Ежегодная международная научно-практическая конференция
«РусКрипто’2019»

Аппаратная криптографическая защита данных в высокоскоростных сетях Ethernet

Александр Иванов
Российская Корпорация Средств Связи

Средства защиты передаваемых данных

- Прикладной уровень (Layer 5÷7)
  - Защита обмена данных между приложениями или сервисами
- Сетевой/Транспортный уровень (Layer 3÷4)
  - Защита передачи данных между IP-узлами или IP-сессиями
- Канальный уровень (Layer 2)
  - Защита Ethernet трафика

Прикладной уровень

- End-to-End защита данных между приложениями и/или сервисами
- Инвариантность относительно сетевых топологий
- Толерантность к задержкам передачи данных
- Гибкость механизмов обмена и генерации ключей
- Требования к производительности исходят от приложения

(допущение: скорость передачи >> производительности)

Сетевой/Транспортный уровень

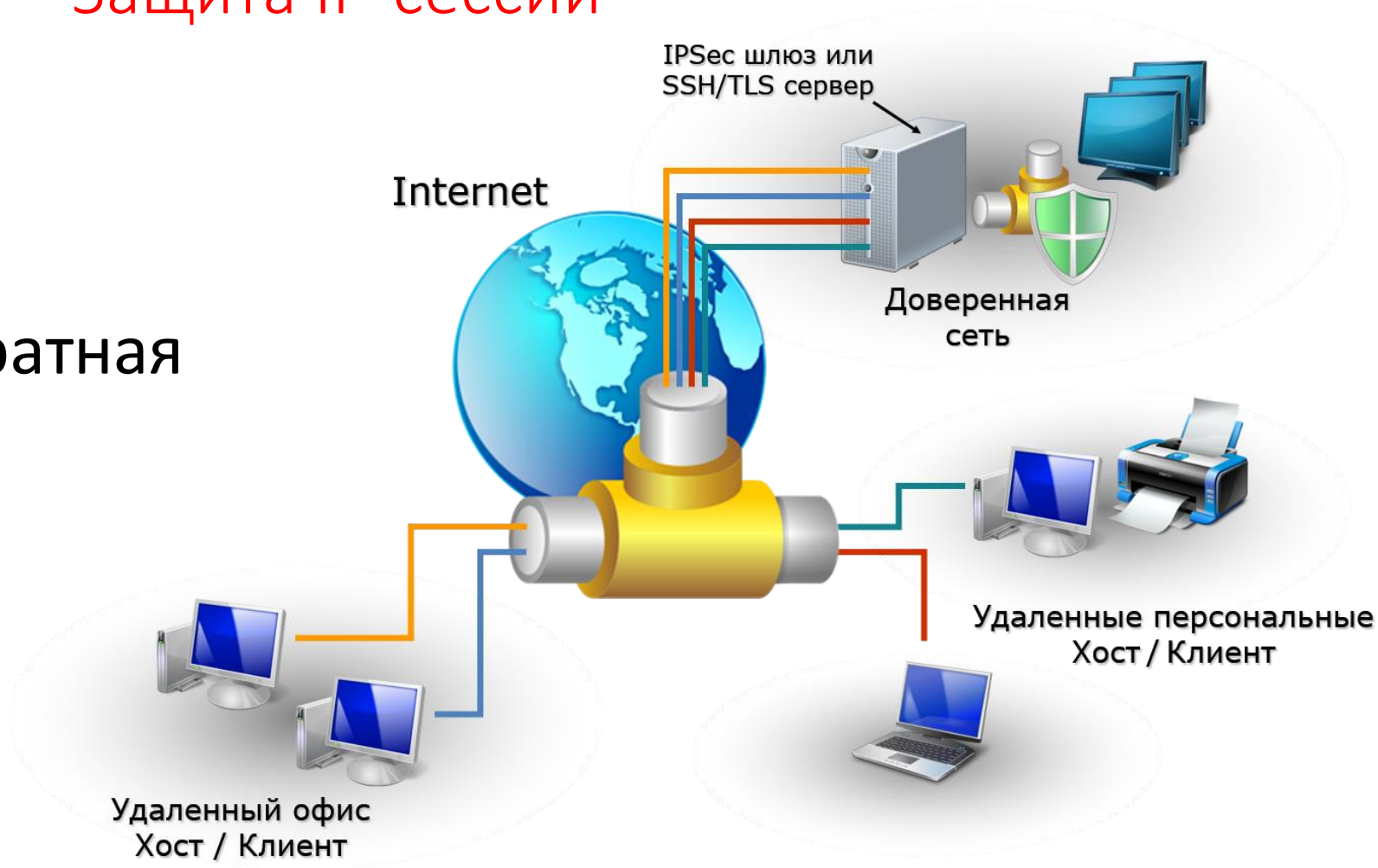
- End-to-End защита IP-узлов или IP-сессий
- Гибкость при построении IP-туннелей
- Наличие стандартизированных решений (IPSec, SSH/TLS)
- Усложнение конфигурирования и увеличение загрузки серверов
- Требования к производительности и к задержкам передачи данных соотносятся с сетевыми требованиями

(требования зависят от особенностей сетевого трафика)

Транспортный уровень

Защита IP-сессий

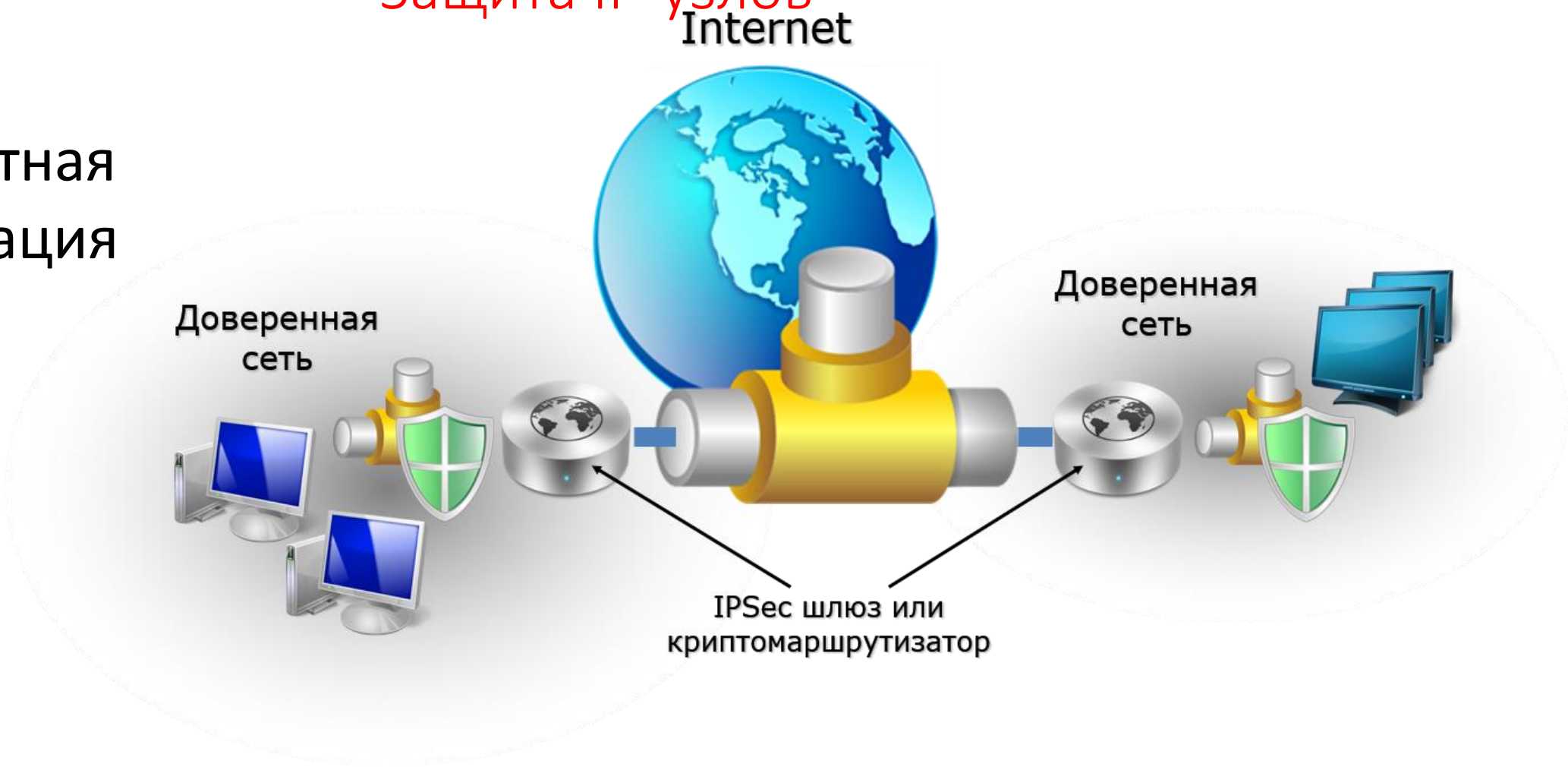
Программно-аппаратная реализация



Сетевой уровень

Защита IP-узлов

Аппаратная реализация



Канальный уровень

- Защита данных Ethernet трафика (защита Ethernet Payload)
- Защита физического соединения (защита Ethernet кадра)
- Отсутствие стандартизированных решений (исключая MACSec)
- Простота конфигурирования
- Требования к производительности к задержкам передачи данных определяются характеристиками канала связи

(требования к каналообразующему оборудованию)

Канальный уровень
защита Ethernet трафика

Аппаратная реализация

Формирование ключей шифрования

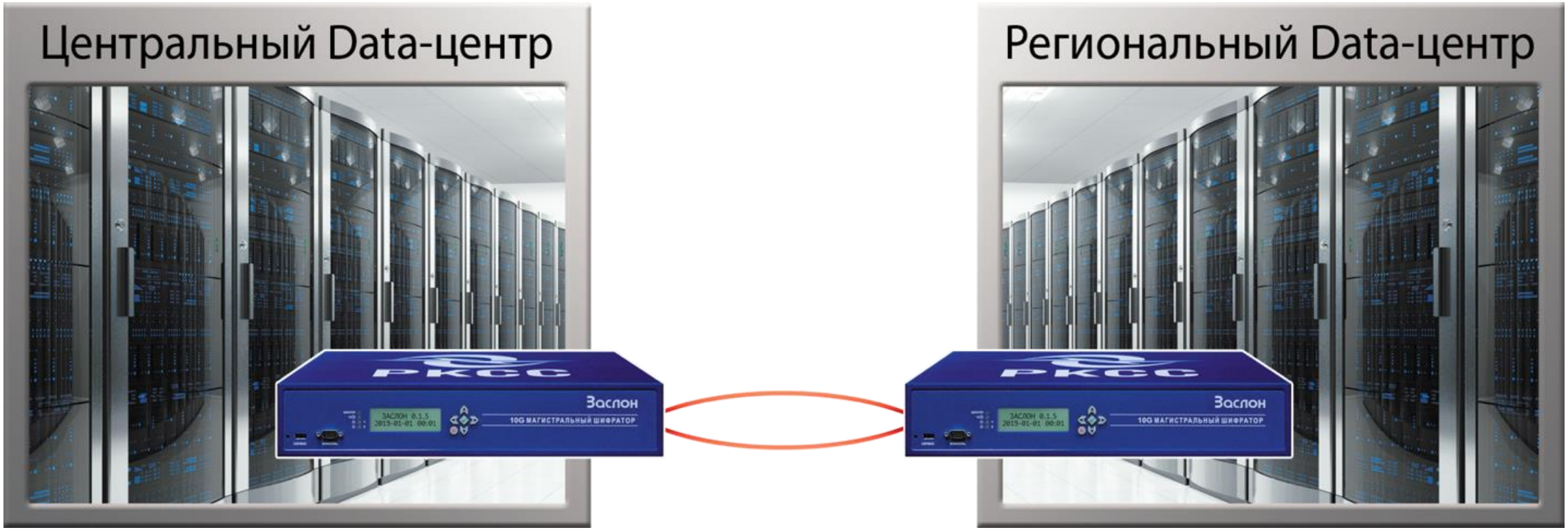
Layer 3: IP (Internet Protocol) - на основе IP-адреса

Layer 2.5: MPLS (Multiprotocol Label Switching) - с учетом метки MPLS

Layer 2: Ethernet - на основе MAC-адреса

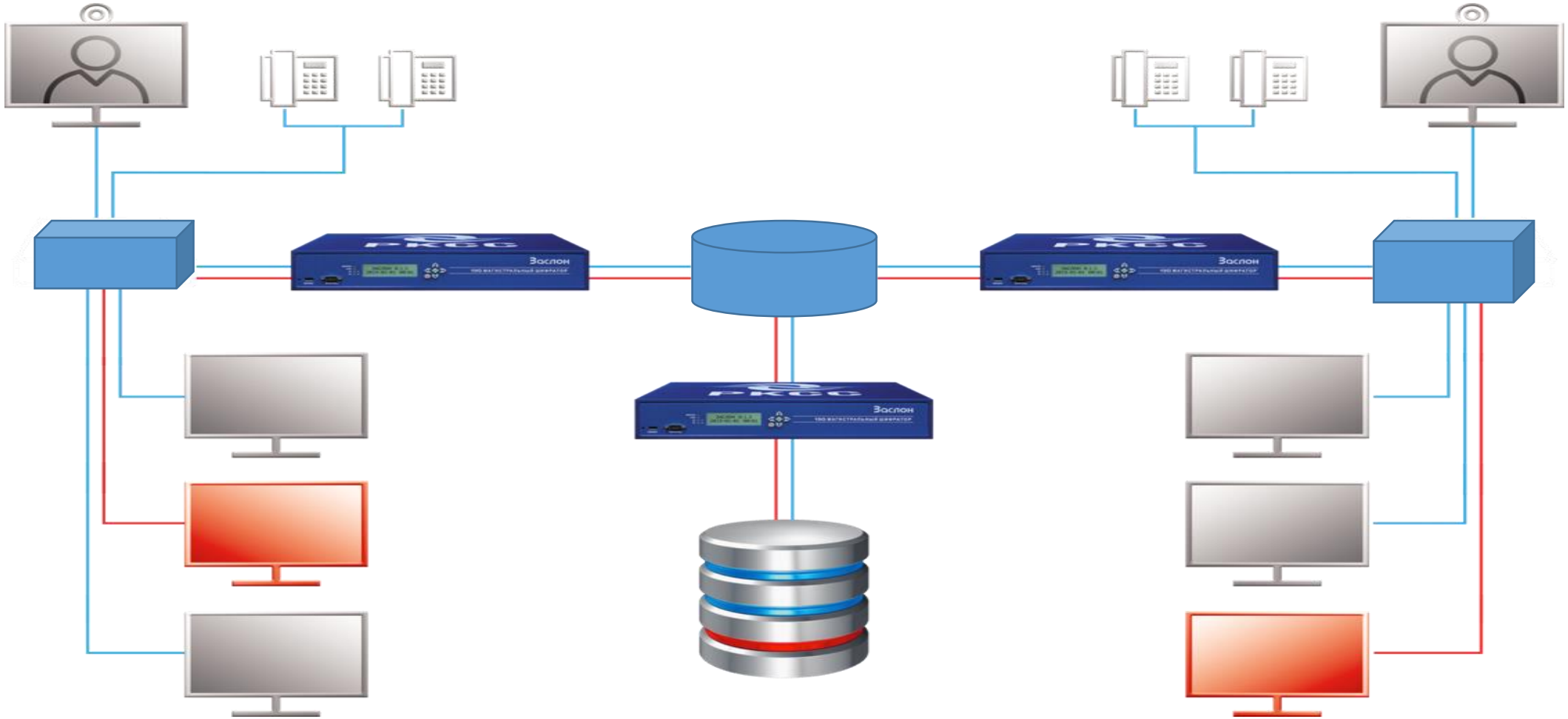
Использование в сетях Ethernet

Распределенные Data-центры



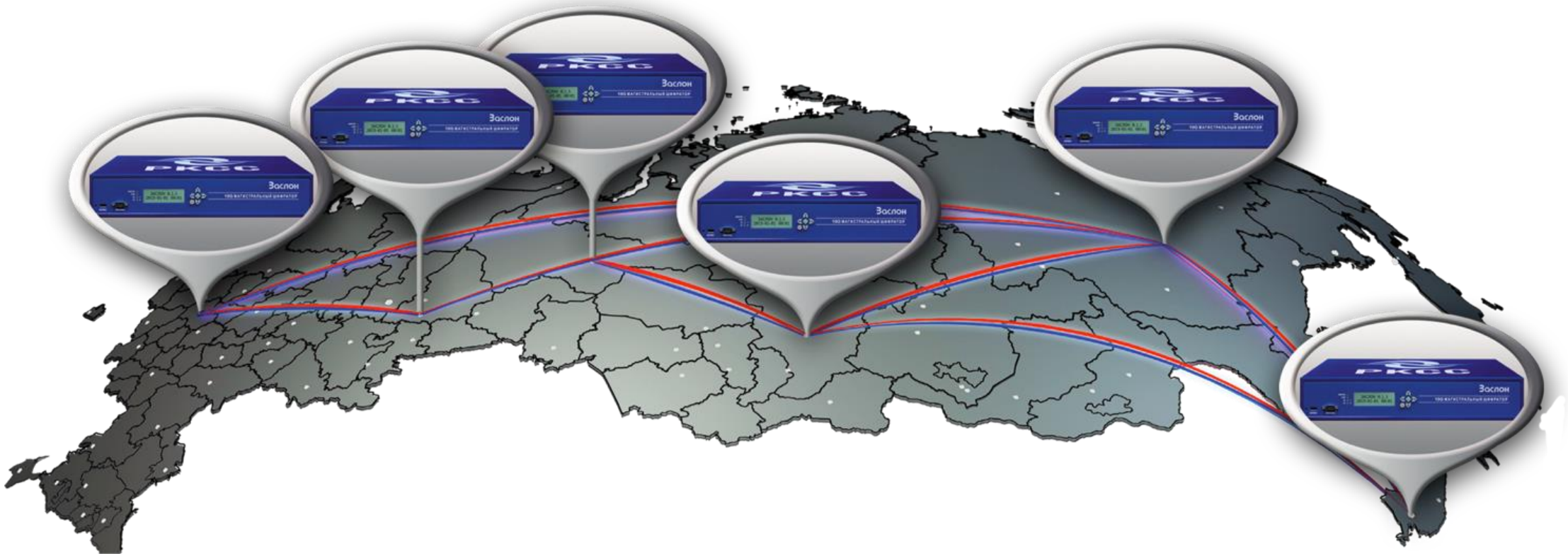
Использование в сетях Ethernet

Защищенные сегменты корпоративных сетей



Использование в сетях Ethernet

Магистральные каналы передачи данных операторов связи



Основные тактико-технические характеристики

- Максимальное заполнение канала со скоростью физического соединения (x10Гбит/с до 100Гбит/с)
- Минимальная задержка (x1μs)
- Минимальный джиттер (x0.1μs)
- Поддержка больших (Jumbo) кадров
- Число защищаемых направлений
- Поддержка основных сетевых серевисов и протоколов (Flow Control, VLAN, MPLS, …)
- Отказоустойчивость:

✓Режим отказоустойчивого кластера (в том числе и попитанию)

✓Время наработки на отказ (x10000 часов)

Важные потребительские характеристики

Принцип «Включай и работай»:

- Без необходимости изменения существующей сетевой инфраструктуры
- Большой объем загружаемой ключевых данных (на несколько лет) с автоматическим отслеживанием расходования и замены
- Несекретный статус оборудования без ключевой информации
- Наличие защиты от несанкционированного доступа
- Автоматическое тестирование и отчет о состоянии устройства в режиме реального времени
- Мониторинг по протоколам SMNP
- Единая система мониторинга и управления с графическим интерфейсом
- Централизованная смена ключей и обновления ПО

Ведущие зарубежные производители

- Atmedia (http://www.atmedia.de/en/index.html)

Ethernet (Layer 2) und IP (Layer 3) encryption 10G/40G < 5µs,

IP-Tunnel mode: Layer 2 over IPv4 or IPv6 (IP or UDP)

- Gemalto (https://safenet.gemalto.com/data-encryption/network-encryption) модель Safenet Ethernet Encryptor CN9120 - 100 Gbps < 2µs
- IDQuantique (http://www.idquantique.com)
- Rohde & Schwarz Cybersecurity (https://cybersecurity.rohde-schwarz.com/en/products/secure-networks/ethernet-encryption-rsrsitline-eth) модель R&S®SITLine ETH 40G < 3µs

Ведущие зарубежные производители

Secunet (http://www.secunet.com/en/topics-solutions/high-security/sina/sina-l2-box/)

Securosys(https://www.securosys.ch/layer-2-encryptor-centurion)

10G/40G < 5µs

Senetas (http://www.senetas.com) Senetas CN9000 - 100G < 2µs

Ведущие зарубежные производители

- Thales (https://www.thalesesecurity.com/products/data-motion-encryption-hardware/datacryptor-5000-series) модель Datacryptor 5000 Series - 10 Gbps: ≤ 4 µsec
- ViaSat (https://www.viasat.com/products/data-in-transit-encryption-for-enterprises) - MACsec IEEE 802.1 100 Gbps

Отечественные разработки

Магистральный шифратор «Заслон-МК» (РКСС)

- Аппаратное шифрование со скоростью физического соединения 10 Гбит/с минимальной задержкой (5µs) и с нулевым джиттером (0.3 µs).
- Фрагментация с настраиваемым размером MTU
- Поддержка Jumbo-кадров, Flow Control, VLAN и MPLS
- Резервирование в режиме отказоустойчивого кластера

- Запас ключевого материала на более чем на 2 года бесперебойной работы
- Синхронизация и мониторинг криптографического материала
- Автоматическая локальная и централизованная удаленная смена ключей шифрования
- Аппаратная генерации ключа шифрования для каждого передаваемого пакета
- 255 одновременных сессий шифрования
- Аппаратная защита от несанкционированного доступа
- Хранение криптографического материала и алгоритмов шифрования в зашифрованном виде
- Инициализация устройства только по ключам активации
- Энергонезависимое хранение ключа активации с возможностью экстренного стирания

Сертифицированный модуль шифратора «Заслон-4»

- Максимальное заполнение канала со скоростью физического соединения
- Минимальные задержки, сравнимые с характеристиками коммуникационного оборудования:

  5μs для кадра 64 байт

  27μs для кадра 1518 байт

  72μs для Jumbo-кадра 9216 байт
- Нулевой джиттер – 0.3μs
- Отчет о состоянии устройства в режиме реального времени
- Графический WEB-интерфейс управления
- Интерфейс командной строки
- Мониторинг по протоколам SMNP
- Журналы событий – тревожный, аудиторский и событийный

Отечественные разработки

Фактор-ТС

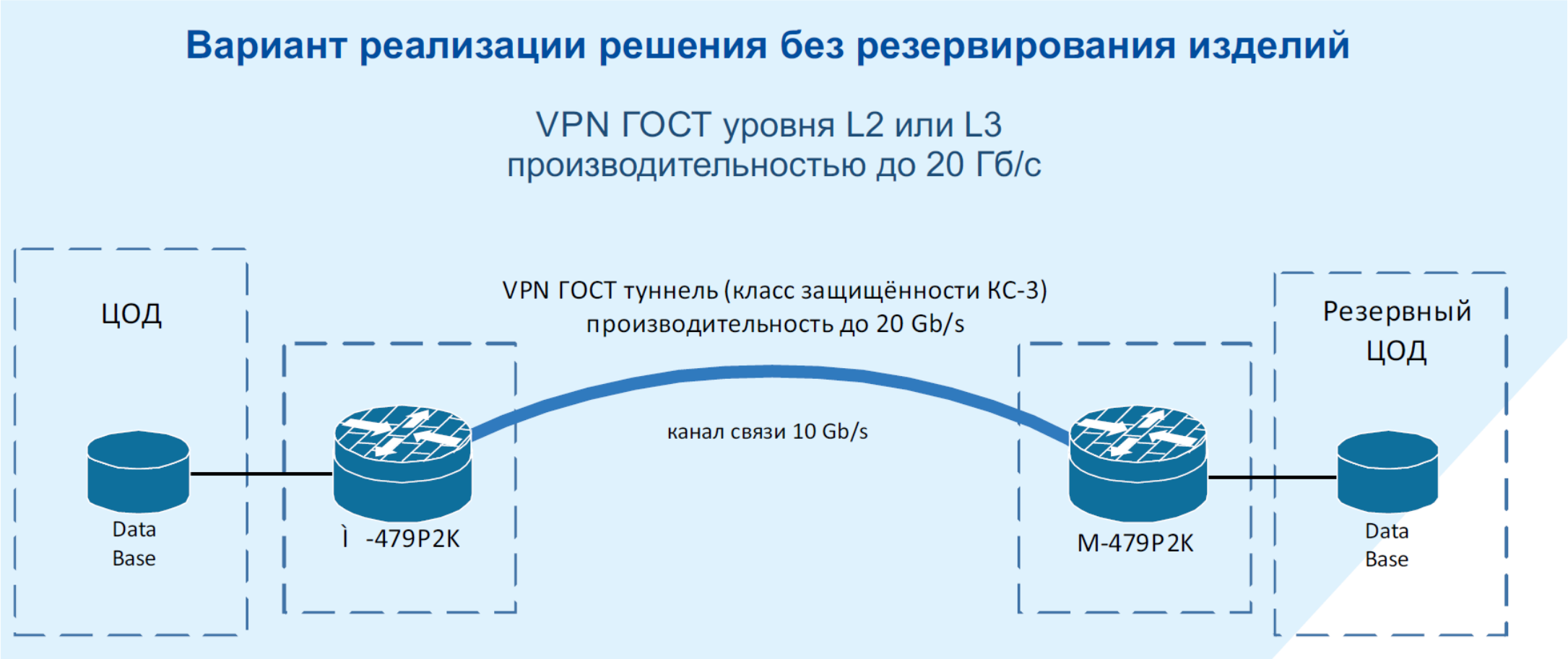
Криптомаршрутизатор

M-479P2K

Характеристики

Количество интерфейсов	12
Максимальная скорость криптографической обработки, Мбит/с	до 19 000
Максимальная производительность кадров в секунду	20 000 000
Конструктив	4Ux19” со встроенной консолью управления
Кол-во L3 VPN туннелей (криптотуннелей)	до 256
Кол-во L2 VPN туннелей (криптотуннелей)	8
Количество изделий в сети	не ограничено (до 10 000 устройств в одной ключевой зоне)
Наличие перешифрования	да

Криптомаршрутизатор М-479Р2К



Вопросы

Контактная информация

Электронная почта:

Ivanov-ag@rkcc.ru

Телефон:

+7 495 9-333-555

Сайты:

www. pkcc.ru www.zaslon-ip.ru