Криптографические протоколы и возможность их использования для построения скрытых логических каналов

Матвеев Сергей Васильевич,
Пензенский филиал ФГУП «НТЦ «Атлас»

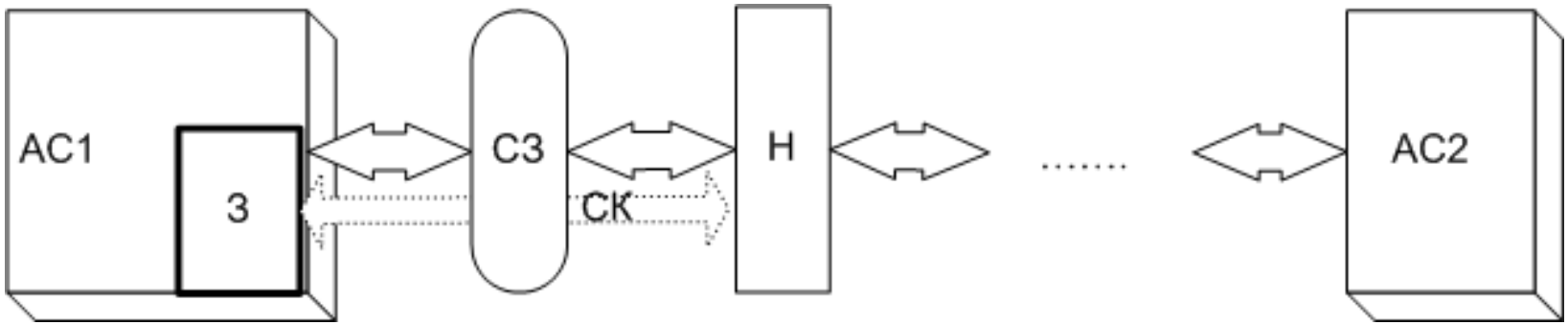
Определение скрытого канала

- Скрытый канал утечки информации - коммуникационный канал, непредусмотренный разработчиком, использующийся для нарушения политики безопасности системы

Нормативные документы

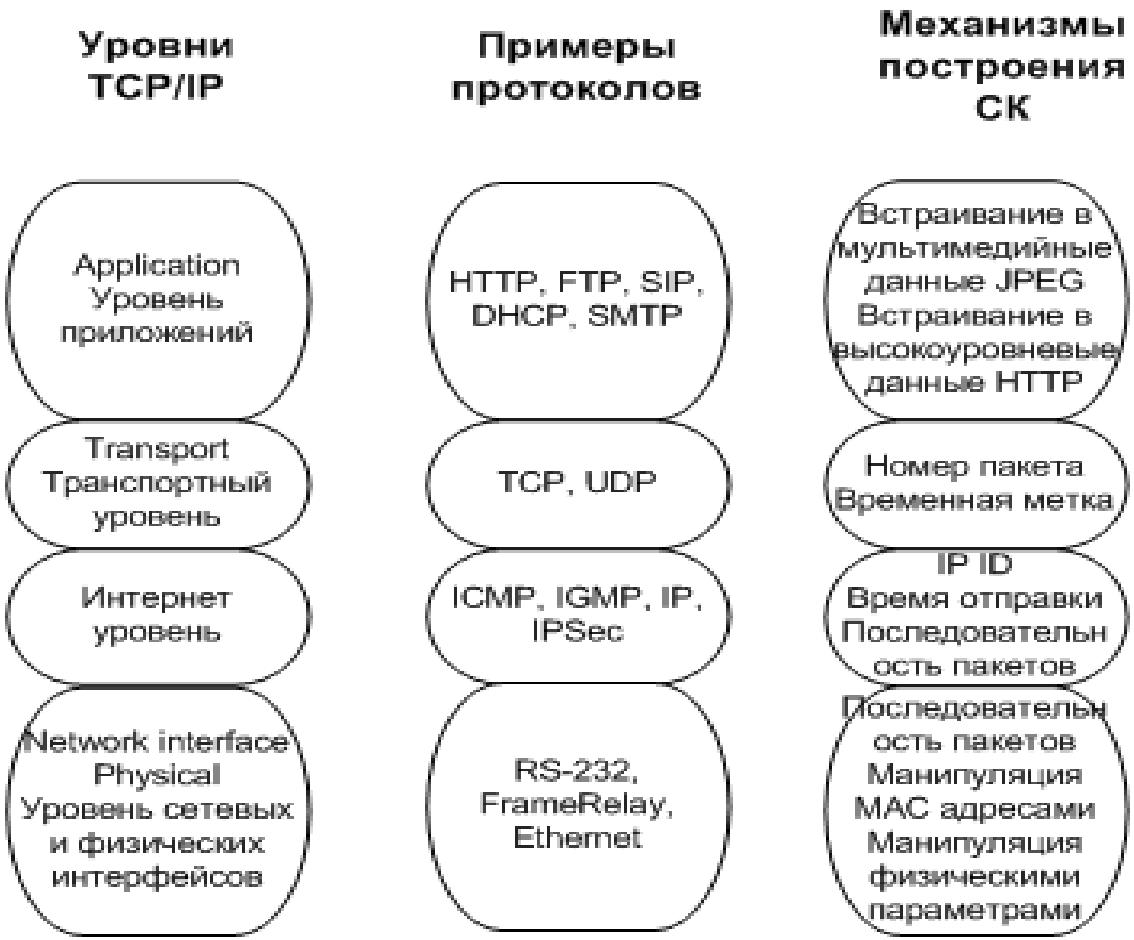
- National Computer Security Center. A guide to understanding covert channel analysis of trusted systems, NCSC-TG-30, ver. 1, Nov. 1993
- ГОСТ Р 53113.1-2008. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения
- ГОСТ Р 53113.2-2009. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.

Общая схема функционирования скрытого канала в автоматизированной системе



- АС1, АС2 – два сегмента автоматизированной системы
- СЗ – комплекс средств защиты,
- Н – внешний нарушитель, осуществляющий несанкционированный доступ к АС либо оказывающий негативное влияние на неё,
- З – внутренний нарушитель системы, формирующий скрытый канал для связи с внешним нарушителем Н

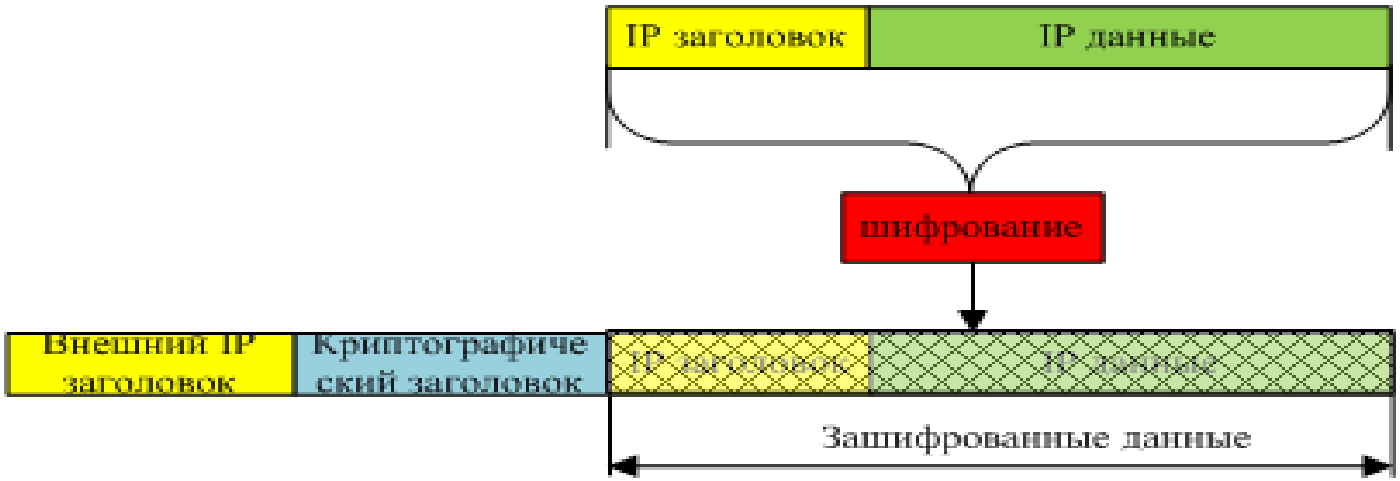
Скрытые каналы в сетевой модели



Способы построения СК

- внедрение данных в поля передаваемых или принимаемых пакетов
- внедрение данных в информационные объекты, приводящее к внешне невидимым изменениям данных объектов
- изменение длин передаваемых пакетов
- изменение длин межпакетных интервалов
- манипуляция адресами отправителя или получателя
- изменение порядка следования сегментов с данными (пакетов, запросов, полей)
- передача собственных информационных пакетов

Туннелирование трафика как способ защиты



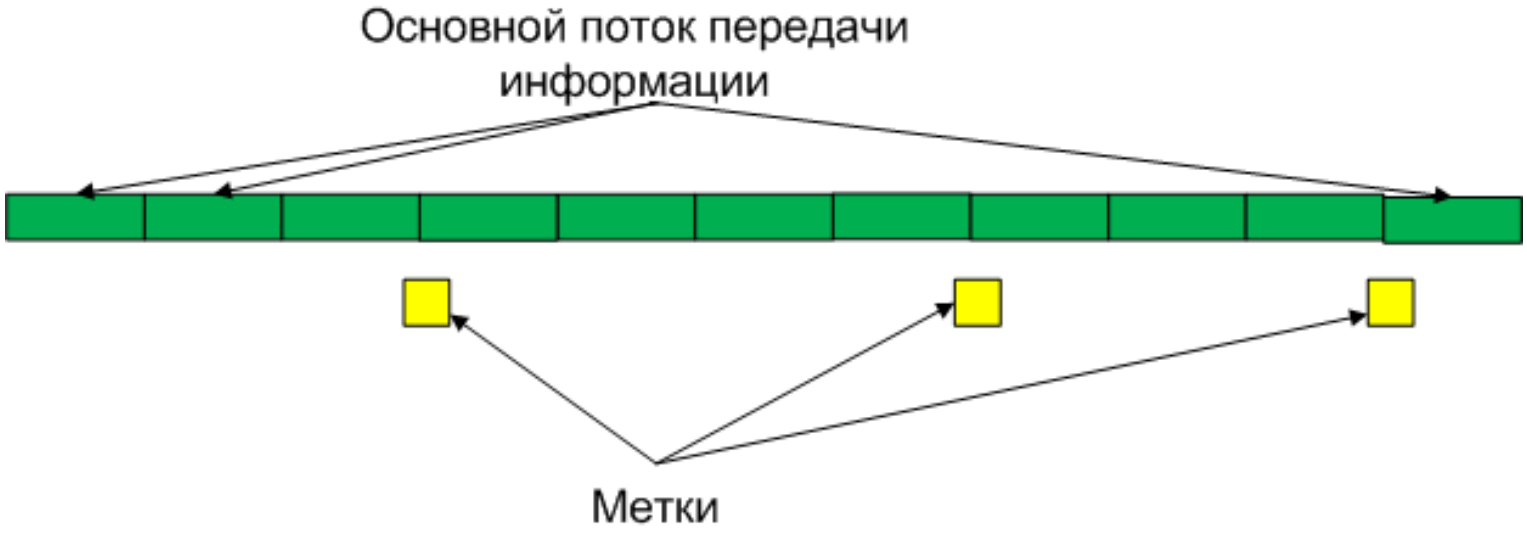
Способы построения СК

- внедрение данных в поля передаваемых или принимаемых пакетов
- внедрение данных в информационные объекты, приводящее к внешне невидимым изменениям данных объектов
- изменение длин передаваемых пакетов
- изменение длин межпакетных интервалов
- манипуляция адресами отправителя или получателя
- изменение порядка следования сегментов с данными (пакетов, запросов, полей)
- передача собственных информационных пакетов
- манипуляция новым адресом получателя

Использование меток для построения скрытых каналов

- Н. А. Грушо, «Скрытые каналы, порожденные метками»// Системы и средства информ., 23:1, «Проблемы информационной безопасности и надежности систем информатики». – 2013.
- А. А. Грушо, Н. А. Грушо, Е. Е. Тимонина, Оценки скорости передачи информации и пропускной способности в скрытых каналах с метками// Информ. и ее примен. 2015, том 9, выпуск 4

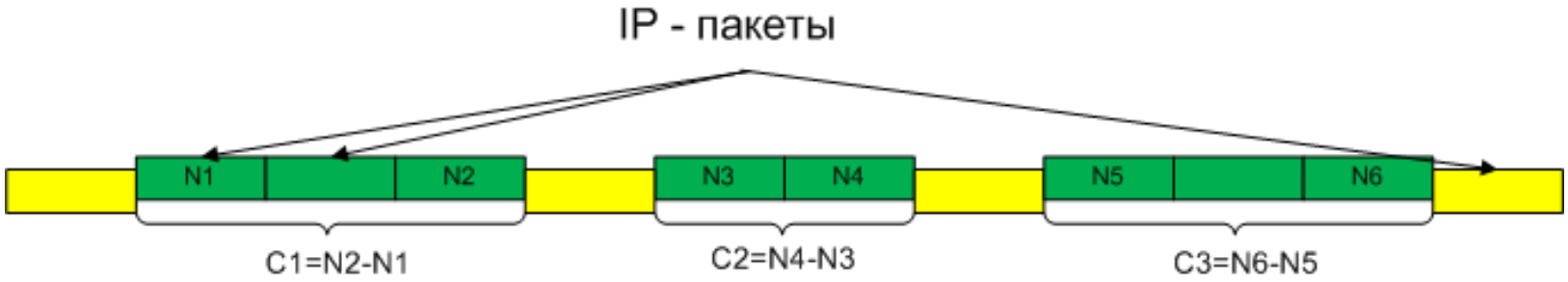
Скрытый канал на основе меток



Варианты внедрения меток

- Адрес получателя
- Номер VPN туннеля
- Значение поля ToS

Частный случай IP сети



N1,..,N6 – значения счетчика в криптографическом заголовке

C1,C2,C3 – кодовые слова в СК

Примеры криптоалгоритмов

- Режим гаммирования ГОСТ Р 34.13-2015
- PD режим для шифрования с аутентификацией (Проект)

Пропускная способность СК

$$\max_n C(n) = \frac{2 \cdot W\left(\frac{2t_{пост} - 1}{e}\right)\left(\log_2\left(2t_{пост} - 1\right) - \log_2\left(W\left(\frac{2t_{пост} - 1}{e}\right)\right)\right)}{(2t_{пост} - 1) \cdot \left(W\left(\frac{2t_{пост} - 1}{e}\right) + 1\right)}$$

W(x) – функция Ламберта

$t_{пост}$ - постоянная составляющая информационного сигнала СК

В нашем случае $t_{пост}$ – длина пакета

Пропускная способность СК

Длина пакета, байт	**512**	**1024**	**1500**
Cmax	0.0011	0.00065	0.00046

Спасибо за внимание!

Вопросы?