Протокол IPSec

(RFC 2401)

Семейство протоколов IPSec

Протокол Authentication Header (AH)

Аутентификация
Контроль целостности

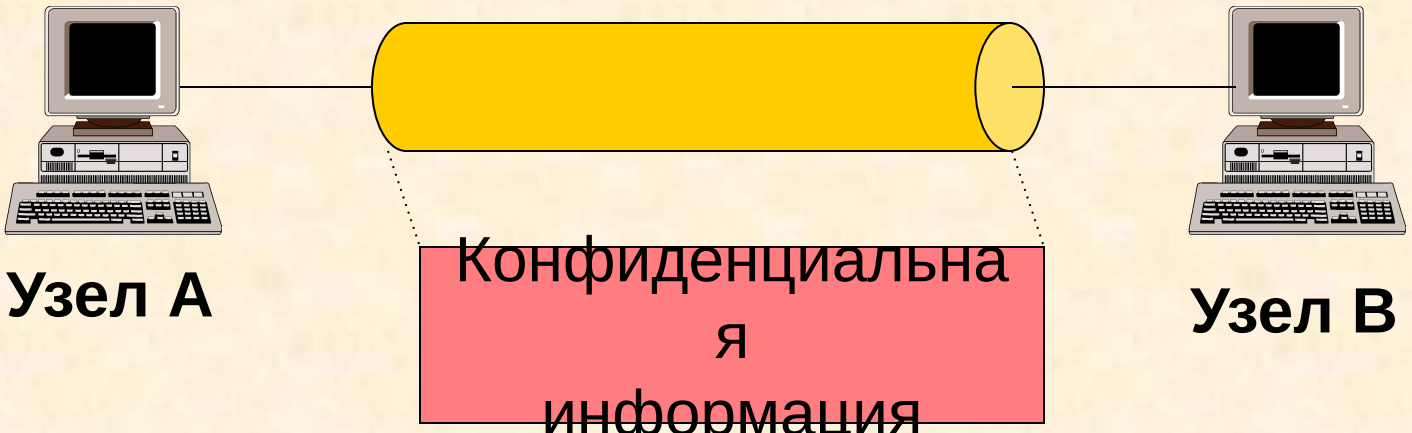
Протокол Encapsulated Security Payload (ESP)

Аутентификация
Контроль целостности
Шифрование

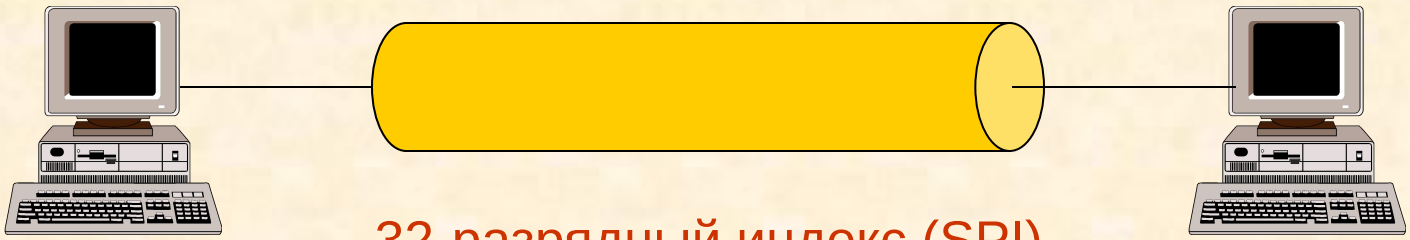
Протокол Internet Key Exchange (IKE)

Согласование алгоритмов шифрования
Обмен ключами

Защищённый канал IPSec



Безопасная ассоциация IPSec



32-разрядный индекс (SPI)

Узел А **Узел В**

IP- адрес узла назначения

SA **SA**

Идентификатор протокола защиты
(AH или ESP)

Безопасная ассоциация IPSec

Базы данных SA

Схемы применения IPSec

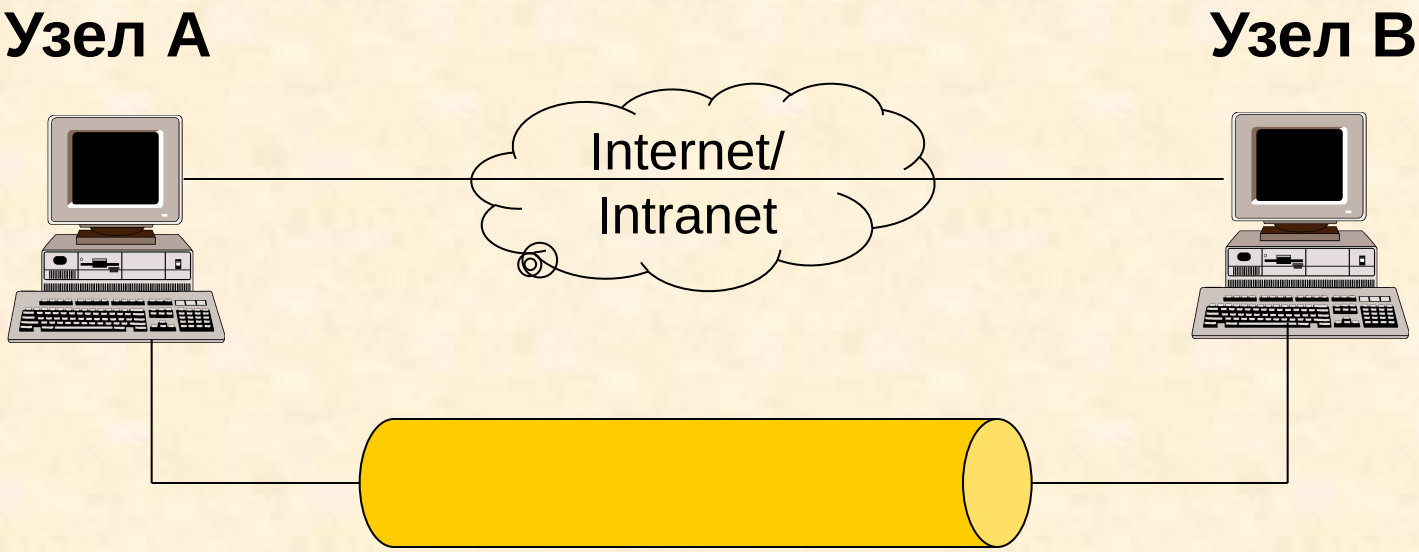


Схема узел-узел (точка-точка)

Схемы применения IPSec

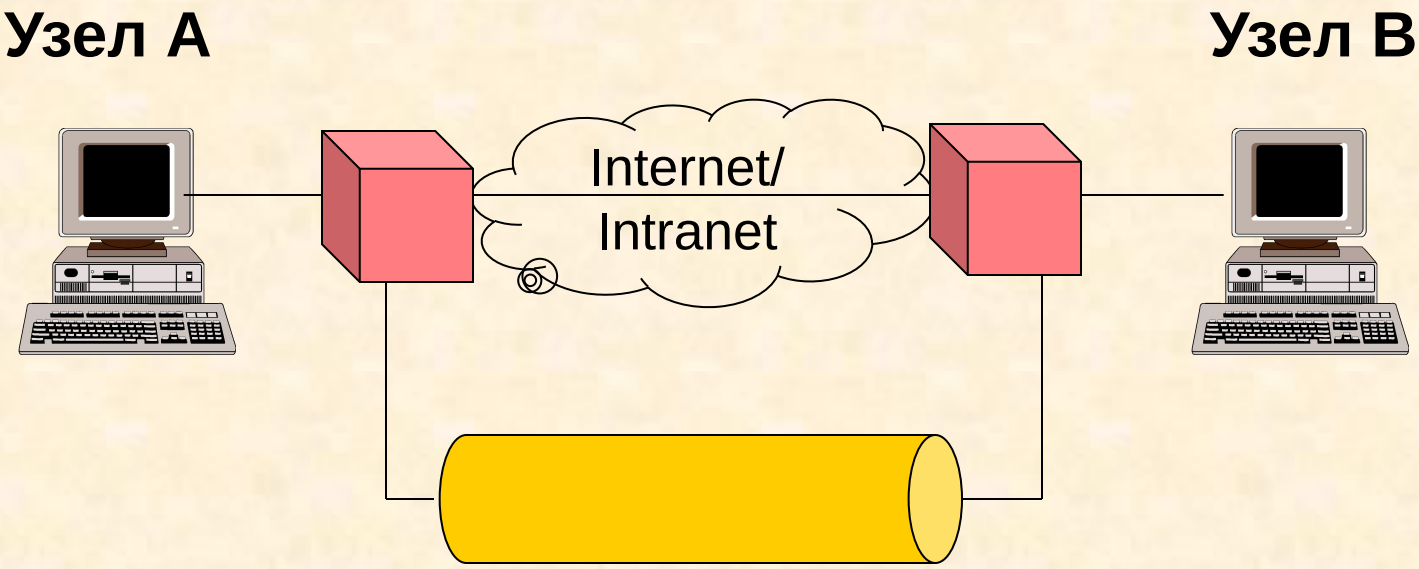
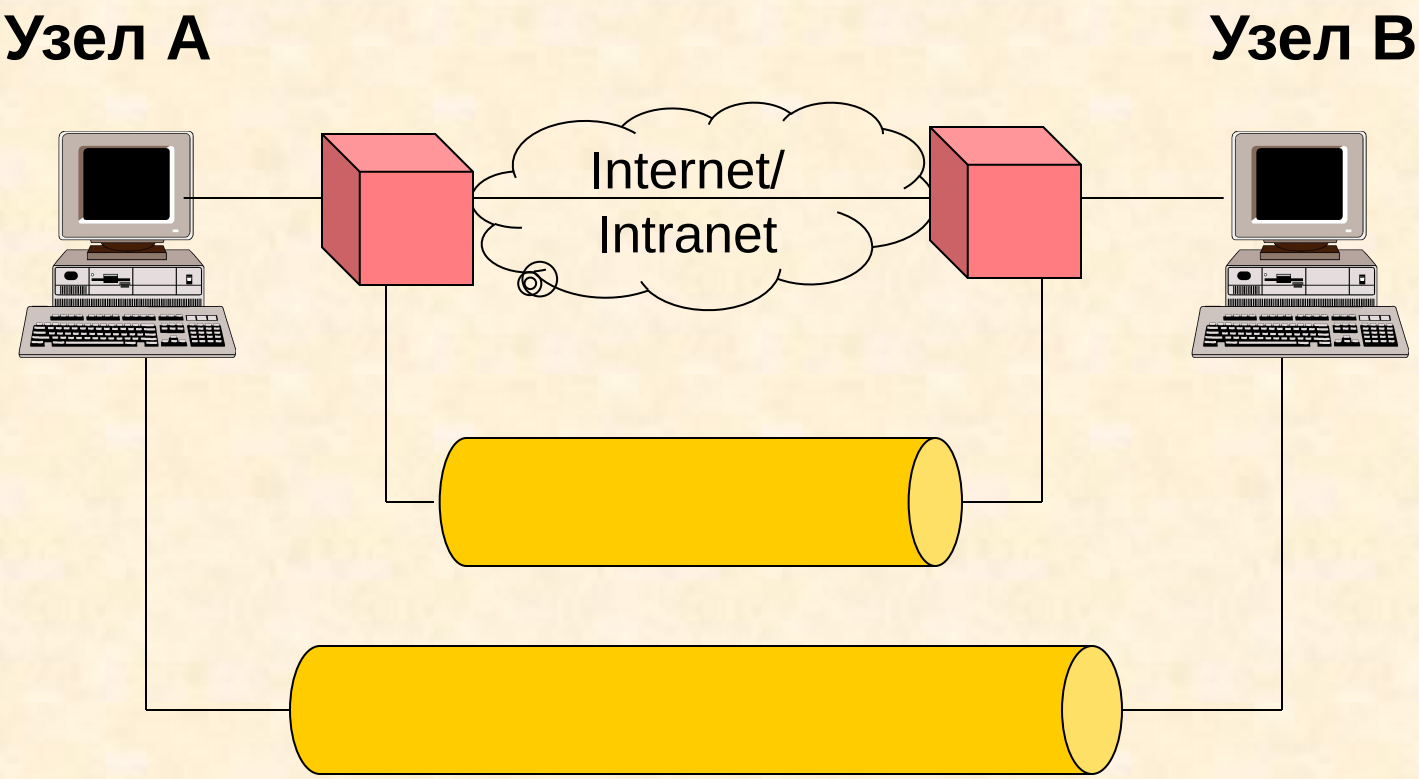


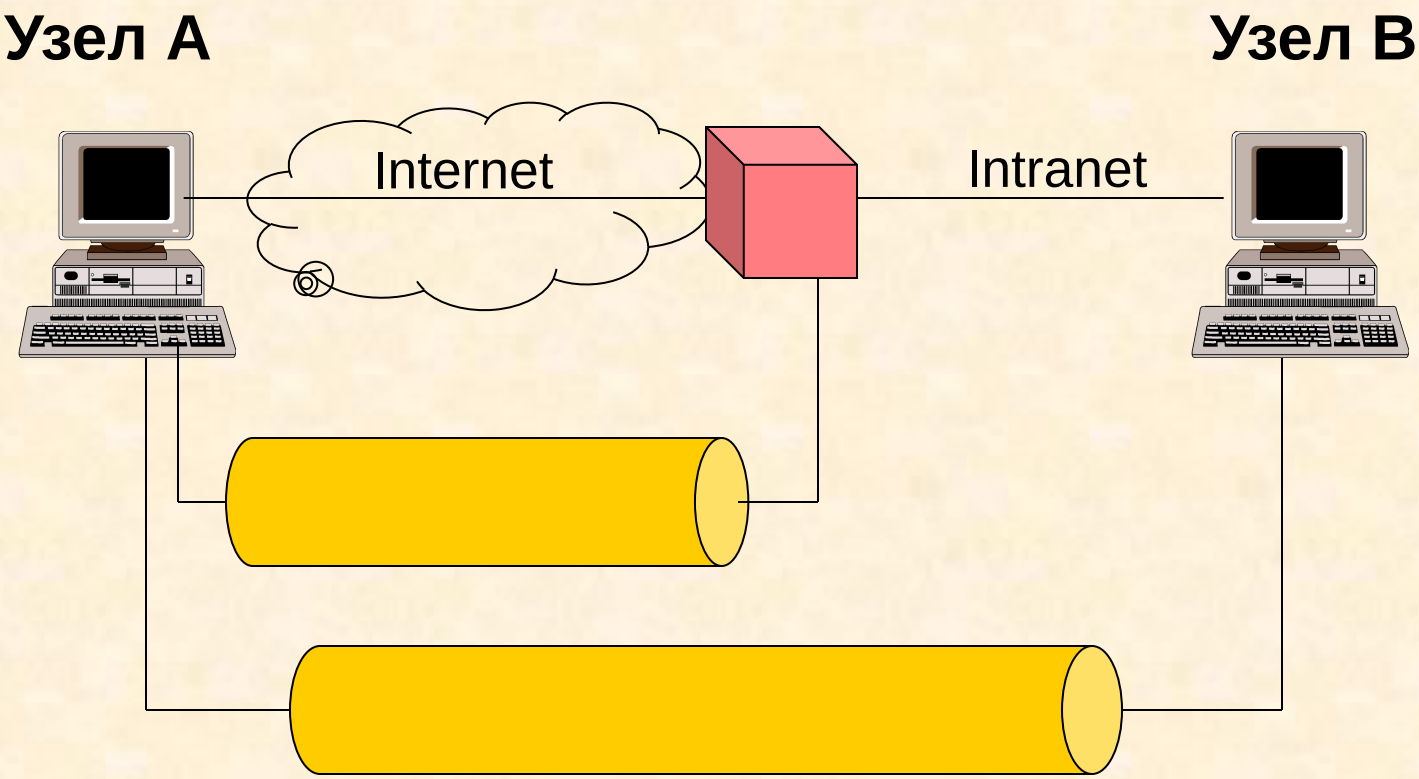
Схема шлюз-шлюз

Схемы применения IPSec



Смешанная схема (вариант 1)

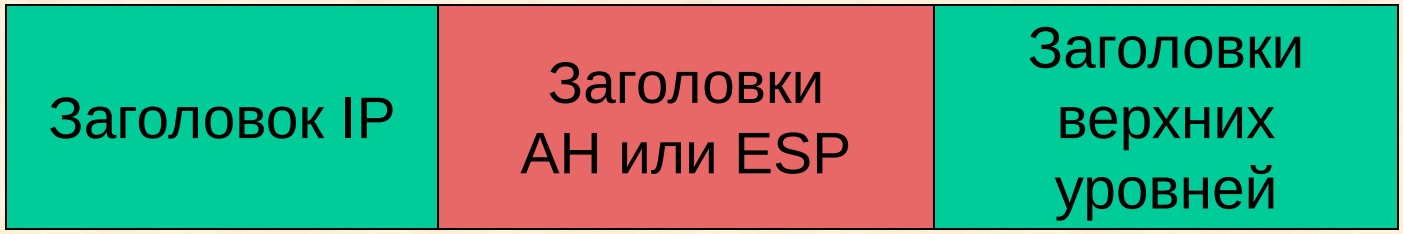
Схемы применения IPSec



Смешанная схема (вариант 2)

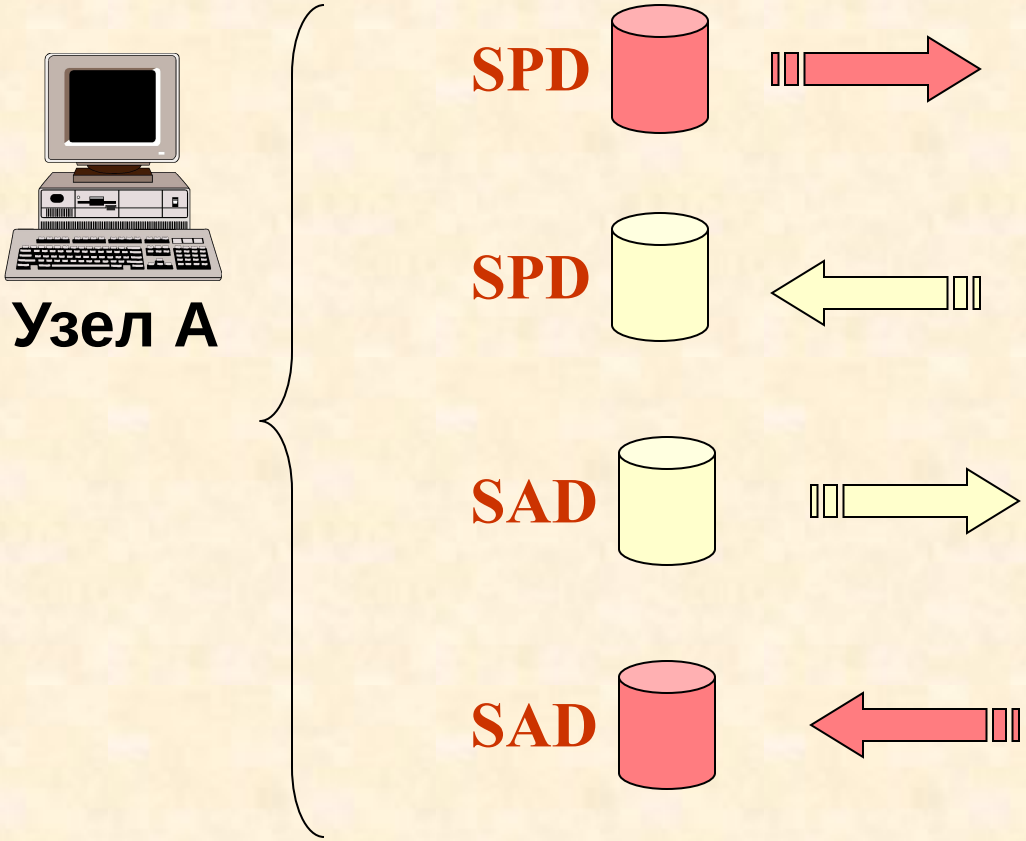
Режимы работы IPSec

Транспортный режим



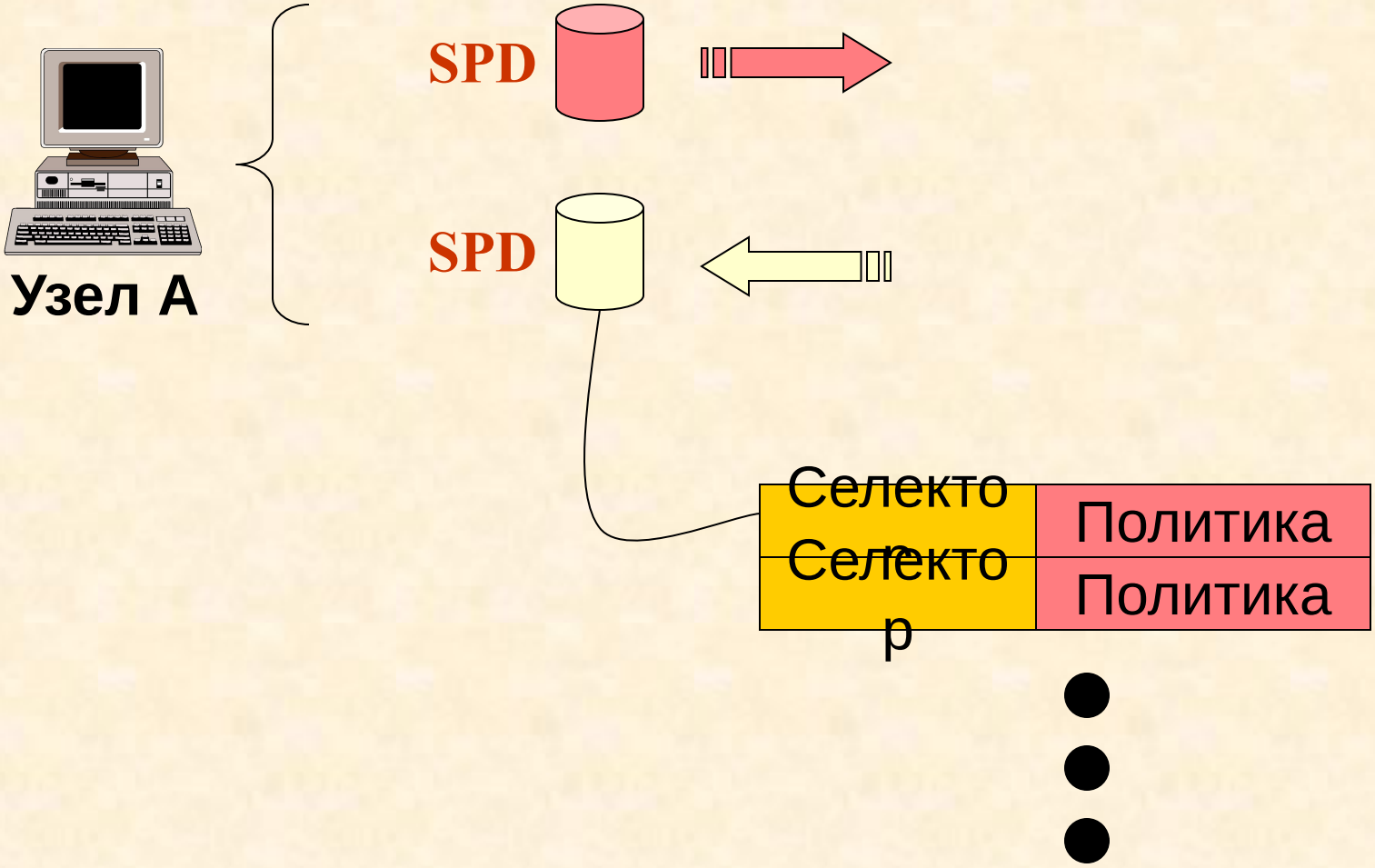
Туннельный режим

Базы данных IPSec

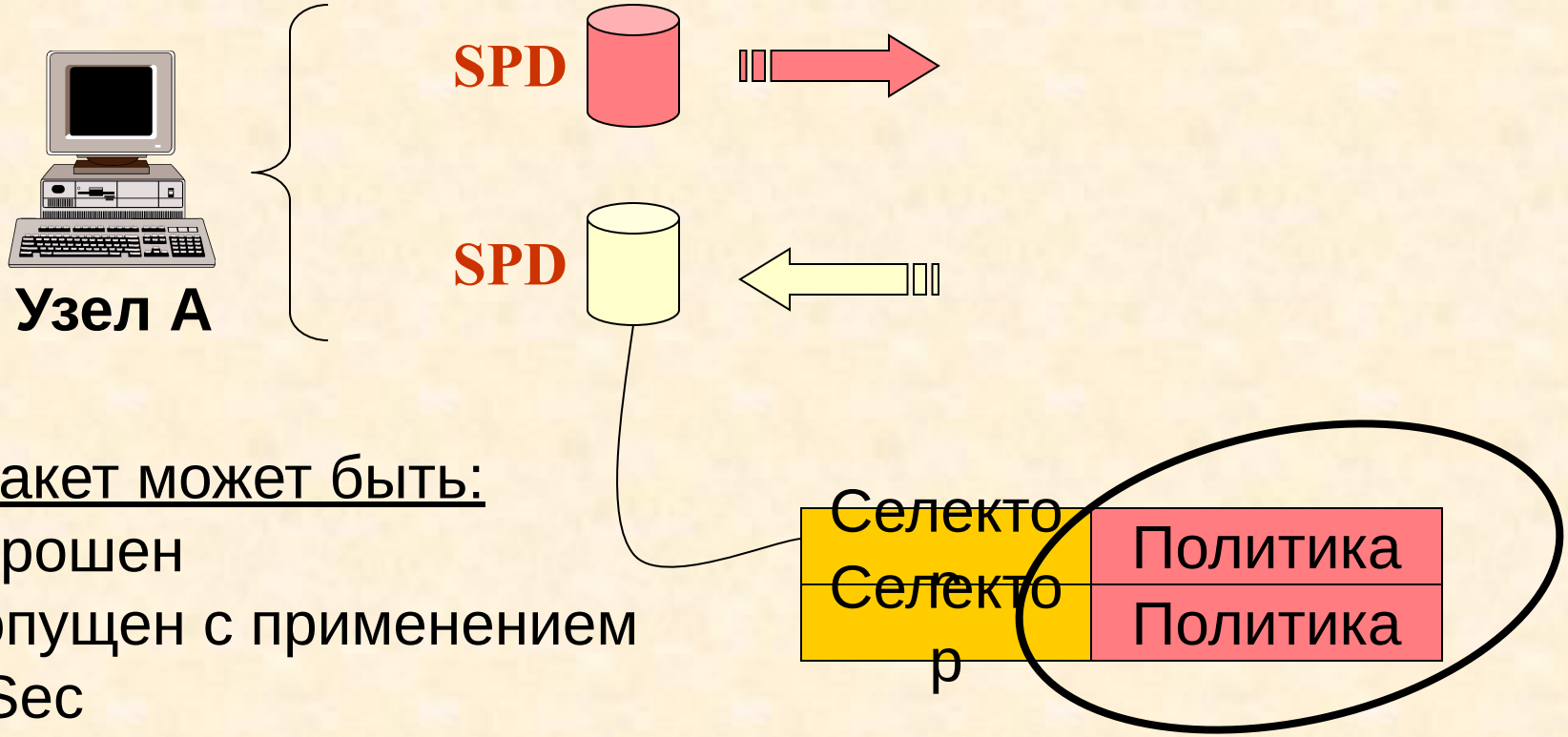


Базы данных SAD и SPD

База данных SPD



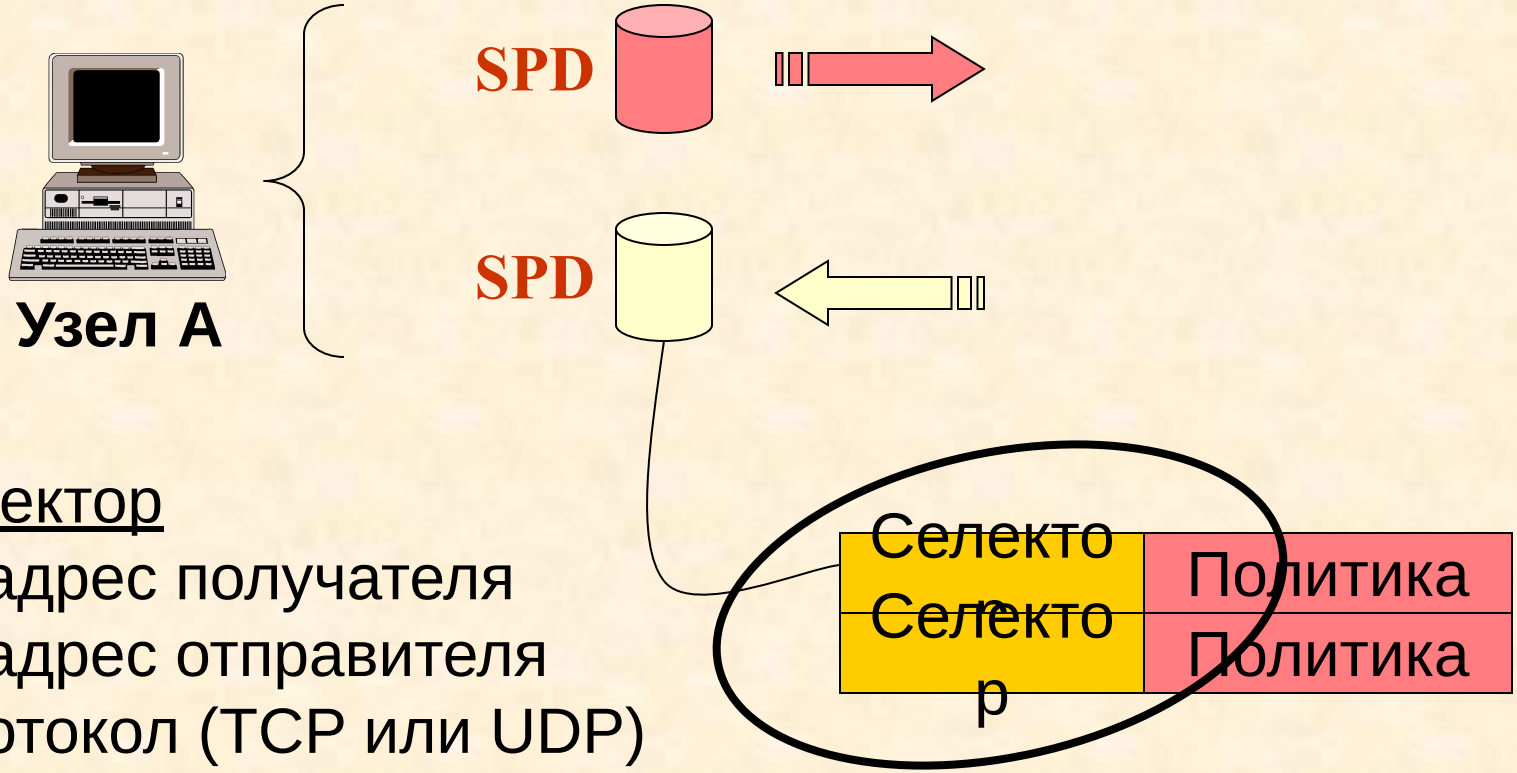
База данных SPD



IP-пакет может быть:

- отброшен
- пропущен с применением IPSec
- пропущен без применения IPSec

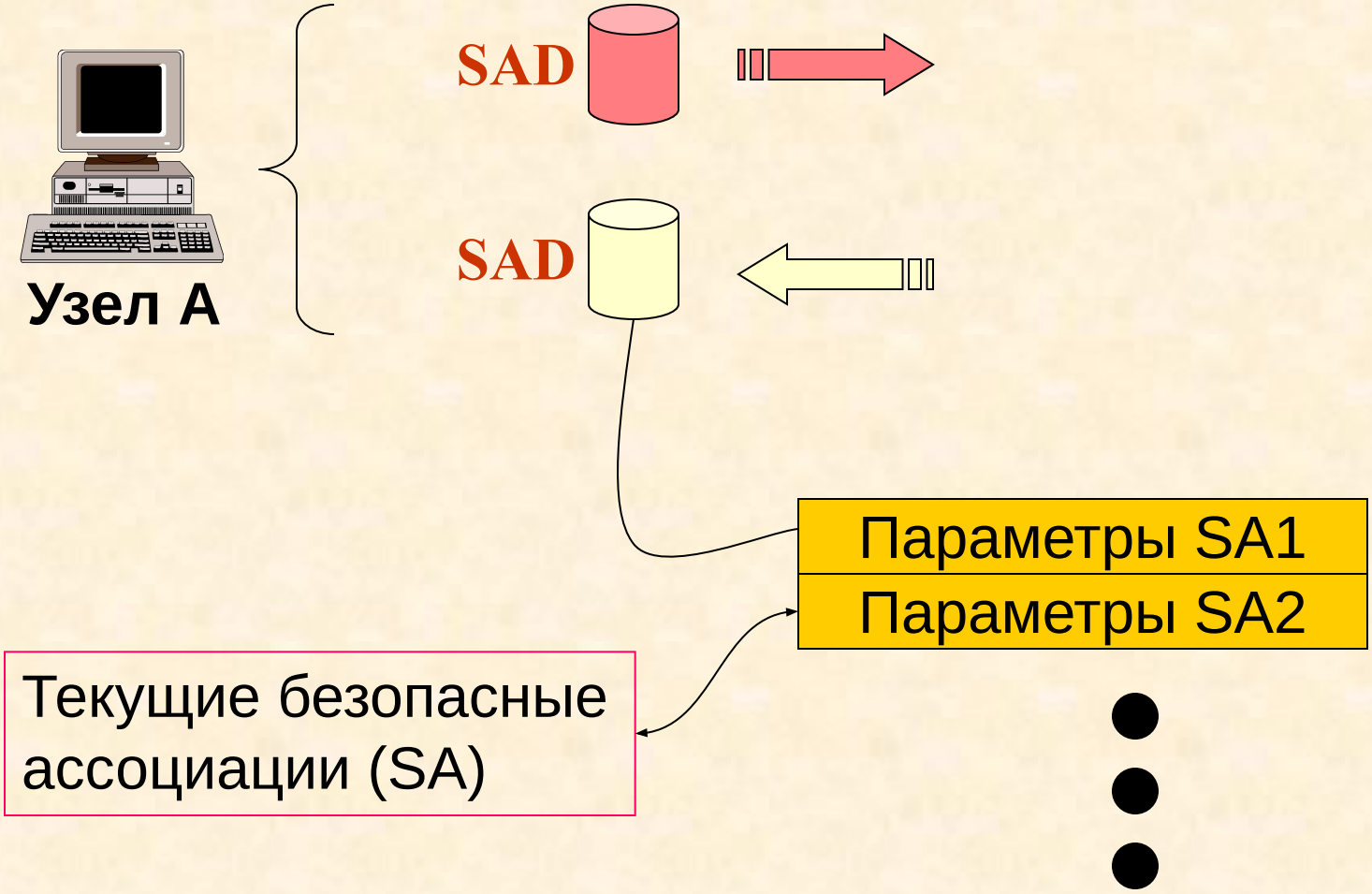
База данных SPD



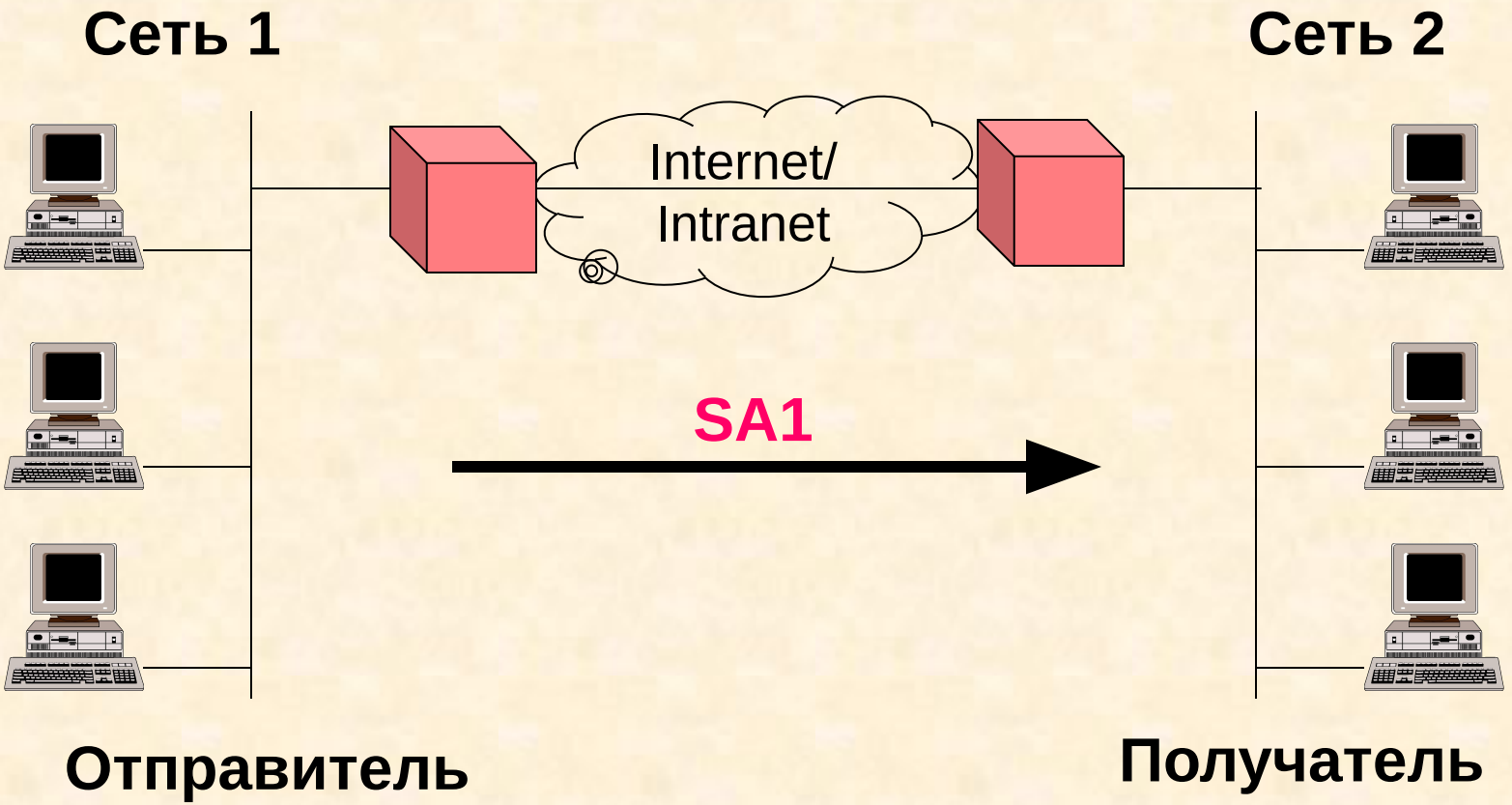
Селектор

- IP-адрес получателя
- IP-адрес отправителя
- Протокол (TCP или UDP)
- Имя FQDN или X.500
- Порт отправителя
- Порт получателя

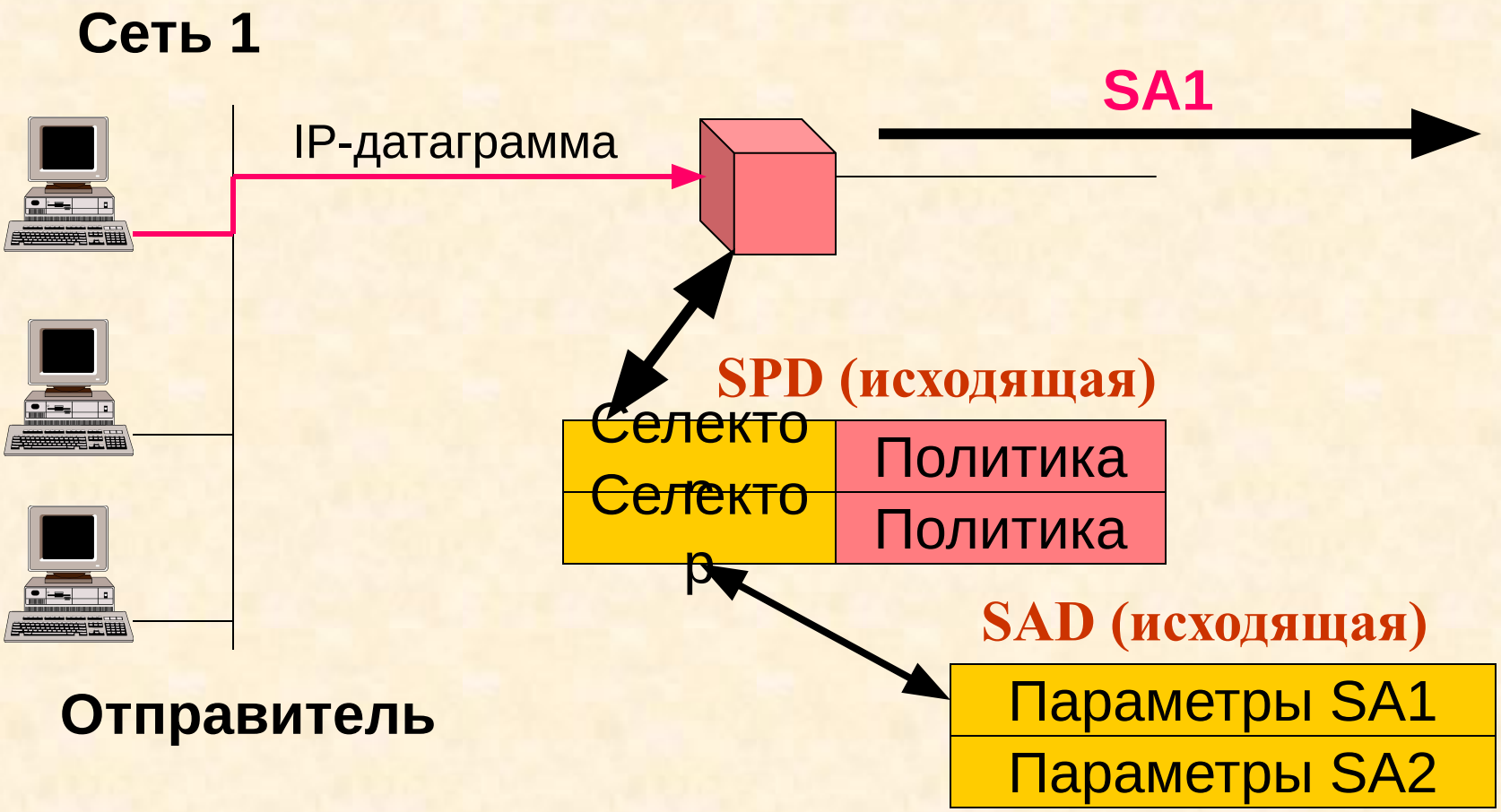
База данных SAD



Пример работы IPSec

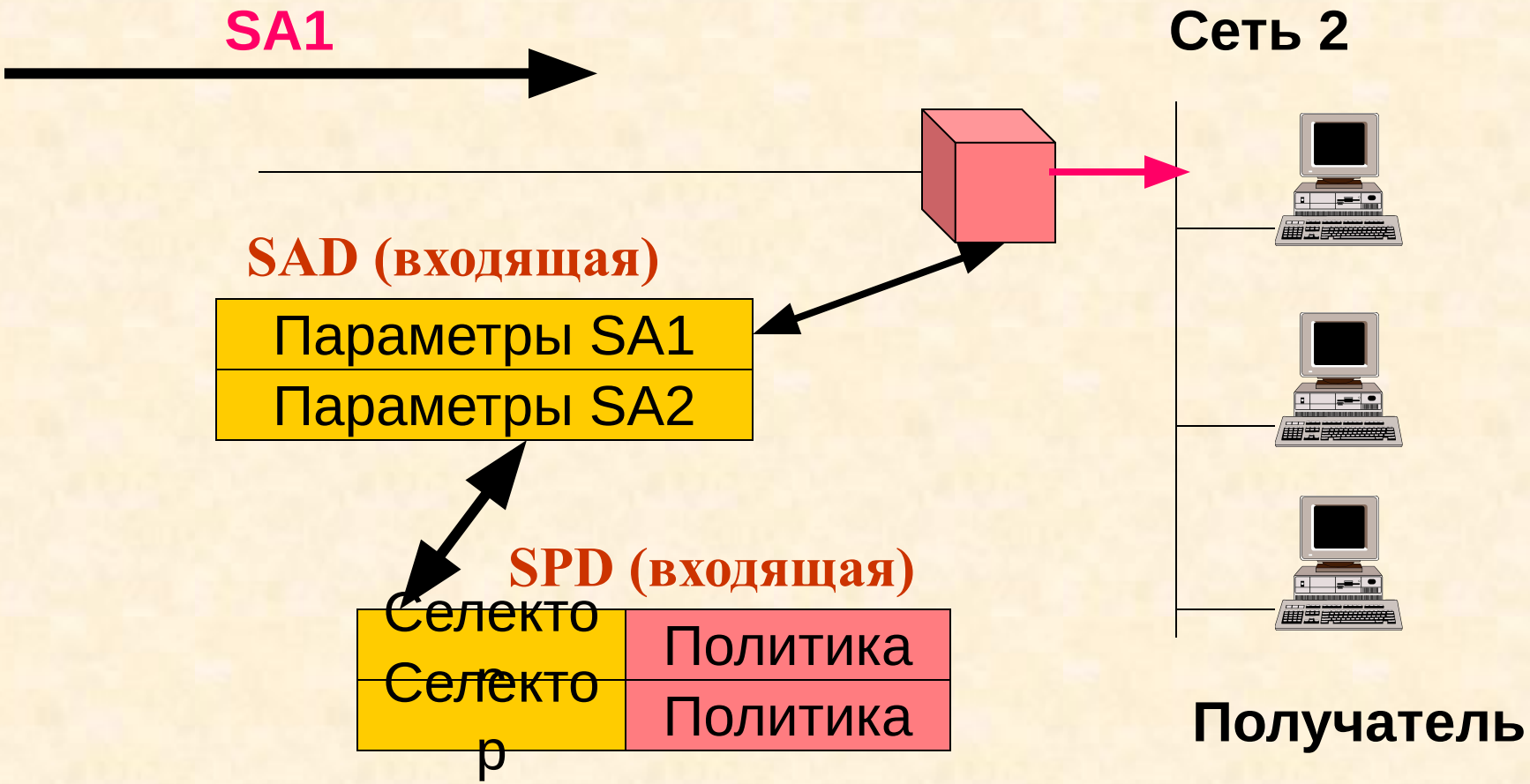


Пример работы IPSec



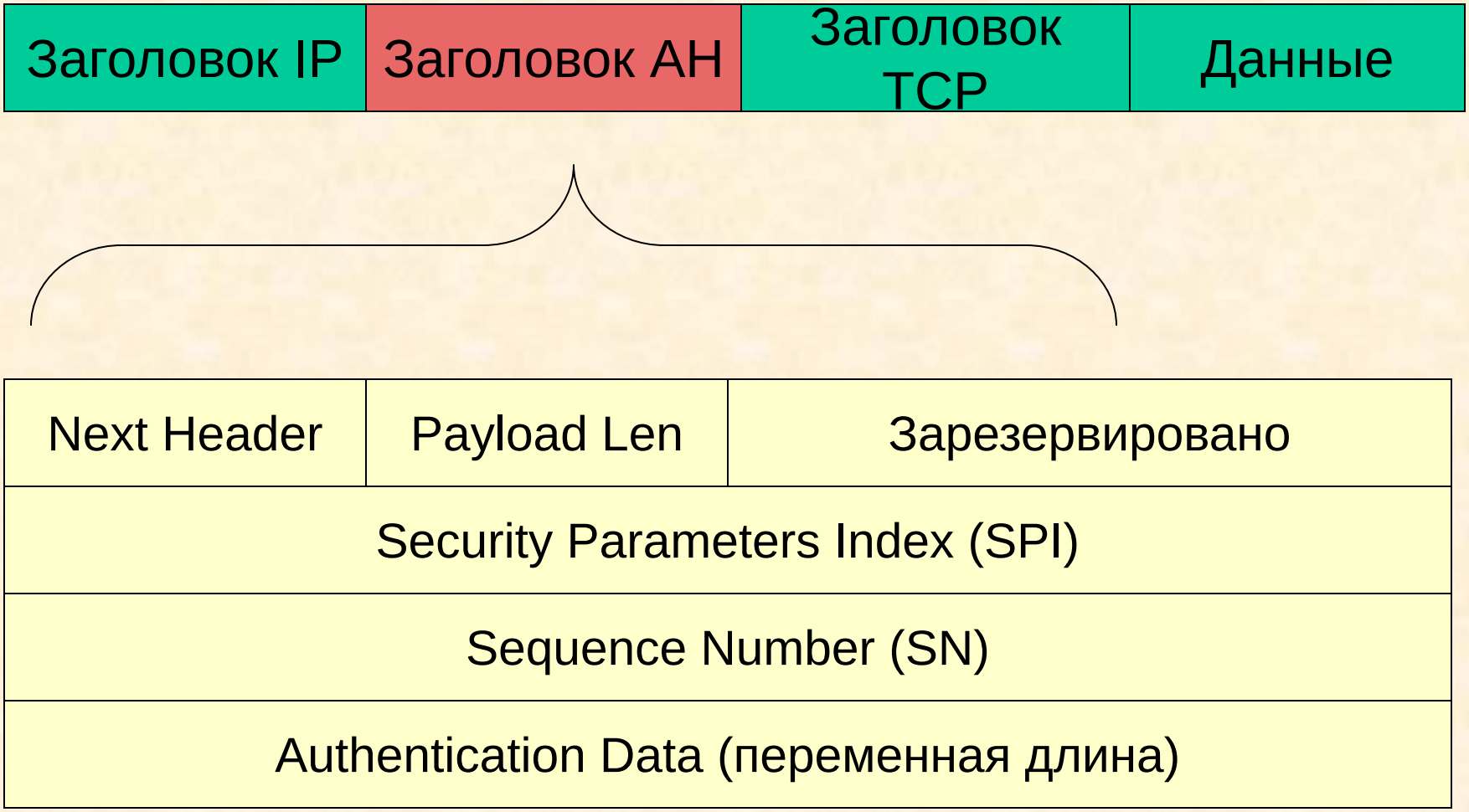
Отправка пакета

Пример работы IPSec

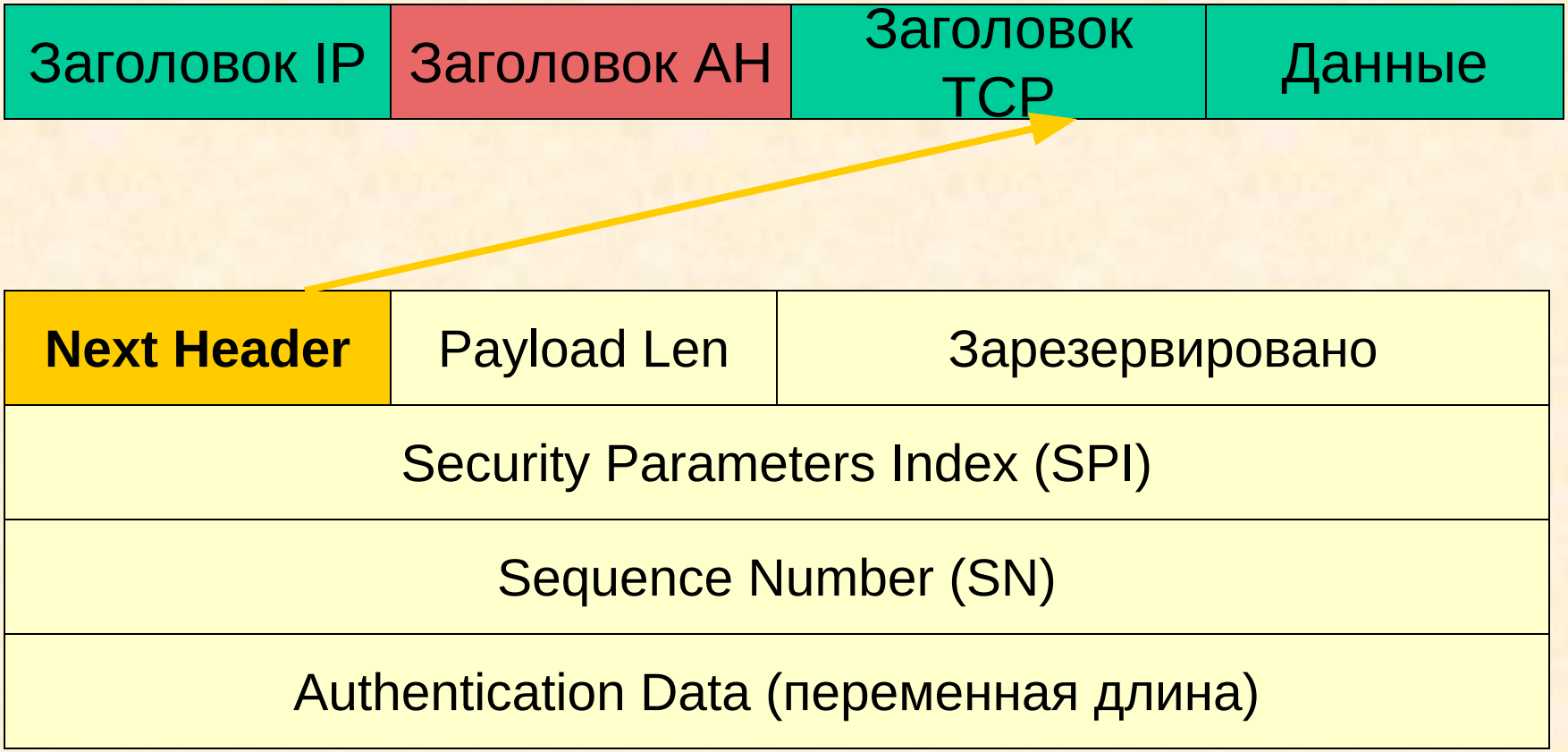


Получение пакета

Протокол AH

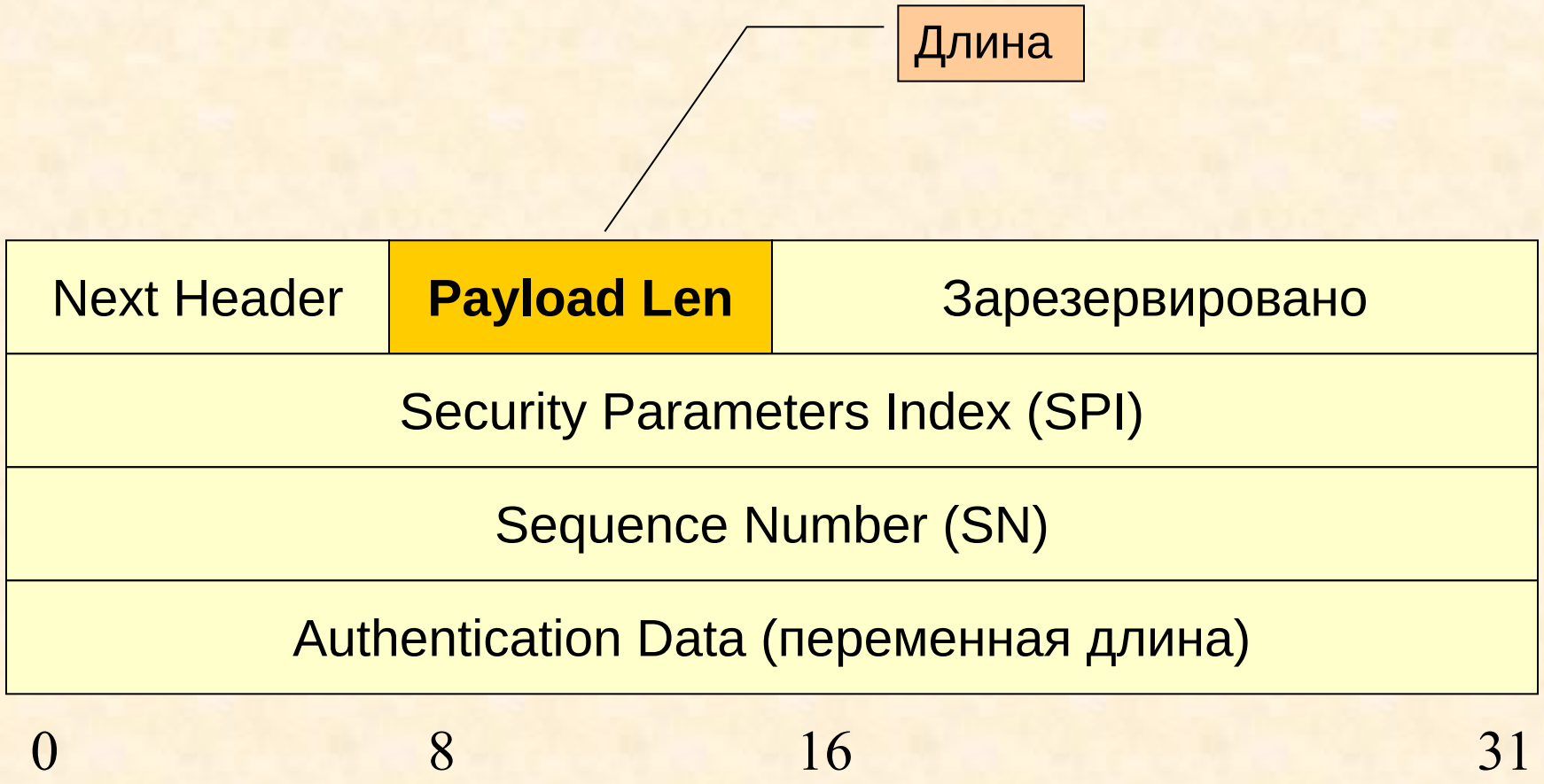

Заголовок IP
Заголовок AH
Заголовок TCP
Данные
Next Header
Payload Len
Зарезервировано
Security Parameters Index (SPI)
Sequence Number (SN)
Authentication Data (переменная длина)
0
8
16
31

Протокол AH



Поле Next Header

Протокол AH



Поле Payload Len

Протокол AH

Метка безопасной ассоциации

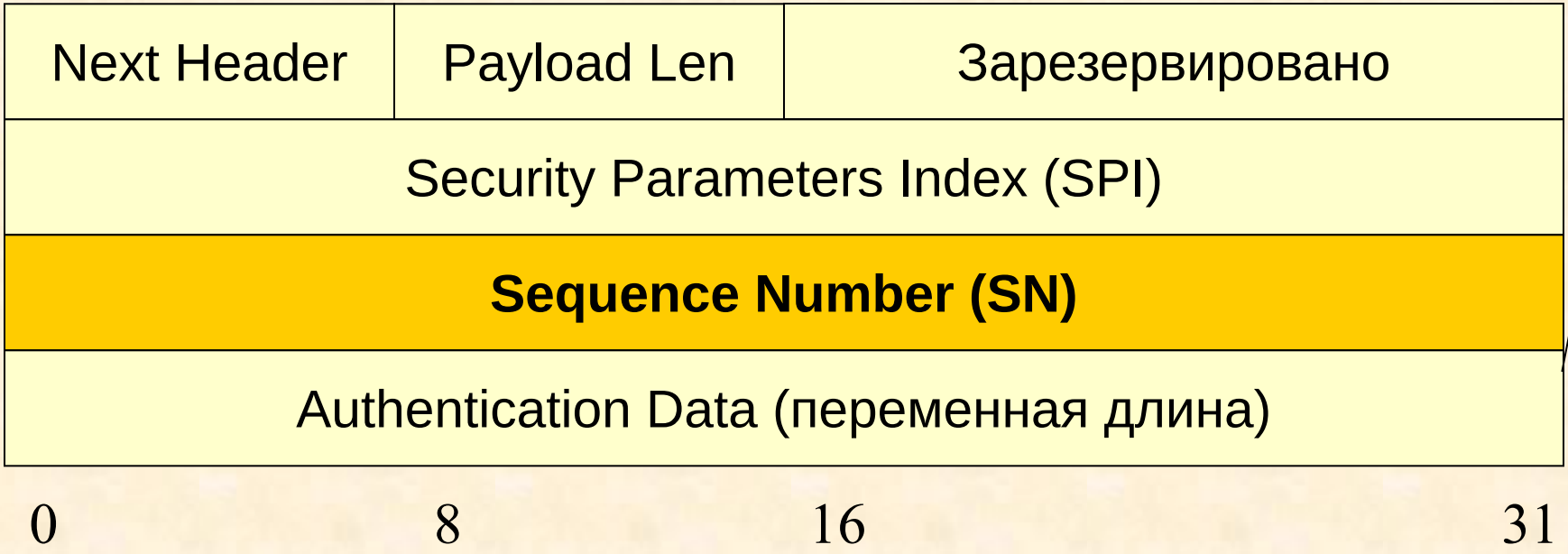
Next Header	Payload Len	Зарезервировано
Security Parameters Index (SPI)		
Sequence Number (SN)		
Authentication Data (переменная длина)		

0 8 16 31

Поле SPI

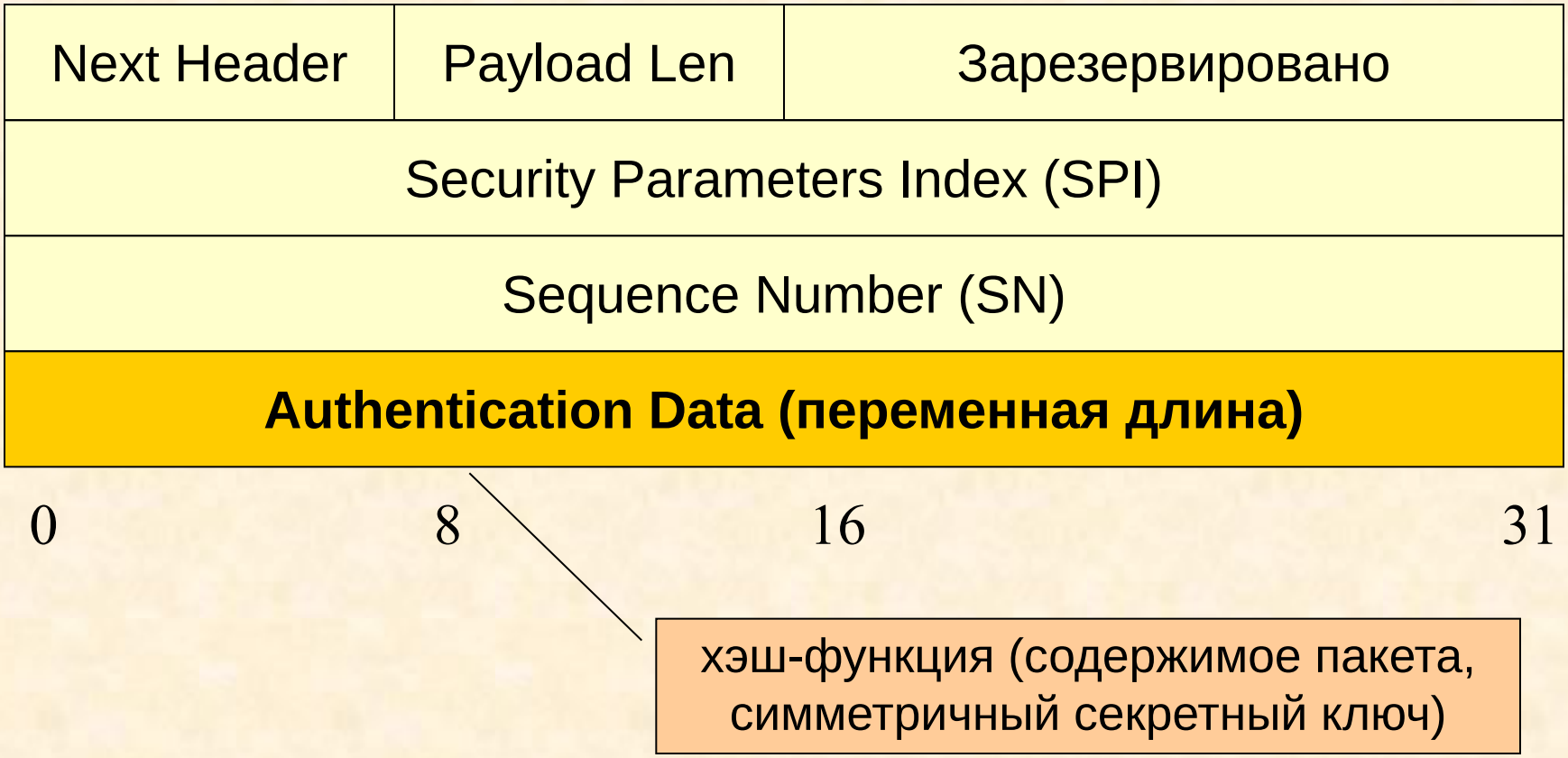
Протокол AH

Наращивается для каждого следующего пакета



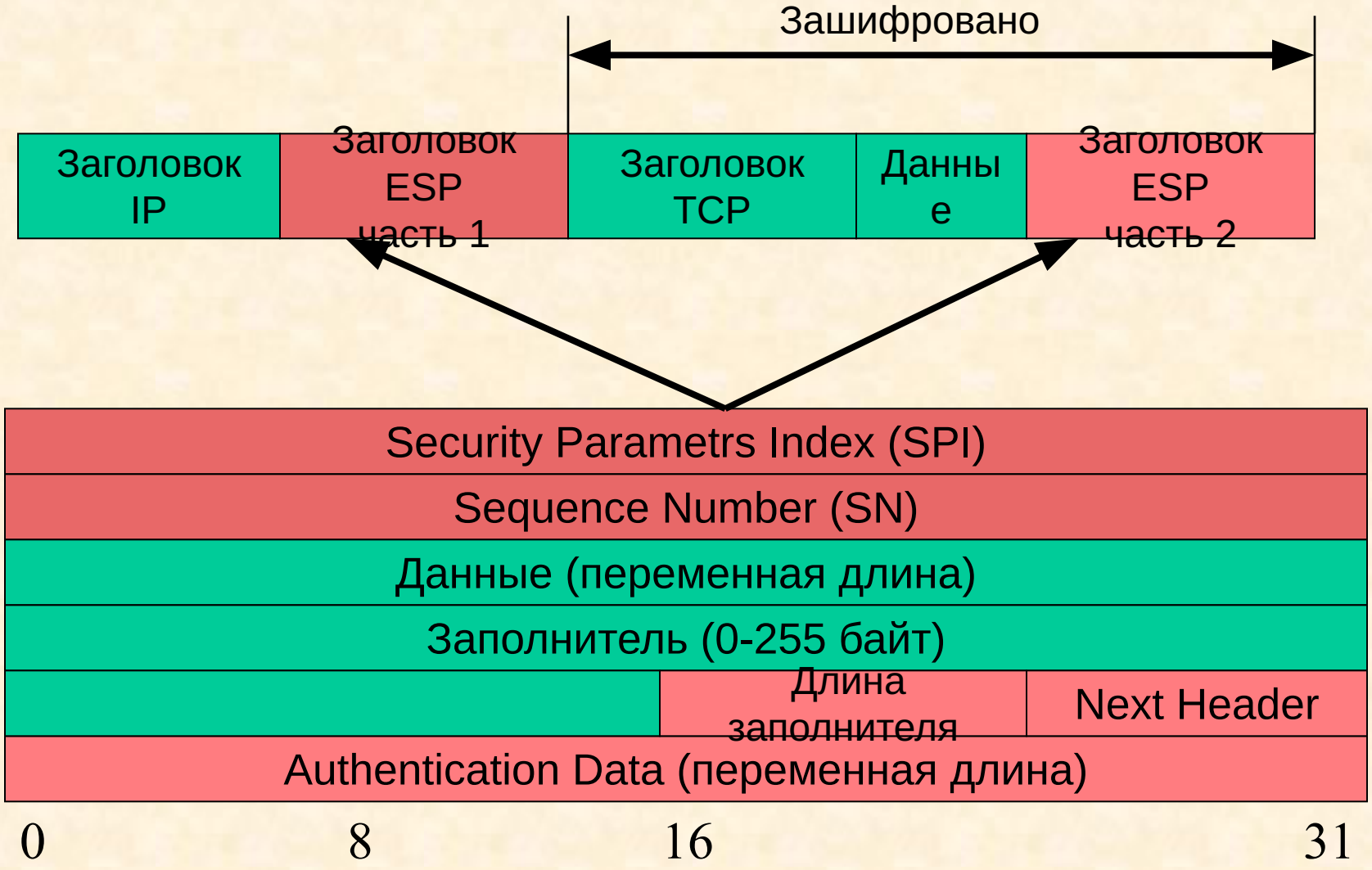
Поле SN

Протокол AH



Поле Authentication Data

Протокол ESP



Протокол ESP

Метка безопасной ассоциации

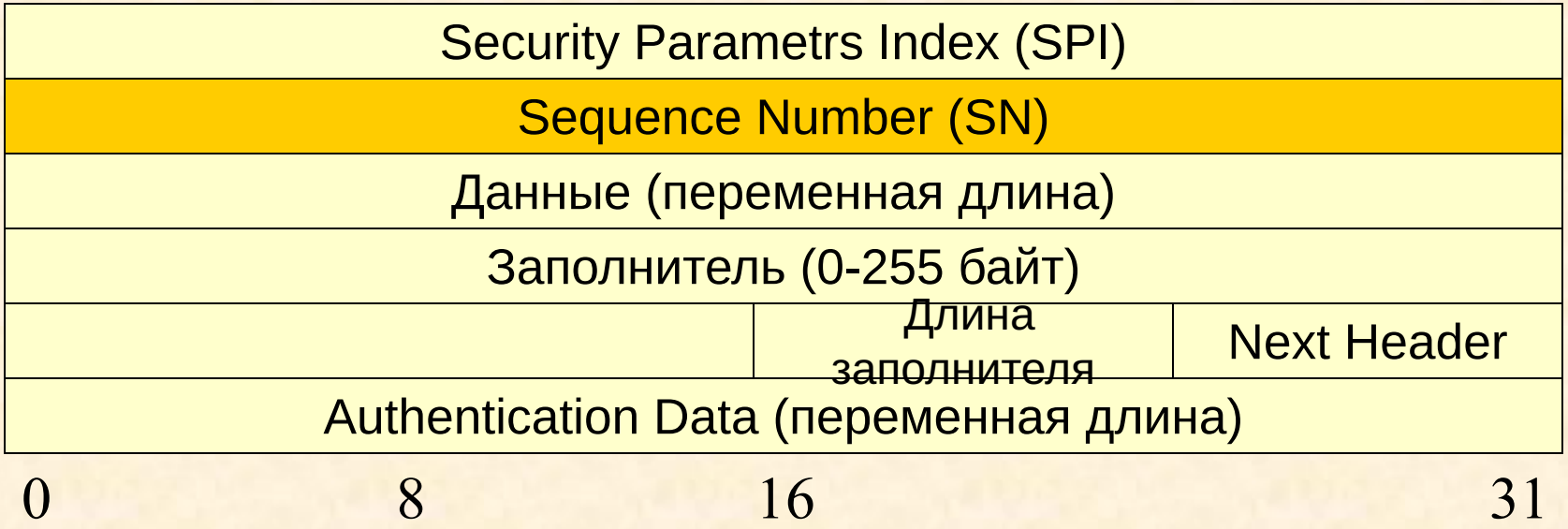
Security Parametrs Index (SPI)		
Sequence Number (SN)		
Данные (переменная длина)		
Заполнитель (0-255 байт)		
	Длина заполнителя	Next Header
Authentication Data (переменная длина)		

0 8 16 31

Поле SPI

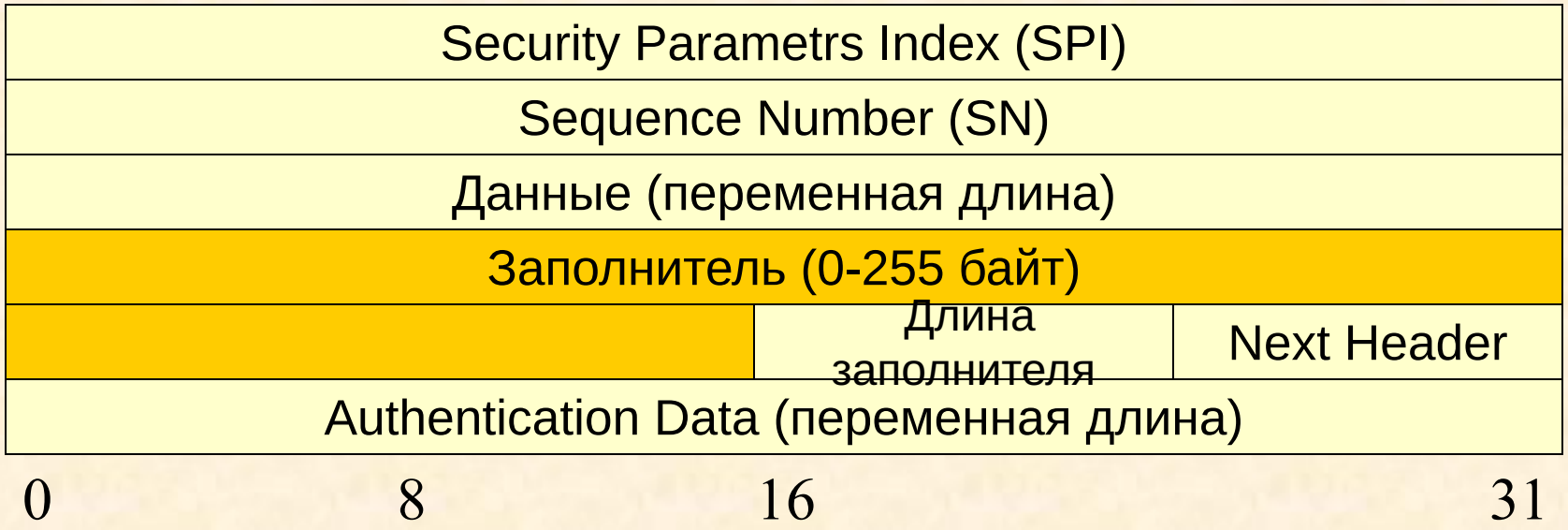
Протокол ESP

Наращивается для каждого следующего пакета



Поле SN

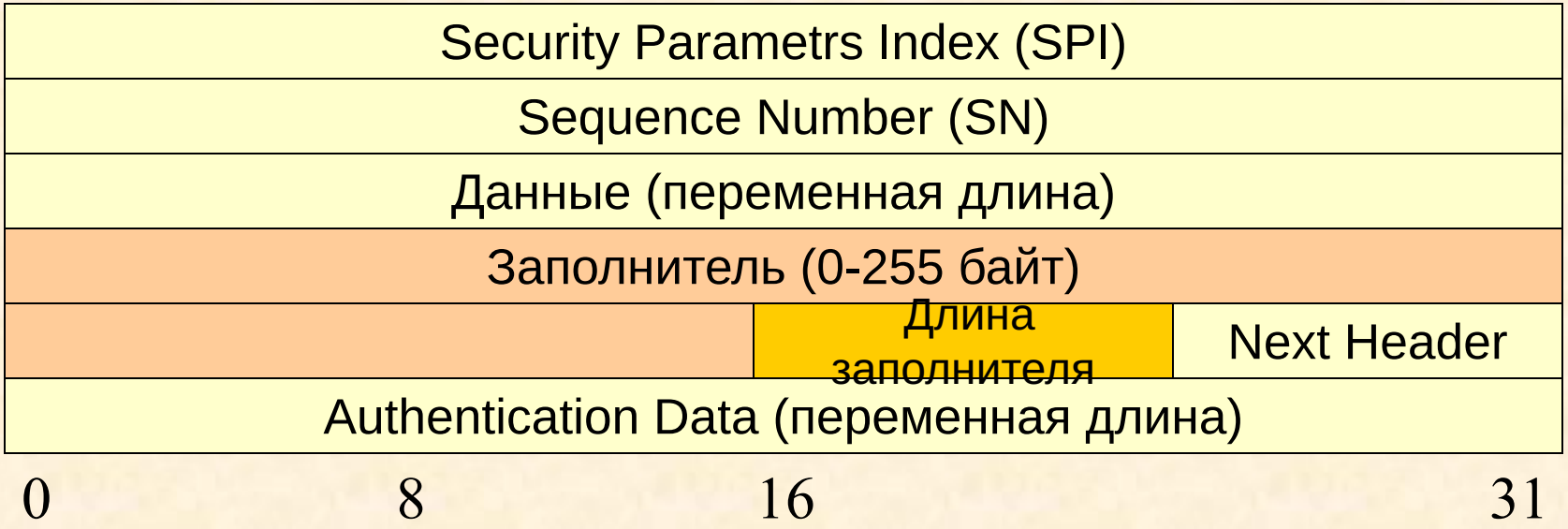
Протокол ESP



- Для правильной работы алгоритмов шифрования
- Для намеренного искажения размера пакета

Поле заполнителя

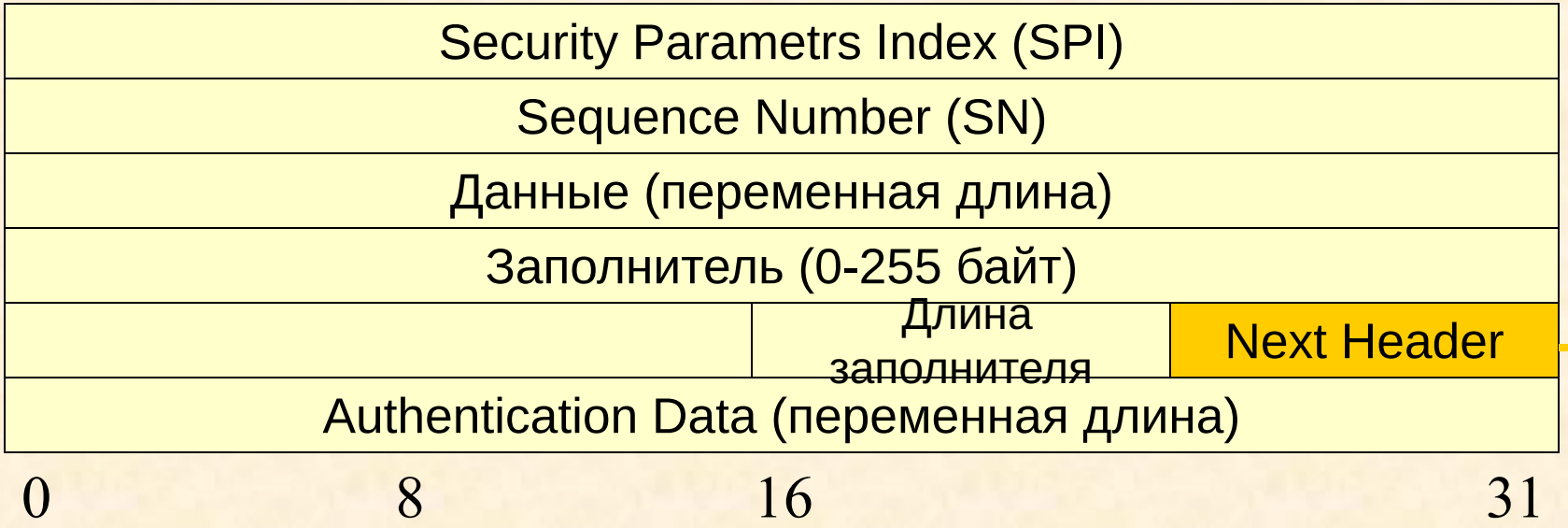
Протокол ESP

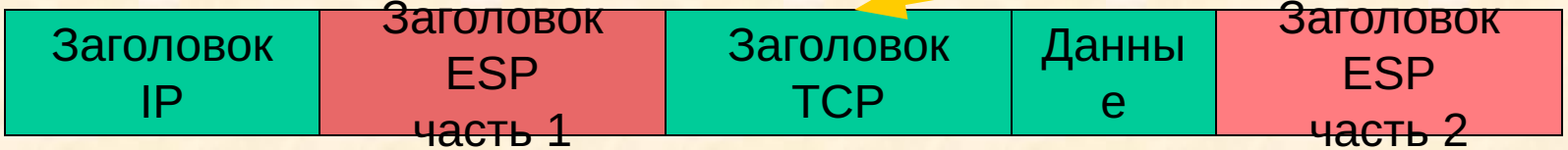


- Длина заполнителя в байтах

Поле длины заполнителя

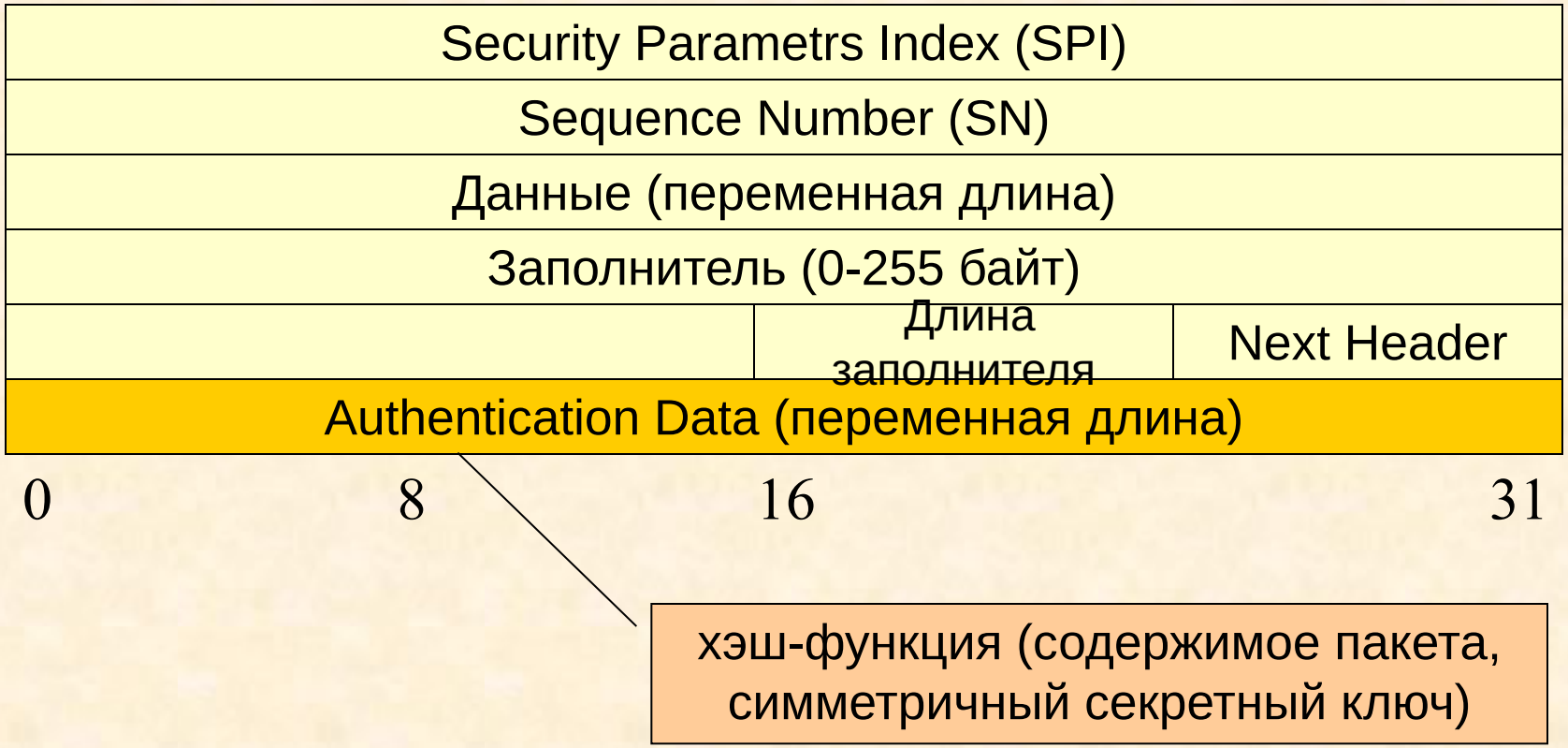
Протокол ESP





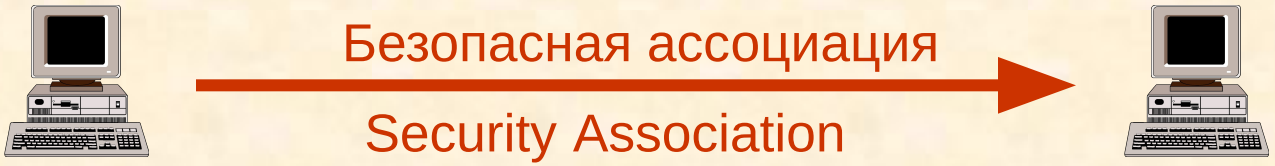
Поле Next Header

Протокол ESP



Поле Authentication Data

Протокол IKE



- 32-разрядный индекс SPI
- IP- адрес узла назначения
- идентификатор протокола защиты (AH или ESP)

Безопасная ассоциация

Протокол IKE

Фаза 1

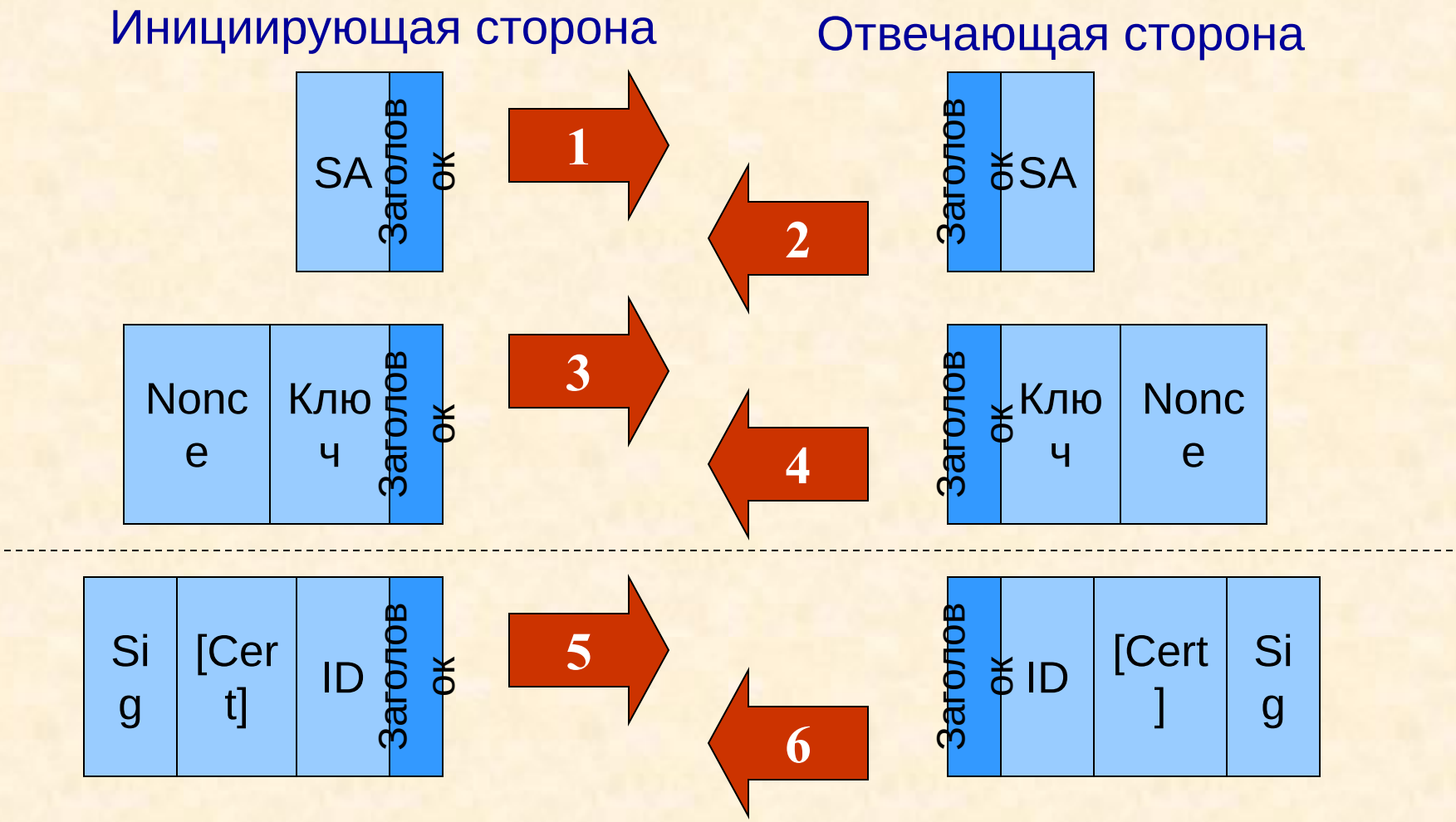
- Установление защищенного соединения для процедуры обмена (IKE SA)

Фаза 2

- Согласование всех параметров, ассоциируемых с общим каналом SA

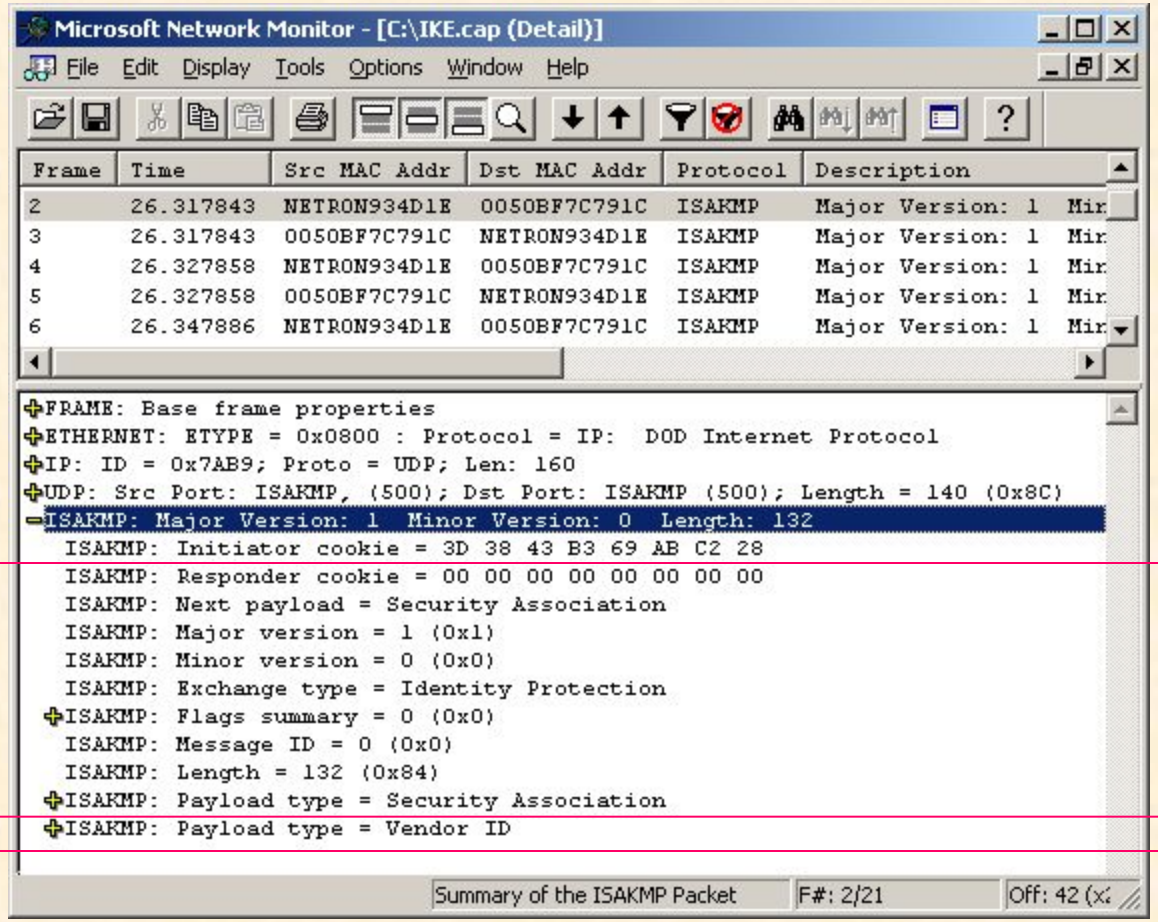
Этапы функционирования протокола IKE

Протокол IKE (фаза 1)



Основной режим установления канала IKE SA

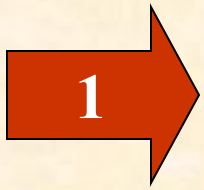
Протокол IKE (фаза 1)



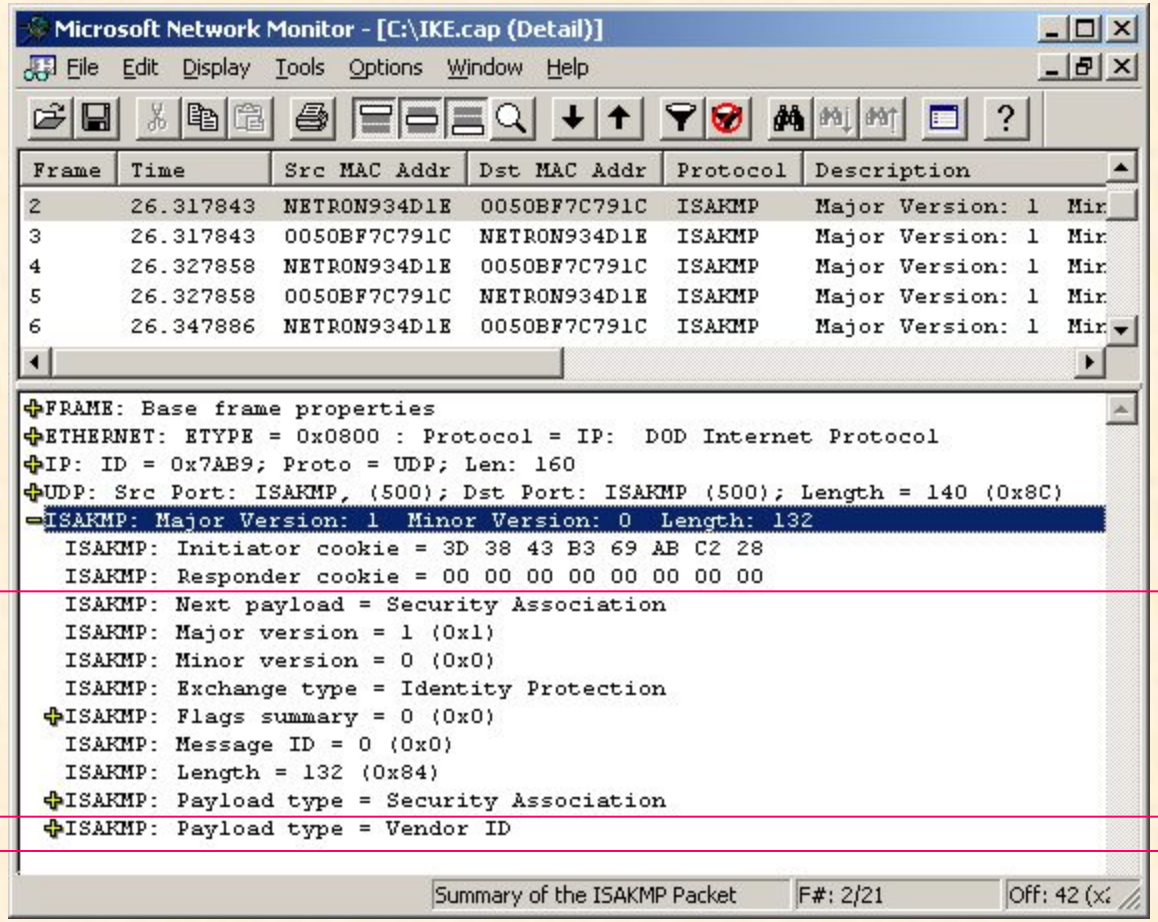
Initiator Cookie

SA

Vendor ID



Протокол IKE (фаза 1)



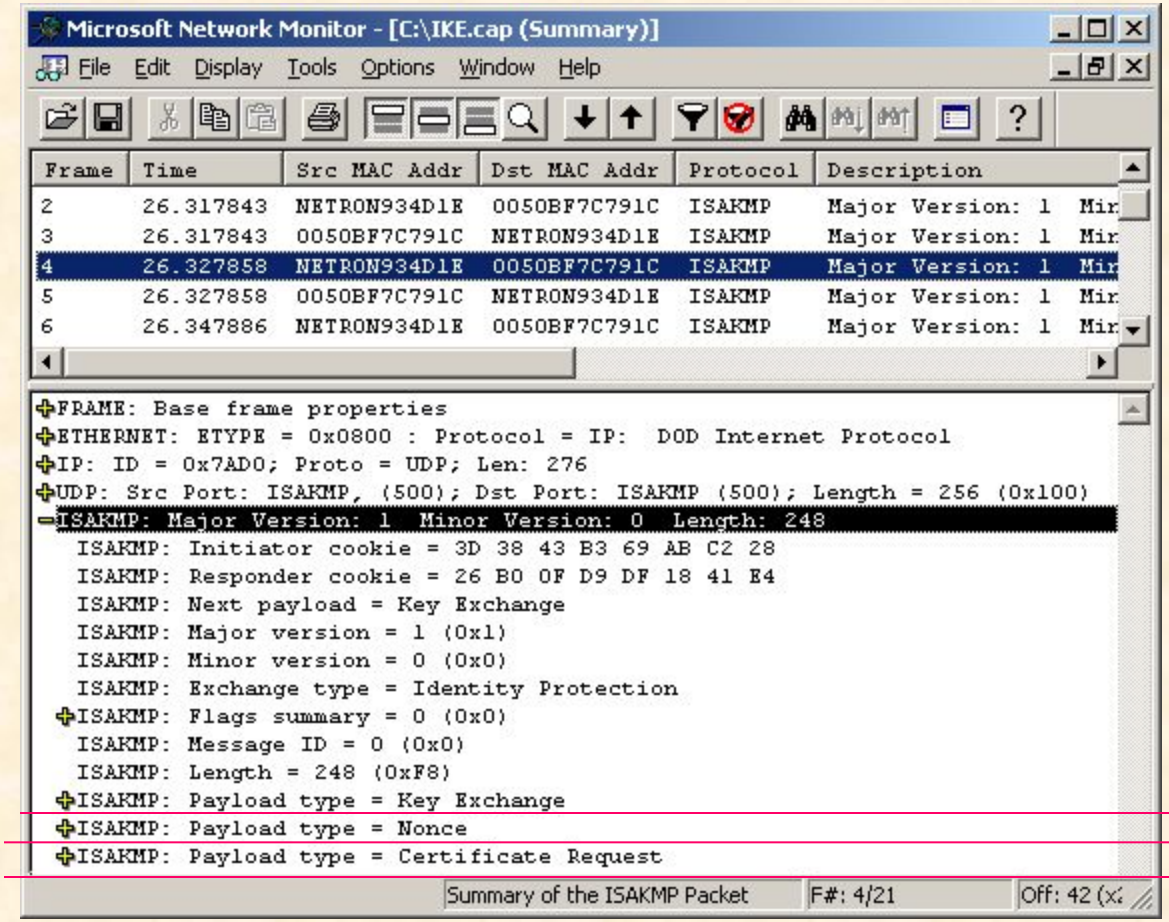
Responder Cookie

SA

Vendor ID

2

Протокол IKE (фаза 1)

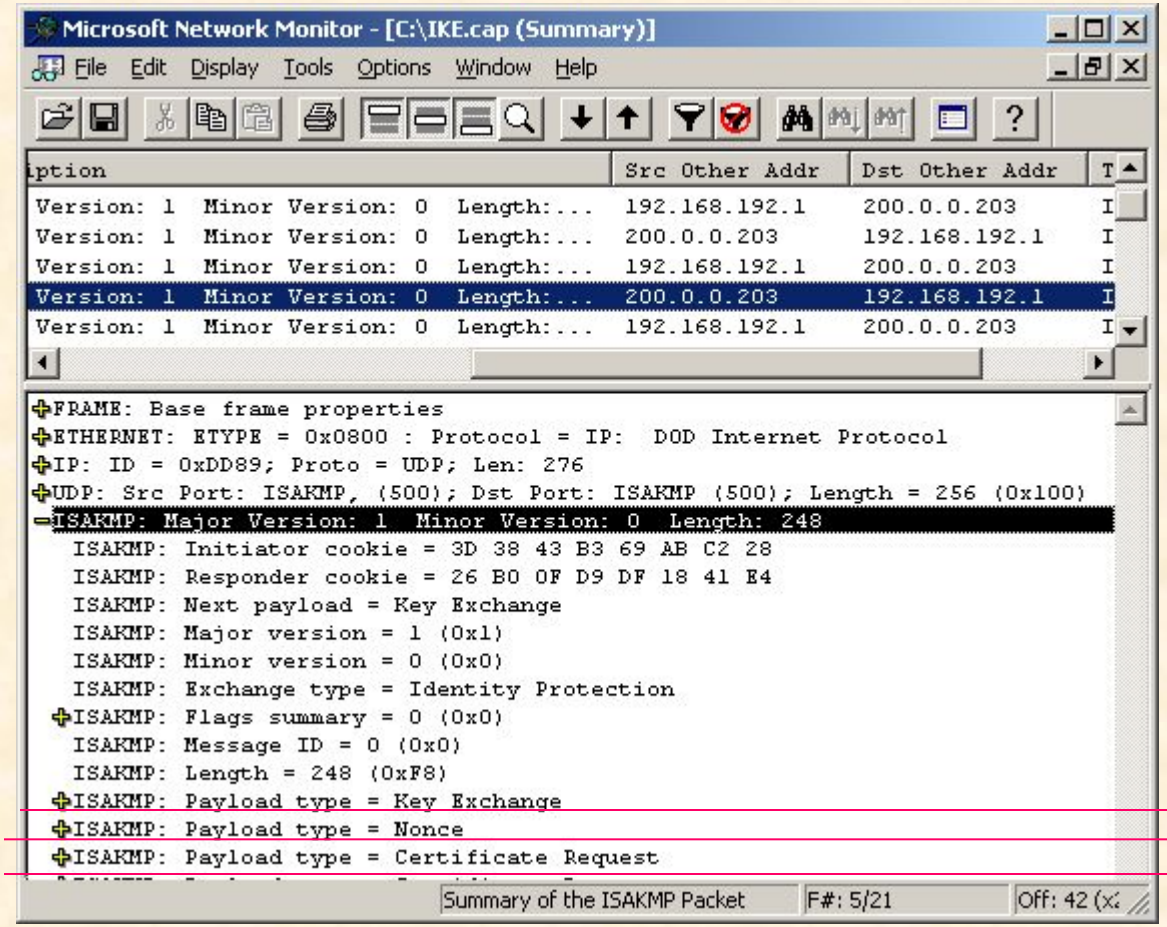


Открытый ключ

Случайное число

Запрос сертификата

Протокол IKE (фаза 1)

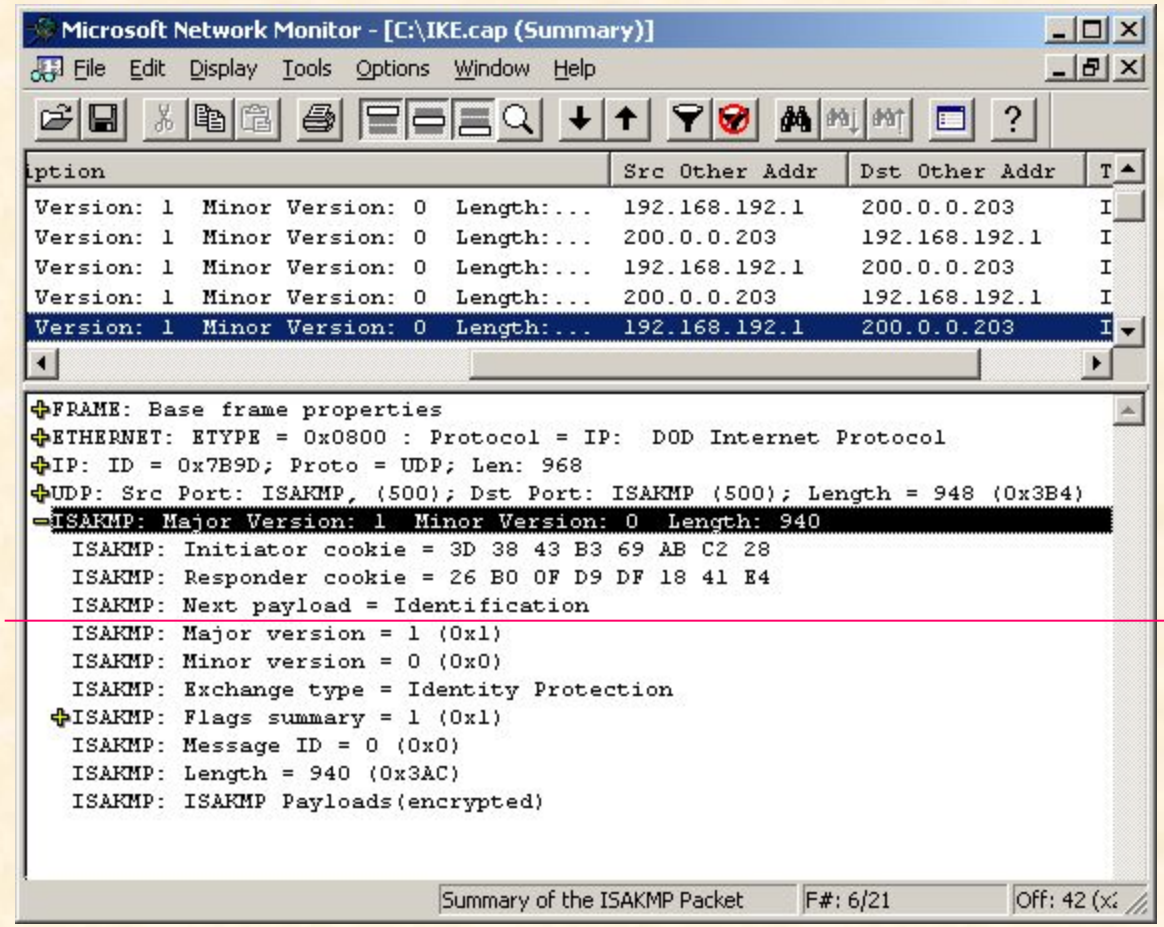


Открытый ключ

Случайное число

Запрос сертификата

Протокол IKE (фаза 1)

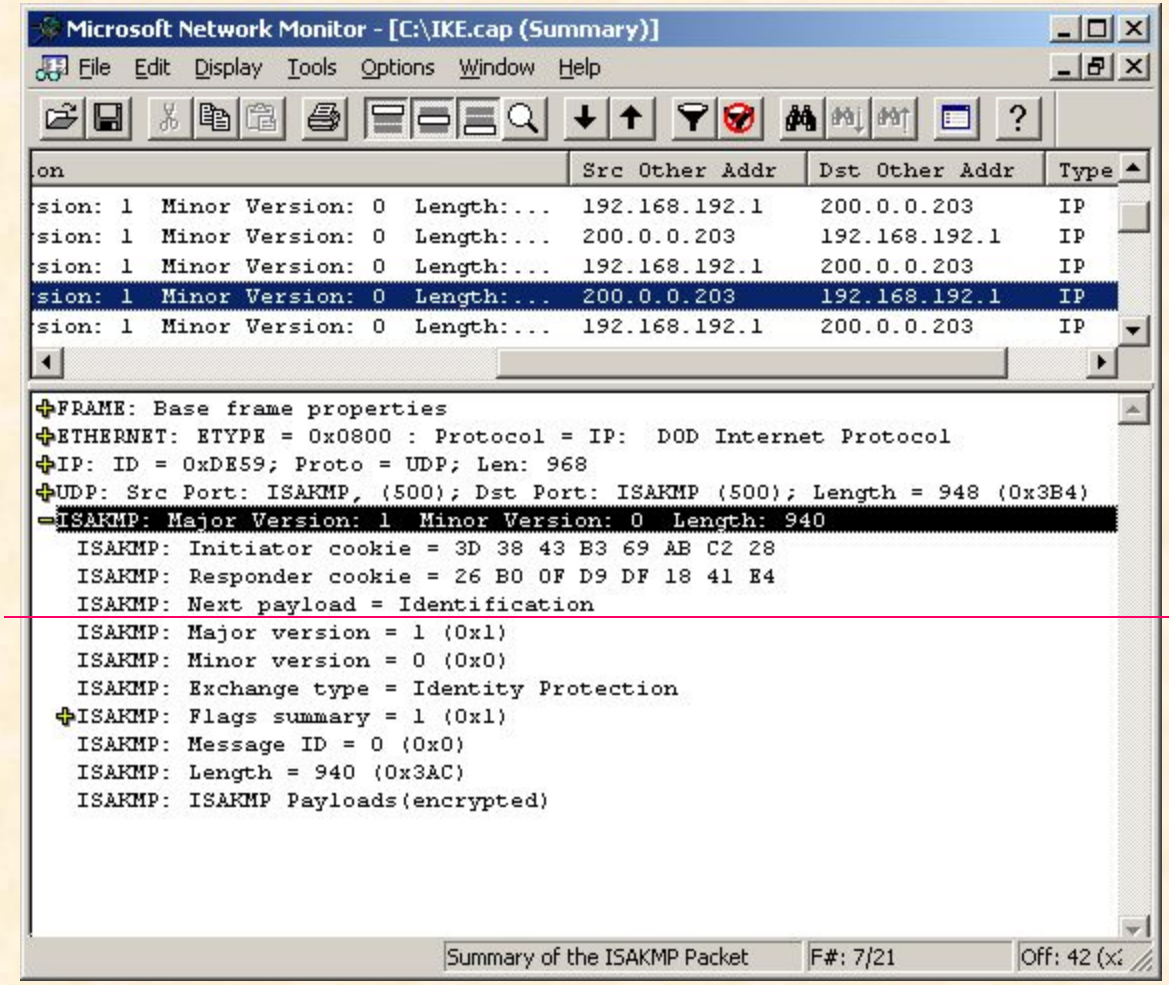


ID

5

В нескольких пакетах

Протокол IKE (фаза 1)



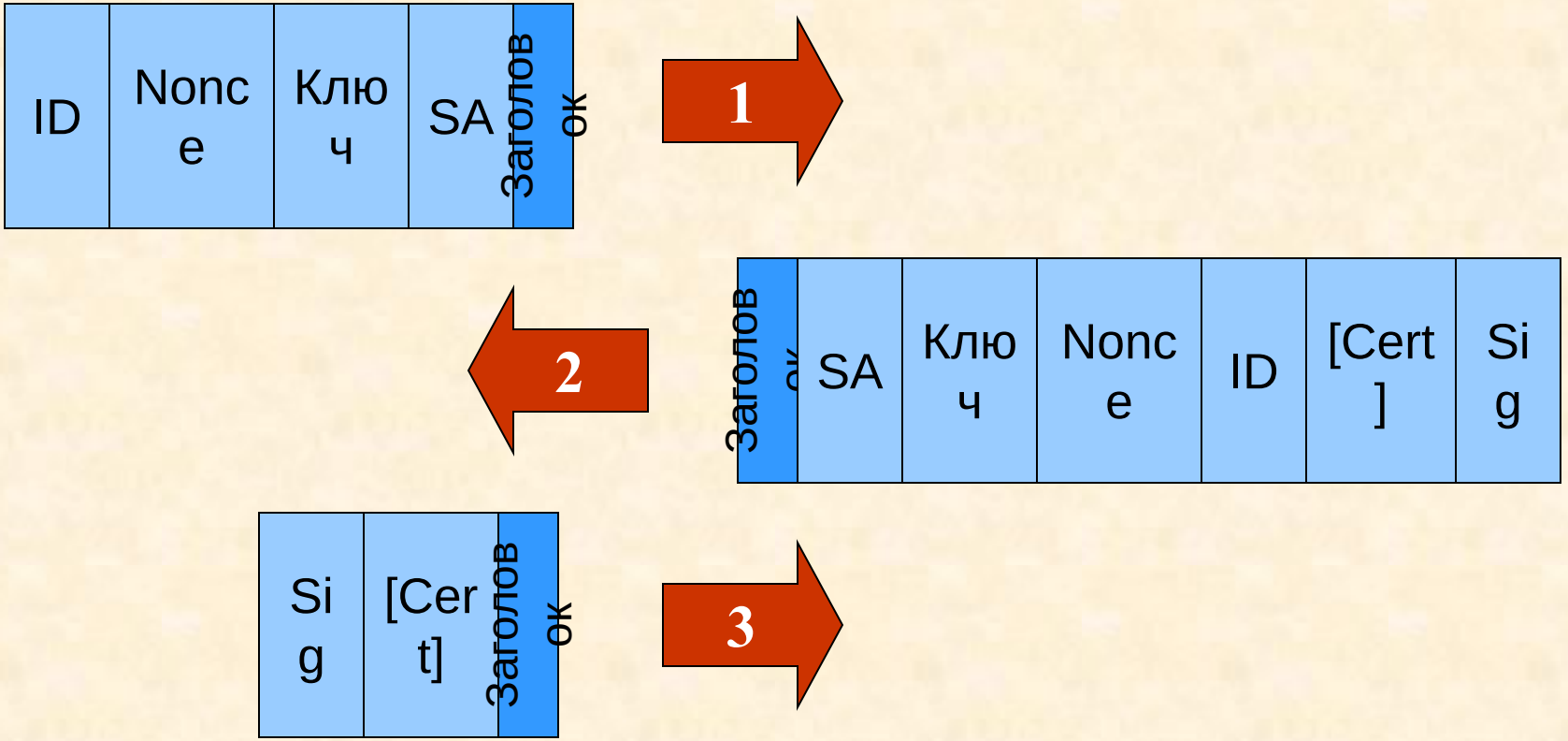
ID

В нескольких пакетах

Протокол IKE

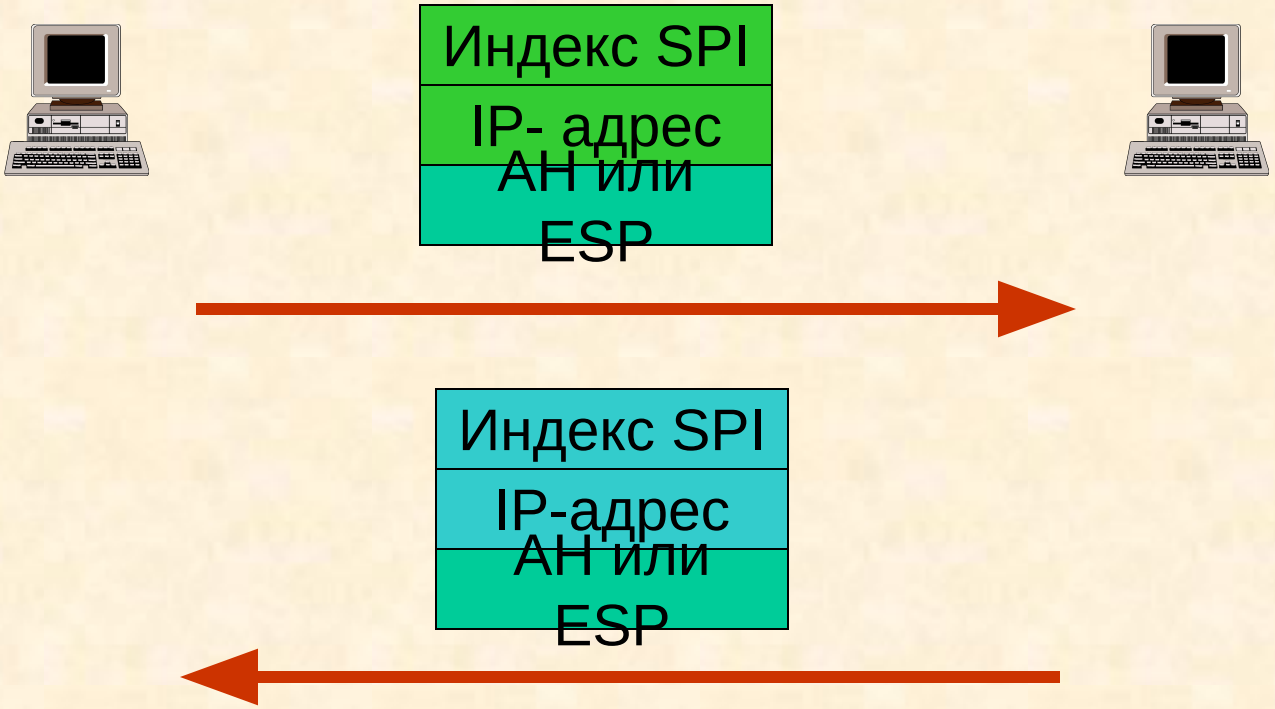
Инициирующая сторона

Отвечающая сторона



Быстрый режим установления канала IKE SA

Протокол IKE



Согласование параметров канала SA

Практическая работа 7
Настройка IPSec

Настройка IPSec средствами ОС Windows 2000