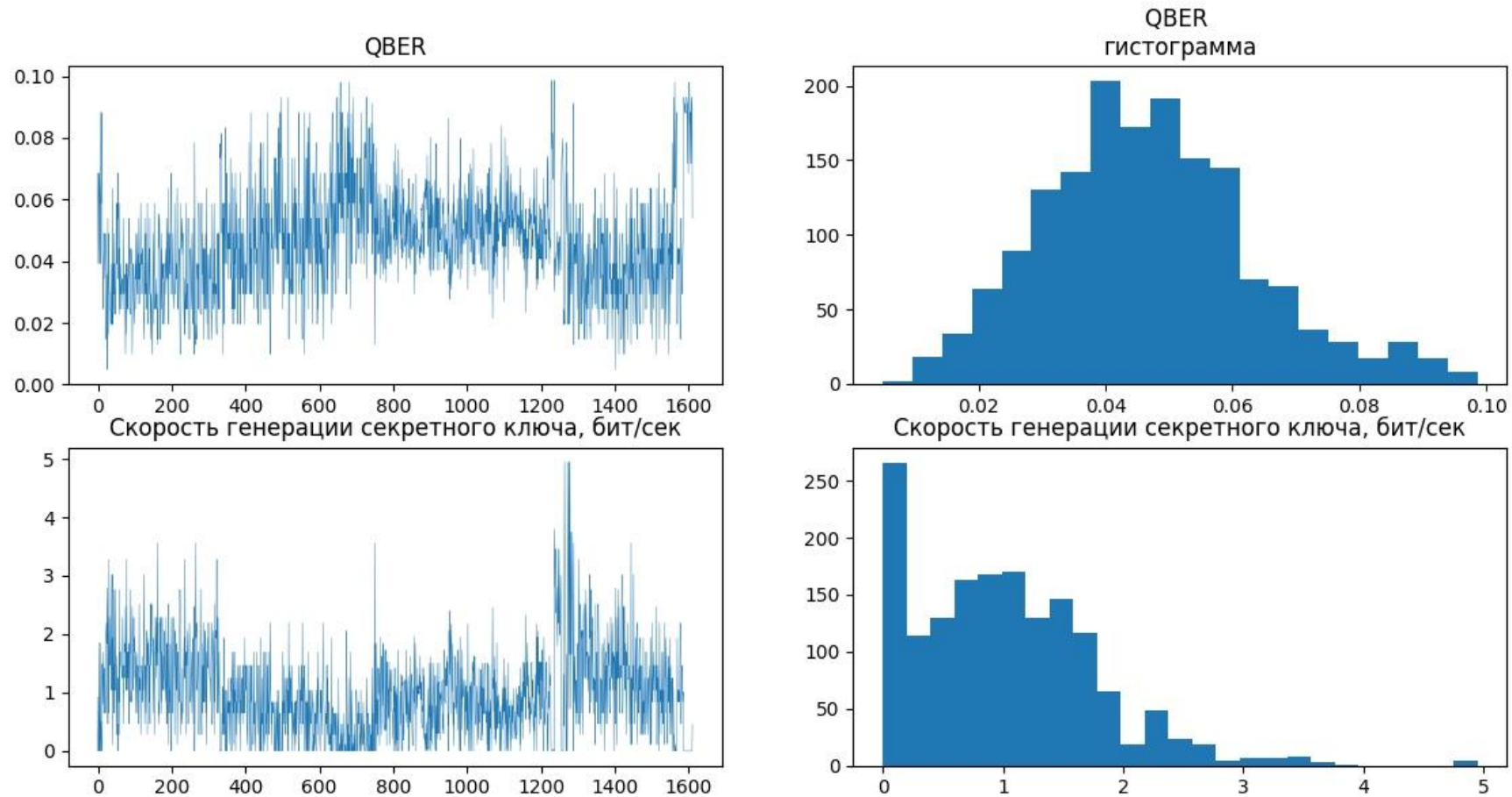
Магистральная квантовая сеть Казань-Чистополь



Узел 1: Казань, КНИТУ-КАИ
Узел 2: Чистополь, Таттелеком

Длина ВОЛС: 160 км
Потери в ВОЛС: 45 дБ

Результаты измерений



Средняя скорость генерации секретного ключа: 1-2 бит/с

Средний коэффициент квантовых ошибок: 5-6%



Длина волокна 300 км
Потери 50 дБ



Длина волны: 1550.12 нм
Ширина спектра лазера: 1 МГц
Индекс модуляции: 0.05
Суммарная мощность: 51,4 пВт
Среднее число фотонов: 0,2
Частота модуляции: 4.8 GHz
Частота смены фазы: 100 МГц
Синхронизация: 100 МГц
Потери в приемном блоке: 6,4 дБ
Потери в оптическом канале: 45 дБ
Видность интерференции 99,3%
Квантовая эффективность SNSPD: 50%
Темновой счет: 0,5 Гц

Независимые испытания

- Ростелеком
- Россети
- ФСО России
- Сбербанк
- Таттелеком

ПРОТОКОЛ № 10						
приемочного испытания по пунктам № 4.1.1 - 4.1.8						
Программы и методики приемочных испытаний						
опытного образца Изделия (ККС) №1.1						
ДШВА.201119.001						
№ 10						
«04» июня 2013 г.						
1. Объект испытания: опытный образец Изделия №1.1 в количестве (1) шт.,						
2. Цель испытания: проверка соответствия объекта испытания требованиям пункта №						
№5.2.3.3 и 5.8.2.5 технического задания:						
Разрабатываемое Изделие должно обеспечивать следующие параметры:						
1) Скорость передачи данных на длине линии 100 км, не менее 10 кбит/с						
2) Квантовый коэффициент ошибок по битам (QBER), на длине линии 100 км, не						
более 0,5%						
3) Скорость передачи данных на длине линии 200 км, не менее 0,1 кбит/с						
4) Квантовый коэффициент ошибок по битам (QBER), на длине линии 200 км, не						
более 2%						
5) Скорость передачи данных на длине линии 25 км, не менее 100 кбит/с						
6) Квантовый коэффициент ошибок по битам (QBER), на длине линии 25 км: не более						
0,5%.						
7) Среднее число фотонов на один передаваемый бит, не более 0,6.						
8) Используемый протокол кодирования BB84						
3. Дата начала испытания: «03» июня 2013 г						
4. Дата окончания испытания: «04» июня 2013 г						
5. Место проведения испытания: ЗАО «СКОНТЕЛ», г. Москва, ул. Малая Пироговская						
д.29, стр.1						
6. Результаты испытания						
Наименование параметра	Ед. изм.	Номера пунктов		Требования к параметру		Измеренное значение
		Программы испытаний	Методик испытаний	Номинальное значение	Предельное отклонение	
Скорость передачи данных на длине линии 100 км, не менее	Кбит/с	4.1.1	6.1	10	-	91 кГц
Квантовый коэффициент ошибок по битам (QBER), на длине линии 100 км, не более	%	4.1.2	6.2	0,5	-	0,45%
Скорость передачи данных на длине линии 200 км, не менее	Кбит/с	4.1.3	6.3	0,1	-	8,3 кГц
Квантовый коэффициент ошибок по битам (QBER), на длине линии 200 км, не более	%	4.1.4	6.4	2	-	1,5%
Скорость передачи данных на длине линии	Кбит/с	4.1.5	6.5	100	-	200 кГц

25 км, не менее							
Квантовый коэффициент ошибок по битам (QBER), на длине линии 25 км, не более	%	4.1.6	6.6	0,5	-	0,04%	-
Среднее число фотонов на один передаваемый бит, не более		4.1.7	6.7	0,6	-	153 пВ	0,26
Используемый протокол кодирования		4.1.8	6.8	BB84	-	BB84	-
Вероятность безотказной работы, не менее	%	4.1.9.1 .1	6.9	95	-	-	96%
Средняя наработка на отказ, не менее	Час.	4.1.9.1 .2	6.10	3000	-	-	84000
Среднее время восстановления, не более	Час.	4.1.9.1 .3	6.11	2	-	-	1,5
Разрабатываемое Изделие должно монтироваться в стандартный шкаф типоразмера	мм	4.1.10	6.10	2180 x800 x1000		2182 x803 x1005	-

7. Выводы

7.1 Объект испытания – опытный образец Изделия (ККС) №1.1 - выдержал испытание по пунктам № 4.1.1 - 4.1.8 Программы и методики приемочных испытаний опытного образца Изделия ДШВА.201119.001.

7.2 Объект испытания полностью соответствует требованиям пункта №№ 5.2.3.3 и 5.8.2.5 технического задания.

7.3 Программа испытаний выполнена полностью.

Испытание проводили

Инженер-исследователь А.А. Корнеев

Ведущий специалист А.В. Антипов

В приложении к протоколу испытаний

Исполнитель

Система передачи данных

Связь с использованием IP-телефонов Grandstream:

Аудиосвязь 32 кбит/с

Видеосвязь 2 Мбит/с



Спасибо за внимание!

ООО «Кванттелеком»
Глейм Артур Викторович
agleim@qcrphotonics.com