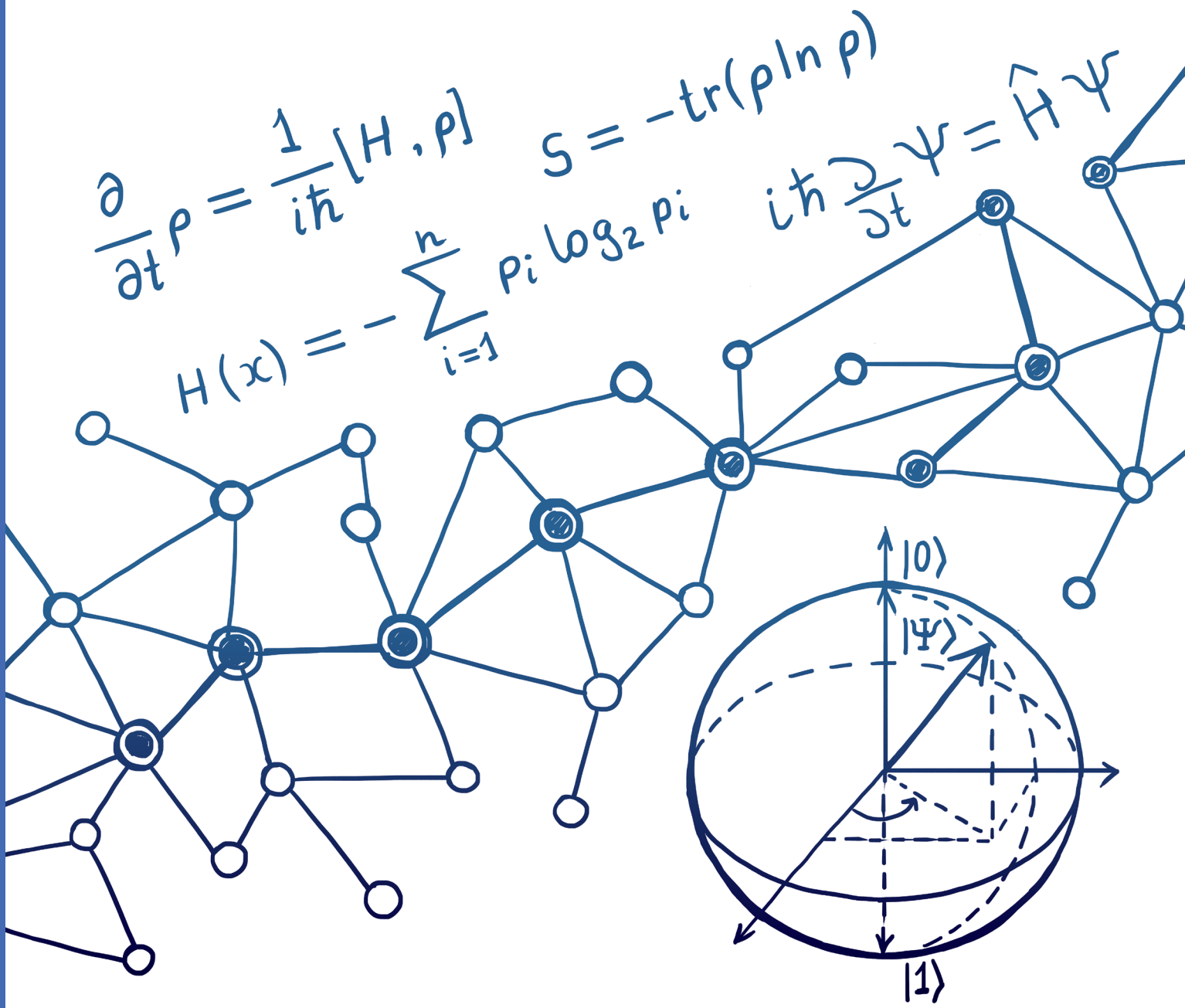
infotecs

ViPNet Quantum Cryptographic Systems

Квантовые криптографические системы



ViPNet Quantum Trusted System Lite

Квантовая криптографическая система выработки и распределения ключей с сетевой топологией «звезда».

ViPNet QTS Lite вырабатывает квантовозащищенные криптографические ключи и доставляет их СКЗИ-потребителям с целью защиты пользовательского трафика, в том числе цифровых аудио- и видеозвонков и текстовых сообщений

Система ViPNet QTS Lite надежно и защищенно формирует симметричные ключи для пар потребителей. Защита от нарушителя с полномочиями администратора обеспечивается за счет автоматической работы и смены всех ключей сразу после ввода в эксплуатацию.

СОСТАВ СИСТЕМЫ

ViPNet РУКС Лайт
распределительный узел квантовой сети Лайт является центром сети в топологии «звезда» для подключаемых к нему клиентских узлов квантовой сети.

ViPNet КУКС Лайт
клиентский узел квантовой сети Лайт используется для подключения абонентов – потребителей квантовозащищенных криптографических ключей.

ViPNet QSS Switch
оптический коммутатор переключает оптические каналы связи при работе квантовой криптографической системы ViPNet QTS Lite. ViPNet QSS Switch не выполняет преобразований сигнала, а лишь оптически коммутирует один или два входа (в зависимости от исполнения) на 12 выходов.

ПРЕИМУЩЕСТВА

01. Емкость квантовой сети:
    > от 1 шт. ViPNet РУКС Лайт (центральный узел «звезды»)
    > от 2 до 1728 шт. ViPNet КУКС Лайт (периферийные узлы «звезды»)

02. Расстояние между ViPNet РУКС Лайт и ViPNet КУКС Лайт может достигать 45 км при использовании одного оптического коммутатора, 35 км для двух уровней коммутации и 25 км для трех уровней

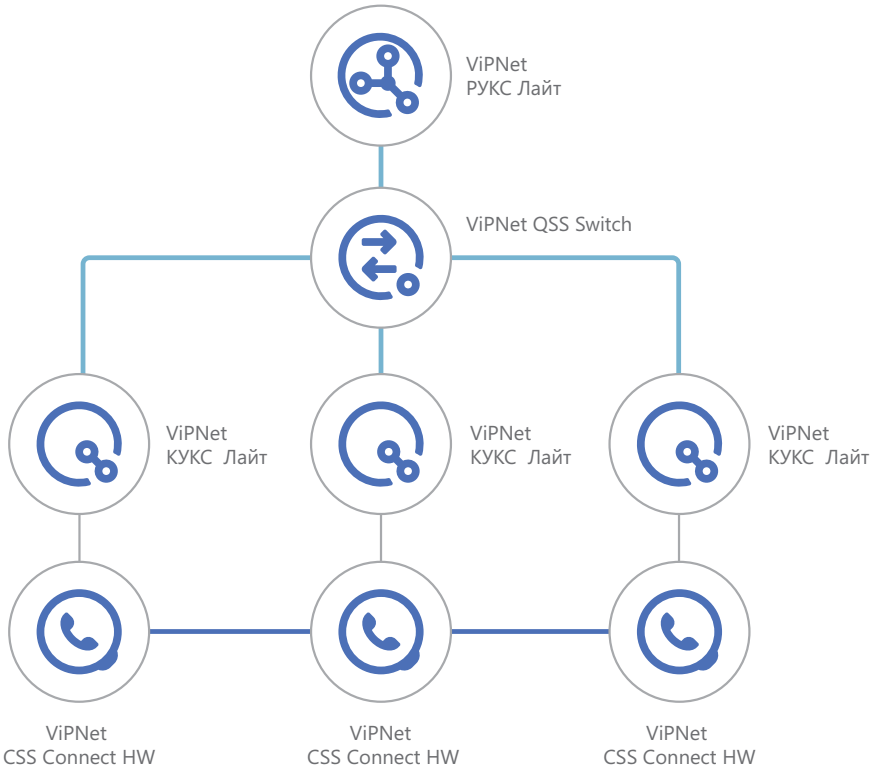
    Разрабатывается новое поколение системы ViPNet QTS Lite 2.0 с увеличенной до 100 км длиной оптического канала при одном уровне коммутации

03. Используется разработанный в России и основанный на квантовых эффектах физический генератор истинно случайных чисел

04. Реализована защита от атаки с расщеплением по числу фотонов (PNS-атака) с помощью алгоритма decoy-states

05. Используется оригинальный протокол КРК с фазо-временным кодированием состояний (Phase-Time Coding) – запатентованная разработка Центра квантовых технологий МГУ имени М.В. Ломоносова

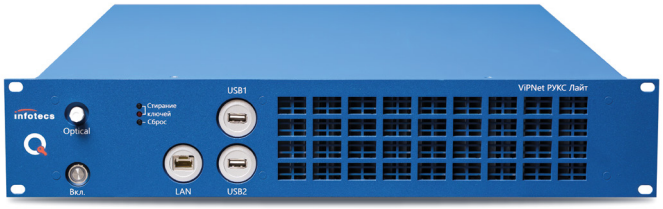
06. Гибридная ключевая система – квантовозащищенные ключи (КЗК) собираются из частей квантовых ключей, выработанных на узлах квантовой сети, и частей классических предраспределенных ключей



Оптический коммутатор переключает квантовые каналы связи до нескольких клиентских (оконечных) узлов сети.

Каждый потребитель в сети получает возможность квантовозащищенного обмена трафиком, текстовыми сообщениями, аудио- и видеозвонками с любым другим потребителем из той же сети (например, в пределах одного офиса).

ViPNet QTS Switch



ViPNet РУКС Лайт

ViPNet КУКС Лайт

	ViPNet РУКС Лайт	ViPNet КУКС Лайт	ViPNet QTS Switch
Назначение	Распределительный узел квантовой сети Лайт	Клиентский узел квантовой сети Лайт	Управляемый оптический коммутатор для масштабирования сети ViPNet QTS
Конструктивное исполнение	19″ 2RU	Midi Tower	19″ 1RU
Сетевой интерфейс	Ethernet LAN 1 Гбит/с		
Оптический интерфейс	FC/UPC		Входных – 1 или 2 Выходных – 12
Датчик случайных чисел	Физический датчик, источник случайности основан на квантовых процессах		–
Физические средства защиты	Датчик несанкционированного доступа (ДНСД) обеспечивает гарантированное удаление криптографических ключей при вскрытии корпуса. Дальнейшая работа ПАК блокируется		–
Электропитание	230 В, 50 Гц, до 250 Вт		230 В, 50 Гц, 15 Вт

ViPNet Quantum Trusted System

Квантовая криптографическая система
выработки и распределения ключей
с произвольной сетевой топологией.

Система ViPNet QTS в автоматическом
режиме вырабатывает и доставляет
квантовозащищенные ключи
в СКЗИ-потребители

Система ViPNet QTS
надежно и защищенно формирует парные симметричные ключи для заданных СКЗИ потребителей ключей.
Это необходимо для обеспечения шифрования данных между парами узлов квантовой сети в режиме «точка-точка», а компрометация любого из оконечных узлов сети не приводит к компрометации всей остальной сети.

СОСТАВ СИСТЕМЫ

ViPNet МУКС
магистральный узел квантовой сети обеспечивает выработку квантовых ключей на участках квантовой сети длиной до 100 км. Несколько ViPNet МУКС соединяются между собой в протяженные квантовые линии связи. За счет построения длинных магистралей квантовозащищенные криптографические ключи поставляются в удаленные друг от друга СКЗИ-потребители.

ViPNet РУКС
распределительный узел квантовой сети устанавливается в точках ветвления квантовой сети и образует центр сети в топологии «звезда». К ViPNet РУКС подключаются оконечные узлы квантовой сети и оптические коммутаторы.

ViPNet КУКС
клиентский узел квантовой сети предназначен для подключения СКЗИ-потребителей.

ПРЕИМУЩЕСТВА

01. ViPNet QTS работает в произвольной сетевой топологии и имеет возможность масштабирования для обеспечения квантовозащищенными ключами неограниченного числа СКЗИ-потребителей

02. Расстояние между двумя сопряженными ViPNet МУКС или между ViPNet МУКС и ViPNet РУКС может достигать 100 км. Расстояние между ViPNet РУКС и ViPNet КУКС может достигать 85 км с использованием одного оптического коммутатора, 75 км для двух уровней коммутации и 65 км для трех уровней

03. Используется разработанный в России и основанный на квантовых эффектах физический генератор истинно случайных чисел

04. Реализована защита от атаки с расщеплением по числу фотонов (PNS-атака) с помощью алгоритма decoy-states

05. При вводе в эксплуатацию ViPNet QTS запускается в автоматическом режиме и производит смену всех ключей, что обеспечивает защиту от нарушителя с полномочиями администратора

ОСОБЕННОСТИ

> Каждый ViPNet МУКС и ViPNet РУКС содержит в себе как передатчик квантовых квазиоднофотонных состояний (Алису), так и приемник квантовых квазиоднофотонных состояний (Боба)

> Квантовозащищенные ключи передаются в СКЗИ-потребители в соответствии с рекомендациями по стандартизации ТК26 для протокола защищенного взаимодействия ККС ВРК и СКЗИ-потребителей ProtoQa, что открывает возможности мультивендорной квантовой сети

> Для проектирования ключевой системы использованы рекомендации по стандартизации ТК26 для ключевой системы полносвязной многоарендаторной сети ISTOQ-M

> Защита информации базируется на фундаментальном принципе квантовой физики о невозможности «подслушивания» квантовой информации без ее изменения (закон о запрете клонирования)

> Обеспечивается стойкость к атакам, возможным при реализации эффективного квантового компьютера. ViPNet QTS не содержит асимметричных криптографических механизмов

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

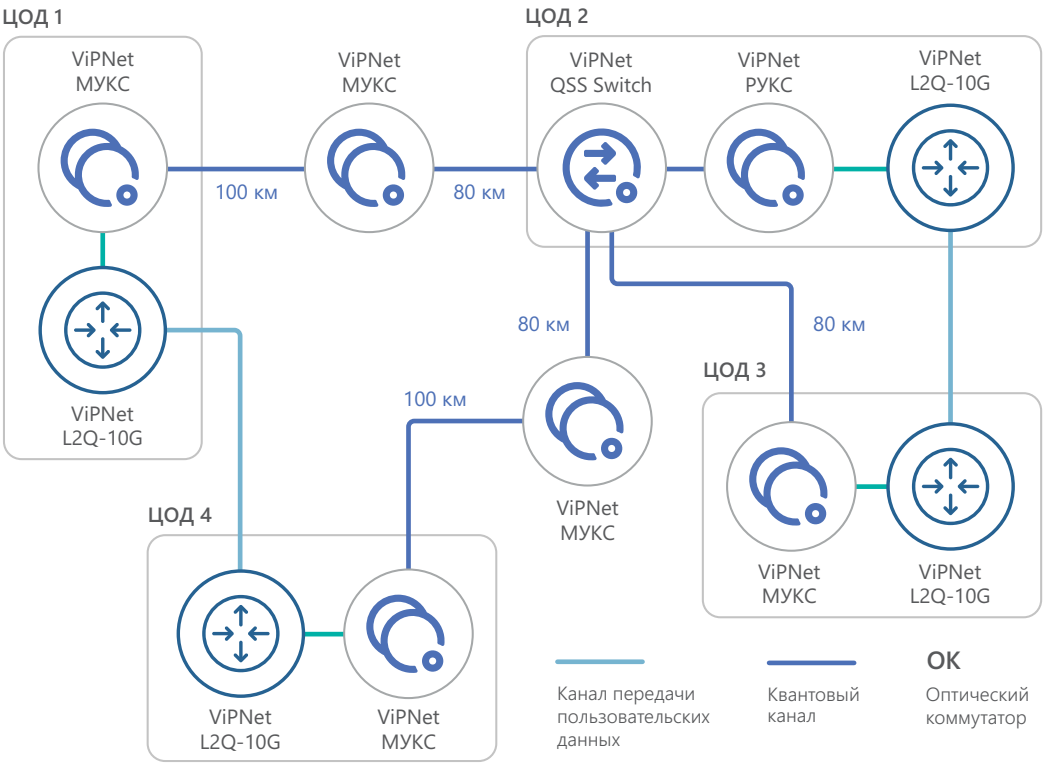


Схема 1.
Защита сети разнесенных ЦОД. Квантовая сеть с ответвлениями, созданными оптическим коммутатором.

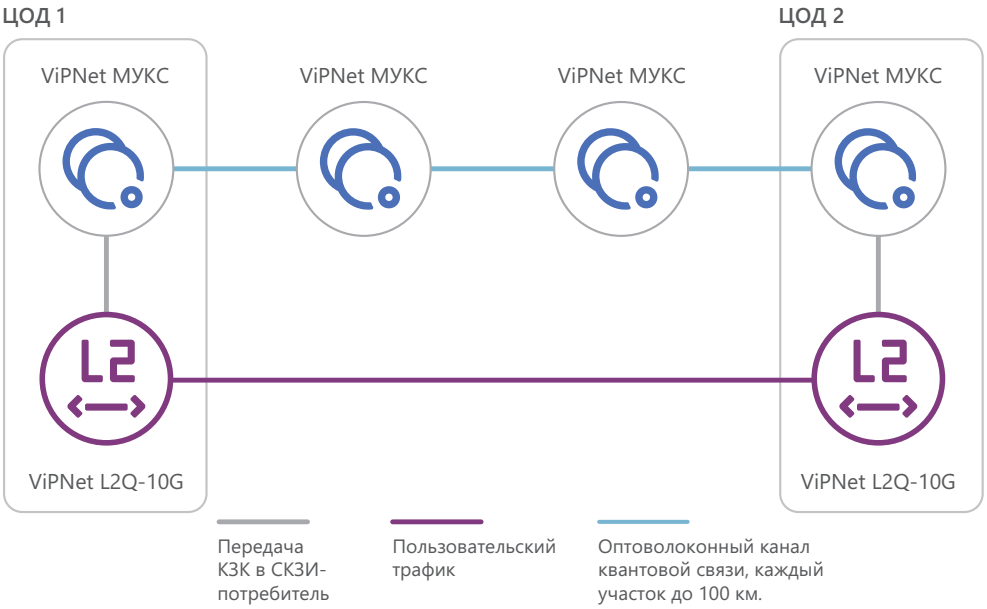
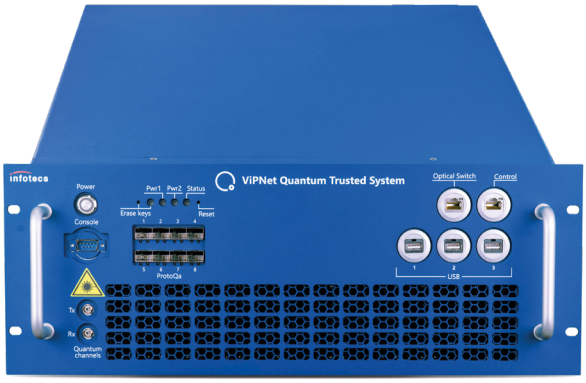


Схема 2.
Протяженная квантовая магистраль соединяет доверенными промежуточными узлами квантовой сети (ViPNet МУКС) участки до 100 км каждый в единую сеть. Пользовательский трафик между расположенными в ЦОД 1 и ЦОД 2 СКЗИ-потребителями (канальными шифраторами ViPNet L2Q-10G) защищен на квантовозащищенных ключах (КЗК).



ViPNet МУКС, ViPNet РУКС

ViPNet КУКС

	ViPNet МУКС	ViPNet РУКС	ViPNet КУКС
Назначение	Магистральный узел квантовой сети	Распределительный узел квантовой сети	Клиентский узел квантовой сети
Конструктивное исполнение	19″ 4RU		19″ 2RU
Сетевой интерфейс	Ethernet LAN 1 Гбит/с 8 портов для подключения СКЗИ-потребителей		
Оптический интерфейс	FC/UPC		
Датчик случайных чисел	Физический датчик, источник случайности основан на квантовых процессах		
Физические средства защиты	Датчик несанкционированного доступа (ДНСД) обеспечивает гарантированное удаление криптографических ключей при вскрытии корпуса. Дальнейшая работа ПАК блокируется		
Электропитание	230 В, 50 Гц, до 500 Вт		230 В, 50 Гц, до 150 Вт

СКЗИ-потребители квантово-защищенных ключей

ViPNet L2Q-10G

>> Криптографическое устройство канального уровня (по стандартной модели OSI), выполненное в форм-факторе 1U, корпус 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 упрощает IT-инфраструктуру и одновременно повышает уровень 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

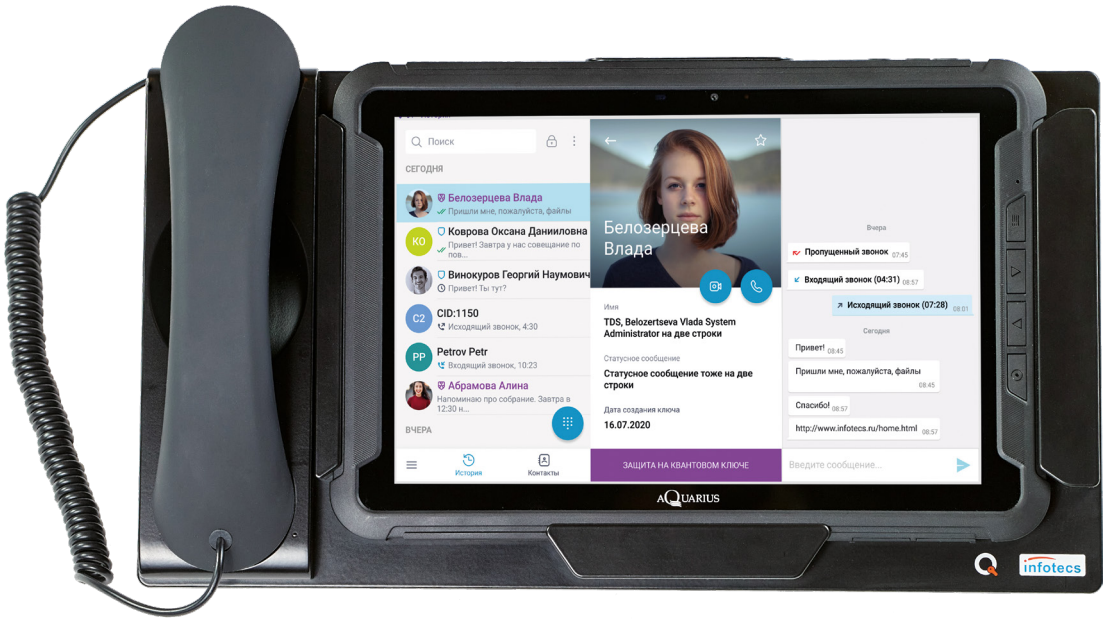
> Минимальная избыточность протокола защиты

> Поддерживает протокол защищенного взаимодействия ККС ВРК и СКЗИ-потребителей ProtoQa

> В процессе сертификации по требованиям ФСБ России к СКЗИ класса КС3

ViPNet CSS Connect HW

>> Стационарный телефонный аппарат с сенсорным экраном устанавливается в контролируемой зоне. ViPNet CSS Connect HW предназначен для осуществления конфиденциальных аудио- и видеовызовов и обмена текстовыми сообщениями между пользователями сети ViPNet, он совместим с мессенджерами ViPNet CSS Connect и системами SIP-телефонии.



01. Стационарный IP-телефон с сенсорным дисплеем

02. Модуль защиты обеспечивает размыкание цепи микрофона и светодиодную индикацию работы микрофона

03. Шифрование по алгоритмам ГОСТ 28147-89, ГОСТ Р 34.12-2015 («Кузнечик»), ГОСТ Р 34.12-2015 («Магма»)

04. Поддержка протокола защищенного взаимодействия ККС ВРК и СКЗИ-потребителей ProtoQa

05. Может размещаться в выделенных помещениях, где циркулирует речевая акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну (до 2 категории помещений)

06. Частота смены ключей до 1 раза в час

07. Получены сертификаты на соответствие требованиям ФСБ России:

> ViPNet CSS Connect HW (исп. 1) и ViPNet CSS Connect HW Special (исп. 1) – требованиям к СКЗИ, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, установленным для класса КС1

> ViPNet CSS Connect HW Special (исп. 1) – требованиям, предъявляемым к основным техническим средствам и системам (ОТСС) 4 категории и размещаемым в выделенных помещениях не выше 2 категории

ViPNet Quantum Key Distribution Simulator

Программный комплекс симуляции квантового распределения ключей (КРК) с возможностью подключения аппаратной периферии в виде оптико-механических узлов. ViPNet QKDSim наглядно демонстрирует принципы квантового распределения ключей, основанного на генерации и детектировании (считывании) оптических информационных состояний

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

В процессе симуляции участвуют 3 объекта:

> передатчик (Алиса) > приемник (Боб) > злоумышленник (Ева)

Информация в оптических состояниях кодируется и декодируется путем изменения параметров поляризации генерируемого светового потока, которые интерпретируются как параметры различных протоколов КРК.

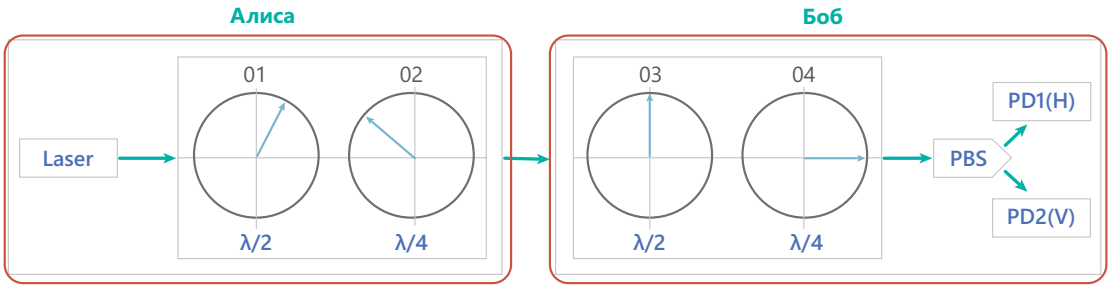
> ViPNet QKDSim позволяет на практике изучить классические и квантовые приемы передачи информации, а также рассмотреть влияние чувствительности и шумов детектора на качество квантового распределения ключей (устойчивость системы)

> Пользователь может ознакомиться с работой трех квантовых протоколов (BB84, ГОКС и B92) и разобраться в разнице режимов передачи информационных состояний (классический, однофотонный и квазиоднофотонный)

> ViPNet QKDSim демонстрирует возможности некоторых атак Евы. Программным способом выбирается атака, в результаты измерений Боба согласно установленному алгоритму вносятся искажения, и определяется успешность перехвата информации Евой для каждого отдельного случая

Пример выполнения протокола BB84.
Схема стенда соответствует схеме аппаратной платформы симулятора КРК.

Оптическая схема в программном комплексе



> Алиса случайным образом выбирает один из базисов. Затем внутри базиса случайно выбирает одно из состояний, соответствующее 0 или 1, и посылает фотоны

> Боб случайно и независимо от Алисы выбирает для каждого поступающего фотона базис плюс или базис крест и измеряет в нем значение фотона

> Для каждого переданного состояния Боб открыто сообщает, в каком базисе проводилось измерение, но результаты измерений остаются в секрете

> Алиса сообщает Бобу по открытому классическому каналу, какие измерения были выбраны в соответствии с исходным базисом Алисы

> Пользователи оставляют только те случаи, в которых выбранные базисы совпали. Эти случаи переводят в биты (0 и 1), и составляют ключ

СЕРТИФИКАЦИЯ

ViPNet Quantum Trusted System Lite (ViPNet QTS Lite)

В 2023 ViPNet РУКС Лайт и ViPNet КУКС Лайт получили сертификаты соответствия ФСБ России:

> временным требованиям к квантовым криптографическим системам выработки и распределения ключей для средств криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, установленным для класса КС.

> требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, установленным для класса КС3.

ViPNet Quantum Trusted System (ViPNet QTS)

Проводятся тематические исследования ViPNet QTS для последующей сертификации в ФСБ России на соответствие:

> временным требованиям к квантовым криптографическим системам выработки и распределения ключей для средств криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, установленным для класса КС и в перспективе для класса КВ.

> требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, установленным для класса КС3 и в перспективе для класса КВ.

infotecs

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

soft@infotecs.ru
hotline@infotecs.ru

www.infotecs.ru

QCS24_00RU

ViPNet Virtual Private Network