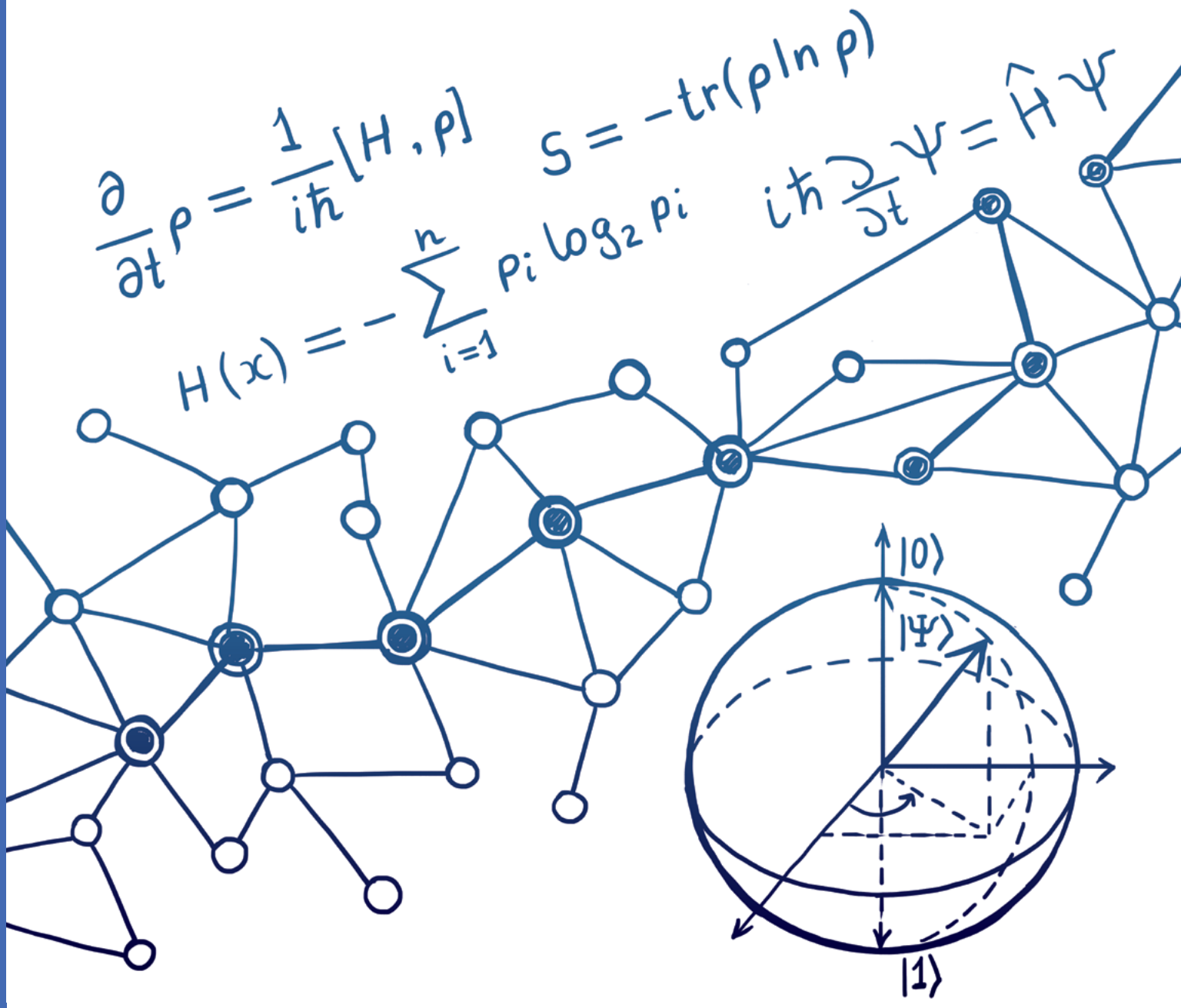
инфотекс

ViPNet Quantum Cryptographic Systems

Квантовые криптографические системы



Квантовая сеть Санкт-Петербурга

Конвергентная сеть ИнфоТеКС			
ViPNet QTS Lite	ИнфоТеКС Артиллерийская	ViPNet РУКС Лайт ViPNet КУКС Лайт ViPNet QSS Switch ViPNet CSS Connect HW	1 шт. 3 шт. 1 шт. 29 шт.
	ИнфоТеКС Парфеновская		

Квантовая телефонная сеть руководства ПАО «Газпром» в «Лахта Центр»			
ViPNet QTS Lite	Башня МФЗ КЗС	ViPNet РУКС Лайт ViPNet КУКС Лайт ViPNet QSS Switch ViPNet CSS Connect HW	1 шт. 3 шт. 1 шт. 25 шт.

Магистральная квантовая сеть РЖД

Защита каналов связи			
ViPNet QTS	Москва – Сочи	ViPNet РУКС ViPNet L2Q-10G	55 шт. 5 шт.

Квантовые сети Москвы

Университетская квантовая сеть			
ViPNet QTS Lite	ИнфоТеКС Отрадное	ViPNet КУКС Лайт ViPNet CSS Connect HW ViPNet РУКС Лайт ViPNet QSS Switch	5 шт. 23 шт. 1 шт. 1 шт.
	МГУ Воробьевы горы		
	МГУ Моховая		
	Кластер Ломоносов (АНО НТЦ ЦК)		
Конвергентная сеть ИнфоТеКС			
ViPNet QTS Lite	ИнфоТеКС Отрадное	ViPNet РУКС Лайт ViPNet КУКС Лайт ViPNet QSS Switch ViPNet CSS Connect HW	1 шт. 3 шт. 1 шт. 49 шт.
	ИнфоТеКС Аэропорт		
Защита каналов ИнфоТеКС			
ViPNet QTS	ИнфоТеКС Отрадное	ViPNet РУКС ViPNet L2Q-10G	3 шт. 3 шт.
	ИнфоТеКС Мишина		
	ИнфоТеКС Аэропорт		
Межуниверситетская квантовая сеть			
ViPNet QTS	НИЦ «Курчатовский институт»	ViPNet РУКС ViPNet L2Q-10G ViPNet QSS Switch	3 шт. 3 шт. 2 шт.
	МГУ Воробьевы горы		
	МТУСИ Авиамоторная		

Квантовые сети Томска

Большой университет Томска			
ViPNet QTS	ТУСУР Ленина	ViPNet РУКС ViPNet L2Q-10G	2 шт. 2 шт.
	ИнфоТеКС Кирова		
Сеть ТУСУР			
ViPNet QTS Lite	ТУСУР Ленина	ViPNet РУКС Лайт ViPNet КУКС Лайт ViPNet QSS Switch ViPNet CSS Connect HW	1 шт. 3 шт. 1 шт. 3 шт.

Томск

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.

ViPNet РУКС-Б

распределительный узел квантовой сети – Боб, с оптическим блоком приемника квантовых состояний, центральный узел сети, обеспечивающий выработку ключей между всеми узлами сети через подключаемые оптические коммутаторы ViPNet QSS Switch. Предназначен для построения топологии «точка-точка» на решениях ViPNet РУКС-Б и ViPNet КУКС или построения топологии «звезда».

ViPNet QSS Switch

оптический коммутатор, обеспечивающий переключение оптических каналов связи при работе квантовой криптографической системы. ViPNet QSS Switch не выполняет преобразований сигнала, а лишь оптически коммутирует 12 выходов.

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

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

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

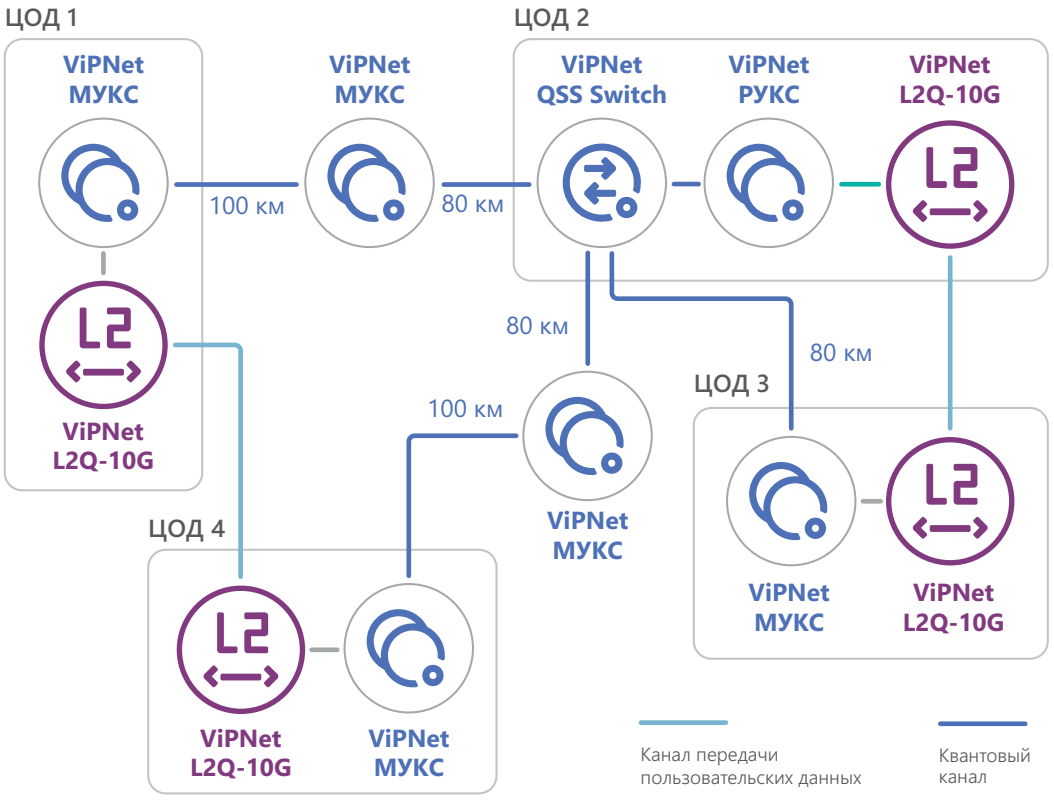


Схема 1.
Защита сети разнесенных ЦОД. Квантовая сеть с ответвлениями, созданными оптическим коммутатором.

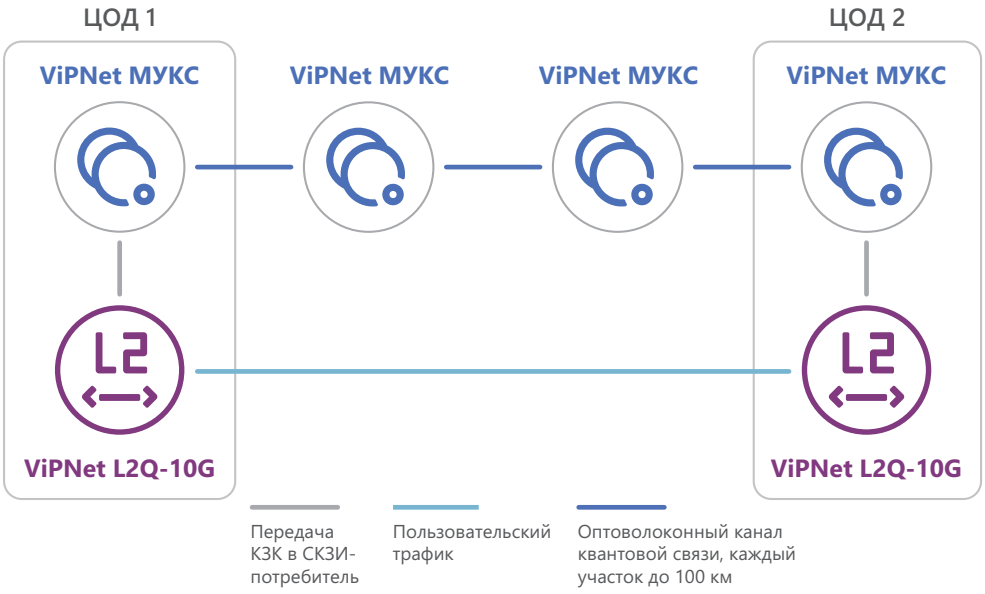


Схема 2.
Протяженная квантовая магистраль соединяет доверенными промежуточными узлами квантовой сети (ViPNet МУКС) участки до 100 км каждый в единую сеть. Пользовательский трафик между расположенными в ЦОД 1и ЦОД 2 СКЗИ-потребителями (канальными шифраторами ViPNet L2Q-10G) защищен на квантовозащищенных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

ViPNet РУКС-Б

ViPNet QSS Switch

	ViPNet РУКС-Б	ViPNet QSS Switch
Назначение	Распределительный узел квантовой сети – Боб	Оптический коммутатор
Конструктивное исполнение	19” 2RU	19” 1RU
Сетевой интерфейс	Ethernet LAN 1 Гбит/с 8 портов для подключения СКЗИ-потребителей	Ethernet LAN 1 Гбит/с
Оптический интерфейс	FC/UPC	FC/UPC, Входных – 1; 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 150 Вт	220 В, 50 Гц, 15 Вт

ViPNet Quantum Random Number Generator

Квантовый генератор случайных чисел ViPNet QRNG — это устройство, создающее истинно случайные последовательности на основе непредсказуемых квантовых явлений. В отличие от псевдослучайных алгоритмов, ViPNet QRNG обеспечивает абсолютную непредсказуемость, что критически важно для шифрования

ViPNet QRNG

Принцип работы ViPNet QRNG основывается на детектировании квазиоднофотонного светодиодного излучения и его последующей математической обработки. В качестве источника квазиоднофотонного излучения применяется полупроводниковый светодиод. Светодиод работает в непрерывном режиме, что повышает темп поступления фотонов на детектор. Путь прохождения квазиоднофотонного излучения от светодиода к фотодетектору максимально короткий и недоступен для перехвата, наблюдения или воздействия извне. В отличие от псевдослучайных программных датчиков, QRNG обеспечивает абсолютную непредсказуемость, что критически важно как для любого СКЗИ, но и для систем квантового распределения ключей.

ПРЕИМУЩЕСТВА

01. Квантовая природа процесса не позволяет предсказывать получаемую последовательность

02. Полученная последовательность случайных чисел дополнительно защищена криптографическим способом

ОБЛАСТЬ ПРИМЕНЕНИЯ

> Криптография

> Статистические расчеты

> Финансовое моделирование

> Экспериментальные науки

> Искусственный интеллект

СКЗИ-потребители квантово-защищенных ключей

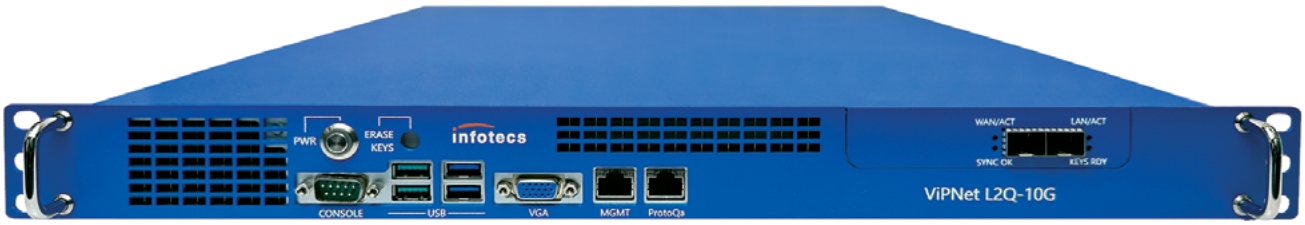
ViPNet L2Q-10G

>> ПАК ViPNet L2Q-10G – шлюз безопасности, обеспечивающий криптографическую защиту данных, передаваемых по каналам Ethernet: темная оптика, MAN, WAN, выделенный канал.

ViPNet L2Q-10G обеспечивает высокую производительность и сверхнизкие задержки, благодаря чему является идеальным решением для реализации защиты критических сервисов, чувствительных к задержкам и пропускной способности канала связи, а также является эффективным средством защиты каналов связи между ЦОД.

ПАК ViPNet L2Q-10G представляет собой устройство 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 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
- Сертификат ФСБ России по требованиям к СКЗИ класса КС3



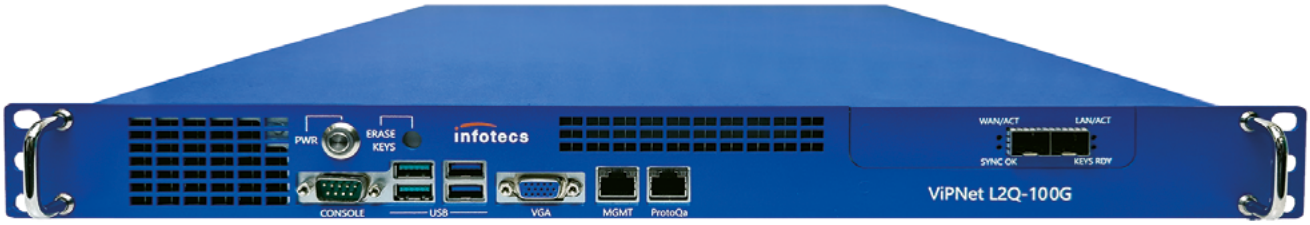
ViPNet L2Q-100G

>> ПАК ViPNet L2Q-100G – шлюз безопасности, обеспечивающий криптографическую защиту данных, передаваемых по каналам Ethernet: темная оптика, MAN, WAN, выделенный канал.

ViPNet L2Q-100G обеспечивает высокую производительность и сверхнизкие задержки, благодаря чему является идеальным решением для реализации защиты критических сервисов, чувствительных к задержкам и пропускной способности канала связи, а также является эффективным средством защиты каналов связи между ЦОД.

ПАК ViPNet L2Q-100G представляет собой устройство 1U, корпус которого спроектирован с учетом жестких требований безопасного функционирования: защита от несанкционированного вскрытия, энергонезависимое хранилище ключей шифрования, резервирование электропитания.

- Высокая производительность шифрования (до 100 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



СКЗИ-потребители

>> ViPNet CSS Connect HW представляет собой стационарный телефонный аппарат с сенсорным экраном, предназначенный для общения пользователей сети ViPNet по защищенному каналу.

ViPNet CSS Connect HW используется для конфиденциального общения через защищенный мессенджер ViPNet CSS Connect и для организации кроссплатформенных защищенных видеоконференций.

ViPNet CSS Connect HW представляет собой специализированное устройство, предназначенное для обеспечения безопасных бизнес-коммуникаций посредством технологии ViPNet с использованием квантовозащищенных ключей, полученных через протокол ProtoQa от ККС ВРК.

ViPNet CSS Connect HW сочетает в себе функции и возможности IP-телефона и планшета на базе операционной системы Android и может использоваться в качестве основного настольного аппаратного телефона для пользователей.

Функциональные возможности, заложенные в этот продукт, позволяют осуществлять голосовое общение пользователей ViPNet CSS Connect, видеозвонки, звонки внутри SIP-инфраструктуры на любой SIP-телефон внутри организации и участие в аудио- и видеоконференциях.

Таким образом, все коммуникации пользователя выполняются через единственное техническое средство, что сокращает затраты на эксплуатацию и поддержку коммуникационных систем.

ПРЕИМУЩЕСТВА

01. Симметричное шифрование данных, устойчивое к атакам с использованием квантового компьютера
02. Защита от нарушителя с полномочиями администратора информационной безопасности благодаря автоматической смене всех ключей сразу после ввода в эксплуатацию
03. Интеграция с существующими сетями ViPNet VPN
04. Сертифицировано ФСБ России по требованиям к СКЗИ класса КС1

Основные характеристики устройства

> 7-дюймовый дисплей с сенсорным управлением и интуитивно понятным пользовательским интерфейсом
> Проводная телефонная трубка, держатель для левшей и правшей
> Gigabit Ethernet (10/100/1000) с 2-портовым коммутатором
> Встроенная камера
> Встроенный Wi-Fi-адаптер
> Интегрированный PoE

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Протоколы/стандарты	TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP, ICMP, DNS, DHCP, PPPoE, NTP, 802.1x, ViPNet®
Сетевые интерфейсы	Два переключаемых порта 10/100/1000 Мбит/с со встроенным модулем PoE/PoE+
Графический дисплей	Емкостный сенсорный ЖК-экран диагональю 8,0" (1280 × 800), 10 точек касания, IPS
Камера	Камера с КМОП-матрицей, защитной шторкой и регулировкой угла наклона, 2 Мп, 1080p, 30 к/с
Bluetooth	Да, встроенный модуль Bluetooth 5.0
Wi-Fi	Да, двухдиапазонный (2,4 и 5 ГГц) с 802.11 a/b/g/n/ac/ax, 2T2R, Wi-Fi Display и AirPlay
Дополнительные разъемы	Разъем RJ9 для гарнитуры (поддерживает EHS-гарнитуры с адаптером Plantronics), разъем 3,5 мм для стереогарнитур с микрофоном, разъем USB 3.0, Type-C, HDMI (выход), HDMI (вход)
Голосовые кодеки и возможности	Широкополосный Opus, G.729A/B
Видеокодеки и возможности	Интеграция с системами ВКС по протоколу SIP или API, разрешение видео до 1080p, частота кадров до 30 к/с, битрейт до 4 Мбит/с, видео с камеры (до 1080p, 30 к/с) + демонстрация экрана (до 1080p, 15 к/с), технология предотвращения мерцания, автофокус и автоэкспозиция
Функции телефонии	Удержание, адресная книга, журнал вызовов, ожидание вызова, отправка сообщений во время разговора
HD-аудио	Да, два всенаправленных микрофона, HD-гарнитура и динамик с поддержкой широкополосного звука
Безопасность	Защита каналов связи с использованием технологии ViPNet. Симметричная криптография, алгоритмы ГОСТ 34.12-2018, 34.13-2018, длина ключа 256 бит, слот для замка Kensington Lock
Питание и энергоэффективность	В комплект поставки входит универсальный адаптер питания. Вход: 100–240 В переменного тока; 50–60 Гц; выход: 12 В постоянного тока, 1,5 А (18 Вт); встроенный модуль PoE 802.3af, класс 3, PoE+ 802.3at, класс 4

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:

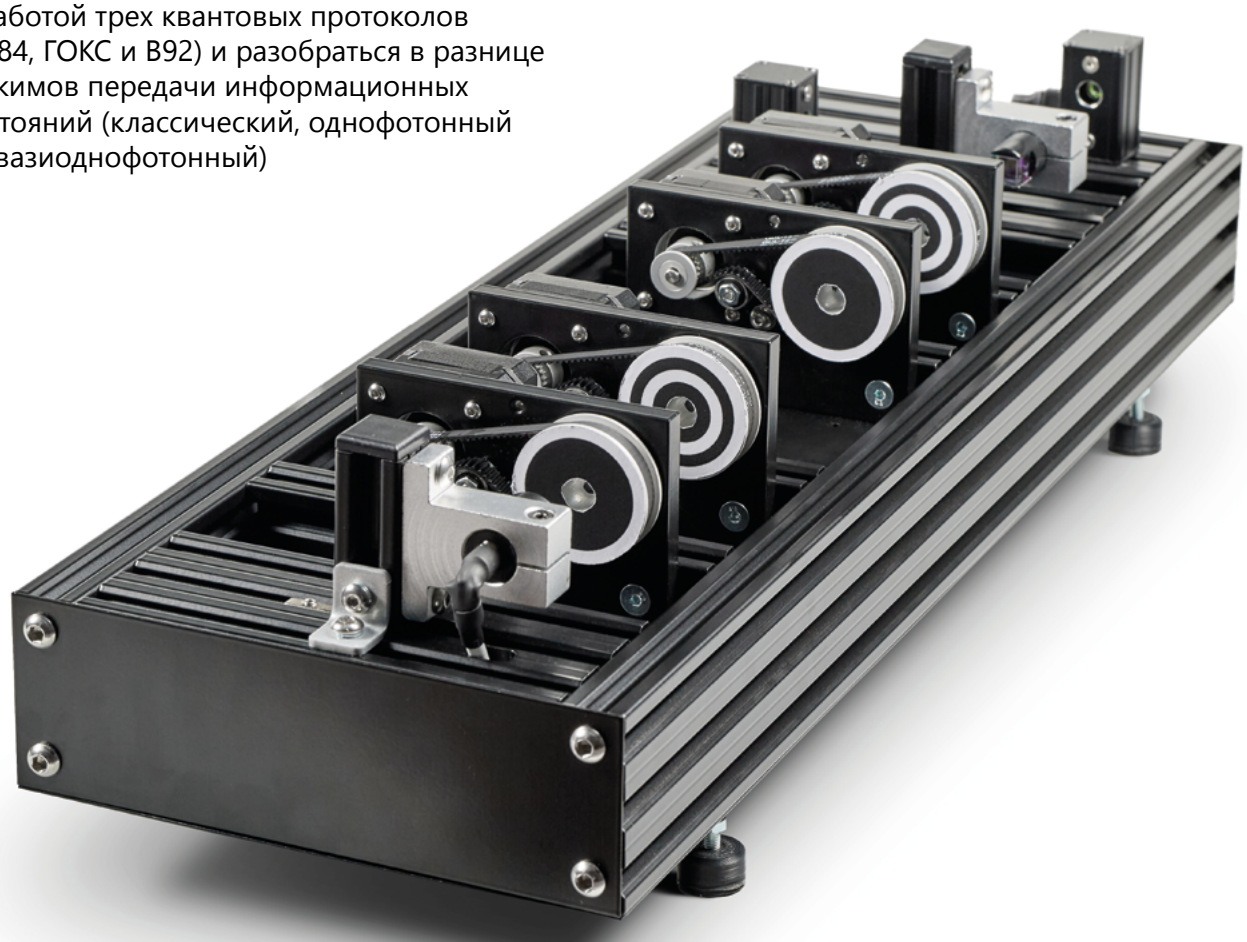
> передатчик (Алиса) > приемник (Боб) > злоумышленник (Ева)

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

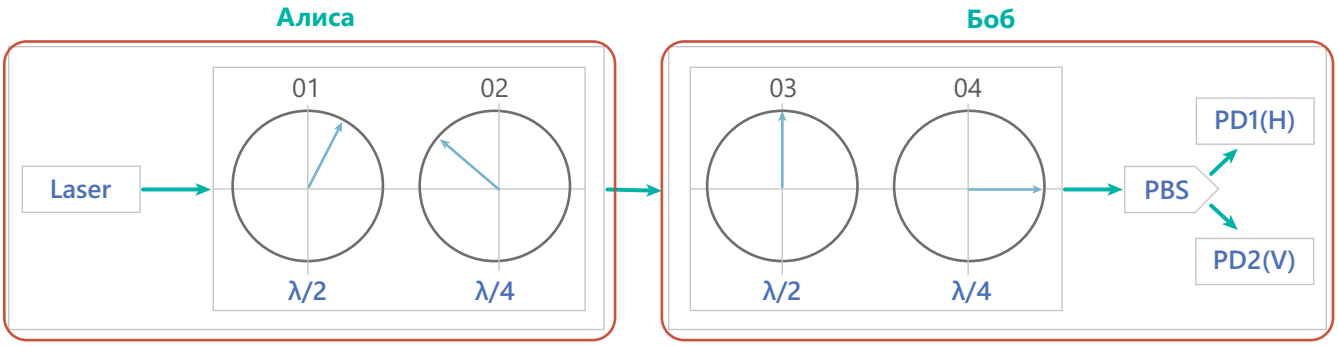
> ViPNet QKDSim позволяет на практике изучить классические и квантовые приемы передачи информации, а также рассмотреть влияние чувствительности и шумов детектора на качество квантового распределения ключей (устойчивость системы)

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

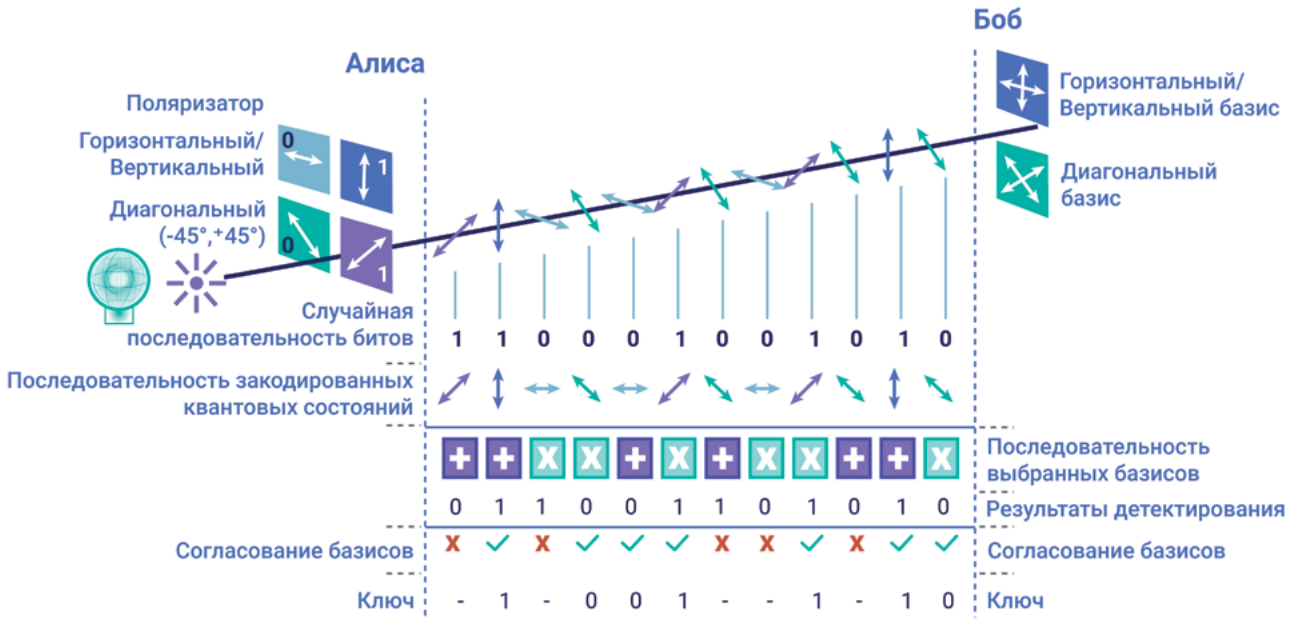
> ViPNet QKDSim демонстрирует возможности некоторых атак Евы. Программным способом выбирается атака, в результаты измерений Боба согласно установленному алгоритму вносятся искажения, и определяется успешность перехвата информации Евой для каждого отдельного случая



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



Оптическая схема в программном комплексе



Поляризационное кодирование в квантовом протоколе BB84

> 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 (ViPNet QTS)

ViPNet РУКС соответствует:

> 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.

Проводятся тематические исследования ViPNet КУКС 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.

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

инфотекс

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

soft@infotecs.ru
hotline@infotecs.ru

www.infotecs.ru

QCS26_00RU

ViPNet Virtual Private Network