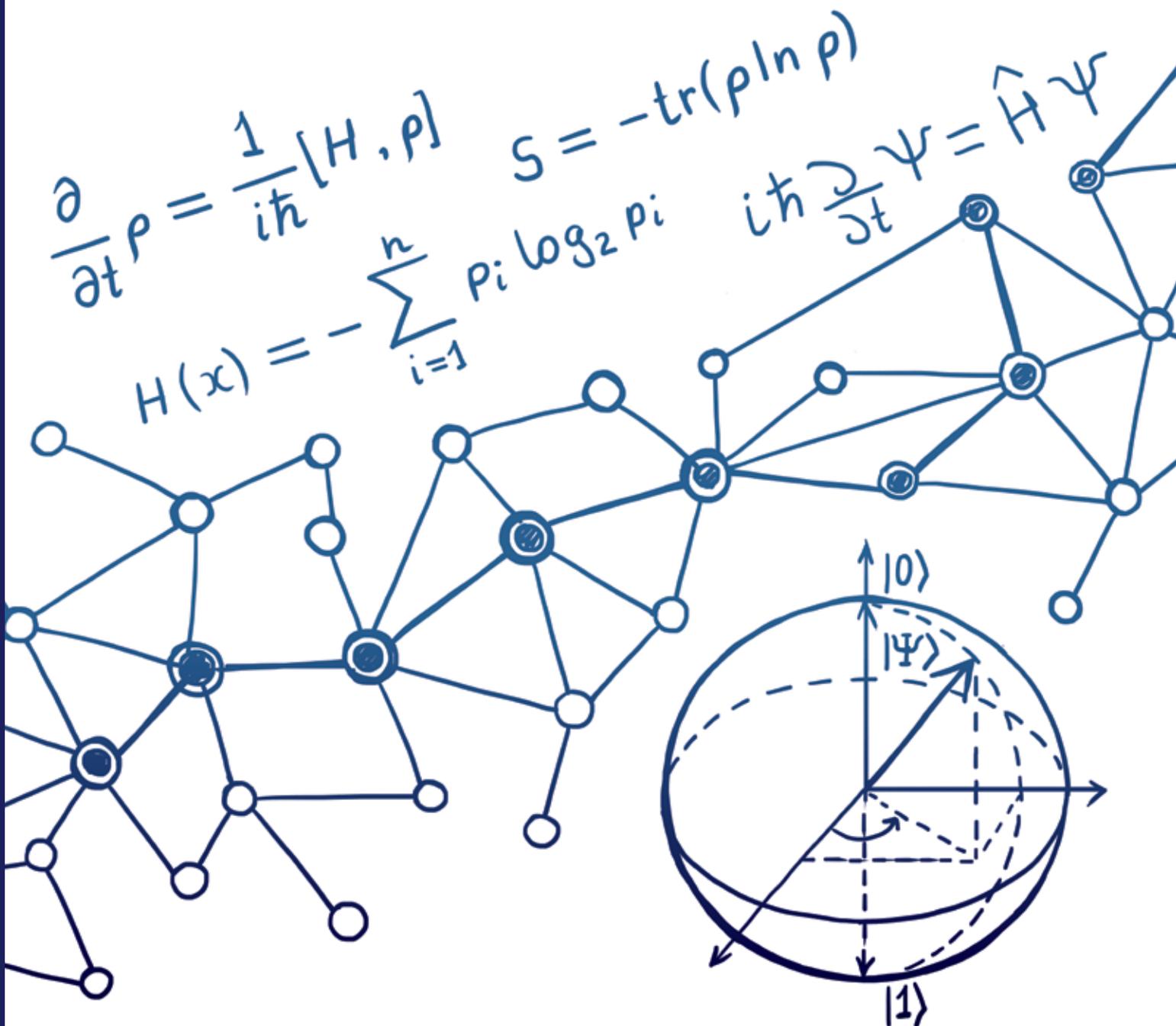


ViPNet Quandor

Комплекс автоматической доверенной доставки криптографических ключей



ViPNet Quandor – квантовая криптографическая система выработки и распределения ключей (ККС ВРК), выполняющая протокол квантового распределения ключей (КРК) и снабжающая симметричными криптографическими ключами средства криптографической защиты информации (СКЗИ)

Совместный проект
АО «ИнфоТеКС» и МГУ имени
М.В. Ломоносова при поддержке
Министерства науки и высшего
образования Российской Федерации



[О ТЕХНОЛОГИИ КРК]

Технология квантового распределения ключей решает важную задачу в криптографии – автоматическую доверенную доставку криптографических ключей в СКЗИ без участия человека.

Технология основана на использовании эффектов квантовой физики, обеспечивающих полную секретность вырабатываемых ключей.

[ОСОБЕННОСТИ]

- Первый продукт в РФ, использующий технологии КРК, разработанный по принципам СКЗИ в соответствии с требованиями ФСБ России
- СКЗИ класса КСЗ (все технические решения принимались с расчетом на последующую сертификацию на класс КВ)
- Обеспечивает защиту информации от атак, в том числе с использованием эффективного квантового компьютера
- Математически доказанная секретность выработанных криптографических ключей
- Гибридная ключевая система на квантовых и предраспределенных ключах. Физический вывод из строя квантового канала и оборудования не приведет к остановке шифрования
- Используется фундаментальный принцип квантовой физики о невозможности «подслушивания» квантовой информации без ее изменения

[ПРЕИМУЩЕСТВА]

- Впервые применяется технология квантового распределения ключей, которая обеспечивает секретность полученных криптографических ключей, основанную на фундаментальных законах природы
- Физический генератор истинно случайных чисел, основанный на квантовых эффектах
- Автоматическая работа после ввода в эксплуатацию
- Автоматическая загрузка ключей в каналные шифраторы ViPNet L2Q-10G один раз в минуту
- Автоматическая выработка секретных криптографических ключей по протоколу КРК при длине квантового канала до 100 км
- Воздушная система охлаждения, совместимая с типовыми условиями для оборудования в центрах обработки данных

СОБСТВЕННОЕ ПРОИЗВОДСТВО



Полный производственный цикл на базе собственного производственного подразделения в Томске



Все инженерные испытания пройдены



В процессе сертификации в ФСБ России



Готовность к поставкам



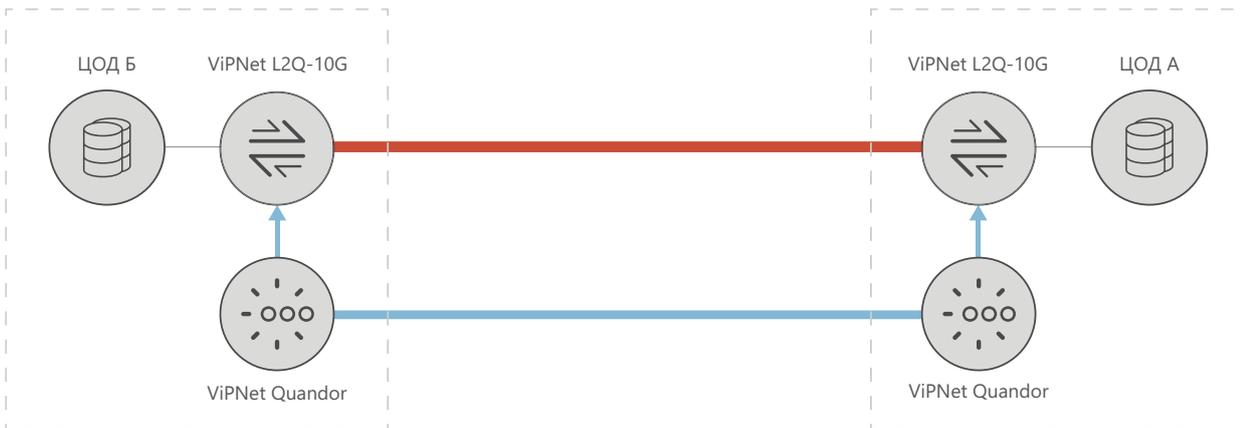
[ИСПОЛЬЗОВАНИЕ]

Один из основных сценариев использования ViPNet Quandor – автоматическая доверенная доставка криптографических ключей для канальных шифраторов ViPNet L2Q-10G.

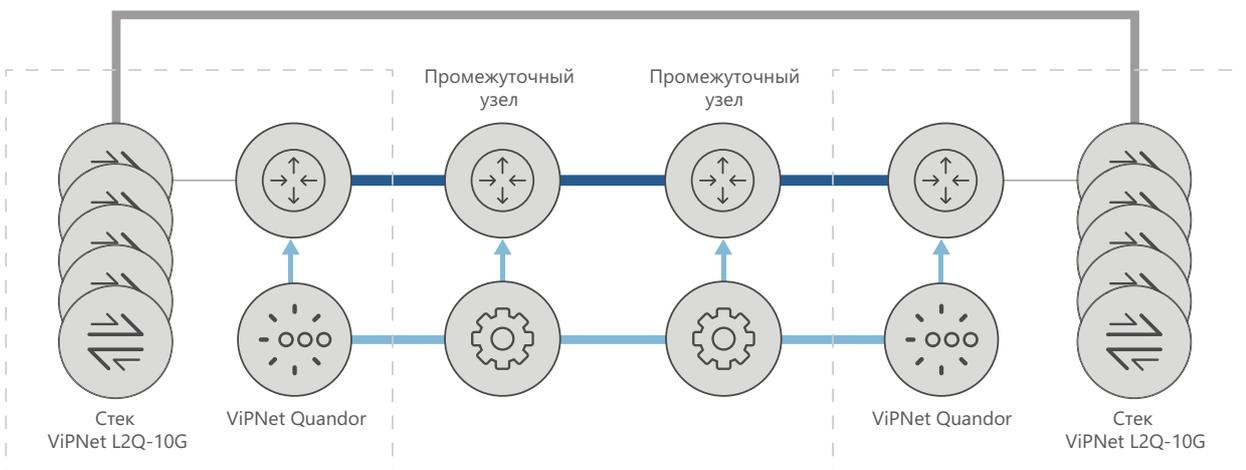
ПАК ViPNet L2Q-10G – шлюз безопасности, обеспечивающий криптографическую защиту протокола Ethernet и предназначенный для защиты магистральных высокоскоростных каналов связи между объектами.

Для использования квантовых ключей к шифратору по защищенному интерфейсу подключается аппаратура ViPNet Quandor, которая устанавливается в контролируемой зоне шифратора.

Основной сценарий использования



Перспективная квантовая магистраль



ViPNet QUANDOR:

- Физический датчик случайных чисел, реализованный с использованием законов квантовой физики
- Математически доказанная стойкость протокола КРК
- Выработка секретных симметричных криптографических ключей на основе принципов квантовой физики
- Стойкость к атакам, возможным при реализации эффективного квантового компьютера

ШИФРАТОРЫ ViPNet L2Q-10G:

- Конфигурация сети шифраторов «точка-точка»
- Размер кадров Ethernet от 64 до 9000 байт
- Скорость шифрования Ethernet кадров размером 110 байт, полудуплекс – 4,4 Гбит/с
- Скорость шифрования Ethernet кадров размером 110 байт, полный дуплекс – 8,8 Гбит/с
- Прозрачность для всех сетевых приложений и протоколов сетевого уровня и выше
- Шифрование с маскированием ключа по алгоритму «Кузнечик» по ГОСТ Р 34.12-2015 в режиме согласно рекомендациям по стандартизации Р1323565.1.026-2019 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование»

ВОЗМОЖНОСТИ

[ПРЕИМУЩЕСТВА ViPNet L2Q-10G ПРИ ИСПОЛЬЗОВАНИИ КВАНТОВЫХ КЛЮЧЕЙ]



Высокая скорость смены криптографических ключей в шифраторах без участия администратора



Администратор не имеет доступа к ключевой информации – криптографические ключи вырабатываются и загружаются автоматически

[ОСОБЕННОСТИ ViPNet L2Q-10G]

ViPNet L2Q-10G – это криптографическое устройство канального уровня (по стандартной модели OSI), выполненное в форм-факторе 1U, корпус которого спроектирован с учетом жестких требований безопасного функционирования – защита от несанкционированного вскрытия, энергонезависимое хранилище ключей шифрования, резервирование электропитания.

- Высокая производительность шифрования (до 10 Гбит/с)
- Низкие вносимые задержки (не более 15 мкс)
- Автоматизированный контроль выработки нагрузки на ключ и «бесшовный» переход на новый ключ позволяют упростить ИТ-инфраструктуру при одновременном увеличении уровня информационной безопасности
- Топология шифраторов «точка-точка»
- Поддержка Jumbo frames – «большой» Ethernet-кадр размером до 9000 байт
- Прозрачен для сетевых протоколов и приложений
- Поддерживает трафик Unicast, Multicast и Broadcast
- Автоматическое определение и соединение парных шифраторов
- Минимальная избыточность протокола защиты

[МОБИЛЬНЫЙ КОМПЛЕКТ]



Быстрое развертывание
на сетях заказчика



Защита во время
транспортировки



Минимальные затраты времени
на ввод в эксплуатацию



Демонстрация законченного рабочего
решения, готового к поставкам

[СПЕЦИФИКАЦИЯ]

Электропитание	~220 В, 50 Гц, 500 Вт
Рабочий диапазон температур, °С	От 0 до +35
Относительная влажность, %	не более 93
Габаритные размеры Ш x В x Г, мм	не более: 19" 2RU (482,6 x 88,1 x 661,0)
Отдельный канал квантовой связи	Выделенное оптоволокно длиной до 100 км без активного оборудования
Тип разъема для подключения к ВОЛС	FC/UPC, FC/PC
Длина волны излучаемых фотонов в лазерных импульсах, нм	1550 ±10
Отдельный канал синхронизации	Выделенное оптоволокно без активного оборудования
Скорость генерации квантовых ключей	1 ключ в минуту
Протокол КРК	Оригинальный протокол на геометрически однородных когерентных состояниях Geometrically Uniform Coherent States (GUCS)
Стойкость протокола	Соответствует «Временным требованиям ККС ВРК (СКЗИ)» ФСБ России от 3.08.2017 г.
Датчик случайных чисел	Физический, реализованный с использованием законов квантовой физики
Физическая безопасность	металлический корпус с датчиком несанкционированного доступа (ДНСД)

[КОМПЛЕКТ ПОСТАВКИ]

Наименование	Кол-во	Описание
ViPNet Quandor Tx	1	Сервер квантового распределения ключей
ViPNet Quandor Rx	1	Клиент квантового распределения ключей
ViPNet L2Q-10G	2	Шлюз безопасности, обеспечивающий криптографическую защиту протокола Ethernet

[СЕРТИФИКАЦИЯ И ОБСЛУЖИВАНИЕ]

ФСБ РОССИИ

В процессе сертификации

ПАТЕНТЫ

RU 2 665 249 C1 – Способ управления интерференционной картиной в однопроходной системе квантовой криптографии

RU 2 706 175 C1 – Способ квантового распределения ключей в однопроходной системе квантового распределения ключей

RU 2 662 641 C1 – Квантовый генератор случайных чисел

СВИДЕТЕЛЬСТВА

Свидетельство
на товарный знак
«ViPNet Quandor»

ГАРАНТИЙНОЕ ОБСЛУЖИВАНИЕ

Сервис гарантийного
обслуживания в течение 1 года

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Сервис технической поддержки уровня «Базовый» на срок 1 год входит в стоимость.

Для получения услуг технической поддержки уровня «Стандартный» и «Расширенный» необходимо заключать отдельный Договор.



+7 495 737-61-92
8 800 250-0-260 (бесплатный звонок по России)

✉ soft@infotecs.ru
hotline@infotecs.ru

🌐 www.infotecs.ru



Содержимое документа носит исключительно информационный характер и не является публичной офертой. Для получения подробной информации об указанных в документе продуктах и услугах вы можете обратиться в АО «ИнфоТекС». Все изображения являются лишь иллюстрациями. Все технические характеристики, внешний вид и комплектность описываемой продукции могут меняться без предварительного уведомления. Символы ™ или ® в документе не используются, однако, если не указано иного, все товарные знаки в данном документе защищены соответствующим правом, которое принадлежит их владельцам.