infotecs

Не IPSec'ом единым, или о целесообразности наличия нескольких рекомендованных ТК26 VPN-протоколов в России

Алексей Уривский
ОАО «ИнфоТеКС»

Альтернативные стандарты

- Выбор лучше его отсутствия
- Здоровая конкуренция полезна
- Разные создатели – разные идеи
- У каждого свой набор достоинств
- Наши не хуже!

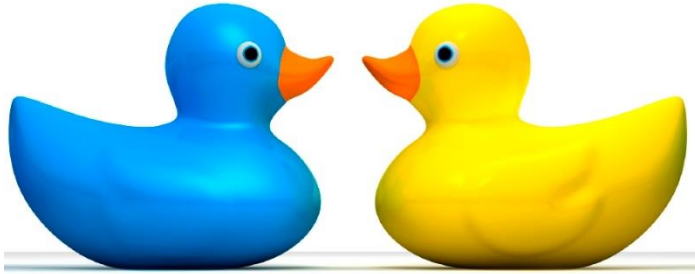
VPN-протокол

- VPN-протокол – это совокупность криптографической и сетевой компоненты, каждая из которых должна
  - быть надежна и безопасна;
  - правильно интегрироваться с другой – нельзя отдельно рассматривать криптографию, не учитывая особенности сетевой части;
  - быть полезна на практике – эксплуатационные аспекты для пользователей чаще важнее теоретических.

IPlir

- IPlir – протокол защиты данных при их передаче в среде IPv4 и IPv6
  - без установления предварительного криптографического соединения;
  - предварительно распределенные секретные ключи;
  - синхронизация межу узлами в каждом пакете.
- Первые версии документов, описывающих IPlir, доступны на форуме сайта ТК 26 http://www.tc26.ru/forum/

IPlir против IPsec ?



- **IPsec**
  - универсален, но сложен в описании;
  - открытие соединения и работа за NAT-устройствами может быть проблемным;
  - Не все реализации совместимы
- **IPlir**
  - более конкретен;
  - не накладывает ограничений на топологию сетей, их адресную структуру и место подключения узлов к сети

Использование «чужих» стандартов

- **Качество стандартов**
  - кто их создает и для какой цели? – RFC может содержать практически любой текст, соответствующий правилам оформления;
  - синтезные принципы и решаемые задачи неизвестны и протокол может быть преднамеренно ослаблен – какой VPN-протокол проанализирован до конца?

- **Зависимость от стандартов**
  - добавление нашей специфики (ГОСТов) ставит нас в подчиненное положение – изменение исходного стандарта требует пересмотра наших документов;
  - учет наших требований в исходном стандарте мало кому нужно – PKCS#11 ver 2.3

infotecs

Вопросы?

Алексей Уривский
urivskiy@infotecs.ru