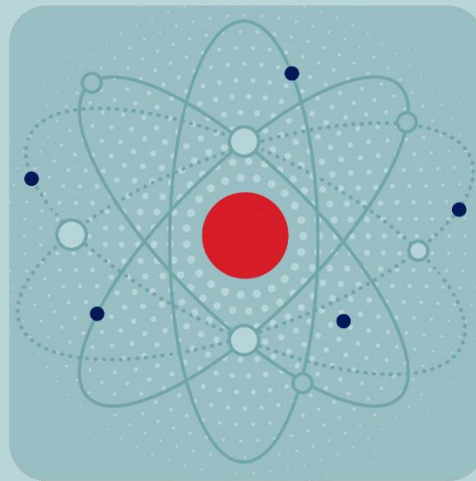


ТЕХНОЛОГИЧЕСКАЯ
ПАРТНЕРСКАЯ КОНФЕРЕНЦИЯ

РУТОКЕН ОАЧ ТЕХНОЛОГИИ ДОВЕРИЯ



КОМПАНИЯ
ПРАКТИВ

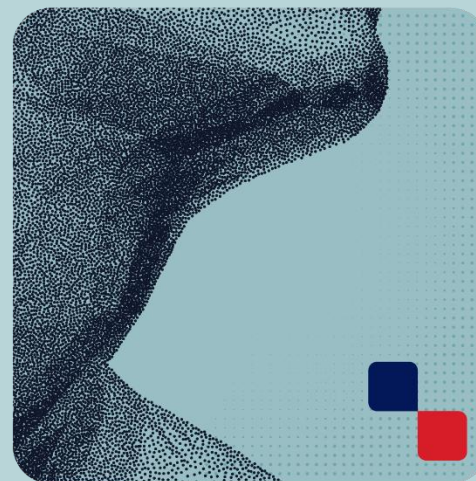
инфотекс



Инженерия надежности: использование КРК и КГСЧ в передаче и защите данных

Дмитрий
Гусев

Заместитель Генерального
директора АО «ИнфоТеКС»



Что такое и зачем нужны системы КРК?



Системы квантового распределения ключей позволяют **быстро** и **независимо от человеческого фактора** вырабатывать симметричные ключи защиты **для классических СКЗИ** – квантово-защищенных ключей.



Системы КРК строятся на базе оптических квантовых систем, в которых критически важная информация о ключах передается в виде единичных квантовых состояний фотонов. Законы квантовой физики запрещают **незаметное** копирование или подделку таких состояний.



Системы КРК внедряются уже сегодня на обычных оптических линиях связи по всему миру, включая Россию.



Концепция магистральных систем КРК позволяет конечным потребителям квантово-защищенных ключей подключаться к общей магистрали, имея только конечный «узел-приемник КЗК».

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.
1 147 км. Создан сегмент Москва – Нижний Новгород

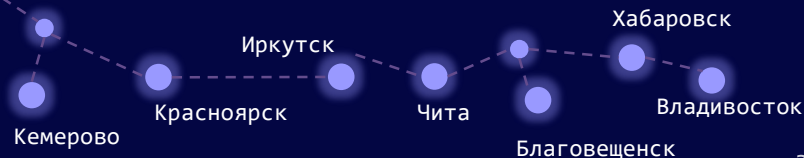
2023 г.
3 295 км. К сети присоединены Воронеж, Ростов-на-Дону, Казань

2024 г.
7 012 км. К сети присоединены Сочи, Саратов, Самара, Челябинск, Екатеринбург и др. крупные города

2025 г.
7 800 км. Замыкание центрального и восточного кольца

15 000 км.

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



Квантовые продукты ViPNet



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

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)



Что такое и зачем нужен КГСЧ (QRNG)?

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, но и для систем квантового распределения ключей

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

Области применения QRNG:

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

VipNet Quantum Random Number Generator

Последовательность получения случайных чисел с помощью VipNet QRNG



1

Генерация квантового события



2

Измерение его результатов

01
10

3

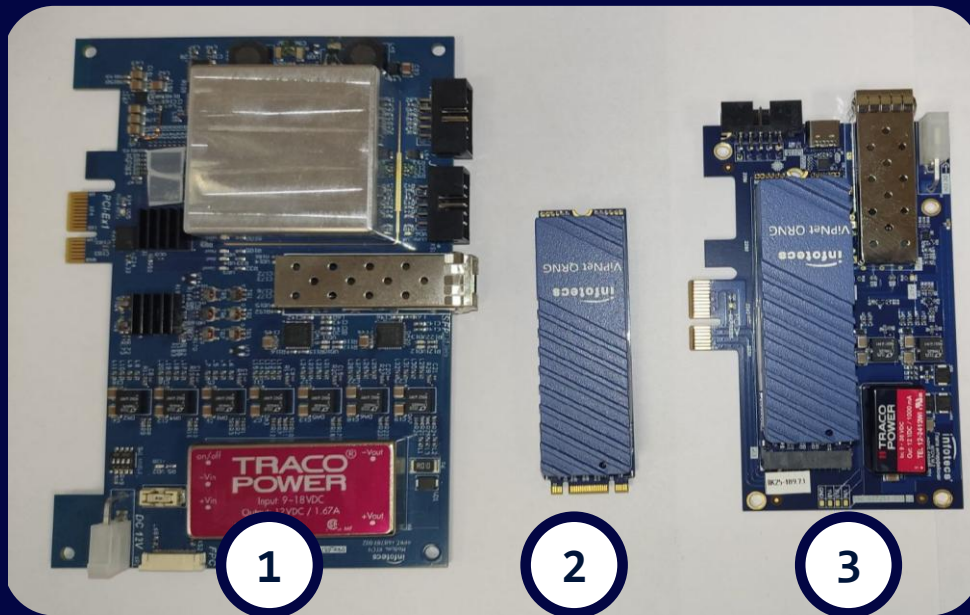
Преобразование его в цифровую форму



4

Полученная последовательность случайных чисел дополнительно защищена криптографическим способом

Модели ViPNet QRNG



1

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

2

КГСЧ М.2 (2x8 см). Передаётся
на сертификацию в составе HSM
по классу КВ

3

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

Сравнение ФДСЧ и КГСЧ

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); 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

Подписывайтесь
на наши соцсети,
там много интересного




инфотекс





**Дмитрий
Гусев**

Заместитель
Генерального
директора
АО «ИнфоТеКс»

