



# Современные тенденции развития квантовых коммуникаций и перспективы построения масштабируемых квантовых сетей

Олег Иванов

Менеджер продуктов  
АО «ИнфоТеКС»



# Угрозы передаваемой информации



Y

X

Z

Раскрытие секретной информации

Время

«Store Now – Decrypt Later»

**перехват** зашифрованных данных, чтобы взломать их позже, когда появятся квантовые компьютеры.

X – срок актуальности информации, в течение которого информация должна оставаться защищённой

Y – время внедрения новой технологии

Z – время до появления ожидаемой угрозы

# Проблемы классической криптографии



## Нагрузка на ключ

размер сообщения, которое можно надёжно зашифровать на криптографическом ключе. Классическое решение проблемы ограниченной нагрузки на ключ – построение дерева производных ключей



## Защита от чтения вперёд/назад

новые криптографические ключи должны быть независимы от старых криптографических ключей, а старые — от новых



## Утечка по побочным каналам

многократное применение одного и того же ключа вызывает скоррелированное э/м и акустическое излучение



## Защита от внутреннего нарушителя

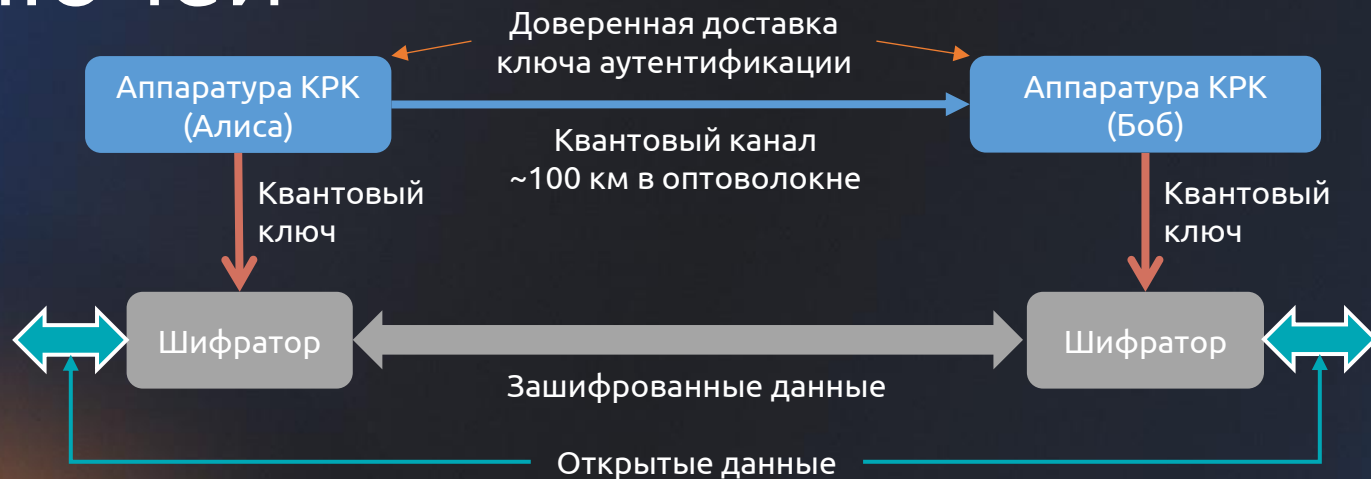
доставка ключей курьером, удостоверяющий центр PKI требуют доверия к третьей стороне

Ampire 360°

Квантовое  
распределение  
ключей



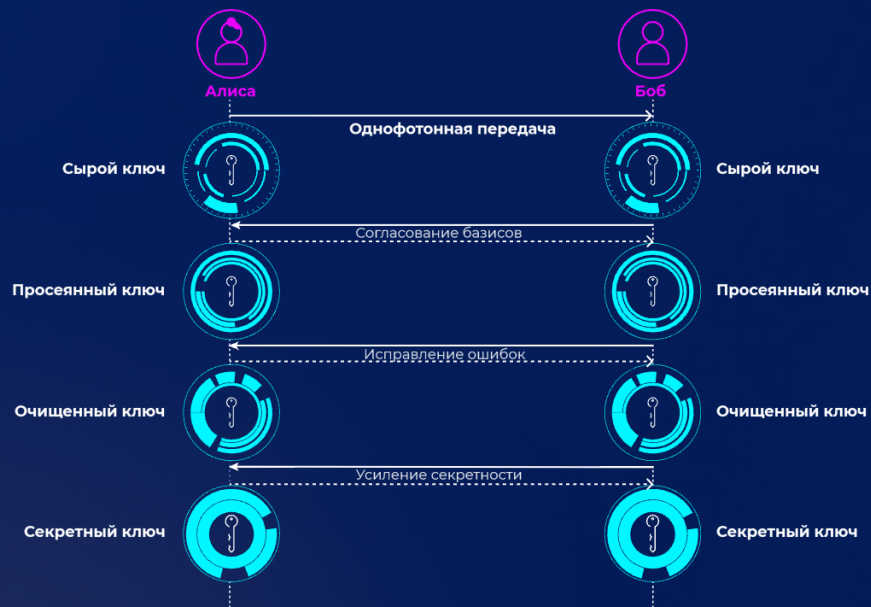
# Квантовое распределение ключей



- Создание у двух абонентов общего ключа
- Доступна частая смена ключей
- Защита от чтения вперед/назад
- Защита от внутреннего нарушителя

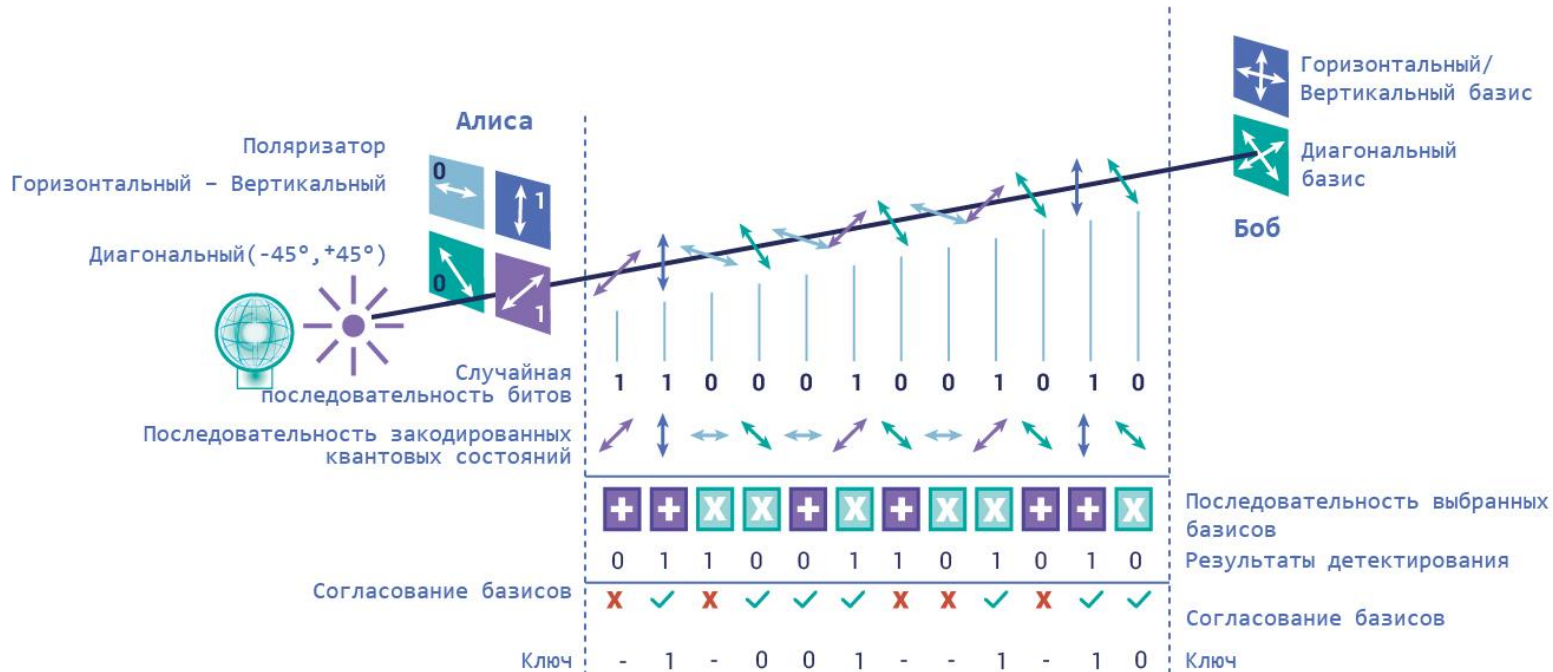
- Дорогие комплектующие
- Расстояние ограничено (~100км)
- Небольшая скорость создания ключей

# Квантовое распределение ключей



- Передача информации осуществляется с помощью квантовых состояний
- Определение совпадающих битов в независимых случайных последовательностях даёт сырой ключ
- Секретность обеспечивается за счет учёта уровня ошибок в квантовом канале
- Служебный канал криптографически аутентифицируется
- Квантовый ключ распределяется на концы квантового канала

# Протокол BB84





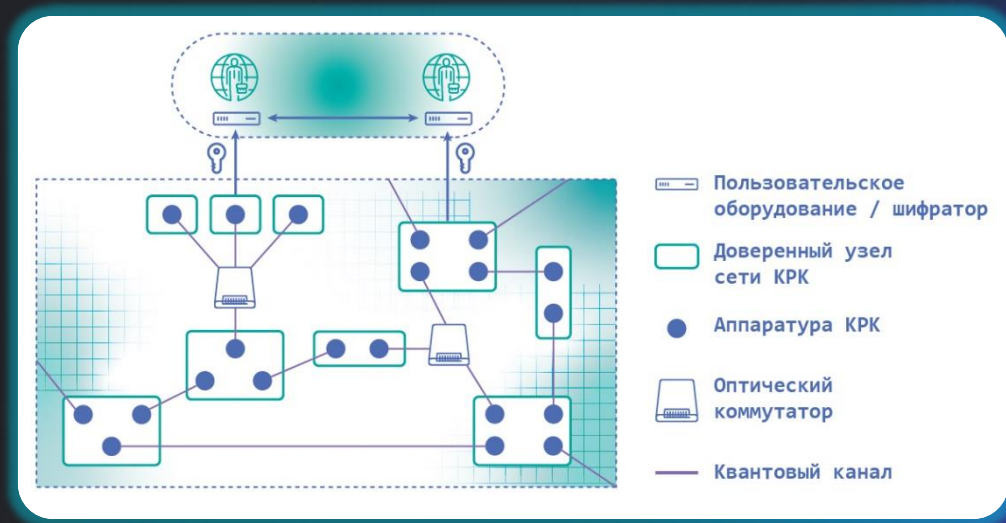
# Применение КРК: сети произвольной топологии



# Сети КРК: принцип построения

Основа сетей КРК — доверенные промежуточные узлы (trusted nodes/relays), соединенные квантовыми каналами

В одной сети КРК можно совмещать сегменты с различной физической реализацией квантового канала и оборудованием разных производителей



# Принцип работы многоsegmentной сети КРК с доверенными узлами

## Магистраль



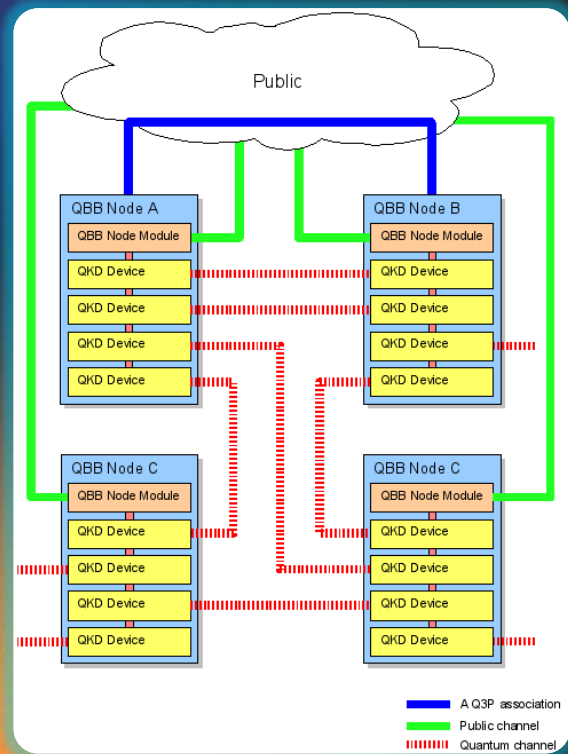
- Квантовозащищённый ключ (КЗК) передаётся по сети под защитой квантовых ключей на сегментах
- КЗК используется шифраторами как аналог квантового ключа

Ampire 360°

Существующие  
решения в стране  
и в мире

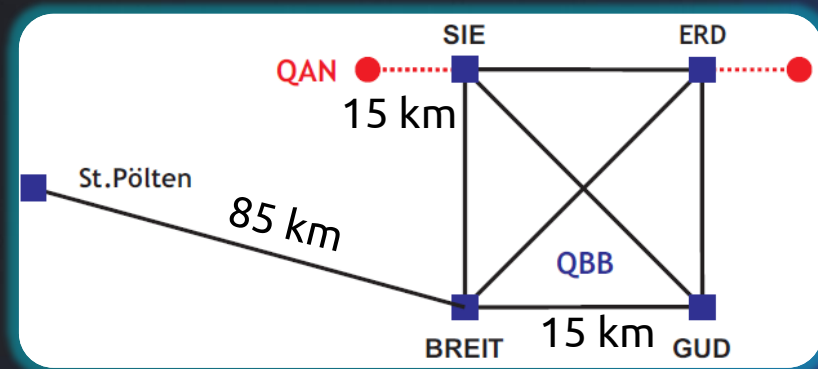


# SECOQC. Евросоюз, 2008



## Поставщики оборудования КРК:

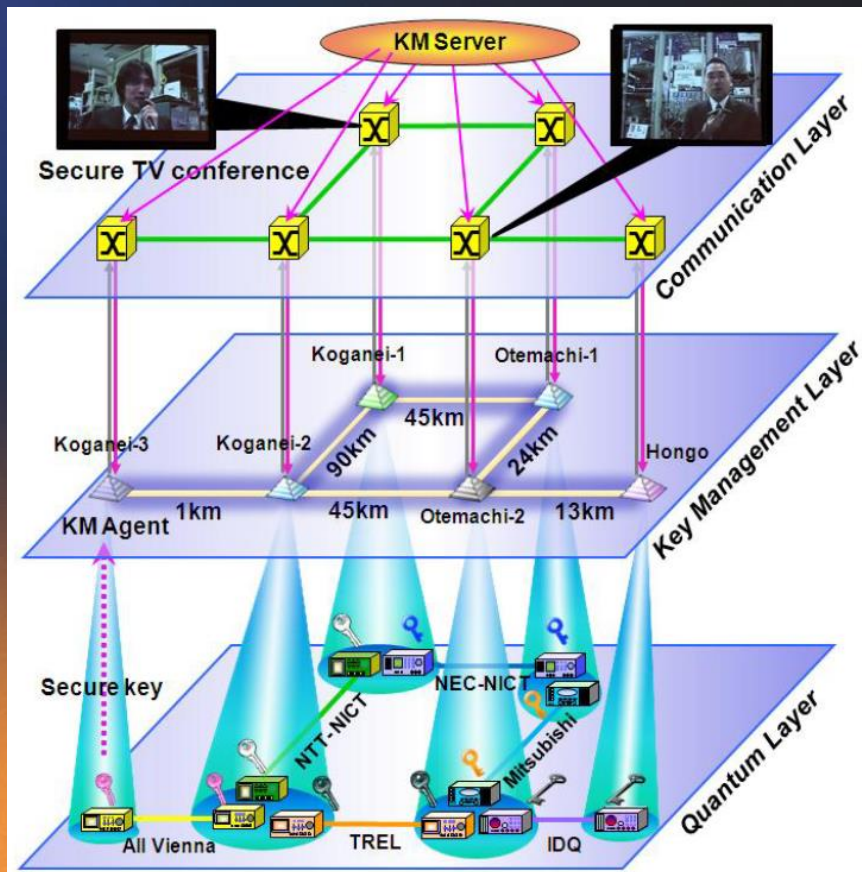
- IdQuantique
- GAP Geneva/IdQuantique/ARC
- Toshiba
- University of Vienna/ARC/KTH



*Outline of the SECOQC Quantum-Key-Distribution Network in Vienna.*

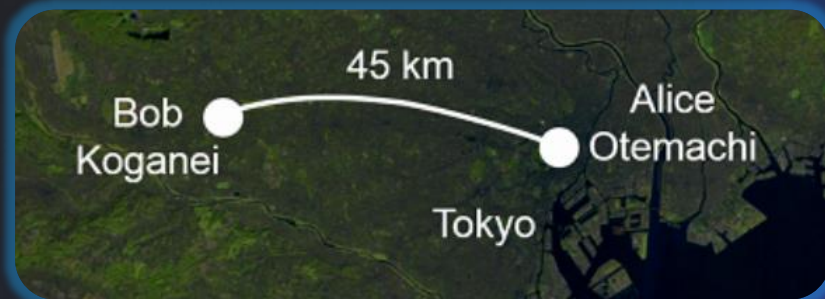
*A. Poppe, M. Peev, O. Maurhart, International Journal of Quantum Information, Volume 6, Number 2 (April 2008)*

# Сеть в Токио, 2010



## Цели:

- Разработка сети КРК для высокоскоростного шифрования данных
- Сравнение оборудования КРК разных производителей (TREL, NEC-NICT, NTT, IDQ, Mitsubishi), построенного на разных принципах



*Field test of quantum key distribution in the Tokyo QKD Network.*

*Sasaki, M. et al. Optics Express, 19(11), 2011*

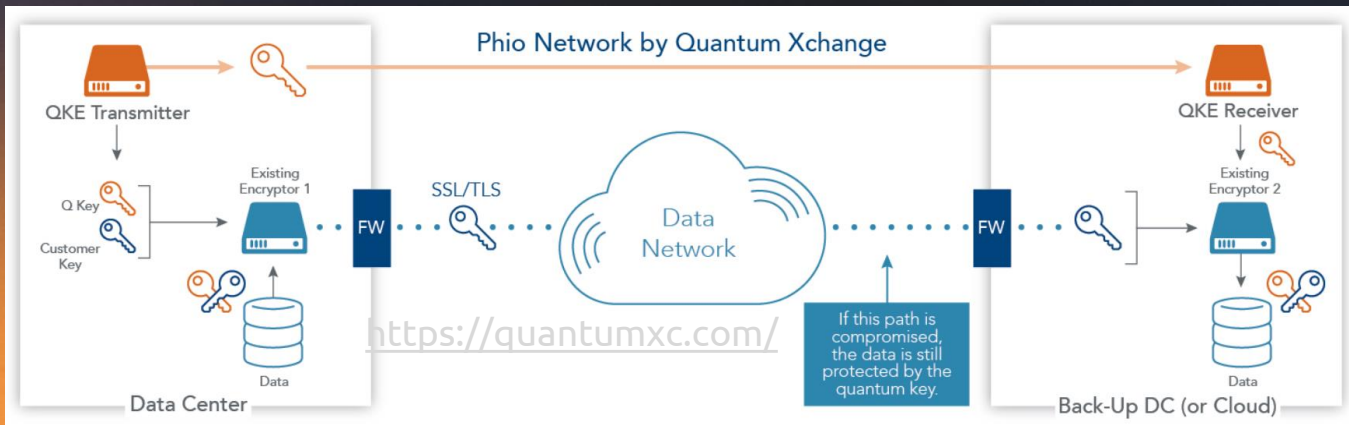
# США. Сеть Quantum XC, 2018

## Цель:

Создать вдоль восточного побережья сеть QKD-as-a-Service

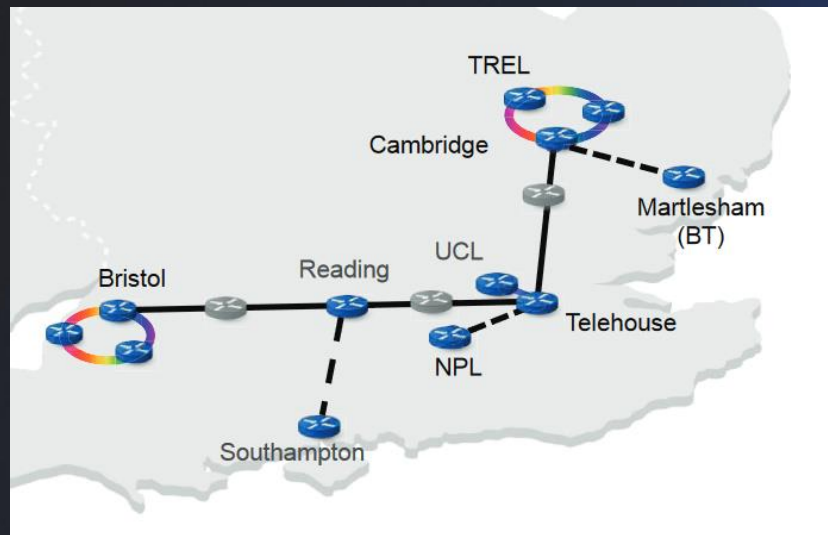
## Оборудование:

- Доверенный узел (QKD Trusted Node™) — совместная разработка Battele и ID Quantique с учётом требований стандарта FIPS 140-2
- КПК — Cerberis, ID Quantique

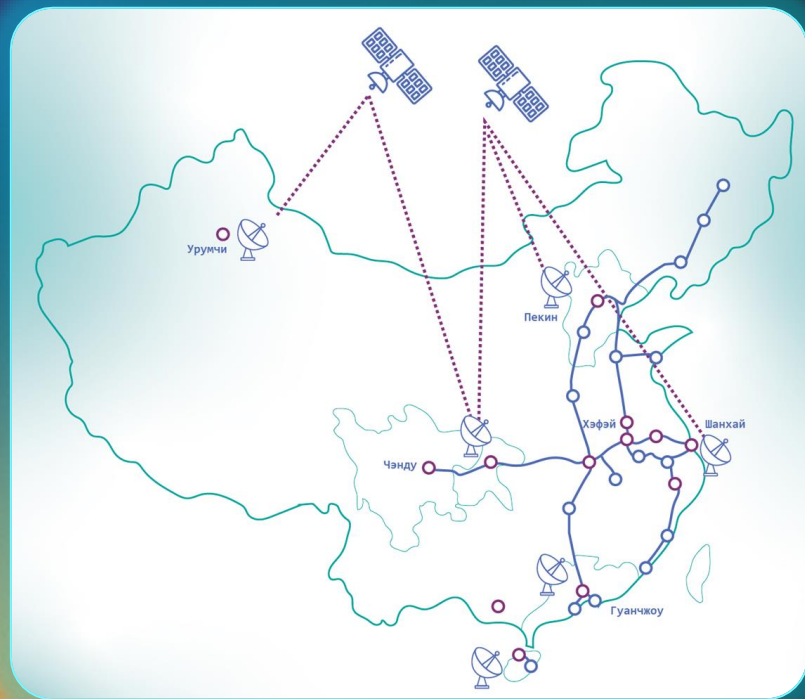


# Великобритания, UK Quantum Network (UKQN) project, 2019

- «Первая в мире квантовая сеть, построенная на коммерческом оборудовании»
- Участки сети до 125 км
- Коробочное оборудование ID Quantique и ADVA
- Скорость передачи данных до 500 Гбит/с



# Сеть КРК в Китае



Создавалась с **2013** года

**>10 000** км протяжённость

**40** сегментов **2** спутника

Оборудование нескольких  
производителей

**>150** потребителей

В мае **2025** года China Telecom Quantum Group объявила о запуске первой коммерческой системы

# Сети КРК в Южной Корее



## Особенности:

- Объявлено о создании в 2022 году
- Соединяет 48 государственных учреждений
- Протяжённость наземных линий — более 800 км
- Построена на оборудовании ID Quantique
- Оператор сети SK Telecom

<https://www.startupticker.ch/en/news/south-korea-relies-on-id-quantique-for-data-security>

Параллельно создаётся сеть КРК на основе оборудования Toshiba и сетевой инфраструктуры KT Corporation

<https://www.global.toshiba/www/company/digitalsolution/news/2022/0328.html>

# Сети КРК в Европе

Программа **Quantum Flagship** с 2018 г.

Бюджет **€1000M**

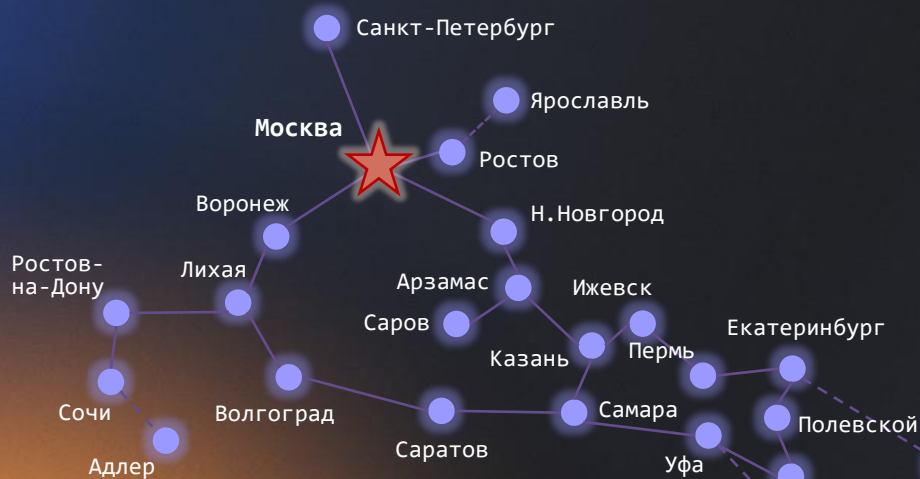
**27** европейских стран

**7** проектов по КРК



Единая магистральная и спутниковая сеть  
КРК **European QCI**  
(Quantum Communication Infrastructure)  
2023-2030 гг.

# Развитие квантовых сетей в России



В режиме 24/7 работает Центр управления и мониторинга магистральной квантовой сети ОАО «РЖД», более 70 000 параметров под мониторингом

## Динамика развития магистральной квантовой сети

2021 г. **707** км. Москва — Санкт-Петербург

2022 г. **1147 км.** Создан сегмент **Москва — Нижний Новгород**

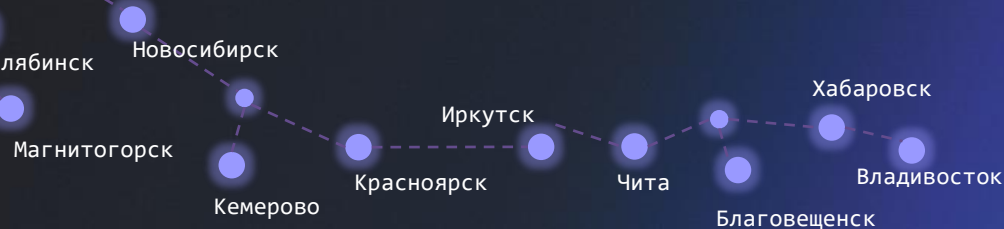
2023 г. **3 295 км.** К сети присоединены **Воронеж, Ростов-на-Дону, Казань**

2024 г. **7012 км.** К сети присоединены **Сочи, Саратов, Самара, Челябинск, Екатеринбург** и др. крупные города

2025 г. **7800 км.** Замыкание центрального и восточного кольца

**15 000**  
KM.

Планируемая общая протяженность квантовой сети в 2030 г. Для обеспечения географической связности страны магистральной квантовой сетью и создания сервиса оператора связи

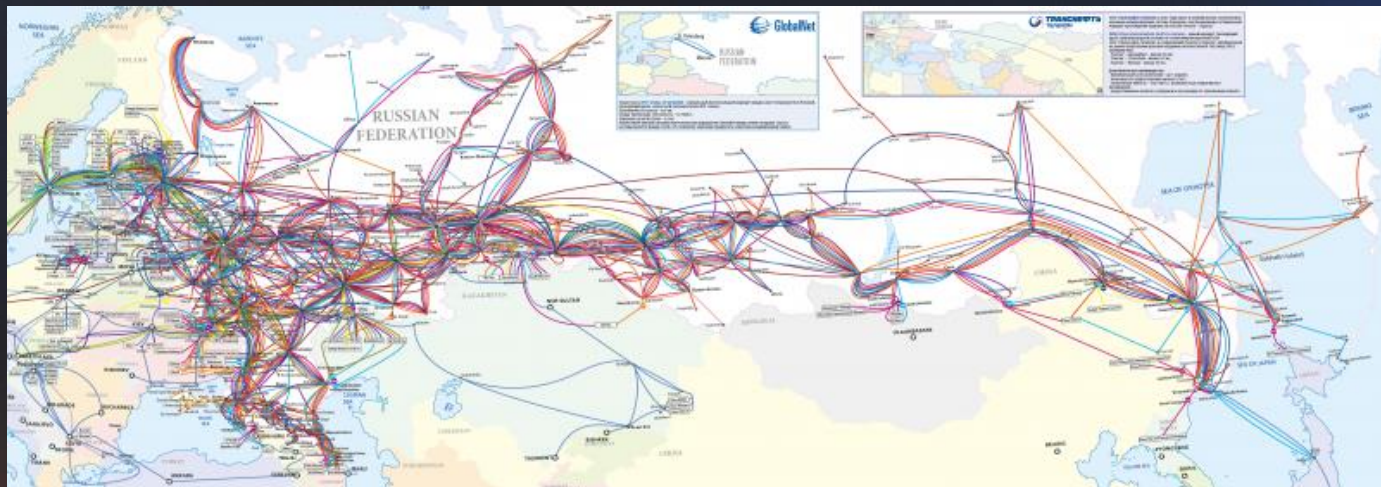


# Карта магистральных сетей связи России

## Инфраструктура для сети КРК

Нет необходимости  
в сверхдальних  
сегментах КРК

Протяжённость  
страны требует КРК  
на спутник

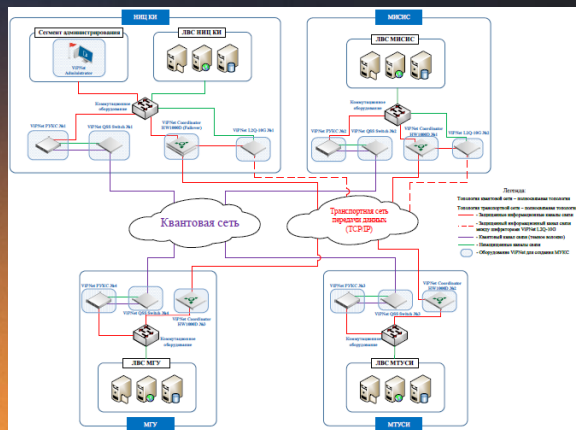


Магистральные сети связи в России (по материалам © [ComNews](#) 21.10.2020)

# Межуниверситетская квантовая сеть России

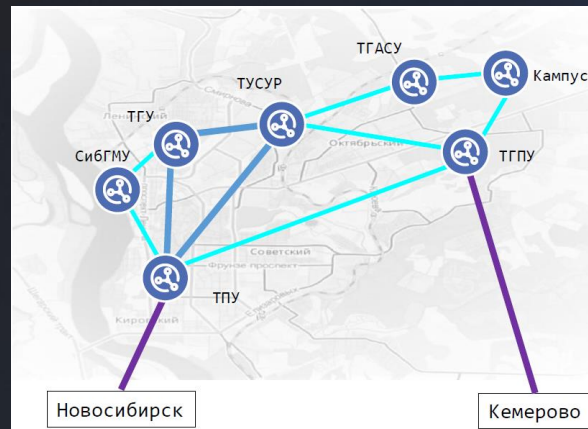
## Московский кластер:

- МГУ
- НИЦ «Курчатовский институт»
- МИСИС
- МТУСИ



## Томский кластер:

- ТУСУР
- СибГМУ
- ТГУ
- ТГАСУ
- ТПУ





ViPNet Quantum  
cryptographic  
systems



# Квантовые продукты ViPNet

Ampire 360°



**Распределительный узел квантовой сети** — предназначен для объединения различных сегментов квантовой сети и построение магистральных квантовых сетей



**Клиентский узел квантовой сети** — оконечные узлы квантовой сети, к которым подключаются потребители ключей



**Оптический коммутатор квантовых сетей** — предназначен для организации оптической сети для передачи квантовых состояний между квантовыми устройствами



# Квантовые продукты ViPNet для обучения

Ampire 360°

**Server Academic Edition** — центральный узел сети, обеспечивающий выработку ключей между всеми узлами



**Client Academic Edition** — оконечные узлы сети, к которым подключаются потребители ключей

**Quantum Key Distribution Simulator** — это программно-аппаратный комплекс симуляции квантового распределения ключей (КРК)



# Квантовый генератор случайных чисел

**Квантовый генератор случайных чисел (QRNG)** — это устройство, создающее истинно случайные последовательности на основе непредсказуемых квантовых явлений. На практике используются оптоэлектронные схемы, формирующие и измеряющие квазиоднофотонные состояния в квантовой системе.

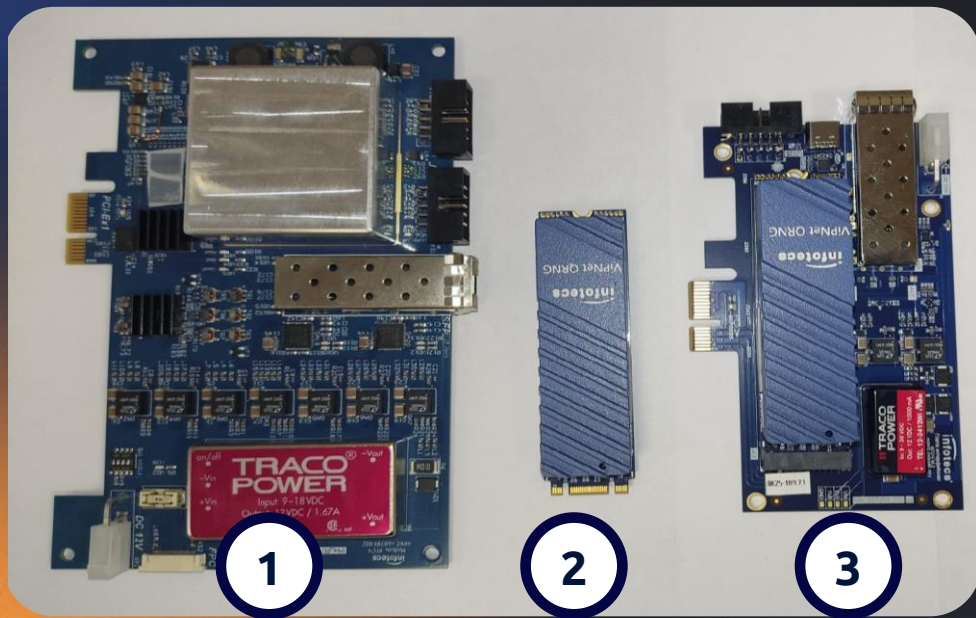
В отличие от псевдослучайных программных датчиков, QRNG обеспечивает абсолютную непредсказуемость, что критически важно как для любого СКЗИ, так и для систем квантового распределения ключей.

Существует много примеров атак и компрометации на криптографических решений, построенных на слабых ПДСЧ/ФДСЧ.

## Области применения QRNG:

- Криптография
- Статистические расчеты
- Финансовое моделирование
- Экспериментальные науки
- Искусственный интеллект

# Квантовый генератор случайных чисел



1

**КГСЧ Ethernet/PCIe (10x15 см).**  
Сертифицирован в составе ViPNet  
РУКС по классу КСЗ

2

**КГСЧ M.2 (2x8 см).** Передаётся  
на сертификацию в составе HSM  
по классу KB

3

**КГСЧ M.2 + переходная плата  
Ethernet/PCIe (7x10 см).** Внедрение  
с РУКС-Б в 2027 г.

# Квантовый генератор случайных чисел

| Характеристики                                    | ГСЧ Гроссмейстер                       | ViPNet QRNG                                                                                                                                                       |
|---------------------------------------------------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Габариты                                          | 15 x 13 x 4,5 мм                       | 80 x 23 x 15.9 мм                                                                                                                                                 |
| Максимальное энергопотребление                    | -                                      | До 3 Вт по цепи питания +3.3В                                                                                                                                     |
| Интерфейс подключения                             | Встраивается через интерфейс SPI и I2C | 1) Переходная плата PCI Express Gen1.0 x 1 (пропускная способность 2.5 Гбит/с);<br>2) M.2, разъем с ключами M+B, совместимость с разъёмами хоста высотой от 4 мм. |
| Источник энтропии                                 | Шумящий диод                           | Квантовый (фотоэффект)                                                                                                                                            |
| Номинальная скорость формирования случайных чисел | 4096 бит/с                             | 170 Мбит/с                                                                                                                                                        |
| Диапазон рабочих температур                       | +5...+50°C                             | +10...+35°C                                                                                                                                                       |

Благодарю  
за внимание



The background features a dark blue gradient with a faint, wireframe globe centered behind the text. The globe is composed of hexagonal cells. In the corners, there are clusters of orange triangles pointing towards the center. The text "Ampire 360°" is centered in white. The "360" is partially overlaid by a large orange diamond shape that has a red-to-orange gradient and a white arrow pointing upwards and to the right, indicating a 360-degree rotation.

**Ampire 360°**