infotecs

ViPNet Quandor
Обзор продукта и планы развития

Александр Поздняков

ViPNet Quandor

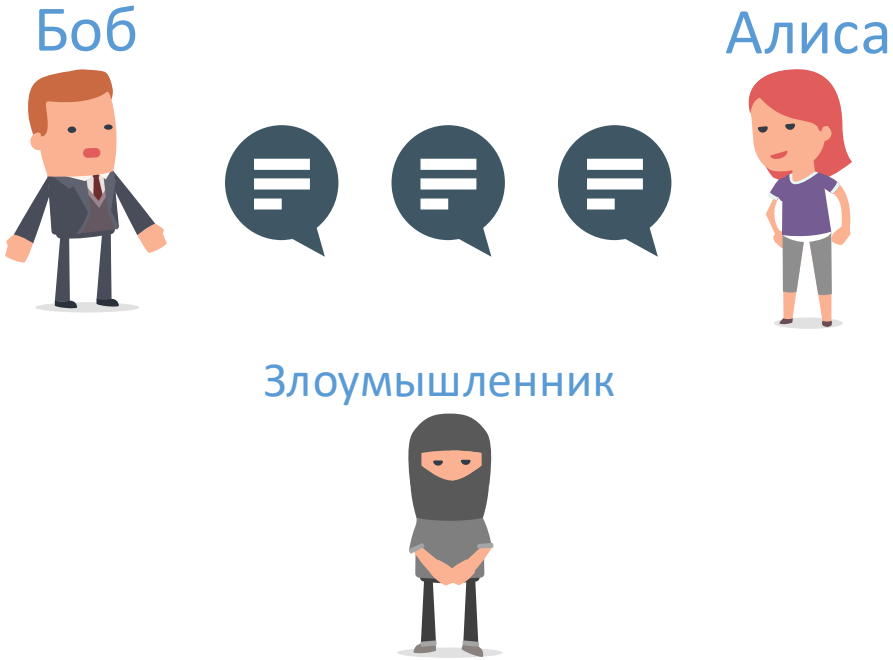
Система автоматической доверенной доставки криптографических ключей

infotecs

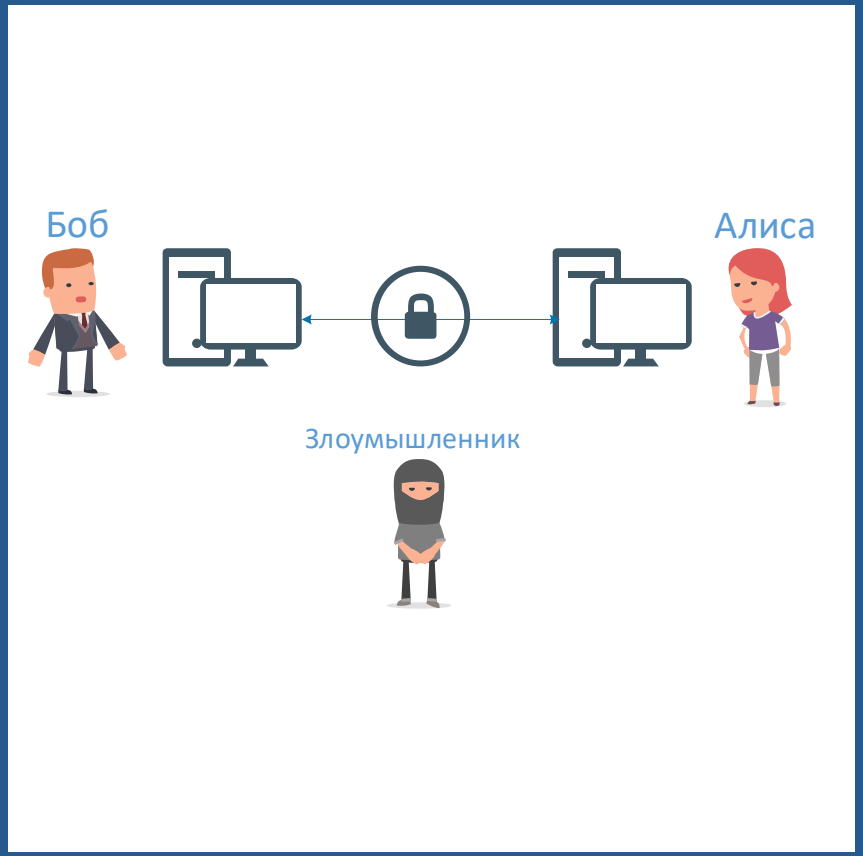
Совместный проект ОАО «ИнфоТеКС» и МГУ имени М.В. Ломоносова

- Выработка ключей и загрузка в СКЗИ происходит автоматически – без участия администратора
- Криптографические ключи с доказательством секретности
- Обеспечивается стойкость к криптографическим атакам при помощи квантового компьютера
- На стадии сертификации в ФСБ России
- Готовность к поставкам

Криптографическая защита информации



Криптографическая защита информации



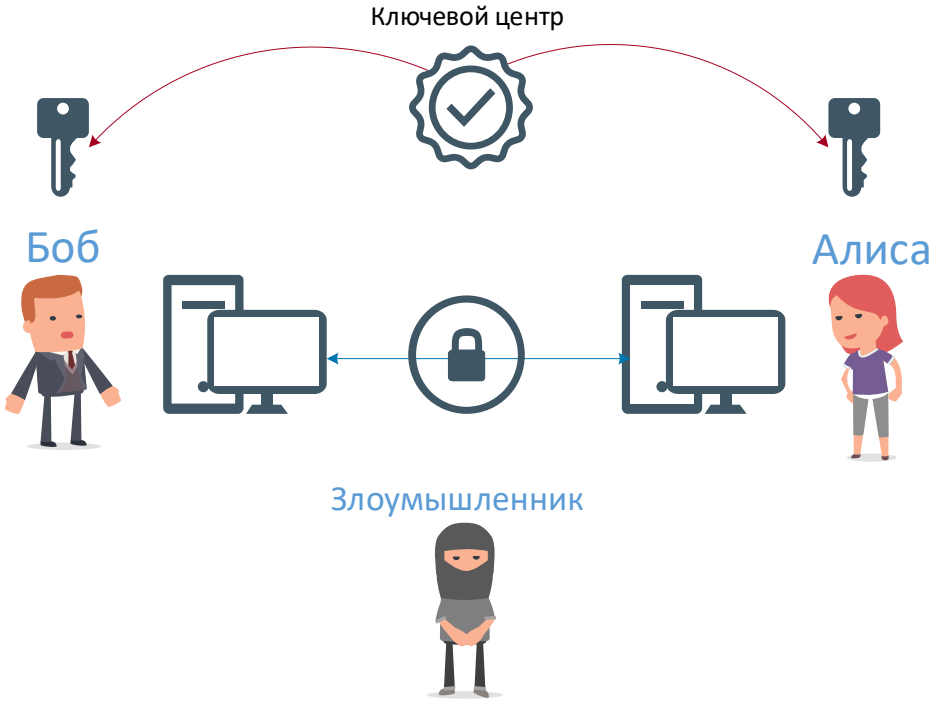
Базовый принцип проектирования СКЗИ:

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

Остается главный вопрос:

Откуда взять ключ?

Криптографическая защита информации



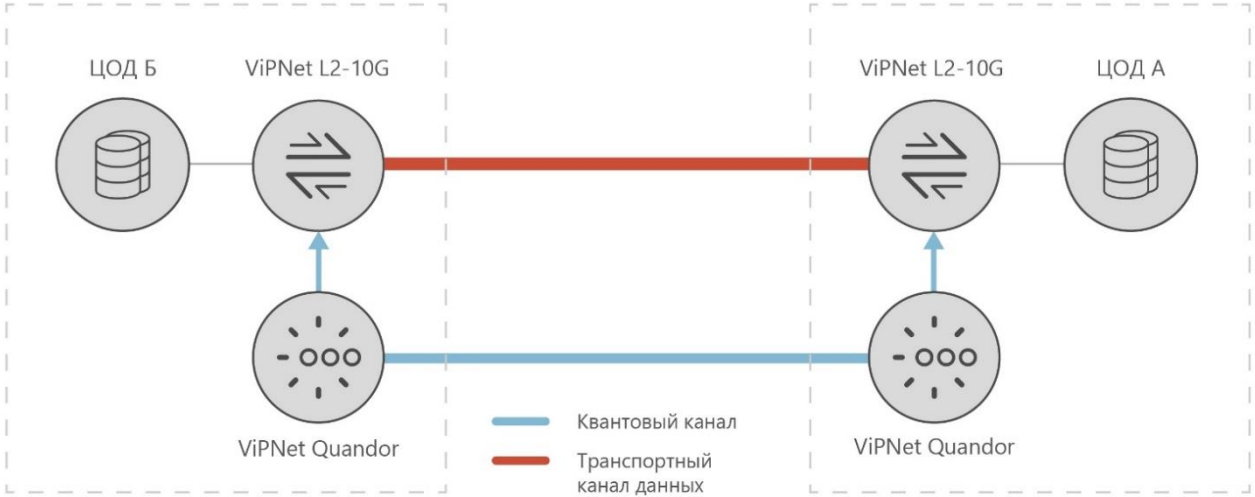
Существует два подхода:

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

или

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

Совместный проект ОАО «ИнфоТеКС»
и МГУ имени М.В. Ломоносова



Базовый сценарий использования – автоматическая доверенная доставка криптографических ключей для канальных шифраторов ViPNet L2-10G

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

Ключевые особенности ViPNet Quandor

- Длина квантового канала 100 км (130 км – экспериментальный предел при идеальных условиях)
- Устанавливается в стандартную стойку
- Автоматическая смена ключей 1 раз в минуту
- ФДСЧ на квантовых эффектах обеспечивает истинную случайность вырабатываемых ключей
- СКЗИ класса КС3 (все технические решения принимались с расчетом последующей сертификации на класс КВ, в плане на 2021 год)
- Гибридная ключевая система на квантовых и предраспределенных ключах. Физический вывод из строя квантового канала и оборудования не приведет к остановке шифрования

В процессе исследования 8 центром ФСБ России

infotecs

Стенд для внутренней эксплуатации ViPNet Quandor в ИнфоТеКС

Комплект оборудования для пилотной эксплуатации ViPNet Quandor на сетях заказчика

- Мобильный комплект для быстрого разворачивания на сетях заказчика
- Защита во время транспортировки
- Минимальные затраты времени на ввод в эксплуатацию
- Демонстрация рабочего решения, готового к поставкам

Александр Поздняков
Менеджер продуктов

Aleksandr.Pozdnyakov@infotecs.ru