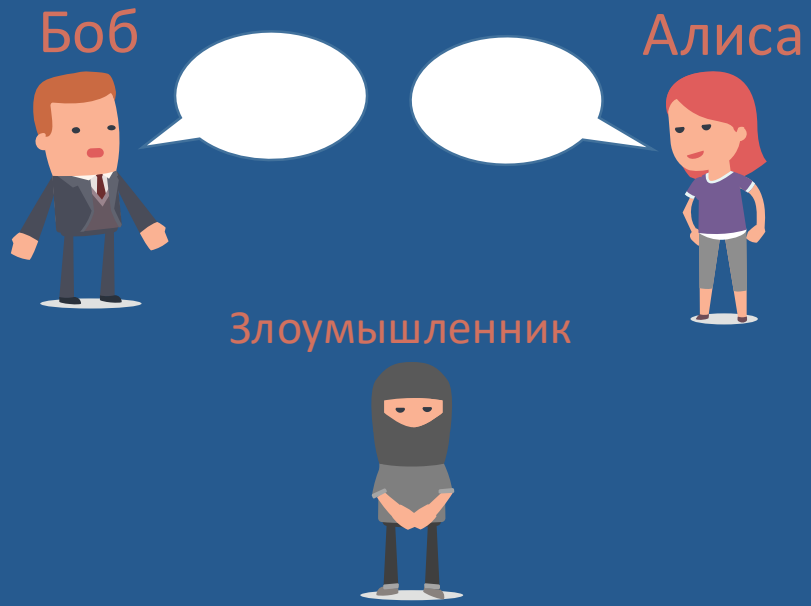
Квантовые технологии в информационной безопасности

Гарантия секретности
Доверие к информационной системе

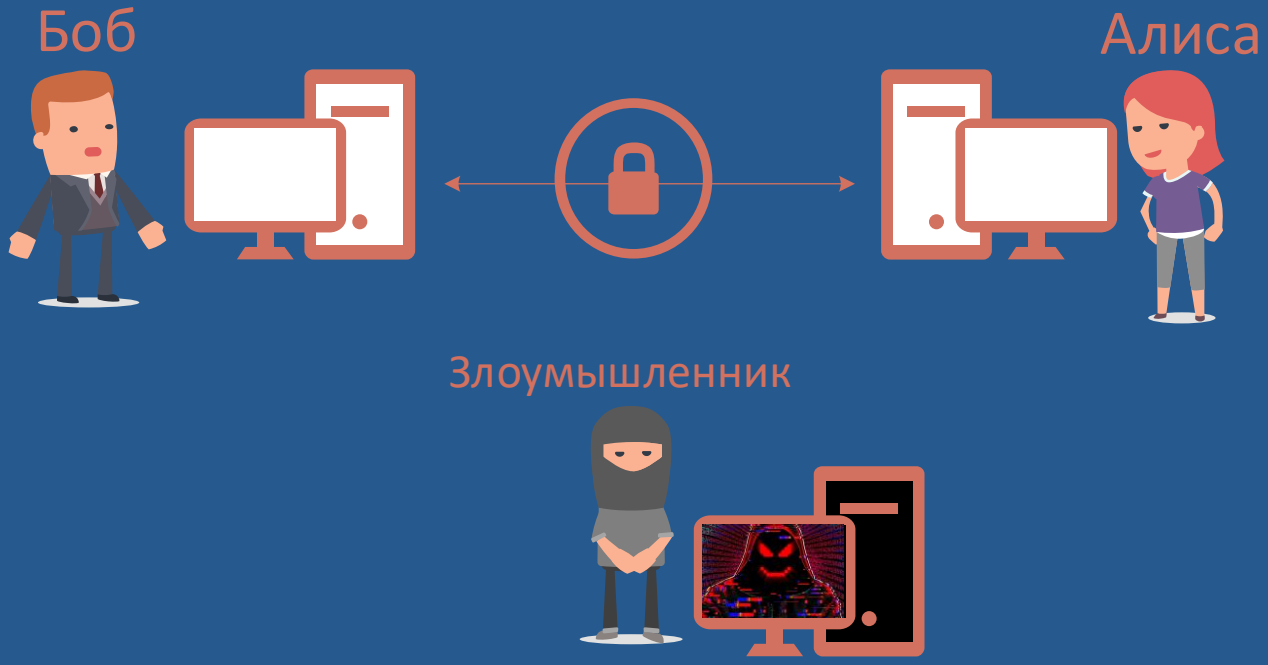
Александр Михайлович Поздняков

Криптография и Информационная безопасность

Основные действующие лица



Криптографическая защита информации



Основа криптостойкости

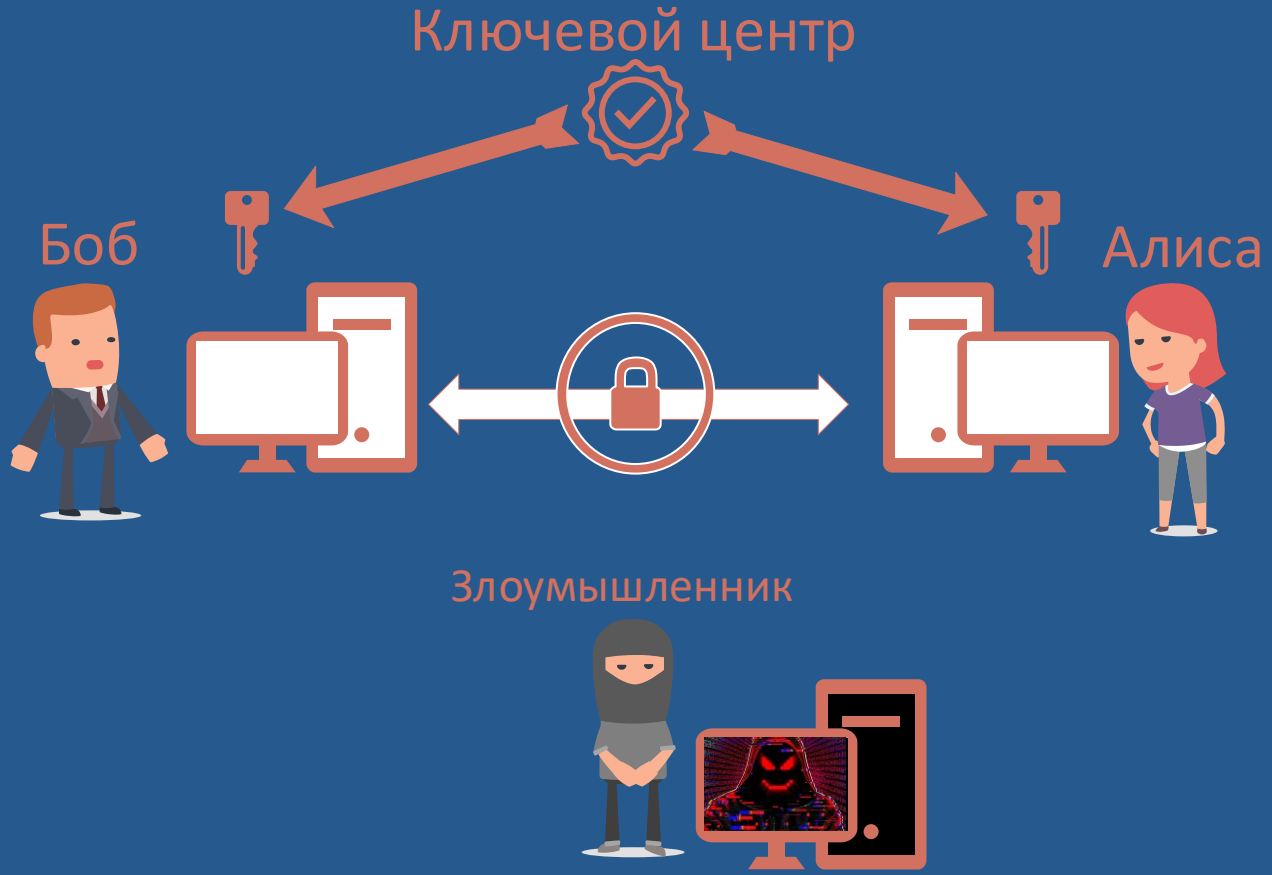
Базовый принцип проектирования средств криптографической защиты информации:

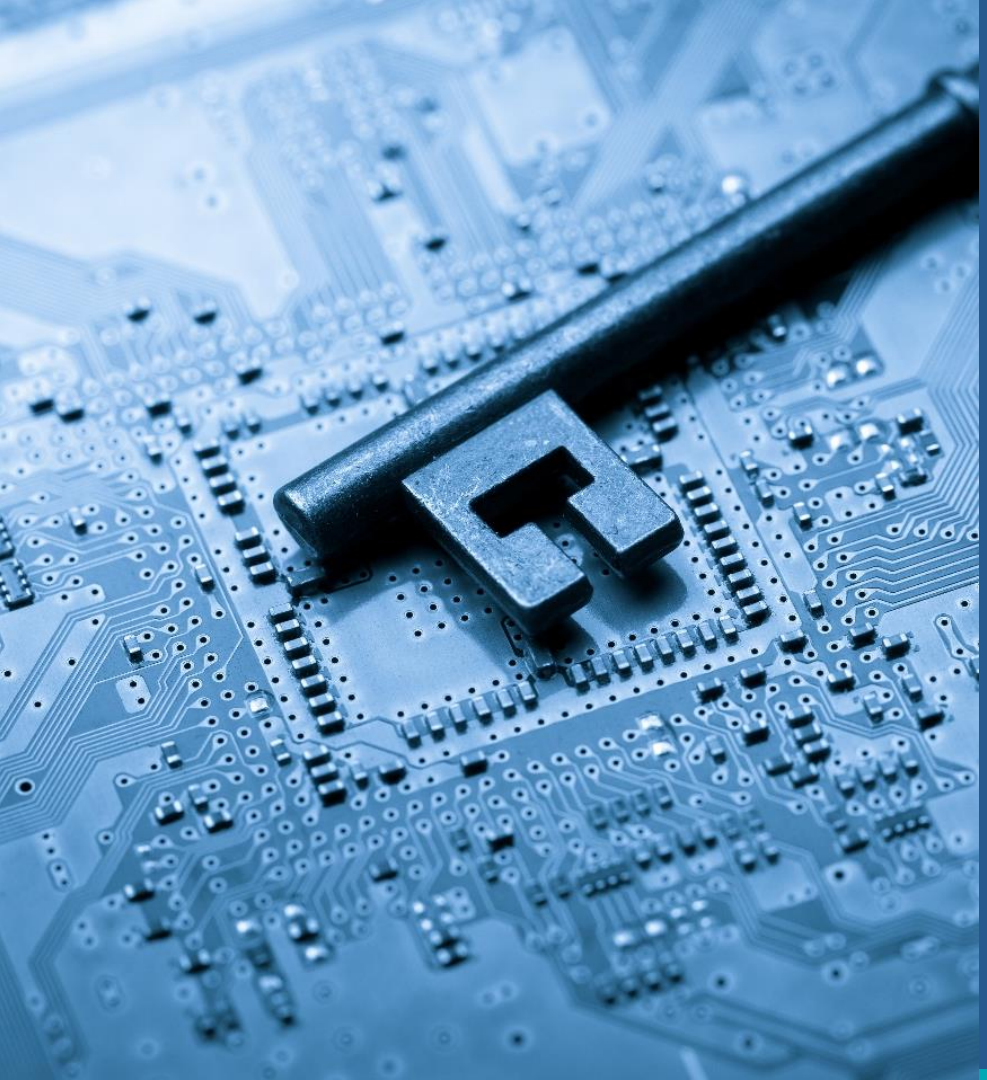
- Секретность алгоритмов шифрования и секретность аппаратной реализации **не определяют** стойкость криптосистемы
- Стойкость криптосистемы определяется лишь **секретностью ключа**

Остается главный вопрос:

Откуда взять ключ?

Криптографическая защита информации





Существует два подхода:

- Доверенный курьер **доставляет ключи** из ключевого центра

  или

- Ключи **вычисляют** при условии двусторонней аутентификации (ассиметричные алгоритмы)

Особенности всех классических механизмов распределения ключей

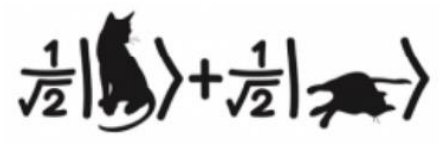
- Дорогостоящие организационно-технические меры. Чем больше людей, участвующих в процессе, тем сложнее обеспечить секретность
- **Не обеспечивается** доказуемая секретность ключей. Доверие к ключам основано лишь на предположении, что у злоумышленника нет достаточного количества вычислительных ресурсов и предположении о том, что злоумышленнику не известен эффективный алгоритм взлома. (**Доказать**, что такого алгоритма нет, **невозможно**)
- Большое влияние «человеческого фактора»
- Создание квантового компьютера приведет к компрометации всех ассиметричных криптографических алгоритмов и протоколов на их основе (DH, RSA, ECDSA TLS/SSL, HTTPS, IPsec, X.509) и снижению стойкости симметричных протоколов
- Не обеспечивают быструю смену ключей автоматически, без участия администратора

Квантовая криптография

Новый вид СКЗИ с использованием технологии квантового распределения ключей

Секретность выработки квантовых ключей основана на следующих принципах:

1. Фотон неделим
2. Невозможно клонировать неизвестное квантовое состояние
3. Невозможно измерить квантовое состояние без его изменения
4. Невозможно различить два неортогональных квантовых состояния



Преимущества технологии квантового распределения ключей

1. Безусловная **секретность** квантовых ключей **доказаная** математически
2. Выработка ключей и загрузка в шифратор происходит автоматически – **без** участия администратора
3. Обеспечивается стойкость к криптографическим атакам при помощи квантового компьютера
4. Высокая скорость смены ключей

Базовые элементы квантовой криптографической системы

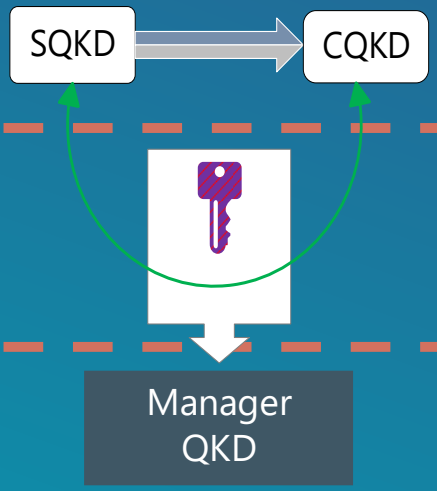


Общий алгоритм КРК

Настройка квантового канала

Создание и передача квантовых состояний

Измерение квантовых состояний



Процедуры выработки секретной согласованной последовательности и процедуры усиления секретности

Управление квантовыми ключами

Защищенное взаимодействие с использованием квантовых ключей

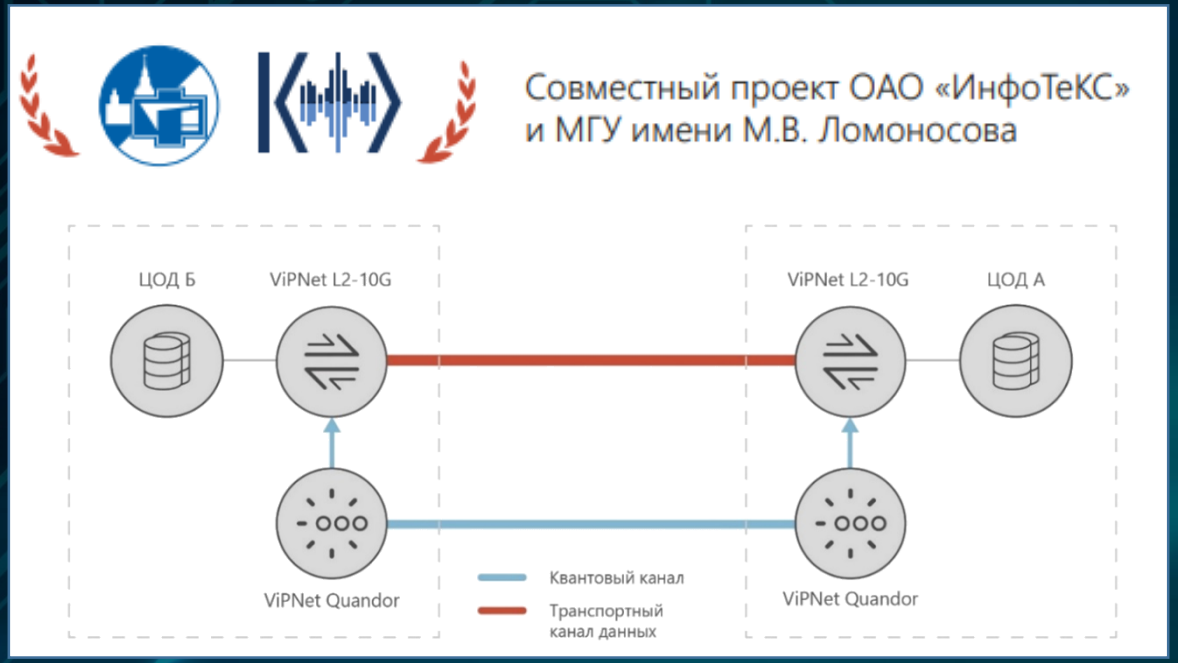




infotecs

ViPNet Quandor

Комплекс автоматической доверенной доставки криптографических ключей



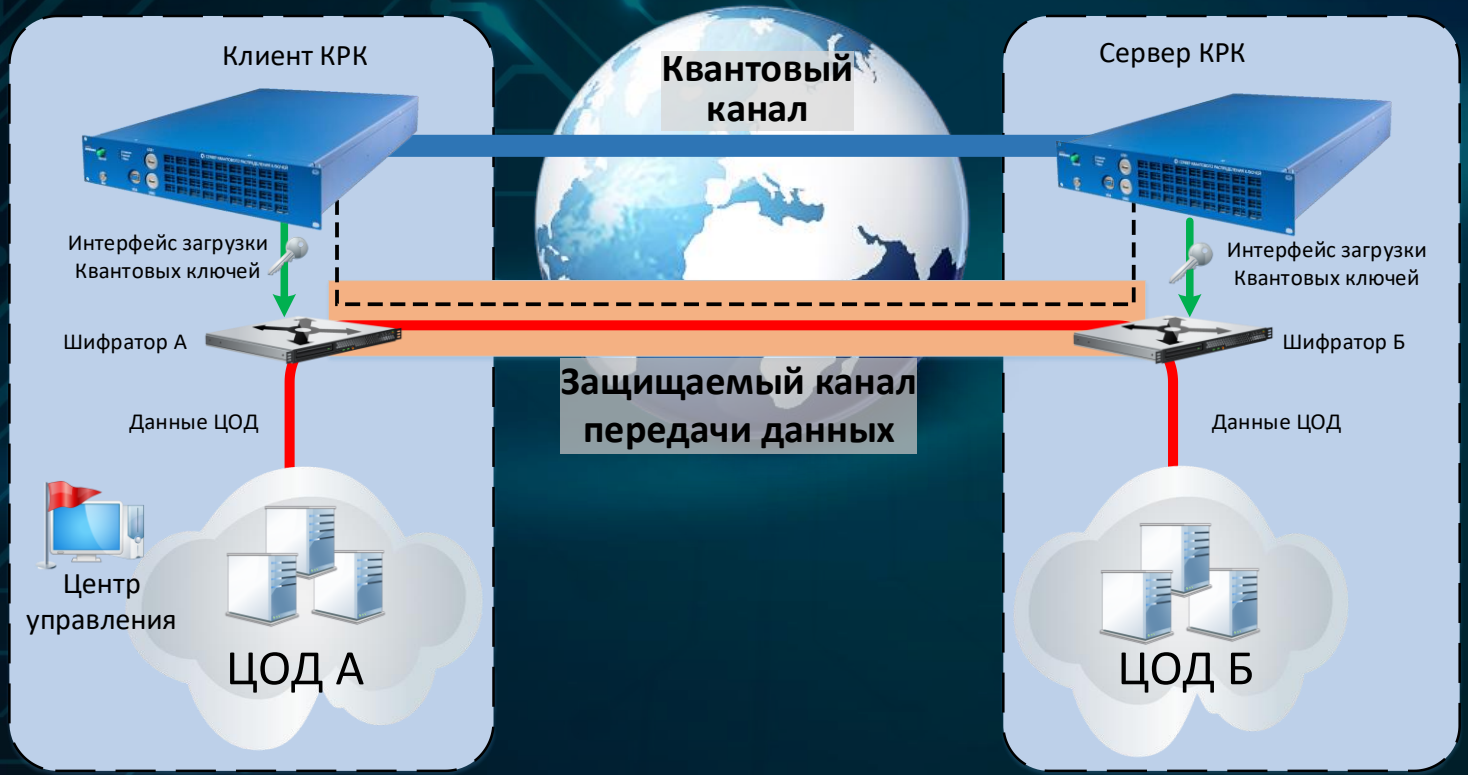
infotecs

ViPNet Quandor

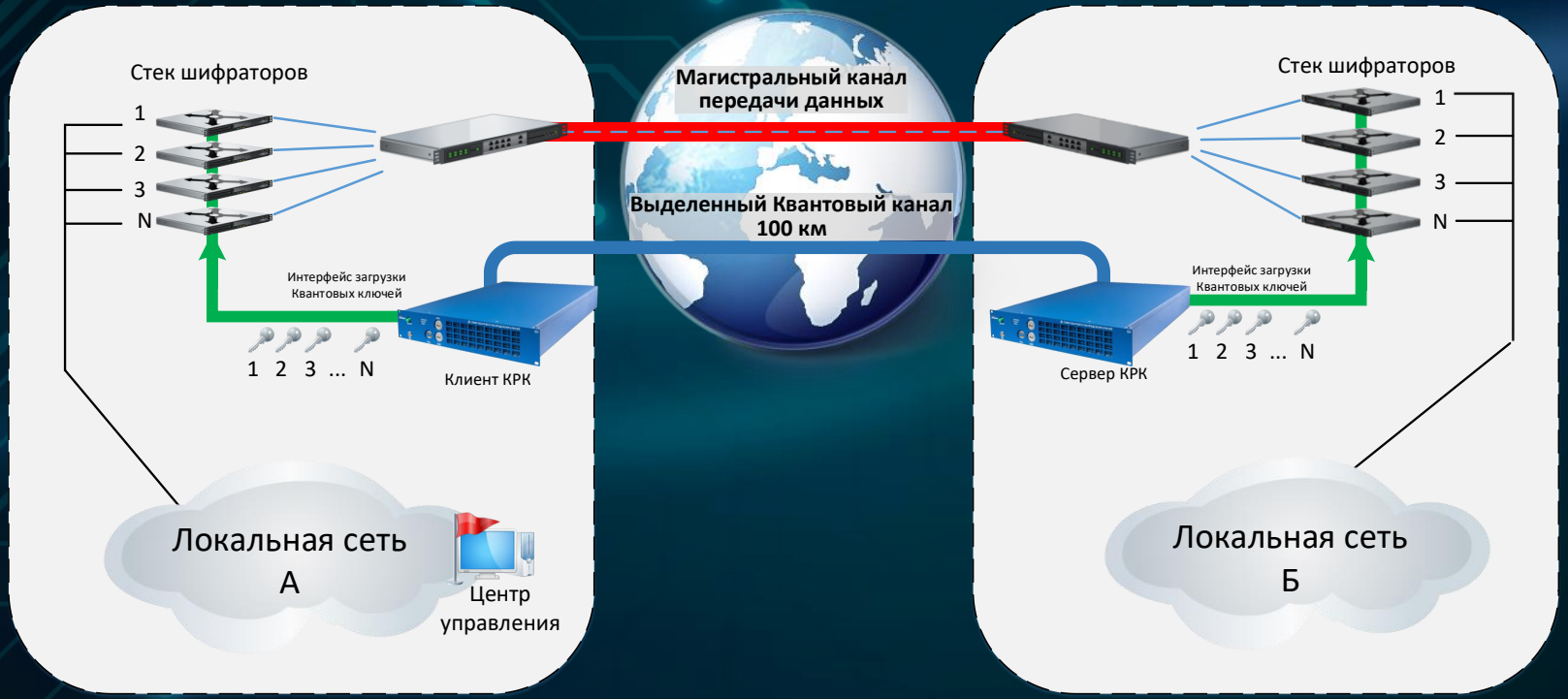
Базовый сценарий – автоматическая доверенная доставка криптографических ключей для канальных шифраторов ViPNet L2.

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

Каналы данных



Защита нескольких каналов



Особенности решения ViPNet Quandor

- Длина квантового канала 100 км
- Не требует дополнительного охлаждения
- Устанавливается в стандартную серверную стойку
- Автоматическая смена ключей не реже чем 1 раз в минуту
- Гибридная ключевая система
- СКЗИ класса КС3
- Стойкость к атакам, возможным при реализации эффективного квантового компьютера
- Математически доказанная стойкость протокола КРК

В процессе исследования 8 центром ФСБ России

Отечественное серийное производство



- Собственное производство
- Предсерийный образец
- Прошел все инженерные испытания
- На стадии сертификации в ФСБ России
- Готовность к пилотным внедрениям и поставкам

ViPNet L2-10G

Шифратор канального уровня, в форм-факторе 1U, корпус которого спроектирован с учетом жестких требований безопасного функционирования:

- защита от несанкционированного вскрытия,
- энергонезависимое хранилище ключей шифрования,
- резервирование электропитания.



- Производительность шифрования до 10 Гбит/с
- Задержка не более 15 мкс
- Автоматизированный контроль выработки нагрузки на ключ и «бесшовный» переход на новый ключ. Позволяет упростить IT-инфраструктуру при одновременном увеличении уровня информационной безопасности
- Топология сети шифраторов «точка-точка»
- Поддержка Jumbo frames – 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

Вопросы



Спасибо за внимание!

Александр Михайлович Поздняков

Aleksandr.Pozdnyakov@infotecs.ru

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow